Citrix 虚拟应用和桌面™ 7 2607 LTSR

> **重要提示：**
>
> 当前版本 (CR) 和长期服务版本 (LTSR) 的产品生命周期策略在 生命周期里程碑 中有所述。

> Citrix Virtual Apps and Desktops 提供虚拟化解决方案，用于通过任何网络将应用程序和桌面交付到任何设备，同时增强数据安全性、降低成本并提高生产力。

Citrix Virtual Apps and Desktops 的长期服务版本 (LTSR) 计划为 Citrix Virtual Apps and Desktops 版本提供稳定性和长期支持。

- 有关用例信息，请参阅 `<https://www.citrix.com/products/citrix-virtual-apps-and-desktops/>`。
- 要了解 Citrix Virtual Apps and Desktops 部署中的组件和技术，请参阅 技术概述。

早期版本

其他当前可用版本的文档位于 Citrix Virtual Apps and Desktops。

对于更早的版本，文档已存档在 旧版文档 中。

Citrix 虚拟应用和桌面在 Citrix 云™ 中

Citrix Cloud Virtual Apps and Desktops 产品是 Citrix DaaS。有关详细信息，请参阅 Citrix DaaS。

有用链接

- Citrix 可支持性包
- LTSR 常见问题解答
- Citrix 虚拟应用和桌面服务选项
- 产品生命周期日期
- 适用于 Citrix Workspace 应用程序的 LTSR 计划

新增功能

关于此版本

Citrix Virtual Apps and Desktops™ 7 2607 LTSR 包含新版本的 Windows Virtual Delivery Agent (VDA) 和多个核心组件的新版本。您可以执行以下操作：

- **安装或升级站点**：使用此版本的 ISO 安装或升级核心组件和 VDA。安装或升级到最新版本可让您使用最新功能。
- **在现有站点中安装或升级 VDA**：如果您已有部署但尚未准备好升级核心组件，则仍可通过安装（或升级到）新 VDA 来使用多项最新的 HDX™ 功能。当您想要在非生产环境中测试增强功能时，仅升级 VDA 会很有帮助。

  将 VDA 升级到此版本后，无需更新计算机目录的功能级别。有关详细信息，请参阅VDA 版本和功能级别。

有关安装和升级说明，请参阅：

- 如果您要构建新站点，请按照安装和配置中的顺序操作。
- 如果您要升级站点，请参阅升级和迁移。

受支持版本和旧版本的文档

受支持版本的文档可在 Citrix Virtual Apps and Desktops 中找到。

生命周期结束 (EOL) 版本文档 PDF 已存档在旧版文档中。

版本信息

- 新增功能
- 已修复问题
- 已知问题
- 弃用和删除

新增功能

本文列出了 Citrix Virtual Apps and Desktops™ 7 2607 LTSR 的新增功能和增强功能。更新按组件组织。

Citrix 虚拟桌面助手

以下更新已添加到 2607 LTSR 版本中的 Citrix Virtual Desktop Assistant 应用程序。现在还可以在以下方面优化或监视会话：

- **图形：** 查看 VDA 会话的当前 HDX 图形配置详细信息。有关详细信息，请参阅图形页面。
- **主动通知：** 当会话资源使用率高或配置文件存储空间接近容量时接收警报。有关详细信息，请参阅主动通知。

HDX

设备

PDF 打印增强功能

基于 PDF 的通用打印机驱动程序现在在 VDA 上提供了一个打印机驱动程序 UI，允许用户为自动创建的打印机配置各种打印设置。此外，打印首选项会发送到打印机并由打印机遵守，而不会将文档留在客户端端点上。有关详细信息，请参阅PDF 打印。

FIDO2 诊断工具

VDA 上现已提供一个新的命令行工具 **CtxFido2Diagnostics.exe**，可帮助用户和管理员排查 FIDO2 重定向配置问题。有关详细信息，请参阅FIDO2 诊断工具。

HDX 连接

EDT MTU 重新发现

现已提供新的计算机策略设置 **MTU 重新发现**。使用此设置可配置 EDT MTU 重新发现。有关详细信息，请参阅Enlightened Data Transport。

Microsoft Entra 单点登录

适用于 Entra 混合加入会话主机的 Microsoft Entra 单点登录现已正式发布。

您还可以使用Microsoft Entra 单点登录计算机策略设置 在会话主机上启用或禁用此功能。

Web 登录 (预览)

您可以启用基于 Web 的登录来登录或解锁您的 Entra 混合加入虚拟桌面。有关详细信息，请参阅 Web 登录。

已发布的应用程序

关闭已发布的应用程序后断开会话

现在可以将应用程序关闭行为从注销用户更改为断开会话。有关详细信息，请参阅 会话管理配置。

Web 工作室

通过搜索和排除列表更快地选择域

现在，在 Web Studio 中查找 Active Directory 域和组织单位 (OU) 更快了。在创建计算机目录期间，当您选择**创建新的 Active Directory 帐户**时，可以直接从**位置（域）**下拉列表中搜索特定域，而无需浏览受信任域的完整列表。

您还可以通过在**设置 > 站点设置**中将无法访问或不必要的域添加到域排除列表来提高域查找性能。Web Studio 会在将来的查询中自动跳过排除的域，从而使“位置（域）”下拉列表和其他域查找的响应速度更快。有关详细信息，请参阅 配置域排除列表。

Amazon WorkSpaces Core 托管实例的灵活计费

现在，在使用 Citrix MCS 预配 Amazon WorkSpaces Core 托管实例时，您可以选择按月（固定费率）和按小时（即用即付）计费模式。

这种灵活性使您能够根据特定的工作负载要求和使用模式优化计算成本。

对于持久性桌面，请使用按月计费模式以受益于可预测的固定费率定价；对于按需或间歇性工作负载，请使用按小时计费。

此功能要求您的 AWS 账户已配置为 Amazon WorkSpaces 计费服务。

有关详细信息，请参阅灵活计费。

思杰 迪莱克特

Citrix DaaS MCP Server Local 现已推出预览版

Citrix Virtual Apps and Desktops 现在包含一个模型上下文协议 (MCP) 服务器，可将支持 MCP 的 AI 代理连接到您的 Citrix Delivery Controller。管理员可以使用 AI 代理查询和排查其 Citrix Virtual Apps and Desktops 站点，包括检索有关交付组、计算机状态和运行状况、会话性能、会话登录等详细信息。有关详细信息，请参阅 Citrix DaaS MCP Server Local。

阿穆莱特 热键 核心工作站

适用于 Amulet Hotkey CoreStation HX2000 的电源管理正式发布

适用于 Amulet Hotkey CoreStation HX2000 的电源管理正式发布。借助此功能，Citrix 通过 Amulet Hotkey CoreStation 插件管理您的 Amulet Hotkey CoreStation 工作负载。借助此插件，您可以创建与 Amulet Hotkey CoreStation 设备的托管连接、创建计算机目录，并使用 PowerShell 命令和 Studio 对计算机进行电源管理。

有关详细信息，请参阅：

- Amulet Hotkey CoreStation 虚拟化环境
- 连接到 Amulet Hotkey CoreStation
- 电源管理 Amulet Hotkey CoreStation VM
- 创建 Amulet Hotkey CoreStation 计算机目录
- 使用令牌注册 WebSocket Amulet Hotkey CoreStation VDA

Citrix 预配™

有关新功能的信息，请参阅其自己的文档中的新增功能文章。

适用于 macOS 的 Citrix 虚拟投递代理

有关新功能的信息，请参阅其自己的文档中的新增功能文章。

联合身份验证服务

有关新功能的信息，请参阅其自己的文档中的新增功能文章。

配置文件管理

有关新功能的信息，请参阅其自己的文档中的新增功能文章。

会话录制

有关新功能的信息，请参阅其自己的文档中的新增功能文章。

已修复的问题

> **注意：**

此版本及后续版本中包含对 Citrix Virtual Apps and Desktops™ 早期版本中问题的修复。

常规

- 当在服务器获取客户端渲染模式下使用浏览器内容重定向时，即使登录页面成功加载，手动基于表单的登录也可能失败。
- 当在地址栏中启用 Google Chrome 的实验性 AI 栏并使用浏览器内容重定向时，重定向页面的顶部中心部分可能会出现剪裁并变得无法交互。
- 当使用集成 Windows 身份验证 (IWA) 单点登录的浏览器内容重定向时，导航到 BCR ACL 策略中包含的 HTTP URL 时，WebSocketAgent 进程可能会崩溃。

计算机创建服务™

- 通过 Nutanix AHV Prism Central 连接更新 MCS 非持久性计算机目录的启用 vTPM 的主映像会触发 VM 重新创建，这可能会使 DNS 预留失效，并需要重新注册利用 MAC 地址进行许可的软件。
- 当您使用已安装并载入 Azure Connected Machine 代理版本 1.61 或更高版本的 Azure 本地 VM 准备主映像时，由于删除代理配置文件时访问被拒绝，MCS 中的目录创建在映像准备过程中失败。作为一种解决方法，在创建主映像时执行以下操作：导航到 `C:\ProgramData\AzureConnectedMachineAgent\Config\agentconfig.json`，右键单击该文件，选择“**属性**”，然后清除“**只读**”属性复选框。
- 使用 Nutanix AHV Prism Central 主机连接向 MCS 目录添加大量 VM 可能会失败并显示 `OutOfMemory` 错误。为避免此问题，请减少单批次创建的 VM 数量。我们建议一次最多添加 10 个 VM。
- 将现有 VDA 升级到版本 2511 后，`MachineGuid` 会更改为计算机的唯一值。任何依赖 `MachineGuid` 进行许可的软件可能需要重新注册。

配置文件管理

- Profile Management 2607 LTSR documentation 提供了有关此版本更新的特定信息。

会话录制

- Session Recording 2607 LTSR documentation 提供了有关此版本更新的特定信息。

Citrix 置备™

- Citrix Provisioning 2607 LTSR documentation 提供了有关此版本更新的特定信息。

工作区环境管理™

- Workspace Environment Management 2607 documentation 提供了有关此版本更新的特定信息。

联邦身份验证服务

- Federated Authentication Service 2607 LTSR documentation 提供了有关此版本更新的特定信息。

已知问题

Citrix Virtual Apps and Desktops™ 7 2607 LTSR 包含以下已知问题：

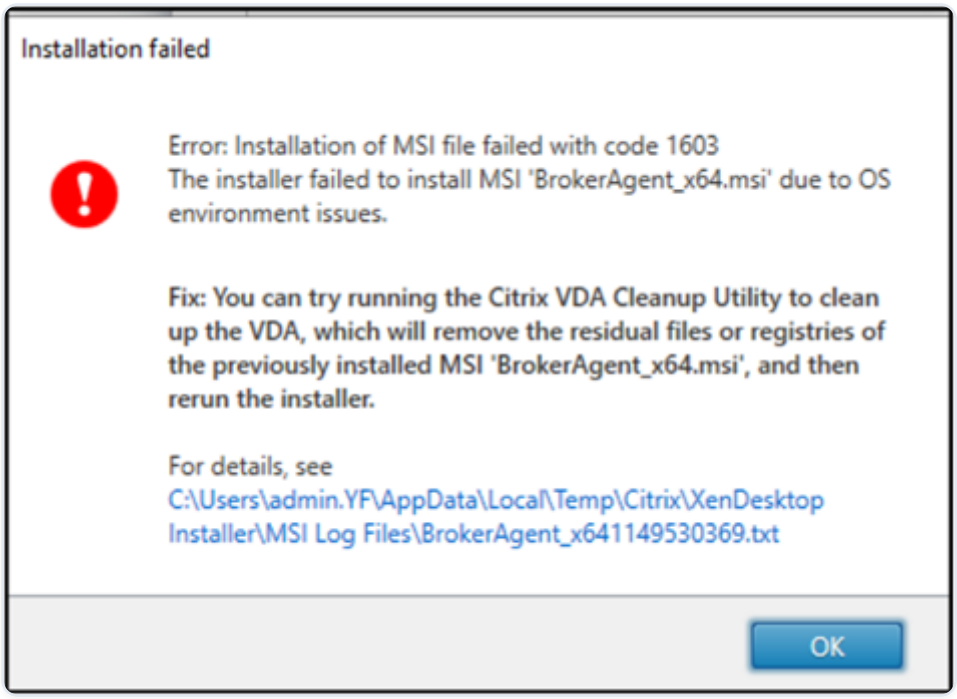
备注

- 如果已知问题有变通方法，则会在问题描述之后提供。
- 以下警告适用于任何建议更改注册表项的变通方法：

> **警告：**
>
> 不正确地编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix® 无法保证可以解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。在编辑注册表之前，请务必备份注册表。

常规

- 在 Windows 10 (22H2) 和 Windows Server 2022 平台上安装 Citrix VDA 期间，您可能会遇到以下错误。



此外，在 broker agent msi 日志中，您可能会看到以下错误消息：

```
MSI (s) (04:D8) [09:46:08:426]: Note: 1: 1722 2: CA_RunInstallAgent 3:
C:\Program Files\Citrix\Virtual Desktop Agent\BrokerAgent.exe 4:
-install

CustomAction CA_RunInstallAgent returned actual error code 1701 (note
this may not be 100% accurate if translation happened inside sandbox)

MSI (s) (04:D8) [09:46:08:427]: Product: Citrix Virtual Desktop Agent -
x64 -- Error 1722. There is a problem with this Windows Installer
package. A program run as part of the setup did not finish as expected.
Contact your support personnel or package vendor. Action
CA_RunInstallAgent, location: C:\Program Files\Citrix\Virtual Desktop
Agent\BrokerAgent.exe, command: -install
```

要解决此问题，请关闭安装程序，重建 Windows 性能计数器，重新启动计算机，然后再次执行安装。有关信息，请参阅 Microsoft 文档 Manually rebuild performance counters for Windows Server 2008 64 bit or Windows Server 2008 R2 systems。

- 如果您启动应用程序栏，然后在适用于 Windows 的 Citrix Workspace™ 应用程序中打开“连接中心”菜单，则应用程序栏不会显示在其托管服务器下方。
- 对于多会话 VDA，**会话限制**设置在运行 Windows Server 2022、Windows 10 企业版多会话和 Windows 11 企业版多会话的会话主机中不适用。

- Microsoft 确认，在使用现代打印对话框时，打印作业之间保留打印设置存在问题，他们正在努力解决。他们目前的预计是 2025 年上半年。现代打印对话框在较新的操作系统版本（例如 Windows 11 和 Windows Server 2025）中默认启用。可以通过执行以下操作将操作系统配置为使用传统打印对话框：

  a. 打开注册表编辑器。

  b. 转到 `HKEY_CURRENT_USER\Software\Microsoft\Print\UnifiedPrintDialog`

  c. 右键单击并选择**新建 > DWORD (32 位) 值**

  d. 将值重命名为 **PreferLegacyPrintDialog**。

  e. 右键单击 **PreferLegacyPrintDialog** 并选择**修改**。

  f. 将值数据设置为 `1` 并单击**确定**。

- 通过 RDP 重新连接到单会话 VDA 时，客户端打印机未被清除。

  在单会话计算机上，当用户使用 RDP 重新连接到同一台计算机时，来自先前 ICA 会话的重定向客户端打印机不会被删除。因此，过时的客户端打印机在会话中仍然可见，但不再起作用。这不影响多会话 VDA。

- 在 Citrix Virtual Apps and Desktops 会话期间，如果支持音频播放的客户端显示器断电重启（先关闭再打开），VDA 的声音控制面板 (mmsys.cpl) 中显示器的音频播放设备名称会从其正确的特定名称更改为“Citrix HDX Audio”。这是一个间歇性问题。作为一种解决方法，请关闭 VDA 的声音控制面板 (mmsys.cpl) 窗口，然后重新启动它。

- 尝试从发布在 Windows Server 2019 Virtual Delivery Agent (VDA) 上的某些应用程序中添加新打印机时，会发生错误，导致打印机无法列出或添加。具体来说，会出现一条错误消息，指示无法访问 `rundll32.exe`。

  作为一种变通方法，请使用应用程序中已可见的打印机，或添加打印机使其在当前会话中可用。

- 如果在会话处于活动状态时更改了客户端计算机上的设备名称，则新名称不会立即反映在会话设置中。此行为会影响播放设备和录制设备。

  作为一种变通方法，要查看更新的设备名称，您必须断开会话连接，然后重新连接。或者，注销会话并重新登录也可以解决此问题。

- 当多个 Chrome 浏览器选项卡（包括那些配置了浏览器内容重定向 (BCR) 的选项卡）同时从一个 Chrome 窗口拖放到另一个窗口时，重定向的内容可能会出现意外行为。

- 如果将包含视频内容的选项卡移动到新窗口，播放可能会停止或视频可能不会显示。

- 将浏览器内容重定向与浏览器配置文件共享结合使用时，不支持具有多个配置文件的 SSO 持久性。

- Windows 11 具有一项新的 UI 功能，可将窗口吸附到桌面。当用户拖动窗口时，桌面上方会出现一个特殊的工具栏。因此，多媒体叠加剪裁逻辑会剪裁顶部/中心区域，这可能是因为此功能使用了新的不可见/透明窗口。

  作为一种变通方法，请参阅：

  - “贴靠窗口”部分。
  - 如何禁用“贴靠窗口”功能

- **在已安装 Citrix VDA 的计算机上进行就地 Windows 升级后，打印可能会失败** 进行就地 Windows 升级后，Citrix 打印提供程序可能不再被调用，这可能导致打印失败。出现此问题的原因是 Windows 升级过程会重置打印提供程序执行顺序，并且不会保留 Citrix 注册的提供程序。Microsoft 已确认这是 Windows 的行为，并且目前在升级期间不会保留执行顺序中的提供程序注册。

解决方法是将打印提供程序重新添加到相应的注册表位置。

```
1.  Open the Registry Editor.

1.  Go to `HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Print\Providers`

1.  Right-click **order** and select **Modify**.

1.  Add the values `Universal Printer` and `Client Printer` above any
other providers.

1.  Reboot the VDA.
```

- 任何使用 MCSIO 写入缓存进行存储优化的目录，请务必在 VDA 安装和升级过程中安装 Citrix MCS I/O 驱动程序。有关详细信息，请参阅 Storage shared by hypervisors 和 Configure cache for temporary data。VDA 上缺少 MCS I/O 驱动程序可能会在更新目录时导致问题。
- 当您尝试使用 Citrix 工具栏从锁定的 Windows 会话注销时，操作失败。此问题在适用于 Linux 的 Citrix Workspace 应用程序 (CWA) 和适用于 Windows 的 CWA 上均会发生。

作为一种变通方法，请确保在尝试断开连接或注销之前 Windows 会话已解锁。如果会话已解锁，断开连接和注销功能将正常工作。

音频

- 当音频设备（例如耳机）通过 USB 重定向通用重定向到 Windows Server 虚拟投递代理 (VDA)（例如 Windows Server 2019 或 2022），并且同一 VDA 上有多个用户会话同时处于活动状态时，单击任务栏右下角的音量图标以调整设置可能会导致 Windows `ShellExperienceHost.exe` 进程意外崩溃。此问题主要发生在音频设备未主动重定向，但同一 VDA 上的另一个会话正在使用通用 USB 音频重定向的会话中。

  作为一种变通方法，通过任务管理器在受影响的会话中重新启动 Windows 资源管理器进程 (explorer.exe)。这可能允许音量图标正常工作而不会崩溃。

机器创建服务™

- 当使用具有多个启用了加速网络的网络接口卡 (NIC) 的计算机配置文件时，请确保所选的 VM 大小支持所有 NIC 上的加速网络。某些 Azure VM 大小（例如 Standard_D2ads_v5）将加速网络限制为单个 NIC。如果计算机配置文件在超出 VM 大小允许的 NIC 数量上启用了加速网络，则计算机将无法开机并显示错误 `VmSizeRestrictedToSingleNicWithAcceleratedNetworkingEnable`。要解决此问题，请选择支持多个 NIC 上的加速网络的 VM 大小，或更新计算机配置文件以仅在一个 NIC 上启用加速网络。
- 如果环境依赖于从主映像继承的通配符证书，则 VDA 版本 2511 上的 TLS 加密会中断。

  作为单会话计算机的解决方法，可以使用每台计算机证书代替。有关详细信息，请参阅 在 VDA 上启用 TLS / DTLS。
- 使用 `InstanceType` 创建的 VM 不支持作为 Red Hat OpenShift 环境中的主映像。
- 在 Red Hat OpenShift 虚拟化环境中创建 MCS 计算机目录时，不能使用具有不同操作系统类型的主映像和计算机配置文件。这是由于 Red Hat OpenShift 管理每种操作系统类型的方式所致。因此，不支持将 Windows VM 用作主映像，而将非 Windows（例如 Linux）VM 用作计算机配置文件，反之亦然。
- 在 AWS 上托管的 VMware 环境中，如果主映像启用了 vTPM，则 MCS 计算机目录创建会失败。此问题影响所有 Citrix Virtual Apps and Desktops 版本，并且是由于 VMware 环境中的问题引起的。如需帮助，请联系 VMware 支持。
- 当将 Machine Creation Services I/O (MCSIO) 与运行 VDA 2607 的 Windows Server 2019 VDA 结合使用时，写入缓存磁盘已成功附加到预配的虚拟机，但仍为空，并且未按预期使用。

  仅在以下情况下观察到此问题：

  - VDA 操作系统为 Windows Server 2019
  - 已安装 VDA 2607

- 计算机目录是使用 MCSIO 预配的

解决方法

在预配计算机之前，在主映像上配置所需的 CVhdFilter 注册表设置。 注册表位置：`HKLM\SYSTEM\CurrentControlSet\Services\CVhdFilter`

解决步骤

a. 在 Windows Server 2019 主映像上，打开注册表编辑器 (regedit.exe)。
b. 导航到：HKLM\SYSTEM\CurrentControlSet\Services\CVhdFilter
c. 右键单击 CVhdFilter 并创建一个新的空键“Parameters”。
d. 重新封装或关闭主映像。
e. 创建主映像的新快照。
f. 更新 MCSIO 计算机目录以使用新快照。
g. 重启已预配的虚拟机。
h. 验证回写缓存 (WBC) 磁盘在正常用户会话活动期间是否已填充。

受影响的版本

- Citrix 虚拟投递代理 (VDA) 2607
- Windows 服务器 2019
- 计算机创建服务 I/O (MCSIO)

配置文件管理

- Profile Management 2607 LTSR 文档 提供了有关此版本中更新的具体信息。

适用于 macOS 的 Citrix 虚拟投递代理

- 适用于 macOS 的 Citrix Virtual Delivery Agent 2607 LTSR 文档

会话录制

- Session Recording 2607 LTSR 文档 提供了有关此版本中更新的具体信息。

工作区环境管理™

- Workspace Environment Management 2607 文档 提供了有关此版本中更新的具体信息。

Citrix 预配™

- Citrix Provisioning 2607 LTSR 文档 提供了有关此版本中更新的具体信息。

联合身份验证服务

- Federated Authentication Service 2607 LTSR 文档 提供了有关此版本中更新的具体信息。

弃用和删除

本文中的公告旨在提前通知您即将淘汰的平台、Citrix® 产品和功能，以便您能够及时做出业务决策。Citrix 会监控客户使用情况和反馈，以确定何时将其撤回。公告可能会在后续版本中发生变化，并且可能不包括所有已弃用的功能。

有关产品生命周期支持的详细信息，请参阅产品生命周期支持策略文章。有关长期服务版本 (LTSR) 服务选项的信息，请参阅 `<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX205549>`。

下表显示了已弃用或已删除的平台、Citrix 产品和功能。**粗体**日期表示此版本中的更改。

弃用

弃用意味着我们打算从未来版本中删除该功能或特性。该功能或特性将继续工作并获得全面支持，直到其被正式删除。此弃用通知可能持续数月或数年。删除后，该功能或特性将不再起作用。此通知旨在为您提供充足的时间来规划和更新代码，然后才删除该功能或特性。如果可能，将建议弃用项的替代方案。

项目	弃用版本	替代方案
Windows 10 上的 VDA 支持	2607	升级到最新的 Windows 版本。
Windows Server 2019 上的 VDA 支持	2607	升级到最新的 Windows Server 版本。
Studio 中的 **上次启动时间 (UTC)** 列以及 **Get-ProvVM** 和 **Get-ProvVMDetails** 响应中的 **LastBootTime** 字段	2607	-

项目	弃用版本	替代方案
每个交付组的许可证覆盖（多类型许可）	2603	Citrix Virtual Apps and Desktops 仅使用站点级许可证设置。交付组覆盖将被忽略，并且“创建和编辑交付组”向导中的“许可证分配”步骤已删除。有关详细信息，请参阅多类型许可。
App-V 完整基础架构的 Studio UI 选项	2603	迁移到 App-V 单管理员模型
零延迟文本，也称为本地文本回显	2603	
支持通过 UDP 传输音频 (通过 UDP 传输音频的实时传输和音频 UDP 端口范围)	2511	将 自适应音频 与 EDT 音频容错模式 结合使用。需要以下最低版本。 虚拟投递代理 • 视窗 2308 • 琳纳克斯 2411 • Mac 2411 Citrix Workspace 应用程序： • 视窗 2309 • 琳纳克斯 2402 • Mac 2402
音频质量 设置（以及对旧版音频编解码器的支持）	2511	使用 自适应音频。需要以下最低版本。

项目	弃用版本	替代方案
		虚拟投递代理 • 视窗 2109 • 琳克斯 2112 • Mac 2411 Citrix Workspace 应用程序 • 视窗 2109 • 琳克斯 2109 • Mac 2109
本地应用程序访问 (LAA)	2511	LAA 没有直接的替代方案。建议客户改为在 VDA 上安装来自端点的本地安装应用程序。LAA 将在 2402 LTSR 或 2507 LTSR 上受支持，直到其维护结束。随着此弃用，Microsoft Internet Explorer 和 Firefox 的本地应用程序访问扩展也已弃用。
HTML5 多媒体重定向	2511	浏览器内容重定向
基于文件的许可	2507	License Activation Service (LAS) 是 Citrix 产品套件中产品激活的下一代技术。使用基于文件的许可的客户需要在 April 15, 2026 之前升级到兼容版本并执行此技术转换。在 April

项目	弃用版本	替代方案
		15, 2026 之后，LAS 将是激活和许可 Citrix 本地组件的唯一方式。
支持 `Get-BrokerMachine`	2507	使用 `Get-BrokerMachineV2`
支持**通用打印优化默认值**策略设置的“图像压缩”部分下的**启用重量级压缩**选项	2507	
支持 `Repair-AcctADAccount` PowerShell 命令	2503	使用以下命令 • `Repair-AcctIdentity`：修复身份帐户，而不更改其当前状态。这可以修复现有预配虚拟机中正在使用的身份帐户。例如，Microsoft Entra 混合加入身份帐户的 `repair userCertificate` 属性。AD 加入身份帐户的 `Repair identity info`（包括计算机密码/信任密钥对）。

项目	弃用版本	替代方案	
		• `Reset-AcctIdentity`：将身份帐户重置为初始状态（例如，从受污染状态重置为可用状态）。这可以将任何受污染的身份帐户重新放回池中，作为可用身份帐户。	
优化 3D HDX 图形策略	2411	使用视频编解码器进行压缩，设置为“针对整个屏幕”。请参阅 `<https://docs.citrix.com/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/policies/reference/ica-policy-settings/graphics-policy-settings.html#use-video-codec-for-compression>`	
NVIDIA GPU 硬件编码 (NVENC)，适用于：vGPU 15 及更早版本，以及驱动程序版本 529.19 及更早版本。	2411	使用当前支持的 NVIDIA 驱动程序：vGPU 16 或更高版本，以及驱动程序版本 536.22 或更高版本。有关 NVIDIA 支持的 vGPU 和驱动程序版本的更多信息，请参阅 `<https://docs.nvidia.com/vgpu/`	

项目	弃用版本	替代方案
		`index.html#driver-versions>`。
支持以下 `-AcctADAccount` PowerShell 命令 • New-AcctADAccount • Add-AcctADAccount	2411	使用 -AcctIdentity PowerShell 命令 • New-AcctIdentity • Add-AcctIdentity
已移除：Update-AcctADAccount		已移除：Update-AcctIdentity
已移除： Remove-AcctADAccount • Unlock-AcctADAccount 命令 • Get-AcctADAccount		已移除： Remove-AcctIdentity • Unlock-AcctIdentity 命令 • Get-AcctIdentity
支持 `-ResetIdentityInfo` PowerShell 命令	2411	使用 `-Recreate` 重新创建身份磁盘。有关信息，请参阅修复活动计算机帐户的身份信息。
基于 MMC 的 Studio	2411	MMC Studio 已在 2511 中移除，请改用 Web Studio。
多显示器挂钩	2407	-
域直通身份验证	2407	使用 用于单点登录的增强型域直通。

项目	弃用版本	替代方案
兰德福 V1	2402	使用 Rendezvous V2。
安全 ICA®	2402	使用 Secure HDX。
对 Windows Server 2016 的 VDA 支持	2402	升级到最新的 Windows Server 版本。
支持在 Windows Server 2016 上运行 Delivery Controller™、Web Studio、Citrix Director、Citrix License Server、Citrix StoreFront、适用于单会话操作系统的服务器 VDI、适用于多会话操作系统的 VDA、Active Directory 林和域以及通用打印服务器	2402	升级到最新版本的 Windows Server。
支持 Microsoft SQL Server 2016 和 2017 版本，用于站点配置、配置日志记录和监视数据库	2402	升级到最新版本的 Microsoft SQL Server。
支持在按需预配功能之前创建的 Azure 目录（“旧版”目录）	2402	重新创建 Azure 旧版目录 VM。这些目录按需预配，从而节省存储成本。
“**目标最小帧速率**”策略	2311	使用“**图形状态指示器**”修改目标最小帧速率。

项目	弃用版本	替代方案
支持在与目录创建区域不同的区域中使用主映像	2311	使用 Azure 计算库将主映像复制到所需区域。
HDX™ 图形显示内存限制设置	2311	分配所需的最小内存量，以确保完全适应客户端的显示布局。
HDX 图形中的渐进模式支持	2311	使用 Thinwire。请参阅渐进模式。
Internet Explorer 11 中对浏览器内容重定向的支持	2311	使用基于 Google Chrome 的浏览器内容重定向。
Broker 中对 SQL Server 2016 的支持	2308	使用最新版本。有关详细信息，请参阅系统要求。
Director 中对 XenApp 5.x 的支持	2308	---
Director 中对 XenApp 6.x 的支持	2308	---
Director 中用于警报的 SCOM Pack	2308	---
Director 中对插件的支持	2308	---
支持 WebRTC SDP 格式（方案 B）	2308	将 Citrix Workspace™ App 升级到受支持的版本。
Microsoft Teams 优化中对单窗口模式的支持	2308	将 Citrix Workspace App 升级到支持多窗口模式的版本。有关详细信息，请参阅功能矩阵和版本支持。

项目	弃用版本	替代方案
对用于 AWS 环境的 `AwsCaptureInstanceProperties` 的支持	2308	使用计算机配置文件。请参阅 使用计算机配置文件创建目录 。
`Schedule-ProvVMUpdate` PowerShell 命令	2305	使用 `Set-ProvVMUpdateTimeWindow`。
`Request-ProvVMUpdate` PowerShell 命令	2305	将 `Set-ProvVMUpdateTimeWindow` 与 `-StartsNow` 和 `-DurationInMinutes -1` 参数一起使用。
`Cancel-ProvVMUpdate` PowerShell 命令	2305	使用 `Clear-ProvVMUpdateTimeWindow`。
在 `New-ProvScheme` 命令中使用的 `DedicatedTenancy` 参数	2303	使用 `TenancyType` 参数。
许可证服务器 VPX	2206	---
在 Azure 环境中预配 VM 的非托管磁盘。	2206	使用托管磁盘。
主机到客户端 (URL) 重定向	2203	双向内容重定向。
支持四种 AWS 特定命令：`Revoke-HypSecurityGroupIngress`、`Revoke-HypSecurityGroupEgress`、`Grant-HypSecuritygroupe`	2203	---

项目	弃用版本	替代方案
`gress` 和 `Grant-HypSecurityGroupIngress`，用于云和本地环境。		
从 VDA 元安装程序中移除了适用于 Windows 的 Citrix Files 和适用于 Outlook 的 Citrix Files。	2203	使用独立安装程序。
从 VDA 元安装程序中移除了 WEM 代理组件。	2203	---
适用于 XenApp 和 XenDesktop、Provisioning Services 以及 StoreFront 的 Citrix SCOM 管理包。有关可受监控的产品版本，请参阅Citrix SCOM 管理包文档。	1912	使用 Director 监控和管理您的部署。有关 SCOM EOL 和替代方案的更多信息，请参阅https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX266943。
移动性 SDK / 移动 SDK（来自前 Citrix Labs）	7.16	已由移动体验策略设置以及托管桌面/应用程序的本机体验取代。

已移除的功能

在 Citrix Virtual Apps and Desktops 中，已移除的项目要么已被删除，要么不再受支持。

项目	在版本中宣布弃用	在版本中移除	替代方案
移除对服务器 VDA 上 Citrix 备份和还原的支持	2603	2603	在安装或升级服务器 VDA 之前手动备份
用于远程电脑访问的 SCCM 集成式局域网唤醒选项。	2012	2511	使用独立局域网唤醒功能。
支持适用于 系统中心配置管理器 的 思杰连接器 3.1	2311	2507	手动执行映像或应用程序更新。
移除对 AWS 卷工作进程的支持	2311	2503	使用直接磁盘上传和下载。请参阅 直接磁盘上传和下载。
支持 SQL Server 2016 和 2017	2402 和 2308	2411	使用 SQL Server 2019 和 2022
支持配置 MCS I/O 回写缓存，使其仅包含磁盘缓存而不包含内存缓存	2402	2411	创建启用了回写缓存的计算机时，选择**内存缓存大小 (MB)** 选项并为其指定一个非零大小。
Citrix Studio 中对 PVS 导入向导的支持	1912 LTSR	2311	使用以下任一方式预配 Citrix Provisioning™ 计算机 • 使用 Citrix Provisioning Console 预配计算

项目	在版本中宣布弃用	在版本中移除	替代方案	
			机，并使用 Citrix Provisioning 设备导出向导将其导出到 Citrix Virtual Apps and Desktops。有关详细信息，请参阅导出设备向导。 • 使用 Web Studio 创建 Citrix Provisioning 目录。有关详细信息，请参阅在 Citrix Studio 中创建 Citrix Provisioning 目录。	
适用于 Windows 的 Citrix Workspace 应用程序 1912	---	2402	使用最新版本。	
HDX 图形全屏 + 文本优化	2311	2311		

项目	在版本中宣布弃用	在版本中移除	替代方案
HDX 3D Pro 对 NVIDIA 帧缓冲捕获 (NVFBC) 的支持	2308	2311	使用桌面复制 API (DDAPI)。
VDA 对策略设置“自动安装内置打印机驱动程序”的支持。	7.16	2311	无。此策略设置仅支持早期操作系统（Windows 7、Windows Server 2012 R2 及更早版本）上的 VDA。
NVIDIA GPU 硬件编码 (NVENC)，适用于：vGPU 11 及更早版本，以及驱动程序版本 466.77 及更早版本。	2305	2305	使用当前支持的 NVIDIA 驱动程序：vGPU 13 或更高版本，版本 471.41 或更高版本。
VDA Meta-Installer 中的 Citrix 支持工具 (SupportabilityTool_x64 .msi)。	---	2212	---
Citrix License Administration Console（最后包含在 Windows 许可证服务器 11.16.3 build 30000 中，并在 Windows 许可证服务器 v11.16.6 build	2003	2006	使用 Citrix 许可管理器。

项目	在版本中宣布弃用	在版本中移除	替代方案
31000 中移除）。			
在 Windows 10 版本 1709 及更早版本上支持 Citrix 间接显示驱动程序 (IDD) 图形适配器。	2003	2003	使用 Citrix 虚拟应用和桌面™ 7 1912 LTSR VDA。
使用 GRID 9 或更早的显示驱动程序通过 NVIDIA GPU (NVENC) 进行硬件编码。	2003	2003	将 GRID 10 显示驱动程序与 Citrix Virtual Apps and Desktops 7 2003 或更高版本 VDA 结合使用，或者使用 Citrix Virtual Apps and Desktops 7 1912 LTSR VDA。
自助密码重置 (SSPR) 功能。	2003	2006	---
对 VDA 和核心服务器组件（包括 Delivery Controller、Studio、Director）的 Microsoft .NET Framework 4.8 以前版本的支持。	1912	2003	升级到 .NET Framework 4.8 版。
在 Windows Server 2012 R2	1912	2003	在受支持的操作系统上安装 VDA。

项目	在版本中宣布弃用	在版本中移除	替代方案
上运行的 VDA。			
Citrix Virtual Apps and Desktops Premium 版的 AppDNA® 应用程序迁移组件。	1909	2003	---
在 32 位 (x86) 计算机上安装 Studio。	1909	2003	在受支持的 x64 操作系统上安装。
对无缝应用程序中 Excel 挂钩的支持。此功能用于为每个 Microsoft Excel 2010 工作簿创建单独的任务栏图标。	1909	1909	---
Windows Server 2012 R2（包括 Service Pack）上的核心服务器组件。包括：Delivery Controller、Studio 和 Director。	1906	2003	安装在较新的受支持操作系统上。
支持 Microsoft SQL Server 2008 R2、2012 和 2014 版本（包括所有 Service Pack 和版本）上的站点配置、配置日志	1906	2003	将数据库安装在受支持的 Microsoft SQL Server 版本上。

项目	在版本中宣布弃用	在版本中移除	替代方案
记录和监视数据库。			
支持 x86 平台上的 Windows 10 上的 VDA。	1906	1909*	将 VDA 安装在受支持的 x64 操作系统上。* 此功能在 Citrix Virtual Apps and Desktops 7 1912 LTSR 中仍受支持。
从 Citrix Virtual Apps and Desktops 安装介质中移除 Citrix Smart Tools 代理。	1903	1906	---
支持 Red Hat Enterprise Linux/CentOS 7.5 上的 Linux VDA。	1903	1903	在更高版本的 Red Hat Enterprise Linux 上安装 Linux VDA。
StoreFront 对 Citrix Virtual Apps and Desktops（以前称为 XenApp and XenDesktop）与 Citrix Receiver 和 Workspace Hub 之间 TLS 1.0 和 TLS 1.1 协议的支持。	7.17	2203	将 Citrix Receivers 升级到支持 TLS 1.2 协议的 Citrix Workspace 应用程序。有关 Citrix Workspace 应用程序的更多信息，请参阅 https://docs.citrix.com/zh-cn/citrix-workspace-app。

项目	在版本中宣布弃用	在版本中移除	替代方案
VDA 对策略设置“自动安装内置打印机驱动程序”的支持。	7.16	2311	无。此策略设置仅支持早期操作系统（Windows 7、Windows Server 2012 R2 及更早版本）上的 VDA。
支持 Framehawk 显示远程处理技术	1811	1903	使用启用 自适应传输 的 Thinwire。
所有 Citrix Virtual Apps and Desktops（以及 XenApp and XenDesktop）版本中对 Citrix Smart Scale 的支持。此功能将于 31 May 2019 终止生命周期。	1808	1906	考虑使用 Citrix Cloud 上的 Virtual Apps and Desktops Service 以改进电源管理功能。
思杰 StoreFront、思杰 VDA、思杰 Studio、思杰 Director 和 思杰 Delivery Controller 不再支持 Microsoft .NET Framework 4.5.1、4.5.2、4.6、4.6.1、4.6.2 和 4.7 版本。	7.18	1808	升级到 .NET Framework 4.7.1 或更高版本。（如果尚未安装，安装程序会自动安装 .NET Framework 4.7.1。）

项目	在版本中宣布弃用	在版本中移除	替代方案
对 Red Hat Enterprise Linux 7.3 上的 Linux VDA 的支持。	7.18	1808	在更高版本的 Red Hat Enterprise Linux 上安装 Linux VDA。
不再支持 SUSE Linux Enterprise Server 11 服务包 4 上的 Linux VDA。	7.16	7.16	在受支持的 SUSE 版本上安装 Linux VDA。
对 VDA 上的 Citrix WDDM 驱动程序的支援	7.16	7.16	Citrix WDDM 驱动程序不再随 VDA 一起安装。
Windows 10 版本 1511 (Threshold 2) 及更早的 Windows 单会话操作系统版本（包括 Windows 8.x 和 Windows 7）上的 VDA（请参阅 `<https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/>`）。	7.15 LTSR（和 7.12）	7.16	在 Windows 10 最低版本 1607 (Redstone 1) 或更新的半年频道上安装单会话操作系统 VDA。如果使用 1607 LTSB，我们建议使用 7.15 VDA。请参阅 CTX224843。

项目	在版本中宣布弃用	在版本中移除	替代方案
Windows Server 2008 R2 和 Windows Server 2012（包括服务包）上的 VDA	7.15 LTSR（和 7.12）	7.16	在受支持的操作系统上安装 VDA。
桌面合成重定向（以前称为 DirectX 命令远程处理）(DCR)	7.15 LTSR	7.16	使用 Thinwire。
Windows Server 2012 和 Windows Server 2008 R2（包括服务包）上的核心组件。包括：交付控制器、管理控制台、监控器、应用商店、许可证服务器和通用打印服务器。	7.15 LTSR	7.18	在受支持的操作系统上安装组件。
Windows Server 2012 和 Windows Server 2008 R2（包括 Service Pack）上的自助式密码重置 (SSPR) 功能	7.15 LTSR	7.18	安装在较新的受支持操作系统上。
在 Windows 7、Windows 8 和 Windows 8.1（包括服务包）上的管理控制台	7.15 LTSR	7.18	在受支持的操作系统上安装 Studio。

项目	在版本中宣布弃用	在版本中移除	替代方案
Flash 重定向	7.15 LTSR	1912	将视频内容创建为 HTML5 视频。对托管内容使用 HTML5 视频重定向，对公共网站使用浏览器内容重定向。有关详细信息，请参阅 Flash 重定向生命周期结束 备注。
Citrix Online 集成 (Goto 产品) 与 StoreFront	7.14 (和 StoreFront 3.11)	StoreFront 3.12	---
在 VDA 安装期间创建并添加到 VDA 计算机上的本地管理员组的用户帐户 CtxAppVCOMAdmin 不再创建。底层“COM”机制也已删除。	7.14	7.14	Windows 服务 CtxAppVService 执行相同的功能。它会自动安装和配置，无需用户交互。
在 Windows Server 2008 32 位上对 Universal Print Server UpsServer 组件的支持	7.14	7.14	安装在较新的受支持操作系统上。
StoreFront 和 Receiver for Web 在 Internet Explorer 8 上的支持	7.13	7.13	---

项目	在版本中宣布弃用	在版本中移除	替代方案
VDA 命令行安装选项 /no_appv，用于阻止安装 Citrix App-V 组件	7.13	7.13	使用命令行安装选项 /exclude "Citrix Personalization for App-V – VDA"。
完整产品安装程序不再在新安装中安装 Citrix.Common.Commands 管理单元，并在升级现有安装时自动将其删除。	7.13	7.13	Citrix.Common.Commands 管理单元提供的一些 PowerShell 命令在 XenApp 6.5 SDK 中仍然可用。
由 *-CtxIcon cmdlet 提供的用于操作图标数据的部分功能。	7.13	7.13	现在由 Broker Service 中的 *-BrokerIcon cmdlet 提供。
旧版 Thinwire 模式	7.12	7.16	使用 Thinwire。如果您在 Windows Server 2008 R2 上使用旧版 Thinwire 模式，请迁移到 Windows Server 2012 R2 或 Windows Server 2016，并使用 Thinwire。
从 StoreFront 2.0、2.1、2.5 和 2.5.2 进行就地升级	7.13	7.16	从这些版本之一升级到更高受支持的版本，然后升级到 XenApp

项目	在版本中宣布弃用	在版本中移除	替代方案
			和 XenDesktop 7.16。
从 XenDesktop 5.6 或 5.6 FP1 进行就地升级	7.12	7.16	将您的 XenDesktop 5.6 或 5.6 FP1 部署迁移到当前的 XenDesktop 版本。为此，请首先升级到 XenDesktop 7.6 LTSR（包含最新 CU），然后升级到最新的 Citrix Virtual Desktops（以前称为 XenDesktop）版本或 LTSR 版本。
在 32 位 (x86) 计算机上安装 Delivery Controller、Director、StoreFront 或 License Server。	7.12	7.16	安装在受支持的 x64 操作系统上。
连接租用	7.12	7.16	使用 本地主机缓存。
在 Windows XP 上使用的 XenDesktop 5.6。不支持在 Windows XP 上安装 VDA。	7.12	7.16	在受支持的操作系统上安装 VDA。

项目	在版本中宣布弃用	在版本中移除	替代方案
支持 CloudPlatform 连接	7.12	2003	使用其他受支持的管理程序或云服务。
支持 Azure 经典部署（也称为 Azure 服务管理）连接	7.12	2003	考虑在 Citrix Cloud 上使用 Virtual Apps and Desktops 服务。
AppDisks 功能（以及支持它的 AppDNA 与 Studio 的集成）	7.13	2003	请使用 Citrix App Layering 解决方案。
Personal vDisk 功能	7.15	2006†	使用 Citrix App Layering 用户层或 用户个性化层 技术。

† 在 Citrix Virtual Apps and Desktops 7 2003 中，Personal vDisk 驱动程序已从 VDA 安装程序中移除。在 Citrix Virtual Apps and Desktops 7 2006 中，Personal vDisk 驱动程序工作流已从 Studio 中移除。

系统要求

简介

本文档中的系统要求在本产品版本发布时有效。我们会定期进行更新。此处未涵盖的组件（例如主机系统、Citrix Workspace™ app 和 Citrix Provisioning™）的系统要求在其各自的文档中进行了说明。

在开始安装之前，请查看准备安装。

除非另有说明，否则如果机器上未检测到所需的版本，组件安装程序会自动部署软件必备项（例如 .NET 和 C++ 软件包）。Citrix® 安装介质也包含部分此类必备软件。

安装介质包含多个第三方组件。在使用 Citrix 软件之前，请检查第三方的安全更新并进行安装。

有关全球化信息，请参阅知识中心文章 CTX119253。

对于可在 Windows Server 上安装的组件和功能，除非另有说明，否则不支持 Nano Server 安装。Server Core 仅支持 Delivery Controller 和 Director。

硬件要求

RAM 和磁盘空间值是除了产品映像、操作系统和机器上其他软件的要求之外的。您的性能会因配置而异。您的配置包括您使用的功能、用户数量以及其他因素。仅使用最低配置可能会导致性能缓慢。

下表列出了核心组件的最低要求。

组件	最低
所有核心组件和 StoreFront™ 位于一台服务器上，仅用于评估，而非生产部署	5 GB RAM
所有核心组件和 StoreFront 位于一台服务器上，用于测试部署或小型生产环境	12 GB RAM
Delivery Controller™（本地主机缓存需要更多磁盘空间）	5 GB RAM，800 MB 硬盘

组件	最低
工作室	1 GB RAM，100 MB 硬盘
监控器	2 GB RAM，200 MB 硬盘
StoreFront	2 GB RAM，有关磁盘建议，请参阅 StoreFront 文档
许可证服务器	8 GB RAM；有关磁盘建议，请参阅 许可文档

交付桌面和应用程序的 VM 大小调整

由于硬件产品复杂多变，且每个部署都有独特需求，因此无法提供具体建议。通常，Citrix Virtual Apps™ VM 的大小调整基于硬件而非用户工作负载。例外情况是 RAM。对于消耗更多 RAM 的应用程序，您需要更多的 RAM。

有关详细信息：

- Citrix Tech Zone 包含有关大小调整的指导。
- Citrix Virtual Apps and Desktops 单服务器可扩展性 讨论了单个物理主机可支持的用户或 VM 数量。

微软 Visual C++

安装 Delivery Controller、Virtual Delivery Agent (VDA) 或 Universal Print Server 时，Citrix 安装程序会自动安装 Microsoft Visual C++ 2015–2022 可再发行组件。

- 如果计算机包含该运行时环境的早期版本（例如 2015-2019），Citrix 安装程序会对其进行升级。
- 如果计算机包含早于 2015 的版本，Citrix 会并行安装较新版本。

交付控制器

> **注意：**

> **许可证服务器版本兼容性：** 确保许可证服务器运行的最低版本为 11.17.2 build 53100。未能满足此先决条件将阻止 Citrix Virtual Apps and Desktops (CVAD) 站点升级和站点创建。

支持的操作系统：

- Windows 服务器 2025
- Windows Server 核心版 2022
- Windows 服务器 2022
- Windows Server 2019，标准版和数据中心版，以及带 Server Core 选项的版本

要求：

- 如果尚未安装 Microsoft .NET Framework 4.8（或更高版本），则会自动安装。
- Windows PowerShell 版本 3.0、4.0 或 5.0。
- Microsoft Visual C++ 2015–2022 可再发行组件。
- 如果您从 Citrix Virtual Apps and Desktops 2407 版升级到 2411 版或更高版本，或者执行 2411 版或更高版本的新安装，请首先将许可证服务器更新到最新版本（11.2.17 build 53100 版或更高版本）。然后，升级 Delivery Controller。否则，UI 上将显示警告消息，并且命令行安装将失败。

注意：

Citrix Virtual Apps and Desktops™ Delivery Controller 不支持只读域控制器 (RODC)。

数据库

注意：

从 2411 版开始，您可以将 Azure SQL 托管实例用于数据库。

支持用于站点配置、配置日志记录和监视数据库的 Microsoft SQL Server 版本：

- SQL Server 2022，速成版、标准版和企业版。
  - 对于新安装：默认情况下，如果在安装 Controller 时未检测到现有受支持的 SQL Server 安装，则会安装带有累积更新 14 的 SQL Server Express 2022。
- SQL Server 2019，速成版、标准版和企业版。

- SQL Server 2025，速成版、标准版和企业版。

支持以下数据库高可用性解决方案（SQL Server Express 除外，它仅支持独立模式）：

- SQL Server AlwaysOn 故障转移群集实例
- SQL Server AlwaysOn 可用性组（包括基本可用性组）
- SQL Server 数据库镜像

Controller 与 SQL Server 站点数据库之间的连接需要 Windows 身份验证。

本地主机缓存注意事项： Microsoft SQL Server Express LocalDB 是 SQL Server Express 的一项功能，本地主机缓存以独立方式使用它。本地主机缓存不需要 SQL Server Express 的任何组件，只需要 SQL Server Express LocalDB。

- 安装 Controller 时，将安装带有累积更新 15 的 Microsoft SQL Server Express LocalDB 2022，以用于本地主机缓存功能。（此安装独立于站点数据库的默认 SQL Server Express 安装。）
- 升级 Controller 时，不会自动升级现有的 Microsoft SQL Server Express LocalDB 版本。有关替换要求和过程，请参阅替换 SQL Server Express LocalDB。

更多数据库信息：

- 数据库
- CTX114501 列出了当前支持的数据库
- 数据库大小调整指南
- 本地主机缓存

网络工作室

> **注意：**
>
> - Web Studio 是一个基于 Web 的管理控制台，可用于配置和管理本地 Citrix Virtual Apps and Desktops 部署。它旨在改善用户体验，并且通常比 Citrix Studio 响应更快。有关安装步骤，请参阅安装 Web Studio。
> - 从版本 2511 开始，Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops 唯一的管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。

> 有关安装和使用 Web Studio 的受支持操作系统、浏览器、显示设置和硬件要求的信息，请参阅 Web Studio 文章中的系统要求。

Citrix 导向器

支持的操作系统：

- Windows 服务器 2025
- Windows Server 核心版 2022
- Windows 服务器 2022
- Windows Server 2019，标准版和数据中心版，以及带 Server Core 选项的版本

要求：

- 如果尚未安装 Microsoft .NET Framework 4.8（或更高版本），则会自动安装。
- Microsoft Internet Information Services (IIS) 7.0 和 ASP.NET 2.0。确保 IIS 服务器角色已安装静态内容角色服务。如果尚未安装此软件，系统将提示您提供 Windows Server 安装介质。然后，系统会为您安装该软件。
- 要查看安装了 Citrix Director 的计算机上的事件日志，必须安装 Microsoft .NET Framework 2.0。

Citrix 配置文件管理：

- 确保在 VDA 上安装了 Citrix Profile Management 和 Citrix Profile Management WMI 插件（安装向导中的**附加组件**页面），并且 Citrix Profile Management Service 正在运行，以便在 Director 中查看用户配置文件详细信息。

系统中心操作管理器 (SCOM) 集成要求：

- 系统中心 2012 R2 操作管理器

查看 Director 支持的浏览器：

- 微软 Edge。
- Firefox ESR（延长支持版本）。
- Chrome 浏览器。

查看 Director 的推荐最佳屏幕分辨率为 1440 x 1024。

适用于单会话操作系统的 Virtual Delivery Agent (VDA)

支持的操作系统：

- Windows 十一
- Windows 10（仅限 x64），任何当前处于主流支持状态的版本。
    - 有关版本支持，请参阅知识中心文章 CTX224843。

要求：

- 如果尚未安装 Microsoft .NET Framework 4.8（或更高版本），则会自动安装。
- Microsoft Visual C++ 2015–2022 可再发行组件。

远程电脑访问使用此 VDA，您将其安装在物理办公电脑上。此 VDA 支持在 Windows 11 和 Windows 10 上为 Citrix Virtual Desktops™ 远程电脑访问提供安全启动。

某些多媒体加速功能（例如 HDX MediaStream Windows Media 重定向）要求在安装 VDA 的计算机上安装 Microsoft Media Foundation。如果计算机未安装 Media Foundation，则多媒体加速功能将不会安装且无法工作。安装 Citrix 软件后，请勿从计算机中删除 Media Foundation。否则，用户将无法登录到计算机。在大多数受支持的 Windows 单会话操作系统版本中，Media Foundation 支持已安装且无法删除。但是，N 版本不包含某些与媒体相关的技术；您可以从 Microsoft 或第三方获取该软件。有关详细信息，请参阅 准备安装。

有关 Linux VDA 信息，请参阅 Linux Virtual Delivery Agent 文章。

要使用服务器 VDI 功能，您可以使用命令行界面在受支持的 Windows Server 计算机上安装适用于 Windows 单会话操作系统的 VDA。有关指导，请参阅 服务器 VDI。

有关在 Windows 7 计算机上安装 VDA 的信息，请参阅 早期操作系统。

适用于多会话操作系统的 Virtual Delivery Agent (VDA)

支持的操作系统：

- Windows 服务器 2025
- Windows 11（仅支持 Citrix DaaS™）
- Windows 10（仅限 x64；仅支持 Citrix DaaS），任何当前处于主流支持状态的版本。
- Windows 服务器 2022
- Windows Server 2019 标准版和数据中心版

安装程序会自动部署以下要求，这些要求也可在 Citrix 安装介质的 **Support** 文件夹中找到：

- 如果尚未安装 Microsoft .NET Framework 4.8（或更高版本），则会自动安装。
- Microsoft Visual C++ 2015–2022 可再发行组件。

如果尚未安装和启用远程桌面服务角色服务，安装程序会自动安装并启用它们。

某些多媒体加速功能（例如 HDX MediaStream Windows Media 重定向）要求在安装 VDA 的计算机上安装 Microsoft Media Foundation。如果计算机未安装 Media Foundation，则多媒体加速功能将不会安装且无法工作。安装 Citrix 软件后，请勿从计算机中删除 Media Foundation；否则，用户将无法登录到计算机。在大多数 Windows Server 版本中，Media Foundation 功能通过服务器管理器安装。有关详细信息，请参阅准备安装。

如果 VDA 上不存在 Media Foundation，则以下多媒体功能将无法工作：

- Windows Media 重定向
- HTML5 视频重定向
- HDX™ RealTime 网络摄像头重定向

有关 Linux VDA 信息，请参阅 Linux Virtual Delivery Agent 文章。

有关在 Windows Server 2008 R2 计算机上安装 VDA 的信息，请参阅早期操作系统。

Amazon WorkSpaces Core 托管实例中的 VDA

支持的操作系统：

- Windows 11 单会话
- Windows 10 单会话
- Windows 服务器 2025
- Windows 服务器 2022
- Windows 服务器 2019
- Windows 服务器 2016
- Ubuntu 服务器 24.04 LTS
- 德比安 12

主机/虚拟化资源

支持以下主机/虚拟化资源（按字母顺序列出）。在适用情况下，支持 *major.minor* 版本，包括这些版本的更新。知识中心文章 CTX131239 包含当前版本信息以及已知问题的链接。

某些功能可能并非在所有主机平台或所有平台版本上都受支持。有关详细信息，请参阅功能文档。

远程电脑访问的局域网唤醒功能需要 Microsoft System Center Configuration Manager 2012 或更高版本。

支持的管理程序：

- **Azure 本地**

  有关详细信息，请参阅Azure 本地环境。

- **XenServer（以前称为 Citrix Hypervisor™）**

  CTX131239 包含当前版本信息以及已知问题的链接。

  有关详细信息，请参阅 XenServer 虚拟化环境。

- **Microsoft System Center 虚拟机管理器**

  包括任何版本的 Hyper-V，可注册到受支持的 System Center Virtual Machine Manager 版本。

  CTX131239 包含当前版本信息以及已知问题的链接。

  有关详细信息，请参阅 Microsoft System Center Virtual Machine Manager 虚拟化环境。

- **努坦尼克斯 Acropolis**

  CTX131239 包含当前版本信息以及已知问题的链接。

  有关详细信息，请参阅Nutanix 虚拟化环境。

- **VMware vSphere 虚拟化平台（vCenter + ESXi）**

  不支持 vSphere vCenter 链接模式操作。

  CTX131239 包含当前版本信息以及已知问题的链接。

  有关详细信息，请参阅 VMware 虚拟化环境。

支持的公共云主机：

- **亚马逊网络服务 (AWS)**

有关使用 AWS 预配虚拟机的信息，请参阅 Amazon Web Services 虚拟化环境。

- **Google Cloud Platform** 有关详细信息，请参阅 Google Cloud Platform 虚拟化环境 和 Citrix DaaS on Google Cloud 入门。
- **Microsoft Azure 资源管理器**

  有关使用 Microsoft Azure Resource Manager 预配虚拟机的信息，请参阅 Microsoft Azure Resource Manager 虚拟化环境。
- **红帽 OpenShift**

  有关使用 Red Hat OpenShift 预配虚拟机的信息，请参阅 Red Hat OpenShift 虚拟化环境。
- **Nutanix 云和合作伙伴解决方案**

  有关使用 Nutanix 云和合作伙伴解决方案的信息，请参阅 Nutanix 云和合作伙伴解决方案。
- **VMware 云和合作伙伴解决方案**

  有关使用 VMware 云和合作伙伴解决方案的信息，请参阅 VMware 云和合作伙伴解决方案。

将公共云主机连接添加到部署时，请考虑以下事项：

- 您需要混合权利许可证。有关混合权利许可证的信息，请参阅 通过混合权利进行过渡和升级 (TTU)。有关添加许可证的信息，请参阅 创建站点。
- 信息源将引导您查阅 Citrix DaaS 文档。如果您熟悉 Citrix DaaS 产品中的公共云主机，则本地版本存在一些差异。
  - Citrix DaaS 大约每四周发布一次更新。因此，您可能会发现 Citrix DaaS 中的某些功能在本地版本中不可用。

Active Directory 功能级别

支持以下 Active Directory 林和域功能级别：

- Windows 服务器 2025
- Windows 服务器 2016
- Windows Server 2012 R2 服务器
- Windows 服务器 2012
- Windows 服务器 2008 R2
- Windows 服务器 2008

> **注意：**
>
> 在升级 Citrix Virtual Apps and Desktops 站点之前，请查看各个功能的要求，因为较新的功能和 VDA 可能需要特定的最低 Active Directory 功能级别。

HDX

音频

适用于 Multi-Stream ICA® 的 UDP 音频在适用于 Windows 的 Citrix Workspace 应用程序和适用于 Linux 13 的 Citrix Workspace 应用程序上受支持。

回声消除在适用于 Windows 的 Citrix Workspace 应用程序上受支持。

请参阅具体的 HDX 功能支持和要求。有关 HDX 功能和 Citrix Workspace 应用程序的更多信息，请参阅功能矩阵。

HDX Windows 媒体传送

以下客户端支持 Windows Media 客户端内容获取、Windows Media 重定向和实时 Windows Media 多媒体转码：适用于 Windows 的 Citrix Workspace 应用程序、适用于 iOS 的 Citrix Workspace 应用程序和适用于 Linux 的 Citrix Workspace 应用程序。

要在 Windows 8 设备上使用 Windows Media 客户端内容获取，请将 Citrix Multimedia Redirector 设置为默认程序：在**控制面板 > 程序 > 默认程序 > 设置默认程序**中，选择 **Citrix Multimedia Redirector**，然后单击**将此程序设置为默认值**或**选择此程序的默认值**。GPU 转码需要具有计算能力 1.1 或更高版本的 NVIDIA CUDA 启用 GPU；请参阅 `<https://developer.nvidia.com/cuda/cuda-gpus>`。

HDX 3D Pro 技术

适用于 Windows 单会话操作系统的 VDA 在运行时检测 GPU 硬件的存在。

托管应用程序的物理机或虚拟机可以使用 GPU 直通或虚拟 GPU (vGPU)：

- GPU 直通适用于：
  - XenServer®
  - 努坦尼克斯 AHV
  - VMware vSphere 和 VMware ESX，其中它被称为虚拟直接图形加速 (vDGA)

- vGPU 可用于：
  - XenServer
  - 努坦尼克斯 AHV
  - 威睿 vSphere

请参阅 `<https://docs.citrix.com/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/graphics/hdx-3d-pro>`。

Citrix 建议主机计算机至少具有 4 GB RAM 和四个虚拟 CPU，时钟速度为 2.3 GHz 或更高。

图形处理单元 (GPU)：

- 对于使用 NVIDIA GRID API 的虚拟化图形加速，您可以将 HDX 3D Pro 与 NVIDIA Virtual GPU (vGPU) 软件版本 13 及更高版本支持的所有 NVIDIA GRID GPU 结合使用，请参阅 `<https://docs.nvidia.com/grid/index.html>`。 有关支持的 Hypervisor 和支持的硬件的详细列表，请参阅 NVIDIA vGPU 软件 文档。
- Intel Xeon 处理器 E3 系列数据中心图形平台和 Intel 数据中心 GPU Flex 系列支持虚拟化图形加速。有关详细信息，请参阅 GPU Flex 系列。
- AMD GPU 支持 AMD 的 mxGPU 虚拟化。有关支持的硬件的详细信息，请参阅 AMD 文档。

用户设备：

- Citrix 最多支持 8 台 4k 显示器，具体取决于硬件资源。根据所使用的 GPU，此最大值可能存在其他硬件限制。
- Citrix 建议用户设备至少具有 4 GB RAM 和一个时钟速度为 1.6 GHz 或更高的 CPU。为了获得最佳性能，我们建议用户设备至少具有 8 GB RAM 和一个时钟速度为 3 GHz 或更高的双核 CPU。
- 对于多显示器访问，Citrix 建议使用配备四核 CPU 的用户设备。
- 必须安装 Citrix Workspace 应用程序。

有关详细信息，请参阅 HDX 3D Pro 文章 和 www.citrix.com/xenapp/3d。

通用打印服务器

通用打印服务器包含客户端和服务器组件。UpsClient 组件包含在 VDA 安装中。您可以在每个打印服务器上安装 UpsServer 组件，这些打印服务器上驻留着您希望在用户会话中使用 Citrix Universal™ Print Driver 预配的共享打印机。

UpsServer 组件支持以下系统：

- Windows Server 2025 服务器
- Windows 服务器 2022
- Windows Server 2019 服务器

要求：

- Microsoft Visual C++ 2015–2022 可再发行组件包
- Microsoft .NET Framework 4.8（至少需要此版本）

对于多会话操作系统的 VDA，打印操作期间的用户身份验证要求通用打印服务器加入与 VDA 相同的域。

独立的客户端和服务器组件包也可供下载。

有关详细信息，请参阅 Citrix 通用打印服务器。

其他

仅支持 Citrix License Server 11.17.2 及更高版本。有关详细信息，请参阅 许可。

有关版本兼容性的详细信息，请参阅 产品兼容性列表。

有关支持的 StoreFront 版本，请参阅StoreFront 系统要求。

有关 Workspace Environment Management (WEM) 的系统要求信息，请参阅 WEM 文档中的 系统要求。

如果您将 Citrix 策略信息存储在 Active Directory 而非站点配置数据库中，则需要 Microsoft 组策略管理控制台 (GPMC)。如果您单独安装 `CitrixGroupPolicyManagement_x64.msi`（例如，在未安装 Citrix Virtual Apps and Desktops 核心组件的计算机上），则该计算机必须安装 Visual Studio 2015 运行时。有关详细信息，请参阅 Microsoft 文档。

如果要使用 GPMC 编辑域 GPO，请在所有包含 Delivery Controller 的计算机上启用组策略管理功能（在 Windows Server Manager 中）。

支持多个 NIC。

默认情况下，当您安装当前 VDA 时，不会安装适用于 Windows 的 Citrix Workspace 应用程序。有关详细信息，请参阅 适用于 Windows 的 Citrix Workspace 应用程序文档。

有关该功能支持的浏览器信息，请参阅 本地应用程序访问。

此版本的 Citrix Virtual Apps and Desktops 需要最低 HDX RealTime Connector 2.9 LTSR。有关详细信息，请参阅 HDX RealTime Optimization Pack 文档。

此产品支持 PowerShell 版本 3 到 5。

技术概述

Citrix Virtual Apps and Desktops™ 是虚拟化解决方案，它使 IT 能够控制虚拟机、应用程序、许可和安全性，同时为任何设备提供随时随地的访问。

Citrix 虚拟应用和桌面™ 允许：

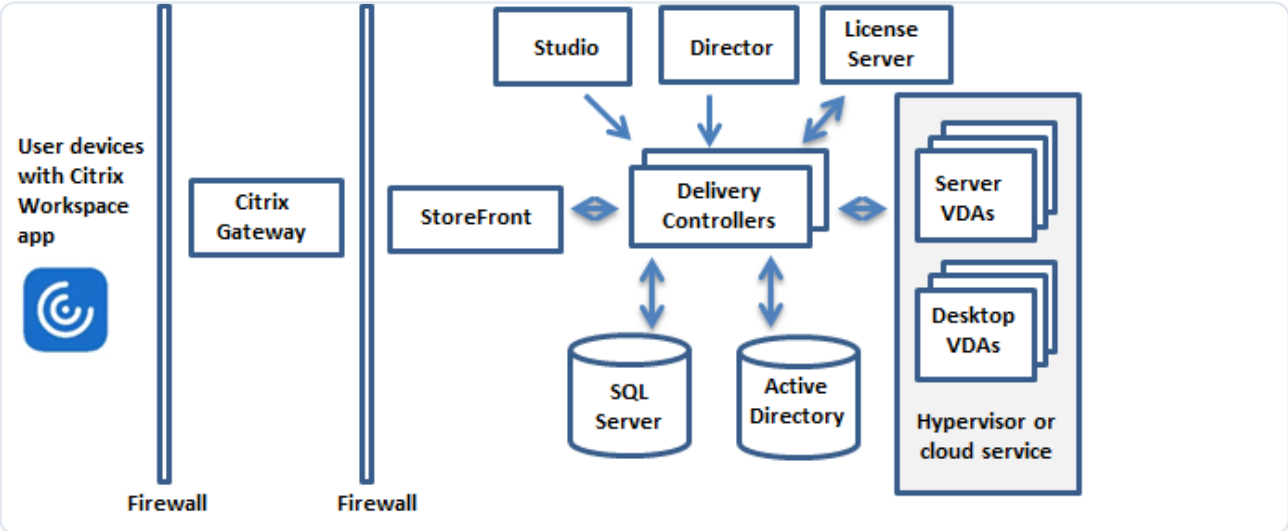
- 最终用户独立于设备的操作系统和界面运行应用程序和桌面。
- 管理员管理网络并控制来自选定设备或所有设备的访问。
- 管理员从单个数据中心管理整个网络。

Citrix Virtual Apps and Desktops 共享一个名为 FlexCast Management Architecture (FMA) 的统一架构。FMA 的主要功能是能够从单个站点运行多个版本的 Citrix Virtual Apps 或 Citrix Virtual Desktops™ 以及集成预配。

关键组件

如果您是 Citrix Virtual Apps and Desktops 的新用户，本文将对您最有帮助。

此图显示了典型部署（称为站点）中的关键组件。



交付控制器™

Delivery Controller 是站点的中央管理组件。每个站点都有一个或多个 Delivery Controller。它安装在数据中心至少一台服务器上。为了提高站点可靠性和可用性，请将 Controller 安装在多台服务器上。如果您的部署包含管理程序或其他服务，Controller 服务会与其通信以：

- 分发应用程序和桌面
- 验证和管理用户访问
- 在用户及其桌面和应用程序之间代理连接
- 优化用户连接
- 负载均衡连接

Controller 的 Broker Service 跟踪哪些用户已登录以及登录位置、用户拥有的会话资源以及用户是否需要重新连接到现有应用程序。Broker Service 运行 PowerShell cmdlet 并通过 TCP 端口 80 与 VDA 上的代理通信。它没有使用 TCP 端口 443 的选项。

Monitor Service 收集历史数据并将其存储在监控数据库中。此服务使用 TCP 端口 80 或 443。

来自 Controller 服务的数据存储在站点数据库中。

Controller 根据需求和管理配置管理桌面状态，并启动和停止它们。

数据库

每个站点至少需要一个 Microsoft SQL Server 数据库来存储配置和会话信息。此数据库存储由构成 Controller 的服务收集和管理的数据。请在数据中心内安装数据库，并确保它与 Controller 具有持久连接。

站点还使用配置日志记录数据库和监控数据库。默认情况下，这些数据库与站点数据库安装在同一位置，但您可以更改此设置。

虚拟投递代理 (VDA)

VDA 安装在您站点中提供给用户的每台物理或虚拟机上。这些机器提供应用程序或桌面。VDA 使机器能够向 Controller 注册，进而使机器及其托管的资源可供用户使用。VDA 建立并管理机器与用户设备之间的连接。VDA 还会验证用户或会话是否具有 Citrix® 许可证，并应用为会话配置的策略。

VDA 通过 VDA 中的代理将会话信息传达给 Controller 中的 Broker Service。代理托管多个插件并收集实时数据。它通过 TCP 端口 80 与 Controller 通信。

“VDA”一词通常用于指代代理及其安装的机器。

VDA 适用于单会话和多会话 Windows 操作系统。适用于多会话 Windows 操作系统的 VDA 允许同时连接多个用户到服务器。适用于单会话 Windows 操作系统的 VDA 仅允许一次一个用户连接到桌面。还提供 Linux VDA。

思杰店面™

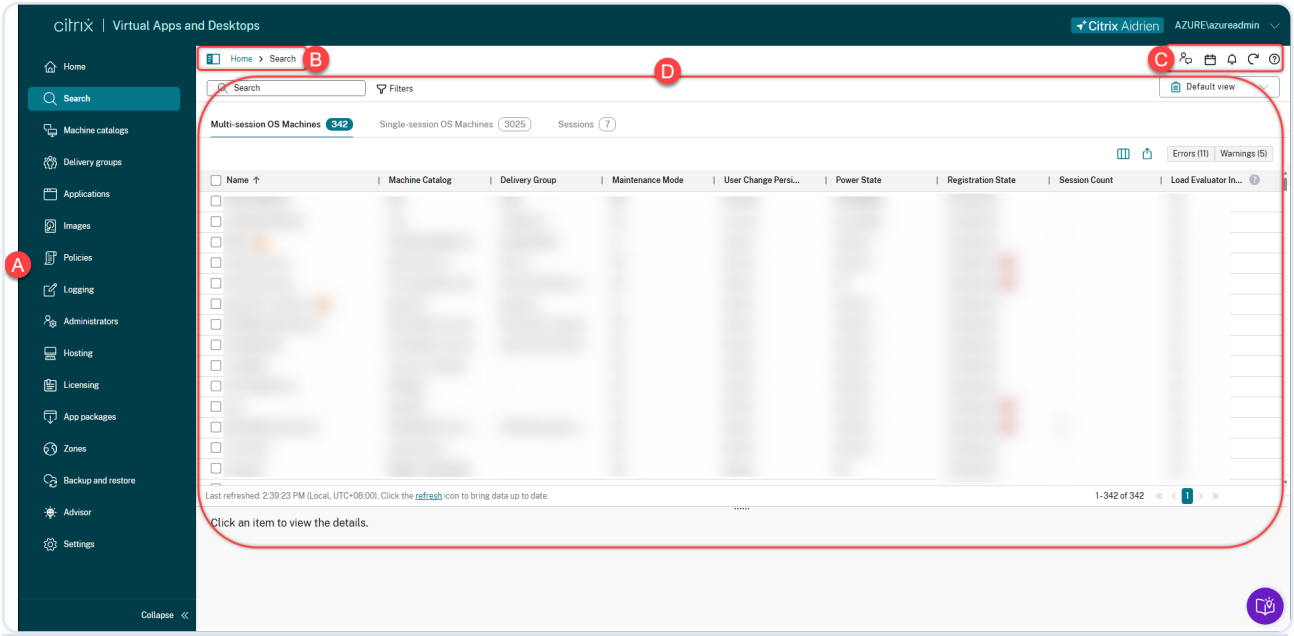
StoreFront 验证用户身份并管理用户访问的桌面和应用程序商店。它可以托管您的企业应用程序商店，为用户提供对其可用的桌面和应用程序的自助服务访问。它还跟踪用户的应用程序订阅、快捷方式名称和其他数据。这有助于确保用户在多个设备上获得一致的体验。

思杰工作区™ 应用

Citrix Workspace 应用程序安装在用户设备和其他端点（例如虚拟桌面）上，为用户提供对文档、应用程序和桌面的快速、安全、自助式访问。Citrix Workspace 应用程序提供对 Windows、Web 和软件即服务 (SaaS) 应用程序的按需访问。对于无法安装特定设备 Citrix Workspace 应用程序软件的设备，适用于 HTML5 的 Citrix Workspace 应用程序通过兼容 HTML5 的 Web 浏览器提供连接。

工作室

Web Studio 是一个基于 Web 的管理控制台，可让您配置和管理本地 Citrix Virtual Apps and Desktops 部署。



标注	区域	描述
A	导航菜单	允许您配置和管理 DaaS 部署以交付虚拟应用程序和桌面。示例包括：搜索、计算机目录、交付组等。有关详细信

标注	区域	描述
		息，请参阅规划和构建部署和管理部署。
B	面包屑导航	提供上下文并支持快速导航回更高级别的页面。
C	常用操作	显示常见操作，例如提交反馈、自定义主页、访问通知中心等。
		• 通知中心提供实时更新和 48 小时内长期运行操作的历史记录。操作运行时，状态通知会显示在常用操作区域下方，以指示其进度。
		• 任务中心显示所有任务的综合列表，按类别组织。用户界面提供筛选、搜索和其他与主视图一致的控件。您可以对任何列出的任务执行操作，包括**删除**和**查看详细信息**等常见操作，以及重新运行任务和导出子任务状态等特定于任务的操作。目前，任务中心支持硬件更新和操作系统磁盘重置任务。
F	工作窗格	显示导航菜单中选定节点的动作和详细信息。

有关详细信息，请参阅安装 Web Studio。

安全私有访问

Citrix Secure Private Access 本地解决方案通过以下方式增强了组织整体的安全性和合规性态势：使用 StoreFront 作为 Web 和 SaaS 应用程序的统一访问门户，以及作为 Citrix Workspace 集成部分的虚拟应用程序和桌面，轻松为基于浏览器的应用程序（内部 Web 应用程序和 SaaS 应用程序）提供零信任网络访问。该解决方案与现有版本的 NetScaler 和 StoreFront 兼容，无需更改版本。有关详细信息，请参阅适用于本地的 Secure Private Access。

思杰 Director

Director 是一种基于 Web 的工具，使 IT 支持和帮助台团队能够监控环境、在问题变得系统关键之前对其进行故障排除，并为最终用户执行支持任务。您可以使用一个 Director 部署连接和监控多个 Citrix Virtual Apps 或 Citrix Virtual Desktops 站点。

Director 显示：

- 来自控制器中代理服务的实时会话数据，其中包括代理服务从 VDA 中的代理程序获取的数据。
- 来自 Controller 中 Monitor Service 的历史站点数据。

Director 使用 Citrix Gateway 设备捕获的 ICA® 性能和启发式数据，从这些数据中构建分析，然后将其呈现给管理员。

您还可以使用 Windows 远程协助，通过 Director 查看并与用户的会话进行交互。

Citrix 许可证服务器

许可证服务器管理您的 Citrix 产品许可证。它与 Controller 通信以管理每个用户会话的许可，并与 Studio 通信以分配许可证文件。一个站点必须至少有一个许可证服务器来存储和管理您的许可证文件。

管理程序或其他服务

管理程序或其他服务托管您站点中的虚拟机。这些虚拟机可以是您用于托管应用程序和桌面的虚拟机，也可以是您用于托管 Citrix Virtual Apps and Desktops 组件的虚拟机。管理程序安装在专门用于运行管理程序和托管虚拟机的宿主机上。

Citrix Virtual Apps and Desktops 支持各种管理程序和其他服务。

尽管许多部署需要管理程序，但提供远程电脑访问时不需要管理程序。当您使用 Provisioning Services (PVS) 预配 VM 时，也不需要管理程序。

其他组件

以下组件也可以包含在 Citrix Virtual Apps and Desktops 部署中。有关详细信息，请参阅其文档。

Citrix 置备™

Citrix Provisioning（以前称为 Provisioning Services）是一个可选组件，可用于某些版本。它为预配虚拟机提供了 MCS 的替代方案。MCS 创建主映像的副本，而 PVS 则将主映像流式传输到用户设备。PVS 不需要管理程序即可执行此操作，因此您可以使用它来托管物理机。PVS 与 Controller 通信以向用户提供资源。

思杰网关

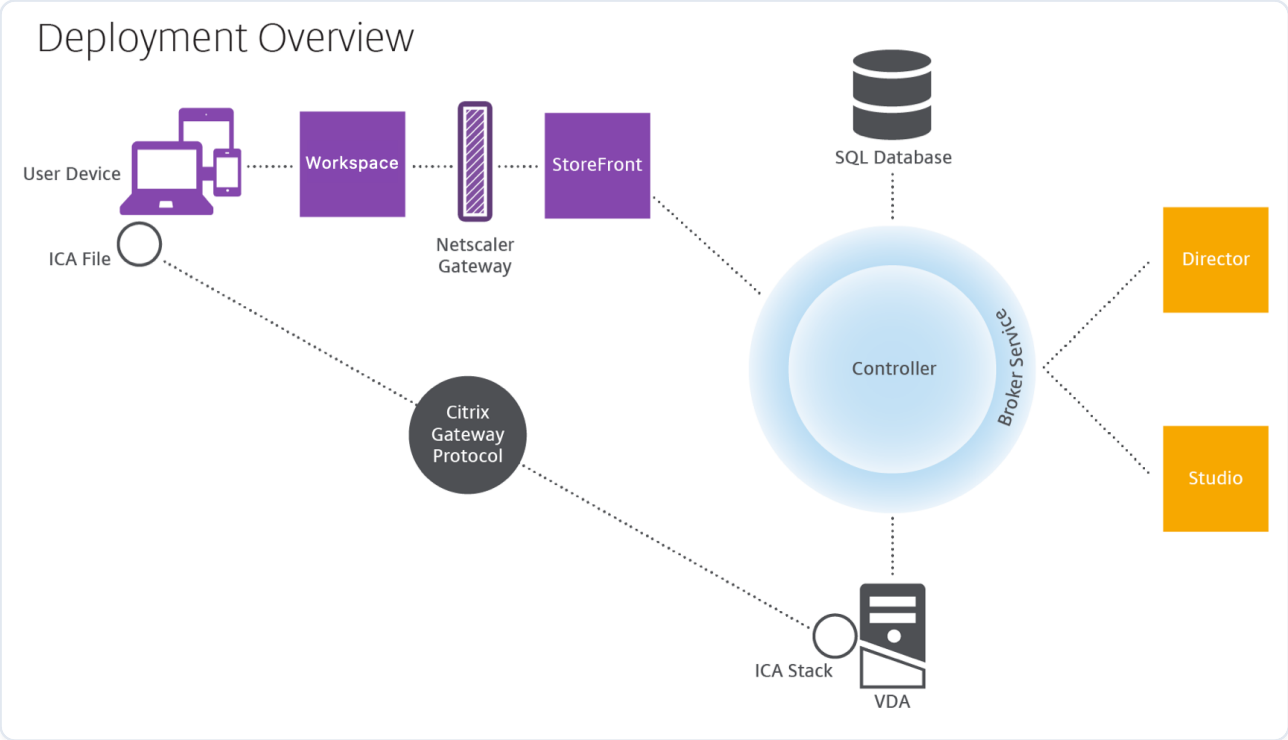
当用户从公司防火墙外部连接时，Citrix Virtual Apps and Desktops 可以使用 Citrix Gateway（以前称为 Access Gateway 和 NetScaler® Gateway）技术通过 TLS 保护这些连接。Citrix Gateway 或 VPX 虚拟设备是部署在非军事区 (DMZ) 中的 SSL VPN 设备。它通过公司防火墙提供单一安全访问点。

思杰 SD-WAN™

在将虚拟桌面交付给分支机构等远程位置用户的部署中，可以采用 Citrix SD-WAN 技术来优化性能。中继器可加速 WAN 上的性能。通过网络中的中继器，分支机构的用户可以在 WAN 上体验到类似 LAN 的性能。Citrix SD-WAN 可以优先处理用户体验的不同部分，例如，当通过网络发送大型文件或打印作业时，分支机构的用户体验不会下降。HDX™ WAN 优化提供令牌化压缩和数据去重，显著降低带宽要求并提高性能。

典型部署的工作原理

一个站点由具有专用角色的计算机组成，这些角色支持可伸缩性、高可用性和故障转移，并提供一种设计上安全的解决方案。一个站点包含安装了 VDA 的服务器和桌面计算机，以及管理访问的 Delivery Controller。



VDA 允许用户连接到桌面和应用程序。对于大多数交付方法，它安装在数据中心的虚拟机上，但它也可以安装在物理 PC 上以实现远程 PC 访问。

Controller 由独立的 Windows 服务组成，这些服务管理资源、应用程序和桌面，并优化和平衡用户连接。每个站点有一个或多个 Controller。由于会话受延迟、带宽和网络可靠性的影响，如果可能，请将所有 Controller 放置在同一 LAN 上。

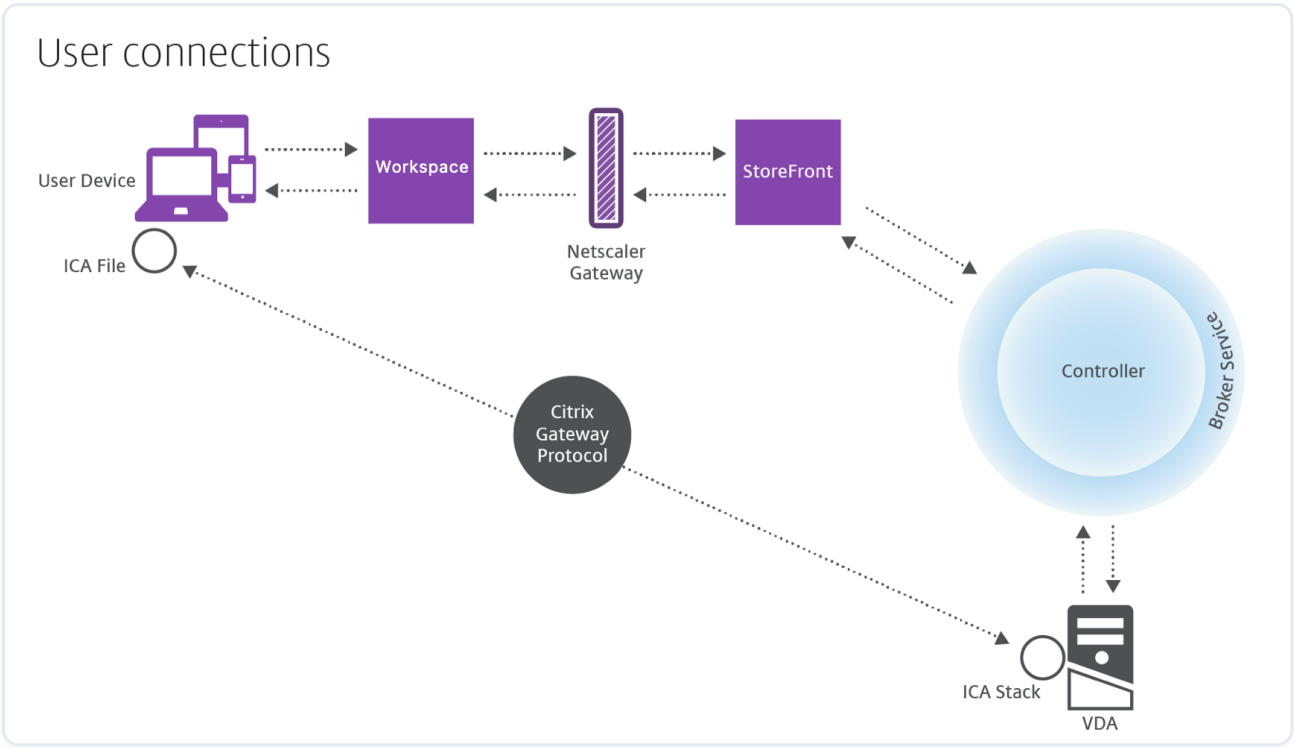
用户从不直接访问 Controller。VDA 充当用户和 Controller 之间的中介。当用户使用 StoreFront 登录时，其凭据会传递到 Controller 上的 Broker Service。然后，Broker Service 根据为其设置的策略获取配置文件和可用资源。

用户连接的处理方式

要启动会话，用户可以通过安装在用户设备上的 Citrix Workspace 应用程序连接，或通过 StoreFront 网站连接。

用户选择所需的物理或虚拟桌面或虚拟应用程序。

用户的凭据通过此路径访问 Controller，Controller 通过与 Broker Service 通信来确定所需的资源。Citrix 建议管理员在 StoreFront 上放置 SSL 证书，以加密来自 Citrix Workspace 应用程序的凭据。



Broker Service 确定用户可以访问哪些桌面和应用程序。

凭据验证后，有关可用应用程序或桌面的信息会通过 StoreFront-Citrix Workspace 应用程序路径发送回用户。当用户从该列表中选择应用程序或桌面时，该信息会沿路径返回到 Controller。然后，Controller 确定用于托管特定应用程序或桌面的正确 VDA。

Controller 将包含用户凭据的消息发送到 VDA，然后将有关用户和连接的所有数据发送到 VDA。VDA 接受连接并通过相同的路径将信息发送回 Citrix Workspace 应用程序。StoreFront 上会收集一组必需参数。然后，这些参数作为 Citrix-Workspace-app-StoreFront 协议对话的一部分发送到 Citrix Workspace 应用程序，或转换为独立计算架构 (ICA) 文件并下载。只要站点设置正确，凭据在此过程中始终保持加密状态。

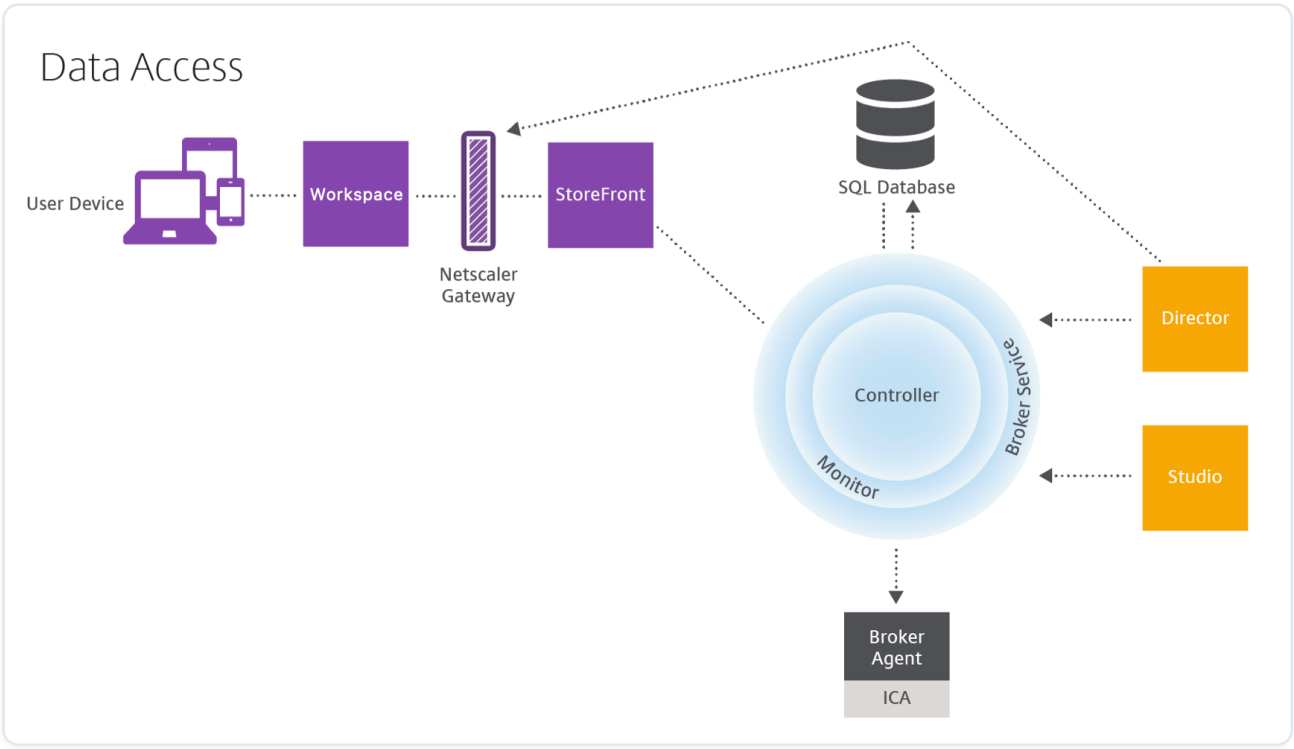
ICA 文件复制到用户设备，并在设备与 VDA 上运行的 ICA 堆栈之间建立直接连接。此连接绕过管理基础结构（Citrix Workspace 应用程序、StoreFront 和 Controller）。

Citrix Workspace 应用程序与 VDA 之间的连接使用 Citrix Gateway Protocol (CGP)。如果连接丢失，会话可靠性功能使用户能够重新连接到 VDA，而无需通过管理基础结构重新启动。可以在 Citrix 策略中启用或禁用会话可靠性。

客户端连接到 VDA 后，VDA 会通知 Controller 用户已登录。然后，Controller 会将此信息发送到站点数据库，并开始在监控数据库中记录数据。

数据访问的工作原理

每个 Citrix Virtual Apps and Desktops 会话都会生成 IT 人员可以通过 Studio 或 Director 访问的数据。使用 Studio，管理员可以从 Broker Agent 访问实时数据来管理站点。Director 访问相同的数据以及存储在监控数据库中的历史数据。它还从 NetScaler Gateway 访问 HDX 数据，以用于技术支持和故障排除。



在 Controller 中，Broker Service 报告计算机上每个会话的会话数据，提供实时数据。Monitor Service 还会跟踪实时数据并将其作为历史数据存储在监控数据库中。

Studio 仅与 Broker Service 通信。它仅访问实时数据。Director 与 Broker Service（通过 Broker Agent 中的插件）通信以访问站点数据库。

Director 还可以访问 Citrix Gateway 以获取有关 HDX 数据的信息。

交付桌面和应用程序

您可以使用计算机目录设置交付应用程序和桌面的计算机。然后，创建交付组以指定将可用的应用程序和桌面（使用目录中的计算机）以及哪些用户可以访问它们。或者，您可以创建应用程序组来管理应用程序集合。

计算机目录

计算机目录是作为单个实体进行管理的虚拟或物理机集合。这些计算机以及其上的应用程序或虚拟桌面是您提供给用户的资源。目录中的所有计算机都具有相同的操作系统和相同的 VDA。它们还具有相同的应用程序或虚拟桌面。

通常，您会创建一个主映像并使用它在目录中创建相同的 VM。对于 VM，您可以指定该目录中计算机的预配方法：Citrix 工具（Citrix Provisioning 或 MCS）或其他工具。或者，您可以使用自己的现有映像。在这种情况下，您必须单独管理目标设备，或使用第三方电子软件分发 (ESD) 工具统一管理。

有效的计算机类型包括：

- **多会话操作系统：** 具有多会话操作系统的虚拟或物理机。用于交付 Citrix Virtual Apps 发布的应用程序（也称为基于服务器的托管应用程序）和 Citrix Virtual Apps 发布的桌面（也称为服务器托管桌面）。这些计算机允许多个用户同时连接到它们。
- **单会话操作系统：** 具有单会话操作系统的虚拟或物理机。用于交付 VDI 桌面（运行单会话操作系统且可选择进行个性化设置的桌面）、VM 托管应用程序（来自单会话操作系统的应用程序）和托管物理桌面。一次只能一个用户连接到每个桌面。
- **远程电脑访问：** 允许远程用户从运行 Citrix Workspace 应用程序的任何设备访问其物理办公电脑。办公电脑通过 Citrix Virtual Desktops 部署进行管理，并且要求在允许列表中指定用户设备。

有关详细信息，请参阅Citrix Virtual Apps and Desktops 映像管理和创建计算机目录。

交付组

交付组指定哪些用户可以在哪些计算机上访问哪些应用程序、桌面或两者。交付组包含来自您的计算机目录的计算机，以及有权访问您站点的 Active Directory 用户。您可以根据用户的 Active Directory 组将用户分配到您的交付组，因为 Active Directory 组和交付组是根据相似要求对用户进行分组的方式。

每个交付组可以包含来自多个目录的计算机，每个目录可以为多个交付组提供计算机。但是，每台单独的计算机一次只能属于一个交付组。

您可以定义交付组中的用户可以访问哪些资源。例如，要向不同用户交付不同的应用程序，您可以在一个目录的主映像上安装所有应用程序，并在该目录中创建足够的计算机以分配给多个交付组。然后，您可以配置每个交付组以交付计算机上安装的不同应用程序子集。

有关详细信息，请参阅创建交付组。

应用程序组

应用程序组比使用更多交付组具有应用程序管理和资源控制优势。使用标记限制功能，您可以将现有计算机用于多个发布任务，从而节省与部署和管理更多计算机相关的成本。标记限制可以看作是

对交付组中的计算机进行细分（或分区）。应用程序组在隔离和排查交付组中部分计算机的问题时也很有用。

有关详细信息，请参阅创建应用程序组。

更多信息

- Citrix 虚拟应用和桌面图表
- 网络端口
- 数据库
- 支持的管理程序和其他服务

数据库

> **注意：**

> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

> Citrix Virtual Apps 或 Citrix Virtual Desktops™ 站点使用三个 SQL Server 数据库：

- **站点：**（也称为站点配置）存储正在运行的站点配置，以及当前的会话状态和连接信息。
- **日志记录：**（也称为配置日志记录）存储有关站点配置更改和管理活动的信息。当启用配置日志记录功能时（默认 = 启用），将使用此数据库。
- **监视：**存储 Director 使用的数据，例如会话和连接信息。

每个 Delivery Controller 都与站点数据库通信。Controller 与数据库之间需要 Windows 身份验证。可以拔下或关闭 Controller，而不会影响站点中的其他 Controller。但是，这意味着站点数据库构成单点故障。如果数据库服务器发生故障，现有连接将继续运行，直到用户注销或断开连接。有关站点数据库不可用时的连接行为的信息，请参阅 本地主机缓存。

Citrix 建议对数据库执行以下操作：

- **定期备份。**定期备份数据库，以便在数据库服务器发生故障时可以从备份中恢复。每个数据库的备份策略可能不同。有关详细信息，请参阅 CTX135207；但请注意，它指的是 CitrixXenDesktopDB，该数据库不再受支持或可供客户使用。
- **定期备份和还原站点、监视和日志记录 SQL Server 数据库。**有关 SQL Server 数据库的特定信息，请参阅 创建 SQL Server 数据库的完整备份和差异备份。

如果您的站点包含多个区域，请确保主区域始终包含站点数据库。每个区域中的 Controller 都与该数据库通信。

高可用性

有几种高可用性解决方案可供考虑，以确保自动故障转移：

- **AlwaysOn 可用性组（包括基本可用性组）：**此企业级高可用性和灾难恢复解决方案于 SQL Server 2012 中引入，可让您最大限度地提高一个或多个数据库的可用性。AlwaysOn 可用性组要求 SQL Server 实例驻留在 Windows Server 故障转移群集 (WSFC) 节点上。有关详细信息，请参阅 使用 SQL Server 的 Windows Server 故障转移群集。
- **SQL Server 数据库镜像：**数据库镜像可确保在活动数据库服务器丢失时，在几秒钟内发生自动故障转移过程，从而使用户通常不受影响。此方法比其他解决方案更昂贵，因为每个数据库服务器都需要完整的 SQL Server 许可证。您不能在镜像环境中使用 SQL Server Express 版本。
- **SQL 群集：**Microsoft SQL 群集技术可用于自动允许一台服务器接管另一台发生故障的服务器的任务和职责。但是，设置此解决方案更复杂，并且自动故障转移过程通常比 SQL 镜像等替代方案慢。
- **使用管理程序的高可用性功能：**使用此方法，您可以将数据库部署为虚拟机，并使用管理程序的高可用性功能。此解决方案比镜像便宜，因为它使用您现有的管理程序软件，并且您还可以使用 SQL Server Express 版本。但是，自动故障转移过程较慢，因为为数据库启动新机器可能需要时间，这可能会中断对用户的服务。

本地主机缓存功能补充了 SQL Server 高可用性最佳实践。即使站点数据库不可用，本地主机缓存也能让用户连接和重新连接到应用程序和桌面。有关详细信息，请参阅 本地主机缓存。

如果站点中的所有控制器都发生故障，您可以将 VDA 配置为在高可用性模式下运行，这允许用户继续访问其桌面和应用程序。在高可用性模式下，VDA 接受来自用户的直接 ICA 连接，而不是由控制器代理的连接。仅在与所有控制器通信失败的极少数情况下使用此功能。此功能不能替代其他高可用性解决方案。有关详细信息，请参阅 CTX 127564。

不支持在 SQL 群集或 SQL 镜像安装中的节点上安装控制器。

安装数据库软件

> **注意：**
>
> 从版本 2411 开始，您可以将 Azure SQL 托管实例用于数据库。

> 默认情况下，如果您在安装第一个 Delivery Controller™ 时未在该服务器上检测到其他 SQL Server 实例，则会安装 SQL Server Express 版本。此默认操作通常足以满足概念验证或试点部署的需求。但是，SQL Server Express 不支持 Microsoft 高可用性功能。

默认安装使用默认的 Windows 服务帐户和权限。有关这些默认值的详细信息，包括将 Windows 服务帐户添加到 sysadmin 角色，请参阅 Microsoft 文档。在此配置中，控制器使用网络服务帐户。控制器不需要任何额外的 SQL Server 角色或权限。

如有必要，您可以为数据库实例选择**隐藏实例**。在 Web Studio 中配置数据库地址时，请输入实例的静态端口号，而不是其名称。有关隐藏 SQL Server 数据库引擎实例的详细信息，请参阅 Microsoft 文档。

对于大多数生产部署以及任何使用 Microsoft 高可用性功能的部署，我们建议仅使用受支持的非 Express 版本的 SQL Server。请将 SQL Server 安装在除安装第一个控制器的服务器之外的其他计算机上。系统要求 列出了受支持的 SQL Server 版本。数据库可以驻留在一台或多台计算机上。

请确保在创建站点之前安装 SQL Server 软件。您不必创建数据库，但如果创建了，则必须为空。还建议配置 Microsoft 高可用性技术。

使用 Windows Update 使 SQL Server 保持最新。

通过站点创建向导设置数据库

在站点创建向导的**数据库**页面上指定数据库名称和地址（位置）。（请参阅 数据库地址格式。）为避免 Director 查询监视服务时出现潜在错误，请勿在监视数据库的名称中使用空格。

数据库页面提供了两种设置数据库的选项：自动和使用脚本。通常，如果您（Web Studio 用户和 Citrix 管理员）拥有所需的数据库权限，则可以使用自动选项。（请参阅 设置数据库所需的权限。）

创建站点后，您可以稍后更改配置日志记录和监视数据库的位置。请参阅 更改数据库位置。

要将站点配置为使用镜像数据库，请完成以下操作，然后继续执行自动或脚本设置过程。

1. 在两台服务器 A 和 B 上安装 SQL Server 软件。

2. 在服务器 A 上，创建打算用作主数据库的数据库。备份服务器 A 上的数据库，然后将其复制到服务器 B。
3. 在服务器 B 上，还原备份文件。
4. 在服务器 A 上启动镜像。

创建站点后，要验证镜像，请运行 PowerShell cmdlet `get-configdbconnection` 以确保连接字符串中的故障转移伙伴已设置为镜像。

如果您稍后在镜像数据库环境中添加、移动或删除 Delivery Controller，请参阅Delivery Controllers。

自动设置

如果您具有所需的数据库权限，请通过完成以下步骤设置数据库：

1. 在站点创建向导的**数据库**页面上，选择**从 Studio 创建和设置数据库**。
2. 提供主数据库的名称和地址。
3. 配置以下 SQL Server 连接选项，以提高数据库连接设置的安全性和灵活性：

   - **加密**：指定连接的加密级别。
   - **信任服务器证书**：选择此项可绕过服务器证书验证。
   - **证书中的主机名**：输入服务器证书必须匹配的主机名。此设置可确保更严格的证书验证。

   有关更多信息，请参阅这篇 Microsoft 文章。

如果您指定的地址处存在数据库，则该数据库必须为空。如果指定地址处不存在数据库，系统会通知您找不到数据库，然后询问您是否要为您创建数据库。当您确认该操作时，Web Studio 会自动创建数据库，然后为主数据库和副本数据库应用初始化脚本。

脚本化设置

如果您没有所需的数据库权限，请向拥有这些权限的人员（例如数据库管理员）寻求帮助。操作顺序如下：

1. 在站点创建向导的**数据库**页面上，选择**生成脚本以手动设置**。此操作会为以下每个主数据库和副本数据库生成以下三种类型的脚本：站点数据库、监视数据库和日志记录数据库。

   - *名称中包含“SysAdmin”的脚本*。此脚本用于创建数据库和 Delivery Controller 登录名。这些任务需要 securityadmin 权限。
   - *名称中包含“DbOwner”的脚本*。此脚本用于在数据库中创建用户角色、添加登录名，然后创建数据库架构。这些任务需要 `db_owner` 权限。

- *名称中包含“Mixed”的脚本*。一个脚本中包含所有任务，无论所需的权限如何。

您可以指明脚本的存储位置。

> **注意：**
>
> 在企业环境中，数据库设置包括可能由具有不同角色（权限）的不同团队处理的脚本：`securityadmin` 或 `db_owner`。如果适用，您可以首先让具有 `securityadmin` 角色的管理员运行“SysAdmin”脚本，然后让具有 `db_owner` 权限的管理员运行“DbOwner”脚本。要生成这些脚本，您还可以使用 PowerShell。有关详细信息，请参阅首选数据库权限脚本。

2. 将这些脚本提供给您的数据库管理员。站点创建向导将在此处自动停止。当您稍后返回以继续站点创建时，系统会提示您。

数据库管理员随后创建数据库。每个数据库必须具有以下特征：

- 使用以 `_CI_AS_KS` 结尾的排序规则。我们建议使用以 `_100_CI_AS_KS` 结尾的排序规则。
- 为获得最佳性能，请启用 SQL Server Read-Committed Snapshot。有关详细信息，请参阅 CTX 137161。
- 配置了高可用性功能（如果适用）。
- 要配置镜像，首先将数据库设置为使用完整恢复模式（简单模式是默认设置）。将主数据库备份到文件并将其复制到镜像服务器。然后，在镜像服务器上还原备份文件。最后，在主服务器上启动镜像。

数据库管理员使用 SQLCMD 命令行实用程序或 SQL Server Management Studio 的 SQLCMD 模式执行以下操作：

- 在 `xxx_Replica.sql` 高可用性 SQL Server 数据库实例上运行每个脚本（如果配置了高可用性）
- 在主 SQL Server 数据库实例上运行每个 `xxx\_Principal.sql` 脚本。

有关 SQLCMD 详细信息，请参阅 Microsoft 文档。

当所有脚本成功完成后，数据库管理员会将三个主数据库地址提供给 Citrix 管理员。

Web Studio 会提示您继续创建站点。您将返回到**数据库**页面，完成以下步骤：

1. 输入地址。

2. 配置以下 SQL Server 连接选项，以提高数据库连接设置的安全性和灵活性：

   - **加密**：指定连接的加密级别。
   - **信任服务器证书**：选择此项可绕过服务器证书验证。
   - **证书中的主机名**：输入服务器证书必须匹配的主机名。此设置可确保更严格的证书验证。

   有关更多信息，请参阅这篇 Microsoft 文章。

如果无法联系托管数据库的任何服务器，则会显示错误消息。

设置数据库所需的权限

您必须是本地管理员和域用户才能创建和初始化数据库（或更改数据库位置）。您还必须具有某些 SQL Server 权限。以下权限可以通过 Active Directory 组成员身份显式配置或获取。如果您的 Web Studio 用户凭据不包含这些权限，系统将提示您输入 SQL Server 用户凭据。

操作	目的	服务器角色	数据库角色
创建数据库	创建合适的空数据库	`dbcreator`	
创建架构	创建所有特定于服务的架构并将第一个控制器添加到站点	`securityadmin` *	`db_owner`
添加控制器	将控制器（第一个除外）添加到站点	`securityadmin` *	`db_owner`
添加控制器（镜像服务器）	将控制器登录添加到当前处于镜像数据库镜像角色中的数据库服务器	`securityadmin` *	
移除控制器	从站点移除控制器	**	`db_owner`
更新架构	应用架构更新或热修复		`db_owner`

* 尽管技术上更具限制性，但在实践中，您可以将 `securityadmin` 服务器角色视为等同于 `sysadmin` 服务器角色。

** 当从站点中移除控制器时，控制器登录到数据库服务器的凭据不会被移除。这是为了避免可能移除同一台计算机上除此 Citrix 产品之外的其他服务正在使用的登录凭据。如果不再需要，必须手动移除该登录凭据。此操作需要 `securityadmin` 服务器角色成员身份。

使用 Web Studio 执行这些操作时，Web Studio 用户必须拥有明确属于相应服务器角色的数据库服务器帐户，或者能够提供此类帐户的凭据。

首选数据库权限脚本

在企业环境中，数据库设置包括必须由具有不同角色（权限）的不同团队处理的脚本：`securityadmin` 或 `db_owner`。

使用 PowerShell，您可以指定首选数据库权限。指定非默认值会导致创建单独的脚本。一个脚本包含需要 `securityadmin` 角色的任务。另一个脚本仅需要 `db_owner` 权限，并且可以由 Citrix 管理员运行，而无需联系数据库管理员。

在 `get-*DBSchema` cmdlet 中，`-DatabaseRights` 选项具有以下有效值：

- `SA`：生成一个脚本，用于创建数据库和 Delivery Controller 登录凭据。这些任务需要 `securityadmin` 权限。
- `DBO`：生成一个脚本，用于在数据库中创建用户角色、添加登录凭据，然后创建数据库架构。这些任务需要 `db_owner` 权限。
- `Mixed`：（默认）所有任务都在一个脚本中，无论所需的权限如何。

有关详细信息，请参阅 cmdlet 帮助。

数据库地址格式

您可以使用以下任一形式指定数据库地址：

- `ServerName`
- `ServerName\InstanceName`
- `ServerName,PortNumber`

对于 AlwaysOn 可用性组，请在位置字段中指定该组的侦听器。

对于数据库镜像，仅指定主服务器地址。Citrix Site Manager 会根据主服务器定位镜像服务器。

有关如何配置独立 SQL Server、数据库镜像和 Always On 高可用性的更多信息，请参阅此CTX 文章。

更改数据库位置

创建站点后，可以更改*配置日志记录*和*监视*数据库的位置。但是，不能更改*站点*数据库的位置。更改数据库位置时，请记住以下注意事项：

- 以前数据库中的数据不会导入到新数据库中。
- 检索日志时，无法从两个数据库聚合日志。
- 新数据库中的第一个日志条目指示发生了数据库更改，但它未标识以前的数据库。
- 启用强制日志记录时，无法更改配置日志记录数据库的位置。
- 不支持在 SQL Server 和 Azure SQL 之间更改数据库位置。

要更改数据库的位置，请执行以下操作：

1. 如果使用 Microsoft SQL Server，请确保在要驻留数据库的服务器上安装了受支持的版本。根据需要设置高可用性功能。
2. 登录到 Web Studio，然后在左侧窗格中选择**设置**。
3. 找到**数据库**磁贴并选择**编辑**。
4. 在**管理数据库**页面上，选择要为其指定新位置的数据库，然后在操作栏中选择**更改数据库**。
5. 指定新位置和数据库名称。如果数据库托管在 Azure SQL 上，请键入具有管理数据库权限的服务主体的凭据。
6. 如果您希望 Web Studio 创建数据库并且您具有相应的权限，请单击**完成**。出现提示时，单击**完成**，然后 Web Studio 会自动创建数据库。Web Studio 尝试使用您的凭据访问数据库。如果失败，系统会提示您输入数据库用户的凭据。然后，Web Studio 会将数据库架构上传到数据库。凭据仅在数据库创建期间保留。
7. 如果您不希望 Web Studio 创建数据库，或者您没有足够的权限，请单击**生成数据库脚本**。生成的脚本包含手动创建数据库和（如果需要）镜像数据库的说明。在上传架构之前，请确保数据库为空，并且至少有一个用户具有访问和更改数据库的权限。

更多信息

- 数据库大小调整工具。
- 在使用 SQL Server 高可用性解决方案时，调整站点数据库大小 和 配置连接字符串。

交付方法

Citrix Virtual Apps and Desktops™ 提供多种交付方法。单一的交付方法可能无法满足您的所有要求。

简介

选择合适的应用程序交付方法有助于提高可扩展性、管理效率和用户体验。

- **已安装的应用程序：** 应用程序是基础桌面映像的一部分。安装过程涉及将 dll、exe 和其他文件复制到映像驱动器，以及修改注册表。有关详细信息，请参阅创建计算机目录。
- **流式应用程序 (Microsoft App-V)：** 应用程序经过配置文件处理，并根据需要通过网络交付到桌面。应用程序文件和注册表设置放置在虚拟桌面上的容器中，并与基础操作系统相互隔离。这种隔离有助于解决兼容性问题。有关详细信息，请参阅部署和交付 App-V 应用程序。
- **分层应用程序 (Citrix App Layering)：** 每个层包含一个应用程序、代理或操作系统。通过集成一个操作系统层、一个平台层（VDA、Citrix Provisioning agent）和多个应用程序层，管理员可以轻松创建新的可部署映像。分层简化了日常维护，因为操作系统、代理和应用程序都存在于单个层中。更新层时，所有包含该层的已部署映像都会更新。有关详细信息，请参阅Citrix App Layering。
- **托管的 Windows 应用程序：** 安装在多用户 Citrix Virtual Apps 主机上并作为应用程序而非桌面部署的应用程序。用户可以从 VDI 桌面或端点设备无缝访问托管的 Windows 应用程序，从而隐藏了应用程序远程执行的事实。有关详细信息，请参阅创建交付组。
- **本地应用程序：** 部署在端点设备上的应用程序。应用程序界面显示在用户的托管 VDI 会话中，即使它在端点上执行。有关详细信息，请参阅本地应用程序访问和 URL 重定向。

对于桌面，请考虑已发布的桌面或 VDI 桌面。

Citrix Virtual Apps™ 已发布的应用程序和桌面

使用多会话操作系统计算机交付 Citrix Virtual Apps and Desktops 已发布的应用程序和已发布的桌面。

用例：

- 您希望通过经济高效的基于服务器的交付方式，最大限度地降低向众多用户交付应用程序的成本，同时提供安全、高清的用户体验。
- 您的用户执行明确定义的任务，不需要个性化或脱机访问应用程序。用户可以包括任务型工作人员，例如呼叫中心操作员和零售员工，或共享工作站的用户。
- 应用程序类型：任何应用程序。

优点和注意事项：

- 数据中心内可管理且可扩展的解决方案。
- 最具成本效益的应用程序交付解决方案。

- 托管应用程序集中管理，用户无法修改应用程序。这提供了始终如一、安全可靠的用户体验。
- 用户必须在线才能访问其应用程序。

用户体验：

- 用户从 StoreFront™、其**开始**菜单或您提供的 URL 请求一个或多个应用程序。
- 应用程序以虚拟方式交付，并在用户设备上以高清无缝显示。
- 根据配置文件设置，用户更改会在用户应用程序会话结束时保存。否则，更改将被删除。

处理、托管和交付应用程序：

- 应用程序处理在托管计算机上进行，而不是在用户设备上进行。托管计算机可以是物理机或虚拟机。
- 应用程序和桌面驻留在多会话操作系统计算机上。
- 计算机通过计算机目录变得可用。
- 计算机目录中的计算机被组织成交付组，这些交付组向用户组交付相同的应用程序集。
- 多会话操作系统计算机支持托管桌面或应用程序（或两者兼有）的交付组。

会话管理和分配：

- 多会话操作系统计算机从一台计算机运行多个会话，以向多个同时连接的用户交付多个应用程序和桌面。每个用户都需要一个会话，他们可以从该会话运行所有托管应用程序。

  例如，用户登录并请求一个应用程序。该计算机上的一个会话将对其他用户不可用。第二个用户登录并请求该计算机托管的应用程序。同一台计算机上的第二个会话现在不可用。如果两个用户都请求更多应用程序，则不需要额外的会话，因为用户可以使用同一会话运行多个应用程序。如果再有两名用户登录并请求桌面，并且同一台计算机上有两个会话可用，则该单台计算机现在正在使用四个会话来托管四个不同的用户。
- 在分配用户的交付组中，将选择负载最低的服务器上的计算机。当用户登录时，会随机分配一台具有可用会话的计算机，以向该用户交付应用程序。

VM 托管应用程序

使用单会话操作系统计算机交付 VM 托管应用程序

用例：

- 您需要一个安全、提供集中管理并支持每台主机服务器多个用户的基于客户端的应用程序交付解决方案。您希望为这些用户提供以高清无缝显示的应用程序。

- 您的用户包括内部员工、外部承包商、第三方协作者以及其他临时团队成员。您的用户不需要离线访问托管应用程序。
- 应用程序类型：可能与其他应用程序不兼容或可能与操作系统交互的应用程序，例如 Microsoft .NET Framework。这些类型的应用程序非常适合在虚拟机上托管。

优点和注意事项：

- 主映像上的应用程序和桌面在数据中心内的计算机上安全地管理、托管和运行，从而提供更具成本效益的应用程序交付解决方案。
- 登录时，用户可以随机分配到配置为托管相同应用程序的交付组中的一台计算机。您还可以静态地将一台计算机分配给单个用户，以便在该用户每次登录时交付应用程序。静态分配的计算机允许用户在虚拟机上安装和管理自己的应用程序。
- 单会话操作系统计算机不支持运行多个会话。因此，每个用户登录时都会占用交付组中的一台计算机，并且用户必须在线才能访问其应用程序。
- 此方法会增加处理应用程序所需的服务器资源量，并增加用户数据所需的存储量。

用户体验：

- 与在多会话操作系统计算机上托管共享应用程序相同的无缝应用程序体验。

处理、托管和交付应用程序：

- 与多会话操作系统计算机相同，不同之处在于它们是虚拟单会话操作系统计算机。

会话管理和分配：

- 单会话操作系统计算机从一台计算机运行单个桌面会话。仅访问应用程序时，单个用户可以使用多个应用程序（并且不限于单个应用程序），因为操作系统将每个应用程序视为一个新会话。
- 在交付组中，用户登录时可以访问静态分配的计算机（每次用户登录到同一台计算机），或根据会话可用性选择的随机分配的计算机。

VDI 桌面

使用单会话操作系统计算机交付 Citrix Virtual Apps and Desktops VDI 桌面。

VDI 桌面托管在虚拟机上，并为每个用户提供桌面操作系统。

VDI 桌面比已发布的桌面需要更多资源，但不需要在其上安装的应用程序支持基于服务器的操作系统。此外，根据您选择的 VDI 桌面类型，这些桌面可以分配给单个用户。这允许用户高度个性化。

为 VDI 桌面创建计算机目录时，您可以创建以下类型的桌面之一：

- **随机非持久性桌面，也称为池化 VDI 桌面：** 每次用户登录到这些桌面之一时，该用户都会连接到从桌面池中选择的桌面。该池基于单个主映像。计算机重新启动时，对桌面的所有更改都将丢失。
- **静态非持久性桌面：** 首次登录期间，会从桌面池中为用户分配一个桌面。（池中的每台计算机都基于单个主映像。）首次使用后，每次用户登录使用桌面时，该用户都会连接到首次使用时分配的同一桌面。计算机重新启动时，对桌面的所有更改都将丢失。
- **静态持久性桌面：** 与其他类型的 VDI 桌面不同，用户可以完全个性化这些桌面。首次登录期间，会从桌面池中为用户分配一个桌面。该用户的后续登录会连接到首次使用时分配的同一桌面。计算机重新启动时，对桌面的更改将保留。

远程电脑访问

远程电脑访问是 Citrix Virtual Apps and Desktops 的一项功能，它使组织能够轻松地允许员工以安全的方式远程访问公司资源。Citrix 平台通过让用户访问其物理办公电脑来实现这种安全访问。如果用户可以访问其办公电脑，他们就可以访问完成工作所需的所有应用程序、数据和资源。远程电脑访问消除了引入和提供其他工具以适应远程办公的需要。例如，虚拟桌面或应用程序及其关联的基础设施。

远程电脑访问使用与交付虚拟桌面和应用程序相同的 Citrix Virtual Apps and Desktops 组件。因此，部署和配置远程电脑访问的要求和过程与部署 Citrix Virtual Apps and Desktops 以交付虚拟资源的要求和过程相同。这种一致性提供了统一的管理体验。用户通过使用 Citrix HDX™ 交付其办公电脑会话来获得最佳用户体验。

有关更多信息，请参阅Remote PC Access。

网络端口

完整的网络端口信息在 Citrix 技术使用的通信端口 中提供。

安装 Citrix® 组件时，操作系统的宿主防火墙也会默认更新，以匹配默认网络端口。

您可能需要端口信息：

- 用于法规遵从。
- 如果 Citrix Virtual Apps and Desktops™ 组件与其他 Citrix 产品或组件之间存在网络防火墙，以便您可以适当地配置该防火墙。
- 如果您使用第三方宿主防火墙（例如防恶意软件软件包随附的防火墙），而不是操作系统的宿主防火墙。
- 如果您更改这些组件上的宿主防火墙配置（通常是 Windows 防火墙服务）。

- 如果您重新配置组件功能以使用不同的端口或端口范围，然后想要禁用或阻止配置中未使用的端口。

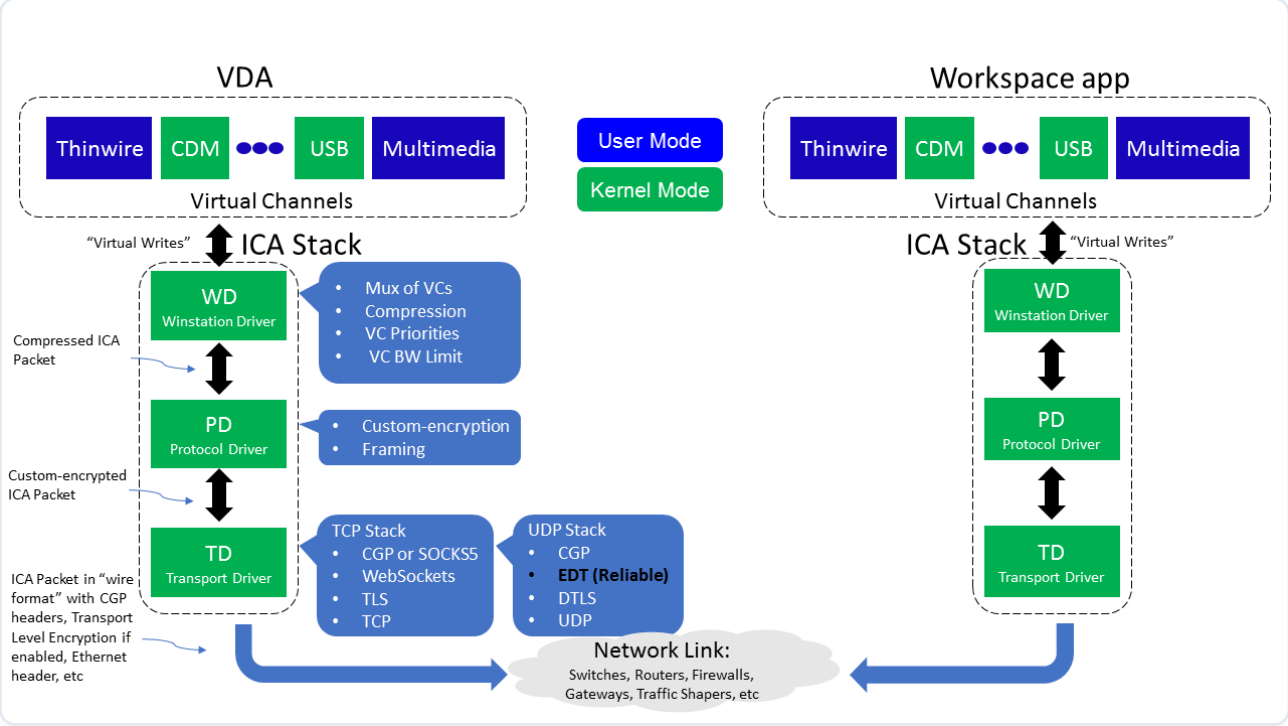
某些端口已在 Internet Assigned Numbers Authority (IANA) 注册。有关这些分配的详细信息可在 `<http://www.iana.org/assignments/port-numbers>` 处获取。但是，IANA 持有的描述性信息并不总是反映当今的使用情况。

此外，VDA 和 Delivery Controller™ 上的操作系统需要传入端口供其自身使用。有关详细信息，请参阅 Microsoft Windows 文档。

HDX™

> **警告：**
>
> 不正确地编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix® 无法保证可以解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。在编辑注册表之前，请务必备份注册表。

> Citrix HDX 代表了一系列广泛的技术，旨在为集中式应用程序和桌面用户在任何设备上、通过任何网络提供高清体验。



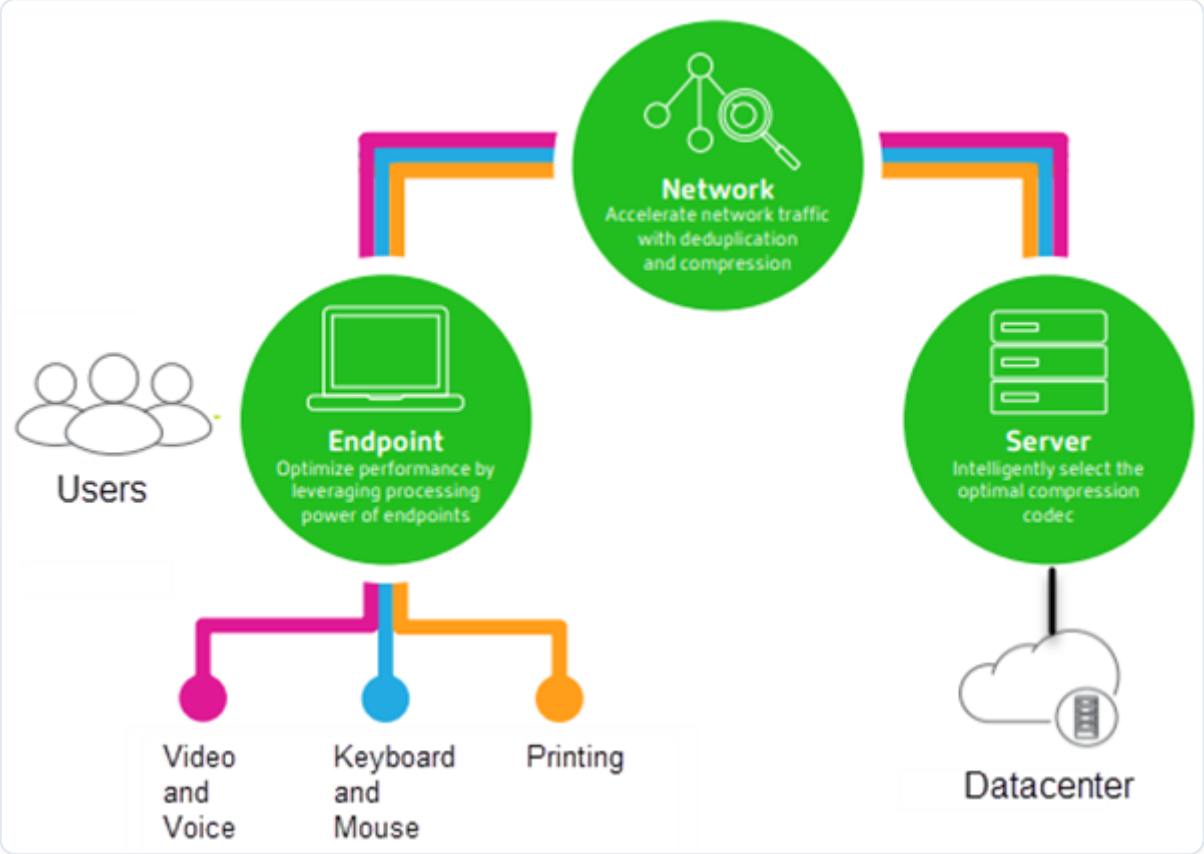
HDX 围绕以下三个技术原则设计：

- 智能重定向

- 自适应压缩
- 数据去重

以不同组合应用这些原则，可优化 IT 和用户体验，降低带宽消耗，并提高每台托管服务器的用户密度。

- **智能重定向** - 智能重定向会检查屏幕活动、应用程序命令、端点设备以及网络和服务器功能，以即时确定如何以及在何处呈现应用程序或桌面活动。呈现可以在端点设备或托管服务器上进行。
- **自适应压缩** - 自适应压缩允许在带宽较窄的网络连接上交付丰富的多媒体显示。HDX 首先评估多个变量，例如输入、设备和显示类型（文本、视频、语音和多媒体）。它选择最佳压缩编解码器以及 CPU 和 GPU 使用的最佳比例。然后，它根据每个独特的用户和基础进行智能调整。这种智能调整是针对每个用户，甚至每个会话进行的。



- **数据去重** - 网络流量去重可减少客户端和服务器之间传输的总数据量。它通过利用常用数据（例如位图图形、文档、打印作业和流媒体）中的重复模式来实现这一点。缓存这些模式只允许更改通过网络传输，从而消除重复流量。HDX 还支持多播多媒体流，即源端的一次传输可供一个位置的多个订阅者查看，而不是为每个用户建立一对一连接。

有关详细信息，请参阅通过高清用户工作区提高工作效率。

在设备端

HDX 利用用户设备的计算能力来增强和优化用户体验。HDX 技术可确保用户在其虚拟桌面或应用程序中获得流畅、无缝的多媒体内容体验。工作区控制使用户能够暂停虚拟桌面和应用程序，并在他们离开的位置从不同的设备恢复工作。

在网络上

HDX 集成了高级优化和加速功能，可在任何网络（包括低带宽和高延迟的 WAN 连接）上提供最佳性能。

HDX 功能可适应环境变化。这些功能平衡了性能和带宽。它们为每个用户场景应用了最佳技术，无论桌面或应用程序是在公司网络上本地访问，还是从公司防火墙外部远程访问。

在数据中心

HDX 利用服务器的处理能力和可扩展性来提供高级图形性能，无论客户端设备功能如何。

Citrix Director 提供的 HDX 通道监控显示用户设备上已连接 HDX 通道的状态。

HDX 洞察

HDX Insight 是 NetScaler® Network Inspector 和 Performance Manager 与 Director 的集成。它捕获有关 ICA 流量的数据，并提供实时和历史详细信息的仪表板视图。此数据包括客户端和服务器端 ICA 会话延迟、ICA 通道的带宽使用情况以及每个会话的 ICA 往返时间值。

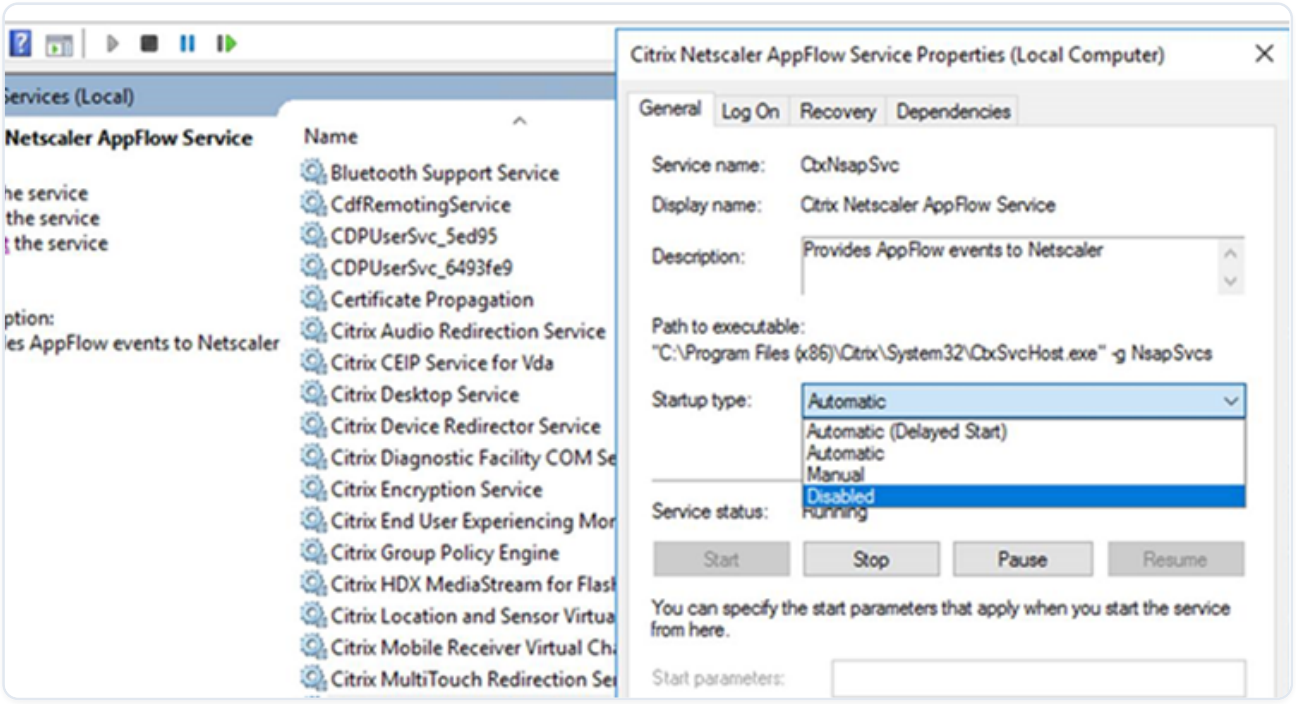
您可以启用 NetScaler 使用 HDX Insight 虚拟通道以未压缩格式传输所有必需的数据点。如果禁用此功能，NetScaler 设备将解密和解压缩分布在各种虚拟通道上的 ICA® 流量。使用单个虚拟通道可降低复杂性、增强可扩展性并更具成本效益。

最低要求：

- NetScaler 版本 12.0 内部版本 57.x
- 适用于 Windows 的 Citrix Workspace™ 应用程序 1808
- 适用于 Windows 的 Citrix Receiver 4.10
- 适用于 Mac 的 Citrix Workspace 应用程序 1808
- 适用于 Mac 的 Citrix Receiver 12.8

启用或禁用 HDX Insight 虚拟通道

要禁用此功能，请将 Citrix NetScaler Application Flow 服务属性设置为“禁用”。要启用此功能，请将服务设置为“自动”。无论哪种情况，我们都建议您在更改这些属性后重新启动服务器计算机。默认情况下，此服务处于启用状态（自动）。



在虚拟桌面上体验 HDX 功能

- 要了解浏览器内容重定向（四种 HDX 多媒体重定向技术之一）如何加速 HTML5 和 WebRTC 多媒体内容的交付：

  a. 下载 Chrome 浏览器扩展程序 并将其安装到虚拟桌面。

  b. 要体验浏览器内容重定向如何加速向虚拟桌面交付多媒体内容，请在桌面上从包含 HTML5 视频的网站（例如 YouTube）观看视频。用户不知道浏览器内容重定向何时运行。要查看是否正在使用浏览器内容重定向，请快速拖动浏览器窗口。您会看到视口和用户界面之间存在延迟或画面不同步。您还可以右键单击网页，然后在菜单中查找**关于 HDX 浏览器重定向**。

- 要了解 HDX 如何提供高清音频：

  a. 将您的 Citrix 客户端配置为最高音频质量；有关详细信息，请参阅 Citrix Workspace 应用程序文档。

  b. 在桌面上使用数字音频播放器（例如 iTunes）播放音乐文件。

HDX 默认情况下为大多数用户提供卓越的图形和视频体验，无需配置。默认情况下，可为大多数用例提供最佳体验的 Citrix 策略设置处于启用状态。

- HDX 会根据客户端、平台、应用程序和网络带宽自动选择最佳交付方法，然后根据不断变化的条件进行自我调整。
- HDX 可优化 2D 和 3D 图形及视频的性能。
- HDX 使用户设备能够直接从 Internet 或 Intranet 上的源提供商流式传输多媒体文件，而不是通过主机服务器。如果未满足此客户端内容获取的要求，则媒体交付将回退到服务器端内容获取和多媒体重定向。通常，无需调整多媒体重定向功能策略。
- 当多媒体重定向不可用时，HDX 会向虚拟桌面交付丰富的服务器渲染视频内容：在包含高清视频的网站（例如 `<http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/>`）上观看视频。

须知：

- 有关 HDX 功能的支持和要求信息，请参阅系统要求文章。除非另有说明，HDX 功能适用于受支持的 Windows 多会话操作系统和 Windows 单会话操作系统计算机，以及远程电脑访问桌面。
- 此内容介绍了如何优化用户体验、提高服务器可伸缩性或降低带宽要求。有关使用 Citrix 策略和策略设置的信息，请参阅本版本的 Citrix 策略 文档。
- 对于包含编辑注册表的说明，请务必谨慎：不正确地编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证可以解决因不正确使用注册表编辑器而导致的问题。使用注册表编辑器时，风险自负。编辑注册表之前，请务必备份注册表。

客户端自动重新连接和会话可靠性

访问托管应用程序或桌面时，可能会发生网络中断。为了获得更流畅的重新连接体验，我们提供了客户端自动重新连接和会话可靠性功能。在默认配置中，会话可靠性首先启动，然后是客户端自动重新连接。

客户端自动重新连接：

客户端自动重新连接会重新启动客户端引擎以重新连接到已断开连接的会话。客户端自动重新连接会在设置中指定的时间后关闭（或断开连接）用户会话。如果客户端自动重新连接正在进行中，系统会向用户发送应用程序和桌面网络中断通知，如下所示：

- **桌面。** 会话窗口显示为灰色，并显示一个倒计时器，指示重新连接发生前的时间。
- **应用程序。** 会话窗口关闭，并向用户显示一个对话框，其中包含一个倒计时器，显示尝试重新连接前的时间。

在客户端自动重新连接期间，会话会重新启动以期望网络连接。在客户端自动重新连接进行时，用户无法与会话交互。

重新连接时，已断开连接的会话会使用保存的连接信息重新连接。用户可以正常与应用程序和桌面交互。

默认客户端自动重新连接设置：

- 客户端自动重新连接超时：120 秒
- 客户端自动重新连接：已启用
- 客户端自动重新连接身份验证：已禁用
- 客户端自动重新连接日志记录：已禁用

有关详细信息，请参阅自动客户端重新连接策略设置。

会话可靠性：

会话可靠性可在网络中断时无缝重新连接 ICA 会话。会话可靠性会在设置中指定的时间后关闭（或断开）用户会话。会话可靠性超时后，自动客户端重新连接设置将生效，尝试将用户重新连接到已断开连接的会话。会话可靠性正在进行时，应用程序和桌面网络中断通知会按如下方式发送给用户：

- **桌面。** 会话窗口变为半透明，并显示一个倒计时器，指示重新连接发生的时间。
- **应用程序。** 窗口变为半透明，同时通知区域会弹出连接中断提示。

会话可靠性处于活动状态时，用户无法与 ICA 会话交互。但是，网络中断后，用户操作（如击键）会立即缓冲几秒钟，并在网络可用时重新传输。

重新连接后，客户端和服务器将从它们在协议交换中的同一点恢复。会话窗口将不再半透明，并且会为应用程序显示相应的通知区域弹出窗口。

默认会话可靠性设置

- 会话可靠性超时：180 秒
- 重新连接 UI 不透明度级别：80%
- 会话可靠性连接：已启用
- 会话可靠性端口号：2598

有关详细信息，请参阅 会话可靠性策略设置。

NetScaler 与自动客户端重新连接和会话可靠性：

如果在服务器上启用了多流和多端口策略，并且以下任何或所有条件为真，则自动客户端重新连接将不起作用：

- 会话可靠性在 NetScaler Gateway 上已禁用。
- NetScaler 设备上发生故障转移。
- NetScaler SD-WAN 与 NetScaler Gateway 配合使用。

HDX 自适应吞吐量

HDX 自适应吞吐量通过调整输出缓冲区智能地微调 ICA 会话的峰值吞吐量。输出缓冲区的数量最初设置为一个较高的值。这个较高的值允许数据更快、更高效地传输到客户端，尤其是在高延迟网络中。提供更好的交互性、更快的文件传输、更流畅的视频播放、更高的帧速率和分辨率，从而增强用户体验。

会话交互性会持续测量，以确定 ICA 会话中的任何数据流是否对交互性产生不利影响。如果发生这种情况，吞吐量会降低，以减少大数据流对会话的影响，并允许交互性恢复。

> **重要提示：**

> HDX 自适应吞吐量通过将此机制从客户端移动到 VDA 来改变输出缓冲区的设置方式，无需手动配置。

> 此功能有以下要求：

- VDA 版本 1811 或更高版本
- 适用于 Windows 的 Workspace 应用程序 1811 或更高版本

提高发送到用户设备的图像质量

以下视觉显示策略设置控制从虚拟桌面发送到用户设备的图像质量。

- 视觉质量。控制用户设备上显示的图像的视觉质量：中、高、始终无损、构建到无损（默认 = 中）。使用默认设置“中”时的实际视频质量取决于可用带宽。
- 目标帧速率。指定从虚拟桌面发送到用户设备的最大每秒帧数（默认 = 30）。对于 CPU 较慢的设备，指定较低的值可以改善用户体验。每秒支持的最大帧速率为 60。
- 显示内存限制。指定会话的最大视频缓冲区大小（以千字节为单位）（默认 = 65536 KB）。对于需要更高颜色深度和更高分辨率的连接，请增加此限制。您可以计算所需的最大内存。

> **注意：**

> **显示内存限制**设置已弃用。通过此更改，Citrix 现在不再限制显示内存。相反，将分配所需的最小内存量，以确保客户端的显示布局得到充分适应。

提高视频会议性能

许多流行的视频会议应用程序已通过多媒体重定向针对 Citrix Virtual Apps and Desktops 交付进行了优化（例如，请参阅 HDX RealTime Optimization Pack）。对于未优化的应用程序，HDX 网络摄像头视频压缩可提高会话期间视频会议中网络摄像头的带宽效率和延迟容忍度。此技术通过专用的多媒体虚拟通道传输网络摄像头流量。与同步 HDX 即插即用 USB 重定向支持相比，此技术使用的带宽更少，并且在 WAN 连接上运行良好。

Citrix Workspace 应用程序用户可以通过选择 Desktop Viewer 的“麦克风和网络摄像头”设置中的 **“不使用我的麦克风或网络摄像头”** 来覆盖默认行为。为防止用户从 HDX 网络摄像头视频压缩切换，请使用“ICA 策略设置”>“USB 设备策略设置”下的策略设置禁用 USB 设备重定向。

HDX 网络摄像头视频压缩要求启用以下策略设置（所有设置默认均已启用）。

- 客户端音频重定向
- 客户端麦克风重定向
- 多媒体会议

如果网络摄像头支持硬件编码，HDX 视频压缩默认使用硬件编码。硬件编码可能比软件编码消耗更多带宽。要强制进行软件压缩，请将以下 DWORD 键值添加到注册表项：HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1。

网络流量优先级

使用支持服务质量 (Quality of Service) 的路由器，可为会话的多个连接上的网络流量分配优先级。有四个 TCP 流和两个用户数据报协议 (UDP) 流可用于在用户设备和服务器之间传输 ICA 流量：

- TCP 流 - 实时、交互式、后台和批量
- UDP 流 - 语音和 Framehawk 显示远程处理

每个虚拟通道都与特定的优先级相关联，并在相应的连接中传输。您可以根据用于连接的 TCP 端口号独立设置通道。

对于安装在 Windows 10、Windows 8 和 Windows 7 计算机上的 Virtual Delivery Agent (VDA)，支持多通道流连接。请与您的网络管理员协作，确保在网络路由器上正确分配了在 **“多端口策略”** 设置中配置的通用网关协议 (CGP) 端口。

仅当配置了多个会话可靠性端口或 CGP 端口时，才支持服务质量。

警告：

使用此功能时，请使用传输安全性。Citrix 建议使用 Internet 协议安全性 (IPsec) 或传输层安全性 (TLS)。仅当连接通过支持多流 ICA 的 NetScaler Gateway 时，才支持 TLS 连接。在内部公司网络上，不支持使用 TLS 的多流连接。

要为多个流连接设置服务质量，请将以下 Citrix 策略设置添加到策略中（有关详细信息，请参阅 多流连接策略设置）：

- 多端口策略 - 此设置指定跨多个连接的 ICA 流量端口，并建立网络优先级。
  - 从 CGP 默认端口优先级列表中选择一个优先级。默认情况下，主端口 (2598) 具有高优先级。
  - 根据需要，在 CGP port1、CGP port2 和 CGP port3 中键入更多 CGP 端口，并为每个端口指定优先级。每个端口必须具有唯一的优先级。

  在 VDA 上明确配置防火墙以允许额外的 TCP 流量。
- 多流计算机设置 - 此设置默认禁用。如果您的环境中使用支持多流的 Citrix NetScaler SD-WAN，则无需配置此设置。在使用第三方路由器或旧版 NetScaler SD-WAN 以实现所需的服务质量时，请配置此策略设置。
- 多流用户设置 - 此设置默认禁用。

要使包含这些设置的策略生效，用户必须注销，然后重新登录网络。

显示或隐藏远程语言栏

语言栏在应用程序会话中显示首选输入语言。如果此功能已启用（默认），则可以从适用于 Windows 的 Citrix Workspace 应用程序中的“**高级首选项 > 语言栏**”UI 显示或隐藏语言栏。通过在 VDA 端使用注册表设置，可以禁用客户端对语言栏功能的控制。如果此功能已禁用，则客户端 UI 设置不生效，并且每个用户的当前设置决定语言栏状态。有关详细信息，请参阅改善用户体验。

要从 VDA 禁用客户端对语言栏功能的控制：

1. 在注册表编辑器中，导航到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI。
2. 创建一个 DWORD 值项 SeamlessFlags，并将其设置为 0x40000。

Unicode 键盘映射

非 Windows Citrix Receiver 使用本地键盘布局 (Unicode)。如果用户更改本地键盘布局和服务器键盘布局（扫描代码），它们可能不同步，并且输出不正确。例如，用户 1 将本地键盘布局从英语更改为德语。用户 1 然后将服务器端键盘更改为德语。即使两个键盘布局都是德语，它们也可能不同步，从而导致字符输出不正确。

启用或禁用 Unicode 键盘布局映射

默认情况下，此功能在 VDA 侧处于禁用状态。要启用此功能，请在 VDA 上使用注册表编辑器 regedit 切换启用此功能。添加以下注册表项：

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名称: EnableKlMap

类型: DWORD

值：1

要禁用此功能，请将 **EnableKlMap** 设置为 0 或删除 **CtxKlMap** 密钥。

启用 Unicode 键盘布局映射兼容模式

默认情况下，Unicode 键盘布局映射会自动挂钩一些 Windows API，以便在您更改服务器端的键盘布局时重新加载新的 Unicode 键盘布局映射。少数应用程序无法被挂钩。为了保持兼容性，您可以将此功能更改为兼容模式，以支持这些未被挂钩的应用程序。添加以下注册表项：

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名称: DisableWindowHook

类型: DWORD

值：1

要使用正常的 Unicode 键盘布局映射，请将 **DisableWindowHook** 设置为 0。

Citrix ICA® 虚拟通道

> **警告：**

> 错误编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。编辑注册表之前，请务必备份注册表。

什么是 ICA 虚拟通道?

Citrix Workspace™ 应用程序与 Citrix Virtual Apps and Desktops™ 服务器之间的大部分功能和通信通过虚拟通道进行。虚拟通道是使用 Citrix Virtual Apps and Desktops 服务器进行远程计算体验的必要组成部分。虚拟通道用于：

- 音频
- COM 端口
- 磁盘
- 图形
- LPT 端口
- 打印机
- 智能卡
- 第三方自定义虚拟通道
- 视频

有时会随 Citrix Virtual Apps and Desktops™ 服务器和 Citrix Workspace 应用程序产品的新版本发布新的虚拟通道，以提供更多功能。

虚拟通道(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/ica-virtual-channels-1.png)

虚拟通道由与服务器端应用程序通信的客户端虚拟驱动程序组成。Citrix Virtual Apps and Desktops 附带各种虚拟通道。它们旨在允许客户和第三方供应商使用提供的软件开发工具包 (SDK) 之一创建自己的虚拟通道。

虚拟通道提供了一种安全的方式来完成各种任务。例如，在 Citrix Virtual Apps 服务器上运行的应用程序与客户端设备通信，或者应用程序与客户端环境通信。

在客户端，虚拟通道对应于虚拟驱动程序。每个虚拟驱动程序都提供特定的功能。有些是正常运行所必需的，有些是可选的。虚拟驱动程序在表示层协议级别运行。通过多路复用 Windows Station (WinStation) 协议层提供的通道，可以同时激活多个协议。

以下功能包含在此注册表路径下的 VirtualDriver 注册表值中：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0`

或者

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0`（适用于 64 位）

- Thinwire3.0（必需）
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- 剪贴板
- ClientComm
- ClientAudio
- LicenseHandler (必需)
- TWI (必需)
- 智能卡
- ICACTL (必需)
- SSPI
- TwainRdr
- 用户体验
- Vd3d

> **注意：**
>
> 您可以通过从注册表项中删除一个或多个这些值来禁用特定的客户端功能。例如，如果要删除客户端剪贴板，请删除单词 **Clipboard**。

> 此列表包含客户端虚拟驱动程序文件及其各自的功能。Citrix Virtual Apps 和适用于 Windows 的 Citrix Workspace 应用程序使用这些文件。它们以动态链接库（用户模式）的形式存在，而不是 Windows 驱动程序（内核模式），通用 USB 虚拟通道中描述的通用 USB 除外。

- vd3dn.dll – 用于桌面合成重定向的 Direct3D 虚拟通道

- vdcamN.dll – 双向音频
- vdcdm30n.dll – 客户端驱动器映射
- vdcom30N.dll - 客户端 COM 端口映射
- vdcpm30N.dll – 客户端打印机映射
- vdctln.dll – ICA 控制通道
- vddvc0n.dll – 动态虚拟通道
- vdeuemn.dll - 最终用户体验监控
- vdgusbn.dll – 通用 USB 虚拟通道
- vdkbhook.dll – 透明按键直通
- vdlfpn.dll – 经由类似 UDP 传输的 Framehawk 显示通道
- vdmmn.dll – 多媒体支持
- vdmrvc.dll – 移动接收器虚拟通道
- vdmtchn.dll - 多点触控支持
- vdscardn.dll – 智能卡支持
- vdsens.dll – 传感器虚拟通道
- vdspl30n.dll – 客户端 UPD
- vdsspin.dll – 科尔贝罗斯
- vdtuin.dll – 透明用户界面
- vdtw30n.dll – 客户端 Thinwire
- vdtwin.dll – 无缝
- vdtwn.dll – 特温

一些虚拟通道被编译到其他文件中。例如，剪贴板映射在 wfica32.exe 中可用。

64 位兼容性

适用于 Windows 的 Citrix Workspace 应用程序与 64 位兼容。与大多数为 32 位编译的二进制文件一样，这些客户端文件也有 64 位编译的等效项：

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll

- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

通用 USB 虚拟通道

通用 USB 虚拟通道实现使用两个内核模式驱动程序以及虚拟通道驱动程序 vdgusbn.dll：

- ctxusbm.sys
- ctxusbr.sys

ICA 虚拟通道的工作原理

虚拟通道以多种方式加载。Shell（服务器的 WfShell 和工作站的 PicaShell）加载一些虚拟通道。一些虚拟通道作为 Windows 服务托管。

由 Shell 加载的虚拟通道模块，例如：

- EUEM
- 特文
- 剪贴板
- 多媒体
- 无缝会话共享
- 时区

有些以内核模式加载，例如：

- CtxDvcs.sys – 动态虚拟通道
- Icausbb.sys – 通用 USB 重定向
- Picadm.sys – 客户端驱动器映射
- Picaser.sys – COM 端口重定向
- Picapar.sys – LPT 端口重定向

服务器端的图形虚拟通道

`ctxgfx.exe` 为基于工作站和终端服务器的会话托管图形虚拟通道。`Ctxgfx` 托管与相应驱动程序交互的平台特定模块（RDSH 为 `Icardd.dll`，工作站为 `vdod.dll` 和 `vidd.dll`）。

对于 XenDesktop® 3D Pro 部署，VDA 上会为相应的 GPU 安装 OEM 图形驱动程序。`Ctxgfx` 加载专用适配器模块以与 OEM 图形驱动程序交互。

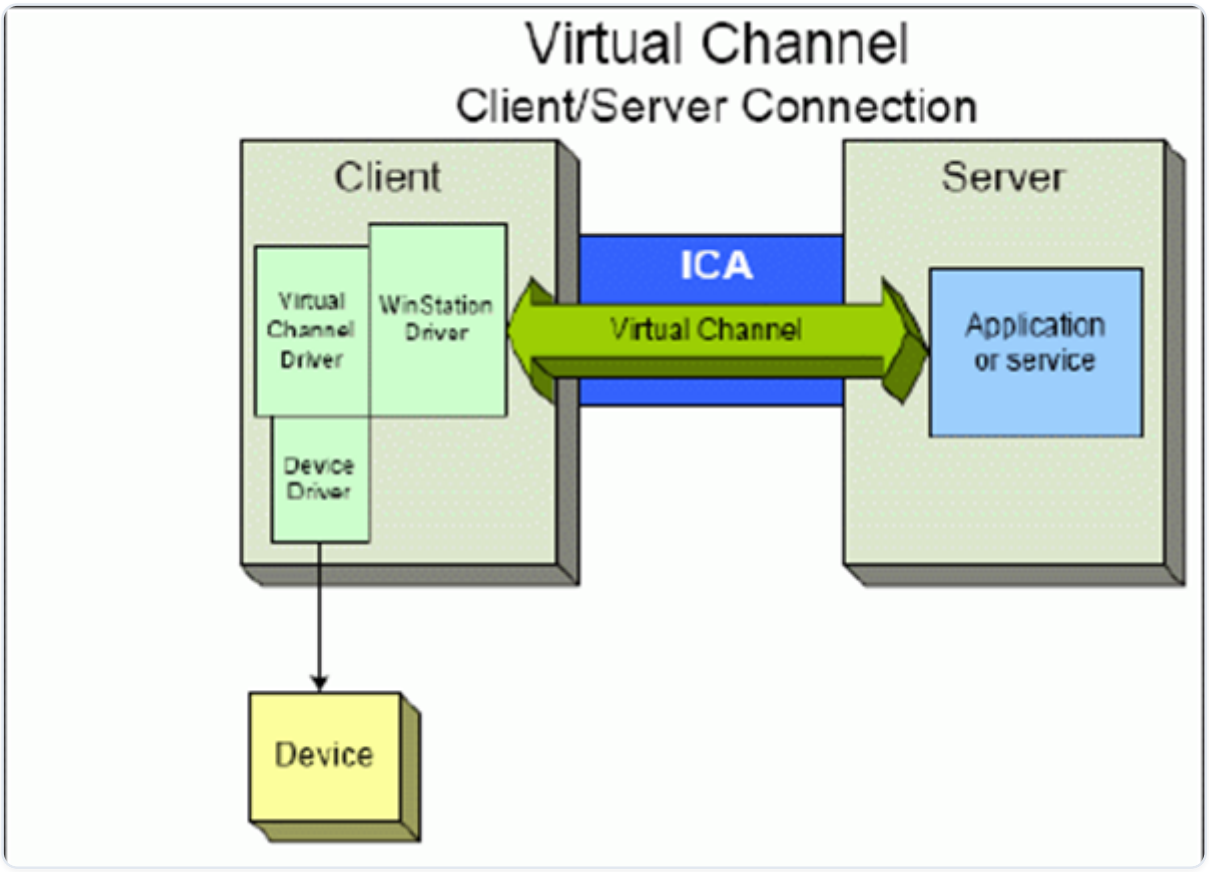
在 Windows 服务中托管专用通道

在 Citrix Virtual Apps and Desktops 服务器上，各种通道作为 Windows 服务托管。这种托管为会话中的多个应用程序和服务器上的多个会话提供了一对多的语义。此类服务的示例包括：

- Citrix 设备重定向器服务
- Citrix 动态虚拟通道服务
- Citrix 最终用户体验监控服务
- Citrix 位置和传感器虚拟通道服务
- Citrix 多点触控重定向服务
- Citrix 打印管理器服务
- Citrix 智能卡服务
- Citrix 音频重定向服务 (仅限 Citrix Virtual Desktops™)
- Citrix ICA 状态通道服务

Citrix Virtual Apps 上的音频虚拟通道使用 Windows 音频服务进行托管。

在服务器端，所有客户端虚拟通道都通过 WinStation 驱动程序 Wdica.sys 路由。在客户端，内置于 wfica32.exe 中的相应 WinStation 驱动程序轮询客户端虚拟通道。此图说明了虚拟通道客户端-服务器连接。



本概述包含使用虚拟通道的客户端-服务器数据交换。

1. 客户端连接到 Citrix Virtual Apps and Desktops 服务器。客户端将其支持的虚拟通道信息传递给服务器。
2. 服务器端应用程序启动，获取虚拟通道的句柄，并可选择查询有关该通道的附加信息。
3. 客户端虚拟驱动程序和服务器端应用程序使用以下两种方法传递数据：
   - 如果服务器应用程序有数据要发送到客户端，数据会立即发送到客户端。当客户端收到数据时，WinStation 驱动程序会从 ICA 流中解复用虚拟通道数据，并立即将其传递给客户端虚拟驱动程序。
   - 如果客户端虚拟驱动程序有数据要发送到服务器，数据会在 WinStation 驱动程序下次轮询时发送。当服务器收到数据时，数据会排队，直到虚拟通道应用程序读取它。无法通知服务器虚拟通道应用程序已收到数据。
4. 当服务器虚拟通道应用程序完成时，它会关闭虚拟通道并释放所有已分配的资源。

使用虚拟通道 SDK 创建自己的虚拟通道

> **注意：**

Citrix SDK 可在 `<https://developer.cloud.com>` 的 Citrix Developer 门户中获取。

使用虚拟通道 SDK 创建虚拟通道需要中级编程知识。使用此方法可在客户端和服务器之间提供主要的通信路径。例如，如果您要在客户端实现设备（如扫描仪）的使用，以便在会话中与某个进程一起使用。

注意：

- 虚拟通道 SDK 需要 WFAPI SDK 来编写虚拟通道的服务器端。
- 由于 Citrix Virtual Apps and Desktops 的安全性增强，您必须指定允许在 ICA 会话中打开哪些虚拟通道。有关详细信息，请参阅虚拟通道允许列表策略设置。

使用 ICA 客户端对象 SDK 创建自己的虚拟通道

使用 ICA 客户端对象 (ICO) 创建虚拟通道比使用虚拟通道 SDK 更容易。通过在程序中使用 **CreateChannels** 方法创建命名对象来使用 ICO。

重要提示：

由于从 10.00 版及更高版本的 Citrix Receiver for Windows（以及 Citrix Workspace apps for Windows）开始增强了安全性，因此在创建 ICO 虚拟通道时必须执行额外的步骤。

虚拟通道的直通功能

当您在 ICA 会话（也称为直通会话）中使用适用于 Windows 的 Citrix Workspace 应用程序时，Citrix 提供的大多数虚拟通道都可未经修改地运行。在额外跃点中使用客户端时需要考虑一些事项。

以下功能在单跳或多跳中以相同方式运行：

- 客户端 COM 端口映射
- 客户端驱动器映射
- 客户端打印机映射
- 客户端 UPD
- 最终用户体验监控

- 通用 USB
- Kerberos (科尔贝罗斯)
- 多媒体支持
- 智能卡支持
- 透明密钥直通
- Twain (特温)

由于固有的延迟特性以及在每个跃点执行的压缩、解压缩和渲染等因素，客户端每增加一个跃点，性能可能会受到影响。受影响的区域包括：

- 双向音频
- 文件传输
- 通用 USB 重定向
- 无缝
- 思睿线

> **重要提示：**
>
> 默认情况下，在直通会话中运行的客户端实例映射的客户端驱动器仅限于连接客户端的客户端驱动器。

Citrix Virtual Desktop 会话与 Citrix Virtual App 会话之间虚拟通道的直通功能

当您在 Citrix Virtual Desktops 服务器（也称为直通会话）上的 ICA 会话中使用适用于 Windows 的 Citrix Workspace 应用程序时，Citrix 提供的大多数虚拟通道都可以未经修改地运行。

具体来说，在 Citrix Virtual Desktops 服务器上，有一个 VDA 挂钩会运行 **picaPassthruHook**。此挂钩使客户端认为它正在 CPS 服务器上运行，并将客户端置于其传统的直通模式。

我们支持以下传统虚拟通道及其功能：

- 客户端
- 客户端 COM 端口映射
- 客户端驱动器映射
- 客户端打印机映射

- 通用 USB（由于性能限制）
- 多媒体支持
- 智能卡支持
- SSON
- 透明按键直通

安全性和 ICA 虚拟通道

确保使用安全是规划、开发和实施虚拟通道的重要组成部分。本文档中包含多处对特定安全领域的引用。

最佳实践

在**连接**和**重新连接**时打开虚拟通道。在注销和**断开连接**时关闭虚拟通道。

在创建使用虚拟通道功能的脚本时，请记住以下准则。

虚拟通道命名：

您最多可以创建 32 个虚拟通道。这 32 个通道中有 17 个是为特殊用途保留的。

- 虚拟通道名称的长度不得超过七个字符。
- 前三个字符保留给供应商名称，后四个字符保留给通道类型。例如，**CTXAUD** 表示 Citrix 音频虚拟通道。

虚拟通道通过七个字符（或更短）的 ASCII 名称来引用。在 ICA 协议的某些早期版本中，虚拟通道是按数字编号的。现在，这些数字根据 ASCII 名称动态分配，从而简化了实施。仅为内部使用开发虚拟通道代码的用户可以使用任何不与现有虚拟通道冲突的七个字符名称。仅使用数字以及大写和小写 ASCII 字符。添加自己的虚拟通道时，请遵循现有的命名约定。有几个预定义通道。预定义通道以 OEM 标识符 CTX 开头，并且仅供 Citrix 使用。

双跳支持：

虚拟通道	是否支持双跳？
音频	否
浏览器内容重定向	否
CDM	是

虚拟通道	是否支持双跳？
CEIP	否
剪贴板	是
康体纽姆 (MRVC)	否
控制虚拟通道	是
HTML5 视频重定向 (v1)	是
键盘、鼠标	是
多点触控	否
NSAPVC	否
打印	是
SensVC	否
智能卡	是
特温	是
USB 虚拟通道	是
WAYCOM 设备 -K2M 使用 USB VC	是
网络摄像头视频压缩	是
Windows Media 重定向	是

另请参阅

- ICA 虚拟通道 SDK
- Citrix Developer Network 是所有涉及使用 Citrix SDK 的技术资源和讨论的中心。在此网络中，您可以找到 SDK、示例代码和脚本、扩展和插件以及 SDK 文档。其中还包括 Citrix Developer Network 论坛，您可以在其中就每个 Citrix SDK 进行技术讨论。

思杰虚拟应用和桌面™ 中的双跳

在 Citrix 客户端会话的上下文中，“双跳”一词指在 Citrix Virtual Desktop 会话中运行的 Citrix Virtual App 会话。下图说明了双跳。

双跳(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/double-hop.png)

在双跳场景中，当用户连接到在单会话操作系统 VDA（称为 VDI）或多会话操作系统 VDA（称为已发布的桌面）上运行的 Citrix Virtual Desktop 时，这被视为第一跳。用户连接到虚拟桌面后，可以启动 Citrix Virtual Apps™ 会话。这被视为第二跳。

您可以使用双跳部署模型来支持各种用例。Citrix Virtual Desktop 和 Citrix Virtual Apps 环境由不同实体管理的情况是一个常见示例。此方法还可以有效解决应用程序兼容性问题。

系统要求

所有 Citrix Virtual Apps and Desktops 版本（包括 Citrix Cloud™ 服务）都支持双跳。

第一跳必须使用受支持的单会话或多会话操作系统 VDA 版本以及 Citrix Workspace 应用程序。第二跳必须使用受支持的多会话操作系统 VDA 版本。有关支持的版本，请参阅产品矩阵页面。

为了获得最佳性能和兼容性，Citrix 建议使用与正在使用的 VDA 版本相同或更新的 Citrix 客户端。

在第一跳涉及第三方（非 Citrix）虚拟桌面解决方案与 Citrix Virtual Apps 会话结合使用的环境中，支持仅限于 Citrix Virtual Apps 环境。如果出现与第三方虚拟桌面相关的任何问题（包括但不限于 Citrix Workspace™ 应用程序兼容性、硬件设备重定向和会话性能），Citrix 只能提供有限的技术支持。作为故障排除的一部分，可能需要在第一跳使用 Citrix Virtual Desktop。

双跳中 HDX™ 的部署注意事项

通常，双跳中的每个会话都是唯一的，并且客户端-服务器功能隔离到给定的跳。本节包含 Citrix 管理员需要特别考虑的领域。Citrix 建议客户对所需的 HDX 功能进行彻底测试，以确保用户体验和性能足以满足给定的环境配置。

图形

在第一跳和第二跳上使用默认图形设置（选择性编码）。对于HDX 3D Pro，Citrix 强烈建议所有需要图形加速的应用程序在第一跳中本地运行，并为 VDA 提供适当的 GPU 资源。

延迟

端到端延迟会影响整体用户体验。考虑第一跳和第二跳之间增加的延迟。这对于硬件设备的重定向尤为重要。

多媒体

服务器端（会话内）的音频和视频内容渲染在第一跳中表现最佳。第二跳中的视频播放需要在第一跳进行解码和重新编码，从而增加带宽和硬件资源利用率。只要可能，音频和视频内容必须限制在第一跳。

USB 设备重定向

HDX 包含通用和优化重定向模式，以支持各种 USB 设备类型。请特别注意每个跳中使用的模式，并使用下表作为参考以获得最佳结果。有关通用和优化重定向模式的更多信息，请参阅通用 USB 设备。

第一跳（VDI 或已发布的桌面）	第二跳（虚拟应用）	支持说明
优化	优化	推荐（基于设备支持）。例如，USB 大容量存储、TWAIN 扫描仪、网络摄像头、音频。
通用	通用	适用于没有优化选项的设备。
通用	优化	尽管技术上可行，但建议在设备支持可用时，在两个跳之间都使用优化模式。
优化	通用	不支持

注意：

由于 USB 协议固有的“多话”特性，性能可能会在跳之间下降。功能和结果因特定设备和应用程序要求而异。在所有设备重定向情况下，强烈建议进行验证测试，这在双跳场景中尤为重要。

FIDO2 重定向

只要中间跳 VDA 上安装的适用于 Windows 的 Citrix Workspace 应用程序版本为 2503 或更高版本，双跳场景就支持 FIDO2 重定向。此外，仅当第二次跳连接通过 ICA 进行时才支持此功能。

支持例外

双跳会话支持大多数 HDX 功能和特性，但以下情况除外：

- 浏览器内容重定向

- 本地应用程序访问
- 适用于 Skype for Business 的实时优化包
- 针对 Microsoft Teams 的优化

安装和配置

在开始每个部署步骤之前，请查看引用的文章，以了解在部署过程中您将看到和指定的内容。

使用以下顺序部署 Citrix Virtual Apps and Desktops。

准备

查看 准备安装 并完成所有必要的任务。

- 在何处查找有关概念、功能、与早期版本的差异、系统要求和数据库的信息。
- 决定在何处安装核心组件时的注意事项。
- 权限和 Active Directory 要求。
- 有关可用安装程序、工具和接口的信息。

安装核心组件

安装 Delivery Controller、Web Studio、Citrix Director 和 Citrix 许可证服务器。您还可以安装 Citrix StoreFront。有关详细信息，请参阅 安装核心组件 或 使用命令行安装。

创建站点

安装核心组件并启动 Studio 后，系统会提示您 创建站点。

安装一个或多个 Virtual Delivery Agent (VDA)

在运行 Windows 操作系统的计算机上安装 VDA，可以在主映像上安装，也可以直接在每台计算机上安装。请参阅 安装 VDA 或 使用命令行安装。如果您想通过 Active Directory 安装 VDA，则提供了示例 脚本。

对于运行 Linux 操作系统的计算机，请遵循 Linux Virtual Delivery Agent 中的指导。

对于远程电脑访问部署，请在每台办公电脑上安装适用于单会话操作系统的 VDA。如果您只需要核心 VDA 服务，请使用独立 `VDAWorkstationCoreSetup.exe` 安装程序和您现有的电子软件分发 (ESD) 方法。（准备安装 介绍了可用的 VDA 安装程序。）

安装可选组件

如果您计划使用 Citrix Universal Print Server，请在其打印服务器上安装其服务器组件。请参阅 安装核心组件 或 使用命令行安装。

要允许 StoreFront 使用 SAML 断言等身份验证选项，请安装 Citrix Federated Authentication Service。

要让最终用户更好地控制其用户帐户，请安装 Self-Service Password Reset。

（可选）将更多 Citrix 组件集成到您的 Citrix Virtual Apps and Desktops™ 部署中。

- Citrix Provisioning 是一个可选组件，它通过将主映像流式传输到目标设备来预配计算机。
- Citrix Gateway 是一种安全的应用程序访问解决方案，它为管理员提供精细的应用程序级策略和操作控制，以保护对应用程序和数据的访问。
- Citrix SD-WAN 是一组设备，可优化 WAN 性能。

创建计算机目录

在 Studio 中创建站点后，系统会引导您 创建计算机目录。

目录可以包含物理机或虚拟机 (VM)。虚拟机可以从主映像创建。当使用管理程序或其他服务提供 VM 时，您首先在该主机上创建主映像。然后，在创建目录时，您指定该映像，该映像用于创建 VM。

创建交付组

在 Web Studio 中创建第一个计算机目录后，系统会引导您 创建交付组。

交付组指定哪些用户可以访问所选目录中的计算机以及这些用户可用的应用程序。

创建应用程序组（可选）

创建交付组后，您可以选择 创建应用程序组。您可以为在不同交付组之间共享的应用程序创建应用程序组，或为由交付组中的部分用户使用的应用程序创建应用程序组。

已知限制

当您使用适用于 Windows 的 Citrix Workspace™ 应用程序 1912 或更早版本时，会话会在一段时间后断开。此问题已在 Citrix Workspace 应用程序的较新 LTSR 和 CR 版本中修复。 有关支持的版本

信息，请参阅 适用于 Windows 的 Citrix Workspace 应用程序 / 适用于 Windows 的 Citrix Receiver 长期服务版本。

机器身份

每台计算机都必须具有唯一的机器身份，也称为计算机帐户。机器身份可以在本地计算机或目录中创建和管理。Citrix® 支持在已加入 Active Directory、已混合加入 Microsoft Entra 或未加入域的计算机上托管虚拟应用程序和桌面。

机器身份类型

支持以下机器身份类型。

机器身份类型	描述
已加入 AD	身份在本地 Active Directory 中创建和管理。预配的计算机使用分配的机器身份加入本地 Active Directory。
已混合加入 Microsoft Entra	身份在本地 Active Directory 中创建，并通过 Microsoft Entra Connect 与 Microsoft Entra ID 同步。预配的计算机加入本地 Active Directory。然后，这些计算机将混合加入 Microsoft Entra。对于导入已混合加入 Microsoft Entra 的 VM，Citrix Virtual Apps and Desktops 会将该 VM 视为已加入 Active Directory 的 VM。
未加入域	身份在本地计算机中创建和管理。不支持将 VM 导入 Citrix Virtual Apps and Desktops。

支持的配置

以下是每种方案支持的配置的详细信息。

支持的基础设施

机器身份	CITRIX 虚拟应用和桌面™	思杰工作区™	思杰店面	思杰网关服务	思杰网关
已加入 AD	是	是	是	是	是

机器身份	CITRIX 虚拟应用和桌面™	思杰工作区™	思杰店面	思杰网关服务	思杰网关
已加入 Microsoft Entra	否	是	否	是	否
Microsoft Entra 混合加入	是	是	是	是	是
未加入域	是	是	否	是	否

支持的工作区身份验证标识提供程序

计算机身份	微软安创身份	活动目录	ACTIVE DIRECTORY 和令牌	奥克塔	SAML	思杰网关	自适应身份验证
已加入 AD	是	是	是	是	是	是	是
Microsoft Entra 混合加入	是	是	是	是	是	是	是
未加入域	是	是	是	是	是	是	是

已加入 Active Directory

Active Directory 是身份验证和授权所必需的。Active Directory 中的 Kerberos 基础结构用于保证与 Delivery Controllers 通信的真实性和机密性。有关 Kerberos 的信息，请参阅 Microsoft 文档。

《系统要求》一文列出了林和域支持的功能级别。要使用策略建模，域控制器必须在所有受支持的服务器操作系统上运行。这不影响域功能级别。

本产品支持：

- **用户帐户和计算机帐户存在于单个 Active Directory 林中的域中的部署。** 用户帐户和计算机帐户可以存在于单个林中的任意域中。在此类部署中，支持所有域功能级别和林功能级别。

- **用户帐户存在于与包含控制器和虚拟桌面计算机帐户的 Active Directory 林不同的 Active Directory 林中的部署。** 在此类部署中，包含控制器和虚拟桌面计算机帐户的域必须信任包含用户帐户的域。可以使用林信任或外部信任。在此类部署中，支持所有域功能级别和林功能级别。
- **控制器计算机帐户存在于与包含虚拟桌面计算机帐户的一个或多个其他 Active Directory 林不同的 Active Directory 林中的部署。** 在此类部署中，包含控制器计算机帐户的域与包含所有虚拟桌面计算机帐户的域之间必须存在双向信任。在此类部署中，所有包含控制器或虚拟桌面计算机帐户的域必须处于“Windows 2000 本机”功能级别或更高。支持所有林功能级别。
- **可写入的域控制器。** 不支持只读域控制器。

可选地，Virtual Delivery Agents (VDA) 可以使用 Active Directory 中发布的信息来确定它们可以向哪些控制器注册（发现）。此方法主要用于向后兼容性，并且仅当 VDA 与控制器位于同一 Active Directory 林中时才可用。有关此发现方法的信息，请参阅基于 Active Directory OU 的发现 和 CTX118976。

> **注意：**
>
> 站点配置完成后，请勿更改 Delivery Controller™ 的计算机名称或域成员身份。

在多 Active Directory 林环境中部署

在具有多个林的 Active Directory 环境中，如果存在单向或双向信任，则可以使用 DNS 转发器或条件转发器进行名称查找和注册。要允许适当的 Active Directory 用户创建计算机帐户，请使用“控制委派向导”。有关此向导的详细信息，请参阅 Microsoft 文档。

如果在林之间存在适当的 DNS 转发器，则 DNS 基础结构中不需要反向 DNS 区域。

如果 VDA 和控制器位于不同的林中，则 `SupportMultipleForest` 键是必需的，无论 Active Directory 和 NetBIOS 名称是否不同。使用以下信息将注册表项添加到 VDA 和 Delivery Controllers：

> **注意：**
>
> 不正确地编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix® 无法保证可以解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。在编辑注册表之前，请务必备份注册表。

> 在 VDA 上，配置：`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`。

- 名称: `SupportMultipleForest`
- 类型: `REG_DWORD`
- 数据: `0x00000001 (1)`

在所有 Delivery Controller 上，配置：`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest`。

- 名称: `SupportMultipleForest`
- 类型: `REG_DWORD`
- 数据: `0x00000001 (1)`

如果您的 DNS 命名空间与 Active Directory 的不同，则可能需要反向 DNS 配置。

已添加一个注册表项，以避免在 VDA 中意外启用 NTLM 身份验证，因为 NTLM 不如 Kerberos 安全。此条目可以替代 `SupportMultipleForest` 条目使用，后者仍可用于向后兼容。

在 VDA 上，配置：`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`。

- 名称: `SupportMultipleForestDdcLookup`
- 类型: `REG_DWORD`
- 数据: `0x00000001 (1)`

此注册表项在双向信任的多林环境中执行 DDC 查找，允许您在初始注册过程中删除基于 NTLM 的身份验证。

如果在设置过程中存在外部信任，则需要 `ListOfSIDs` 注册表项。如果 Active Directory FQDN 与 DNS FQDN 不同，或者包含域控制器的域的 NetBIOS 名称与 Active Directory FQDN 不同，则 `ListOfSIDs` 注册表项也是必需的。要添加注册表项，请使用以下信息：

对于 VDA，找到注册表项 `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs`。

- 名称: `ListOfSIDs`
- 类型: `REG_SZ`

- 数据：Controller 的安全标识符 (SID)。（SID 包含在 `Get-BrokerController` cmdlet 的结果中。）

如果存在外部信任，请在 VDA 上进行以下更改：

1. 找到文件 `Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config`。
2. 创建文件的备份副本。
3. 使用文本编辑程序（例如记事本）打开文件。
4. 找到文本 `allowNtlm="false"` 并将其更改为 `allowNtlm="true"`。
5. 保存文件。

添加 `ListOfSIDs` 注册表项并编辑 `brokeragent.exe.config` 文件后，重新启动 Citrix Desktop Service 以应用更改。

下表列出了支持的信任类型：

信任类型	可传递性	方向	此版本中支持
父级和子级	可传递的	双向	是
树根	可传递的	双向	是
外部	不可传递	单向或双向	是
林	可传递的	单向或双向	是
快捷方式	可传递的	单向或双向	是
领域	可传递或不可传递	单向或双向	否

有关复杂的 Active Directory 环境的更多信息，请参阅 CTX134971。

下一步操作

有关如何创建本地 Active Directory (AD) 加入的计算机身份的身份池的信息，请参阅 本地 Active Directory 加入的计算机身份的身份池。

Microsoft Entra 混合加入

本文介绍了创建 Microsoft Entra 混合加入目录以及注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录的身份池的要求，此外还包括系统要求部分中概述的要求。

Microsoft Entra 混合加入的计算机使用本地 AD 作为身份验证提供程序。您可以将它们分配给本地 AD 中的域用户或组。要启用 Microsoft Entra ID 无缝 SSO 体验，您需要将域用户同步到 Microsoft Entra ID。

> **注意：**
>
> Microsoft Entra 混合加入的 VM 在联合和托管身份基础结构中均受支持。

Microsoft Entra 混合加入的要求

- VDA 类型：单会话（仅限桌面）或多会话（应用程序和桌面）
- VDA 版本：2212 或更高版本
- 预配类型：Machine Creation Services™ (MCS)，持久和非持久
- 分配类型：专用和池化
- 托管平台：任何虚拟机管理程序或云服务

Microsoft Entra 混合加入的限制

- 如果使用 Citrix 联合身份验证服务 (FAS)，则单点登录将定向到本地 AD 而非 Microsoft Entra ID。在这种情况下，建议配置基于 Microsoft Entra 证书的身份验证，以便在用户登录时生成主刷新令牌 (PRT)，这有助于在会话内实现对 Microsoft Entra 资源的单点登录。否则，PRT 将不存在，并且对 Microsoft Entra 资源的 SSO 将不起作用。有关使用 Citrix 联合身份验证服务 (FAS) 实现对混合加入的 VDA 进行 Microsoft Entra 单点登录 (SSO) 的信息，请参阅 混合加入的 VDA。
- 在创建或更新计算机目录时，请勿跳过映像准备。如果您想跳过映像准备，请确保主 VM 不是 Microsoft Entra 或 Microsoft Entra 混合加入的。

Microsoft Entra 混合加入的注意事项

- 创建 Microsoft Entra 混合加入的计算机需要目标域中的 `Write userCertificate` 权限。请确保在目录创建期间输入具有该权限的管理员凭据。
- Microsoft Entra 混合加入过程由 Citrix 管理。您需要按如下方式在主 VM 中禁用由 Windows 控制的 `autoWorkplaceJoin`。手动禁用 `autoWorkplaceJoin` 的任务仅适用于 VDA 2212 或更早版本。

  a. 运行 `gpedit.msc`。

  b. 导航到 **计算机配置 > 管理模板 > Windows 组件 > 设备注册**。

c. 将 **将域加入的计算机注册为设备** 设置为 **禁用**。

- 创建计算机身份时，选择配置为与 Microsoft Entra ID 同步的组织单位 (OU)。
- 对于基于 Windows 11 22H2 的主 VM，请在主 VM 中创建一个计划任务，该任务在系统启动时使用 SYSTEM 帐户执行以下命令。在主 VM 中计划任务的此任务仅适用于 VDA 2212 或更早版本。

```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'

$WorkplaceJoinKeyPath = 'HKLM:
\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin'

$MaxCount = 60



for ($count = 1; $count -le $MaxCount; $count++)

{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)

  {

    $provider = (Get-Item -Path
$VirtualDesktopKeyPath).GetValue("Provider", $null)

    if ($provider -eq 'Citrix')

    {

        break;

    }



    if ($provider -eq 1)

    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "Provider"
-Value "Citrix" -Force
```

```
        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name
"autoWorkplaceJoin" -Value 1 -Force

        Start-Sleep 5

        dsregcmd /join

        break

    }

  }



  Start-Sleep 1

}
```

- 默认情况下，Microsoft Entra Connect 每 30 分钟同步一次。预配的计算机在首次启动时可能需要长达 30 分钟才能加入 Microsoft Entra 混合。

已注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录

已加入 Microsoft Entra 混合的目录、持久性单会话和多会话 VM（已注册到 Microsoft Intune）使用具有共同管理功能的设备凭据。

共同管理使您能够使用 Configuration Manager 和 Microsoft Intune 同时管理 Windows 10 或更高版本的设备。有关详细信息，请参阅共同管理。

已注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录的先决条件

在启用此功能之前，请验证：

- 您的 Azure 环境符合使用 Microsoft Intune 的许可要求。有关详细信息，请参阅 Microsoft 文档。
- 您有一个已启用共同管理的有效 Configuration Manager 部署。有关详细信息，请参阅 Microsoft 文档。

已注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录的要求

- VDA 类型：单会话或多会话

- VDA 版本：2407 或更高版本
- 预配类型：Machine Creation Service (MCS)，持久性。已注册到 Microsoft Intune 的非持久性单会话和多会话 VM 的 Microsoft Entra 混合加入目录目前处于预览阶段。请参阅将混合 Entra ID 加入的非持久性 VM 注册到 Microsoft Intune。
- 分配类型：专用和池化
- 托管平台：任何虚拟机管理程序或云服务

已注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录的限制

- 在创建或更新计算机目录时，请勿跳过映像准备。
- Configuration Manager 的基于 Internet 的客户端管理 (IBCM) 不受支持。

已注册到 Microsoft Intune 的 Microsoft Entra 混合联接目录的注意事项

- 如果目录中同时启动的计算机过多，Intune 注册可能会延迟。

  Microsoft 对每个租户的 Intune 注册施加了限制，该限制规定了在特定时间范围内可以注册的设备数量。允许的设备数量因与租户关联的 Microsoft Intune 许可证数量而异。请咨询您的 Microsoft 客户团队以了解您的租户的允许限制。此方法有助于 Microsoft Intune 注册更好地扩展以适应大型环境。

  对于持久性计算机，所有设备完成 Intune 注册可能需要初始等待时间。

  对于非持久性计算机，请考虑限制 Autoscale™ 或手动电源操作中的并发电源操作。
- 配置 Configuration Manager 的云连接。有关详细信息，请参阅 Microsoft 文档。
- 在主 VM 上手动安装 Configuration Manager 客户端，而无需使用 `.\CCMSetup.exe /mp:SCCMServer /logon FSP=SCCMServer` 分配站点代码。SCCMServer 是您环境中的 SCCM 服务器名称。有关详细信息，请参阅 Microsoft 文档。
- MCS 创建的计算机使用自动站点分配机制来查找发布到 Active Directory 域服务的站点边界组。确保在您的环境中配置了 **Configuration Manager** 的 边界和边界组。如果自动站点分配不可用，可以通过以下注册表设置在主 VM 中配置静态 Configuration Manager 站点代码：

  键：

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MachineIdentityServiceAgent\DeviceManagement
  ```

  值名称：`MdmSccmSiteCode`

  值类型：**字符串**

值数据：`the site code to be assigned`

- 配置 Microsoft Intune 以删除陈旧设备。这可确保您的设备记录保持最新。有关删除陈旧设备的信息，请参阅 使用清理规则自动删除设备。

下一步操作

有关创建 Microsoft Entra 混合联接目录的身份池的更多信息，请参阅 Microsoft Entra 混合联接计算机身份的身份池。

非域加入

本文介绍了使用 Citrix Virtual Apps and Desktops 创建非域加入目录的要求，以及 系统要求 部分中概述的要求。

要求

- 控制平面：请参阅 支持的配置
- VDA 类型：单会话（仅限桌面）或多会话（应用程序和桌面）
- VDA 版本：2311 或更高版本
- 预配类型：Machine Creation Services™ (MCS)，持久和非持久
- 分配类型：专用和池化
- 托管平台：MCS 支持的所有平台
- 必须启用 Rendezvous V2

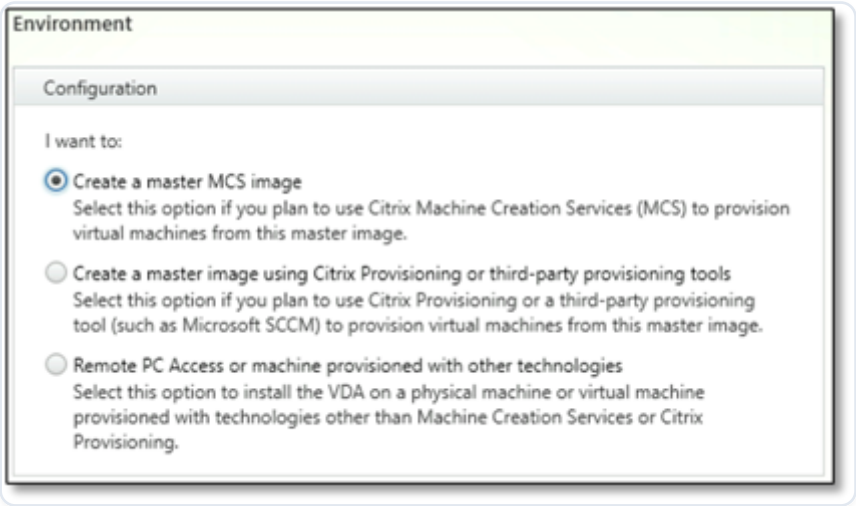
限制

- 不支持服务连续性。
- 每当我们使用多会话非域加入 VDA 时，本地用户配置文件数据将不会保留，并在注销时删除。

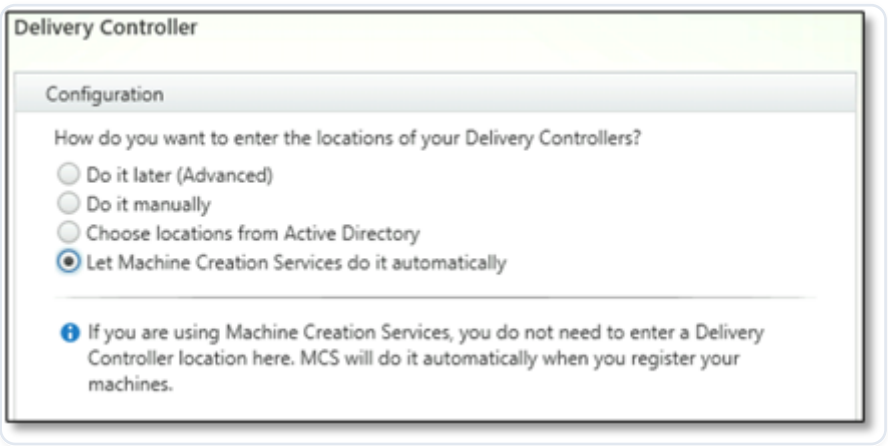
VDA 安装和配置

请按照以下步骤安装 VDA：

1. 请确保在安装向导中选择以下选项：
    - 在“环境”页面上，选择 **创建主 MCS 映像**。



- 在“Delivery Controller™”页面上，选择 **让 Machine Creation Services 自动执行**。



下一步操作

资源位置和托管连接可用后，请继续创建身份池。有关创建非域加入计算机身份的身份池的更多信息，请参阅 非域加入计算机身份的身份池。

会话身份验证

Citrix 支持多种方法对用户进行虚拟桌面和应用程序会话身份验证。可用选项取决于您的环境配置方式；具体来说，包括用户帐户所在的目录服务（例如 Active Directory 或 Microsoft Entra ID）、会话主机加入的目录服务以及用于首次登录 Citrix 环境的身份提供程序。这些因素决定了身份验证是通过传统凭据、智能卡、联合断言还是基于证书的机制来处理。本节概述了可用的身份验证方法以及它们如何与不同的部署场景相对应。

Microsoft Entra 单点登录

当使用 Microsoft Entra ID 凭据访问 Microsoft Entra 混合加入会话主机上的虚拟应用程序和桌面时，您可以利用单点登录 (SSO)。

有关 DaaS，请参阅 Microsoft Entra 单点登录。

支持的基础设施

以下是 Microsoft Entra 单点登录支持的基础设施组件概述：

计算机身份	思杰 DAAS	CVAD 本地部署	思杰店面云	思杰店面	思杰网关服务	NETSCALER 网关
已加入 Microsoft Entra	是	否	是	否	是	是
Microsoft Entra 混合加入	是	是	是	是	是	是

注意：

在 StoreFront 中，Microsoft Entra 单点登录仅支持现代 UI 体验，不支持经典 UI 体验。

支持的访问方法

以下是 Citrix 环境中可用的访问方法：

- **本机访问**：您使用本机 Citrix Workspace 应用程序客户端访问 Citrix Storefront 并建立会话连接。
- **浏览器访问**：您通过浏览器访问 Citrix Storefront，并使用适用于 HTML5 客户端的 Citrix Workspace 应用程序连接到虚拟应用程序或桌面会话。
- **混合访问**：您通过浏览器访问 Citrix Storefront，并使用本机 Workspace 应用程序客户端连接到虚拟应用程序或桌面会话。

以下是 Microsoft Entra 单点登录支持的访问方法概述：

访问方法	视窗	林纳克斯	MAC	CHROME 操作系统	安卓	IOS
本机	是	是	是	是	是	是
浏览器	是	是	是	是	是	是

访问方法	视窗	林纳克斯	MAC	CHROME 操作系统	安卓	IOS
混合	是	是	是	否	否	否

注意：

您必须允许弹出窗口，以便单点登录在浏览器和混合访问中正常工作。

系统要求

以下是使用 Microsoft Entra 单点登录的系统要求：

- 控制平面：Citrix Virtual Apps and Desktops™ 2607 LTSR 或更高版本
- 访问层：StoreFront 2607 LTSR 或更高版本
- 虚拟投递代理 (VDA)
  - Windows：版本 2507 或更高版本
- Citrix Workspace 应用程序
  - Windows：版本 2508 或更高版本
  - Linux：版本 2604.10 或更高版本
  - Mac：版本 2607 或更高版本
  - HTML5：版本 2603.10 或更高版本
  - Chrome OS：版本 2603 或更高版本
  - Android：版本 2511 或更高版本
  - iOS：版本 2607 或更高版本
- 具有本机启动功能的 Web 浏览器：
  - 微软 Edge 配合 Citrix Web 扩展
  - 谷歌 Chrome 配合 Citrix Web 扩展
- 具有浏览器启动功能的 Web 浏览器：任何受支持的 Web 浏览器。
- 会话主机操作系统：

- Windows 11，版本 24H2，并安装了 2025 年 9 月 Windows 11 累积更新 (KB5065789) 或更高版本（内部版本 26100.6725）
- Windows Server 2025，并安装了 2026 年 1 月 Windows Server 2025 累积更新 (KB5073379) 或更高版本（内部版本 26100.32230）

> **注意：**
>
> 仅当用户将在 **Windows** 或 **Mac** 设备中利用混合访问时，才需要 Citrix Web Extension。如果用户利用本机或浏览器访问，则不需要 Citrix Web Extension。

注意事项

- 如果您的用户将利用混合访问，他们必须使用 Microsoft Edge 或 Google Chrome，并安装 Citrix Web 扩展。混合访问的 Microsoft Entra 单点登录不支持其他浏览器。
- 当使用 Microsoft Entra 单点登录登录会话时，不支持自动客户端重新连接。使用此登录方法时，此功能会自动禁用。在网络中断的情况下，会话可靠性仍可用于自动重新连接。
- 当虚拟桌面被锁定后，默认行为是显示 Windows 锁定屏幕。根据您的身份验证要求，您可能需要更改会话锁定行为。有关更多详细信息，请参阅 会话锁定行为。
- 对于 Microsoft Entra 混合加入的会话主机，默认情况下，单点登录不适用于特权组（如域管理员）的成员。要启用此功能，请将该组或用户添加到 Microsoft Entra Kerberos 访问的只读域控制器 (RODC) 允许列表中。有关详细信息，请参阅 Microsoft Entra Kerberos TGT 和 Active Directory 访问控制。
- Microsoft Entra 单一登录要求启用 Windows 设置 **允许将自定义 SSP 和 AP 加载到 LSASS 中**（默认）。请注意，如果您通过 Microsoft Intune 部署**适用于 Windows 10 及更高版本的安全基线**模板，则此设置将自动禁用并阻止 SSO，因此您必须更新 Intune 设备配置策略以使其保持启用状态。

如何配置 Microsoft Entra 单一登录

概述

Microsoft Entra 单一登录的配置包含以下步骤：

1. Azure 和 Microsoft Entra ID 的配置。
    a. 注册 Citrix 资源和客户端应用程序。
    b. 为 Citrix 资源应用程序启用 Microsoft Entra ID 远程桌面服务身份验证协议。

c. 隐藏用户同意提示。

d. 批准客户端应用程序。

e. 创建 Kerberos 服务器对象（仅限 Microsoft Entra 混合联接环境）。

f. 审查 Microsoft Entra 条件访问策略。

2. Citrix 配置。

a. 预配具有所需操作系统版本、身份类型和 VDA 版本的会话主机。

b. 配置 StoreFront。

c. 在您的站点中启用 Microsoft Entra 单一登录。

d. 在您的交付组中启用 Microsoft Entra 单一登录。

微软 Azure 和 微软 Entra ID 配置

为了利用 Microsoft Entra 单一登录，您必须首先在 Microsoft Entra ID 租户中为 Windows 启用 Microsoft Entra 身份验证，这将允许颁发所需的身份验证令牌，从而使用户能够登录到已加入 Microsoft Entra 和混合加入 Microsoft Entra 的会话主机。

执行 Azure 配置的人员必须至少被分配以下 Microsoft Entra 内置角色 之一或同等角色：

- 应用程序管理员
- 云应用程序管理员

配置可以通过 Azure 门户、使用 Microsoft Graph PowerShell SDK 或 Microsoft Graph API 完成。以下部分提供了通过 Azure 门户完成配置的详细信息。如果您更喜欢使用 Microsoft Graph PowerShell SDK 或 Microsoft Graph API，请参阅 Microsoft Entra 单一登录 Azure 配置。

注册 CITRIX 应用程序

您必须在 Azure 租户中注册多租户 Citrix Resource 应用程序，并创建单租户 Client 应用程序。

首先，您必须注册 Citrix Resource 应用程序。为此，请使用以下同意 URL 之一：

- 美国、欧盟、亚太地区：`https://login.microsoftonline.com/common/adminconsent?client_id=3a510bb1-e334-4298-831e-3eac97f8b26c`
- 日本：`https://login.microsoftonline.com/common/adminconsent?client_id=0027603f-364b-40f2-98be-8ca4bb79bf8b`

Resource 应用程序注册后，您需要创建单租户 Client 应用程序。
创建单租户 Client 应用程序

1. 转到 Azure 门户。

2. 导航到 **Microsoft Entra ID > 企业应用程序**。
3. 选择**新建应用程序**。
4. 选择**创建自己的应用程序**。
5. 输入应用程序名称，选择**注册应用程序以与 Microsoft Entra ID 集成**，然后单击**创建**。
6. 在**支持的帐户类型**下，选择**仅限单租户**，然后单击**注册**。
7. 导航到 **Microsoft Entra ID > 应用注册**，然后选择**所有应用程序**。
8. 搜索并点击您刚刚创建的应用程序。
9. 点击 **添加重定向 URI**。
10. 您需要添加三个重定向 URI：**Web**、**单页应用程序** 和 **移动和桌面应用程序**。

    a. 对于每个 URI，选择 **添加重定向 URI**。

    b. 输入重定向 URI。有关要添加的内容的详细信息，请参阅下表。

平台类型	重定向 URI	备注
Web	客户特定的 NetScaler 登录 URI	URI 字符串是根据您特定的 NetScaler URL 计算的。
移动和桌面应用程序	`ctxaadsso://citrix.aad.redirect`	完全按原样输入此 URI。
SPA 应用程序（单页应用程序）	StoreFront 应用商店 Web URL	输入您的 StoreFront 应用商店的 Web URL。例如，如果通过浏览器访问您的应用商店的 URL 是 `https://finance.acme.com/Citrix/MyStoreWeb`，则 SPA 重定向 URI 必须是 `https://finance.acme.com/Citrix/MyStoreWeb`。如果您的环境中存在多个应用商店，则必须将所有应用商店的 Web URL 输入为 SPA 重定向 URI。

    c. 选择 **配置**。

11. 添加所有重定向 URI 后，您需要向客户端应用程序添加一个 API 权限。
    a. 在“管理”下的左侧窗格中，选择 **API 权限**。
    b. 选择 **添加权限**。
    c. 选择 **我的组织使用的 API**。
    d. 选择 Citrix 资源应用程序 (**Citrix-Workspace-Resource**)。
    e. 在权限列表中，选中 **user_impersonation**。
    f. 选择 **添加权限**。
12. 在左侧窗格中，选择 **概述**，并记下分配的应用程序 ID。

注册客户端应用程序
创建并配置应用程序后，您必须同意应用程序权限。

您可以在 Azure 门户中同意应用程序的权限：

1. 导航到 **微软 Entra 标识 > 企业应用程序**。
2. 搜索并选择客户端应用程序。
3. 在“安全性”下的左侧窗格中，选择 **权限**。
4. 单击 **授予管理员同意 \<tenantName\>**
5. 同意这些权限。

或者，您可以使用管理员同意 URL: `https://login.microsoftonline.com/<EntraTenantID>/adminconsent?client_id=<clientAppID>`

> **注意：**
>
> 您必须将 `<EntraTenantID>` 替换为您的 Entra 租户 ID，并将 `<clientAppID>` 替换为客户端应用程序的应用程序 ID。

Citrix 资源应用程序权限
以下是应用程序的权限：

API 名称	声明值	权限	类型
微软图形	User.Read	登录并读取用户配置文件	委派

对于美国、欧盟和 APS，该应用程序称为 **Citrix-Workspace-Resource** (application ID 3a510bb1-e334-4298-831e-3eac97f8b26c)。

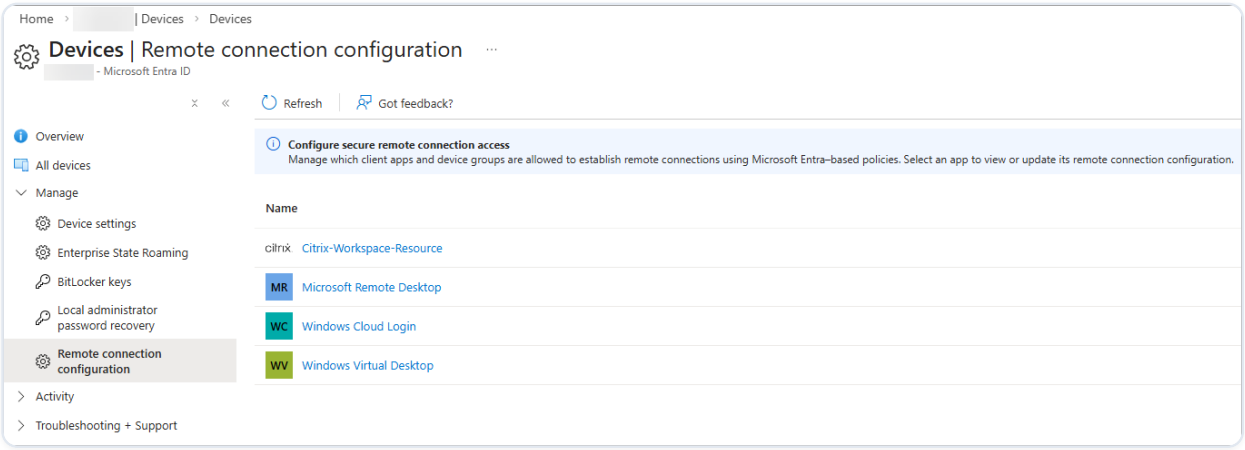
对于日本，该应用程序称为 **Citrix-Workspace-Resource-JP** (application ID 0027603f-364b-40f2-98be-8ca4bb79bf8b)。
Citrix 客户端应用程序权限
以下是应用程序的权限：

API 名称	声明值	权限	类型	
思杰-工作区-资源 Citrix-工作区-资源-JP	user_impersonation	Citrix Entra ID 单点登录	委派	
微软图形	User.Read	登录并读取用户配置文件	委派	

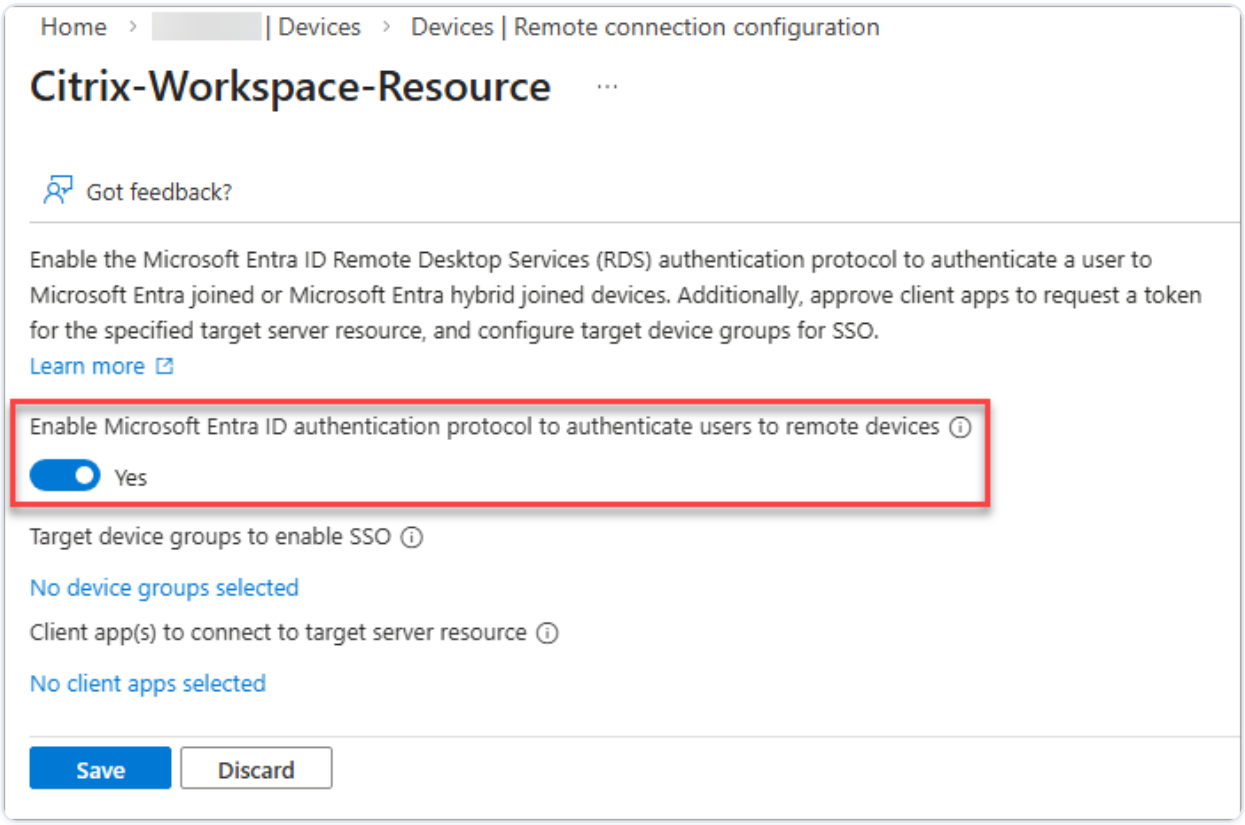
启用 MICROSOFT ENTRA ID 远程桌面服务身份验证协议

您必须在 Citrix Resource 应用程序中启用 Microsoft Entra ID 远程桌面服务身份验证协议。为此：

1. 在 Azure 门户 中，导航到 `Microsoft Entra ID` > `Devices` > `Manage` > `Remote connection configuration`。



2. 选择名为 **Citrix-Workspace-Resource** 的资源。
3. 启用 **Microsoft Entra ID 远程桌面服务身份验证协议**。



4. 继续隐藏用户同意提示。

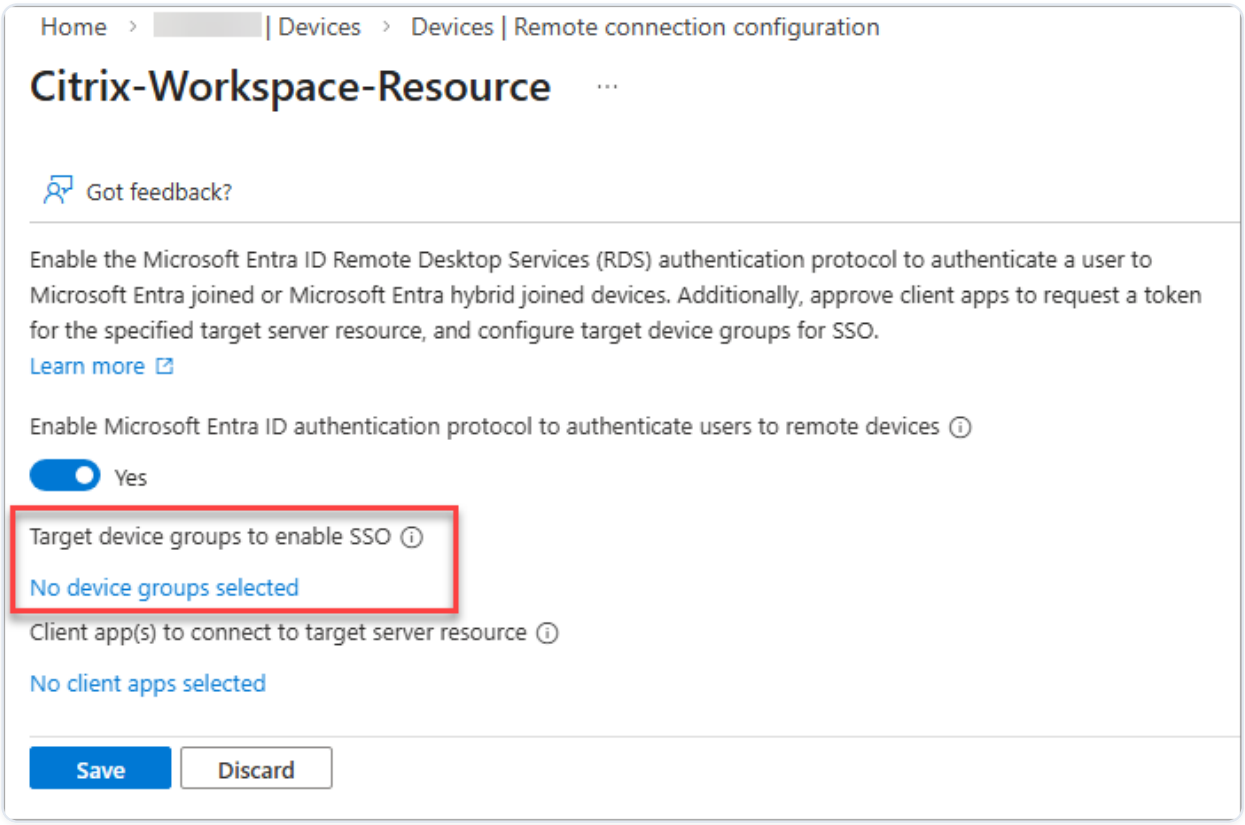
隐藏用户同意提示对话框

默认情况下，当用户连接到启用了 Microsoft Entra 单一登录的 Microsoft Entra 加入或 Microsoft Entra 混合加入会话主机时，系统会提示他们允许远程桌面连接，此时他们必须选择“**是**”以允许单一登录。Microsoft Entra 将记住最多 15 个唯一的会话主机 30 天，之后会再次提示。

您可以通过配置目标设备列表来隐藏此对话框。要配置设备列表，您必须在 Microsoft Entra ID 中创建一个或多个组，这些组包含 Microsoft Entra 加入和/或 Microsoft Entra 混合加入的会话主机，然后在资源应用程序中授权这些组，最多可授权 10 个组。

一旦您启用了 Microsoft Entra ID 远程桌面服务身份验证协议并创建了组：

1. 单击链接以添加目标设备组并选择相应的组。



注意

强烈建议创建动态组以简化组的成员资格管理。虽然动态组通常在 5-10 分钟内更新，但大型租户可能需要长达 24 小时。

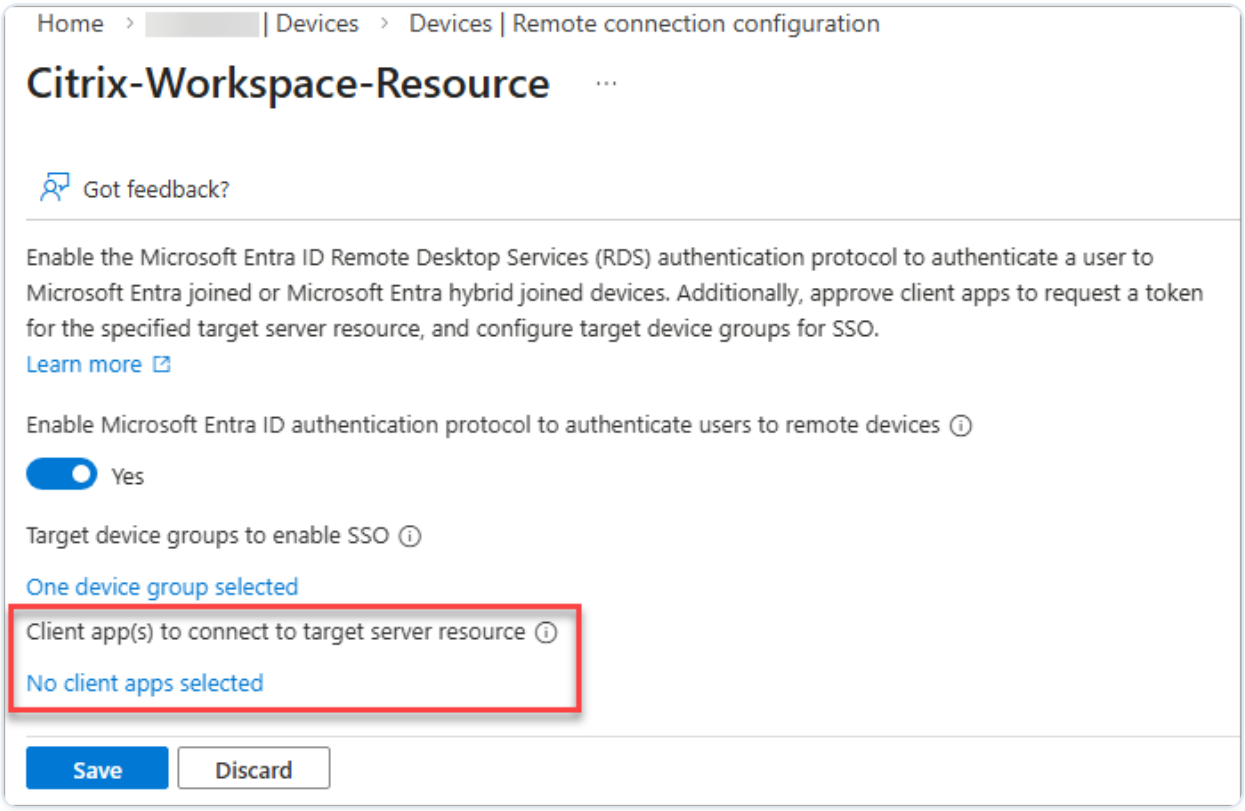
动态组需要 Microsoft Entra ID P1 许可证或 Intune for Education 许可证。有关详细信息，请参阅组的动态成员资格规则。

1. 继续批准客户端应用程序。

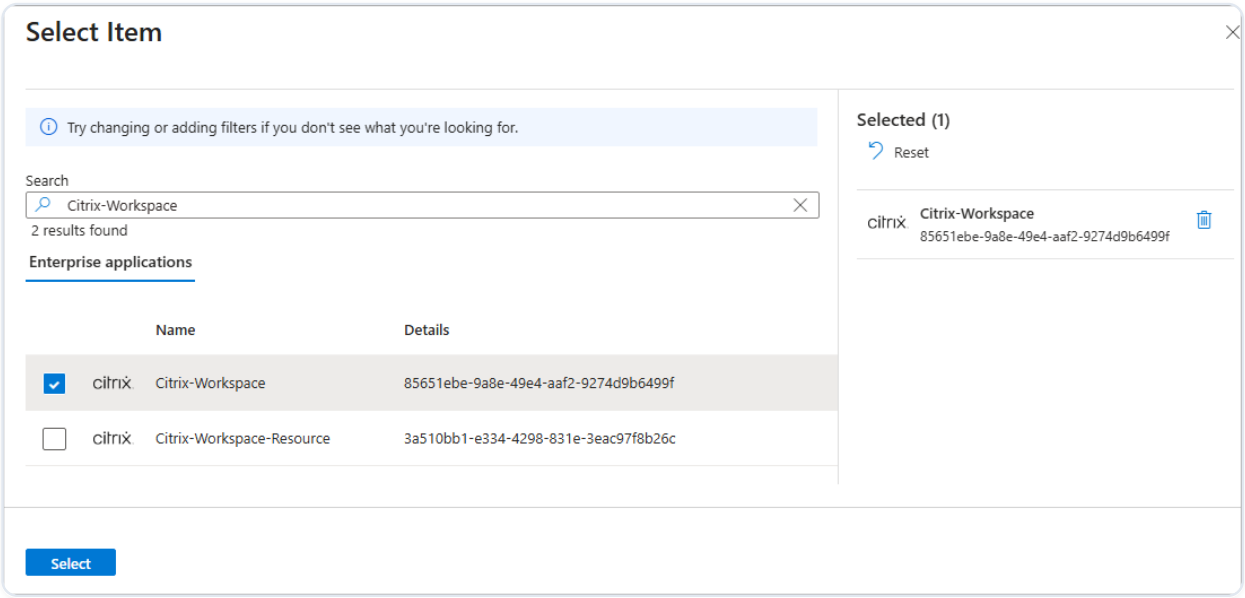
批准客户端应用程序

您必须在 Citrix 资源应用程序中将 Citrix Client 应用程序明确添加为已批准的客户端：

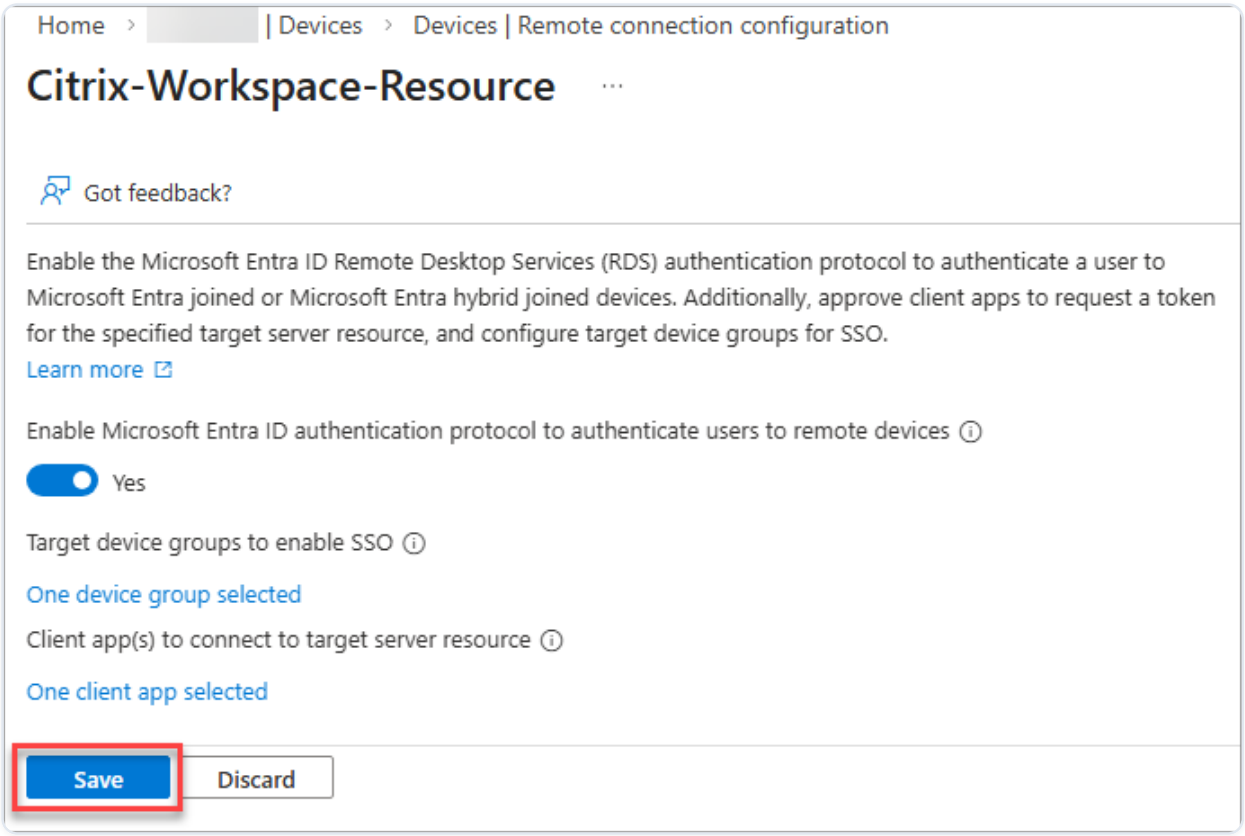
1. 单击链接以添加您的受信任客户端应用程序。



2. 选择 Citrix Client 应用程序。



3. 选择**保存**以将配置更改应用于 Citrix 资源应用程序。



4. 继续创建 Kerberos 服务器对象。

创建 KERBEROS 服务器对象

如果您的会话主机是 Microsoft Entra 混合加入的，则必须在用户和计算机帐户所在的 Active Directory 域中配置 Kerberos 服务器对象。有关详细信息，请参阅创建 Kerberos 服务器对象。

查看 MICROSOFT ENTRA 条件访问策略

如果您使用或计划使用 Microsoft Entra 条件访问策略，请查看应用于 Citrix 资源应用程序 的配置，以确保用户获得预期的登录体验。

有关在使用 Microsoft Entra 单一登录时配置条件访问的详细指南，请参阅 Microsoft 文档。请记住，所需的条件访问设置必须应用于 **Citrix 资源应用程序**，而不是 Citrix 客户端应用程序或 Microsoft 应用程序。

Citrix 会话主机

确保满足会话主机的系统要求：

1. 确保会话主机已 Microsoft Entra 混合加入。
2. 按照系统要求安装所需的操作系统版本和内部版本。
3. 按照系统要求安装所需的 VDA 版本。

MICROSOFT ENTRA 混合加入的会话主机

当使用 Citrix Machines Creation Services、Citrix Provisioning 或 Windows 365 部署 Microsoft Entra 混合加入的会话主机时，请继续下一节。如果您使用任何其他工具或方法预配 Microsoft Entra 混合加入的主机，则必须将以下注册表值添加到您的会话主机：

- 键：`HKLM\SYSTEM\CurrentControlSet\Control\Citrix`
- 值类型：**DWORD**
- 值名称：`AzureADJoinType`
- 数据: `1`

会话锁定行为

当虚拟桌面被锁定时，默认行为是显示 Windows 锁定屏幕。此时，支持的桌面解锁身份验证方法是**用户名和密码**或**智能卡**。

> **注意**
>
> Citrix Web 登录（预览版）允许您使用基于 Web 的 Entra 身份验证解锁桌面。有关详细信息，请参阅Web 登录。

> 如果您部署了无密码环境，用户不知道其密码，建议将会话锁定行为配置为断开会话连接，而不是显示锁定屏幕。

您可以通过 Intune 或组策略启用**锁定远程会话时断开 Microsoft 身份平台身份验证**设置来配置此行为。有关详细步骤，请参阅配置 Azure 虚拟桌面的会话锁定行为。

Citrix 访问和控制平面

STOREFRONT 配置

要在 StoreFront 中启用 Microsoft Entra 单点登录，请参阅 StoreFront 文档中的 Entra ID single-on 。

在 WEB STUDIO 中启用 MICROSOFT ENTRA 单点登录

要在您的站点上启用 Microsoft Entra 单点登录，您必须添加客户端和资源应用程序详细信息以及重定向 URI。有关详细信息，请参阅 Settings 文档。

为交付组启用 MICROSOFT ENTRA 单点登录

使用 Web Studio

1. 在 Web Studio 中转到交付组，然后单击 **创建交付组**。

2. 在 **用户** 页面上，选择 **Microsoft Entra 混合加入** 作为身份类型。
3. 在以下页面上完成配置。有关参考，请参阅 创建交付组。

使用 PowerShell

1. 创建新的交付组并将 VDA 添加到交付组。将用户（AD 帐户）分配给 VDA。
2. 将交付组 `MachineLogonType` 设置为 `HybridAzureAd`。例如：

```
Get-BrokerDesktopGroup -Name <dgName> | Set-BrokerDesktopGroup
-MachineLogOnType "HybridAzureAd"
```

3. 信任 Xml 服务。

```
Add-PSSnapin Citrix.Broker.Admin.V2

Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

4. 设置 SSO 参数（请参阅下表获取指导）。

```
Set-BrokerSite -AzureGlobalCloudId "B16898C6-
A148-4967-9171-64D755DA8520" -AzureSSOnAuthorizeUrl "<URL>"
-AzureSSOnClientId "<clientAppID>" -AzureSSOnRedirectUrl "<URL>"
-AzureSSOnResourceAppId "<resourceAppID>"
```

下表提供了参数及其默认值的详细信息：

参数	默认值	描述
AzureGlobalCloudId	B16898C6-A148-4967-9171-64D755DA8520	标识 Windows 中的 Entra CloudAP。
AzureSSOnAuthorizeUrl	`https://login.microsoftonline.com/common/`	初始登录 URL。这取决于 Entra 租户所在的 Azure 云（例如 Azure Commercial 与 Azure Gov）
AzureSSOnClientId	无默认值	客户端应用程序的应用程序 ID。

参数	默认值	描述
AzureSSOnRedirectUrl	无默认值	身份验证后重定向 URI。它必须是客户端应用程序中配置为重定向 URI 的 URL。
AzureSSOnResourceAppId	3a510bb1-e334-4298-831e-3eac97f8b26c	Citrix 资源应用程序的应用程序 ID。

在 VDA 上配置 MICROSOFT ENTRA 单点登录

默认情况下，VDA 上已启用 Microsoft Entra 单点登录。要为部分会话主机启用或禁用此功能，请使用Microsoft Entra 单点登录策略设置。

客户端设备

确保满足客户端设备的系统要求：

1. 安装 系统要求 中指定的 Citrix Workspace 应用程序版本。
2. 如果您的用户将利用混合访问，请确保已安装 Citrix Web Extension。如果您的用户将使用本机或浏览器访问，则不需要 Citrix Web Extension。

故障排除

> **注意**
>
> 有关 StoreFront 问题的故障排除，请参阅 诊断日志。

已知问题

- 如果 Storefront 显示错误 `There was a failure with the mapped account`，这可能是因为用户是 Entra ID 用户，但在 Active Directory 中没有匹配的用户。
- 如果会话启动在 ICA 文件发布之前失败，请确保已启用 XML 信任。
- 如果 VDA 状态停留在“正在初始化”，请确保 Active Directory 中的计算机对象位于与 Entra ID 同步的 OU 中。
- 如果在 Entra ID 中禁用了“**保持登录状态 (KMSI)**”，则 Linux 和 macOS 客户端设备上的单点登录将失败。

单点登录失败时

如果在访问虚拟桌面或应用程序时单点登录失败，请按以下步骤操作：

1. 确认 StoreFront 中已启用 Microsoft Entra 单点登录。
2. 确认您的站点中已启用 Microsoft Entra 单点登录。
3. 确认交付组中已启用 Microsoft Entra 单点登录。
4. 确认用户使用的访问方法受支持。
5. 如果用户正在使用混合访问，请确认已安装 Citrix Web Extension。
6. 确认客户端设备正在运行所需的 Citrix Workspace 应用程序版本。
7. 确认您的会话主机正在运行所需的 Windows 版本。
8. 确认您的会话主机正在运行所需的 VDA 版本。
9. 确保会话主机上未启用 Windows 设置 `Always prompt for password upon connection`。此设置默认禁用，可以通过组策略或 Intune 在 `Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security` 下进行配置。您可以通过在注册表中查找 `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services` 下的值 `fPromptForPassword` 来检查该设置是否已启用。如果该值设置为 `1`，则表示该设置已启用，单点登录将不可用。如果该值缺失或设置为 `0`，则表示该设置已禁用。
10. 确认会话主机中 `AzureADJoinType` 设置配置正确：
    - 键：`HKLM\SYSTEM\CurrentControlSet\Control\Citrix`
    - 值类型：**DWORD**
    - 值名称：`AzureADJoinType`
    - 值数据：`1` (Microsoft Entra 混合加入)
11. 确保在 Citrix Studio 中，虚拟桌面或应用程序分配给 Active Directory 身份，而不是 Entra ID 身份。
12. 确认通过运行以下 PowerShell 命令正确配置了交付组的登录类型：

    ```
    Get-BrokerDesktopGroup -Name <deliveryGroupName>
    ```

    对于 Microsoft Entra 混合加入的会话主机，`MachineLogOnType` 必须设置为 `HybridAzureAd`。
13. 确认 Citrix 资源应用程序和单租户客户端应用程序已注册到 Microsoft Entra 租户。

14. 确认 Microsoft Entra ID RDS 身份验证协议已在 Citrix 资源应用程序上启用。
15. 确认客户端应用程序已作为批准的客户端应用程序添加到 Citrix 资源应用程序中。
16. 如果您的会话主机已加入 Microsoft Entra 混合模式，请确认已在用户和计算机帐户所在的 Active Directory 域中创建了 Kerberos 服务器对象。
17. 检查您的 Microsoft Entra 条件访问策略。确保没有策略应用于 Citrix 客户端应用程序，并且应用于 Citrix 资源应用程序或会话主机的任何策略都已正确配置，以免影响单点登录体验。

联邦身份验证服务

Citrix 联邦身份验证服务 (FAS) 允许用户在通过 SAML 或 OpenID Connect (OIDC) 等不提供 Windows 密码的现代身份提供商进行身份验证的环境中，对 Citrix 虚拟桌面和应用程序进行单点登录 (SSO)，从而确保无缝访问已加入 Active Directory 域的会话主机。

有关更多详细信息，请参阅联合身份验证服务文档。

智能卡

Citrix Virtual Apps and Desktops 和 Citrix DaaS 支持智能卡登录虚拟桌面和应用程序，并在活动会话中使用。智能卡提供基于证书的双因素身份验证，通过同时要求物理卡和 PIN 码来增强安全性。这使得组织能够满足合规性要求、保护敏感数据，并为已经依赖智能卡进行 Windows 登录或安全应用程序的用户简化访问。一旦通过身份验证，用户还可以在会话中使用智能卡对文档进行数字签名、加密电子邮件或访问其他支持智能卡的应用程序，从而确保在本地和虚拟环境中获得一致且安全的体验。

有关智能卡的文档，了解更多详细信息。

Web 登录 (预览)

您可以使用 Citrix Web 登录凭据提供程序来启用基于 Entra ID 的 Windows 身份验证。这允许用户使用 Entra ID 中启用的任何身份验证方法登录或解锁其虚拟桌面。

> **重要**
>
> Web 登录目前处于预览阶段。此功能不提供支持，尚不建议在生产环境中使用。

系统要求

以下是使用 Web 登录的系统要求：

- 虚拟投递代理

  - Windows：**单会话**版本 2607 或更高版本

- Citrix Workspace 应用程序
  - Windows：版本 2607 或更高版本
- 会话主机身份：Entra 混合加入
- 会话主机操作系统：
  - Windows 11，版本 24H2，并安装了 2025 年 9 月 Windows 11 累积更新 (KB5065789) 或更高版本（内部版本 26100.6725）

如何配置 Web 登录

Citrix Web 登录默认处于禁用状态。要启用它，请按照以下步骤操作：

1. 完成 Microsoft Entra 单点登录 文档中描述的**Azure 和 Microsoft Entra ID 配置**。如果您的环境中已启用 Microsoft Entra 单点登录，则可以继续执行下一步。

   相关步骤包括：

   a. 注册 Citrix 资源和客户端应用程序。
   b. 为 Citrix 资源应用程序启用 Microsoft Entra ID 远程桌面服务身份验证协议。
   c. 隐藏用户同意提示。
   d. 批准客户端应用程序。
   e. 创建 Kerberos 服务器对象（仅限 Microsoft Entra 混合加入环境）。
   f. 审查 Microsoft Entra 条件访问策略。

2. 在 Citrix 策略中启用 **Web 登录** 设置，并将策略应用于相应的交付组。

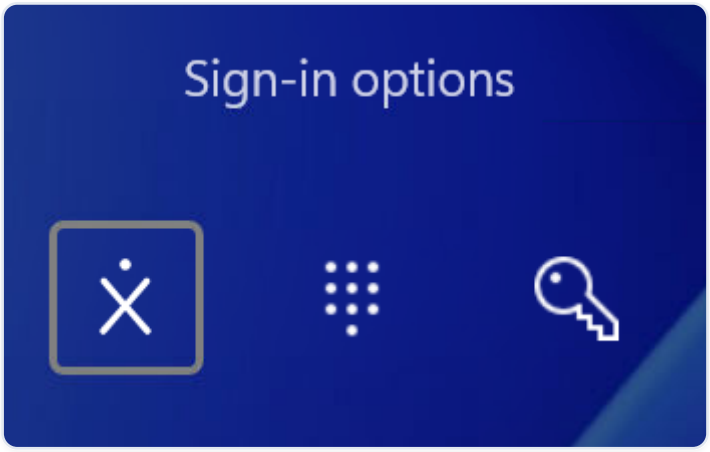
> **注意**
>
> - 无需使用 Microsoft Entra 单点登录即可使用 Web 登录。
> - 如果您的环境中没有此策略设置，您可以通过注册表启用 Web 登录：
>   - 键：HKLM\SOFTWARE\Policies\Citrix\ICAPolicies
>   - 值类型: DWORD
>   - 值名称：AllowWebSignIn

- 值数据: 1

如何使用 Web 登录

要使用 Citrix Web 登录登录或解锁您的虚拟桌面：

1. 从可用的登录方法中选择 Citrix 磁贴。



2. 单击 **Citrix Web 登录**。



3. 身份验证提示弹出后，使用所需的身份验证方法进行身份验证。

注意

用户可用的身份验证方法由 Microsoft Entra ID 中启用的内容决定。

准备安装

部署 Citrix Virtual Apps and Desktops™ 始于安装以下组件。此过程为向防火墙内的用户交付应用程序和桌面做准备。

- 一个或多个 Delivery Controller
- 思杰 Director
- 思杰 StoreFront™
- Citrix 许可证服务器
- 一个或多个 Citrix Virtual Delivery Agent (VDA)
- 可选组件和技术，例如通用打印服务器、联合身份验证服务和自助密码重置

对于防火墙外的用户，请安装并配置一个额外组件，例如 Citrix Gateway。有关介绍，请参阅将 Citrix Virtual Apps and Desktops 与 Citrix Gateway 集成。

> **注意：**

> 请确保在服务器操作系统和工作站操作系统上满足以下 Microsoft 先决条件：

> - Microsoft **卷影复制**和 **Microsoft 软件卷影复制提供程序**服务正在运行。有关详细信息，请参阅卷影复制服务。
> - **MS-Defender** 版本必须高于 4.18.2105.5。有关详细信息，请参阅Microsoft Defender 防病毒安全智能和产品更新。

> 如果您的部署包含 Windows Server 工作负载，请配置 Microsoft RDS 许可证服务器。

您可以使用产品 ISO 上的完整产品安装程序部署许多组件和技术。您可以使用独立的 VDA 安装程序安装 VDA。独立的 VDA 安装程序可在 Citrix 下载站点上获取。所有安装程序都提供图形和命令行界面。请参阅安装程序。

产品 ISO 包含用于在 Active Directory 中安装、升级或删除计算机 VDA 的示例脚本。您还可以使用这些脚本来管理 Machine Creation Services (MCS) 和 Citrix Provisioning（以前称为 Provisioning Services）使用的映像。有关详细信息，请参阅使用脚本安装 VDA。

安装前要查看的信息

- 技术概述：熟悉产品及其组件。

- 安全性：规划部署环境时。
- 已知问题：此版本中可能遇到的问题。
- 数据库：了解系统数据库以及如何配置它们。在 Controller 安装过程中，您可以安装 SQL Server Express 作为站点数据库。在安装核心组件后创建站点时，可以配置大多数数据库信息。
- 远程电脑访问：如果您要部署一个环境，使用户能够远程访问其办公室中的物理计算机。
- 连接和资源：如果您使用虚拟机管理程序或其他服务来托管或预配用于应用程序和桌面的 VM。在创建站点时（安装核心组件后），您可以配置第一个连接。在此之前设置您的虚拟化环境。
- Microsoft System Center Configuration Manager：如果您使用 ConfigMgr 管理对应用程序和桌面的访问，或者如果您将局域网唤醒功能与远程电脑访问结合使用。
- **公有云主机连接：**如果您拥有混合权利许可证，则可以创建到公有云的主机连接。有关混合权利许可证的信息，请参阅 Hybrid Rights Renewals。有关公有云权利以及此更改原因的信息，请参阅 CTX270373。

组件安装位置

查看 System requirements 以了解支持的平台、操作系统和版本。组件必备项会自动安装，除非另有说明。有关 Citrix StoreFront 和 Citrix 许可证服务器支持的平台和必备项，请参阅其文档。

您可以将核心组件安装在同一台服务器上，也可以安装在不同的服务器上。

- 将所有核心组件安装在一台服务器上适用于评估、测试或小型生产部署。
- 为了适应未来的扩展，请考虑将组件安装在不同的服务器上。例如，将 Studio 安装在与安装 Controller 的服务器不同的计算机上，可以远程管理站点。
- 对于大多数生产部署，建议将核心组件安装在单独的服务器上。

  在其他服务器上安装其他组件之前，请先安装 Citrix 许可证服务器和许可证。
- 要在 Server CoreOS（例如交付控制器）上安装受支持的组件，您必须(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-core/install-command.html)。该操作系统类型不提供图形界面，因此请在其他位置安装 Studio 和其他工具，然后将它们指向控制器服务器。

您可以在同一台服务器上安装 Delivery Controller™ 和多会话操作系统 VDA。启动安装程序并选择 Delivery Controller（以及您希望在该计算机上安装的任何其他核心组件）。然后再次启动安装程序并选择多会话操作系统的 **Virtual Delivery Agent**。

确保每个操作系统都具有最新更新。

确保所有计算机都具有同步的系统时钟。保护计算机之间通信的 Kerberos 基础结构需要同步。

对于 XenServers，即使虚拟机显示为已注册，其电源状态也可能显示为未知。要解决此问题，请编辑注册表项 `HostTime` 值以禁用与主机的时钟同步：

```
HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\HostTime="Local"
```

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\XenTools\HostTime="Local"
```

> **提示：**
>
> 默认值为 `HostTime="UTC"`。将此值更改为 UTC 以外的值，例如 `Local`。此更改可有效禁用与主机的时钟同步。

> 有关 Windows 10 单会话计算机的优化指南，请参阅 CTX216252。

不应安装组件的位置：

- 不要在 Active Directory 域控制器上安装任何组件。
- 不支持在 SQL Server 群集安装、SQL Server 镜像安装中的节点上或在运行 Hyper-V 的服务器上安装控制器。

如果您尝试在当前产品版本不支持的 Windows 操作系统上安装或升级 VDA，则会显示一条消息，引导您阅读一篇介绍相关选项的文章。

权限和 Active Directory 要求

您必须是域用户，并且是安装组件的计算机上的本地管理员。

要使用独立 VDA 安装程序，您必须具有提升的管理员权限或使用“**以管理员身份运行**”。

在开始安装之前，请配置您的 Active Directory 域。

- 系统要求 列出了支持的 Active Directory 功能级别。Active Directory 加入 包含更多信息。
- 您必须至少有一个运行 Active Directory 域服务的域控制器。
- 请勿在域控制器上安装任何 Citrix Virtual Apps and Desktops™ 组件。
- 在 Studio 中指定组织单位名称时，请勿使用正斜杠 (/)。

用于安装 Citrix 许可证服务器的 Windows 用户帐户会自动配置为委派管理完全管理员。

有关详细信息：

- 安全最佳实践

- 委派管理
- 有关 Active Directory 配置的 Microsoft 文档

安装指南、注意事项和最佳实践

安装任何组件期间

- 从完整产品介质安装或升级 Delivery Controller、Studio、License Server 或 Director 时，如果 Citrix 安装程序检测到计算机上存在先前 Windows 安装导致的待处理重新启动，安装程序将停止并显示退出/返回代码 9。系统会提示您重新启动计算机。

  这不是 Citrix 强制重新启动。这是由于计算机上先前安装的其他组件引起的。如果发生这种情况，请重新启动计算机，然后再次启动 Citrix 安装程序。

  使用命令行界面时，您可以通过在命令中包含 `/no_pending_reboot_check` 选项来阻止检查待处理的重新启动。
- 通常，如果某个组件具有先决条件，则安装程序会在它们不存在时部署它们。某些先决条件可能需要重新启动计算机。
- 在安装之前、期间和之后创建对象时，请为每个对象指定唯一的名称。例如，为网络、组、目录和资源提供唯一的名称。
- 如果某个组件未能成功安装，安装将停止并显示错误消息。已成功安装的组件将保留。您无需重新安装它们。
- 安装（或升级）组件时，Citrix Analytics 会自动收集。默认情况下，安装完成后，这些数据会自动上传到 Citrix。此外，安装组件时，您会自动加入 Citrix 客户体验改善计划 (CEIP)，该计划会上传匿名数据。

  在安装过程中，您还可以选择参与其他 Citrix 技术，这些技术会收集诊断信息以用于维护和故障排除。有关这些计划的信息，请参阅 Citrix Insight Services。
- 如果 VDA 安装失败，MSI 分析器会解析失败的 MSI 日志，并显示确切的错误代码。如果这是一个已知问题，分析器会建议一篇 CTX 文章。分析器还会收集有关失败错误代码的匿名数据。此数据包含在 CEIP 收集的其他数据中。如果您终止 CEIP 注册，则收集的 MSI 分析器数据将不再发送到 Citrix。

VDA 安装期间

- 适用于 Windows 的 Citrix Workspace™ 应用程序可用，但在安装 VDA 时默认不安装。您或您的用户可以从 Citrix 网站下载、安装（和升级）适用于 Windows 的 Citrix Workspace 应用程序以及其他 Citrix Workspace 应用程序。或者，您可以从 StoreFront 服务器提供这些 Citrix Workspace 应用程序。请参阅 StoreFront 文档。

- 必须启用 Microsoft Print Spooler 服务。如果该服务被禁用，则无法成功安装 VDA。
- 必须禁用 Windows Protected Print (WPP) 模式。如果启用了 WPP 模式，则无法成功安装 VDA。
- 大多数受支持的 Windows 版本都已预装 Microsoft Media Foundation。如果计算机没有 Media Foundation（例如 N 版本），则某些多媒体功能将不会安装且无法工作。
  - Windows Media 重定向
  - HTML5 视频重定向
  - HDX™ RealTime 网络摄像头重定向

  您可以确认此限制，或者结束 VDA 安装并在安装 Media Foundation 后重新启动。在图形界面中，此选择会显示在消息中。在命令行中，您可以使用 `/no_mediafoundation_ack` 选项来确认此限制。
- 安装 VDA 时，会自动创建一个名为 **Direct Access Users** 的新本地用户组。在单会话操作系统 VDA 上，此组仅适用于 RDP 连接。在多会话操作系统 VDA 上，此组适用于 ICA® 和 RDP 连接。
- VDA 必须具有有效的 Controller 地址才能进行通信。否则，无法建立会话。您可以在安装 VDA 时或之后指定 Controller 地址。请记住，必须完成此操作。有关详细信息，请参阅 VDA 注册。

VDA 安装后和安装期间的重新启动

VDA 安装结束时需要重新启动。默认情况下，该重新启动会自动发生。

将 VDA 升级到版本 7.17（或更高支持版本）时，升级期间会发生重新启动。这是无法避免的。

要最大程度地减少 VDA 安装期间所需的重新启动次数：

- 确保在开始 VDA 安装之前已安装受支持的 .NET Framework 版本。
- 对于 Windows 多会话操作系统计算机，请在安装 VDA 之前安装并启用 RDS 角色服务。

如果您在安装 VDA 之前未安装这些必备项：

- 如果您使用的是图形界面或不带 `/noreboot` 选项的命令行界面，则计算机在安装必备项后会自动重新启动。
- 如果您使用的是带 `/noreboot` 选项的命令行界面，则必须手动启动重新启动。

升级 VDA 版本时，升级过程中会发生重启。这是无法避免的。

安装或升级失败时恢复

> **注意：**
>
> 此功能仅适用于工作站 VDA。为确保更可靠、更流畅的安装体验，服务器 VDA 不再支持“故障时恢复”功能。Citrix 建议在安装或升级服务器 VDA 之前手动创建备份。

> 如果工作站 VDA 安装或升级失败，并且启用了“故障时恢复”功能，则计算机将恢复到安装或升级开始之前设置的还原点。

当工作站 VDA 安装或升级在启用此功能的情况下开始时，安装程序会在实际安装或升级开始之前创建一个系统还原点。如果 VDA 安装或升级失败，计算机将恢复到还原点状态。`%temp%/Citrix` 文件夹包含部署日志和有关恢复的其他信息。

默认情况下，此功能处于禁用状态。

如果您计划启用此功能，请确保未通过 GPO 设置禁用系统还原 (`Computer Configuration > Administrative Templates > System > System Restore`)。

在安装或升级工作站 VDA 时启用此功能：

- 使用 VDA 安装程序的图形界面（例如，使用 **Autostart** 或不带任何恢复或静默选项的 `XenDesktopVDASetup.exe` 命令）时，在“**附加组件**”页面上选中 **Citrix Backup and Restore Service** 复选框。

  如果安装/升级成功完成，则还原点不会被使用，但会保留。
- 使用命令行运行 VDA 安装程序并添加以下选项之一：`/enablerestorecleanup`、`/enablerestore` 或 `/includeadditional` "Citrix Backup and Restore"。
  - 如果您使用 `/enablerestorecleanup` 选项，并且安装/升级成功完成，则还原点将自动删除。
  - 如果您使用 /enablerestore 或 /includeadditional "Citrix Backup and Restore" 选项，并且安装/升级成功完成，则还原点不会被使用，但会保留。

> **注意：**
>
> 如果您尝试在服务器 VDA 上使用 `/enablerestorecleanup`、`/enablerestore` 或 `/includeadditional` "Citrix Backup and Restore" 选项，安装程序将忽略这些选项并继续，而不会创建备份。

安装程序

完整产品安装程序

使用 ISO 中提供的完整产品安装程序，您可以：

- 安装、升级或删除核心组件：Delivery Controller、Studio、Director 和 License Server。
- 安装或升级 StoreFront。
- 安装或升级用于单会话或多会话操作系统的 Windows VDA。
- 在您的打印服务器上安装 Universal Print Server `UpsServer` 组件。
- 安装 联邦身份验证服务。
- 安装 会话录制。
- 安装 工作区环境管理。

> **注意：**
>
> Workspace Environment Management™ 代理安装程序未本地化。它仅提供英文版本。

要从多会话操作系统为单个用户（例如，用于 Web 开发）交付桌面，请使用完整产品安装程序的命令行界面。有关详细信息，请参阅 Server VDI。

独立 VDA 安装程序

独立 VDA 安装程序可在 Citrix 下载页面上获取。（它们不随产品安装介质提供。）独立 VDA 安装程序比完整产品 ISO 小得多。它们更容易适应以下部署：

- 使用本地暂存或复制的电子软件分发 (ESD) 软件包
- 拥有物理机
- 拥有远程办公室

默认情况下，自解压独立 VDA 中的文件会提取到 **Temp** 文件夹。与使用完整产品安装程序相比，提取到 **Temp** 文件夹时，计算机上需要更多的磁盘空间。但是，提取到 **Temp** 文件夹的文件在安装完成后会自动删除。或者，您可以使用带绝对路径的 `/extract` 命令。

有四种独立的 VDA 安装程序可供下载。

多会话操作系统虚拟投递代理 (VDAServerSetup.exe)：

为多会话操作系统安装 VDA。它支持完整产品安装程序提供的所有多会话操作系统 VDA 选项。

单会话操作系统虚拟投递代理 (VDAWorkstationSetup.exe)：

为单会话操作系统安装 VDA。它支持完整产品安装程序提供的所有单会话操作系统 VDA 选项。

单会话操作系统核心服务虚拟投递代理 (VDAWorkstationCoreSetup.exe)：

为单会话操作系统安装 VDA，该 VDA 针对远程电脑访问部署或核心 VDI 安装进行了优化。远程电脑访问使用物理机。核心 VDI 安装是未用作映像的 VM。它仅安装此类部署的 VDA 连接所需的核心服务。因此，它仅支持完整产品或 `VDAWorkstationSetup.exe` 安装程序中有效选项的子集。

此安装程序不安装或不包含用于以下目的的组件：

- 应用虚拟化。
- 配置文件管理。将 Citrix Profile Management 从安装中排除会影响 Citrix Director 显示。有关详细信息，请参阅安装 VDA。
- 计算机身份服务。
- Citrix MCS I/O 驱动程序
- Citrix 备份和还原
- deviceTRUST
- uberAgent
- WEM

`VDAWorkstationCoreSetup.exe` 安装程序不安装或不包含以下组件：适用于 Windows 的 Citrix Workspace 应用程序 (CWA)、Citrix Secure Access Client (CSA)、Citrix 用户个性化层 (UPL)、会话录制代理 (SRAGENT) 和 Citrix Assistant App (ASSISTANTAPP)。

使用 `VDAWorkstationCoreSetup.exe` 等同于使用完整产品或 `VDAWorkstationSetup` 安装程序安装单会话操作系统 VDA，并执行以下任一操作：

- 在图形界面中：在**环境**页面上选择“远程电脑访问”选项。
- 在命令行界面中：指定 `/remotepc` 选项。
- 在命令行界面中：指定 `/components vda` 以及列出所有有效附加组件名称的 `/exclude` 选项。

您可以通过运行完整产品安装程序来稍后安装省略的组件/功能。该操作使您能够安装所有缺失的组件。

`VDAWorkstationCoreSetup.exe` 安装程序会自动安装 Browser Content Redirection MSI。此自动安装适用于 VDA 2003 及更高版本支持的版本。

单会话核心服务虚拟投递代理 (VDASingleSessionCoreSetup.exe)：

适用于 Windows 365 Cloud PC 和远程电脑部署的新型轻量级单会话 VDA 元安装程序。此安装程序基于现有 VDAWorkstationCoreSetup.exe 安装程序构建，提供必要的 VDA 组件以及配置文件管理、deviceTRUST、uberAgent、WEM、备份和还原以及 VDA 升级代理。可以使用命令行选项 /enablerestore 或 /enablerestorecleanup 启用备份和还原功能。

它显著减小了程序包大小，并提高了基于云的工作负载的安装可靠性。此安装程序专为现代远程电脑场景设计，为在 Windows 365 和远程电脑上部署 Citrix 工作负载提供了简化且高性能的选项。

使用单会话 VDA 安装程序的最佳实践

对于单会话操作系统，有四种不同的安装程序可用。完整产品 VDA 安装程序和 VDAWorkstationSetup.exe 安装程序提供所有组件的安装，而 VDAWorkstationCoreSetup.exe 和 VDASingleSessionCoreSetup.exe 安装程序不包含某些默认和附加组件。

为了保持环境稳定性、一致的性能和持续的可支持性，Citrix 建议在 Citrix VDA 的整个生命周期（包括安装、升级和卸载）中，使用一致的安装程序类型。混合使用安装程序类型可能会带来某些风险。

混合安装程序类型相关的风险：

场景 1： 如果单会话 VDA 最初使用 VDAWorkstationCoreSetup.exe 或 VDASingleSessionCoreSetup.exe 安装程序安装，随后使用完整产品 VDA 安装程序或 VDAWorkstationSetup.exe 安装程序进行升级，则除非明确排除，否则以前排除的组件可能会在升级期间安装。

场景 2： 如果单会话 VDA 最初使用完整产品 VDA 安装程序或 VDAWorkstationSetup.exe 安装，随后使用 VDAWorkstationCoreSetup.exe 或 VDASingleSessionCoreSetup.exe 进行升级，则核心服务 VDA 安装程序未安装的任何组件都将从升级中排除。这些组件在升级过程中既不会升级，也不会在卸载期间删除。

场景 3： 如果单会话 VDA 最初使用 VDAWorkstationCoreSetup.exe 安装程序安装，随后使用 VDASingleSessionCoreSetup.exe 进行升级，您将体验到新功能。如果您下次使用 VDAWorkstationCoreSetup.exe 进行升级，则 VDASingleSessionCoreSetup.exe 新增的组件在升级过程中既不会升级，也不会在卸载期间删除。

解决混合安装程序类型的指南：

如果需要混合安装程序类型，则必须确保在升级过程中包含相同的组件。

如果安装程序类型不慎混用，导致安装了额外的组件或某些组件脱离了管理，并且需要恢复到以前的环境，请按以下步骤操作：

- **对于场景 1：** 从 Windows 的卸载或更改程序功能中卸载 VDA，然后使用您最初使用的安装程序（VDAWorkstationCoreSetup.exe 或 VDASingleSessionCoreSetup.exe）重新安装 VDA。
- **对于场景 2：** 使用完整产品 VDA 安装程序或 VDAWorkstationSetup.exe 安装程序升级缺失的组件。
- **对于场景 3：** 如果您打算继续利用新功能，请使用 VDASingleSessionCoreSetup.exe 安装程序升级缺失的组件。或者，如果您在通过 VDASingleSessionCoreSetup.exe 升级后不希望使用新功能，请首先从 Windows 的卸载或更改程序功能中卸载 VDA，然后使用 VDAWorkstationCoreSetup.exe 重新安装 VDA。

Citrix 安装返回代码

安装日志包含组件安装结果，其形式为 Citrix 返回代码，而非 Microsoft 值。

- 0 = 成功
- 1 = 失败
- 2 = 部分成功
- 3 = 部分成功且需要重新启动
- 4 = 失败且需要重新启动
- 5 = 用户取消
- 6 = 命令行参数错误
- 7 = 发现新版本
- 8 = 成功，需要重新启动
- 9 = 文件锁定，需要重新启动
- 10 = 已中止
- 11 = 介质失败
- 12 = 许可证失败
- 13 = 预检失败
- 14 = 已中止，待处理重新启动检查
- 15 = 预检通过 - 在使用新的 /precheckonly 命令行选项后，如果预检通过，则返回此值。
- 16 = 预检失败 - 在使用新的 /precheckonly 命令行选项后，如果预检失败，则返回此值。
- 17 = 可选软件失败 - 当新的可选软件组件之一安装失败，并且已选择“如果任何其他选定组件失败，则继续 VDA 安装或升级”时，将返回此值。

例如，当使用 Microsoft System Center Configuration Manager 等工具时，如果安装日志包含返回代码 3，则脚本化的 VDA 安装可能看似失败。这可能发生在 VDA 安装程序正在等待您必须启动的重新启动时（例如，在服务器上安装 RDS 角色先决条件之后）。只有在安装了所有先决条件和选定组件，并且安装后重新启动计算机，VDA 安装才被视为成功。

或者，您可以将安装包装在 CMD 脚本中（这些脚本返回 Microsoft 退出代码），或者更改 Configuration Manager 包中的成功代码。

为 Windows Server 工作负载配置 Microsoft RDS 许可证服务器

此产品在交付 Windows Server 工作负载（例如 Windows 2016）时访问 Windows Server 远程会话功能。这通常需要远程桌面服务客户端访问许可证 (RDS CAL)。VDA 必须能够联系 RDS 许可证服务器以请求 RDS CAL。安装并激活许可证服务器。有关详细信息，请参阅 Microsoft 文档 激活远程桌面服务许可证服务器。对于概念验证环境，您可以使用 Microsoft 提供的宽限期。

使用此方法，您可以让此服务应用许可证服务器设置。您可以在映像上的 RDS 控制台中配置许可证服务器和每用户模式。您还可以使用 Microsoft 组策略设置配置许可证服务器。有关详细信息，请参阅 Microsoft 文档 使用客户端访问许可证 (CAL) 许可 RDS 部署。

要使用组策略设置配置 RDS 许可证服务器：

1. 在可用计算机上安装远程桌面服务许可证服务器。该计算机必须始终可用。Citrix 产品工作负载必须能够访问此许可证服务器。
2. 使用 Microsoft 组策略指定许可证服务器地址和每用户许可证模式。有关详细信息，请参阅 Microsoft 文档 为 RD 会话主机服务器指定远程桌面许可模式。

Windows 10 工作负载需要适当的 Windows 10 许可证激活。我们建议您遵循 Microsoft 文档来激活 Windows 10 工作负载。

更多信息

对于特定主机类型的资源位置设置：

- AWS 云环境
- XenServer 虚拟化环境
- Google Cloud 环境
- Microsoft Azure 资源管理器云环境
- Microsoft System Center 配置管理器环境
- Microsoft System Center 虚拟机管理器虚拟化环境
- Nutanix 虚拟化环境

- Nutanix 云和合作伙伴解决方案
- VMware 虚拟化环境
- VMware 云和合作伙伴解决方案

Amulet Hotkey CoreStation 虚拟化环境

Citrix Virtual Apps and Desktops™ 通过 Citrix 管理的 Amulet Hotkey CoreStation 插件管理您的 Amulet Hotkey CoreStation 工作负载。借助此插件，您可以创建与 Amulet Hotkey CoreStation 机箱的连接、创建目录以及对目录中的计算机进行电源管理。

关键步骤

1. 设置您的 Amulet Hotkey CoreStation 环境。
2. 创建与 Amulet Hotkey CoreStation 机箱的连接。
3. 创建 Amulet Hotkey CoreStation 计算机目录。

> **注意：**
>
> 在创建目录之前，请确保拥有一台或多台 Amulet Hotkey CoreStation 节点，并在这些节点上安装 VDA。您可以将 Amulet Hotkey CoreStation 机箱视为管理程序，将节点视为虚拟机。

4. 创建交付组。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关创建和管理连接的信息，请参阅 连接到 Amulet Hotkey CoreStation。

更多信息

- 创建和管理连接与资源
- 创建计算机目录

AWS 云环境

本文将指导您如何将 AWS 账户设置为可与 Citrix Virtual Apps and Desktops 配合使用的资源位置。该资源位置用于在 AWS EC2 和 Amazon WorkSpaces Core 托管实例中预配工作负载。有关 Amazon WorkSpaces Core 托管实例支持的操作系统类型列表，请参阅 Amazon WorkSpaces Core 托管实例中的 VDA。

不同可配置资源位置的比较：适用于 AWS EC2 的 MCS、适用于 Amazon WorkSpaces Core 托管实例的 MCS 以及 适用于 Amazon WorkSpaces Core 捆绑包的快速部署。

适用于 AWS EC2 的 MCS	适用于 AMAZON WORKSPACES CORE 托管实例的 MCS	适用于 AMAZON WORKSPACES CORE 捆绑包的快速部署
Citrix® 处理您 AWS 账户中的 VM 预配	Citrix 处理您 AWS 账户中的 VM 预配	Amazon 处理 AWS 托管的 WorkSpaces 账户中的 VM 预配
用于 VM 生命周期管理的高级 MCS 工作流	用于 VM 生命周期管理的高级 MCS 工作流	5 步快速简便的工作流
EC2 实例	WorkSpaces Core 托管实例（利用直接启动到您的 AWS 账户中的按需 EC2 实例）	WorkSpaces 捆绑包，完全由 AWS 管理的容量（更高级别的抽象）
无 Microsoft 365 许可支持	BYOL Microsoft 365 支持	BYOL Microsoft 365 支持
Windows 服务器、Windows 桌面和 Linux	Windows 服务器、Windows 桌面和 Linux	Windows 服务器、Windows 桌面
持久和非持久 VM	持久和非持久 VM	仅持久 VM
仅按需付费	按需付费	仅按月固定价格
思杰 DaaS 和 思杰虚拟应用和桌面™	思杰 DaaS 和 思杰虚拟应用和桌面™	仅限 Citrix DaaS

完成本文中的任务后，您的资源位置将包含以下组件：

- 一个虚拟私有云 (VPC)，其中包含单个可用区内的公共子网和私有子网。
- 一个实例，在 VPC 的私有子网中运行，既作为 Active Directory 域控制器又作为 DNS 服务器。

- 在 VPC 的公共子网中充当堡垒主机的实例。此实例用于启动到私有子网中实例的 RDP 连接，以进行管理。完成资源位置设置后，您可以关闭此实例，使其不再易于访问。当您必须管理私有子网中的其他实例（例如 VDA 实例）时，可以重新启动堡垒主机实例。

任务概述

设置具有公共和私有子网的虚拟私有云 (VPC)。 完成此任务后，AWS 会在公共子网中部署一个带有弹性 IP 地址的 NAT 网关。此操作使私有子网中的实例能够访问 Internet。公共子网中的实例可访问入站公共流量，而私有子网中的实例则不能。

配置安全组。安全组充当虚拟防火墙，控制 VPC 中实例的流量。您将规则添加到安全组中，以允许公共子网中的实例与私有子网中的实例通信。您还将这些安全组与 VPC 中的每个实例关联。

创建 DHCP 选项集。对于 Amazon VPC，默认提供 DHCP 和 DNS 服务，这会影响您在 Active Directory 域控制器上配置 DNS 的方式。Amazon 的 DHCP 无法禁用，并且 Amazon 的 DNS 只能用于公共 DNS 解析，而不能用于 Active Directory 名称解析。要指定通过 DHCP 传递给实例的域和名称服务器，请创建 DHCP 选项集。该集会分配 Active Directory 域后缀并为 VPC 中的所有实例指定 DNS 服务器。为确保实例加入域时自动注册主机 (A) 和反向查找 (PTR) 记录，请为添加到私有子网的每个实例配置网络适配器属性。

将堡垒主机和域控制器添加到 VPC。通过堡垒主机，您可以登录到私有子网中的实例以设置域并将实例加入域。

任务 1：设置 VPC

1. 在 AWS 管理控制台中，选择 **VPC**。
2. 在 VPC 控制面板中，选择 **Create VPC**（创建 VPC）。
3. 选择 **VPC and more**。
4. 在 NAT 网关 ($) 下，选择 **In 1 AZ** 或 **1 per AZ**。
5. 在 DNS 选项下，保持选中 **Enable DNS hostnames**。
6. 选择 **Create VPC**。AWS 会创建公共和私有子网、Internet 网关、路由表和默认安全组。

任务 2：配置安全组

此任务为您的 VPC 创建并配置以下安全组：

- 一个公共安全组，用于关联公共子网中的实例。
- 一个私有安全组，用于关联私有子网中的实例。

要创建安全组：

1. 在 VPC 控制面板中，选择 **Security Groups**。
2. 为公共安全组创建一个安全组。选择 **Create Security Group**，然后输入该组的名称标签和描述。在 VPC 中，选择您之前创建的 VPC。选择 **Yes, Create**。

配置公共安全组

1. 从安全组列表中，选择公共安全组。
2. 选择“**入站规则**”选项卡并选择“**编辑**”以创建以下规则：

类型	源
所有流量	选择私有安全组。
所有流量	选择公共安全组。
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (会话可靠性)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. 完成后，选择**保存**。
4. 选择“**出站规则**”选项卡并选择“**编辑**”以创建以下规则：

类型	目标
所有流量	选择私有安全组。
所有流量	0.0.0.0/0
ICMP	0.0.0.0/0

5. 完成后，选择**保存**。

配置私有安全组

1. 从安全组列表中，选择私有安全组。
2. 如果您尚未设置来自公共安全组的流量，则必须设置 TCP 端口；选择“**入站规则**”选项卡并选择“**编辑**”以创建以下规则：

类型	源
所有流量	选择私有安全组。
所有流量	选择公共安全组。
ICMP	选择公共安全组。
TCP 53 (DNS)	选择公共安全组。
UDP 53 (DNS)	选择公共安全组。
80 (HTTP)	选择公共安全组。
TCP 135	选择公共安全组。
TCP 389	选择公共安全组。
UDP 389	选择公共安全组。
443 (HTTPS)	选择公共安全组。
TCP 1494 (ICA/HDX)	选择公共安全组。
TCP 2598 (会话可靠性)	选择公共安全组。
3389 (RDP)	选择公共安全组。
TCP 49152–65535	选择公共安全组。

3. 完成后，选择“**保存**”。
4. 选择“**出站规则**”选项卡并选择“**编辑**”以创建以下规则：

类型	目标
所有流量	选择私有安全组。

类型	目标
所有流量	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. 完成后，选择**保存**。

任务 3：启动实例

执行以下步骤以创建两个 EC2 实例并解密 Amazon 生成的默认管理员密码：

1. 在 AWS 管理控制台中，选择 **EC2**。
2. 在 EC2 控制面板中，选择 **启动实例**。
3. 选择 Windows Server 计算机映像和实例类型。
4. 在“**配置实例详细信息**”页面上，为实例输入名称并选择您之前设置的 VPC。
5. 在 **子网** 中，为每个实例进行以下选择：
   - 堡垒主机：选择公共子网
   - 域控制器：选择私有子网
6. 在 **自动分配公有 IP 地址** 中，为每个实例进行以下选择：
   - 堡垒主机：选择“**启用**”。
   - 域控制器：选择“**使用默认设置**”或“**禁用**”。
7. 在 **网络接口** 中，输入您的私有子网 IP 范围内的主 IP 地址，供域控制器使用。
8. 如有必要，在 **添加存储** 页面上，修改磁盘大小。
9. 在 **标记实例** 页面上，为每个实例输入一个易记的名称。
10. 在 **配置安全组** 页面上，选择 **选择现有安全组**，然后为每个实例进行以下选择：
    - 堡垒主机：选择公有安全组。
    - 域控制器：选择私有安全组。
11. 查看您的选择，然后选择 **启动**。
12. 创建新的密钥对或选择现有密钥对。如果您创建新的密钥对，请下载您的私钥 (.pem) 文件并将其保存在安全位置。在获取实例的默认管理员密码时，您必须提供您的私钥。

13. 选择 **启动实例**。选择 **查看实例** 以显示您的实例列表。请等待新启动的实例通过所有状态检查后再访问它。
14. 获取每个实例的默认管理员密码：
    a. 从实例列表中，选择实例，然后选择 **连接**。
    b. 转到 **RDP 客户端** 选项卡，选择 **获取密码**，并在出现提示时上传您的私钥 (`.pem`) 文件。
    c. 选择 **Decrypt Password** 以获取人类可读的密码。AWS 会显示默认密码。
15. 重复步骤 2 中的步骤，直到您创建了两个实例：
    - 一个位于公共子网中的堡垒主机实例
    - 您的私有子网中的一个实例，用作域控制器。

任务 4：创建 DHCP 选项集

1. 在 VPC 控制面板中，选择 **DHCP Options Sets**。
2. 输入以下信息：
    - 名称标签：为该集输入一个易记的名称。
    - 域名：输入配置域控制器实例时使用的完全限定域名。
    - 域名服务器：输入分配给域控制器实例的私有 IP 地址和字符串 **AmazonProvidedDNS**，用逗号分隔。
    - NTP 服务器：将此字段留空。
    - NetBIOS 名称服务器：输入域控制器实例的私有 IP 地址。
    - NetBIOS 节点类型：输入 **2**。
3. 选择 **是，创建。**
4. 将新集与您的 VPC 关联：
    a. 在 VPC 控制面板中，选择 **您的 VPC**，然后选择您之前设置的 VPC。
    b. 选择 **操作 > 编辑 DHCP 选项集**。
    c. 出现提示时，选择您创建的新集，然后选择 **保存**。

任务 5：配置实例

1. 使用 RDP 客户端连接到堡垒主机实例的公共 IP 地址。出现提示时，输入管理员帐户的凭据。
2. 从堡垒主机实例启动远程桌面连接，并连接到您要配置的实例的私有 IP 地址。出现提示时，输入实例的管理员凭据。

3. 对于私有子网中的所有实例，配置 DNS 设置：
    a. 选择 **开始 > 控制面板 > 网络和 Internet > 网络和共享中心 > 更改适配器设置**。双击显示的网络连接。
    b. 选择 **属性 > Internet 协议版本 4 (TCP/IPv4) > 属性**。
    c. 选择 **高级 > DNS**。确保以下设置已启用，然后选择 **确定**：
        - 在 DNS 中注册此连接的地址
        - 在 DNS 注册中使用此连接的 DNS 后缀
4. 要配置域控制器：
    a. 使用服务器管理器，添加具有所有默认功能的 Active Directory 域服务角色。
    b. 将实例提升为域控制器。在提升过程中，启用 DNS 并使用创建 DHCP 选项集时指定的域名。出现提示时，重新启动实例。

有关 AWS 权限的信息，请参阅 所需的 AWS 权限 - Amazon EC2 和 所需的 AWS 权限 - Amazon WorkSpaces Core 托管实例。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关创建和管理连接的信息，请参阅：
    - 连接到 AWS EC2
    - 连接到 Amazon WorkSpaces Core 托管实例

更多信息

- 创建和管理连接与资源
- 创建计算机目录

Azure Local 环境

Azure Local（基于 Azure Arc）是一种超融合基础设施 (HCI) 解决方案，可将本地系统连接到 Azure，以实现基于云的服务、监视和管理。

先决条件

- Azure Local 群集：2503 或更高版本
  - 已创建存储路径
  - 已创建并启用了 DHCP 的逻辑网络
- 要部署 Azure Local 群集，请参阅 Microsoft 文档 关于 Azure Local 部署。

注意事项

- 不支持 Windows 10 和 11 多会话工作负载。

主要步骤

在 Azure Local 群集中创建 MCS 目录的关键步骤如下：

1. 创建主机连接。
2. 创建目录。

下一步操作

- 有关创建到 Azure Local 的连接，请参阅 连接到 Azure Local。

更多信息

- 创建和管理连接与资源

XenServer® 虚拟化环境

XenServer 简化了您的运营管理，为密集型工作负载提供高清用户体验。

要设置 XenServer，请参阅准备安装。

下一步

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关在 XenServer 中创建和管理连接的信息，请参阅连接到 XenServer

更多信息

- 创建和管理连接和资源

- 创建计算机目录

Google Cloud 环境

Citrix Virtual Apps and Desktops™ 允许您在 Google Cloud 上预配和管理计算机。

要求

- Citrix Cloud™ 帐户。本文中描述的功能仅在 Citrix Cloud 中可用。
- 一个 Google Cloud 项目。该项目存储与计算机目录关联的所有计算资源。它可以是现有项目，也可以是新项目。
- 在您的 Google Cloud 项目中启用四个 API。有关详细信息，请参阅启用 Google Cloud API。
- Google Cloud 服务帐户。该服务帐户向 Google Cloud 进行身份验证，以启用对项目的访问。有关详细信息，请参阅 配置和更新服务帐户。
- 启用 Google 私有访问。有关详细信息，请参阅启用 Google 私有访问。

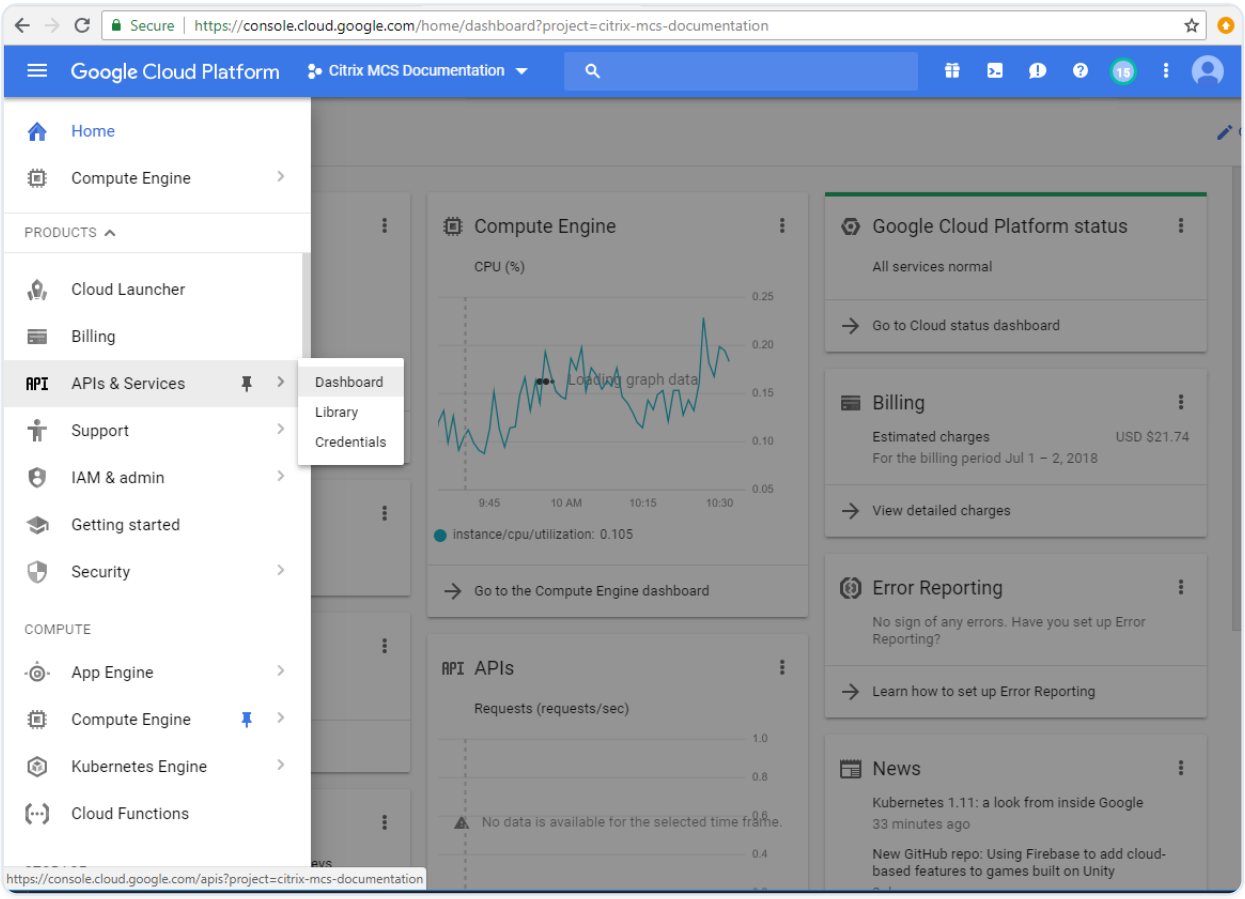
启用 Google Cloud API

要通过 Web Studio 使用 Google Cloud 功能，请在您的 Google Cloud 项目中启用以下 API：

- 计算引擎 API
- 云资源管理器 API
- 身份与访问管理 (IAM) API
- Cloud Build 接口
- Cloud 密钥管理服务 (KMS)

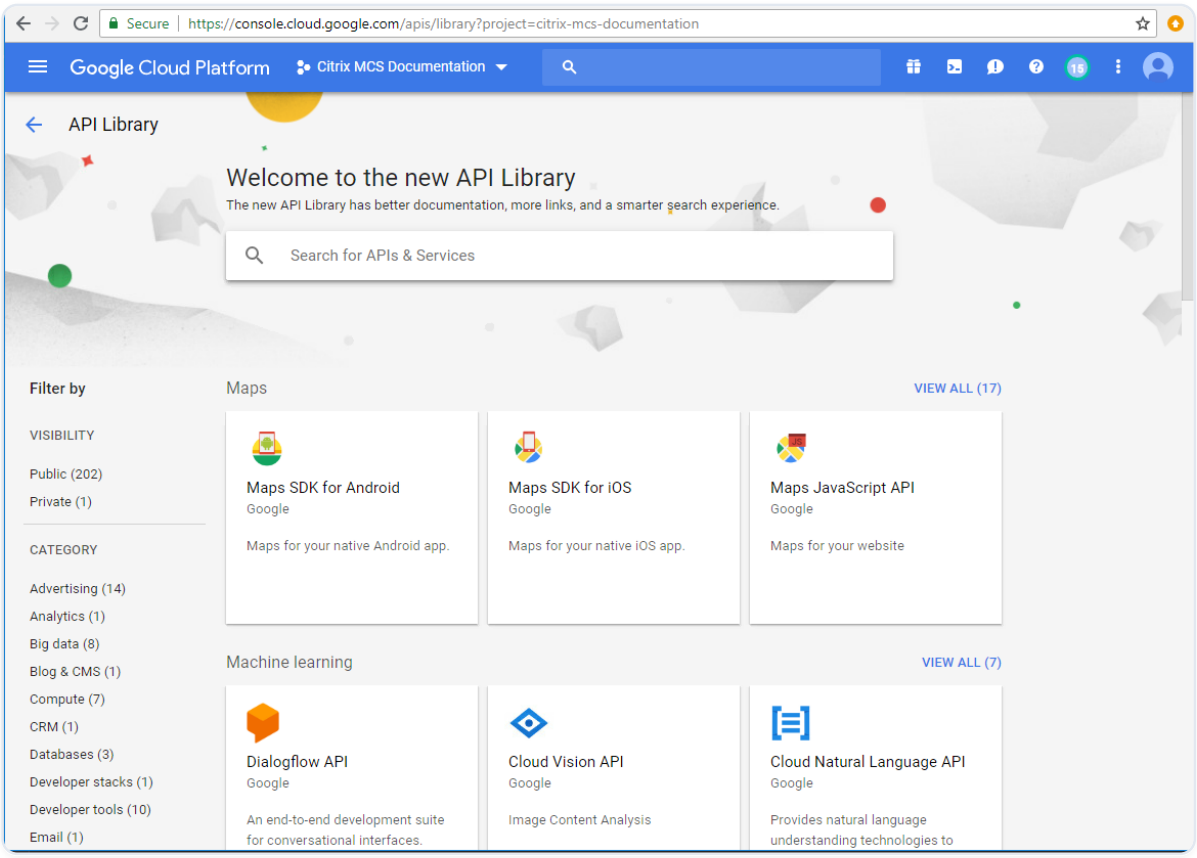
在 Google Cloud 控制台中，完成以下步骤：

1. 在左上角菜单中，选择 **API 和服务 > 控制面板**。



2. 在**控制面板**屏幕上，确保已启用 Compute Engine API。如果 未启用，请按照以下步骤操作：

   a. 导航到**API 和服务 > 库**。



b. 在搜索框中，键入 *Compute Engine*。

c. 从搜索结果中，选择**Compute Engine API**。

d. 在**Compute Engine API**页面上，选择**启用**。

3. 启用云资源管理器 API。

a. 导航到**API 和服务 > 库**。

b. 在搜索框中，键入 *Cloud Resource Manager*。

c. 从搜索结果中，选择**Cloud Resource Manager API**。

d. 在**Cloud Resource Manager API**页面上，选择**启用**。API 的状态将显示。

4. 同样，启用 **身份与访问管理 (IAM) API** 和 **云构建 API**。

您还可以使用 Google Cloud Shell 启用 API。为此，请执行以下操作：

1. 打开 Google 控制台并加载 Cloud Shell。
2. 在 Cloud Shell 中运行以下四个命令：
   - 启用计算服务：gcloud services enable compute.googleapis.com
   - 启用云资源管理器服务：gcloud services enable cloudresourcemanager.googleapis.com
   - gcloud 服务 启用 iam.googleapis.com
   - gcloud 服务 启用 cloudbuild.googleapis.com
3. 如果 Cloud Shell 提示，请单击**授权**。

配置和更新服务帐号

> **注意：**
>
> GCP 将在 April 29, 2024 之后对 Cloud Build Service 的默认行为和服务帐号的使用引入更改。有关详细信息，请参阅 Cloud Build 服务帐号更改。您在 April 29, 2024 之前启用了 Cloud Build API 的现有 Google 项目不受此更改的影响。但是，如果您希望在 April 29 之后保留现有的 Cloud Build Service 行为，则可以在启用 Cloud Build API 之前创建或应用组织策略以禁用约束实施。因此，以下内容分为两部分：April 29, 2024 之前 和 April 29, 2024 之后。如果您设置了新的组织策略，请按照 April 29, 2024 之前 部分操作。

April 29, 2024 之前

Citrix Cloud 在 Google Cloud 项目中使用三个独立的服务帐户：

- *Citrix Cloud 服务帐号*：此服务帐号使 Citrix Cloud 能够访问 Google 项目、预配和管理计算机。此服务帐号使用 Google Cloud 生成的 密钥 对 Google Cloud 进行身份验证。

  您必须按照此处所述手动创建此服务帐号。有关详细信息，请参阅 创建 Citrix Cloud 服务帐号。

  您可以使用电子邮件地址识别此服务帐号。例如，`<my-service-account>@<project-id>.iam.gserviceaccount.com`。

- *Cloud Build 服务帐号*：启用 启用 Google Cloud API 中提及的所有 API 后，此服务帐号会自动预配。要查看所有自动创建的服务帐号，请在 **Google Cloud** 控制台中导航到 **IAM 和管理 > IAM**，然后选中 **包括 Google 提供的角色授予** 复选框。

  您可以通过以 **项目 ID** 和单词 **cloudbuild** 开头的电子邮件地址识别此服务帐号。例如，`<project-id>@cloudbuild.gserviceaccount.com`

  验证服务帐号是否已获得以下角色。如果必须添加角色，请按照向 Cloud Build 服务帐号添加角色中概述的步骤操作。

  - Cloud Build 服务帐户
  - 计算实例管理员
  - 服务帐号用户

- *Cloud Compute 服务帐号*：一旦 Compute API 激活，Google Cloud 就会将此服务帐号添加到在 Google Cloud 中创建的实例。此帐号具有 IAM 基本编辑者角色以执行操作。但是，如果您删除默认权限以进行更精细的控制，则必须添加一个需要以下权限的 **Storage Admin** 角色：

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

您可以通过以 **Project ID** 和单词 **compute** 开头的电子邮件地址来识别此服务帐号。例如，`<project-id>-compute@developer.gserviceaccount.com`。

创建 CITRIX CLOUD 服务帐号

要创建 Citrix Cloud 服务帐号，请执行以下步骤：

1. 在 Google Cloud 控制台中，导航到 **IAM & Admin > Service accounts**。

2. 在 **Service accounts** 页面上，选择 **CREATE SERVICE ACCOUNT**。
3. 在 **Create service account** 页面上，输入所需信息，然后选择 **CREATE AND CONTINUE**。
4. 在“**授予此服务帐号项目访问权限**”页面上，单击“**选择角色**”下拉菜单并选择所需的角色。如果要添加更多角色，请单击“**+添加其他角色**”。

   每个帐户（个人或服务）都具有定义项目管理的各种角色。向此服务帐户授予以下角色：

   - 计算管理员
   - Storage 管理员
   - Cloud Build 编辑者
   - 服务帐号用户
   - 云数据存储用户
   - Cloud KMS 加密操作员

   Cloud KMS 加密操作员需要以下权限：

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list
   - cloudkms.cryptoKeyVersions.useToDecrypt
   - cloudkms.cryptoKeyVersions.useToEncrypt

   > **注意：**
   >
   > 启用所有 API 以获取创建新服务帐户时可用的完整角色列表。

5. 单击“**继续**”
6. 在“**授予用户对此服务帐户的访问权限**”页面上，添加用户或组以授予他们在此服务帐户中执行操作的权限。
7. 单击“**完成**”。
8. 导航到 IAM 主控制台。
9. 识别已创建的服务帐户。
10. 验证角色是否已成功分配。

注意事项：

创建服务帐户时，请考虑以下事项：

- “**授予此服务帐户对项目的访问权限**”和“**授予用户对此服务帐户的访问权限**”步骤是可选的。如果选择跳过这些可选配置步骤，则新创建的服务帐户不会显示在“**IAM 和管理 > IAM**”页面中。
- 要显示与服务帐户关联的角色，请添加角色而不跳过可选步骤。此过程可确保角色显示在已配置的服务帐户中。

CITRIX CLOUD 服务帐户密钥

在 Citrix DaaS 中创建连接需要 Citrix Cloud 服务帐户密钥。该密钥包含在凭据文件 (.json) 中。创建密钥后，文件会自动下载并保存到 **Downloads** 文件夹。创建密钥时，请务必将密钥类型设置为 JSON。否则，Web Studio 无法解析它。

要创建服务帐户密钥，请导航到“**IAM 和管理 > 服务帐户**”，然后单击 Citrix Cloud 服务帐户的电子邮件地址。切换到“**密钥**”选项卡，然后选择“**添加密钥 > 创建新密钥**”。请务必选择 **JSON** 作为密钥类型。

> **提示：**
>
> 使用 Google Cloud 控制台中的“**服务帐户**”页面创建密钥。我们建议您定期更改密钥以确保安全。您可以通过编辑现有的 Google Cloud 连接，向 Citrix Virtual Apps and Desktops™ 应用程序提供新密钥。

向 CITRIX CLOUD 服务帐号添加角色

要向 Citrix Cloud 服务帐号添加角色，请执行以下操作：

1. 在 Google Cloud 控制台中，导航到 **IAM 和管理 > IAM**。
2. 在“**IAM > 权限**”页面上，找到您创建的服务帐号，该帐号可通过电子邮件地址识别。

   例如，`<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 选择铅笔图标以编辑服务帐号主体的访问权限。
4. 在所选主体选项的“**编辑对“project-id”的访问权限**”页面上，选择“**添加其他角色**”以逐个将所需角色添加到您的服务帐号，然后选择“**保存**”。

向 CLOUD BUILD 服务帐号添加角色

要向 Cloud Build 服务帐号添加角色，请执行以下操作：

1. 在 Google Cloud 控制台中，导航到 **IAM 和管理 > IAM**。

2. 在“**IAM**”页面上，找到 Cloud Build 服务帐号，该帐号可通过以“**项目 ID**”和单词“**cloudbuild**”开头的电子邮件地址识别。

   例如，`<project-id>@cloudbuild.gserviceaccount.com`

3. 选择铅笔图标以编辑 Cloud Build 帐号角色。
4. 对于所选的主体选项，在**“project-id”的编辑访问权限页面**上，选择**添加其他角色**以逐个将所需角色添加到您的 Cloud Build 服务帐号，然后选择**保存**。

> **注意：**
>
> 启用所有 API 以获取完整的角色列表。

April 29, 2024 之后

Citrix Cloud 在 Google Cloud 项目中使用两个独立的服务帐号：

- *Citrix Cloud 服务帐号*：此服务帐号使 Citrix Cloud 能够访问 Google 项目、预配和管理计算机。此服务帐号使用 Google Cloud 生成的 密钥 对 Google Cloud 进行身份验证。

  您必须手动创建此服务帐号。

  您可以使用电子邮件地址识别此服务帐号。例如，`<my-service-account>@<project-id>.iam.gserviceaccount.com`。

- *Cloud Compute 服务帐号*：启用启用 Google Cloud API中提及的所有 API 后，此服务帐号将自动预配。要查看所有自动创建的服务帐号，请在 **Google Cloud** 控制台中导航到 **IAM 和管理 > IAM**，然后选中**包括 Google 提供的角色授予**复选框。此帐号具有 IAM 基本编辑者角色以执行操作。但是，如果您删除默认权限以获得更精细的控制，则必须添加需要以下权限的 **Storage Admin** 角色：

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

  您可以通过以**项目 ID** 和单词 **compute** 开头的电子邮件地址识别此服务帐号。例如，`<project-id>-compute@developer.gserviceaccount.com.`.

  验证是否已向服务帐号授予以下角色。

- Cloud Build 服务帐户
- 计算实例管理员
- 服务帐号用户

创建 CITRIX CLOUD 服务帐号

要创建 Citrix Cloud 服务帐号，请执行以下步骤：

1. 在 Google Cloud 控制台中，导航到 **IAM & Admin > Service accounts**。
2. 在 **Service accounts** 页面上，选择 **CREATE SERVICE ACCOUNT**。
3. 在 **Create service account** 页面上，输入所需信息，然后选择 **CREATE AND CONTINUE**。
4. 在“**授予此服务帐号项目访问权限**”页面上，单击“**选择角色**”下拉菜单并选择所需的角色。如果要添加更多角色，请单击“**+添加其他角色**”。

   每个帐户（个人或服务）都具有定义项目管理的各种角色。向此服务帐户授予以下角色：

   - 计算管理员
   - Storage 管理员
   - Cloud Build 编辑者
   - 服务帐号用户
   - 云数据存储用户
   - Cloud KMS 加密操作员

   Cloud KMS 加密操作员需要以下权限：

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

   > **注意：**
   >
   > 启用所有 API 以获取创建新服务帐户时可用的完整角色列表。

5. 单击“**继续**”

6. 在“**授予用户对此服务帐户的访问权限**”页面上，添加用户或组以授予他们在此服务帐户中执行操作的权限。
7. 单击“**完成**”。
8. 导航到 IAM 主控制台。
9. 识别已创建的服务帐户。
10. 验证角色是否已成功分配。

注意事项：

创建服务帐户时，请考虑以下事项：

- “**授予此服务帐户对项目的访问权限**”和“**授予用户对此服务帐户的访问权限**”步骤是可选的。如果选择跳过这些可选配置步骤，则新创建的服务帐户不会显示在“**IAM 和管理 > IAM**”页面中。
- 要显示与服务帐户关联的角色，请添加角色而不跳过可选步骤。此过程可确保角色显示在已配置的服务帐户中。

CITRIX CLOUD 服务帐户密钥

在 Citrix DaaS 中创建连接需要 Citrix Cloud 服务帐户密钥。该密钥包含在凭据文件 (.json) 中。创建密钥后，该文件会自动下载并保存到 **Downloads** 文件夹。创建密钥时，请务必将密钥类型设置为 JSON。否则，Web Studio 无法对其进行解析。

要创建服务帐户密钥，请导航到“**IAM 和管理 > 服务帐户**”，然后单击 Citrix Cloud 服务帐户的电子邮件地址。切换到“**密钥**”选项卡，然后选择“**添加密钥 > 创建新密钥**”。请务必选择 **JSON** 作为密钥类型。

> **提示：**
>
> 在 Google Cloud 控制台的“**服务帐号**”页面中创建密钥。我们建议您定期更改密钥以确保安全。您可以通过编辑现有 Google Cloud 连接，向 Citrix Virtual Apps and Desktops 应用程序提供新密钥。

向 CITRIX CLOUD 服务帐号添加角色

要向 Citrix Cloud 服务帐号添加角色，请执行以下操作：

1. 在 Google Cloud 控制台中，导航到 **IAM 和管理 > IAM**。
2. 在“**IAM > 权限**”页面上，找到您创建的服务帐号，该帐号可通过电子邮件地址识别。

   例如，`<my-service-account>@<project-id>.iam.gserviceaccount.com`

3. 选择铅笔图标以编辑服务帐号主体的访问权限。
4. 在所选主体选项的“**编辑对“project-id”的访问权限**”页面上，选择“**添加其他角色**”以逐个将所需角色添加到您的服务帐号，然后选择“**保存**”。

向 CLOUD COMPUTE 服务帐号添加角色

要向 Cloud Compute 服务帐号添加角色，请执行以下操作：

1. 在 Google Cloud 控制台中，导航到 **IAM 和管理 > IAM**。
2. 在 **IAM** 页面上，找到 Cloud Compute 服务帐号，该帐号可通过以 **项目 ID** 和单词 **compute** 开头的电子邮件地址进行识别。

   例如，`<project-id>-compute@developer.gserviceaccount.com`
3. 选择铅笔图标以编辑 Cloud Build 帐号角色。
4. 对于所选的主体选项，在**“project-id”的编辑访问权限页面**上，选择**添加其他角色**以逐个将所需角色添加到您的 Cloud Build 服务帐号，然后选择**保存**。

> **注意：**
>
> 启用所有 API 以获取完整的角色列表。

存储权限和存储桶管理

Citrix Virtual Apps and Desktops 改进了 Google Cloud 服务 的云构建失败报告流程。此服务在 Google Cloud 上运行构建。Citrix Virtual Apps and Desktops 创建一个名为 `citrix-mcs-cloud-build-logs-{region}-{5 random characters}` 的存储桶，Google Cloud 服务在此存储桶中捕获构建日志信息。此存储桶上设置了一个选项，可在 30 天后删除内容。此过程要求用于连接的服务帐户具有设置为 `storage.buckets.update` 的 Google Cloud 权限。如果服务帐户没有此权限，Citrix Virtual Apps and Desktops 将忽略错误并继续执行目录创建过程。如果没有此权限，构建日志的大小会增加，并且需要手动清理。

启用私有 Google 访问

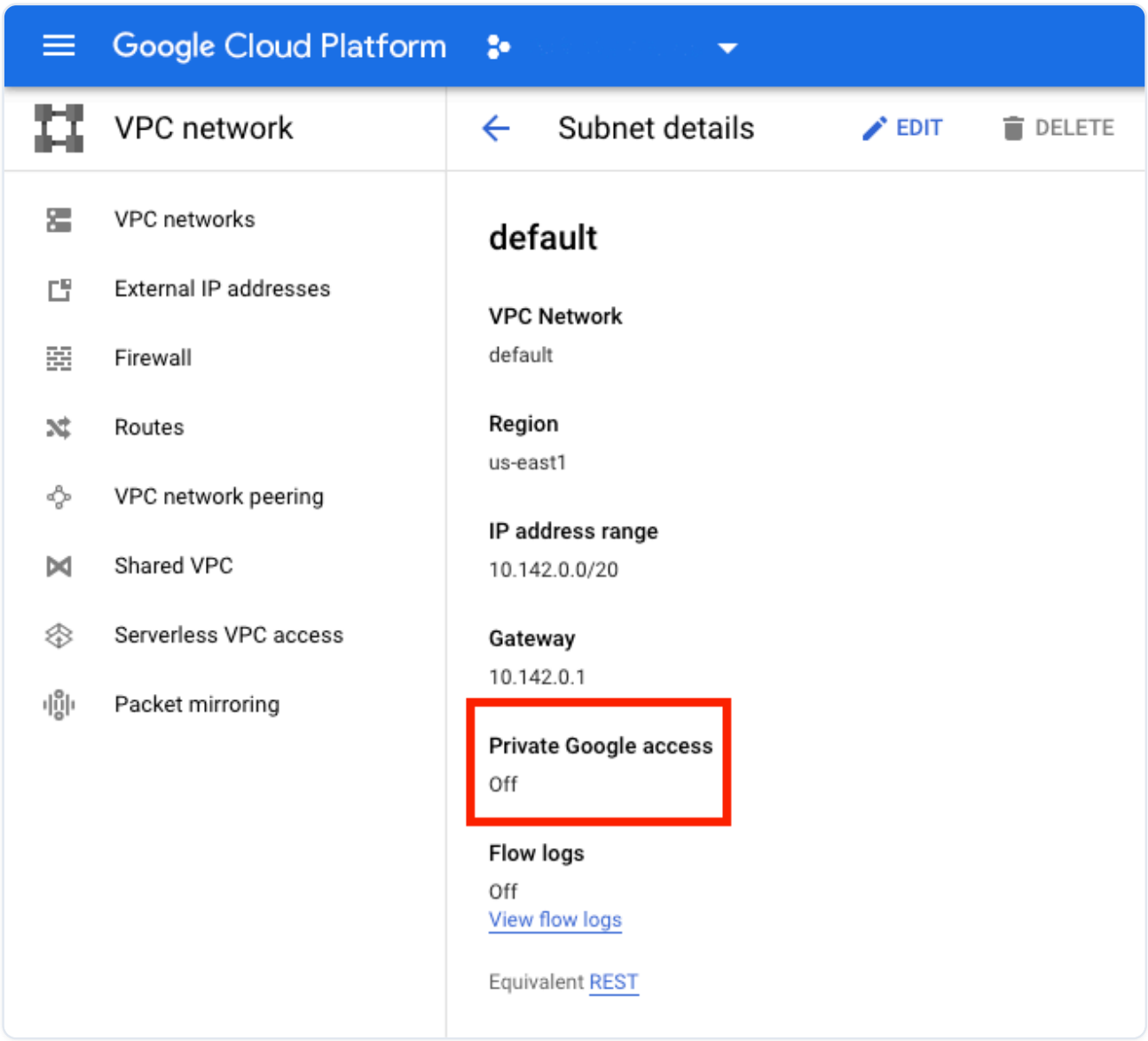
当虚拟机缺少分配给其网络接口的外部 IP 地址时，数据包只会发送到其他内部 IP 地址目标。启用私有访问后，虚拟机将连接到 Google API 和相关服务使用的外部 IP 地址集。

> **注意：**

> 无论是否启用私有 Google 访问，所有具有和不具有公共 IP 地址的虚拟机都必须能够访问 Google 公共 API，尤其是在环境中安装了第三方网络设备的情况下。

> 为确保子网中的 VM 可以在没有公共 IP 地址的情况下访问 Google API 以进行 MCS 预配：

1. 在 Google Cloud 中，访问 **VPC 网络配置**。
2. 在“子网详细信息”屏幕中，启用 **Private Google access**。



有关详细信息，请参阅配置 Private Google Access。

> **重要提示：**

> 如果您的网络配置为阻止 VM 访问 Internet，请确保您的组织承担为 VM 连接的子网启用 Private Google access 所带来的风险。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关在 Google Cloud 环境中创建和管理连接的信息，请参阅 连接到 Google Cloud 环境

更多信息

- 创建和管理连接与资源
- 创建计算机目录

HPE Moonshot 虚拟化环境

Citrix Virtual Apps and Desktops™ 通过现有的 Citrix 管理的 HPE Moonshot 插件管理您的 HPE Moonshot 工作负载。在升级或安装 Citrix Virtual Apps and Desktops 2503 版本时，Citrix 管理的 HPE Moonshot 插件会自动安装。借助此插件，您可以创建与 HPE Moonshot 机箱的连接、创建目录以及对目录中的计算机进行电源管理。

主要步骤

1. 设置您的 HPE 环境。
2. 创建与 HPE Moonshot 机箱的连接。
3. 创建计算机目录。

> **注意：**
>
> 在创建目录之前，请确保拥有一台或多台 HPE Moonshot 刀片节点，并在这些节点上安装 VDA。您可以将 HPE Moonshot 机箱视为管理程序，将刀片节点视为虚拟机。

4. 创建交付组。
5. 将其余未受管的 HPE Moonshot 节点迁移到受管目录或交付组。

> **注意：**
>
> 使用 Web Studio 而不是基于 MMC 的 Studio。

故障排除

如果同时安装了 Citrix 管理和 HPE 管理的 HPE Moonshot 插件，并且

- 如果要使用 **HPE 管理的 Moonshot 插件**，则必须卸载 Citrix 管理的 HPE Moonshot 插件并更新 `RegisterPlugin` 缓存。为此：

  a. 以管理员身份打开 PowerShell 并运行以下命令以卸载 Citrix 管理的 HPE Moonshot 插件：

  ```
  $CtxMnsht = Get-WmiObject -Class Win32_Product | Where-
  Object{$_.Name -Contains "Citrix HPE Moonshot Plugin"}

  $CtxMnsht.Uninstall()
  ```

  b. 运行以下命令以注册 HPE 管理的 Moonshot 插件：

  ```
  cd "C:\Program Files\Common Files\Citrix\HCLPlugins\"

  .\RegisterPlugins.exe -PluginsRoot "C:\Program Files\Common
  Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0\"
  ```

  c. 插件注册成功后，从**任务管理器**重新启动以下服务：

     a. CitrixBrokerService

     b. CitrixHostService

     c. CitrixMachineCreationService

  d. 运行 `Get-HypHypervisorPlugins` 以检查插件是否安装在 Delivery Controller 上。输出中的 `DisplayName` 字段必须显示为 HPE Moonshot Machine Manager。

- 如果您想再次安装 Citrix 管理的 HPE Moonshot 插件，请执行以下操作：

  a. 安装 `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin.msi`。`E:\` 是 ISO。

  b. 以管理员身份打开 PowerShell 并运行以下命令以注册 Citrix 管理的 HPE Moonshot 插件：

  ```
  C:\Program Files\Common Files\Citrix\HCLPlugins> .
  \RegisterPlugins.exe -pluginsroot .\CitrixMachineCreation\v1.0.0.0\
  ```

c. 插件注册成功后，从任务管理器重新启动以下服务：

   a. CitrixBrokerService

   b. CitrixHostService

   c. CitrixMachineCreationService

1. 运行 `Get-HypHypervisorPlugins` 以检查插件是否安装在 Delivery Controller 上。输出中的 DisplayName 字段必须显示为 HPE Moonshot。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关在 HPE Moonshot 中创建和管理连接的信息，请参阅 连接到 HPE Moonshot

更多信息

- 创建和管理连接与资源
- 创建计算机目录

Microsoft Azure 资源管理器 云环境

在 Citrix Virtual Apps and Desktops™ 部署中使用 Microsoft Azure Resource Manager 预配虚拟机时，请熟悉以下内容：

- 微软 Entra ID: `<https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/>`
- 同意框架: `<https://docs.microsoft.com/zh-cn/azure/active-directory/manage-apps/plan-an-application-integration>`
- 服务主体: `<https://docs.microsoft.com/zh-cn/azure/active-directory/develop/app-objects-and-service-principals/>`

要设置 Microsoft Azure Resource Manager，请参阅准备安装。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点

- 有关在 Azure 环境中创建和管理连接的信息，请参阅连接到 Microsoft Azure

更多信息

- 创建和管理连接与资源
- 创建计算机目录
- CTX219211：设置微软 Microsoft Entra 帐户
- CTX219243: 授予 XenApp 和 XenDesktop 访问您的 Azure 订阅的权限
- CTX219271: 使用站点到站点 VPN 部署混合云

微软系统中心配置管理器环境

使用 Microsoft System Center Configuration Manager (Configuration Manager) 管理应用程序和桌面访问的站点可以通过以下选项将该用途扩展到 Citrix Virtual Apps and Desktops™：

- 使用 SCCM 安装 VDA。
- **Configuration Manager Wake Proxy 功能：** Remote PC Access 的 Wake on LAN 功能受 Configuration Manager 支持。有关详细信息，请参阅局域网唤醒 - SCCM 集成。
- **Citrix Virtual Apps and Desktops 属性：** 属性 使您能够识别 Citrix Virtual Desktops™，以便通过 Configuration Manager 进行管理。（在某些版本中，Configuration Manager 使用 Citrix Virtual Apps and Desktops 的旧名称：XenApp and XenDesktop。）

属性

Microsoft System Center Configuration Manager 可使用属性来管理虚拟桌面。

Configuration Manager 中显示的布尔属性显示为 `1` 或 `0`，而不是 true 或 false。

这些属性适用于 `Citrix_virtualDesktopInfo` 类中的 `Root\Citrix\DesktopInformation` 命名空间。属性名称来自 Windows Management Instrumentation (WMI) 提供程序。

属性	描述
`AssignmentType`	设置 IsAssigned 的值。有效值为：`ClientIP`、`ClientName`、`None` 和 `User`（将 `IsAssigned` 设置为 `True`）
`BrokerSiteName`	返回与 `HostIdentifier` 相同的值
`DesktopCatalogName`	与桌面关联的计算机目录。

属性	描述
`DesktopGroupName`	与桌面关联的交付组。
`HostIdentifier`	返回与 `BrokerSiteName` 相同的值。
`IsAssigned`	`True` 用于将桌面分配给用户，设置为 `False` 以用于随机桌面
`IsMasterImage`	允许对环境做出决策。例如，在映像上而不是在预配的计算机上安装应用程序。有效值为：`True` 在用作映像的 VM 上。此值在安装期间根据选择进行设置，或者在从该映像预配的 VM 上清除。
`IsVirtualMachine`	`True` 用于虚拟机，`false` 用于物理机。
`OSChangesPersist`	如果桌面操作系统映像在每次重新启动时都重置为干净状态，则为 `False`；否则为 `true`。
`PersistentDataLocation`	Configuration Manager 存储持久数据的位置。用户无法访问此位置。
`BrokerSiteName`, `DesktopCatalogName`, `DesktopGroupName`, `HostIdentifier`	在桌面向控制器注册时确定。对于尚未完全注册的桌面，它们为空。

要收集属性，请在 Configuration Manager 中运行硬件清单。要查看属性，请使用 Configuration Manager 资源管理器。在这些情况下，名称包含空格或与属性名称略有不同。例如，`BrokerSiteName` 显示为 `Broker Site Name`。

- 配置 Configuration Manager 以从 Citrix VDA 收集 Citrix WMI 属性
- 使用 Citrix WMI 属性创建基于查询的设备集合
- 基于 Citrix WMI 属性创建全局条件
- 使用全局条件定义应用程序部署类型要求

您还可以在 `Root\ccm_vdi` 命名空间中的 Microsoft 类 `CCM_DesktopMachine` 中使用 Microsoft 属性。有关详细信息，请参阅 Microsoft 文档。

Microsoft System Center 虚拟机管理器 虚拟化环境

如果您使用 Hyper-V 和 Microsoft System Center Virtual Machine Manager (VMM) 来提供虚拟机，请遵循此指导。

此版本支持 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/system-requirements.html) 中列出的 VMM 版本。

> **注意：**
>
> 不支持混合 Hyper-V 群集（包含运行不同 Hyper-V 版本的服务器）。
>
> 您可以使用 Citrix Provisioning（以前称为 Provisioning Services）和 Machine Creation Services™ 来预配：

- 第 1 代支持的桌面或服务器操作系统 VM。
- 第 2 代支持的桌面或服务器操作系统 VM，包括安全启动支持。

安装和配置管理程序

> **重要提示：**
>
> 所有 Delivery Controller 必须与 VMM 服务器位于同一林中。

1. 在服务器上安装 Microsoft Hyper-V 服务器和 VMM。
2. 在所有 Controller 上安装 System Center Virtual Machine Manager 控制台。控制台版本必须与管理服务器版本匹配。尽管较早的控制台可以连接到管理服务器，但如果版本不同，则预配 VDA 将失败。
3. 验证以下帐户信息：

   您在 Studio 中指定主机时使用的帐户是相关 Hyper-V 计算机的 VMM 管理员或 VMM 委派管理员。如果此帐户在 VMM 中仅具有委派管理员角色，则在主机创建过程中，存储数据不会在 Studio 中列出。

   用于 Studio 集成的用户帐户还必须是每个 Hyper-V 服务器上管理员本地安全组的成员。此配置支持 VM 生命周期管理，例如 VM 创建、更新和删除。

   不支持在运行 Hyper-V 的服务器上安装 Controller。

在大型部署中，如果单个 SCVMM 管理不同数据中心中的多个群集，则可以限制委派管理员的主机组范围。

要限制主机组范围，请在 Microsoft System Center Virtual Machine Manager (VMM) 控制台中使用委派管理员角色：

1. 在“**创建用户角色向导**”中，选择“Fabric Administrator (Delegated Administrator)”作为用户角色。
2. 在“**成员**”中，添加您要在 Active Directory 中用作委派管理员的用户帐户。
3. 在 **范围** 中，选择您希望委派管理员访问的主机组。
4. 使用委派管理员用户凭据创建新的 **运行身份帐户**。稍后使用这些凭据创建管理程序连接。请勿使用主管理员角色帐户。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关在 SCVMM 中创建和管理连接的信息，请参阅连接到 Microsoft System Center Virtual Machine Manager

更多信息

- 创建和管理连接与资源
- 创建计算机目录

Nutanix 虚拟化环境

通过 Nutanix Prism Central 使用 Nutanix AHV Prism Central 主机连接将 Citrix Virtual Apps and Desktops 连接到 Nutanix AHV 集群。此主机连接：

- 支持包含电源管理和 MCS 预配的 VDA 的计算机目录。
- 使用模板版本在 AHV 群集之间启用 MCS 主映像共享。
- 简化主机连接上的证书信任。
- 无需在 Cloud Connector 上安装 Nutanix 插件。

请参阅 AHV 上的 Nutanix Prism Central。

您还可以使用 Nutanix Prism Element on AHV，将 Nutanix Acropolis 作为主机连接，在 Citrix Virtual Apps and Desktops 部署中提供 VM。但是，此设置过程需要在 Citrix Virtual Apps and Desktops 环境中安装并注册 Nutanix 插件。请参阅 Nutanix Prism Element on AHV。

有关 Nutanix Acropolis MCS 插件安装指南的更多信息，请参阅 Nutanix 支持门户。

适用于 AHV 的 Nutanix Prism Central

Citrix 开发并维护了一个插件，用于将 Citrix Virtual Apps and Desktops 与 Nutanix Prism Central on AHV 集成。此插件已与 Citrix Delivery Controllers 集成，无需单独安装插件。

Nutanix AHV Prism Central 插件已预安装在 Citrix 管理的 Delivery Controllers 上，无需在 Delivery Controllers 上单独安装。有关 Citrix 管理的组件和服务的信息，请参阅 技术概述。

先决条件

Nutanix AHV Prism Central 需要以下各项：

- Prism Central 版本 pc.2025.2 或更高版本。有关详细支持的 Prism Central 版本，请参阅 Citrix Virtual Apps and Desktops (MCS) 和 Citrix Provisioning (PVS) 支持的虚拟机管理程序。
- Nutanix AHV 集群的 AOS 7.3 或更高版本。
- Nutanix AHV 集群必须注册到 Prism Central。
- Citrix 管理员帐户必须具有足够的权限才能创建主机连接、计算机目录和交付组。有关详细信息，请参阅配置委派管理。
- Citrix Cloud™ 通过 Cloud Connector 与 Nutanix Prism Central 通信。因此，必须可以从 Cloud Connector 访问 Nutanix Prism Central 实例。

功能限制

由于 Nutanix Prism 和 API 的限制，针对 Windows VM 的电源操作（例如客户机重新启动或客户机关机）可能会失败。要解决此问题，我们建议按照文档 从 Prism 或 API 启动的电源操作可能对 Windows VM 失败 中的 Nutanix 说明在 VDA 上应用设置。

关键步骤

1. 设置您的 Nutanix 虚拟化环境。有关信息，请参阅 准备安装 或 激活未使用的域。
2. 创建到 Nutanix AHV Prism Central 的连接
3. 使用 Nutanix 计算机模板版本创建计算机目录。

适用于 AHV 的 Nutanix Prism Element

Nutanix Prism Element on AHV 要求在所有 Delivery Controllers 上安装 Nutanix 插件，Citrix Virtual Apps and Desktops 必须在这些 Delivery Controllers 上创建到具有 Nutanix 管理程序的资源位置的主机连接。

关键步骤

1. 安装并注册 Nutanix 插件。
2. 设置您的 Nutanix 虚拟化环境。有关信息，请参阅添加资源类型 或 激活未使用的域。
3. 创建连接。
4. 创建计算机目录。

安装并注册 Nutanix 插件

在所有 Cloud Connector 上完成安装和注册 Nutanix 插件的步骤。有关安装 Nutanix 插件的信息，请参阅 Nutanix 文档站点。

后续步骤

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关在 Nutanix 环境中创建和管理连接的信息，请参阅 连接到 Nutanix

更多信息

- (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections.html)
- (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-create.html)

Nutanix 云和合作伙伴解决方案

努坦尼克斯 AHV 棱镜中心

Citrix Virtual Apps and Desktops 支持以下云管理程序中的 Nutanix Cloud Clusters (NC2)，用于 Citrix 管理的 Nutanix AHV Prism Central 插件。

- 亚马逊云服务 (AWS)
- 微软 Azure

Nutanix 云集群

Citrix Virtual Apps and Desktops 支持 AWS 和 Azure 上的 Nutanix 云集群。Nutanix 集群简化了应用程序在私有云或多个公有云上的运行方式。

有关设置 NC2 的更多信息，请参阅：

- AWS 上的 Nutanix 云集群部署和用户指南
- Azure 上的 Nutanix 云集群部署和用户指南。

要求

您需要以下帐户才能使用 NC2：

- Nutanix 帐户
- 对于 AWS：具有以下权限的 AWS 帐户。
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess
- 对于 Azure：
  - 有效的“Azure 上的 NC2”许可证
  - 包含以下角色之一的 Azure 帐户：
    - 全局管理员
    - 云应用程序管理员
    - 应用程序管理员
    - 所有 权限

Azure 上的 NC2 权限

```
Microsoft.Compute/register/action

Microsoft.Compute/availabilitySets/write

Microsoft.Compute/availabilitySets/delete

Microsoft.Compute/disks/read

Microsoft.Compute/disks/write
```

```
Microsoft.Compute/disks/delete

Microsoft.Compute/locations/usages/read

Microsoft.Compute/availabilitySets/read

Microsoft.Compute/virtualMachines/*

Microsoft.Compute/snapshots/*

Microsoft.Compute/images/*

Microsoft.Network/register/action

Microsoft.Network/natGateways/*

Microsoft.Network/networkInterfaces/*

Microsoft.Network/networkSecurityGroups/*

Microsoft.Network/publicIPAddresses/*

Microsoft.Network/virtualNetworks/*

Microsoft.Network/locations/usages/read

Microsoft.Storage/register/action

Microsoft.Storage/checknameavailability/read Microsoft.Storage/locations/
checknameavailability/read Microsoft.Storage/locations/usages/read

Microsoft.Storage/storageAccounts/write

Microsoft.Storage/storageAccounts/read

Microsoft.Storage/storageAccounts/delete Microsoft.Storage/
storageAccounts/blobServices/containers/clearLegalHold/action
Microsoft.Storage/storageAccounts/blobServices/containers/delete
Microsoft.Storage/storageAccounts/blobServices/containers/lease/action

Microsoft.Storage/storageAccounts/blobServices/containers/ read
Microsoft.Storage/storageAccounts/blobServices/containers/ write
Microsoft.Storage/storageAccounts/blobServices/read Microsoft.Storage/
```

```
storageAccounts/blobServices/write Microsoft.Storage/storageAccounts/
listAccountSas/action Microsoft.Storage/storageAccounts/listkeys/action
Microsoft.Storage/storageAccounts/listServiceSas/action Microsoft.Storage/
storageAccounts/regeneratekey/action Microsoft.Storage/storageAccounts/
revokeUserDelegationKeys/action Microsoft.ResourceHealth/
AvailabilityStatuses/read Microsoft.ResourceHealth/events/read

Microsoft.ResourceHealth/AvailabilityStatuses/current/read

Microsoft.ManagedIdentity/userAssignedIdentities/* Microsoft.Resources/
subscriptions/locations/read Microsoft.Resources/subscriptions/
resourceGroups/read Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourcegroups/deployments/read

Microsoft.Resources/subscriptions/resourcegroups/deployments/write
Microsoft.Resources/subscriptions/resourcegroups/resources/read
Microsoft.Resources/subscriptions/tagNames/read Microsoft.Resources/
subscriptions/tagNames/write Microsoft.Resources/subscriptions/tagNames/
delete Microsoft.Resources/subscriptions/tagNames/tagValues/write
Microsoft.Resources/subscriptions/tagNames/tagValues/read
Microsoft.Resources/subscriptions/tagNames/tagValues/delete
Microsoft.Resources/tags/read

Microsoft.Resources/tags/write

Microsoft.Resources/tags/delete

Microsoft.Resources/providers/read

Microsoft.Compute/sshPublicKeys/read

Microsoft.Compute/sshPublicKeys/write

Microsoft.Compute/sshPublicKeys/delete Microsoft.Compute/sshPublicKeys/
generateKeyPair/action Microsoft.Nutanix/Interfaces/read

Microsoft.Nutanix/Interfaces/write

Microsoft.Nutanix/Interfaces/delete

Microsoft.Nutanix/Nodes/read

Microsoft.Nutanix/Nodes/write
```

```
Microsoft.Nutanix/Nodes/delete

Microsoft.Nutanix/register/action

Microsoft.Network/virtualHubs/*

Microsoft.Network/routeTables/read

Microsoft.Network/routeTables/write

Microsoft.Network/routeTables/delete

Microsoft.Network/routeTables/join/action

Microsoft.Network/routeTables/routes/read Microsoft.Network/routeTables/
routes/write Microsoft.Network/routeTables/routes/delete
Microsoft.CostManagement/query/read

Microsoft.CostManagement/views/read Microsoft.CostManagement/
externalSubscriptions/query/read Microsoft.CostManagement/
externalSubscriptions/dimensions/read Microsoft.CostManagement/
externalSubscriptions/read Microsoft.CostManagement/
externalBillingAccounts/forecast/read

Microsoft.CostManagement/externalBillingAccounts/read

Microsoft.CostManagement/externalBillingAccounts/query/read
Microsoft.CostManagement/externalBillingAccounts/ externalSubscriptions/
read Microsoft.CostManagement/externalSubscriptions/forecast/read
Microsoft.CostManagement/operations/read Microsoft.CostManagement/
forecast/read

Microsoft.Network/virtualWans/write

Microsoft.Network/virtualWans/read

Microsoft.Network/virtualWans/delete Microsoft.Network/virtualWans/
virtualHubs/read Microsoft.Network/virtualWans/join/action
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ read
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ write
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ delete
Microsoft.Network/privateEndpoints/pushPropertiesToResource/ action
Microsoft.Network/privateEndpoints/read
```

```
Microsoft.Network/privateEndpoints/write Microsoft.Network/
privateEndpoints/delete Microsoft.Network/privateDnsZones/read
Microsoft.Network/privateDnsZones/delete Microsoft.Network/
privateDnsZones/join/action Microsoft.Network/privateDnsZones/write
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/ write

Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/delete

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
deleteBlobVersion/action

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
action Microsoft.Storage/storageAccounts/blobServices/containers/ blobs/
read Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/
read

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/write
Microsoft.Storage/storageAccounts/blobServices/containers/ blobs/write
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
action Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
modifyPermissions/action
```

创建 Nutanix 集群

1. 登录您的 Nutanix 帐户。
2. 导航到 Nutanix 集群选项，然后单击 **启动**。**Nutanix 控制台** 将打开。有关详细信息：
   - 在 AWS 上开始使用 Nutanix 集群(https://next.nutanix.com/nutanix-cloud-clusters-nc2-149/get-started-with-nutanix-cluster-on-aws-39424)
   - Microsoft Azure 上的 Nutanix 云集群
3. 选择创建新 VPC 的选项。

集群创建完成后，检索 Nutanix Prism 的地址。

故障排除

集群创建过程可能会因以下错误而失败：

- **集群未能在给定时间内创建。正在删除集群**
- **主机 Nutanix 集群 - 节点 XXXXXXXXXXX: 实例 i-xxxxxxxxxxxxx: 禁用网络接口源/目标检查错误。**
- **主机 Nutanix 集群 - 节点 XXXXXXXXXXX: 无法获取实例 i-xxxxxxxxxxxxx 网络接口信息**

如果集群创建失败，请尝试在其他区域重新创建一个。在重试之前，请务必删除 Nutanix CloudFormation Stack (CFS)。

> **注意：**
>
> 除了其他资源，Nutanix CFS 还会创建：
>
> - 一个名为 Nutanix Cluster xxxxxxxxxxxx 10.0.0.0/16 的 VPC
> - 两个子网 10.0.128.0/24 和 10.0.129.0/24
> - 一个 Internet 网关
> - 一个 NAT 网关

检索 Prism 服务器地址

1. 将 NC2 群集注册到 Prism Central 服务器。请参阅 将群集注册到 Prism Central。
2. 使用 Prism Central 服务器的主机名或 IP 地址作为地址。

适用于 Nutanix Prism Element 的 NC2

Citrix Virtual Apps and Desktops 支持在以下云管理程序中使用 Nutanix Cloud Clusters (NC2)，以用于 Nutanix Prism Element 插件。

- 亚马逊云服务 (AWS)

AWS 上的 Nutanix 云集群

有关 AWS 上的 Nutanix 云群集的更多信息，请参阅 AWS 上的 Nutanix 云群集部署和用户指南。

> **提示：**
>
> 此支持提供与 Nutanix 本地群集相同的功能。仅支持单个群集，即 *Prism Element*。有关详细信息，请参阅 此处。

> 要在 AWS 上使用 NC2，您需要以下帐户：

- 一个 Nutanix 帐户
- 具有以下权限的 AWS 帐户：
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

有关创建 Nutanix 群集以及群集创建失败时的故障排除，请参阅 创建 Nutanix 群集 和 故障排除。

集群创建完成后，检索 **Nutanix Prism** 的地址：

检索 Prism 服务器地址

1. 转到 **Nutanix 控制台**。
2. 在控制台的右上角，将鼠标悬停在链接 **Launch Prism Element** 上并复制 URL。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关创建和管理 Nutanix 云和合作伙伴解决方案连接的信息，请参阅 连接到 Nutanix 云和合作伙伴解决方案

更多信息

- 创建和管理连接与资源
- 创建计算机目录

Oracle C3 虚拟化环境 (预览版)

Citrix Virtual Apps and Desktops 通过 Citrix 管理的 Oracle C3 插件在 Citrix Virtual Apps and Desktops 控制平面中管理您的 Oracle Compute Cloud@Customer (Oracle C3) 工作负载。借助此插件，您可以创建到 Oracle C3 的连接、创建目录，并对目录中的计算机进行电源管理。

> **注意：**

- 适用于 Citrix Virtual Apps and Desktops 2607 LTSR 的 Oracle C3 仅适用于拥有混合权利或通用许可证的客户。
- 独立的 Oracle C3 环境目前不支持。

先决条件

开始之前：

- 确保您的环境可以使用 Oracle C3 REST API。Oracle C3 的 `<system_name>.<domain name>` 是 API 连接所必需的。请参阅 使用 API 管理 Compute Cloud@Customer 资源。
- 准备用于 Oracle C3 身份验证的 IAM 配置 `.ini` 文件和私钥。确保区域设置为 `<system_name>.<domain_name>`。
- 如果 Oracle C3 受私有 CA 证书保护，请获取证书指纹，以便在连接设置期间进行信任验证。

主要步骤

1. 设置您的 Oracle C3 环境。
2. 创建到 Oracle C3 端点的连接。
3. 创建计算机目录。

> **注意：**
>
> 在创建目录之前，请确保一台或多台 Oracle C3 计算机可用，并且这些计算机上已安装 VDA。

4. 创建交付组。
5. 将所有剩余的非托管 Oracle C3 计算机迁移到托管目录或交付组中。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关创建和管理连接的信息，请参阅 连接到 Oracle C3

更多信息

- 创建和管理连接与资源
- 创建计算机目录

Red Hat OpenShift 虚拟化环境

Citrix® 通过 Citrix 管理的 OpenShift 插件管理您的 Red Hat OpenShift 工作负载。借助此插件，您可以为 OpenShift 群集创建托管连接和托管单元、创建目录以及对目录中的计算机进行电源管理。

支持以下配置：

- **网络选项：**
  - Linux 网桥和 OVS 网桥：可用于群集网络。
- **存储选项：**
  - 本地存储：支持用于节点上的持久性存储。
  - Red Hat OpenShift Data Foundation (ODF) 块存储：支持集群范围的分布式块存储。请参阅“配置 ODF 块存储”。

> **配置 ODF 块存储**
>
> Citrix 支持将 ODF 块存储 `(ocs-storagecluster-ceph-rbd)` 用于计算机目录。OpenShift 插件通过容器化数据导入器 (CDI) 预配 VM 磁盘，CDI 会为每个存储类发布一个 StorageProfile。在创建托管单元之前，请配置以下内容：
>
> - 安装 OpenShift Virtualization (CNV)，包括 CDI。确认存在与您的 ODF 块存储类同名的 StorageProfile。
> - 在该 StorageProfile 中，确认已设置 `accessModes` 和 `volumeMode`。
> - 确认已设置 `dataImportCronSourceFormat`。如果设置为 `snapshot`，还要确认已设置 `snapshotClass` 并且快照类使用与存储类相同的 CSI 驱动程序 — 对于 ODF 块存储，为 `openshift-storage.rbd.csi.ceph.com`。

  - **NetApp 存储：** 支持企业级外部存储集成。

主要步骤

- 设置您的 Red Hat OpenShift 环境。
- 创建与 OpenShift 群集的连接和资源。
- 创建计算机目录。
- 创建交付组。

设置您的 Red Hat OpenShift 环境

1. *创建 OpenShift 群集并获取群集 API 地址*：在 OpenShift 控制台中，设置群集后，导航到 **Home > Overview > Details**，然后获取群集 API 地址。
2. *创建服务帐户并使用 OpenShift 命令行界面 (CLI) (oc 命令) 获取服务帐户令牌*: 服务帐户令牌是与服务帐户关联的身份验证凭据。服务帐户用于向 OpenShift 验证 OpenShift 插件。每个服务帐户都与一个 命名空间 关联。
3. *配置服务帐户的权限*: 一个服务帐户可以有多个角色，每个角色都包含定义 OpenShift 插件可以在哪些资源上执行哪些操作的权限。角色通过 **角色绑定** 进行绑定，**角色绑定** 有两种类型：
    a. **集群范围的角色绑定**：用于从 OpenShift 接收事件。 命名空间绑定的角色绑定：用于管理特定命名空间中的 VM。
    b. **命名空间绑定的角色绑定**：用于管理特定命名空间中的 VM。
4. *创建命名空间（项目）*: OpenShift 中的命名空间是一个隔离环境，它将 VM 或网络等资源分组，从而实现更好的组织和访问控制。**命名空间** 是 Kubernetes 术语，而 **项目** 是 OpenShift 术语。从 OpenShift 插件的角度来看，它们是相同的。部署 VM 需要命名空间。使用 OpenShift 控制台或 OpenShift Container Platform CLI 创建命名空间。
5. *在目标命名空间下创建一个网络附加定义*: 网络附加定义指定了在 OpenShift 中运行的 VM 的网络配置。在 **网络 > 网络附加定义** 下，您可以查看每个命名空间的网络附加定义。
6. *配置存储类*: 存储类定义了 VM 存储的分配方式。在 **存储 > 存储类** 下，您可以配置并查看存储提供商列表。

创建服务帐户

1. 下载并解压 oc 命令行工具。
2. 使用您的登录 ID 访问 OpenShift 控制台。
3. 单击您的用户配置文件，然后单击 **复制登录命令**。
4. 单击 **显示令牌** 并复制令牌。
5. 使用 oc 命令行运行登录命令。示例：

```
.\oc.exe login --token=<token> --server=<server address>
```

6. 创建服务帐户。

   - 如果要在默认命名空间下创建服务帐户，请运行：

     ```
     .\oc.exe create sa <service account name>
     ```

   - 如果您想在自己的命名空间下创建服务帐户，请运行：

     ```
     .\oc.exe create sa <service account name> -n mynamespace
     ```

7. 为密钥创建 `YAML` 文件。示例：

   - 如果您在默认命名空间下创建服务帐户：

     ```
     apiVersion: v1

     kind: Secret

     metadata:

     name: service account name

     annotations:

     kubernetes.io/service-account.name: service account name

     type: kubernetes.io/service-account-token
     ```

   - 如果您在自己的命名空间下创建服务帐户：

     ```
     apiVersion: v1

     kind: Secret

     metadata:

     name: service account name
     ```

```
namespace: mynamespace

annotations:

kubernetes.io/service-account.name: service account name

 type: kubernetes.io/service-account-token
```

8. 应用 YAML。

```
.\oc.exe apply -f <yamlFile.yaml>
```

注意：

`oc` 描述了获取令牌的密钥。该令牌用作密码。

为服务帐户创建角色和角色绑定

通过集群范围的角色绑定，服务帐户拥有读取整个集群中所有 VM 事件的权限，从而允许 OpenShift 插件为所有与 VM 相关的事件维护一个事件监视器。 通过命名空间角色绑定，服务帐户拥有管理目标命名空间中 VM 的权限。 您可以使用脚本创建角色并将其绑定到服务帐户。请参阅 `<https://github.com/citrix/citrix-mcs-sdk-samples/tree/main/OpenShift/Hosting%20Connection/Role/>`。

下一步

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关创建和管理连接的信息，请参阅连接到 Red Hat OpenShift

更多信息

- 创建和管理连接和资源
- 创建计算机目录

VMware 虚拟化环境

如果您使用 VMware 提供虚拟机，请遵循此指南。

安装 vCenter Server 和相应的管理工具。（不支持 vSphere vCenter Linked Mode 操作。）

如果您计划使用 MCS，请勿禁用 vCenter Server 中的 Datastore Browser 功能（如 `<https://kb.vmware.com/s/article/2101567>` 中所述）。禁用此功能后，MCS 将无法正常工作。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关在 VMware 环境中创建和管理连接的信息，请参阅 连接到 VMware

更多信息

- 创建和管理连接与资源
- 创建计算机目录

VMware 云和合作伙伴解决方案

Citrix Virtual Apps and Desktops™ 支持以下 VMware 云和合作伙伴解决方案：

- Azure VMware 解决方案 (AVS)
- 谷歌云 VMware 引擎
- 在 Amazon Web Services (AWS) 上运行的 VMware Cloud

Azure VMware 解决方案 (AVS) 集成

Citrix Virtual Apps and Desktop 服务支持 AVS。AVS 提供包含由 Azure 基础架构创建的 vSphere 群集的云基础架构。利用 Citrix Virtual Apps and Desktop 服务使用 AVS 预配 VDA 工作负载，其方式与在本地环境中使用 vSphere 相同。

设置 AVS 群集

要使 Citrix Virtual Apps™ and Desktop 服务能够使用 AVS，请在 Azure 中执行以下步骤：

- 请求主机配额
- 注册 Microsoft.AVS 资源提供程序
- 网络清单

- 创建 Azure VMware Solution 私有云
- 访问 Azure VMware Solution 私有云
- 在 Azure 中为您的 VMware 私有云配置网络
- 配置适用于 Azure VMware Solution 的 DHCP
- 在 Azure VMware Solution 中添加网络段
- 验证 Azure VMware Solution 环境

为 AZURE 企业协议客户请求主机配额

在 Azure 门户的“**帮助 + 支持**”页面中，选择“**新建支持请求**”，并包含以下信息：

- 问题类型:技术
- 订阅:选择您的订阅
- 服务:所有服务 > Azure VMware Solution
- 资源:一般问题
- 摘要:需要容量
- 问题类型:容量管理问题
- 问题子类型:客户请求额外主机配额/容量

在支持票证的 **Description** 中，在 **Details** 选项卡中包含以下信息：

- POC 或生产
- 区域名称
- 主机数量
- 任何其他详细信息

> **注意：**

> AVS 最少需要三台主机，并建议您使用 N+1 主机冗余。

> 指定支持票证的详细信息后，选择 **Review + Create** 以将请求提交到 Azure。

注册 MICROSOFT.AVS 资源提供程序

请求主机配额后，注册资源提供程序：

1. 登录到 Azure 门户。

2. 在 Azure 门户菜单上，选择 **所有服务**。
3. 在 **所有服务** 菜单中，输入订阅，并选择 **订阅**。
4. 从订阅列表中选择订阅。
5. 选择 **资源提供程序** 并在搜索栏中输入 **Microsoft.AVS**。
6. 如果资源提供程序未注册，请选择 **注册**。

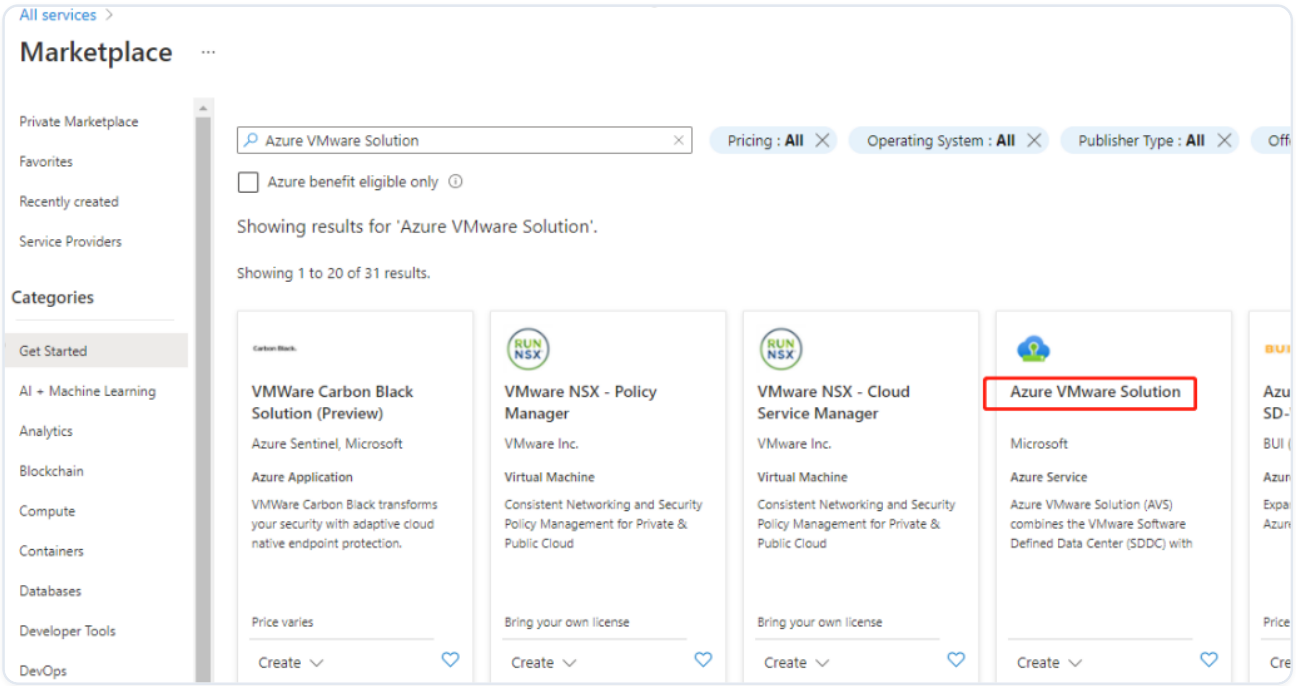
网络注意事项

AVS 提供需要特定网络地址范围和防火墙端口的网络服务。有关详细信息，请参阅 Azure VMware Solution 的网络规划清单。

创建 AZURE VMWARE SOLUTION 私有云

在考虑了环境的网络要求后，创建一个 ASV 私有云：

1. 登录 Azure 门户。
2. 选择 **创建新资源**。
3. 在 **搜索市场** 文本框中键入 *Azure VMware Solution*，然后从列表中选择 **Azure VMware Solution**。



图像

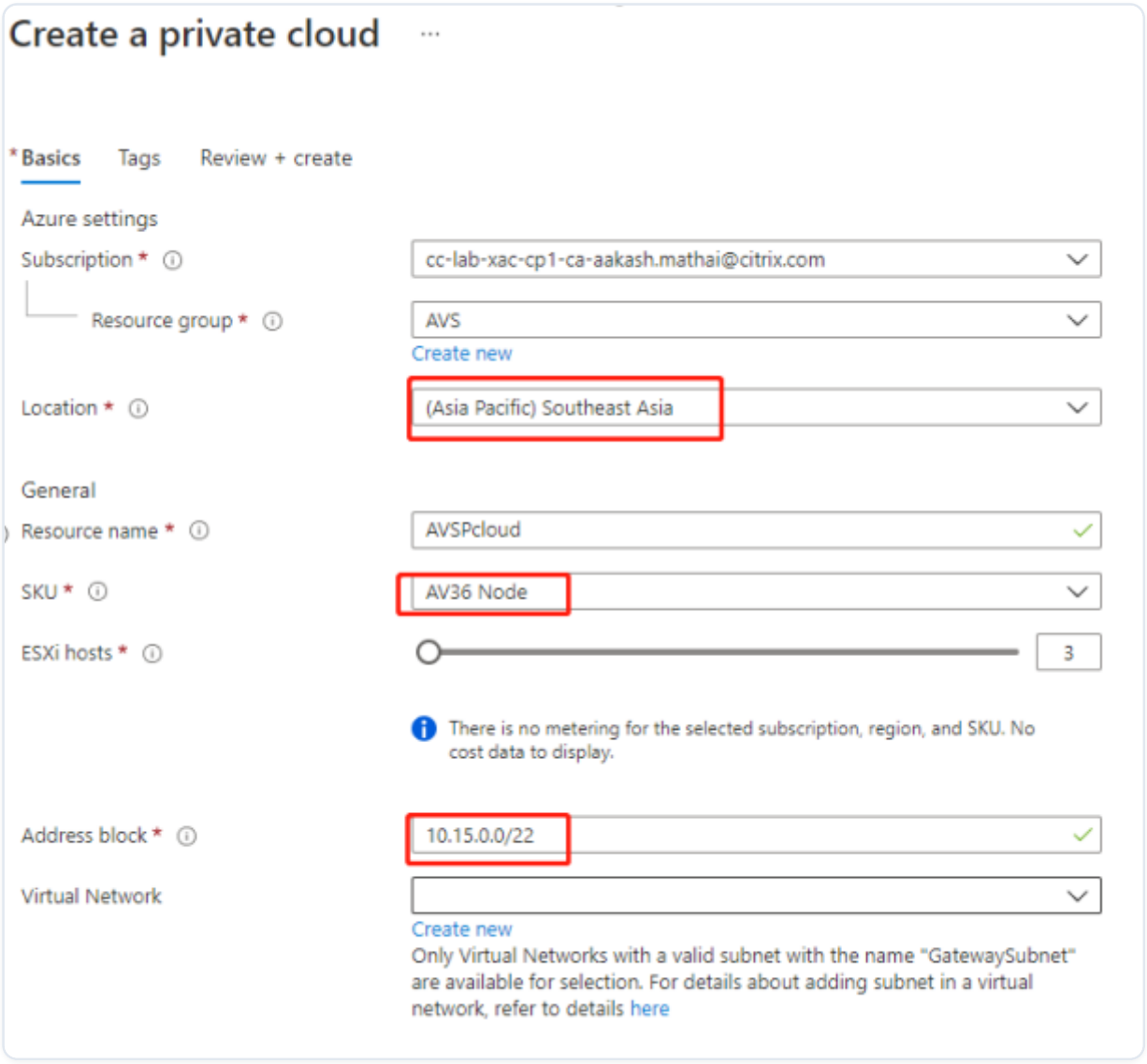
在 **Azure VMware Solution** 窗口中：

1. 选择 **创建**。
2. 单击**基本信息**选项卡。
3. 使用下表中的信息，输入字段的值：

字段	值
订阅	选择您计划用于部署的订阅。Azure 订阅中的所有资源将一起计费。
资源组	选择您的私有云的资源组。Azure 资源组是一个逻辑容器，Azure 资源部署和管理于其中。或者，您可以为您的私有云创建一个新的资源组。
位置	选择一个位置，例如美国东部。这是您在规划阶段定义的区域。
资源名称	提供您的 Azure VMware Solution 私有云的名称。
SKU	选择 AV36。
主机	显示为私有云集群分配的主机数量。默认值为 3，部署后可以增加或减少。
地址块	为私有云提供一个 IP 地址块。CIDR 代表私有云管理网络，将用于集群管理服务，例如 vCenter Server 和 NSX-T Manager。使用 /22 地址空间，例如 10.175.0.0/22。该地址应是唯一的，并且不与其他的 Azure 虚拟网络以及本地网络重叠。
虚拟网络	将其留空，因为 Azure VMware Solution ExpressRoute 线路是在部署后步骤中建立的。

在“**创建私有云**”屏幕中：

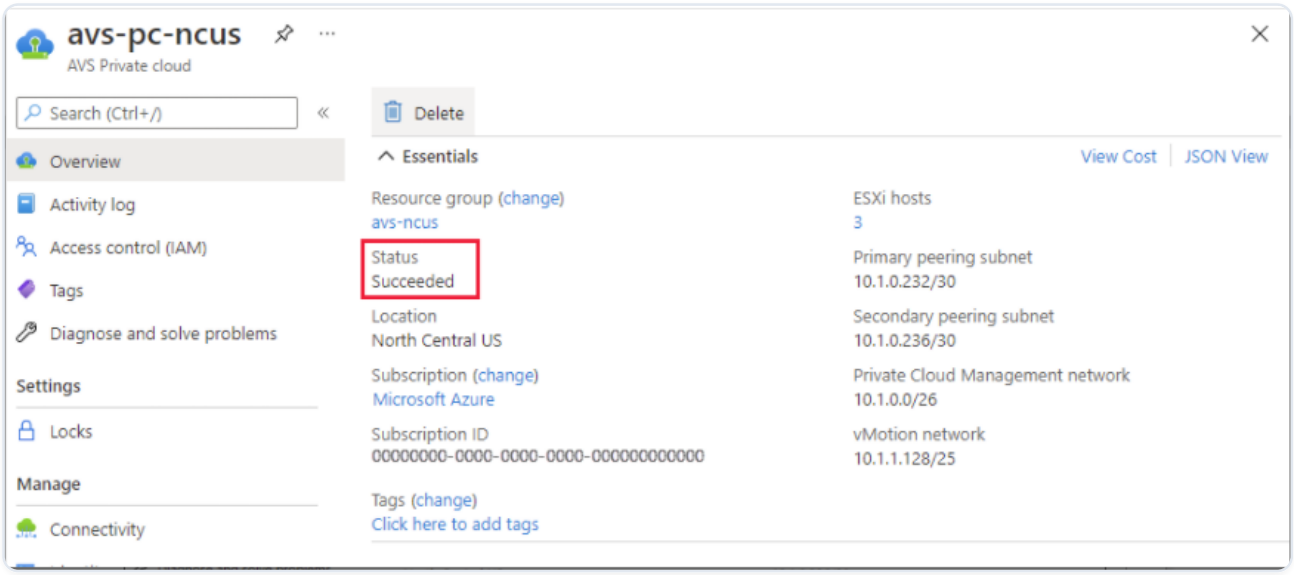
1. 在**位置**字段中，选择具有 AVS 的区域；资源组区域与 AVS 区域相同。
2. 在 **SKU** 字段中，选择 **AV36 Node**。
3. 在 **地址块** 字段中指定一个 IP 地址。例如，10.15.0.0/22。
4. 选择“**审查 + 创建**”。
5. 审查信息后，单击“**创建**”。



提示：

创建私有云可能需要 3-4 小时。向集群添加单个主机可能需要 30-45 分钟。

验证部署是否成功。导航到您创建的资源组并选择您的私有云。一旦 **状态** 为 **成功**，部署即完成。



访问 AZURE VMWARE SOLUTION 私有云

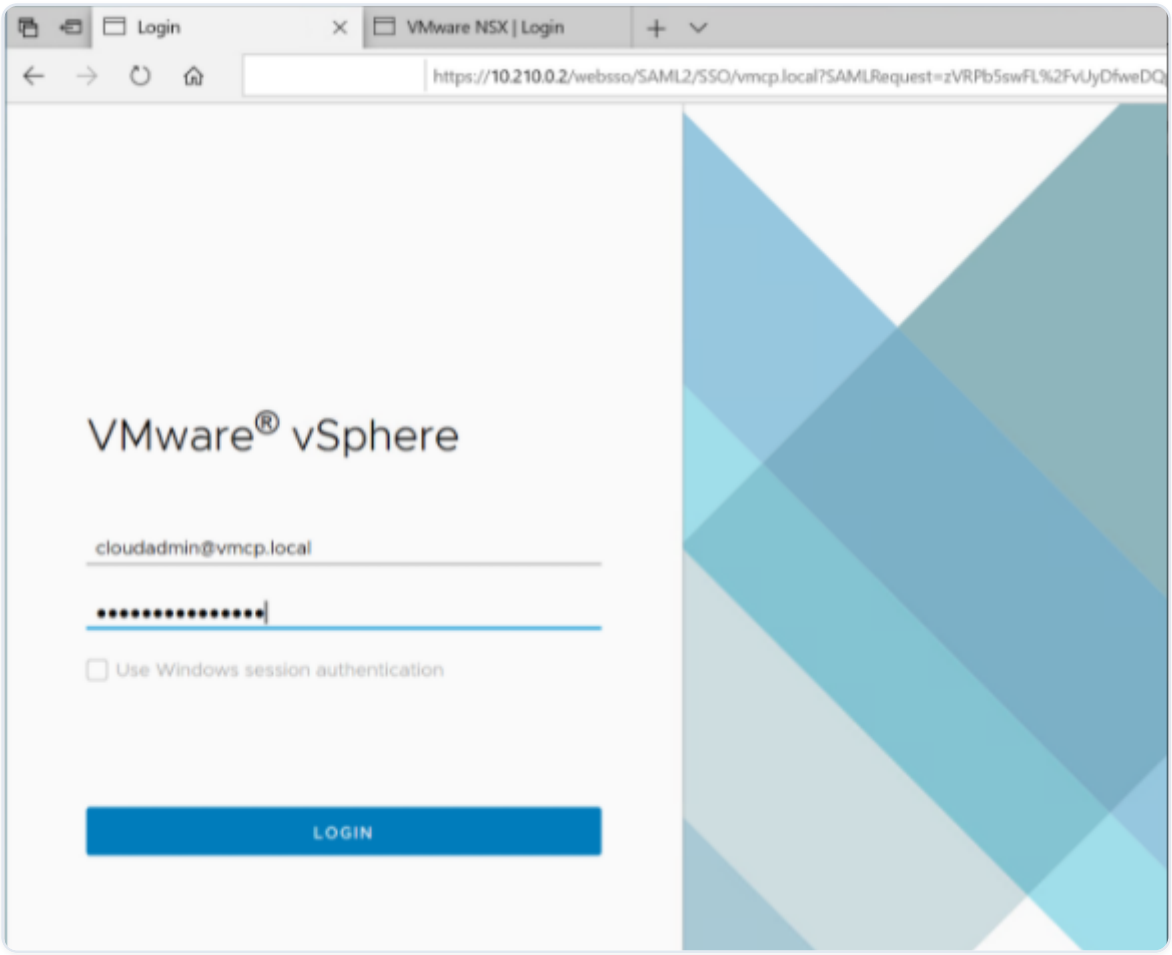
创建私有云后，创建 Windows VM 并连接到私有云的本地 vCenter。

创建新的 Windows 虚拟机

1. 在资源组中，选择 **+ 添加**，然后搜索并选择 **Microsoft Windows 10/2016/2019**。
2. 单击**创建**。
3. 输入所需信息，然后选择“**审查 + 创建**”。
4. 验证通过后，选择“**创建**”以开始虚拟机创建过程。

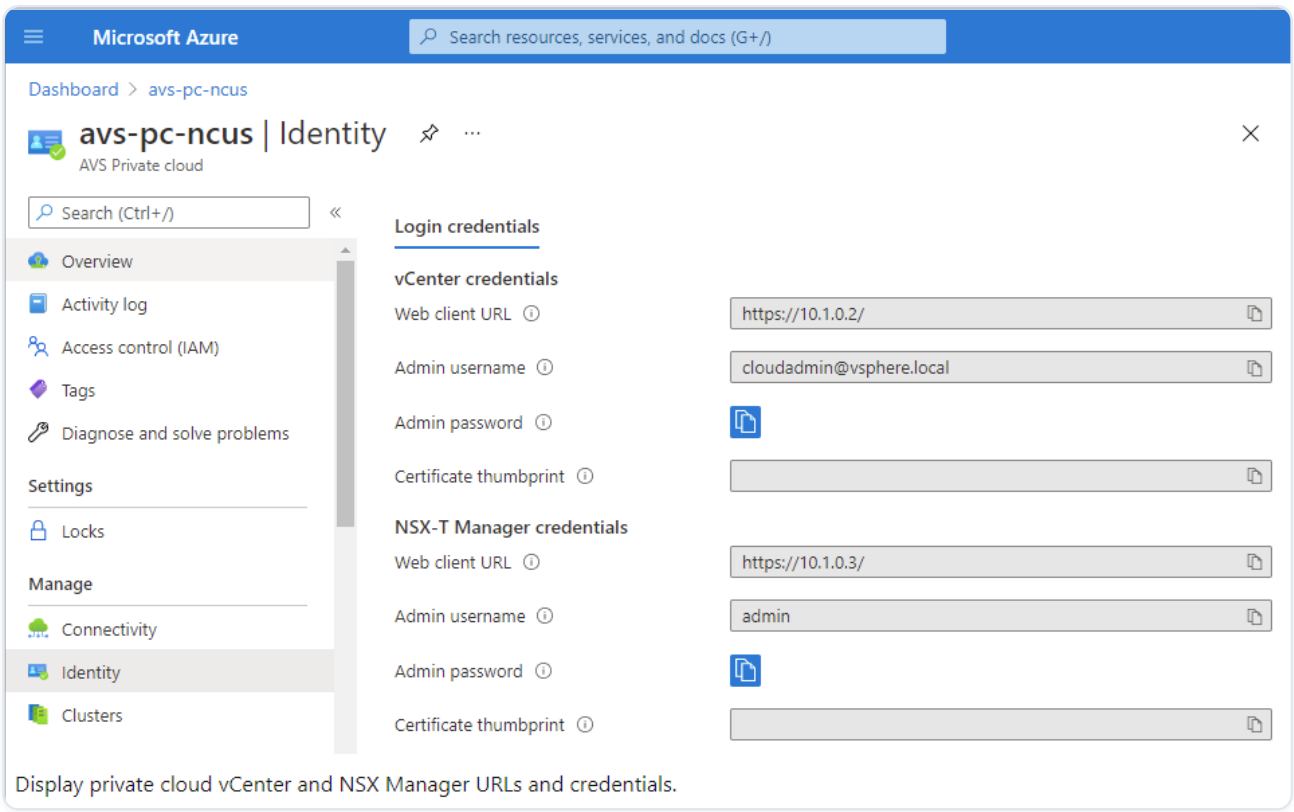
连接到私有云的本地 vCenter

1. 以云管理员身份登录 **vSphere Client with VMware vCenter SSO**。



2. 在 Azure 门户中，选择您的私有云，然后选择 **管理 > 身份**。

私有云 vCenter 和 NSX-T Manager 的 URL 和用户凭据显示如下：



确认 URL 和用户凭据后：

1. 导航到您在上一步中创建的 VM 并连接到该虚拟机。
2. 在 Windows VM 中，打开浏览器并在两个浏览器选项卡中导航到 vCenter 和 NSX-T Manager URL。在 vCenter 选项卡中，输入上一步中的 *cloudadmin@vmcp.local* 用户凭据。

在 AZURE 中为您的 VMWARE 私有云配置网络

访问 ASV 私有云后，通过创建虚拟网络和网关来配置网络。
创建虚拟网络

1. 登录 Azure 门户。
2. 导航到之前创建的资源组。
3. 选择 **+ 添加** 以定义新资源。
4. 在 **搜索市场** 文本框中，键入 *虚拟网络*。找到虚拟网络资源并选择它。
5. 在**虚拟网络**页面上，选择**创建**以设置您的私有云的虚拟网络。
6. 在**创建虚拟网络**页面上，输入您的虚拟网络的详细信息。
7. 在**基本信息**选项卡上，输入虚拟网络的名称，选择相应的区域，然后单击**下一步：IP 地址。**
8. 在**IP 地址**选项卡上，在 IPv4 地址空间下，输入之前创建的地址。

> **重要提示：**

> 使用的地址不得与您创建私有云时使用的地址空间重叠。

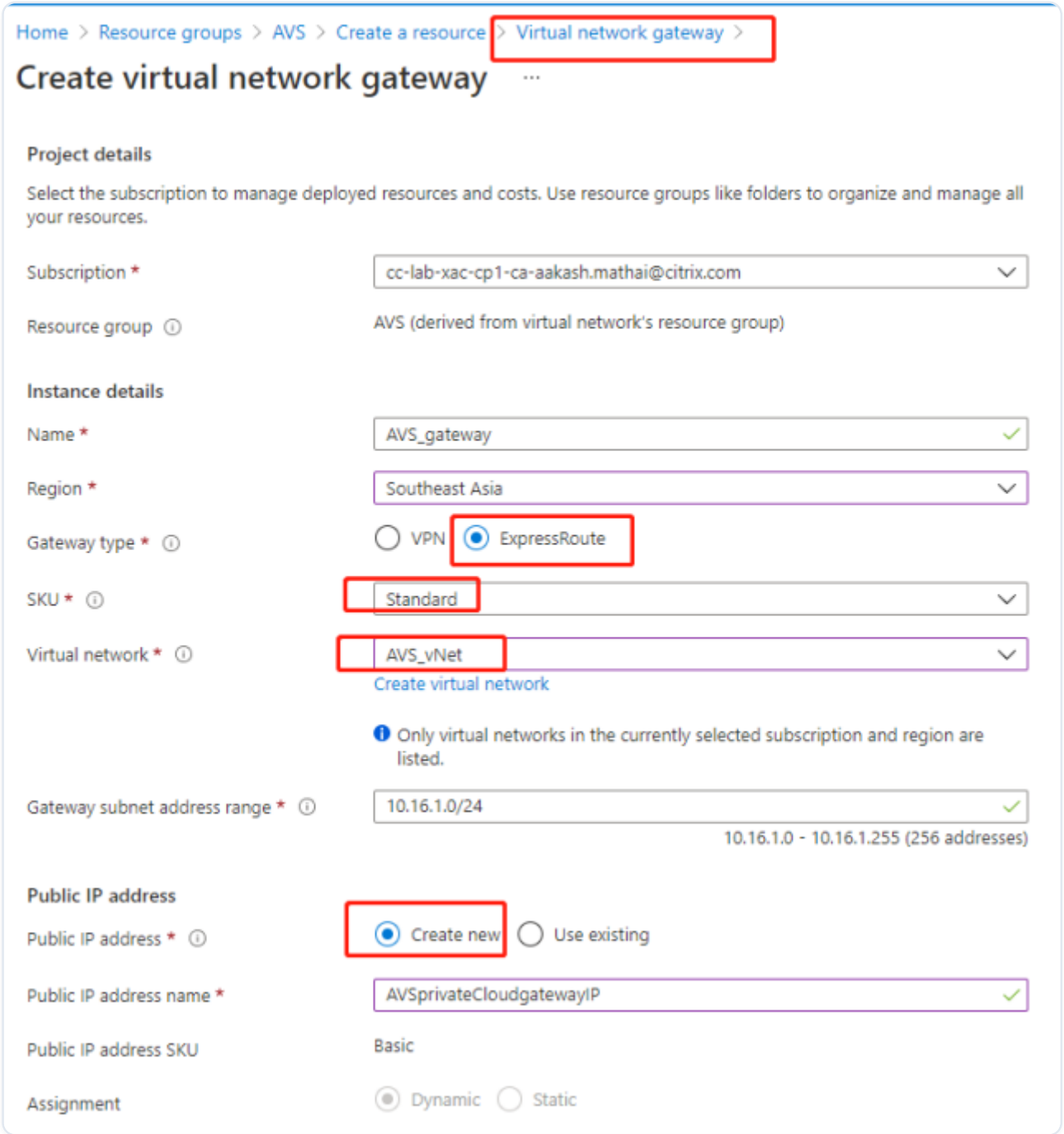
> 输入地址空间后：

1. 选择**+ 添加子网**。
2. 在**添加子网**页面上，为子网指定名称和适当的地址范围。
3. 单击**添加。**
4. 选择**审核 + 创建**。
5. 验证信息并单击**创建**。部署完成后，虚拟网络将显示在资源组中。

创建虚拟网络网关
创建虚拟网络后，创建虚拟网络网关。

1. 在您的资源组中，选择**+ 添加**以添加新资源。
2. 在“**搜索市场**”文本框中，键入 *虚拟网络网关*。找到虚拟网络资源并选择它。

3. 在“**虚拟网络网关**”页面上，单击“**创建**”。
4. 在“**创建虚拟网络网关**”页面上的“**基本信息**”选项卡中，为字段提供值。
5. 单击“**审查 + 创建**”。



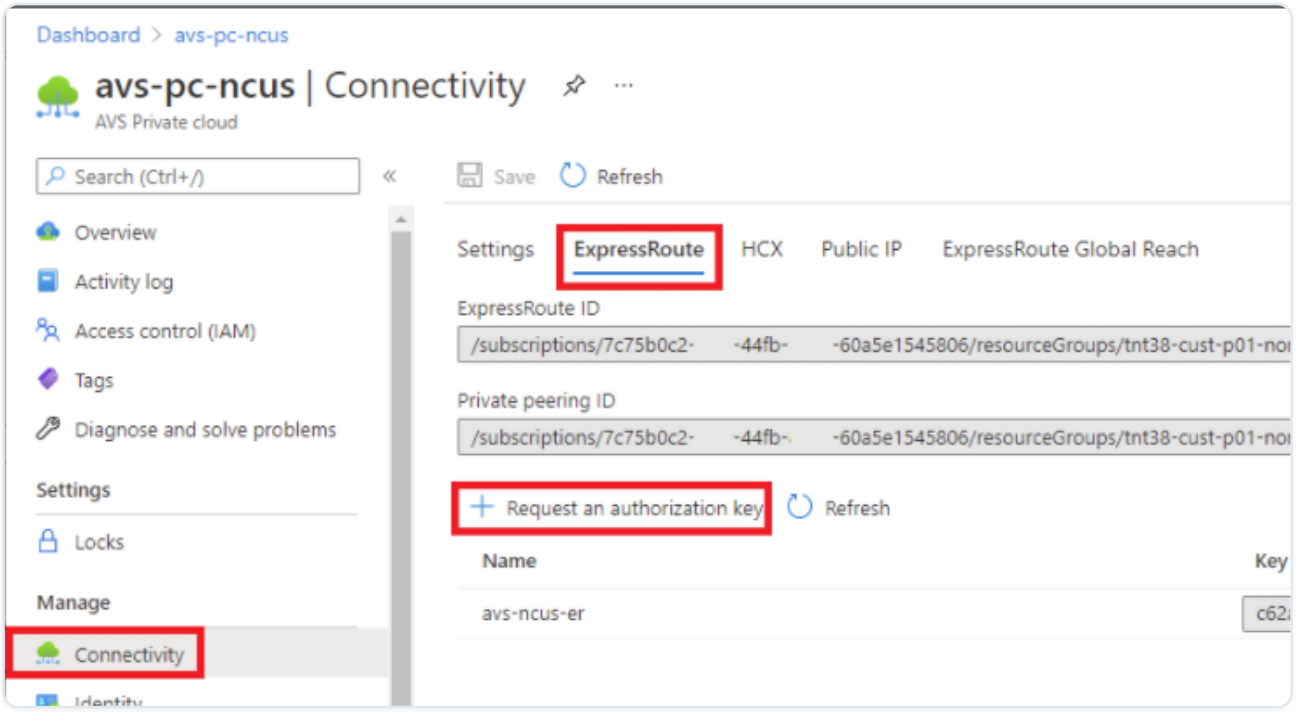
审查虚拟网络网关配置后，单击“**创建**”以部署虚拟网络网关。 部署完成后，将您的 **ExpressRoute** 连接连接到包含 Azure AVS 私有云的虚拟网络网关。

将 EXPRESSROUTE 连接到虚拟网络网关

部署虚拟网络网关后，在其与 Azure AVS 私有云之间添加连接：

1. 请求 ExpressRoute 授权密钥。

2. 在 Azure 门户中，导航到“**Azure VMware Solution 私有云**”。选择“**管理 > 连接 > ExpressRoute**”，然后选择“**+ 请求授权密钥**”。



请求授权密钥后：

1. 输入密钥名称，然后单击“**创建**”。创建密钥可能需要大约 30 秒。创建后，新密钥将显示在私有云的授权密钥列表中。
2. 复制 **授权密钥** 和 **ExpressRoute ID**。您将需要它们来完成对等过程。授权密钥会在一段时间后消失，因此请在它出现后立即复制。
3. 导航到您计划使用的**虚拟网络网关**，并选择“**连接 > + 添加**”。
4. 在“**添加连接**”页面上，提供字段值，然后选择“**确定**”。

Azure ASV 添加连接(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-avs-add-connection-v2.png)

连接已在您的 ExpressRoute 线路和您的虚拟网络之间建立：

Azure ASV 连接成功(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-avs-connection-succeeded.png)

配置适用于 AZURE VMWARE SOLUTION 的 DHCP

将 ExpressRoute 连接到虚拟网关后，配置 DHCP。
使用 NSX-T 托管您的 DHCP 服务器
在 NSX-T Manager 中：

1. 选择“**网络 > DHCP**”，然后选择“**添加服务器**”。

2. 对于“**服务器类型**”，选择“**DHCP**”，提供服务器名称和 IP 地址。
3. 单击 **保存**。
4. 选择“**第 1 层网关**”，选择第 1 层网关上的垂直省略号，然后选择“**编辑**”。
5. 选择“**未设置 IP 分配**”以添加子网。
6. 对于“**类型**”，选择“**DHCP 本地服务器**”。
7. 对于“**DHCP 服务器**”，选择“**默认 DHCP**”，然后单击“**保存**”。
8. 再次点击“**保存**”，然后选择“**关闭编辑**”。

Azure ASV 添加 NSX-T 服务器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-avs-nsx-t-add-server.png)

在 AZURE VMWARE SOLUTION 中添加网络段

设置 DHCP 后，添加网络段。

要添加网络分段，请在 NSX-T Manager 中选择“**网络 > 分段**”，然后点击“**添加分段**”。

Azure ASV 添加 NSX-T 分段(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-avs-nsx-t-add-segment.png)

在“**分段配置文件**”屏幕中：

1. 输入该分段的**名称**。
2. 选择“**Tier-1 网关 (TNTxx-T1)**”作为“**连接的网关**”，并将“**类型**”保留为“**灵活**”。
3. 选择预配置的覆盖**传输区域 (TNTxx-OVERLAY-TZ)**。
4. 点击“**设置子网**”。

Azure ASV 添加 NSX-T 分段配置文件(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-avs-nsx-t-segment-profiles.png)

在“**子网**”部分中：

1. 输入网关 IP 地址。
2. 选择“**添加**”。

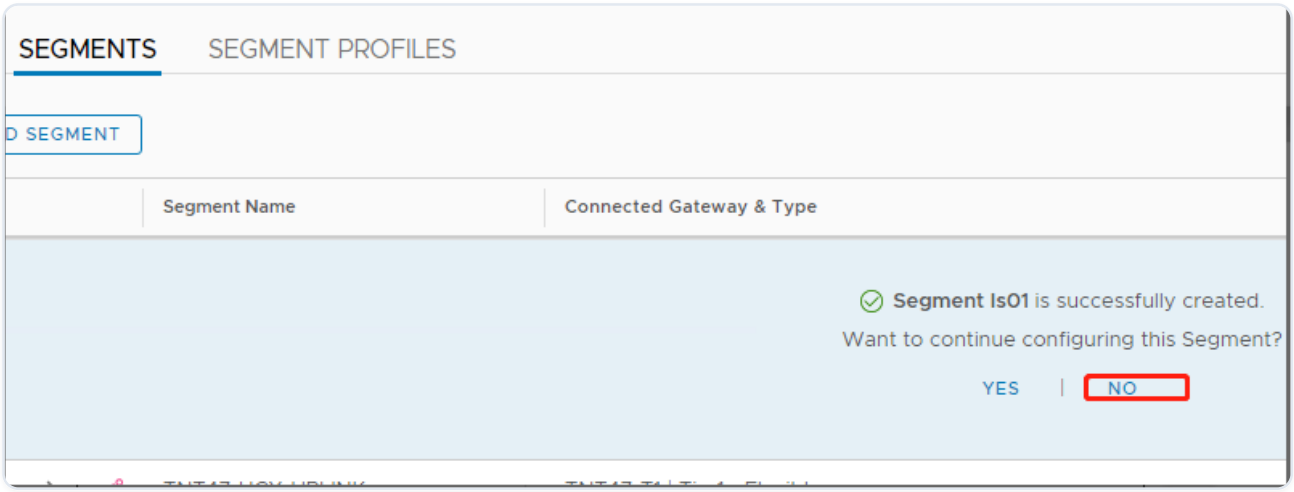
> **重要提示：**

> 此分段 IP 地址必须属于 Azure 网关 IP 地址，10.15.0.0/22。

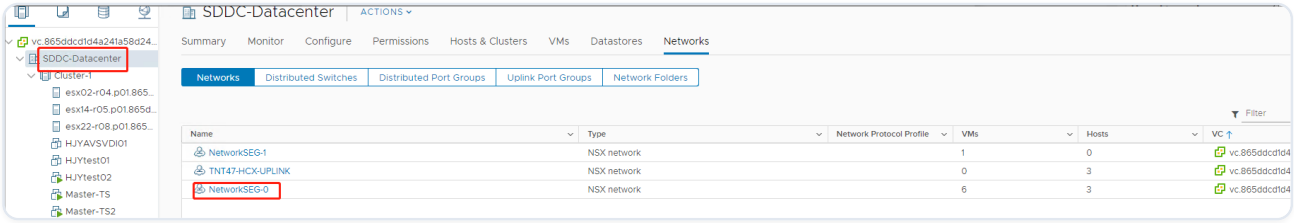
> DHCP 范围应属于网段 IP 地址：



选择 **否** 以拒绝继续配置分段的选项：



在 vCenter 中，选择 **网络 > SDDC-数据中心**：

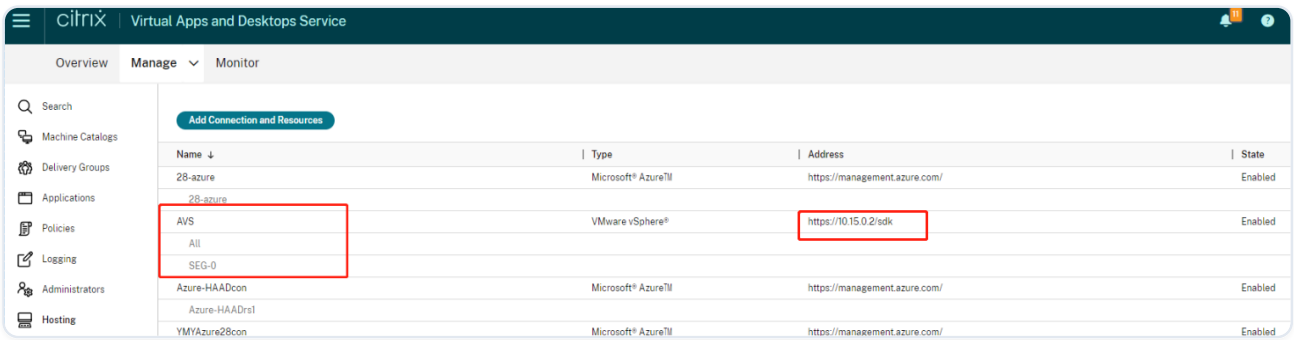


验证 AZURE AVS 环境

在 Azure 资源组中设置直接连接和连接器：

Azure ASV ASV 验证连接(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-avs-verify-connection-create-dc-v2.png)

使用 vCenter 凭据验证连接：



谷歌云 VMware 引擎

Citrix Virtual Apps and Desktops 允许您将基于 VMware 的本地 Citrix 工作负载迁移到 Google Cloud VMware Engine。

配置 Google Cloud VMware 引擎

以下过程介绍了如何在 Google Cloud VMware 引擎上获取和设置集群。

访问 VMWARE ENGINE 门户

1. 在 **Google Cloud Console** 中，单击导航菜单。
2. 在 **计算** 部分中，单击 **VMware Engine** 以在新浏览器选项卡中打开 VMware Engine。

创建第一个私有云的要求

您必须拥有 Google Cloud VMware Engine 的访问权限、可用的 VMware Engine 节点配额以及适当的 IAM 角色。在继续创建私有云之前，请准备以下要求：

1. 请求 API 访问权限和节点配额。有关详细信息，请参阅 请求 API 访问权限和配额。
2. 记下您要用于 VMware 管理设备和 HCX 部署网络的地址范围。有关详细信息，请参阅 网络要求。
3. 获取 VMware Engine Service 管理员 IAM 角色。

创建您的第一个私有云

1. 访问 VMware Engine 门户。
2. 在 VMware Engine 主页上，单击 **创建私有云**。将列出托管位置和硬件节点类型。
3. 选择私有云的节点数。至少需要三个节点。
4. 为 VMware 管理网络输入一个无类别域间路由 (CIDR) 范围。
5. 为 HCX 部署网络输入一个 CIDR 范围。

> **重要提示：**
>
> CIDR 范围不得与您的任何本地或云子网重叠。CIDR 范围必须为 /27 或更高。

6. 选择 **审核并创建**。
7. 查看设置。要更改任何设置，请单击 **Back**。
8. 单击 **Create** 开始创建私有云。

当 VMware Engine 创建您的新私有云时，它会部署多个 VMware 组件并为私有云中的集群设置初始 Autoscale™ 策略。私有云创建可能需要 30 分钟到 2 小时。预配完成后，您会收到一封电子邮件。

设置 谷歌云 VMWARE ENGINE VPN 网关

要与 Google Cloud VMware Engine 建立初始连接，您可以使用 VPN 网关。这是一个基于 OpenVPN 的客户端 VPN，您可以使用它连接到您的 VMware 软件定义数据中心 (SDDC) vCenter 并执行任何所需的初始配置。

在部署 VPN 网关之前，请配置部署 SDDC 的区域的 **Edge Services** 范围。为此：

1. 登录 **Google Cloud VMware Engine** 门户，然后转到 **Network > Regional Settings**。单击 **Add Region**。
2. 选择部署 SDDC 的区域，并启用 **Internet Access** 和 **Public IP Service**。
3. 提供规划期间记录的 Edge Services 范围，然后单击 **Submit**。启用这些服务需要 10-15 分钟。

   完成后，Edge Services 在“区域设置”页面上显示为 **Enabled**。启用这些设置允许将公共 IP 分配给您的 SDDC，这是部署 VPN 网关的要求。

要部署 VPN 网关：

1. 在 **Google Cloud VMware Engine** 门户中，转到 **网络 > VPN 网关**。单击 **创建新的 VPN 网关**。
2. 提供 VPN 网关的名称以及规划期间保留的客户端子网。单击“**下一步**”。
3. 选择要授予 VPN 访问权限的用户。单击“**下一步**”。
4. 指定必须通过 VPN 访问的网络。单击“**下一步**”。
5. 将显示摘要屏幕。验证选择，然后单击“**提交**”以创建 VPN 网关。将显示 VPN 网关页面，其中新 VPN 网关的状态为“**正在创建**”。
6. 状态变为“**运行中**”后，单击新的 VPN 网关。
7. 单击“**下载我的 VPN 配置**”以下载包含 VPN 网关预配置 OpenVPN 配置文件的 ZIP 文件。提供了通过 UDP/1194 和 TCP/443 连接的配置文件。选择您的首选项并将其导入 Open VPN，然后连接。
8. 转到“**资源**”并选择您的 SDDC。

连接 VPN

1. 通过 VPN 网关设置在本地网络和私有云之间建立点到站点连接。请参阅 设置 Google Cloud VMware Engine VPN 网关。
2. 上传在 设置 Google Cloud VMware Engine VPN 网关 中下载的 VPN 配置。

3. 导入到您的 VPN 客户端，例如 OpenVPN Connect。

有关详细信息，请参阅 使用 VPN 连接。

创建第一个子网

从 VMware Engine 门户访问 NSX-T Manager
创建子网的过程在 NSX-T 中进行，您可以通过 VMware Engine 访问 NSX-T。请执行以下操作以访问 NSX-T Manager。

1. 登录到 **Google Cloud VMware Engine** 门户。
2. 从主导航中，转到 **资源**。
3. 单击与要创建子网的私有云对应的 **私有云名称**。
4. 在私有云的详细信息页面上，单击 **vSphere Management Network** 选项卡。
5. 单击与 NSX-T Manager 对应的 **FQDN**。
6. 出现提示时，输入您的登录凭据。如果您已设置 vIDM 并将其连接到身份源（例如 Active Directory），请改用您的身份源凭据。

> **提醒：**
>
> 您可以从私有云详细信息页面检索生成的凭据。

为子网设置 DHCP 服务
在创建子网之前，请设置 DHCP 服务：

在 NSX-T Manager 中：

1. 转到 **网络 > DHCP**。网络仪表板显示 DHCP 服务创建了一个 Tier-0 和一个 Tier-1 网关。
2. 要开始预配 DHCP 服务器，请单击 **添加服务器**。
3. 为 **服务器类型** 选择 **DHCP**，提供服务器名称和 IP 地址。
4. 单击 **保存** 以创建 DHCP 服务。

执行以下操作以将此 DHCP 服务附加到相关的 Tier-1 网关。DHCP 服务已预配了一个默认的 Tier-1 网关：

1. 选择 **Tier 1 网关**，选择 Tier-1 网关上的垂直省略号，然后选择 **编辑**。
2. 在 **IP 地址管理** 字段中，选择 **未设置 IP 分配**。
3. 为 **类型** 选择 **DHCP 本地服务器**。

4. 为 **DHCP 服务器** 选择您创建的 DHCP 服务器。
5. 单击 **保存**。
6. 单击 **关闭编辑**。

您现在可以在 NSX-T 中创建网络分段。有关 NSX-T 中 DHCP 的更多信息，请参阅 VMware DHCP 文档。

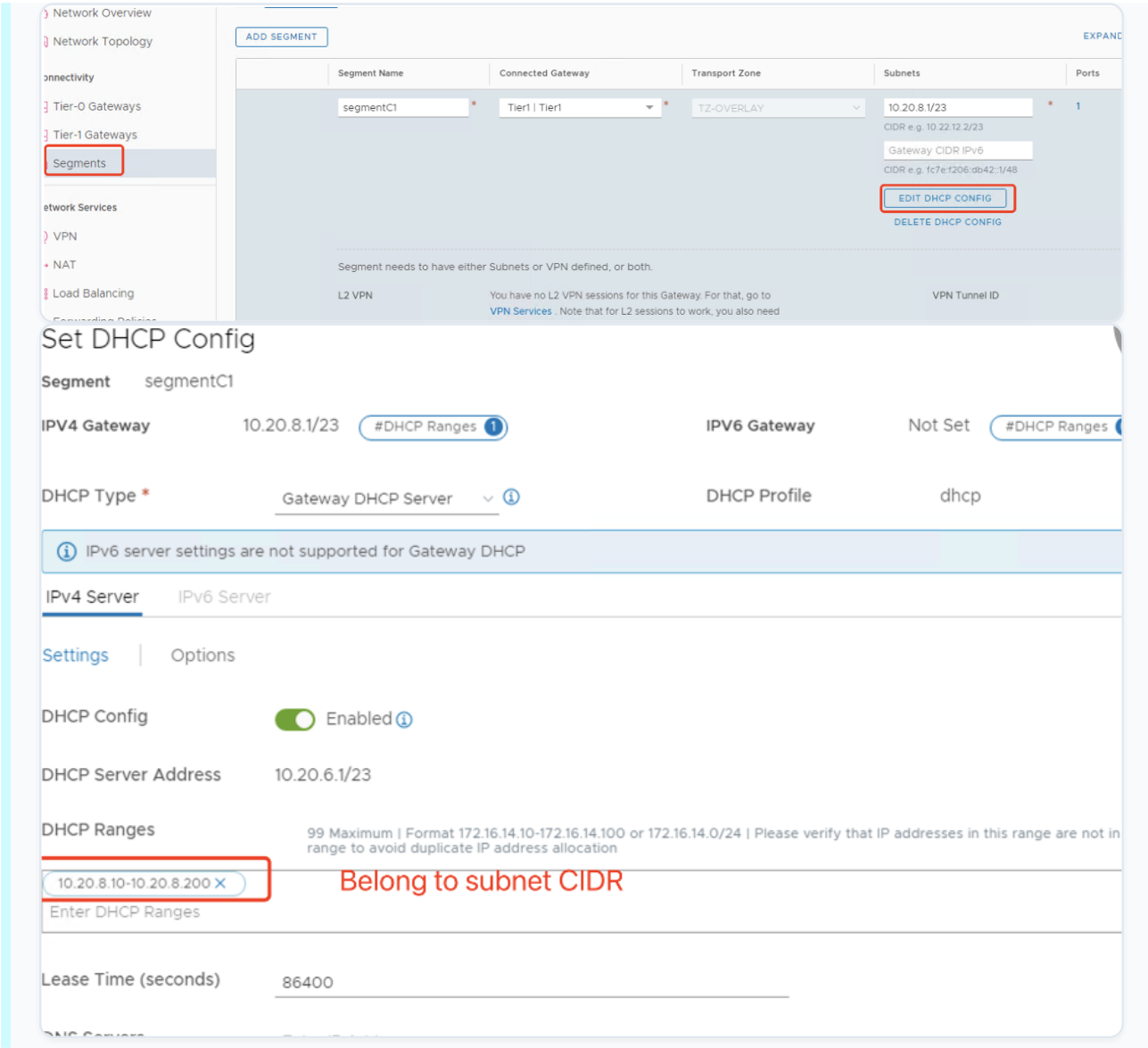
在 NSX-T 中创建网络分段

对于工作负载 VM，您可以为私有云创建作为 NSX-T 网络分段的子网：

1. 在 NSX-T Manager 中，转到 **网络 > 分段**。
2. 单击 **添加分段**。
3. 输入分段的名称。
4. 选择 **Tier-1** 作为 **连接的网关**，并将类型保留为 **灵活**。
5. 单击 **设置子网**。
6. 单击 **添加子网**。
7. 在 **网关 IP/前缀长度** 中输入子网范围。将子网范围指定为以 **.1** 作为最后一个八位字节。例如，**10.12.2.1/24**。
8. 指定 DHCP 范围，然后单击 **添加**。
9. 在 **传输区域** 中，从下拉列表中选择 **TZ-OVERLAY**。
10. 单击 **保存**。现在，您可以在 vCenter 中创建 VM 时选择此网络段。

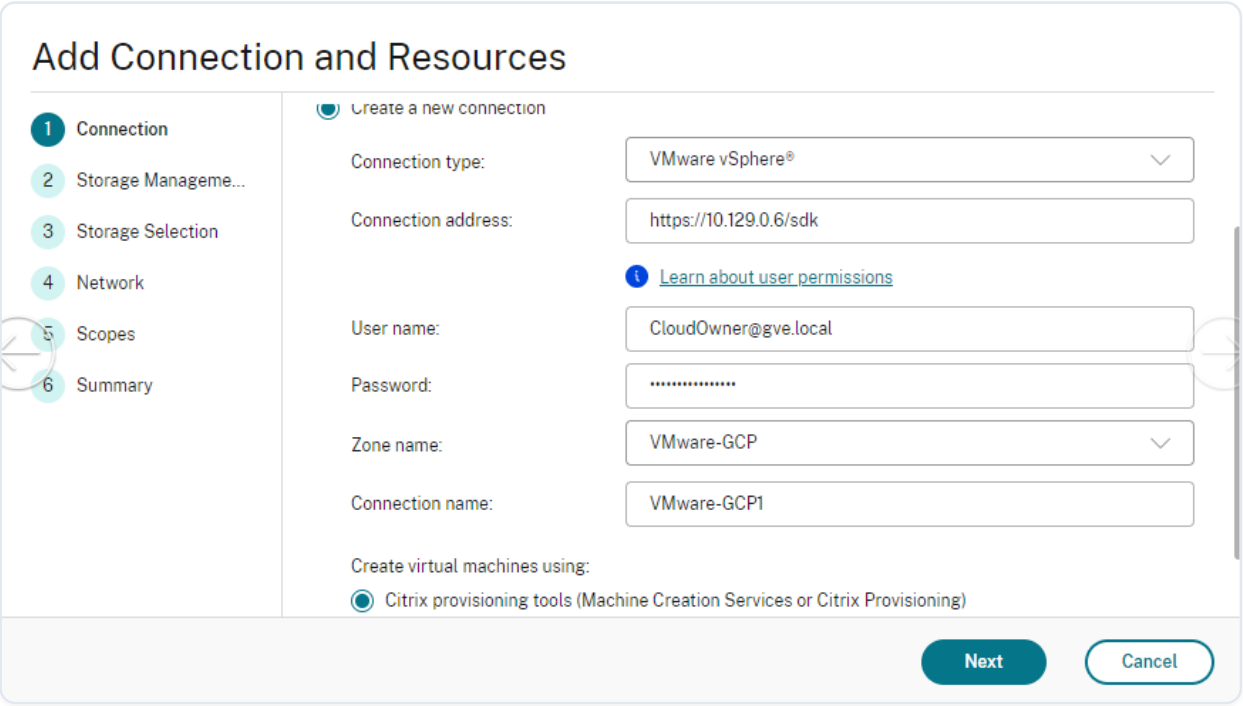
在给定区域中，您最多可以使用私有服务访问从 VMware Engine 设置 100 条到 VPC 网络的唯一路由。这包括（例如）私有云管理 IP 地址范围、NSX-T 工作负载网络段和 HCX 网络 IP 地址范围。此限制包括该区域中的所有私有云。

> **注意：**
>
> 存在一个 Google Cloud 配置问题，因此您需要多次配置 DHCP 范围设置。因此，请务必在 Google Cloud 配置后配置 DHCP 范围设置。单击 **编辑 DHCP 配置** 以配置 DHCP 范围。



在 CITRIX STUDIO 中创建 GOOGLE CLOUD VMWARE 连接

1. 在 vCenter 中创建计算机。
2. 启动 Citrix Studio 应用程序。
3. 选择托管节点，然后单击 **添加连接和资源**。
4. 在 **连接** 屏幕上，选择 **创建新连接**，以及以下详细信息：



a. 将 **连接类型** 选择为 **VMware vSphere**。

b. 在**连接地址**中，输入 vCenter 私有 IP 地址。

c. 输入 vCenter 凭据。

d. 输入连接名称。

e. 选择用于创建虚拟机的工具。

5. 在“**网络**”屏幕上，选择在 NSX-T 服务器中创建的子网。

6. 完成向导。

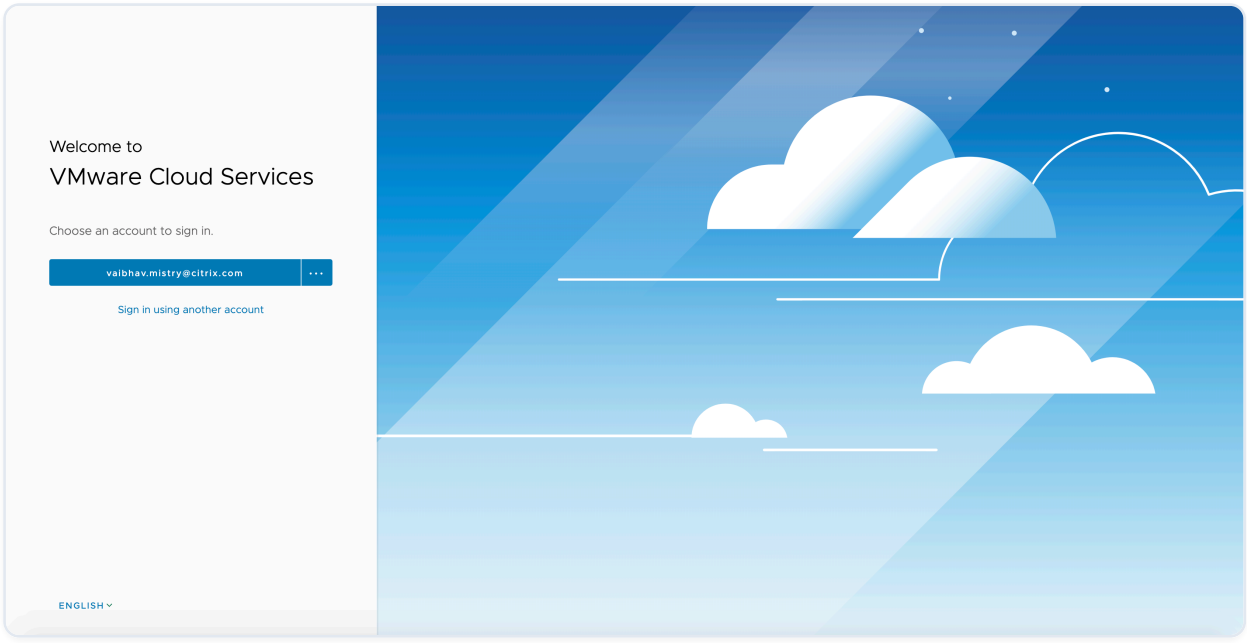
亚马逊网络服务 (AWS) 上的 VMware 云

Amazon Web Services (AWS) 上的 VMware Cloud 使您能够将基于 VMware 的本地 Citrix 工作负载迁移到 AWS Cloud。

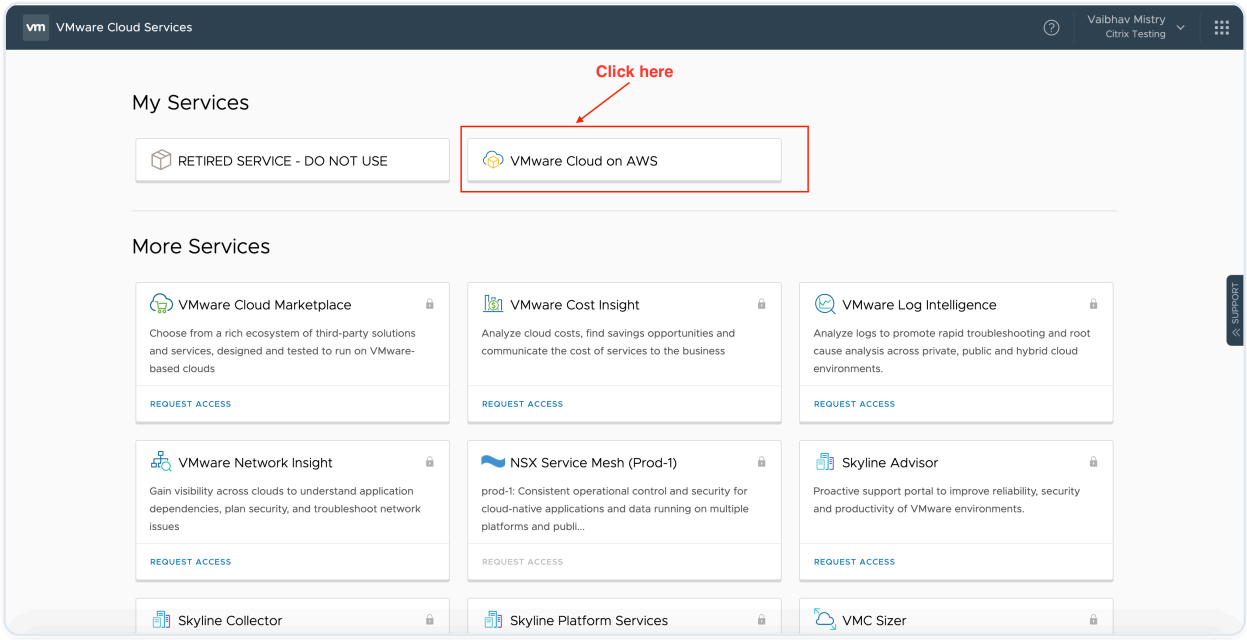
本文介绍了在 AWS 上设置 VMware Cloud 的过程。

访问 VMware Cloud 环境

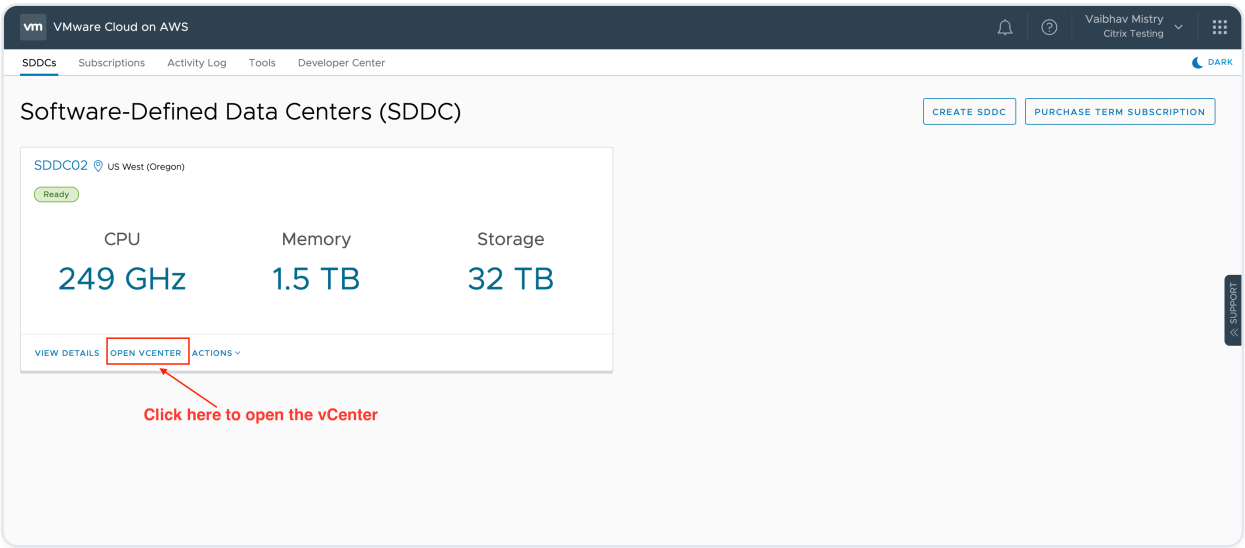
1. 使用 URL `<https://console.cloud.vmware.com/>` 登录到 VMware Cloud 服务。

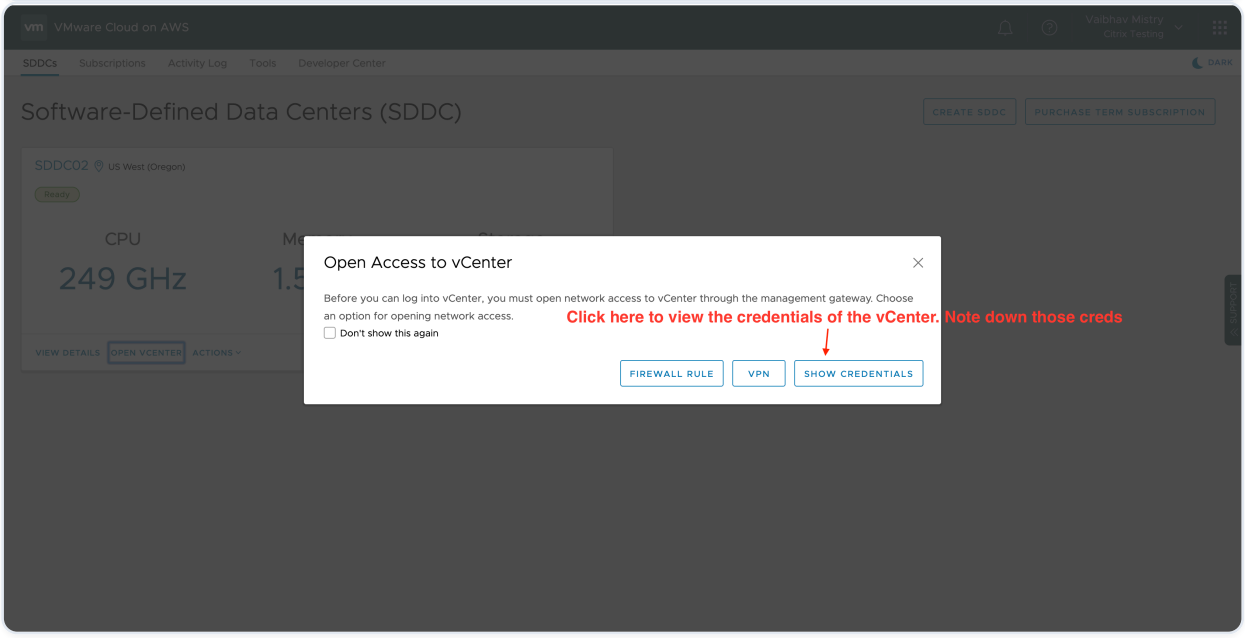


2. 单击**Amazon Web Services 上的 VMware Cloud**。将显示“软件定义数据中心 (SDDC)”页面。

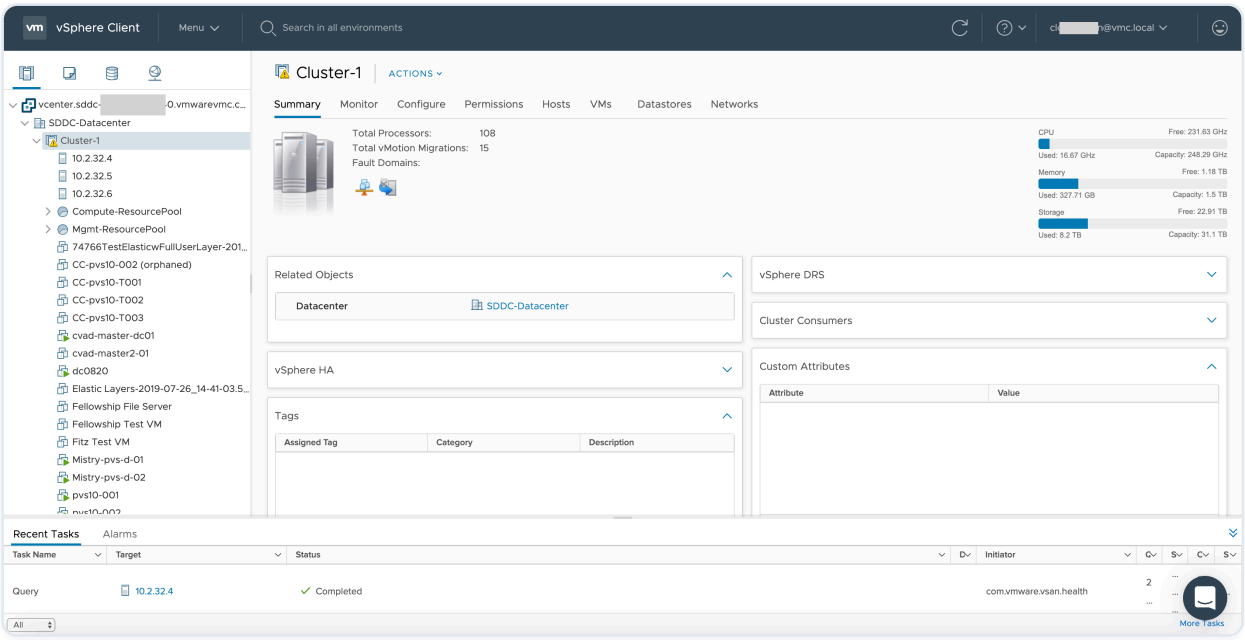


3. 单击**打开 VCENTER**，然后单击**显示凭据**。记下凭据以供以后使用。





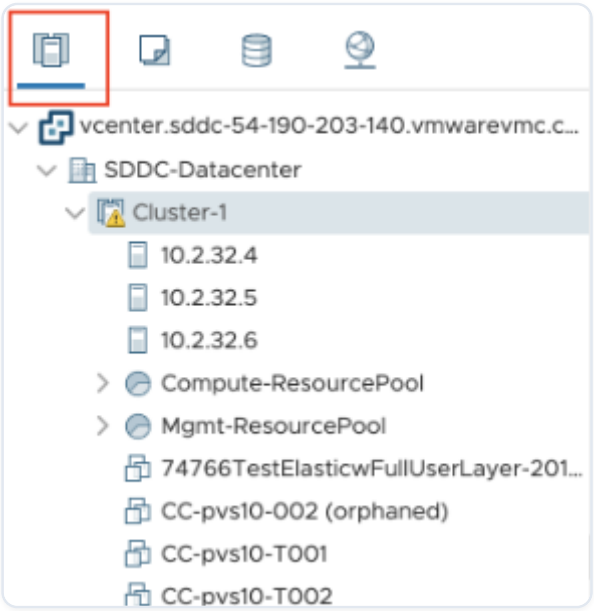
4. 打开 Web 浏览器并输入 vSphere Web Client 的 URL。
5. 输入所记录的凭据，然后单击“**登录**”。vSphere 客户端网页与本地环境类似。



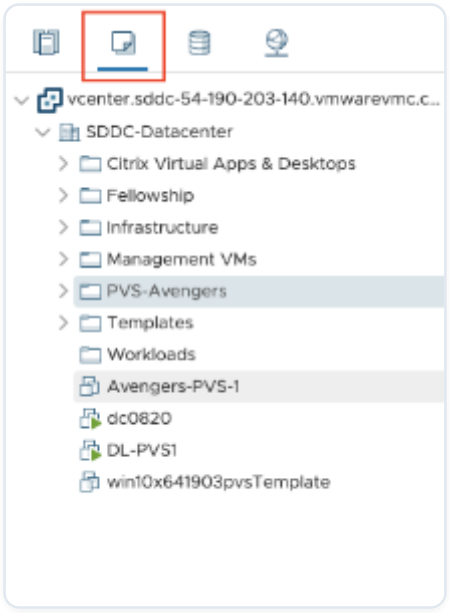
关于 VMware 云环境

vSphere 客户端网页上有四种视图。

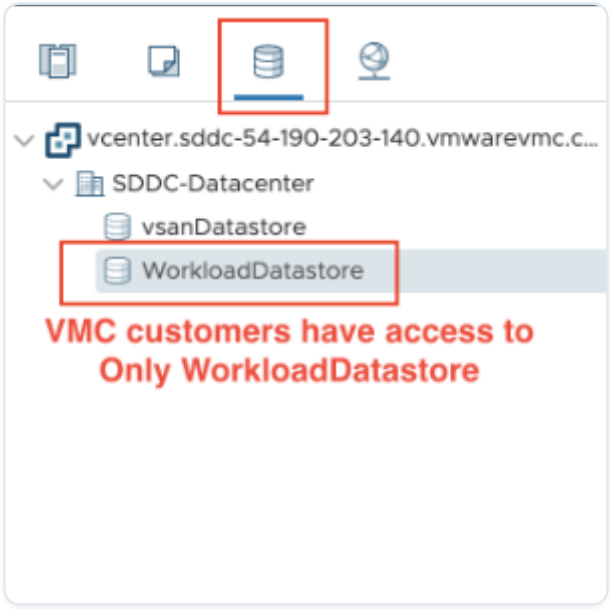
- 主机和群集视图：您无法创建新的群集，但云管理员可以创建多个资源池。



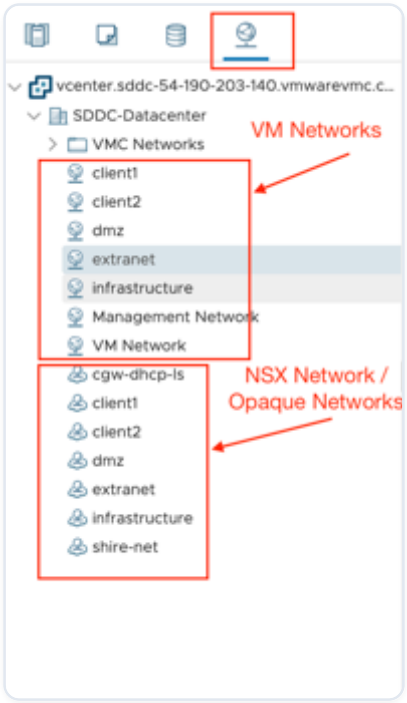
- VM 和模板视图：云管理员可以创建许多文件夹。



- 存储视图：在 Citrix Studio 中添加托管单元时，请选择 **WorkloadDatastore** 存储，因为您只能访问 Workload Datastore。



- 网络视图：VMware 云网络和不透明网络的图标不同。



设置群集后，请参阅 VMware 虚拟化环境 以添加连接和资源。

后续步骤

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关创建和管理连接的信息，请参阅连接到 VMware 云和合作伙伴解决方案

更多信息

- 创建和管理连接与资源
- 创建计算机目录

安装核心组件

重要提示：

- Citrix 会根据其合法权益（包括许可证合规性）收集基本的许可数据。有关详细信息，请参阅 Citrix 许可数据。
- 确保许可证服务器运行的最低版本为 11.17.2 build 53100。未能满足此必备条件将阻止 Citrix Virtual Apps and Desktops 站点升级和站点创建。

> 核心组件包括 Citrix 交付控制器™、Citrix Studio、Web Studio、Citrix Director 和 Citrix 许可证服务器。

> **注意：**

> Citrix Studio 是一个基于 Windows 的管理控制台，可用于配置和管理本地 Citrix Virtual Apps and Desktops 部署。Web Studio 是 Citrix Studio 的下一代产品，它是一个基于 Web 的管理控制台，提供与 Citrix Studio 相同的所有功能。有关 Web Studio 的详细信息，请参阅 安装 Web Studio。

> （在 2003 之前的版本中，核心组件包括 Citrix StoreFront。您仍然可以通过单击 **Citrix StoreFront** 磁贴或运行安装介质上提供的命令来安装 StoreFront。）

开始安装之前，请查看本文和 准备安装。

本文介绍了安装核心组件时的安装向导顺序。提供了命令行等效项。有关详细信息，请参阅 使用命令行安装。

步骤 1. 下载产品软件并启动向导

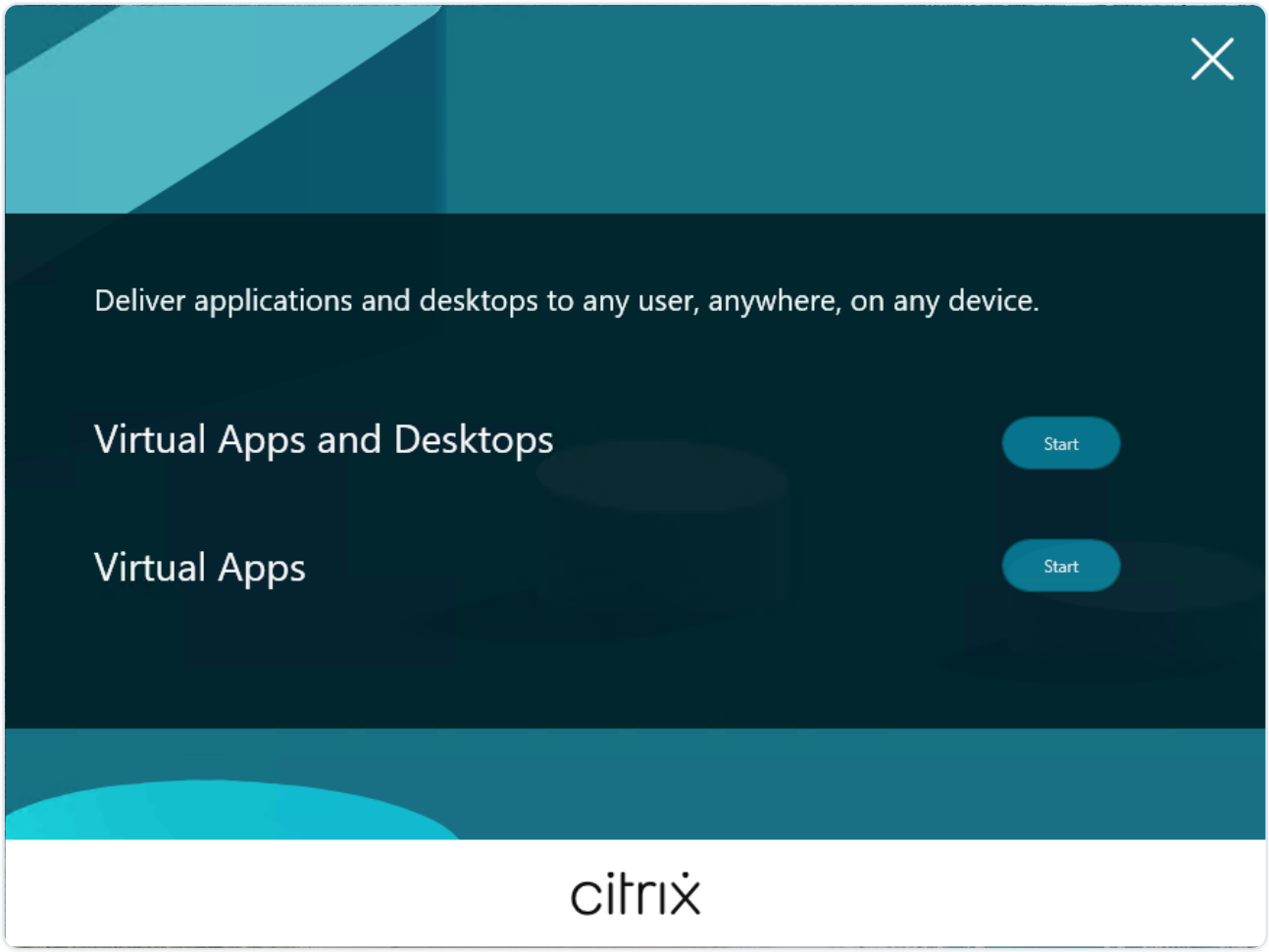
使用您的 Citrix 帐户凭据访问 Citrix Virtual Apps and Desktops™ 下载页面。下载产品 ISO 文件。

解压缩文件。或者，刻录 ISO 文件的 DVD。

使用本地管理员帐户登录到要安装核心组件的计算机。

将 DVD 插入驱动器或装载 ISO 文件。如果安装程序未自动启动，请双击 **AutoSelect** 应用程序或装载的驱动器。

步骤 2. 选择要安装的产品



点击要安装的产品旁边的“**开始**”：Virtual Apps 或 Virtual Apps and Desktops。

（如果计算机上已安装 Citrix Virtual Apps and Desktops™ 组件，则此页面不会出现。）

命令行选项：`/xenapp` 以安装 Citrix Virtual Apps。如果省略该选项，则安装 Citrix Virtual Apps and Desktops。

步骤 3. 选择要安装的内容

组件安装程序中的组件选择页面(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/what-to-install-2.png)

如果您是初次使用，请选择“**Delivery Controller**”。（在后续页面上，您将选择要在此计算机上安装的特定组件。）

如果您已安装 Controller（在此计算机上或另一台计算机上），并且想要安装其他组件，请从“**扩展部署**”部分选择该组件。

命令行选项：`/components`

步骤 4. 阅读并接受许可协议

组件安装程序中的许可协议页面(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/core-license-75.png)

在“**许可协议**”页面上，阅读许可协议后，表明您已阅读并接受该协议。然后单击“**下一步**”。

步骤 5. 选择要安装的组件和安装位置

组件安装程序中的核心组件页面(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/core-components-75.png)

在“**核心组件**”页面上：

- **位置**：默认情况下，组件安装在 `C:\Program Files\Citrix` 中。对于大多数部署，默认设置即可。如果指定其他位置，则该位置必须对网络服务具有执行权限。
- **组件**：默认情况下，所有核心组件的复选框均处于选中状态。将所有核心组件安装在一台服务器上适用于概念验证、测试或小型生产部署。对于大型生产环境，Citrix 建议将 Director、StoreFront、Secure Private Access 和许可证服务器安装在单独的服务器上。

> **注意：**
>
> 如果您要在多台服务器上安装组件，请先安装 Citrix 许可证服务器和许可证，然后再在其他服务器上安装其他组件。有关指导，请参阅 Citrix Virtual Apps and Desktops 许可指南的“自动安装”部分。

> 当您选择不在本机上安装所需的某个核心组件时，会出现一个图标提醒您。该提醒会提示您安装该组件，但并非必须在本机上安装。

单击**下一步**。

命令行选项：`/installdir`、`/components`、`/exclude`

硬件检查

安装或升级 Delivery Controller 时，会检查硬件。如果计算机的 RAM 小于建议量 (5 GB)，安装程序会发出警报，这可能会影响站点的稳定性。有关详细信息，请参阅 硬件要求。

图形界面：将出现一个对话框。

- 建议：单击“**取消**”以停止安装。向计算机添加更多 RAM，然后再次开始安装。

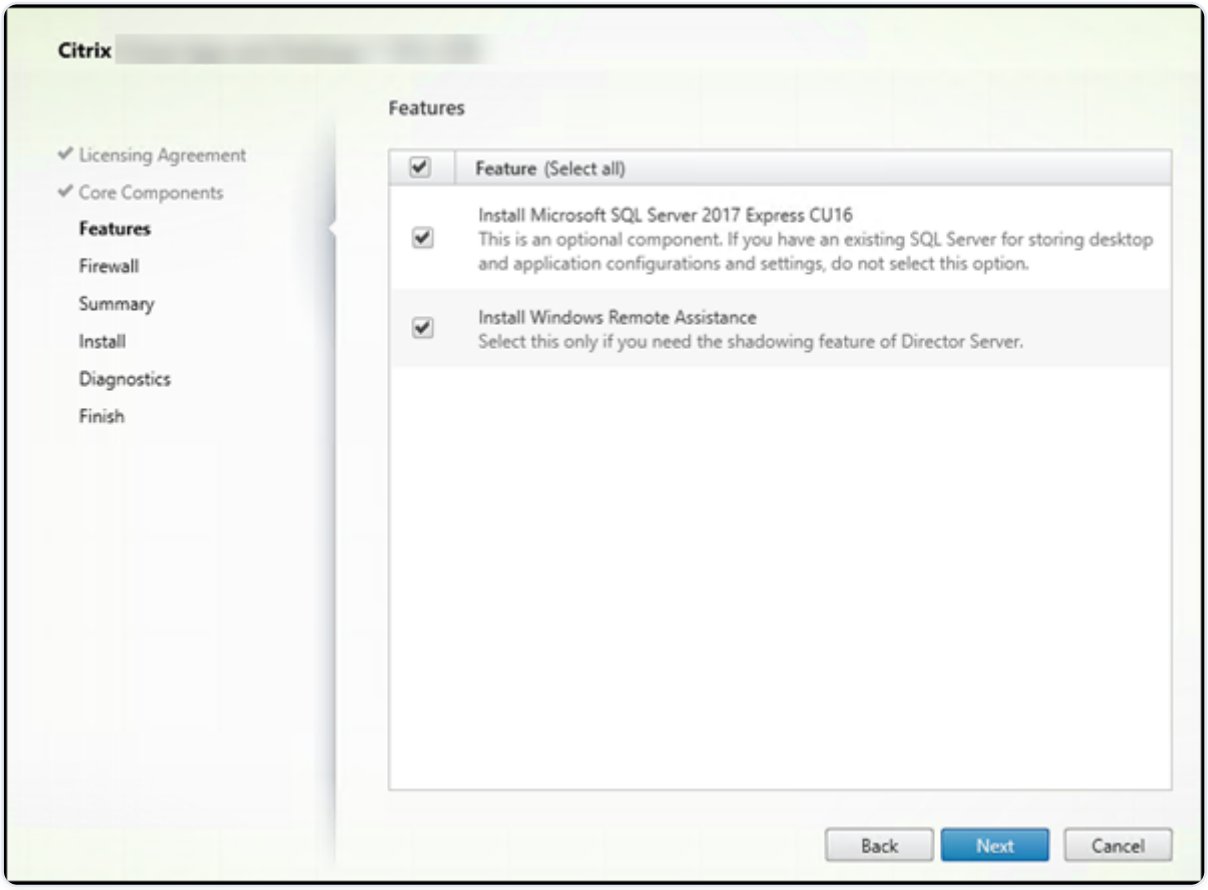
- 或者，单击“**下一步**”以继续安装。站点可能会出现稳定性问题。

命令行界面： 安装/升级结束。安装日志包含一条消息，描述了发现的问题和可用选项。

- 建议：向计算机添加更多 RAM，然后再次运行该命令。
- 或者，使用 `/ignore_hw_check_failure` 选项再次运行该命令以覆盖警告。您的站点可能会出现稳定性问题。

升级时，如果操作系统或 SQL Server 版本不再受支持，您也会收到通知。请参阅 升级和迁移。

步骤 6. 启用或禁用功能



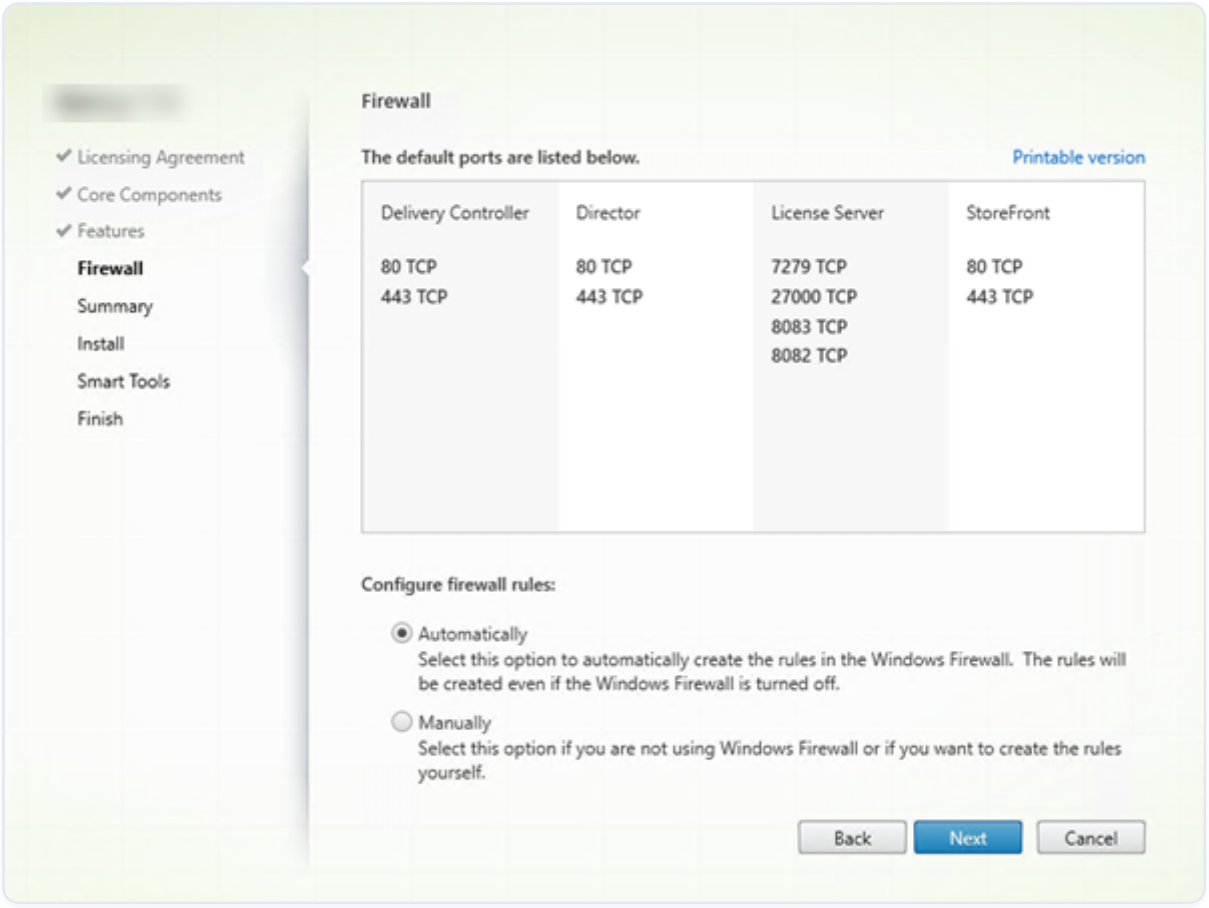
在“**功能**”页面上：

- 选择是否安装 Microsoft SQL Server Express 作为站点数据库。默认情况下，此选项处于启用状态。如果您不熟悉 Citrix Virtual Apps and Desktops 数据库，请查看数据库。
- 安装 Director 时，Windows 远程协助会自动安装。您可以选择是否在 Windows 远程协助中启用影子功能，以用于 Director 用户影子。启用影子功能会打开 TCP 端口 3389。默认情况下，此功能处于启用状态。默认设置适用于大多数部署。此功能仅在安装 Director 时显示。

单击“**下一步**”。

命令行选项：`/nosql`（阻止安装），`/no_remote_assistance`（阻止启用）

步骤 7. 打开 Windows 防火墙端口



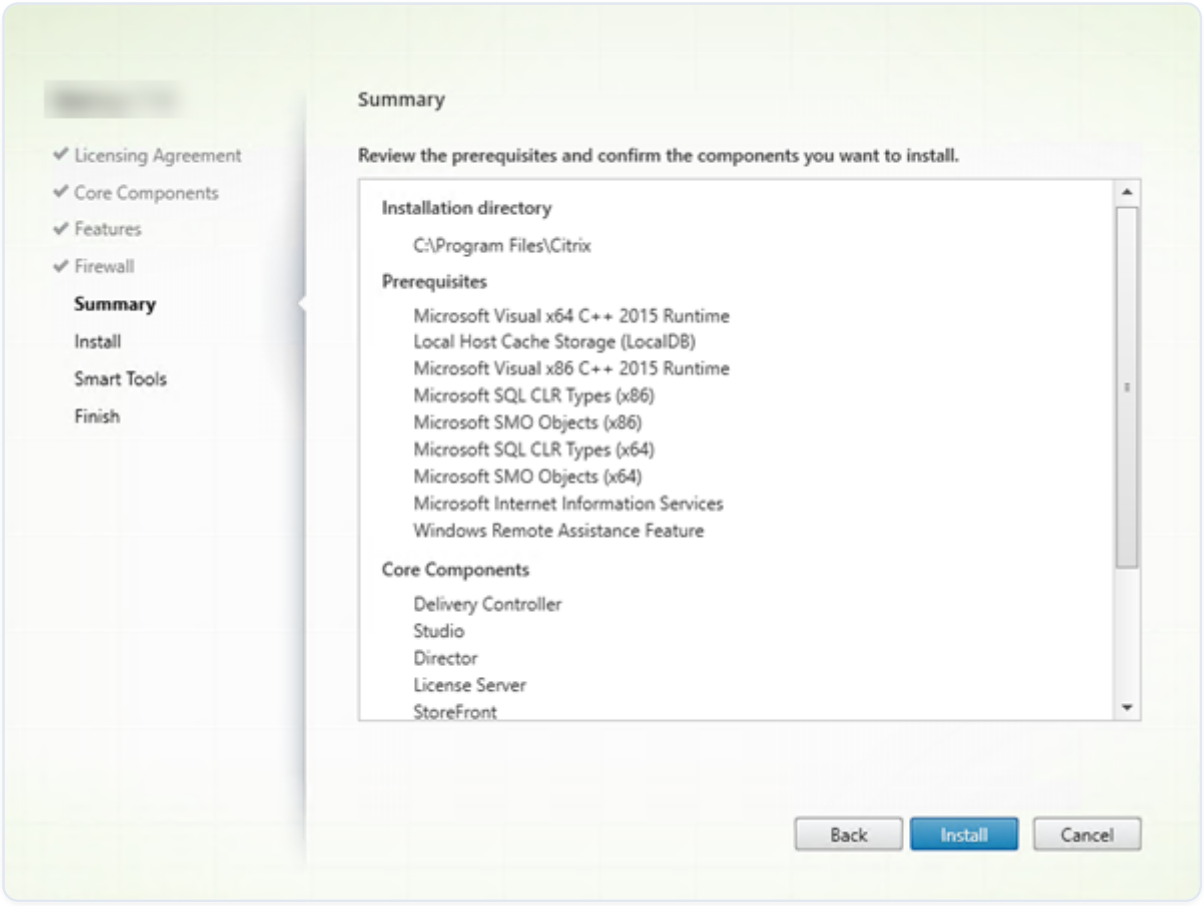
默认情况下，如果 Windows 防火墙服务正在运行，即使防火墙未启用，**防火墙**页面上的端口也会自动打开。默认设置适用于大多数部署。有关端口信息，请参阅网络端口。

单击“**下一步**”。

（该图显示了在此计算机上安装所有核心组件时的端口列表。此类安装通常仅用于测试部署。）

命令行选项：`/configure_firewall`

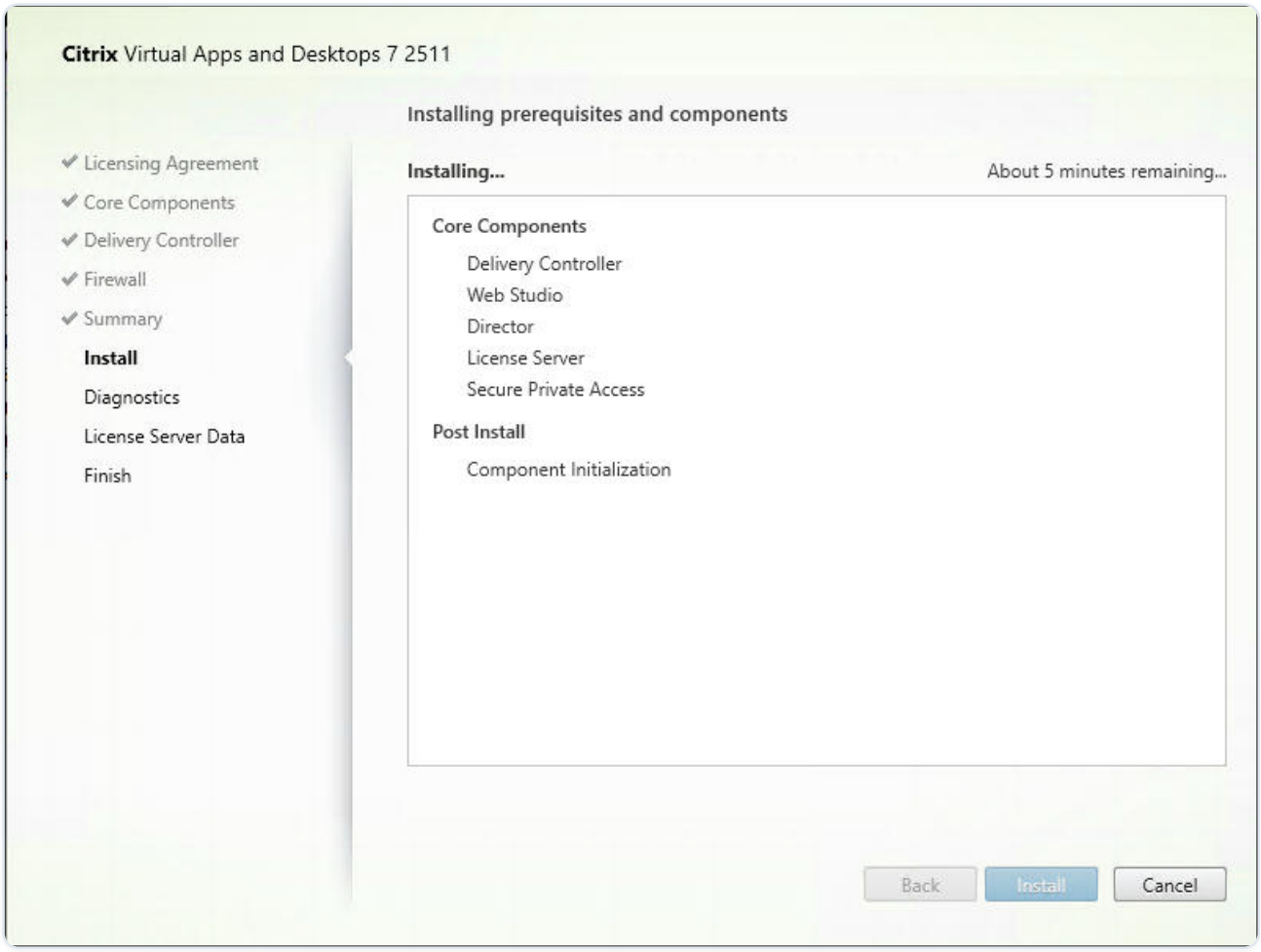
步骤 8. 查看必备条件并确认安装



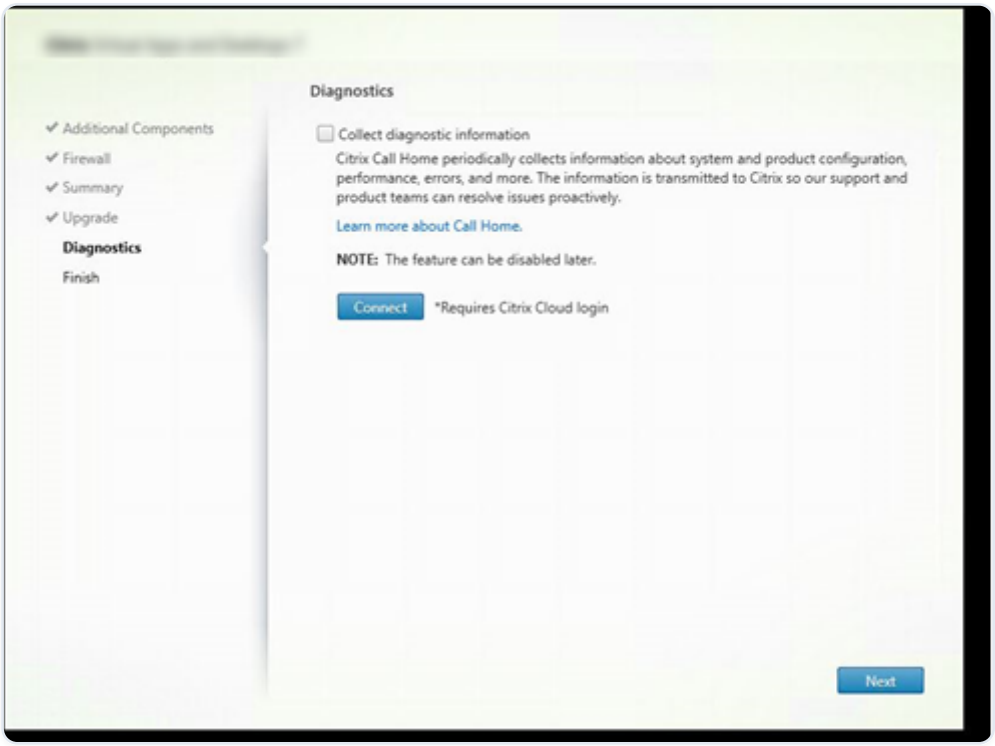
摘要页面列出了将要安装的内容。使用“**返回**”按钮返回到之前的向导页面并根据需要更改选择。

准备就绪后，单击“**安装**”。

显示屏显示安装进度：



步骤 9. 与 Cloud Software Group 共享诊断信息



在**诊断**页面上，选择是否参与 Citrix Call Home。

使用图形界面安装 Delivery Controller 时，将显示此页面。安装 StoreFront（但不是 Controller）时，向导会显示此页面。安装其他核心组件（但不是 Controller 或 StoreFront）时，向导不会显示此页面。

在升级过程中，如果 Call Home 已启用或者安装程序遇到与 Citrix Telemetry Service 相关的错误，则不会显示此页面。

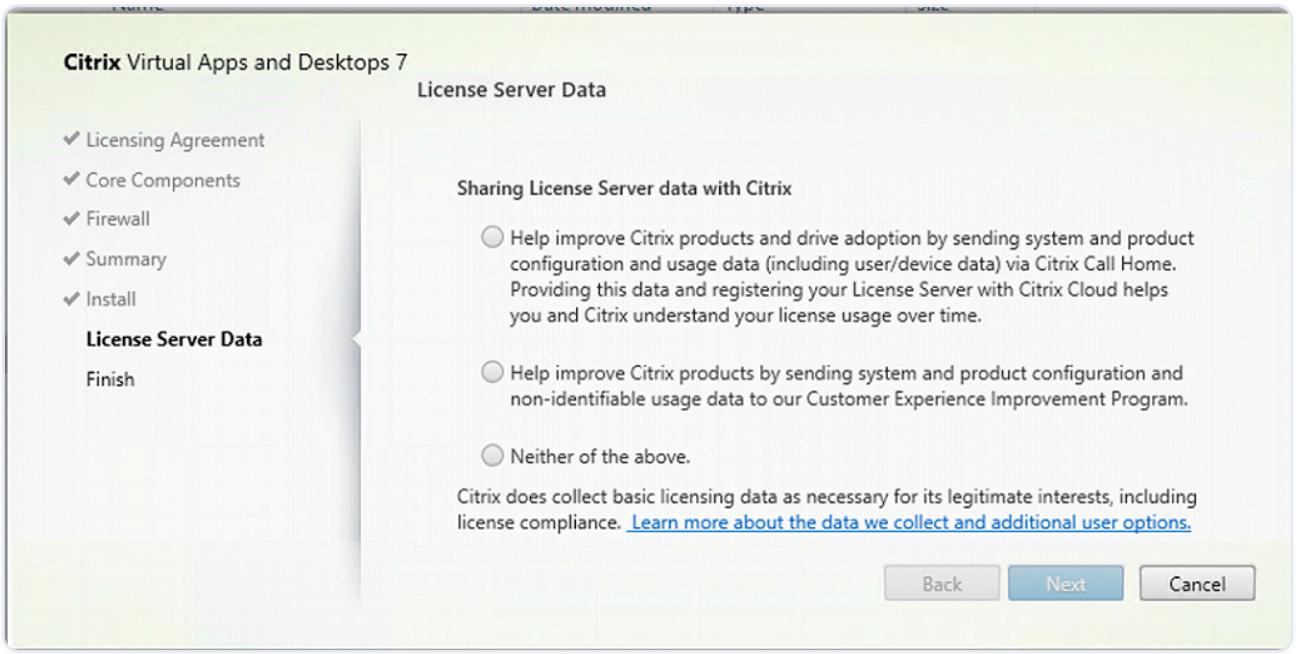
如果您选择参与（默认），请单击**连接**。出现提示时，输入您的 Citrix 帐户凭据。您可以在安装后更改您的注册选择。

凭据验证后（或者如果您选择不参与），单击**下一步**。

如果您在**诊断**页面上单击**连接**而未首先选择**收集诊断信息**，则在关闭**连接到 Citrix Insight Services** 对话框后，**下一步**按钮将禁用。您无法移动到下一页。要重新启用**下一步**按钮，请选择并立即取消选择**收集诊断信息**。

有关详细信息，请参阅 Call Home。

步骤 10. 与 Cloud Software Group 共享许可证服务器数据



在**许可证服务器数据**页面上，我们请求您共享 Call Home 数据或客户体验改善计划 (CEIP) 数据以协助我们。此外，Cloud Software Group 还要求收集基本的许可数据，包括许可证合规性，以满足其合法利益。

安装许可证服务器时，将显示**许可证服务器数据**页面：

- 作为独立组件。
- 作为核心组件，在安装 Delivery Controller 期间。

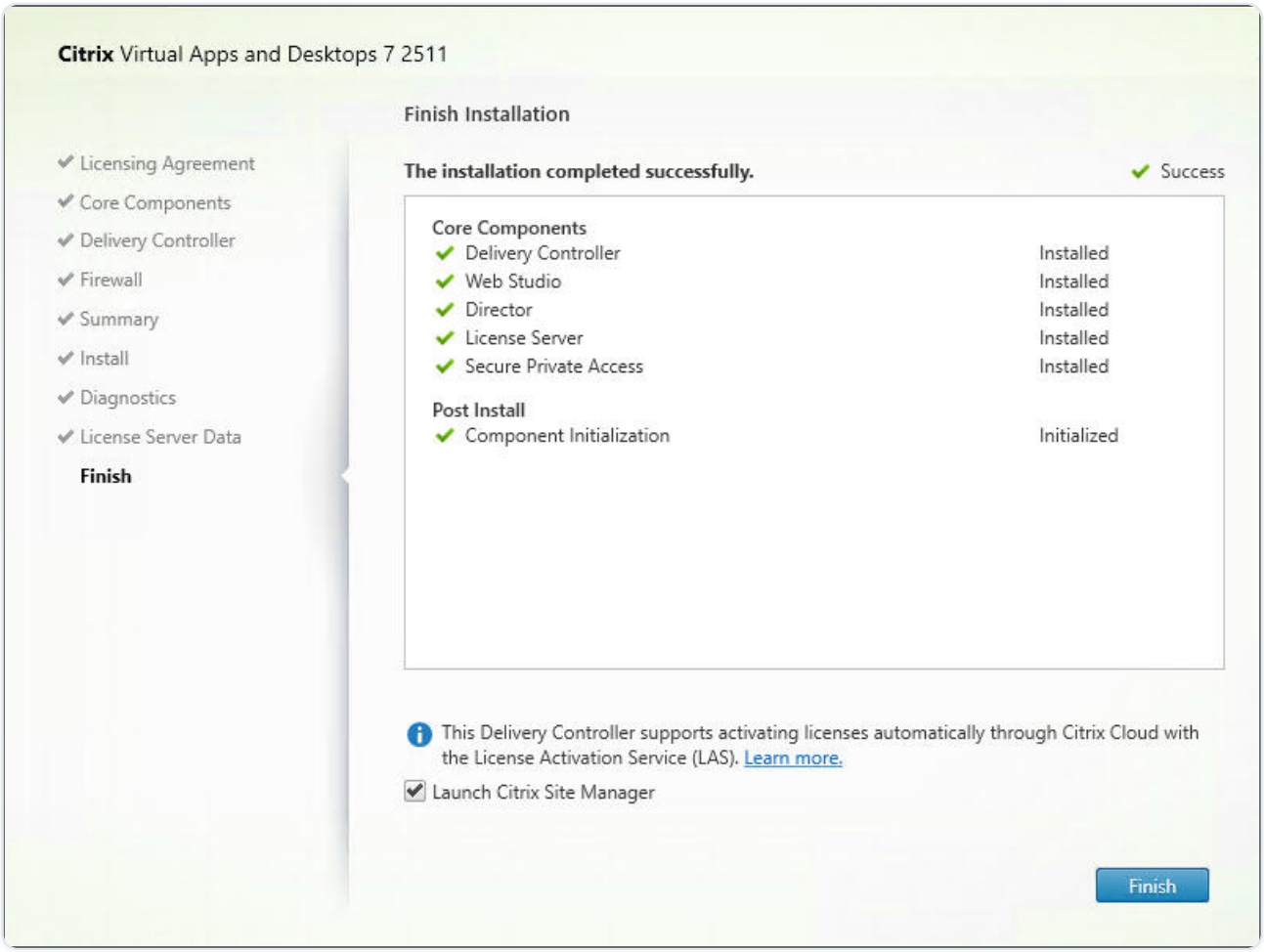
在升级期间，如果配置已在 `/CITRIX.opt:` 文件中设置，则此页面不会出现。

许可证服务器监控多种类型的用户数据，例如许可数据、Call Home 数据和 CEIP 数据。要启用 Call Home 数据和 CEIP 数据收集，您必须选择参与（选择加入）。

有关如何在使用命令行安装时启用 Call Home 和 CEIP 数据收集的更多信息，请参阅用于安装核心组件的命令行选项。

有关 Cloud Software Group 许可数据收集的更多信息，请参阅Citrix 许可数据收集程序。

步骤 11. 完成此安装



完成页面包含所有已成功安装和初始化的必备项和组件的绿色复选标记。

单击“**完成**”。

> **注意：**
>
> 当您升级到版本 2511 时，安装程序会自动卸载 Citrix Studio（基于 MMC）。您的配置数据存储在数据库中，不受自动卸载的影响。

步骤 12. 在其他计算机上安装剩余的核心组件

如果您已在一台计算机上安装了所有核心组件，请继续执行后续步骤。否则，请在其他计算机上运行安装程序以安装其他组件。您还可以在其他服务器上安装更多 Controller。

后续步骤

安装所有必需组件后，使用 Web Studio 创建站点。

创建站点后，安装 VDA。

您可以随时使用完整产品安装程序通过以下组件扩展部署：

- **Universal Print Server 服务器组件：** 在您的打印服务器上启动安装程序。

  a. 在**扩展部署**部分中选择 **Universal Print Server**。

  b. 接受许可协议。

  c. 在**防火墙**页面上，默认情况下，如果 Windows 防火墙服务正在运行，即使防火墙未启用，也会在防火墙中打开 TCP 端口 7229 和 8080。如果您想手动打开端口，可以禁用此默认操作。

  要从命令行安装此组件，请参阅用于安装通用打印服务器的命令行选项。
- 联合身份验证服务。
- 会话记录。
- 工作区环境管理。
- 安装 uberAgent
- 安装 deviceTRUST 代理
- WEM 快速入门指南

安装 Web Studio

> **注意：**
>
> Citrix Studio (MMC Studio) 已从版本 2511 开始移除，不再受支持。本文假设 Web Studio 是唯一正在使用的管理控制台。

简介

Web Studio 是一个基于 Web 的管理控制台，提供与 Citrix Studio 相同的功能。Web Studio 具有与 Citrix DaaS Studio 界面 相同的外观和体验，通过提供原生 Web 体验来现代化您的管理体验。

您可以将 Web Studio 部署到安装了 Internet Information Service (IIS) 的任何 Windows 服务器。有两种部署选项：

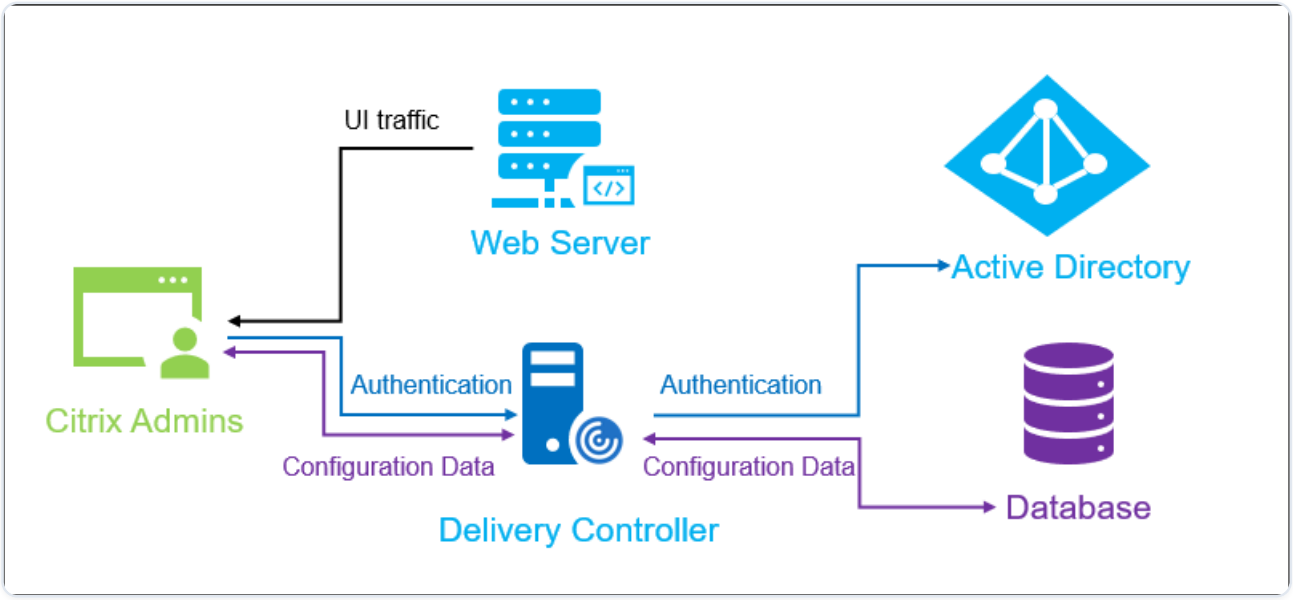
- 安装在专用服务器上：

  对于性能和可扩展性至关重要的大型环境，我们建议将 Web Studio 安装在专用服务器上。此服务器也可以选择托管 Director。

- 与交付控制器™集成：

  对于快速部署和更简单的环境，请将 Web Studio 直接安装在 Delivery Controller 上。此方法非常适合将最小化管理开销作为优先事项的小型部署。

下图显示了 Web Studio 体系结构：



启动并运行 Web Studio 的一般工作流程如下：

1. 安装 Web Studio。
2. 设置站点。
3. 将 Delivery Controller 添加到 Web Studio 进行管理。
4. (可选) 将 Web Studio 配置为 Delivery Controller 的代理
5. (可选) 禁用 Pendo。
6. Web Studio 的安全服务器配置
7. 登录 Web Studio。

要设置负载均衡的 Web Studio 部署，请参阅 本文。

Web Studio 中的新增功能

请参阅 新增功能 文章。

系统要求

下表列出了安装和使用 Studio 所支持的操作系统、浏览器、显示设置和硬件要求。

支持的操作系统

操作系统	版本	SERVER CORE 支持
Windows 服务器 2025	标准版，数据中心版	是
Windows 服务器 2022	标准版，数据中心版	是
Windows 服务器 2019	标准版，数据中心版	是
Windows 服务器 2016	标准版，数据中心版	是

支持的浏览器

浏览器	最低支持版本
微软 Edge	92
Firefox ESR（延长支持版本）	90
谷歌浏览器	92
Safari 浏览器	14

显示要求

要求	值
推荐屏幕分辨率	1440 × 1024

硬件要求

资源	最低要求
内存	1 GB RAM

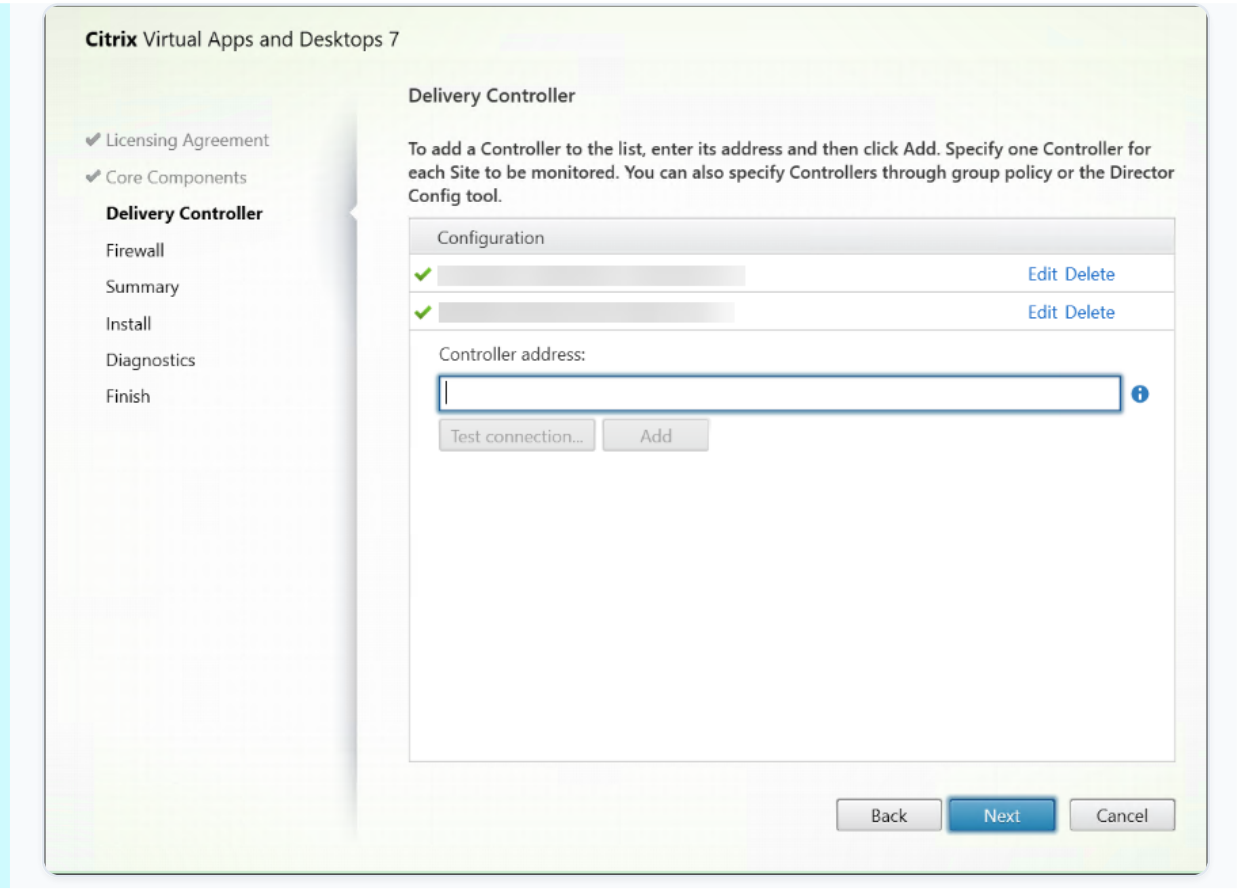
资源	最低要求
磁盘空间	100 MB

安装 Web Studio

以下信息是对 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-core-components.html) 中 指南的补充。要安装 Web Studio：

- 使用 Citrix Virtual Apps and Desktops™ 的完整产品 ISO 安装程序安装 Web Studio。ISO 安装程序会检查先决条件，安装任何缺失的组件，设置 Web Studio 网站（如果包含在 Delivery Controller 安装中，则在 Delivery Controller 上），并执行基本配置。
- 如果安装期间未包含 Web Studio，请使用安装程序添加 Web Studio。
- 安装 Web Studio 时，系统会提示您键入 Delivery Controller 的 FQDN。

> **注意：**
>
> - 我们建议在同一版本上运行 Web Studio 和 Delivery Controller，以确保完整功能。
> - 您可以添加多个 Delivery Controller。Web Studio 会尝试以随机顺序连接它们。如果 Web Studio 尝试连接的 Delivery Controller 不可达，Web Studio 会自动回退到其他 Delivery Controller。
> - 如果在**核心组件**中选择了 Director 并已安装，则您在此处添加的 Delivery Controller 将同时用于 Web Studio 和 Director。
> - 如果 Delivery Controller 配置为 TLS（推荐），则输入的 FQDN 必须与安装在 Delivery Controller 上的证书的通用名称或主题备用名称匹配。
> - Web Studio 可以安装在任何 **Site ID = 1** 的 IIS 网站上，无论网站名称如何。此功能使您可以在自定义 IIS 站点而不是**默认网站**下托管 Web Studio。
>   - 如果在运行 ISO 安装程序之前未安装 IIS，安装程序会自动配置 IIS 并在**默认网站**（Site ID = 1）下部署 Web Studio。安装后，可以根据需要重命名网站名称。
>   - 如果 IIS 已安装，您可以提前创建一个具有您首选名称和物理路径的 IIS 站点，只要其 **Site ID** 为 **1** 即可。然后 Web Studio 将直接安装在该站点下，无需进一步配置。



- 在**完成**页面上，查看已安装的组件，然后单击**完成**。

  启动站点管理器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/launch-site-manager.png)

> **注意：**
>
> 您还可以使用命令行安装 Web Studio。示例：`.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local" /configure_firewall /quiet`。有关更多信息，请参阅使用命令行安装。

配置 TLS 证书

默认情况下，如果 IIS 尚未配置 HTTPS，安装程序会使用服务器的 FQDN 作为证书的公用名创建自签名证书，并将其绑定到端口 443。此行为允许用户从本地计算机访问 Web Studio，但从其他计算机连接的用户会看到安全警告，因为该证书不受信任。我们建议将此证书替换为由企业或公共证书颁发机构 (CA) 签名的证书。有关详细信息，请参阅 在 Web Studio 和 Director 上启用 TLS。如果 IIS 中已配置 TLS 证书，则安装程序不会进行任何更改。

> **注意：**

> 要详细了解如何保护 Web Studio 部署，请参阅 保护 Web Studio 部署。

设置站点

要设置 Citrix Virtual Apps and Desktops 部署（也称为站点），请使用 Citrix Site Manager 工具。该工具随 Delivery Controller 自动安装。

要设置站点，请执行以下步骤：

1. 在 Delivery Controller 上，打开桌面“开始”菜单，然后选择 **Citrix > Citrix Site Manager**。
2. 在 Citrix Site Manager 中，选择 **Create a site**。将显示“站点设置”向导。
3. 创建站点并按如下方式配置其设置：
   - 在“**简介**”页面上，键入站点的名称。
   - “**数据库**”页面包含用于设置站点、监视和配置日志记录数据库的选项。有关详细信息，请参阅 步骤 3. 数据库。
   - 在“**许可**”页面上，指定许可证服务器地址，然后指明要使用（安装）哪个许可证。有关详细信息，请参阅 步骤 4. 许可。
4. 在“**摘要**”页面上，检查所有设置，然后单击“**提交**”。

   此 Controller 的 IP 地址会自动添加到站点。

   > **注意：**
   >
   > 创建站点的用户将成为该站点的完全管理员。有关详细信息，请参阅 委派管理。

如果在创建站点后安装新的 Controller，则必须将该 Controller 添加到站点。详细步骤如下：

1. 在此新控制器上运行 Citrix Site Manager。
2. 选择 **加入现有站点**。
3. 键入已添加到站点的控制器的地址。
4. 单击 **提交**。

将 Delivery Controller 添加到 Web Studio 进行管理

使用 Studio 配置工具将 Delivery Controller 添加到 Web Studio 进行管理。此工具位于 Web Studio 安装文件夹中。

默认情况下，该工具安装在以下默认文件夹中。

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

假设您要为要使用 Web Studio 管理的站点配置以下两个 Delivery Controller：`ddc1.studio.local` 和 `ddc2.studio.local`。运行以下 PowerShell 命令：

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

注意：

- 该工具需要计算机管理员权限。
- 由于 IIS 服务器上的缓存设置，Delivery Controller 配置更改可能不会立即生效。要立即生效，请转到 Web Studio 服务器，打开 Internet Information Services (IIS) Manager，导航到 *Server_name* > **站点** > *安装 Web Studio 的 IIS 站点名称（站点 ID = 1）*，然后在“管理网站”窗格中选择 **重新启动**。
- 当您使用新 FQDN 重新部署 Delivery Controller 时，请使用 `StudioConfig.exe` 和 `C:\Program Files\Citrix\Web Studio\Site\assets\json\manifest.json` 文件更新其在 Web Studio 中的 FQDN。如果您不更新 `manifest.json` 文件，旧 FQDN 仍会显示在 Web Studio 登录窗口中。因此，您必须在登录时输入新的 FQDN 作为替代。
- 要查看所有支持的参数，请运行 `StudioConfig.exe --help`。

（可选）将 Web Studio 配置为 Delivery Controller 的代理

默认情况下，当您使用 Web Studio 控制台管理部署时，您通过 Web 浏览器连接到 Web Studio 服务器和 Delivery Controller。我们为您提供了一个选项，可将 Web Studio 服务器配置为 Delivery Controller 的代理。因此，在管理部署时，您只需连接到 Web Studio 服务器。

本节指导您将 Web Studio 服务器配置为 Delivery Controller 的代理。我们假设 Web Studio 和 Delivery Controller 安装在不同的服务器上。

在开始之前，请验证您的部署中是否已安装所有必需的核心组件。有关详细信息，请参阅安装核心组件。

要为 Web Studio 启用代理模式，请执行以下步骤：

1. 在 Web Studio 服务器上，以管理员身份运行 Windows PowerShell。
2. 运行以下命令，其中将 `fqdn_of_webstudio_machine` 替换为 Web Studio 服务器的 FQDN。

`& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enableproxy --proxyserver "fqdn_of_webstudio_machine"`

> **注意：**
>
> 如果您有负载平衡的 Web Studio 部署，请将 `fqdn_of_webstudio_machine` 替换为负载平衡器服务器（也称为虚拟服务器）的 FQDN。有关详细信息，请参阅设置负载平衡的 Web Studio 部署。

要为 Web Studio 禁用代理模式，请运行此 PowerShell 命令：

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy
```

（可选）启用或禁用 Pendo

从版本 2411 开始，Web Studio 集成了 Pendo，默认情况下已启用。Pendo 按照Citrix 隐私策略 收集您的使用数据。它还在 Web Studio 的右下角添加了一个图标，为您提供上下文功能信息和反馈选项。如果您不想共享使用数据，可以使用 Studio 配置工具禁用 Pendo。

此工具位于 Web Studio 安装文件夹中。默认情况下，该工具安装在以下文件夹中：`C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`。

要禁用 Pendo，请执行以下步骤：

1. 登录 Web Studio。如果右下角出现图标，则表示 Pendo 已启用。
2. 在 Web Studio 服务器上，以管理员身份运行 Windows PowerShell。 运行此 PowerShell 命令：

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disablependo
```

要启用 Pendo，请运行此命令：

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enablependo
```

Web Studio 的安全服务器配置

将以下安全配置应用于托管 Web Studio 的服务器，以提高安全性。这些设置在服务器级别应用，而不是在 Web Studio 本身中应用。

禁用中等强度 SSL 密码 (SWEET32)

Web Studio 服务器可能使用中等强度密码 `TLS_RSA_WITH_3DES_EDE_CBC_SHA`，该密码容易受到 SWEET32 攻击。 要禁用该密码，请在 Web Studio 服务器上运行以下 PowerShell 命令：

```
Disable-TlsCipherSuite -Name TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

禁用已弃用的 TLS 1.0 和 1.1 协议

TLS 1.0 和 TLS 1.1 已弃用，不应在 Web Studio 服务器上启用。 要禁用它们：

1. 打开注册表编辑器 (`regedit.exe`)。
2. 转到 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocol`。
3. 如果以下子项不存在，请创建它们：
   - `TLS 1.0\Client`
   - `TLS 1.0\Server`
   - `TLS 1.1\Client`
   - `TLS 1.1\Server`
4. 在每个 `Client` 和 `Server` 键中，创建以下 `DWORD (32-bit)` 值：
   - `Enabled` = `0`
   - `DisabledByDefault` = `1`（可选但建议）
5. 重新启动服务器以应用更改。

登录 Web Studio

1. 如果使用默认端口号 443，请在 `https://<address of the server hosting Web Studio>/Citrix/Studio` 访问 Web Studio。如果配置了不同的端口，请使用 `https://<address of the server hosting Web Studio>:<port number>/Citrix/Studio`。

   如果您已将 Delivery Controller 添加到 Web Studio 并且它们可访问，则会出现登录页面。

   > **注意：**

> 在以下情况下，将显示**无法登录**页面：
>
> - 尚未为站点指定任何 Delivery Controller。系统会提示您添加一个以进行连接。
> - 指定的 Delivery Controller 不可达。单击 **测试** 以检查连接。或者，输入备用 Delivery Controller，然后单击 **连接**。

2. 输入 **用户名**、**密码** 和 **域**。
3. 单击 **登录**。

后续步骤

1. 安装 VDA
2. 使用 Web Studio 向用户交付虚拟应用程序和桌面，方法是：
   a. 创建计算机目录
   b. 创建交付组
   c. 创建应用程序组（可选）

使用命令行安装

> **重要提示：**
>
> - 如果您正在升级，并且当前版本使用或安装了 Personal vDisk 或 AppDisks 软件，请参阅删除 PvD、AppDisks 和不受支持的主机。
> - Citrix 会根据其合法权益（包括许可合规性）收集基本的许可数据。有关详细信息，请参阅 Citrix 许可数据。

简介

本文适用于在 Windows 操作系统计算机上安装组件。有关适用于 Linux 操作系统的 VDA 的信息，请参阅Linux Virtual Delivery Agent。

本文介绍了如何发出产品安装命令。在开始任何安装之前，请查看准备安装。该文章包含对可用安装程序的说明。

要查看命令执行进度和返回值，您必须是原始管理员或使用**以管理员身份运行**。有关详细信息，请参阅 Microsoft 命令文档。

作为直接使用安装命令的补充，产品 ISO 上提供了示例脚本，用于在 Active Directory 中的计算机上安装、升级或删除 VDA。有关详细信息，请参阅使用脚本安装 VDA。

如果您尝试在不受此 Citrix Virtual Apps and Desktops 版本支持的 Windows 操作系统版本上安装或升级，则会显示一条消息，引导您了解有关选项的信息。请参阅早期操作系统。

有关 Citrix 如何报告组件安装结果的信息，请参阅Citrix 安装返回代码。

使用完整产品安装程序

要访问完整产品安装程序的命令行界面：

1. 从 Citrix 下载产品包。访问下载站点需要 Citrix 帐户凭据。
2. 解压缩文件。或者，刻录 ISO 文件的 DVD。
3. 使用本地管理员帐户登录到要安装组件的服务器。
4. 将 DVD 插入驱动器或装载 ISO 文件。
5. 从介质上的 `\x64\XenDesktop Setup` 目录中，运行相应的命令。

   安装核心组件： 运行 `XenDesktopServerSetup.exe`，并使用 安装核心组件的命令行选项 中列出的选项。

   安装 VDA： 运行 `XenDesktopVDASetup.exe`，并使用 安装 VDA 的命令行选项 中列出的选项。

   安装 StoreFront： 在安装介质的 `x64 > StoreFront` 文件夹中运行 `CitrixStoreFront-x64.exe`。

   安装通用打印服务器： 请遵循 安装通用打印服务器的命令行选项 中的指导。

   安装联合身份验证服务： Citrix 建议使用图形界面。

   安装会话录制： 请遵循 会话录制 中的指导。

   安装工作区环境管理： 请遵循 工作区环境管理 中的指导。

   安装 Secure Private Access： 在安装介质的 `x64 > XenDesktop` Setup 文件夹中运行 `XenDesktopSPASetup.exe`。请遵循 安装 Secure Private Access 的命令行选项 中的指导。

安装核心组件的命令行选项

使用 `XenDesktopServerSetup.exe` 命令安装核心组件时，以下参数选项有效。有关选项的更多详细信息，请参阅 安装核心组件。

注意：

- 在使用用于安装核心组件的命令行选项时，请勿使用 `/exclude`。
- 如果您使用 `/components` 升级一个组件，则其他组件也可能会升级。这是为了避免不同组件之间潜在的兼容性问题。
- 如果您只想升级一个组件，请使用该组件的独立安装程序。请参阅 升级和迁移。

- **/ceipoptin** *ceipoptin* 等等.

  启用 Call Home 数据和客户体验改善计划 (CEIP) 数据的收集。有效值为：

  - `DIAGNOSTIC`：选择此值以启用 Citrix 许可收集 Call Home 数据。
  - `ANONYMOUS`：选择此值以启用 Citrix 许可收集未识别的 CEIP 数据（不识别用户）。
  - `NONE`：选择此值以禁用 Citrix 许可收集 CEIP 数据。

  有关 Call Home 数据收集的详细信息，请参阅 Citrix Licensing Call Home。

  有关 CEIP 数据收集的更多详细信息，请参阅 Citrix Licensing Customer Experience Improvement Program。

  有关 CEIP 数据的更多详细信息，请参阅 Citrix Licensing CEIP data elements。

  有关许可证服务器许可数据的更多详细信息，请参阅 Citrix Licensing Data。

- **/components** *组件 ...*

  逗号分隔的用于安装或删除的组件列表。有效值为：

  - `CONTROLLER`：控制器
  - `WEBSTUDIO`：工作室
  - `DESKTOPDIRECTOR`: 导向器
  - `LICENSESERVER`：Citrix 许可证服务器
  - `SECUREPRIVATEACCESS`: 安全专用访问

要仅安装 VDA 并排除其他 Citrix 组件的安装，请指定 /components vda。

使用 VDAWorkstationCoreSetup_xxxx.exe 安装程序时，此选项无效。该安装程序无法安装 Citrix Workspace 应用程序或其他 Citrix 组件。

如果省略此选项，则会安装所有组件（如果还指定了 `/remove` 选项，则会删除所有组件）。

（在 2003 之前的版本中，有效值包括 `STOREFRONT™`。对于 2003 及更高版本，请使用使用完整产品安装程序 中提到的专用 StoreFront 安装命令）。

- **/仅限先决条件**

  将仅安装所选组件的必备项。不会安装任何 Citrix 产品组件。

- **/configure_firewall**

  如果 Windows 防火墙服务正在运行，即使防火墙未启用，也会打开正在安装的组件使用的 Windows 防火墙中的所有端口。如果您使用的是第三方防火墙或没有防火墙，则必须手动打开端口。

- **禁用体验指标**

  阻止在安装、升级或删除过程中收集的分析数据自动上传到 Citrix。

- **/help** 或 **/h**

  显示命令帮助。

- **/ignore_hw_check_failure**

  允许 Delivery Controller 安装或升级继续，即使硬件检查失败（例如，由于 RAM 不足）。有关详细信息，请参阅硬件检查。

- **/ignore_site_test_failure**

  仅在 Controller 升级期间有效。通常，任何站点测试失败都会被忽略，升级会继续进行。如果省略（或设置为 false），任何站点测试失败都会导致安装程序失败，而不会执行升级。默认值 = false

  在升级期间，如果检测到不受支持的 SQL Server 版本，则此选项将被忽略。有关详细信息，请参阅检查 SQL Server 版本。

- **/installdir** ***目录***

  现有空目录，组件将安装在此处。默认值 = `c:\Program Files\Citrix`。

- **/日志路径** ***路径***

日志文件位置。指定的文件夹必须存在。安装程序不会创建它。默认值 = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  仅在安装 Director 时有效。禁用使用 Windows 远程协助的用户影子功能。

- **/noreboot**（禁止重新启动）

  防止安装后重新启动。（对于大多数核心组件，默认情况下不启用重新启动。）

- **/noresume**（禁止恢复）

  默认情况下，如果在安装过程中需要重新启动计算机，安装程序会在重新启动完成后自动恢复。要覆盖默认设置，请指定 `/noresume`。如果您必须重新装载介质或希望在自动化安装期间捕获信息，这会很有帮助。

- **/无SQL**

  防止在安装 Controller 的服务器上安装 Microsoft SQL Server Express。如果省略此选项，则会安装 SQL Server Express 作为站点数据库。

  此选项不影响用于本地主机缓存的 SQL Server Express LocalDB 的安装。

- **/quiet** 或 **/passive**

  安装期间不显示用户界面。安装过程的唯一证据在 Windows 任务管理器中。如果省略此选项，则会启动图形界面。

- **/删除**

  删除使用 `/components` 选项指定的核心组件。

- **/删除所有**

  删除所有已安装的核心组件。

- **/发送体验指标**

  自动将安装、升级或删除期间收集的分析数据发送给 Citrix。如果省略此选项（或指定了 `/disableexperiencemetrics`），则分析数据将在本地收集，但不会自动发送。

- **/临时目录** *目录*

  安装期间用于存放临时文件的目录。默认值 = `c:\Windows\Temp`。

- **/Xen应用**

  安装 Citrix Virtual Apps。如果省略此选项，则安装 Citrix Virtual Apps and Desktops™。

安装核心组件的示例

以下命令在服务器上安装 Delivery Controller™、Studio、Citrix Licensing 和 SQL Server Express。组件通信所需的防火墙端口将自动打开。

`\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,webstudio,licenseserver /configure_firewall`

以下命令在服务器上安装 Citrix Virtual Apps™ Controller、Studio 和 SQL Server Express。组件通信所需的防火墙端口将自动打开。

`\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components controller,webstudio /configure_firewall`

以下命令在服务器上安装 Delivery Controller、Secure Private Access 和 SQL Server Express。组件通信所需的防火墙端口将自动打开。

`\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall`

如果您从 Citrix Virtual Apps and Desktops 2407 版升级到 2411 或更高版本，或者执行 2411 或更高版本的新安装，请首先将许可证服务器更新到最新版本（版本 11.2.17 build 51000）。然后，升级 Delivery Controller。否则将导致命令行安装和升级失败。运行以下命令以升级许可证服务器和 Delivery Controller、Studio 和 Citrix Director 等组件（假设您位于已装载 ISO 中的 \x64 文件夹内）。

1. 运行以下命令：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   如果您已将许可二进制文件复制到任何本地驱动器，请运行以下命令：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. 运行以下命令：

   ```
   \x64\XenDesktop Setup\XenDesktopServerSetup.exe /components
   "CONTROLLER,WEBSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
   ```

使用独立 VDA 安装程序

访问下载站点需要 Citrix 帐户凭据。您必须在开始安装之前拥有提升的管理权限，或者使用**以管理员身份运行**。

1. 从 Citrix 下载相应的软件包：
   - 多会话操作系统虚拟投递代理：`VDAServerSetup_xxxx.exe`
   - 单会话操作系统虚拟投递代理：`VDAWorkstationSetup_xxxx.exe`
   - 单会话操作系统核心服务虚拟投递代理：`VDAWorkstationCoreSetup_xxxx.exe`
2. 要么先将文件从包中提取到现有目录，然后运行安装命令，要么直接运行包。

   要在安装文件之前提取它们，请使用 `/extract` 和绝对路径，例如 `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`。目录必须存在。否则，提取将失败。然后，在单独的命令中，使用本文中列出的有效选项运行相应的命令。

   - 对于 `VDAServerSetup_XXXX.exe`，运行 `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
   - 对于 `VDAWorkstationCoreSetup_XXXX.exe`，运行 `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
   - 对于 `VDAWorkstationSetup_XXXX.exe`，运行 `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

   要运行下载的包，请运行其名称：`VDAServerSetup.exe`、`VDAWorkstationSetup.exe` 或 `VDAWorkstationCoreSetup.exe`。使用本文中列出的有效选项。

如果您熟悉完整产品安装程序：

- 运行独立的 `VDAServerSetup.exe` 或 `VDAWorkstationSetup.exe` 安装程序，就像它是 `XenDesktopVdaSetup.exe` 命令一样，除了名称不同。
- `VDAWorkstationCoreSetup.exe` 安装程序有所不同，因为它支持其他安装程序可用选项的子集。

逗号分隔的用于安装或删除的组件列表。有效值为：

- `VDA`：虚拟投递代理
- `CSA`：Citrix 安全访问™ 客户端

- `PLUGINS`: 适用于 Windows 的 Citrix Workspace™ 应用程序
- `UPL`: Citrix 用户个性化层（仅适用于 WS VDA）
- `SRAGENT`: 会话录制代理
- `ASSISTANTAPP`: Citrix Assistant App（仅适用于 WS VDA）
- `CEAL`: Citrix 弹性应用分层（仅适用于 TS VDA）

要安装 VDA 和适用于 Windows 的 Citrix Workspace 应用程序，请指定 /components vda,plugins 或根本不指定任何组件。

从该版本开始，Citrix Device Trust、Citrix uberAgent 和 Citrix Workspace Environment Management™ (WEM) Agent 已集成到默认 VDA 安装中。这些组件作为 VDA 设置的一部分静默安装，不再作为单独的组件进行管理。

> **注意：**
>
> 如果在环境中检测到现有独立版本的 Citrix uberAgent®，安装程序将不会安装、升级或卸载它。
>
> 要仅安装 VDA 并排除安装其他 Citrix 组件，请指定 `/components vda`。

使用 VDAWorkstationCoreSetup_xxxx.exe 安装程序时，此选项无效。该安装程序无法安装 Citrix Workspace 应用程序或其他 Citrix 组件。

用于安装 VDA 的命令行选项

以下选项适用于以下一个或多个命令（安装程序）：`VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe` 和 `VDAWorkstationCoreSetup_xxxx.exe`。

有关选项的更多详细信息，请参阅 安装 VDA。

- ***/components*** *组件*\[,*组件*\]

  逗号分隔的用于安装或删除的组件列表。有效值为：

  - `VDA`: 虚拟投递代理
  - `PLUGINS`: 适用于 Windows 的 Citrix Workspace 应用程序
  - `CSA`: Citrix 安全访问客户端
  - `UPL`: Citrix 用户个性化层（仅适用于 WS VDA）

- `SRAGENT`：会话录制代理
- `ASSISTANTAPP`：Citrix Assistant App（仅适用于 WS VDA）
- `CEAL`：Citrix 弹性应用分层（仅适用于 TS VDA）

要安装 VDA 和适用于 Windows 的 Citrix Workspace 应用程序，请指定 `/components vda,plugins, CSA, UPL` 或根本不指定任何组件。如果未指定任何组件，则默认仅安装 VDA、SRAGENT 和 ASSISTANTAPP。

要仅安装 VDA 并排除安装 Citrix Workspace 应用程序和其他组件，请指定 `/components vda`。

此选项在使用 `VDAWorkstationCoreSetup_xxxx.exe` 安装程序时无效。该安装程序无法安装 Citrix Workspace 应用程序。

- **仅限先决条件**

  将仅安装所选组件的必备项。不会安装任何 Citrix 产品组件。

- **controllers** "*控制器* \[*控制器*\]"

  VDA 可以与之通信的 Controller 的 FQDN，以空格分隔，并用直引号括起来。请勿同时指定 `/site_guid` 和 `/controllers` 选项。

- **禁用体验指标**

  阻止自动上传在安装、升级或删除期间收集到 Citrix 的分析数据。

- **/enable_hdx_ports**

  如果检测到 Windows 防火墙服务，即使防火墙未启用，也会打开 VDA 和已启用功能（Windows 远程协助除外）所需的 Windows 防火墙中的端口。如果您使用的是其他防火墙或没有防火墙，则必须手动配置防火墙。有关端口信息，请参阅网络端口。

  要打开 HDX 自适应传输使用的 UDP 端口，除了此 `/enable_hdx_ports` 选项外，还请指定 `/enable_hdx_udp_ports` 选项。

- **/enable_hdx_udp_ports**

  如果检测到 Windows 防火墙服务，即使防火墙未启用，也会在 Windows 防火墙中打开 HDX 自适应传输使用的 UDP 端口。如果您使用不同的防火墙或不使用防火墙，则必须手动配置防火墙。有关端口信息，请参阅网络端口。

  要打开 VDA 使用的额外端口，除了此 `/enable_hdx_udp_ports` 选项外，还请指定 `/enable_hdx_ports` 选项。

- **/enable_hdx_tls_dtls**

为 HDX™ Direct V1 打开 TCP 和 UDP 端口 443。

- **/enable_real_time_transport**

  启用或禁用将 UDP 用于音频数据包（用于音频的实时音频传输）。启用此功能可以提高音频性能。如果希望在检测到 Windows 防火墙服务时自动打开 UDP 端口，请包含 `/enable_hdx_ports` 选项。

- **/enable_remote_assistance**

  启用 Windows 远程协助中的影子功能，以便与 Director 结合使用。如果指定此选项，Windows 远程协助将在防火墙中打开动态端口。

- **/enablerestore** 或 **/enablerestorecleanup**

  （仅适用于单会话 VDA）如果 VDA 安装或升级失败，则启用自动返回到还原点。

  如果安装/升级成功完成：

  - `/enablerestorecleanup` 指示安装程序删除还原点。
  - `/enablerestore` 指示安装程序保留还原点，即使未使用该还原点。

  有关详细信息，请参阅安装或升级失败时恢复。

- **/ENABLE_SECURE_DEFAULTS**

  将各种功能的默认设置从启用更改为禁用，以实现更安全的开箱即用配置。相关功能包括：客户端驱动器重定向、特殊文件夹重定向、拖放、客户端 TWAIN 设备重定向、客户端 USB 即插即用设备重定向、客户端打印机重定向、客户端剪贴板重定向和客户端麦克风重定向。

- **/enable_ss_ports**

  如果在检测到 Windows 防火墙服务时，即使防火墙未启用，也会打开 Windows 防火墙中屏幕共享所需的端口。如果您使用不同的防火墙或不使用防火墙，则必须手动配置防火墙。

- **/SKIPHDXDRIVERCHECK**

  跳过对 VDA 元安装程序中 HDX™ 驱动程序的检查。

- **/排除** “*组件*”

  阻止安装一个或多个用逗号分隔的可选组件，每个组件都用直引号括起来。例如，在不受 MCS 管理的映像上安装或升级 VDA 不需要计算机身份服务组件。有效值如下：

多会话操作系统	单会话操作系统	单会话操作系统核心服务
Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in
Citrix Backup and Restore	Citrix Backup and Restore	Citrix Browser Content Redirection
Citrix deviceTRUST®	Citrix deviceTRUST	Citrix deviceTRUST
uberAgent®	uberAgent	uberAgent
Citrix Secure Access Client	Citrix Secure Access Client	Citrix Secure Access Client
Citrix Workspace Environment Management™ Agent	Citrix Workspace Environment Management Agent	Citrix Workspace Environment Management Agent
Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Personalization for App-V - VDA
Citrix MCS IODriver	Citrix MCS IODriver	Citrix Telemetry Service
Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA	Citrix Universal™ Print Client
Citrix Profile Management	Citrix Profile Management	Citrix Vda Log Capture Service
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in	CSE Component
Citrix Rendezvous V2	Citrix Rendezvous V2	Director VDA Plug-in
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in

多会话操作系统	单会话操作系统	单会话操作系统核心服务
`Citrix Vda Log Capture Service`	`Citrix Vda Log Capture Service`	`VDA WMI Proxy Plug-in`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`	
`CSE Component`	`CSE Component`	
`Director VDA Plug-in`	`Director VDA Plug-in`	
`Machine Identity Service`	`Machine Identity Service`	
`Machine Management Provider`	`Machine Management Provider`	
`VDA Monitor Plug-in`	`User Personalization Layer`	
`VDA WMI Proxy Plug-in`	`VDA Monitor Plug-in`	
	`VDA WMI Proxy Plug-in`	
`Citrix App Protection Component`	`Citrix App Protection Component`	`Citrix App Protection Component`
`Citrix HyperV Filter Driver`	`Citrix HyperV Filter Driver`	
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Session Recording Agent`	`Session Recording Agent`	
`Elastic App Layering`	`Citrix Assistant App`	

将 Citrix Profile Management 从安装中排除 (`/exclude "Citrix Profile Management"`) 会影响使用 Citrix Director 对 VDA 进行监视和故障排除。在“**用户详细信息**”和“**端点**”页面上，“个性

化”面板和“登录持续时间”面板将失败。在“**控制板**”和“**趋势**”页面上，“平均登录持续时间”面板仅显示已安装 Profile Management 的计算机的数据。

即使您使用的是第三方用户配置文件管理解决方案，Citrix 仍建议您安装并运行 Citrix Profile Management Service。不需要启用 Citrix Profile Management Service。

如果同时指定 `/exclude` 和 `/includeadditional` 且组件名称相同，则不会安装该组件。

使用 `VDAWorkstationCoreSetup.exe` 安装程序时，此选项无效。该安装程序会自动排除其中许多项目。

- **/h** 或 **/help**

  显示命令帮助。

- **/includeadditional** "*组件*"\[,"*组件*"\]

  包括安装一个或多个用直引号括起来的逗号分隔的可选组件。当您创建远程电脑访问部署并希望安装默认情况下不包含的其他组件时，此选项会很有帮助。有效值如下：

多会话操作系统	单会话操作系统
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

如果同时指定 `/exclude` 和 `/includeadditional` 且组件名称相同，则不会安装该组件。

- **/installdir** *目录*

  将安装组件的现有空目录。默认值 = `c:\Program Files\Citrix`。

- **/install_mcsio_driver**

  请勿使用。请改用 `/includeadditional "Citrix MCS IODriver"` 或 `/exclude "Citrix MCS IODriver"`。

- **/logpath** *路径*

  日志文件位置。指定的文件夹必须存在。安装程序不会创建它。默认值 = "`%TEMP%\Citrix\XenDesktop Installer`"

  此选项在图形界面中不可用。

- **/主映像**

  仅在虚拟机上安装 VDA 时有效。将 VDA 设置为用于创建其他计算机的映像。此选项等同于 `/mastermcsimage`。

  使用 `VDAWorkstationCoreSetup_xxxx.exe` 安装程序时，此选项无效。

- **/MCS主映像**

  指定此计算机将用作 Machine Creation Services 的映像。此选项等同于 `/masterimage`。

- **/PVS主映像**

  指定此计算机将用作映像，通过 Citrix Provisioning™ 或第三方预配工具（例如 Microsoft System Center Configuration Manager）来预配 VM。

- **/websocket令牌** *WebSocket令牌*

  创建 Web Socket VDA。WebSocketToken 用于所需的令牌。

- **/websockettokenfile** *包含 WebSocket 令牌的文件*

  创建 Web Socket VDA。*FileContainingWebSockToken* 用于包含所需令牌的文件。

- **/websocket令牌stdin** <*WebSocket令牌*

  创建 Web Socket VDA。<*WebSocketToken* 用于通过 STDIN 传入的所需令牌。

- **/no_mediafoundation_ack**

  确认未安装 Microsoft Media Foundation，并且多个 HDX 多媒体功能将不会安装且无法工作。如果省略此选项且未安装 Media Foundation，则 VDA 安装将退出，因为未满足先决条件。大多

数受支持的 Windows 版本都已安装 Media Foundation，N 版本除外。如果*手动*启用“Windows 功能”>“媒体功能”，则 Citrix Meta Installer 查找的注册表项可能没有设置值。在开始安装过程之前，请检查 `SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` 注册表项以确认该值存在且不为空。

- **/nodesktopexperience**（不安装桌面体验）

  增强桌面体验功能不再可用。如果指定此选项（和策略设置），则会将其忽略。

  仅在为多会话操作系统安装 VDA 时有效。阻止启用增强桌面体验功能。此功能也通过增强桌面体验 Citrix 策略设置进行控制。

- **/noreboot**（禁止重新启动）

  阻止安装后重新启动。VDA 必须在重新启动后才能使用。

- **/noresume**（禁止恢复）

  默认情况下，如果在安装过程中需要重新启动计算机，安装程序会在重新启动完成后自动恢复。要覆盖默认设置，请指定 `/noresume`。如果您必须重新装载介质或希望在自动化安装期间捕获信息，这会很有帮助。

- **/物理机**

  将此参数与 `/remotepc` 一起用于 RemotePC 安装。否则，VDA 在某些用户场景中可能无法按预期运行。

- **/portnumber** *端口*

  仅当指定了 `/reconfig` 选项时有效。用于启用 VDA 与 Controller 之间通信的端口号。除非是端口 80，否则以前配置的端口将被禁用。

- **/proxyconfig** “*地址或 PAC 文件路径*”

  如果您计划在您的环境中使用 Rendezvous V2 协议以及 Gateway Service 等服务，并且您的网络中存在用于出站连接的非透明代理，请在此处指定代理。仅支持 HTTP 代理。用于 Rendezvous 协议的代理地址或 PAC 文件路径。此命令行会自动安装 Citrix Rendezvous V2，如同使用了 /includeadditional "Citrix Rendezvous V2"。有关功能详细信息，请参阅 Rendezvous 协议。

  - 代理地址格式：`http://<url-or-ip>:<port>`
  - PAC 文件格式：`http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** 或 **/passive**

安装期间不会出现用户界面。安装和配置过程的唯一证据在 Windows 任务管理器中。如果省略此选项，则会启动图形界面。

- **/重新配置**

  与 `/portnumber`、`/controllers` 或 `/enable_hdx_ports` 选项一起使用时，自定义以前配置的 VDA 设置。如果指定此选项但未同时指定 `/quiet` 选项，则会启动用于自定义 VDA 的图形界面。

- **/远程电脑**

  仅适用于远程 PC 访问部署（单会话操作系统）或代理连接（多会话操作系统）。不包括安装任何附加组件（请参阅带有 `/exclude` 和 `/includeadditional` 选项的组件列表）。

  使用 `VDAWorkstationCoreSetup.exe` 安装程序时，此选项无效。该安装程序会自动排除这些组件的安装。

  `/remotepc` 与 `/servervdi` 选项不兼容。

- **/删除**

  删除使用 `/components` 选项指定的组件。

- **/remove_appdisk_ack**

  授权 VDA 安装程序卸载 AppDisks™ VDA 插件（如果已安装）。

- **/remove_pvd_ack**

  授权 VDA 安装程序卸载 Personal vDisk（如果已安装）。

- **/删除所有**

  删除 VDA。它不会删除 Citrix Workspace 应用程序（如果已安装）。

- **/REMOVEALLWITHCWA**

  删除 CWA 以及 VDA。

- **/发送体验指标**

  在安装、升级或删除过程中自动将收集到的分析数据发送给 Citrix。如果省略此选项（或指定了 `/disableexperiencemetrics` 选项），则分析数据将在本地收集，但不会自动发送。

- **/服务器VDI**

  在受支持的 Windows 多会话计算机上安装用于单会话操作系统的 VDA。在 Windows 多会话计算机上安装用于多会话操作系统的 VDA 时，请省略此选项。

使用此选项之前，请参阅 Server VDI。

仅将此选项与完整产品 VDA 安装程序一起使用。

- **/站点GUID** *GUID*

  站点的 Active Directory 组织单位 (OU) 的全局唯一标识符。当您使用 Active Directory 进行发现时（自动更新是推荐的默认发现方法），这会将虚拟桌面与站点关联。站点 GUID 是 Studio 中显示的站点属性。请勿同时指定 `/site_guid` 和 `/controllers` 选项。

- **/临时目录** *目录*

  安装期间用于存放临时文件的目录。默认值 = `c:\Windows\Temp`。

  此选项在图形界面中不可用。

- **/虚拟机**

  仅在 VM 上安装 VDA 时有效。覆盖安装程序对物理机的检测，因为传递给 VM 的 BIOS 信息使其显示为物理机。

  此选项在图形界面中不可用。

- **/XenDesktop云**

  指示 VDA 安装在 Citrix DaaS (Citrix Cloud™) 部署中。

安装 VDA 的示例

使用完整产品安装程序安装 VDA：

以下命令将为单会话操作系统和 Citrix Workspace 应用程序安装 VDA 到 VM 上的默认位置。此 VDA 将用作映像并使用 MCS 预配 VM。VDA 将首先在域 `mydomain` 中名为 `Contr-Main` 的服务器上向 Controller 注册。VDA 将使用用户个性化层和 Windows 远程协助。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /
controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional
"user personalization layer" /mastermcsimage /enable_remote_assistance
```

使用 VDAWorkstationCoreSetup 独立安装程序安装单会话操作系统 VDA：

以下命令在单会话操作系统上安装核心服务 VDA，用于远程 PC 访问或 VDI 部署。Citrix Workspace 应用程序和其他非核心服务未安装。指定了 Controller 的地址，Windows 防火墙服务中的端口将自动打开。管理员将处理重新启动。

`VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot`

自定义 VDA

安装 VDA 后，您可以自定义多项设置。从产品介质上的 `\x64\XenDesktop Setup` 目录中，运行 `XenDesktopVdaSetup.exe`，使用以下一个或多个选项，这些选项在 安装 VDA 的命令行选项 中进行了描述。

- `/reconfigure`（自定义 VDA 时必需）
- `/h` 或 `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

排除 VDA 故障

- 在交付组的 Studio 显示中，**详细信息**窗格中的**已安装 VDA 版本**条目可能不是计算机上安装的版本。计算机的 Windows 程序和功能显示屏会显示实际的 VDA 版本。
- VDA 安装后，必须先向 Delivery Controller 注册，然后才能向用户交付应用程序或桌面。

  要了解 VDA 注册方法以及如何排查注册问题，请参阅 VDA 注册。

安装 Universal Print Server 的命令行选项

以下选项对 `XenDesktopPrintServerSetup.exe` 命令有效。

- **/enable_upsserver_port**

如果未指定此选项，安装程序将从图形界面显示**防火墙**页面。选择**自动**让安装程序自动添加 Windows 防火墙规则，或选择**手动**让管理员手动配置防火墙。

在打印服务器上安装软件后，请按照 Citrix Universal Print Server (UPS) 中的指导配置 Universal Print Server。

安装 Secure Private Access 的命令行选项

以下选项对两者均有效：

1. CVAD 安装程序：`XenDesktopSPASetup.exe`

2. SPA 本地安装程序：`SecurePrivateAccessSetup_XXXX.exe`

- **/enable_spa_ports**

  如果检测到 Windows 防火墙服务，即使防火墙未启用，也会打开 Secure Private Access 所需的 Windows 防火墙端口。如果您使用的是其他防火墙或没有防火墙，则必须手动配置防火墙。有关端口信息，请参阅 网络端口。

- **/无 SQL**

  阻止在安装 Secure Private Access 的服务器上安装 Microsoft SQL Server Express。如果省略此选项，则会安装 SQL Server Express 作为站点数据库使用。

- **/help 或 /h 或 /?**

  显示命令帮助

- **/noreboot**（禁止重新启动）

  阻止安装后重新启动。Secure Private Access 必须在重新启动后才能使用。

- **/quiet 或 /passive**

  安装期间不会出现用户界面。安装和配置过程的唯一证据在 Windows 任务管理器中。如果省略此选项，则会启动图形界面。

- **/删除**

  删除安全私有访问。

有关这些选项的更多详细信息，请参阅 Secure Private Access 安装程序。

更多信息

有关 Citrix 如何报告组件安装结果的信息，请参阅 Citrix 安装返回代码。

安装 VDA

> **重要提示：**
>
> - 如果您正在升级，并且当前版本安装了 Personal vDisk 或 AppDisks 软件，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/upgrade-migrate/preparation.html#remove-pvd-appdisks-and-unsupported-hosts)。

- Citrix® 分发的二进制文件现已签名。签名二进制文件表示它们已通过 Citrix 生成的证书或真实的第三方证书进行验证。

适用于 Windows 计算机的 VDA 有两种类型：适用于多会话操作系统的 VDA 和适用于单会话操作系统的 VDA。（有关适用于 Linux 计算机的 VDA 的信息，请参阅 (/zh-cn/linux-virtual-delivery-agent.html) 文档。）

在开始安装之前，请查看 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-prepare.html) 并完成所有准备任务。

在安装 VDA 之前，请安装核心组件。您也可以在安装 VDA 之前创建站点。

本文介绍了安装 VDA 时的安装向导序列。提供了命令行等效项。有关详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-core/install-command.html)。

步骤 1. 下载产品软件并启动向导

如果您使用的是完整产品安装程序：

1. 如果您尚未下载产品 ISO：
   - 使用您的 Citrix 帐户凭据访问 Citrix Virtual Apps and Desktops™ 下载页面。下载产品 ISO 文件。
   - 解压缩文件。或者，刻录 ISO 文件的 DVD。
2. 在要安装 VDA 的映像或计算机上使用本地管理员帐户。将 DVD 插入驱动器或装载 ISO 文件。如果安装程序未自动启动，请双击装载驱动器上的 **AutoSelect** 应用程序。

   安装向导启动。

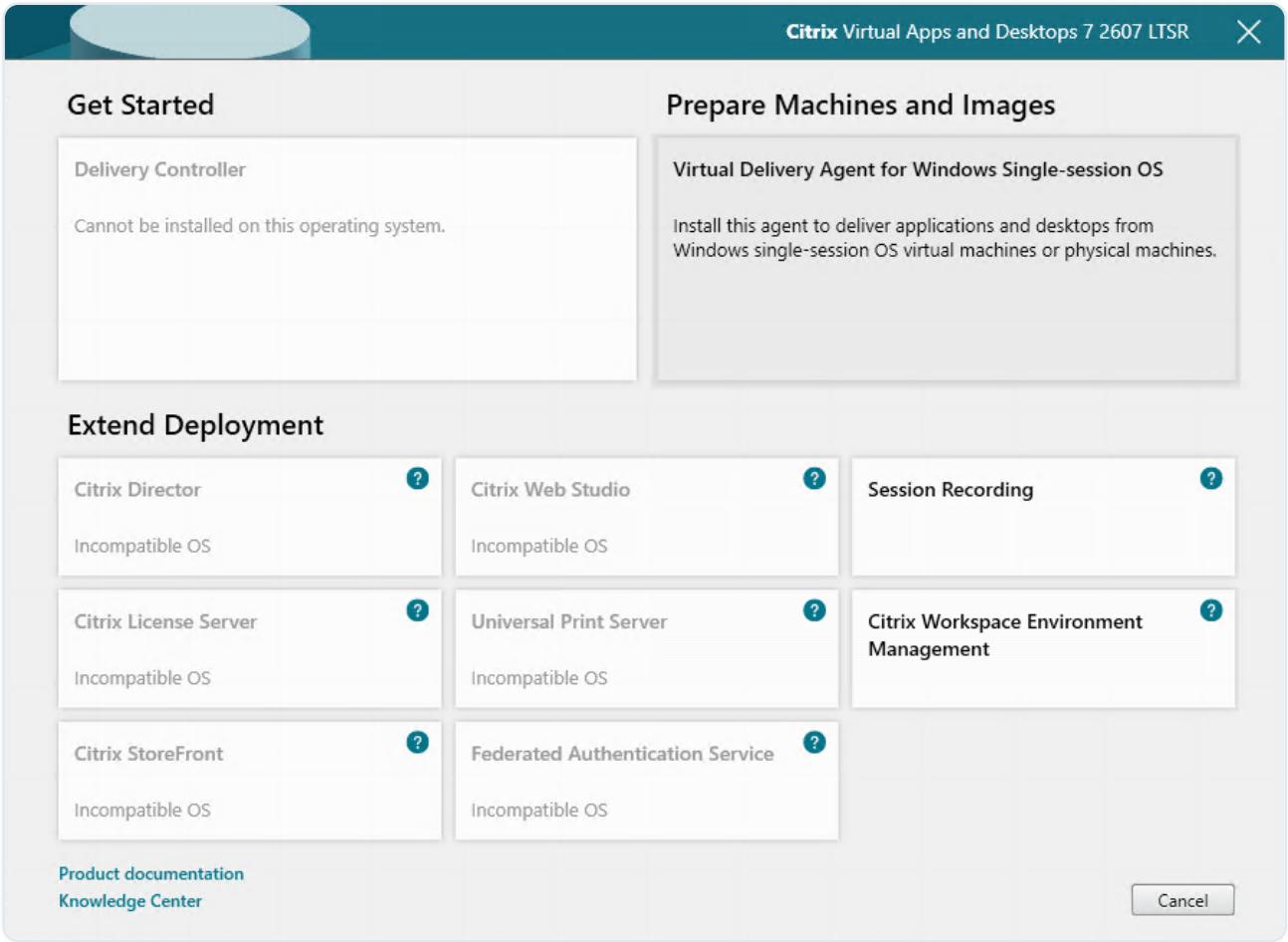
步骤 2. 选择要安装的产品

组件安装程序中的产品安装页面 (/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/product-selector2-75.png)

在要安装的产品（Citrix Virtual Apps 或 Citrix Virtual Desktops）旁边单击“**开始**”。（如果计算机已安装 Citrix Virtual Apps 或 Citrix Virtual Desktops 组件，则此页面不会出现。）

命令行选项：`/xenapp` 以安装 Citrix Virtual Apps。如果省略此选项，则安装 Citrix Virtual Desktops。

步骤 3. 选择 VDA



选择“**Virtual Delivery Agent**”条目。安装程序知道它是在单会话还是多会话操作系统上运行，因此它只提供适当的 VDA 类型。

例如，当您在 Windows Server 2019 计算机上运行安装程序时，适用于多会话操作系统的 VDA 选项可用。不提供适用于单会话操作系统的 VDA 选项。

如果您尝试在不受此 Citrix Virtual Apps and Desktops™ 版本支持的操作系统上安装（或升级到）Windows VDA，将显示一条消息，引导您了解有关选项的信息。

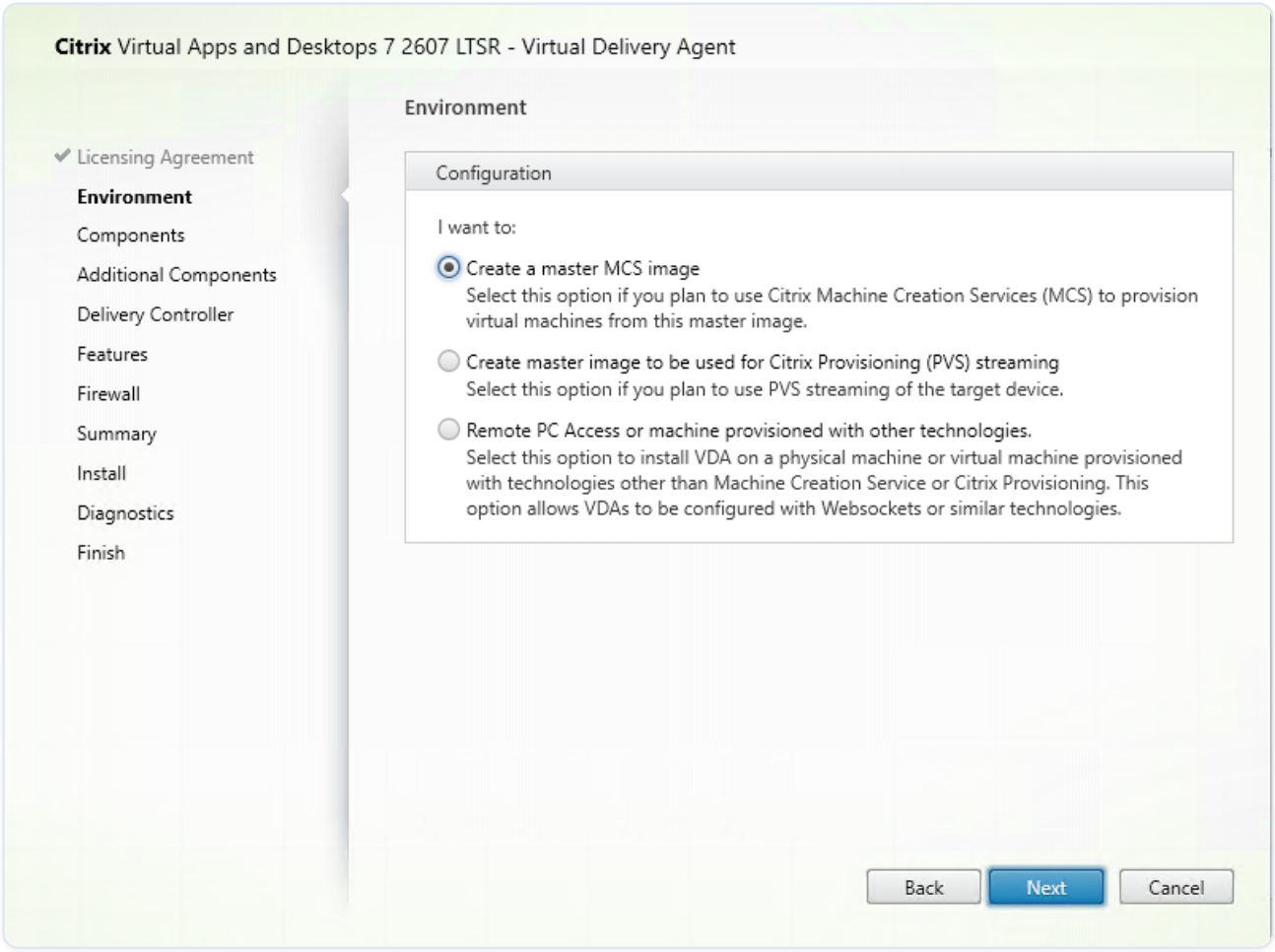
如果您使用的是独立软件包：

1. 使用您的 Citrix 帐户凭据访问 Citrix Virtual Apps and Desktops™ 下载页面。下载相应的软件包：
    - `VDAServerSetup_2607.exe`：多会话操作系统 VDA *版本*
    - `VDAWorkstationSetup_2607.exe`：单会话操作系统 VDA *版本*
    - `VDAWorkstationCoreSetup_2607.exe`：单会话操作系统核心服务 VDA *版本*
    - `VDASingleSessionCoreSetup_2607.exe`：新的单会话操作系统核心服务 VDA 版本

2. 右键单击软件包并选择“**以管理员身份运行**”。

   安装向导启动。

步骤 4. 指定 VDA 的使用方式



在“**环境**”页面上，指定您计划如何使用 VDA，并指明您是否将此计算机用作预配更多计算机的映像。

您选择的选项会影响自动安装哪些 Citrix Provisioning™ 工具（如果有），以及 VDA 安装程序“附加组件”页面上的默认值。

安装 VDA 时，会自动安装多个 MSI（预配及其他）。防止其安装的唯一方法是在命令行安装中使用 `/exclude` 选项。

选择以下选项之一：

- **创建主 MCS 映像：** 如果您计划使用 Machine Creation Services™ 预配 VM，请选择此选项以在 VM 映像上安装 VDA。此选项将安装 Machine Identity Service。这是默认选项。

  命令行选项：`/mastermcsimage` 或 `/masterimage`

> **重要提示：**
>
> 安装介质或 ISO 映像必须在本地装载。不支持从网络驱动器装载 ISO 映像以安装软件。

- **使用 Citrix Provisioning 或第三方预配工具创建主映像：** 如果您计划使用 Citrix Provisioning 或第三方预配工具（例如 Microsoft System Center Configuration Manager）预配 VM，请选择此选项以在 VM 映像上安装 VDA。

  命令行选项：`/masterpvsimage`

- （仅在多会话操作系统计算机上显示）**启用与服务器的代理连接：** 选择此选项可在物理或虚拟机上安装 VDA，该虚拟机不会用作预配其他计算机的映像。

  命令行选项：`/remotepc`

- （仅在单会话操作系统计算机上显示）**启用远程电脑访问：** 选择此选项可在物理计算机上安装 VDA，以用于远程电脑访问。

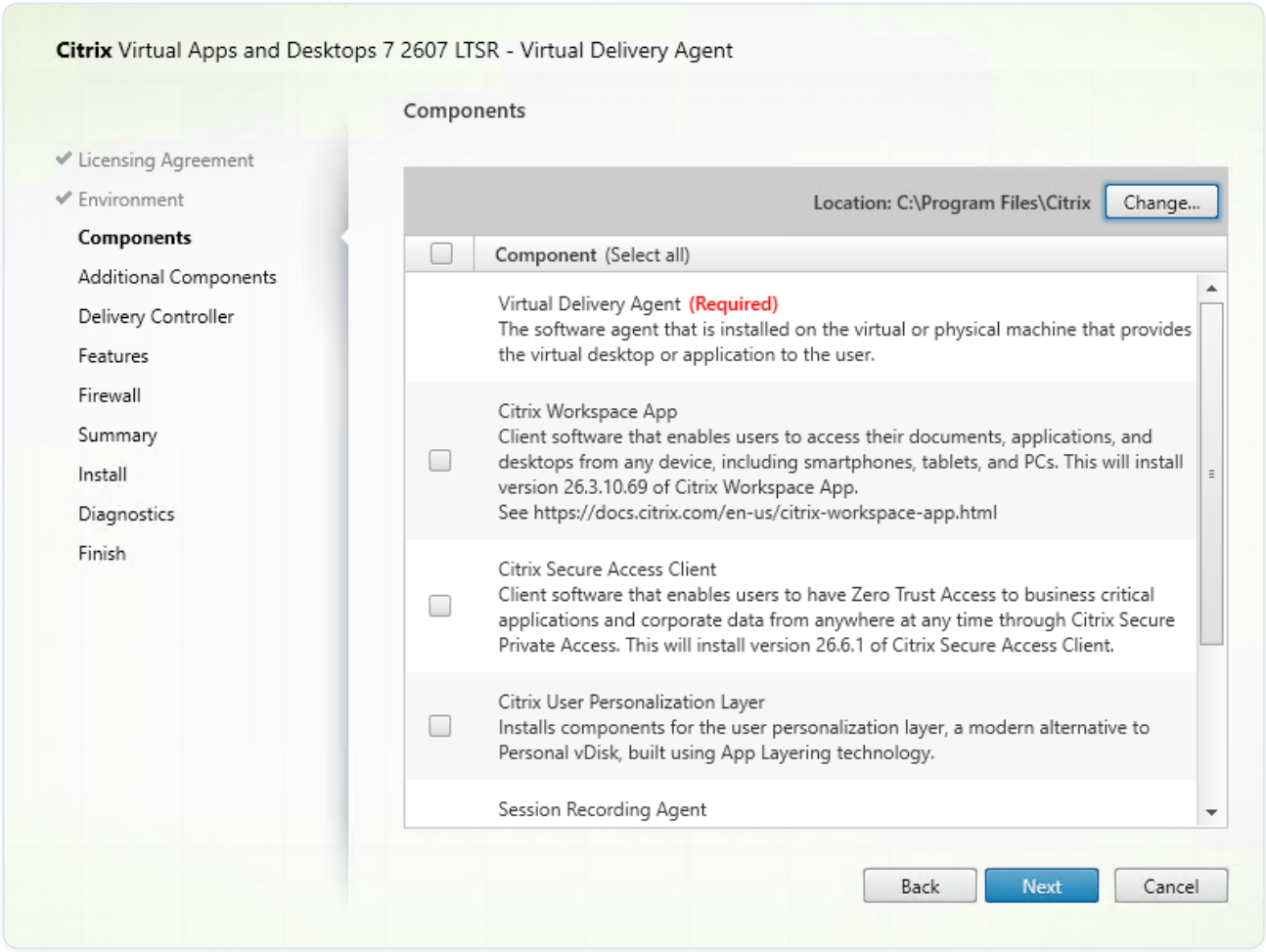
  命令行选项：`/remotepc`

单击“**下一步**”。

此页面不显示：

- 如果您正在升级 VDA
- 如果您使用的是 `VDAWorkstationCoreSetup_xxxx.exe`、`VDASingleSessionCoreSetup_xxxx.exe`、`VDAServerSetup_xxxx.exe` 或 `VDAWorkstationSetup_xxxx.exe` 安装程序

步骤 5. 选择要安装的组件和安装位置



> **注意：**
>
> 从版本 2603 开始，以前在“可选软件”页面上列出的组件已移至“组件”页面。

> 在**组件**页面上：

- **位置：** 默认情况下，VDA 安装在 `C:\Program Files\Citrix` 中。此默认设置适用于大多数部署。如果您指定不同的位置，则该位置必须具有网络服务的 `execute` 权限。
- **组件：** 默认情况下，会话录制代理和 Citrix Virtual Desktop Assistant 与 VDA 一起安装。如果您使用的是 `VDAWorkstationCoreSetup.exe` 安装程序或 `VDASingleSessionCoreSetup.exe` 安装程序，则只会安装 VDA，并且不会显示其他组件。

单击“**下一步**”。

命令行选项：`/installdir "C:\Program Files\VDA" /components "VDA","CSA","PLUGINS"` 用于将 Virtual Delivery Agent、Citrix Workspace Environment Management™ 代理、Citrix deviceTRUST、Citrix uberAgent、Citrix Secure Access Client 和 Citrix Workspace 应用程序安装到指定目录中。

注意：

在以下情况下，您可以在 VDA 安装、升级或卸载期间选择安装、升级或卸载 Citrix Workspace 应用程序和其他组件：

- 在 VDA 安装和升级到 2607 期间，您可以选择包含或排除组件和 CWA 插件。
  - 默认情况下，**Citrix Workspace 应用程序 (CWA)**、**Citrix Secure Access Client (CSA)**、**Citrix 用户个性化层 (UPL)（仅适用于 WS VDA）**和 **Citrix Elastic App Layering (CEAL)（仅适用于 TS VDA）**未选择安装，如果需要，您可以在安装期间选择它们。 **会话录制代理 (SRAGENT)** 和 **Citrix Virtual Desktop Assistant (ASSISTANTAPP)（现在在 TS VDA 和 WS VDA 上均可用）**默认选择安装，如果需要，您可以在安装期间取消选择它们。
  - **Citrix Device Trust**、**Citrix uberAgent** 和 **Citrix Workspace Environment Management™ 代理**现已与 VDA 集成并始终安装。为防止其安装，管理员必须使用受支持的 `/exclude` 命令行选项。**uberAgent** 也默认安装，从 VDA 2511 开始，以及在 2603 中，它无法通过 GUI 或命令行 (CLI) 从安装中排除。
  - 默认情况下，**Citrix Workspace Environment Management™ 代理**在**基本部署**中运行，这是一种功能有限的单机模式，不连接到 WEM 基础结构。要通过将代理连接到 Citrix Cloud 中的 WEM 服务或本地部署来启用完整的 WEM 功能，请通过组策略配置设置。有关详细信息，请参阅这篇 WEM 文章。
  - **Citrix 用户个性化层：** 安装用户个性化层的 MSI。有关详细信息，请参阅用户个性化层。
  - **命令行更改**

    `/components VDA,CSA`：此命令将安装 **VDA** 和 **CSA**（已选择），以及 **Citrix Device Trust**、**Citrix uberAgent** 和 **Citrix Workspace Environment Management agent**（默认集成）。

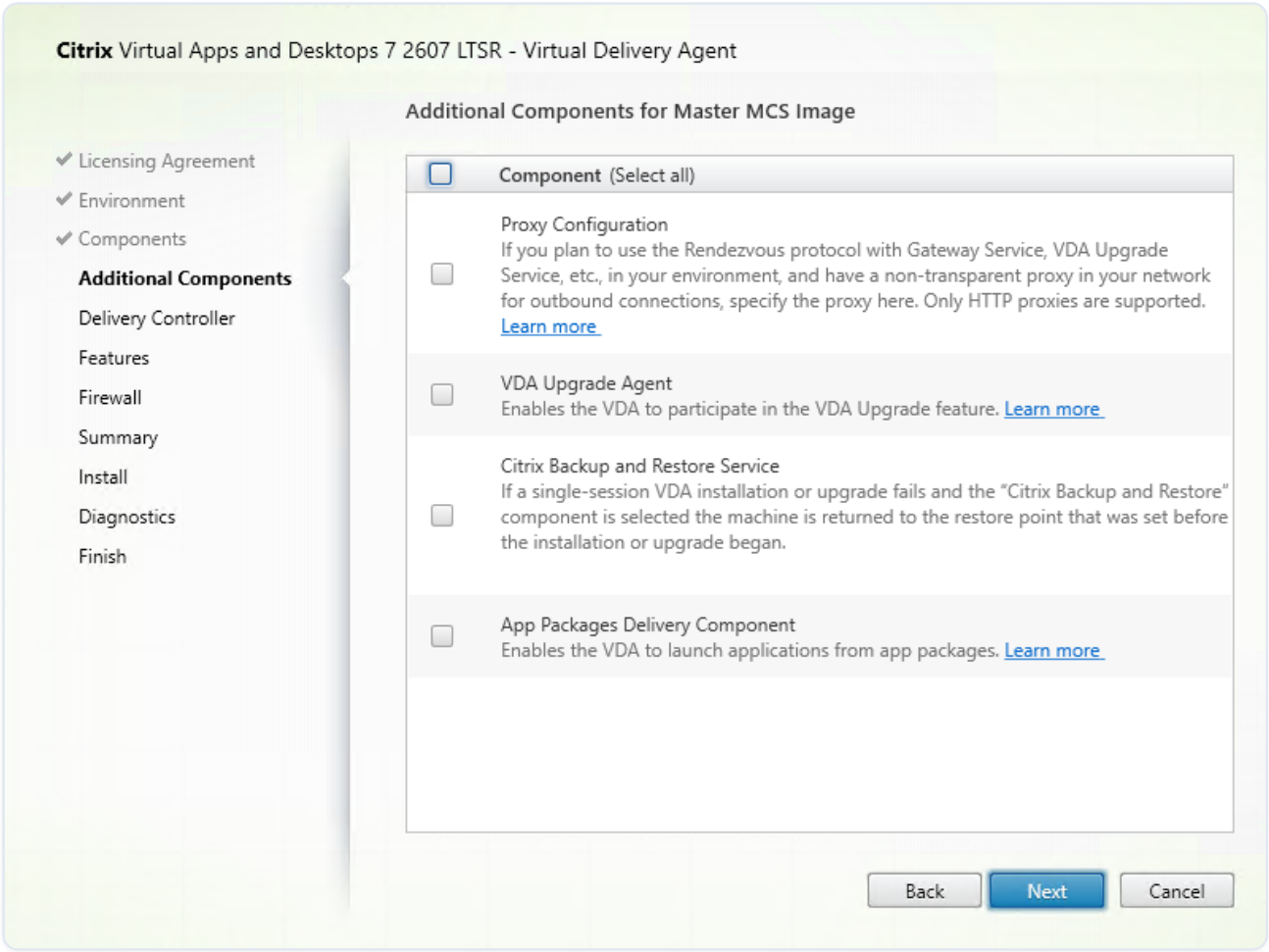
`/components VDA`：此命令将安装 **VDA**，以及 **Citrix Device Trust**、**Citrix uberAgent** 和 **Citrix Workspace Environment Management agent**，因为这些组件现已集成到 VDA 本身中。如果您将 Citrix Device Trust、Citrix uberAgent 和 Citrix Workspace Environment Management agent 指定为与 `/components` 选项一起使用的参数，则 VDA 元安装程序会记录一条通知，指示从 `/components` 选项中删除了这些参数。随后，VDA 元安装程序将继续安装或升级 VDA。

`/components`：此命令是无效命令，它必须始终包含 VDA。可以根据需要添加其他组件进行安装。

将 `/exclude` 命令用于默认集成组件：`/exclude` 选项始终优先。它可用于阻止安装默认集成组件。示例：`/exclude "Citrix Device Trust","Citrix Universal Print Client"`。此命令将安装包含 Citrix Workspace Environment Management agent 的 VDA，但不安装 Citrix Device Trust 和 Citrix Universal Print Client。

- 在 VDA 升级期间，如果 VDA 中尚未安装 Citrix Workspace app、Citrix Secure Access Client 和 Citrix 用户个性化层（仅适用于 WS VDA）、Session Recording Agent、Citrix Virtual Desktop Assistant 和 Elastic App Layering（仅适用于 TS VDA），则可以选择安装它们。
- 在 VDA 升级期间，如果已安装用户个性化层或 Elastic App Layering，则会将其选为“**必需**”，并升级该组件。
- 在 VDA 升级期间，如果 Citrix Workspace app 和其他已安装插件的版本可以升级，则会显示升级它们的选项。
- 在 VDA 卸载期间，您可以选择是否卸载 Citrix Workspace app (CWA) 和任何其他已安装的组件。默认情况下，除 CWA 之外的所有组件都会自动卸载。CWA 的处理方式不同，除非明确选择，否则不会将其删除。

步骤 6. 安装其他组件



"其他组件"页面包含用于启用或禁用随 VDA 安装其他功能和技术的复选框。在命令行安装中，可以使用 `/exclude` 或 `/includeadditional` 选项明确省略或包含一个或多个可用组件：

- **/includeadditional** "*组件*"\[,"*组件*"\] ...
- **排除** "*组件*"\[,"*组件*"\] ...

下表指示此页面上各项的默认设置。默认设置取决于您在**"环境"**页面上选择的选项。

附加组件页面	环境页面："带 MCS 的主映像"或"带 CITRIX PROVISIONING 的主映像"已选定	环境页面："启用与服务器的代理连接"（适用于多会话操作系统）或"远程电脑访问"（适用于单会话操作系统）已选定
应用程序包交付组件	未选定	未选定
Citrix VDA 升级代理	未选定	未选定
Citrix 备份和还原	未选定	未选定
Citrix 会合 V2	未选定	未选定

如果出现以下情况，此页面将不显示：

- 您正在使用 `VDAWorkstationCoreSetup.exe` 安装程序或 `VDASingleSessionCoreSetup.exe`。此外，附加组件的命令行选项不适用于该安装程序。
- 您正在升级 VDA，并且所有附加组件都已安装。如果某些附加组件已安装，则页面仅列出未安装的组件。

选中或清除以下复选框。（这些组件在安装程序中可能以不同的顺序显示。）

- **应用程序包交付组件**：如果您使用 Microsoft App-V 包中的应用程序，请安装此组件。有关详细信息，请参阅部署和交付 App-V 应用程序。

  命令行选项：`/includeadditional "App Packages Delivery Component"` 启用组件安装，`/exclude "App Packages Delivery Component"` 阻止组件安装。

- **Citrix Profile Management**：此组件管理用户配置文件中的用户个性化设置。有关详细信息，请参阅Profile Management。

  将 Citrix Profile Management 从安装中排除会影响使用 Citrix Director 对 VDA 进行的监视和故障排除。在**用户详细信息**和**端点**页面上，**个性化**面板和**登录持续时间**面板将失败。在**控制板**和**趋势**页面上，**平均登录持续时间**面板仅显示已安装 Profile Management 的计算机的数据。

  即使您正在使用第三方用户配置文件管理解决方案，Citrix 仍建议您安装并运行 Citrix Profile Management Service。不需要启用 Citrix Profile Management Service。

  命令行选项：`/includeadditional "Citrix Profile Management"` 启用组件安装，`/exclude "Citrix Profile Management"` 阻止组件安装。

- **Citrix Profile Management WMI 插件**：此插件在 WMI（Windows Management Instrumentation）对象中提供 Profile Management 运行时信息（例如，配置文件提供程序、配置文件类型、大小和磁盘使用情况）。WMI 对象向 Director 提供会话信息。

  命令行选项：`/includeadditional "Citrix Profile Management WMI Plug-in"` 启用组件安装，`/exclude "Citrix Profile Management WMI Plug-in"` 阻止组件安装。

> **注意：**

> 从 2507 LTSR 开始，**Citrix Profile Management** 和 **Citrix Profile Management WMI 插件**现在是 VDA 的一部分，并针对**主映像/MCS/PVS** 用例自动安装。对于**远程 PC** 用例，这些组件**默认不安装**。在所有情况下，已安装的组件都会自动升级。命令行行为与以前的版本保持不变。

- **VDA 升级代理**：仅适用于 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops service）部署。使 VDA 能够参与 VDA 升级功能。您可以使用该功能从管理控制台立即或在计划时间升级目录的 VDA。如果未安装此代理，您可以通过在计算机上运行 VDA 安装程序来升级 VDA。

  命令行选项：`/includeadditional "Citrix VDA Upgrade Agent"` 启用组件安装，`/exclude "Citrix VDA Upgrade Agent"` 阻止组件安装。

- **MCSIO 存储优化写入缓存**：安装 Citrix MCS I/O 驱动程序。有关详细信息，请参阅管理程序共享存储 和配置临时数据缓存。

  命令行选项：`/includeadditional "Citrix MCS IODriver"` 启用组件安装，`/exclude "Citrix MCS IODriver"` 阻止组件安装。

  > **注意：**
  >
  > 从版本 2607 开始，**用于存储优化的 MCSIO 写入缓存**现在是 VDA 的一部分，并针对 **Master Image/MCS** 用例自动安装。对于 **Remote PC** 用例，此组件**默认不安装**。在所有情况下，已安装的组件都会自动升级。命令行行为与以前的版本保持不变。

- **代理配置**： 如果您计划在环境中使用 Rendezvous 协议以及 Gateway Service、VDA 升级服务等，并且您的网络中存在用于出站连接的非透明代理，请在此处指定代理。仅支持 HTTP 代理。

  如果安装此组件，请在“**Rendezvous 代理配置**”页面上指定代理地址或 PAC 文件路径。有关功能详细信息，请参阅Rendezvous 协议。

  命令行选项：`/includeadditional "Citrix Rendezvous V2"` 启用组件安装，`/exclude "Citrix Rendezvous V2"` 阻止组件安装。

- **Citrix 备份和还原**： 如果 VDA 安装或升级失败，此组件可以将计算机恢复到安装或升级之前完成的备份。

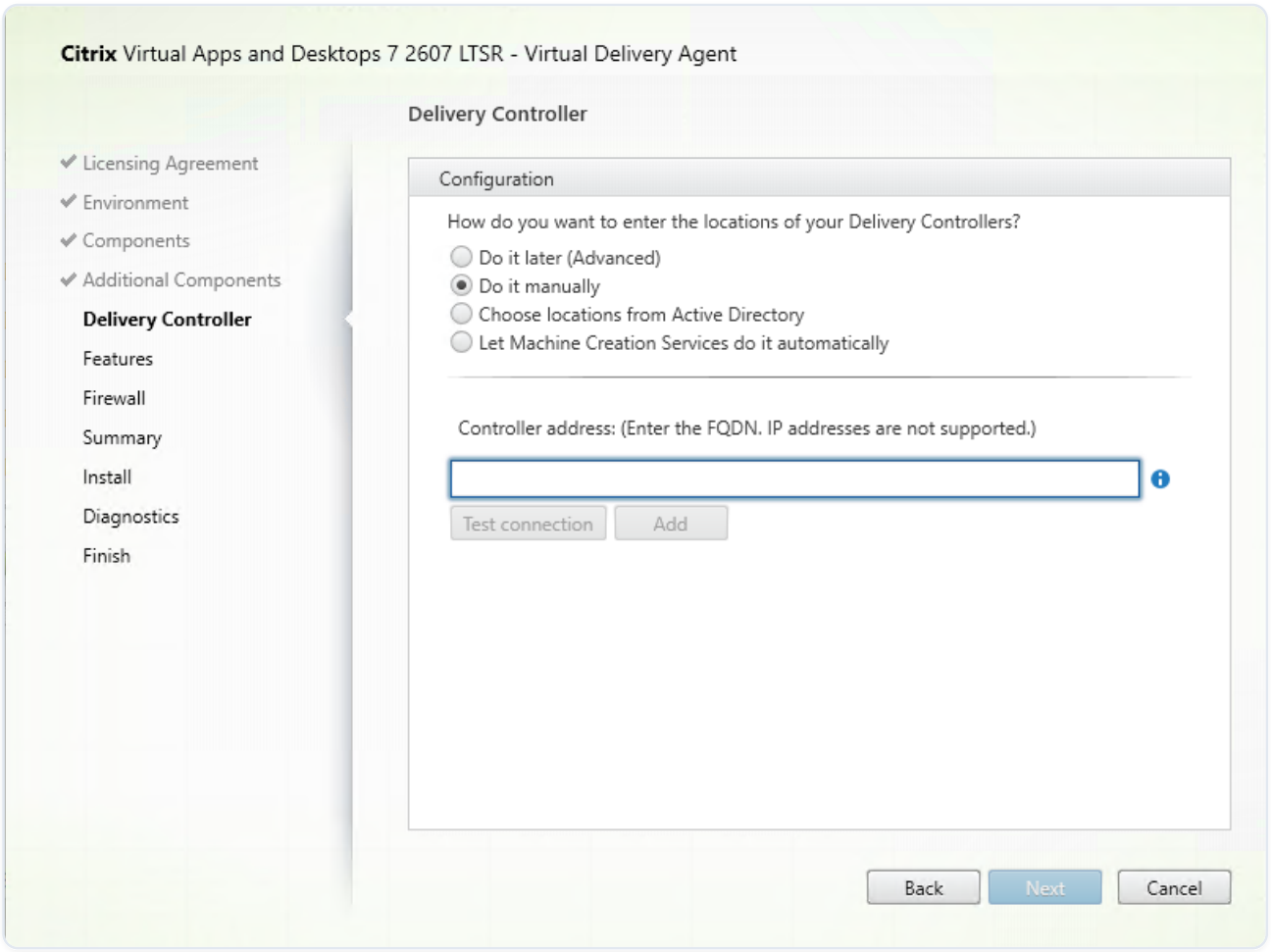
  确保满足 准备安装 中提到的 Microsoft 先决条件。

  命令行选项：`/includeadditional "Citrix Backup and Restore"` 启用组件安装，`/exclude "Citrix Backup and Restore"` 阻止组件安装。

  > **注意：**

> 从版本 2603 开始，Citrix 备份和还原组件仅适用于工作站 VDA。如果启用了 MCS 存储优化，则桌面操作系统的备份或还原可能会失败。要解决此问题，请在元安装程序中禁用 MCS 存储优化选项。

步骤 7. Delivery Controller™ 地址



在“**Delivery Controller**”页面上，选择输入已安装 Controller 地址的方式。Citrix 建议您在安装 VDA 时指定地址（**手动执行**）。VDA 必须拥有此信息才能向 Controller 注册。如果 VDA 无法注册，用户将无法访问该 VDA 上的应用程序和桌面。

- **手动执行：**（默认）输入已安装 Controller 的 FQDN，然后单击“**添加**”。如果您安装了更多 Controller，请添加它们的地址。
- **稍后执行（高级）：**如果选择此选项，向导会要求您在继续之前确认是否要执行此操作。要稍后指定地址，您可以重新运行安装程序或使用 Citrix 组策略。向导还会在“**摘要**”页面上提醒您。
- **从 Active Directory 中选择位置：**仅当计算机已加入域且用户是域用户时有效。
- **使用 WebSocket 令牌：**创建 WebSocket VDA。WebSocketToken 用于所需的令牌。
- **让 Machine Creation Services 自动执行：**仅在使用 MCS 预配计算机时有效。

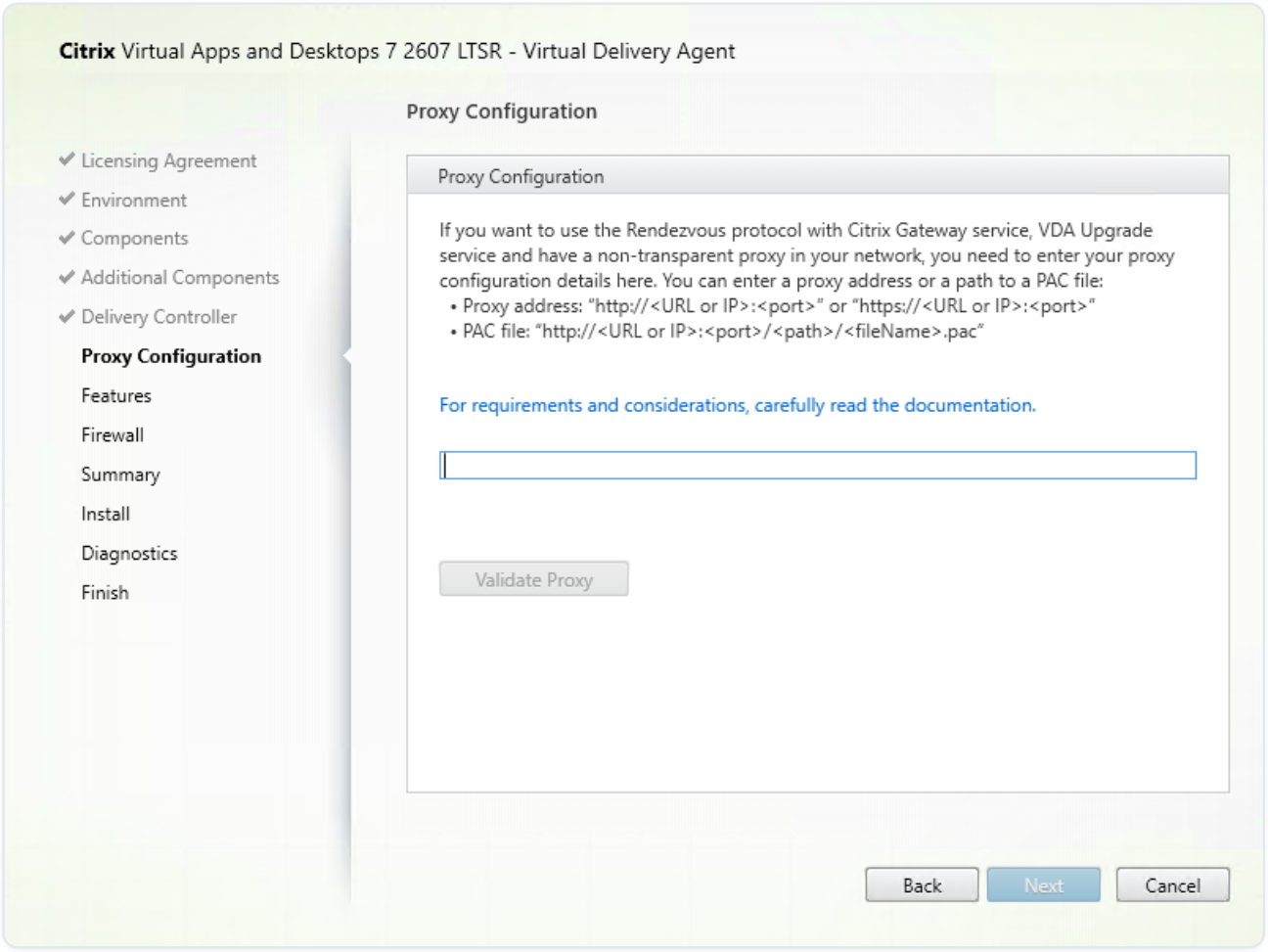
单击**下一步**。如果您选择了**稍后执行 (高级)**，系统会提示您确认稍后指定 Controller 地址。

其他注意事项：

- 地址不能包含非字母数字字符。
- 如果在 VDA 安装期间和组策略中指定地址，则策略设置将覆盖安装期间提供的设置。
- VDA 成功注册要求用于与 Controller 通信的防火墙端口处于打开状态。此操作在向导的**防火墙**页面上默认启用。
- 指定 Controller 位置（在 VDA 安装期间或之后）后，您可以使用自动更新功能在添加或删除 Controller 时更新 VDA。有关 VDA 如何发现 Controller 并向其注册的详细信息，请参阅VDA 注册。

命令行选项：`/controllers`

步骤 8. 代理配置



代理配置页面仅在您在**附加组件**页面上启用了**代理配置**复选框时显示。

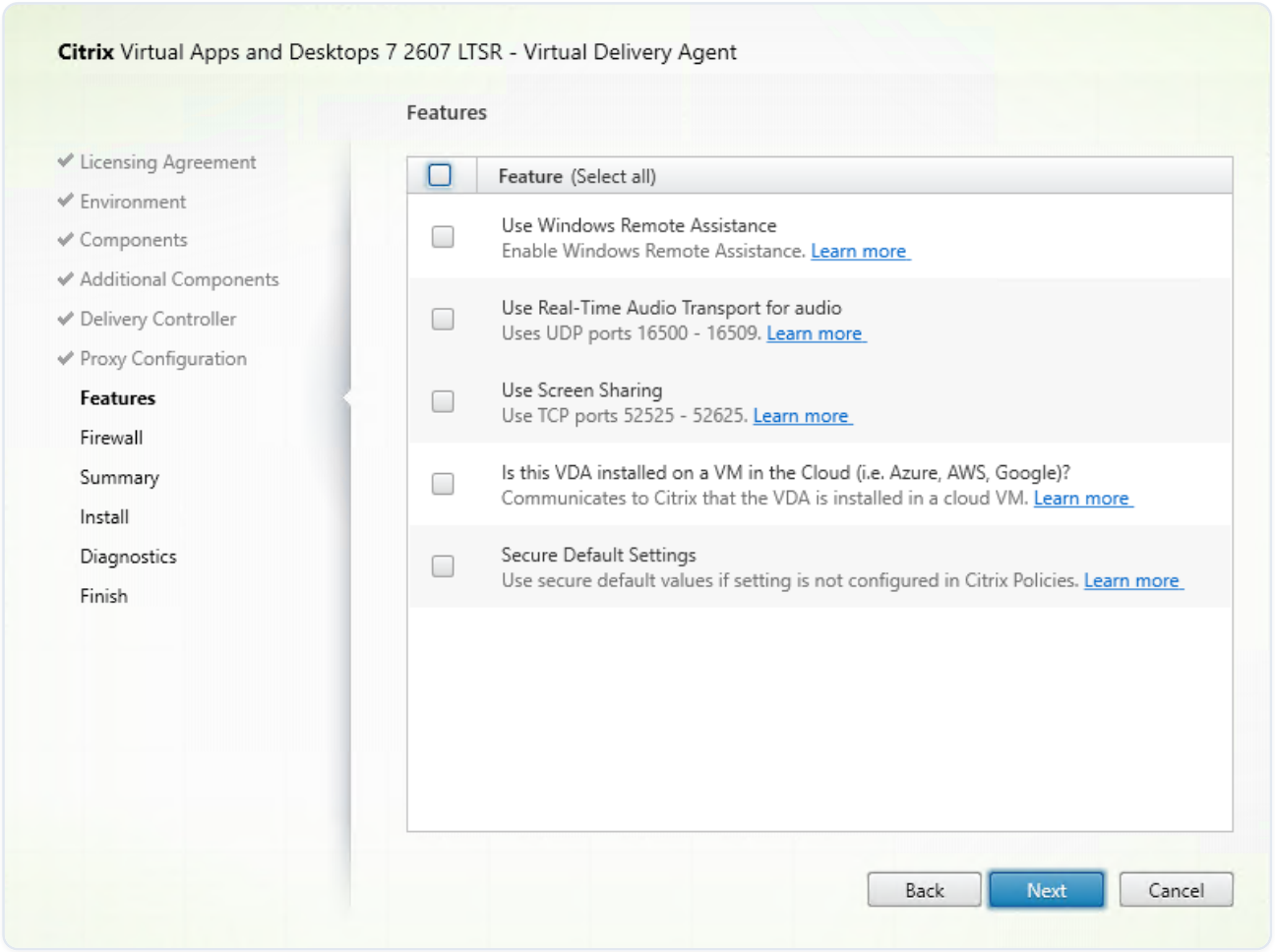
1. 选择是按代理地址还是 PAC 文件路径指定代理源。
2. 指定代理地址或 PAC 文件路径。

- 代理地址格式：`http://<url-or-ip>:<port>`
- PAC 文件格式：`http://<url-or-ip>:<port>/<path>/<filename>.pac`

代理端口的防火墙必须打开，连接测试才能成功。如果无法连接到代理，您可以选择是否继续 VDA 安装。

命令行选项：`/proxyconfig`

步骤 9. 启用或禁用功能



在**功能**页面上，使用复选框启用或禁用要使用的功能。

- **使用 Windows 远程协助：** 启用此功能后，Windows 远程协助将与 Director 的用户影子功能一起使用。Windows 远程协助会在防火墙中打开动态端口。（默认 = 禁用）

  命令行选项：`/enable_remote_assistance`
- **使用实时音频传输进行音频传输：** 如果您的网络中广泛使用 IP 语音，请启用此功能。此功能可降低延迟并提高音频在有损网络上的弹性。它允许使用 RTP over UDP 传输音频数据。（默认 = 禁用）

  命令行选项：`/enable_real_time_transport`

- **使用屏幕共享：** 启用后，屏幕共享使用的端口将在 Windows 防火墙中打开。（默认 = 禁用）

  命令行选项：`/enable_ss_ports`

- **此 VDA 是否安装在云中的 VM 上：** 此设置有助于 Citrix 正确识别本地和服务 (Citrix Cloud™) VDA 部署的资源位置，以用于遥测目的。此功能对客户侧利用率没有影响。如果您的部署使用 Citrix DaaS，请启用此设置（默认 = 禁用）。

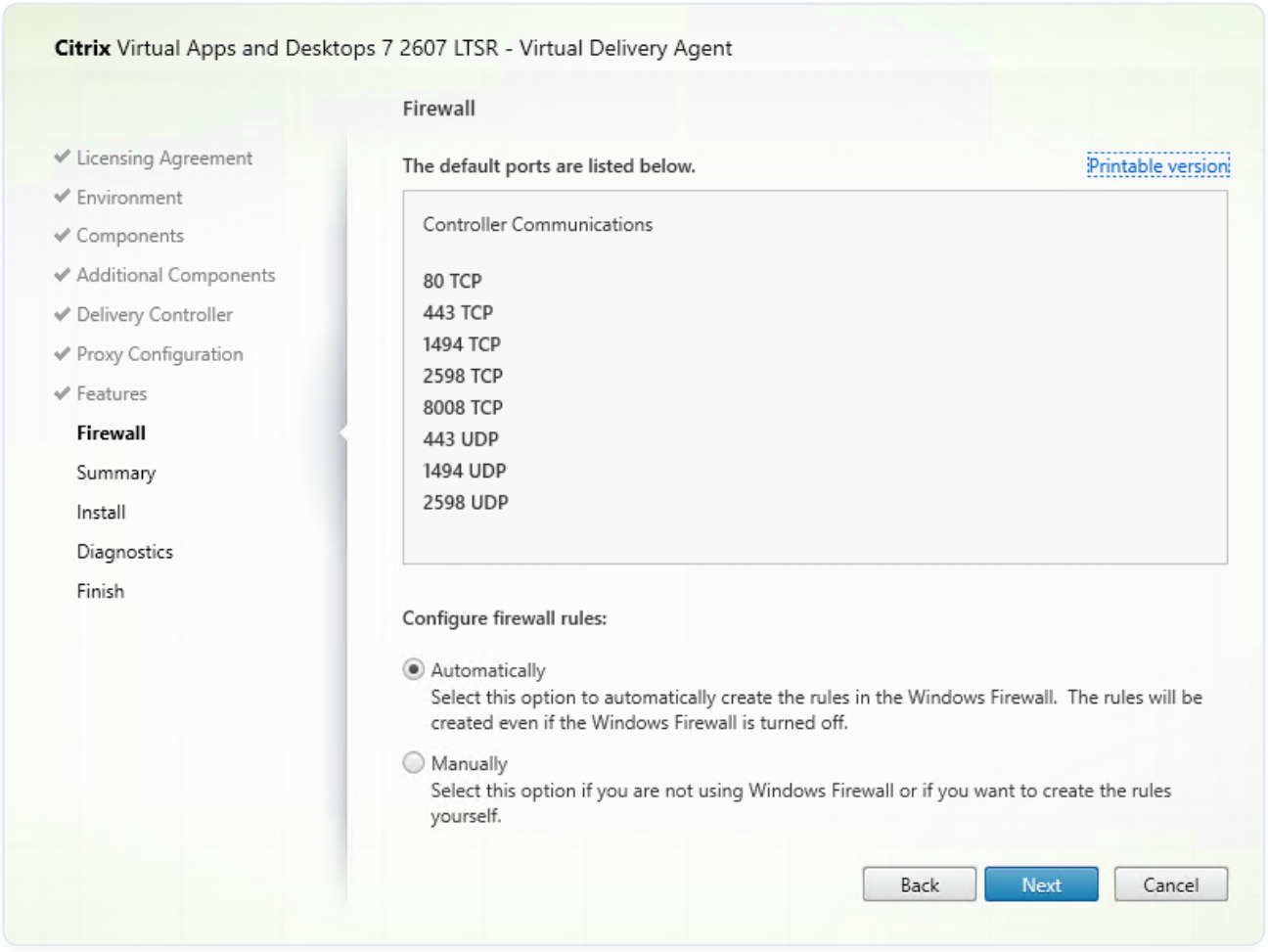
  命令行选项：`/xendesktopcloud`

- **安全默认设置：** 此选项将各种功能的默认设置从启用更改为禁用，以实现更安全的开箱即用配置。相关功能包括：客户端驱动器重定向、特殊文件夹重定向、拖放、客户端 TWAIN 设备重定向、客户端 USB 即插即用设备重定向、客户端打印机重定向、客户端剪贴板重定向和客户端麦克风重定向。

命令行选项：`/ENABLE_SECURE_DEFAULTS`

单击**下一步**。

步骤 10. 防火墙端口

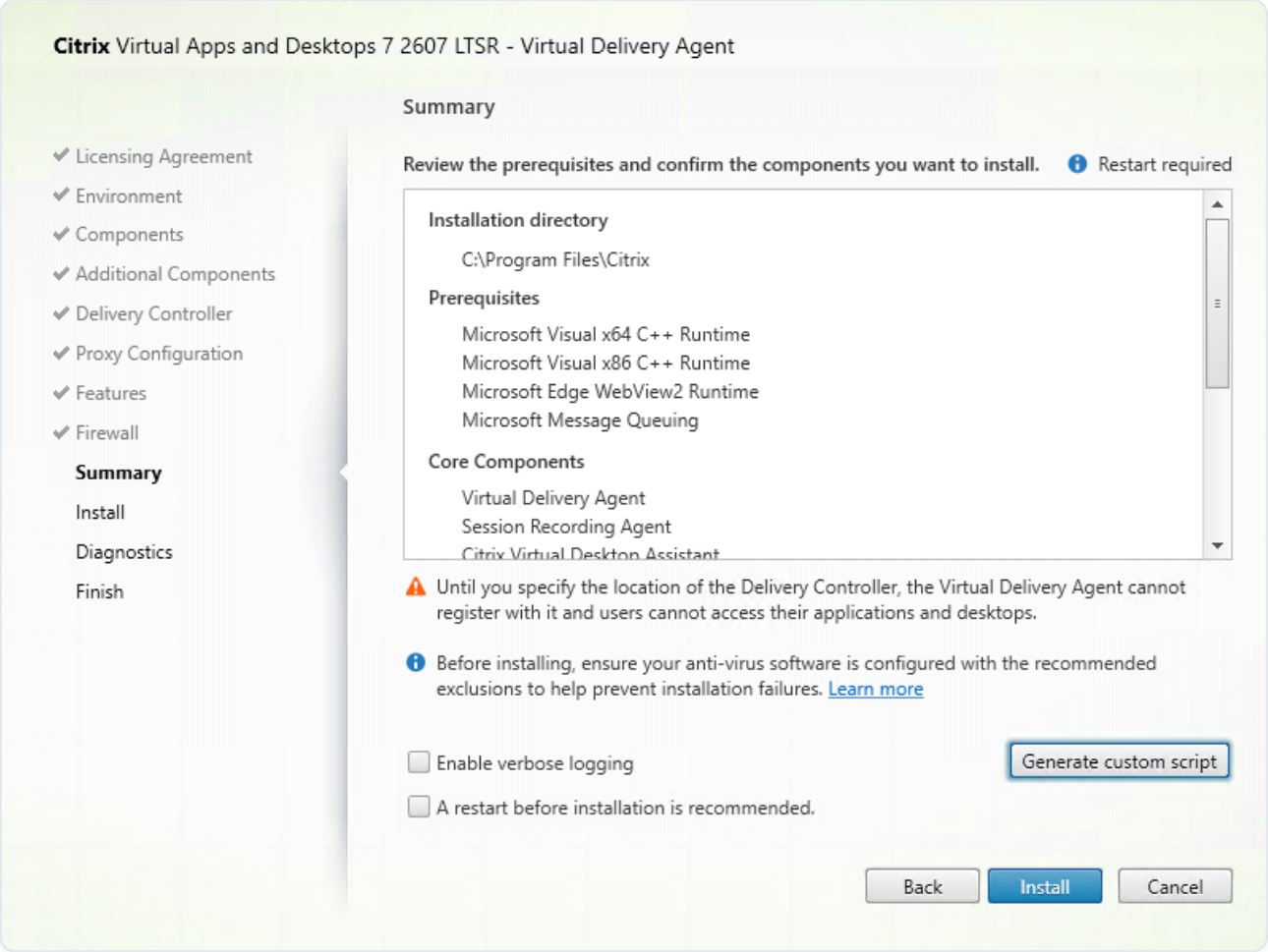


在“**防火墙**”页面上，默认情况下，如果 Windows 防火墙服务正在运行，即使防火墙未启用，端口也会自动打开。此默认设置适用于大多数部署。有关端口信息，请参阅网络端口。

单击**下一步**。

命令行选项：`/enable_hdx_ports`

步骤 11. 查看必备条件并确认安装



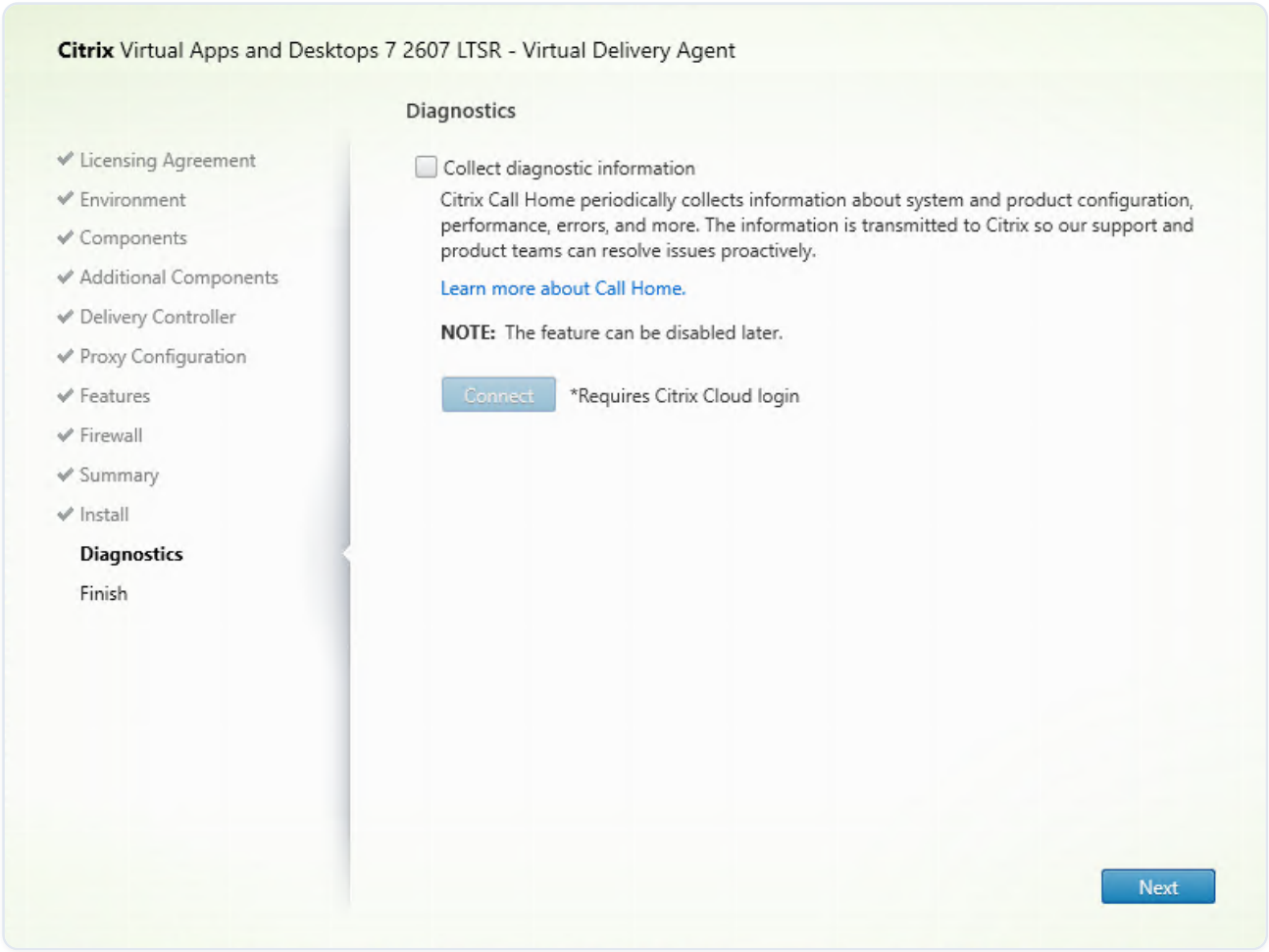
“**摘要**”页面列出了将要安装的内容。使用“**返回**”按钮返回到之前的向导页面并更改选择。

准备就绪后，单击“**安装**”。

如果尚未安装或启用必备条件，计算机可能会重启一次或多次。请参阅准备安装。

> **注意：**
>
> 此时，您还可以单击“**摘要**”页面上的“**生成自定义脚本**”按钮，根据您当前的安装选择创建命令行脚本。此脚本可以重复用于以无人参与模式安装或升级 VDA。

步骤 12. 诊断



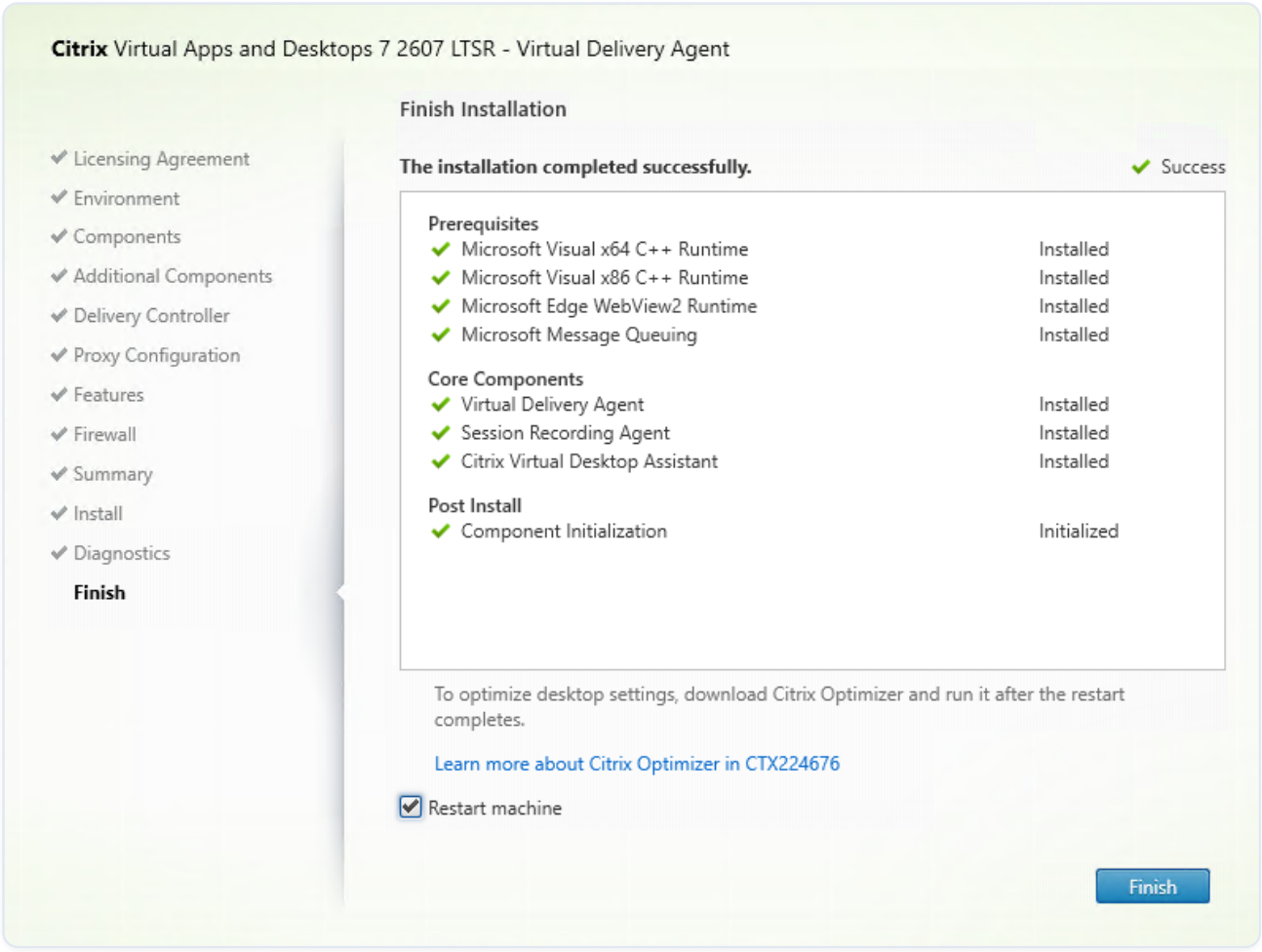
在“**诊断**”页面上，选择是否参与 Citrix Call Home。如果您选择参与（默认），请单击“**连接**”。出现提示时，输入您的 Citrix 帐户凭据。

凭据验证后（或者如果您选择不参与），单击“**下一步**”。

使用完整产品安装程序时，如果您在“**诊断**”页面上单击“**连接**”而未首先选择“**收集诊断信息**”，则在关闭“**连接到 Citrix Insight Services**”对话框后，“**下一步**”按钮将禁用。您无法移动到下一页。要重新启用“**下一步**”按钮，请选择并立即取消选择“**收集诊断信息**”。

有关详细信息，请参阅Call Home。

步骤 13. 完成此安装



完成页面包含所有已成功安装和初始化的先决条件和组件的绿色复选标记。

单击**完成**。默认情况下，计算机将自动重新启动。尽管您可以禁用此自动重新启动，但在计算机重新启动之前，VDA 无法使用。

后续步骤

如有需要，请重复上述步骤在其他计算机或映像上安装 VDA。

安装所有 VDA 后，启动 Studio。如果您尚未创建站点，Studio 会自动引导您完成该任务。完成该任务后，Studio 会引导您创建计算机目录，然后创建交付组。请参阅：

- 创建站点
- 创建计算机目录
- 创建交付组

Citrix 优化器

Citrix Optimizer 是一款适用于 Windows 操作系统的工具，可帮助 Citrix 管理员通过删除和优化各种组件来优化 VDA。

安装 VDA 并完成最终重新启动后，下载并安装 Citrix Optimizer。请参阅 CTX224676。该 CTX 文章包含下载包以及有关安装和使用 Citrix Optimizer 的说明。

自定义 VDA

要自定义已安装的 VDA：

1. 在 Windows 的“删除或更改程序”功能中，选择“**Citrix Virtual Delivery Agent**”或“**Citrix Remote PC Access/VDI Core Services VDA**”。然后右键单击并选择“**更改**”。
2. 选择**自定义 Virtual Delivery Agent 设置**。安装程序启动后，您可以更改：
   - Controller 地址
   - 用于向 Controller 注册的 TCP/IP 端口（默认值 = 80）
   - 是否自动打开 Windows 防火墙端口

故障排除

- 有关 Citrix 如何报告组件安装结果的信息，请参阅 Citrix 安装返回代码。
- 在交付组的 Studio 显示中，**详细信息**窗格中的**已安装的 VDA 版本**条目可能不是计算机上安装的版本。计算机的 Windows 程序和功能显示屏会显示实际的 VDA 版本。
- VDA 安装完成后，它无法向用户交付应用程序或桌面，直到它向 Delivery Controller 注册。

  要了解 VDA 注册方法以及如何排查注册问题，请参阅 VDA 注册。

已知限制

当您使用适用于 Windows 的 Citrix Workspace 应用程序 1912 或更早版本时，会话会在一段时间后断开。此问题已在较新的 LTSR 和 CR 版本的 Citrix Workspace 应用程序中修复。 有关支持的版本信息，请参阅 适用于 Windows 的 Citrix Workspace 应用程序 / 适用于 Windows 的 Citrix Receiver 长期服务版本。

配置与 VDA 安装相关的 Windows Defender 访问控制

客户配置 Windows Defender 访问控制 (WDAC) 设置以禁止加载未签名的二进制文件。因此，通过 VDA 安装程序分发的未签名二进制文件将被禁止，这会限制 VDA 安装。

Citrix® 现在使用 Citrix 代码签名证书对所有 Citrix 生成的二进制文件进行签名。此外，Citrix 还使用证书对随产品分发的第三方二进制文件进行签名，该证书将这些第三方二进制文件认证为受信任的二进制文件。

重要提示：

从包含未签名第三方二进制文件的旧 VDA 升级到包含已签名二进制文件的新 VDA 版本时，可能不会始终将已签名二进制文件放置在升级后的计算机上。 这是由于操作系统中的一种机制，即系统升级不会替换相同版本的二进制文件。 尽管第三方二进制文件已签名，但其版本由第三方控制，Citrix 无法更新，导致这些二进制文件未更新。为避免此限制：

1. 将二进制文件包含在允许列表中。这消除了对二进制文件进行签名的需要。
2. 卸载旧 VDA 并安装新 VDA。这类似于全新 VDA 安装，并且将安装已签名版本。

使用向导创建新基本策略

WDAC 允许您添加受信任的二进制文件以在您的系统上运行。安装 WDAC 后，**Windows Defender 应用程序控制策略向导**会自动打开。

要添加二进制文件，必须创建新的基本 WDAC 策略。本节提供了 Citrix 推荐的创建基本策略的指南。

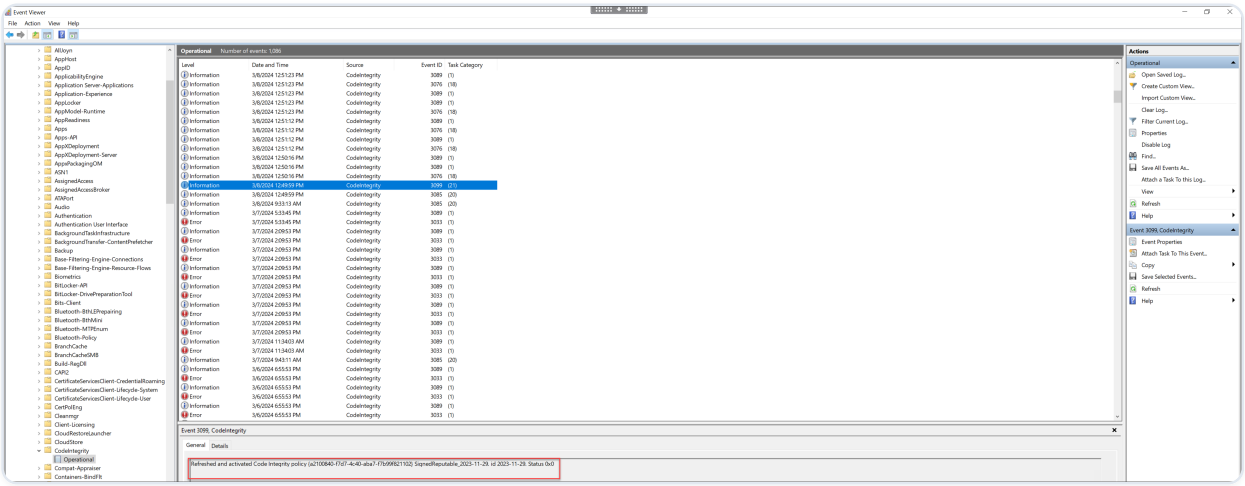
- 选择**签名和信誉模式**作为基本模板，因为它授权 Windows 操作系统组件、从 Microsoft Store 安装的应用程序、所有 Microsoft 签名的软件以及第三方 Windows 硬件兼容驱动程序。
- **启用审核模式**，因为它允许您在强制实施新的 Windows Defender 应用程序控制策略之前对其进行测试。
- 为**文件规则**添加**自定义规则**，以指定识别和信任应用程序的级别并提供参考文件。通过选择“发布者”作为规则类型，可以选择由 Citrix 证书之一签名的参考文件。
- 添加规则后，导航到保存 `.XML` 和 `.CIP` 文件的文件夹。`.XML` 文件包含策略中定义的所有规则。可以对其进行配置以更改、添加或删除任何规则。
- 在部署 WDAC 策略之前，必须将 `.XML` 文件转换为其二进制形式。WDAC 文件将 `.XML` 文件转换为 `.CIP` 文件。
- 将 `.CIP` 文件复制并粘贴到：C:\WINDOWS\System32\CodeIntegrity\CiPolicies\Active 并重新启动计算机。生成的策略将以审核模式应用。
- 有关创建基本策略的分步过程，请参阅使用向导创建新基本策略。

应用此策略后，WDAC 不会就由指定发布者/CA 机构签名的任何 Citrix 文件发出警告。

同样，我们可以为由第三方签名的文件创建发布者级别规则。

验证已应用的策略

1. 计算机重新启动后，打开**事件查看器**，然后转到**应用程序和服务日志 > Microsoft > Windows > CodeIntegrity > Operational**。
2. 确保已应用的策略已激活。



3. 查找违反策略的日志并检查该文件的属性。首先，确认它已签名。如果未签名且此计算机已进行 VDA 升级，则很可能是上述限制中描述的情况。如果已签名，则此文件可能已使用备用证书签名，如前所述。

使用 Citrix 证书签名的 Citrix 生成文件的示例如下：`C:\Windows\System32\drivers\picadm.sys`。使用 Citrix 第三方证书签名的第三方二进制文件的示例如下：`C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`。

VDA 安装和升级预检查

引入了一项解耦的 VDA 安装和升级预检，使客户能够在继续操作之前主动识别潜在问题。此检查会验证所有依赖项和先决条件，为每个条件提供明确的通过/失败状态。如果发生任何故障，将提供包含具体建议的详细补救指南。实际的安装或升级过程是独立的，并且必须在预检查完成后手动启动。

本文概述了执行 VDA 安装和升级预检查的步骤。

步骤 1. 运行命令行

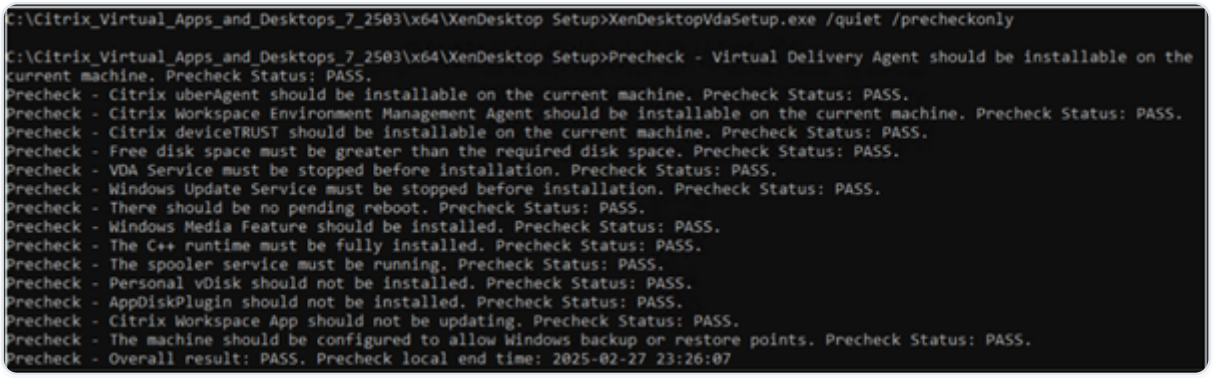
> **注意：**

- 预检查仅支持命令行模式。
- 运行此命令时不会启动安装或升级。

要执行预检查，请将 `/precheckonly` 选项添加到您常用的安装或升级命令中。将检查 VDA 安装或升级的所有预检查条件。

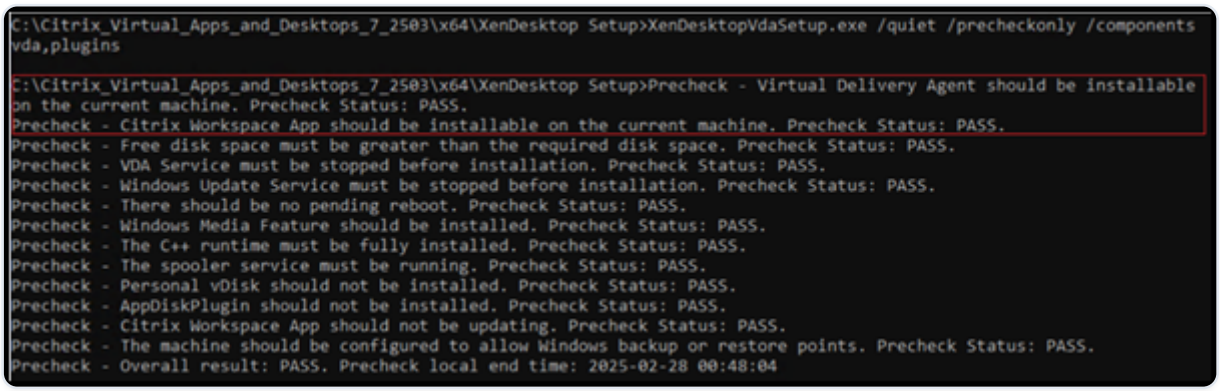
执行默认安装和升级的预检查

运行以下命令以执行预检查并确保计算机状态处于可接受状态： `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly`



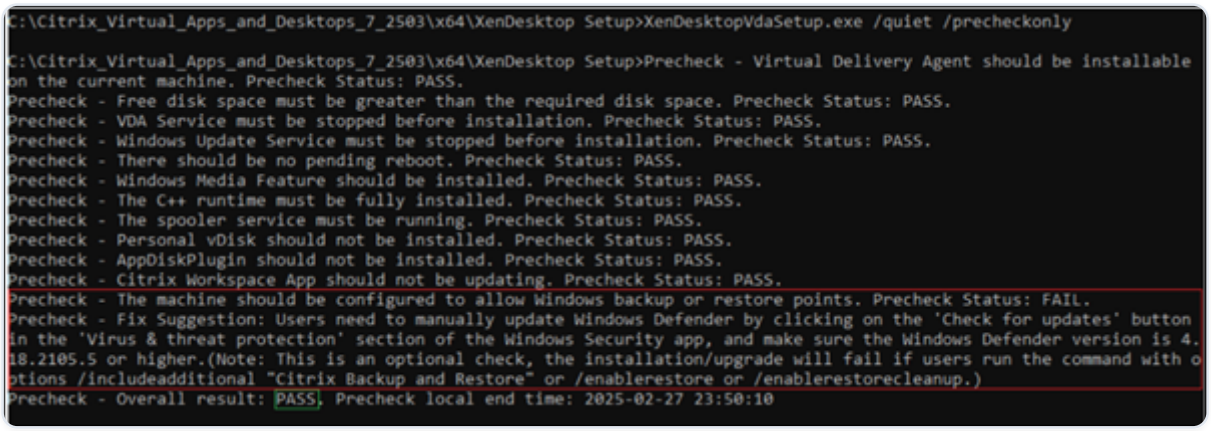
执行指定组件的安装和升级预检查

要在安装或升级之前检查特定组件的先决条件，请将 `/precheckonly` 添加到您的命令中。 `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /components vda,plugins`



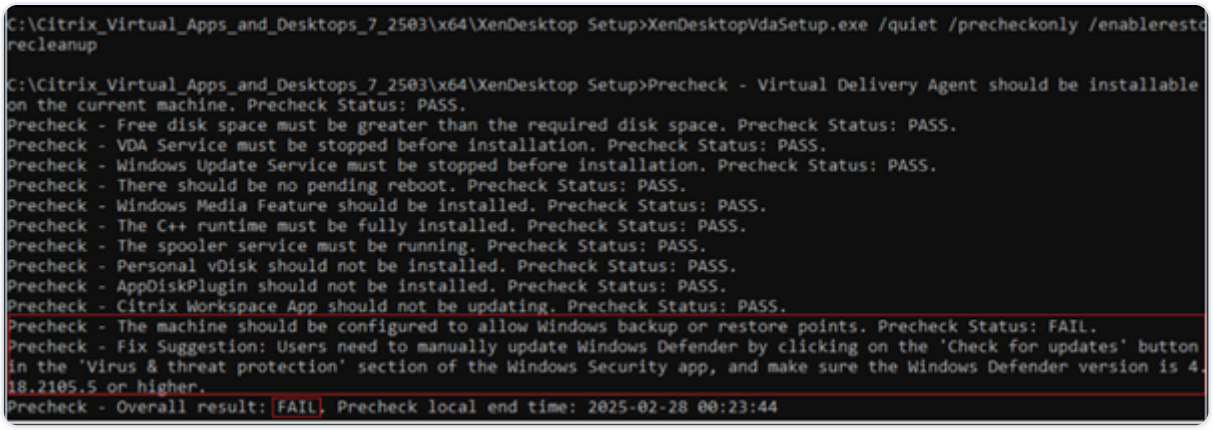
执行附加组件（Citrix 备份和还原）的安装和升级预检查

命令 `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly` 检查 Citrix 备份和还原组件的先决条件，作为可选检查。如果所有预检查都通过（可选检查除外），则总体结果为“通过”。



以下命令检查 Citrix Backup and Restore 组件的必备条件，作为强制检查的一部分：

- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /includeadditional "Citrix Backup and Restore"`
- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /enablerestore`
- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /enablerestorecleanup`



步骤 2. 查看预检查结果

预检查结果显示在命令行中，记录在 `%temp%/Citrix/XenDesktop Installer/XenDesktop Installation.log` 中并保存在 `%temp%/Citrix/XenDesktop Installer/PrecheckResult_{yyyyMMddHHmmss}.json` 中。如果预检查失败，则总体结果为 `FAIL`，并为每个问题提供建议的修复措施。

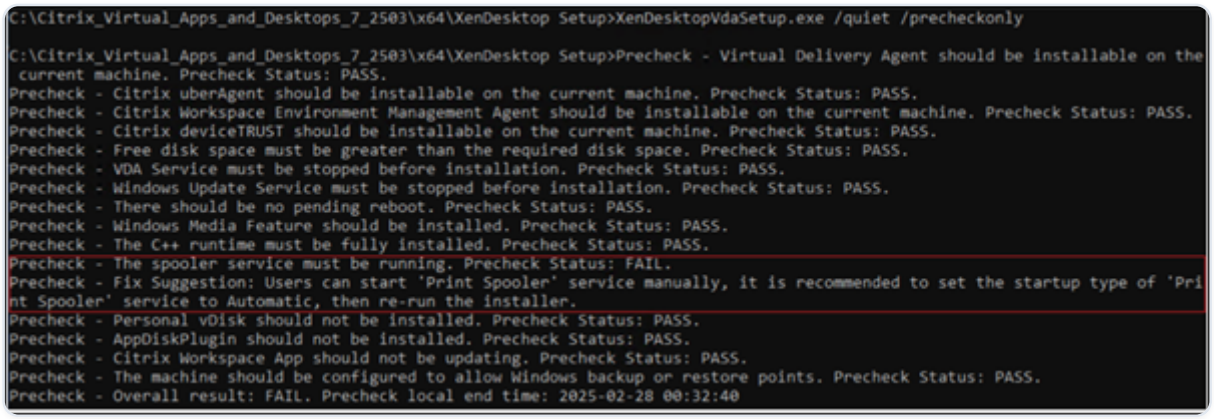
命令行输出

命令行中的预检查结果包括：

- 预检查标准
- 预检查状态

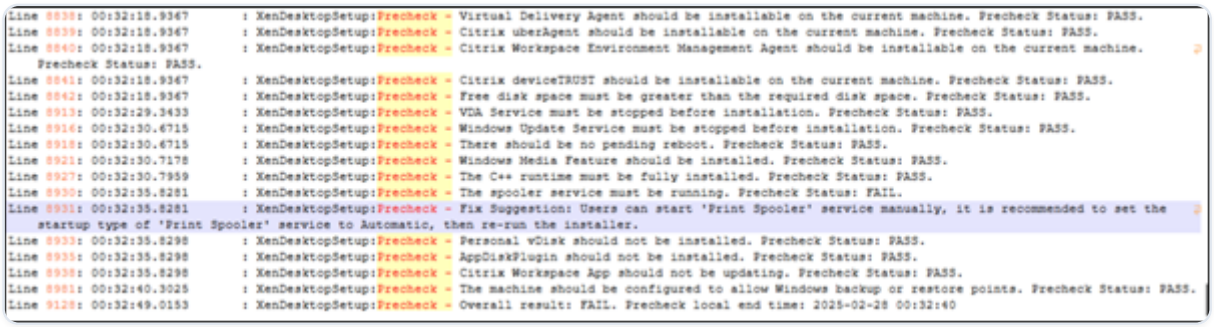
- 失败修复建议
- 总体结果
- 结束时间。

如果结果为 `FAIL`，则修复建议可在以 **Precheck - Fix Suggestion:** 开头的行中找到。



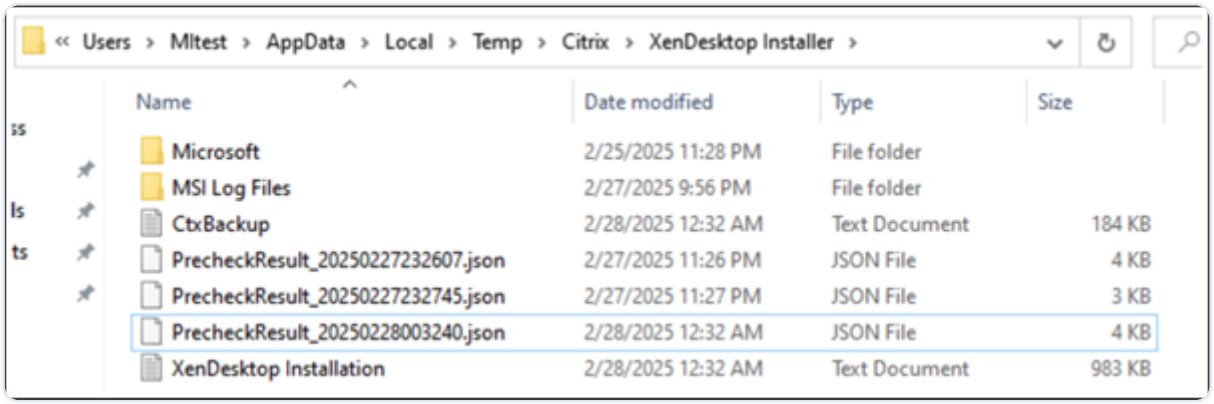
日志输出

`XenDesktop Installation.log` 中的预检查结果与命令行中显示的结果一致。要找到它们，请在日志文件中搜索 `Precheck -`。 如果总体结果为 `FAIL`，则修复建议可在包含 `Precheck - Fix Suggestion:` 的行中找到。



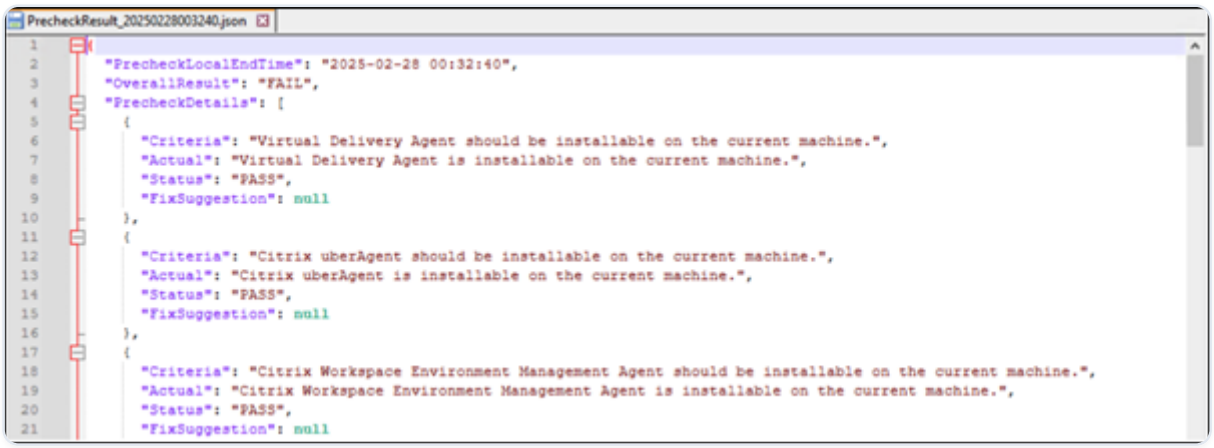
JSON 输出

每次运行带有 `/quiet /precheckonly` 的命令时，都会生成一个 `.json` 文件。该文件名为 `PrecheckResult_{yyyyMMddHHmmss}.json`，并带有时间戳后缀。

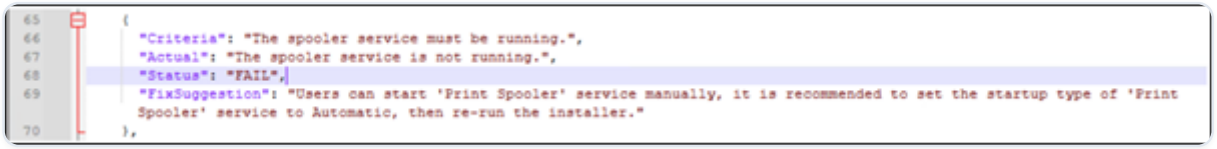


`.json` 文件包括：

- 预检查本地结束时间
- 总体结果
- 预检查详细信息
  - 标准
  - 实际值
  - 状态
  - 修复建议



状态为 `FAIL` 的每个预检查项目的修复建议可以在 `.json` 文件中的预检查详细信息部分下找到。



VDA 元安装程序助手工具

1. 简介

VDA 元安装程序助手工具包含一套工具，可协助通过 SCCM 任务序列进行 VDA 安装，以及一个用于分析安装日志和识别潜在问题的实用程序。

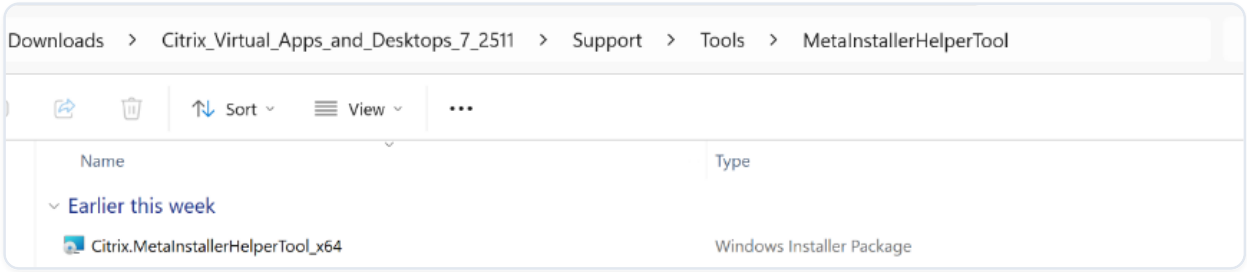
凭借简单的 MSI 安装和直观的用户界面，元安装程序助手工具提供了多项基本功能：

- **检查 SCCM 任务序列：** 此工具可帮助审查和验证现有 SCCM 任务序列，以确保其与 VDA 安装要求兼容。
- **生成任务序列参考：** 此工具自动创建参考任务序列，以帮助将 VDA 安装集成到 SCCM 部署工作流中，同时最大限度地减少手动配置。

- **VDA 安装日志分析器：** 此工具可帮助审查安装日志以识别错误、警告或故障。该工具会生成一份报告，突出显示根本原因、可能的解决方案以及成功部署的建议。

2. 安装

1. 从 Citrix 虚拟应用和桌面 下载页面 下载 Citrix 虚拟应用和桌面 产品 ISO。
2. 从 `\Support\Tools\MetaInstallerHelperTool` 文件夹中找到 Citrix.MetaInstallerHelperTool_x64.msi。



3. 双击 Citrix.MetaInstallerHelperTool_x64.msi 以安装该工具。

> **注意：**
>
> 此工具不是 VDA 的一部分。您可以将其安装在 VDA 上或任何本地设备上。

4. 安装后，在“开始”菜单中搜索“MetaInstallerHelperTool”，以管理员身份启动应用程序。

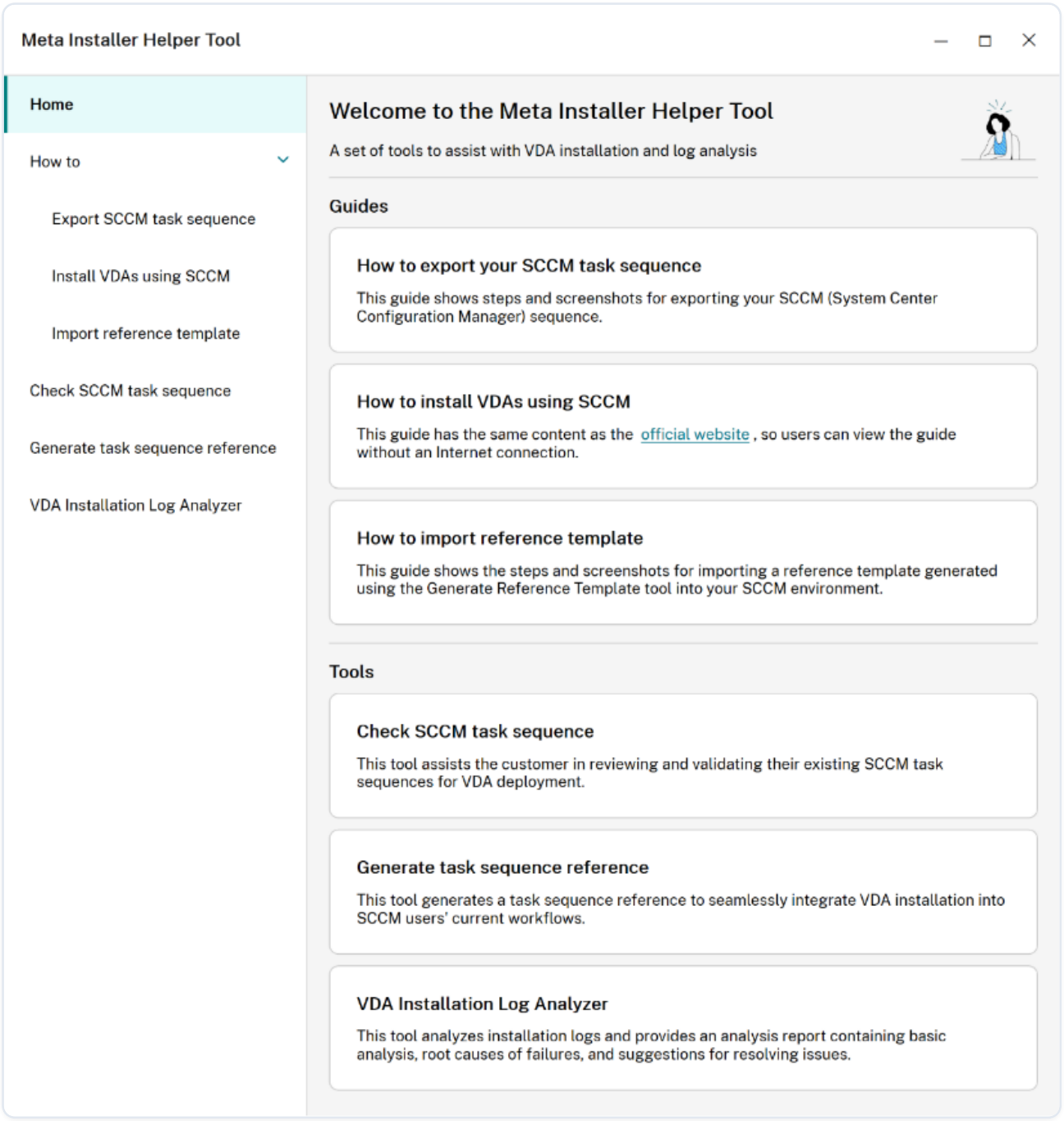


3. 用户界面 (UI) 概述

启动应用程序“MetaInstallerHelperTool”后，将出现主用户界面，该界面设计直观，易于导航和使用。

“**主页**”部分提供了“操作方法”部分中的指南说明，以及用于检查 SCCM 序列、生成任务序列模板和分析 VDA 安装日志的工具的功能说明。

您可以通过从左侧导航面板中选择相应的选项卡来访问这些指南和工具。



“**操作方法**”部分提供了导出任务序列、使用 SCCM 安装 VDA 以及导入带有屏幕截图和步骤的参考模板的指南。

- 请参阅“如何导出任务序列”以获取 SCCM 任务序列，供“检查 SCCM 任务序列”工具使用。
- 请参阅“如何使用 SCCM 安装 VDA”以安装 VDA。“检查 SCCM 任务序列”工具和“生成任务序列模板”工具也将参考本指南。
- 请参阅“如何导入参考模板”，将“生成任务序列模板”工具生成的模板作为参考模板导入到您的 SCCM 环境中。

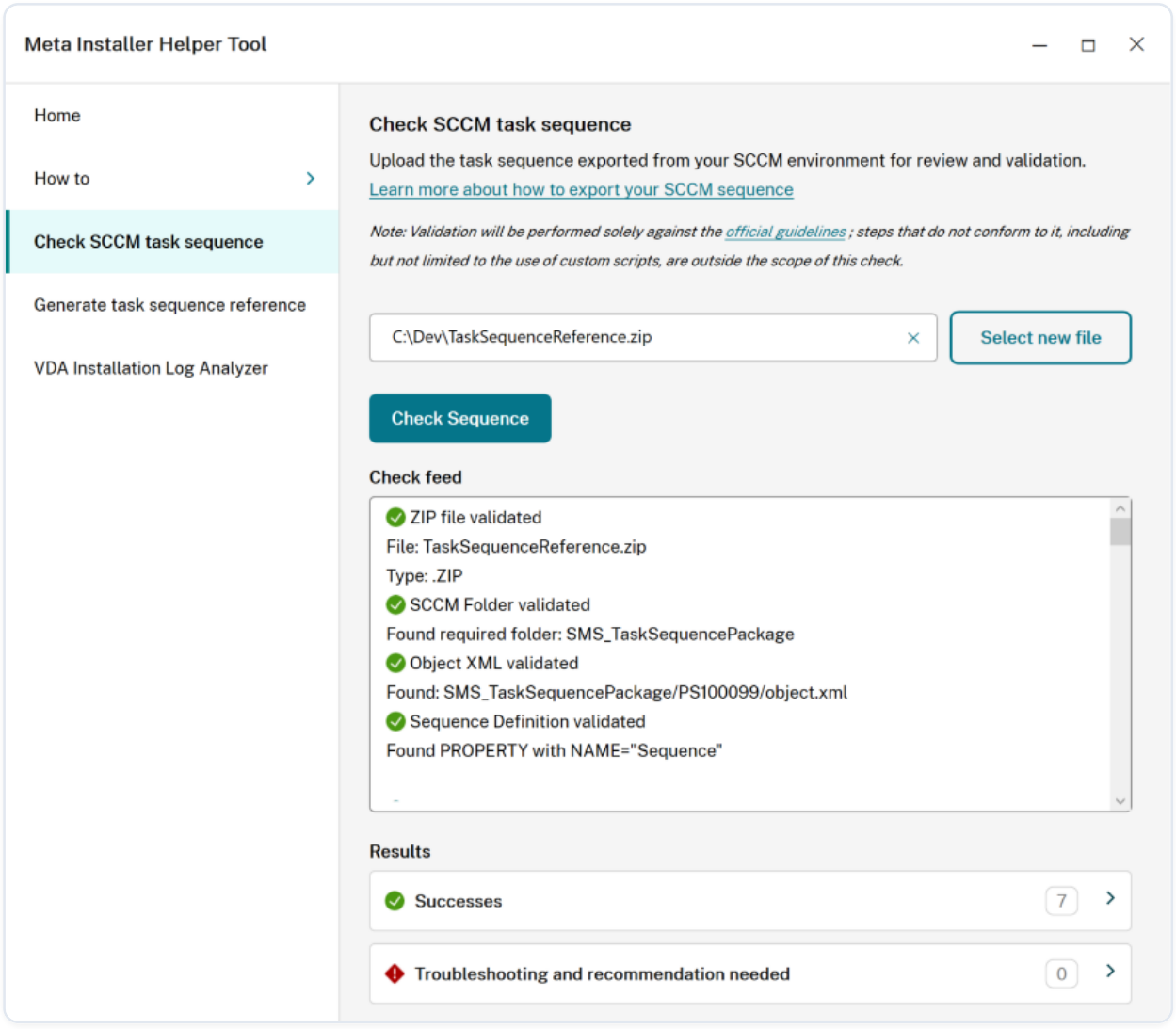
“**检查 SCCM 任务序列**”、“**生成任务序列模板**”和“**VDA 安装日志分析器**”部分可让您执行 Meta Installer Helper Tool 的核心任务。

4. 工具

1. 检查 SCCM 任务序列

   上传从 SCCM 环境导出的任务序列以进行审查和验证。

   该工具将检查上传的文件是否为 zip 文件，以及是否包含所需的 SCCM 任务序列文件夹结构、所需的 .xml 对象文件和有效的任务序列定义。它还将根据任务序列进行命令行参数分析和安装条件分析。



2. 生成任务序列参考

   此工具根据 Citrix 官方指南 生成任务序列模板，用于通过 SCCM 安装 VDA。

   您可以将其导入到 SCCM 环境中，作为将 VDA 安装集成到任务序列中的参考模板。

   Meta 安装程序生成任务序列(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/metainstaller-generate-task-sequence.png)

3. VDA 安装日志分析器

使用自动模式直接在 VDA 上分析安装日志，或者手动上传包含 VDA 安装日志的 .zip 文件进行分析。

Meta 安装程序日志分析器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/metainstaller-vda-log-analyzer.png)

在 VDA 上以**自动模式**运行时，该工具会自动检测日志存储路径并在本地分析安装日志。分析结果将保存，所有日志文件和报告都将打包成一个 ZIP 文件。

Meta 安装程序日志分析器 1(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/metainstaller-vda-log-analyzer1.png)

在**手动模式**下，您必须上传一个包含 VDA 安装日志的 .zip 文件进行分析。默认情况下，日志文件存储在以下位置：`%TEMP%\Citrix\XenDesktop Installer`

如果默认日志路径已修改，您可以在 Windows 注册表的以下位置验证当前位置：`Computer\HKLM\Software\Citrix\MetaInstall\LogPath`

该工具会提取上传的 .zip 文件，分析其内容，并保存分析结果以供查看。

Meta 安装程序日志分析器 2(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/metainstaller-vda-log-analyzer2.png)

使用脚本安装 VDA

> **注意：**
>
> Citrix 不对因适应客户生产环境而修改的脚本引起的问题负责。对于任何与安装相关的 Citrix 问题，请使用 Citrix 支持门户 提交技术支持案例并附上相关安装日志。

> 本文适用于在 Windows 操作系统计算机上安装 VDA。有关适用于 Linux 操作系统的 VDA 的信息，请参阅 Linux Virtual Delivery Agent 文档。

安装介质包含用于在 Active Directory 中为计算机安装、升级或删除 Virtual Delivery Agent (VDA) 的示例脚本。您还可以使用这些脚本来维护 Machine Creation Services™ 和 Citrix Provisioning（以前称为 Provisioning Services）使用的主映像。

所需访问权限：

- 脚本需要对 VDA 安装命令所在的网络共享具有“所有人读取”访问权限。安装命令在完整产品 ISO 中为 `XenDesktopVdaSetup.exe`，在独立安装程序中为 `VDAWorkstationSetup.exe` 或 `VDAServerSetup.exe`。
- 日志记录详细信息存储在每台本地计算机上。为了集中记录结果以供审查和分析，脚本需要对相应的网络共享具有“所有人读取和写入”访问权限。

要检查脚本运行结果，请检查中央日志共享。捕获的日志包括脚本日志、安装程序日志和 MSI 安装日志。每次安装或删除尝试都记录在一个带时间戳的文件夹中。文件夹标题以 PASS 或 FAIL 前缀指示操作结果。您可以使用标准目录搜索工具在中央日志共享中查找失败的安装或删除。这些工具提供了在目标计算机上本地搜索的替代方法。

在开始任何安装之前，请阅读并完成 准备安装 中的任务。

使用脚本安装或升级 VDA

1. 从安装介质上的 `\Support\AdDeploy\` 获取示例脚本 **InstallVDA.bat**。Citrix 建议您在自定义脚本之前备份原始脚本。
2. 编辑脚本：
   - 指定要安装的 VDA 版本：`SET DESIREDVERSION`。完整值可在安装介质的 ProductVersion.txt 文件中找到。但是，不要求完全匹配。
   - 指定将调用安装程序的网络共享。指向布局的根目录（树的最高点）。脚本运行时会自动调用相应版本的安装程序（32 位或 64 位）。例如：`SET DEPLOYSHARE=\\fileserver1\share1`。
   - （可选）指定用于存储集中式日志的网络共享位置。例如：`SET LOGSHARE=\\fileserver1\log1)`。
   - 按照使用命令行安装中所述指定 VDA 配置选项。`/quiet` 和 `/noreboot` 选项默认包含在脚本中，并且是必需的：`SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT /NORESUME`。
3. 使用组策略启动脚本，将脚本分配给包含您的计算机的 OU。此 OU 应仅包含要安装 VDA 的计算机。当该 OU 中的计算机重新启动时，脚本将在所有计算机上运行。VDA 将安装在每台具有受支持操作系统的计算机上。

使用脚本删除 VDA

1. 从安装介质上的 `\Support\AdDeploy\` 获取示例脚本 UninstallVDA.bat。Citrix 建议您在自定义脚本之前备份原始脚本。
2. 编辑脚本。

- 指定要删除的 VDA 版本：`SET CHECK\_VDA\_VERSION`。完整值可在安装介质的 ProductVersion.txt 文件中找到（例如 7.0.0.3018）。但是，不需要完全匹配。
- （可选）指定用于存储集中式日志的网络共享位置。

3. 使用组策略启动脚本，将脚本分配给包含您的计算机的 OU。此 OU 应仅包含要从中删除 VDA 的计算机。当 OU 中的计算机重新启动时，脚本将在所有计算机上运行。VDA 将从每台计算机中删除。

故障排除

- 脚本会生成内部日志文件，描述脚本执行进度。脚本在开始部署后的几秒钟内将 `Kickoff_VDA_Startup_Script` 日志复制到中央日志共享。您可以验证整个过程是否正常运行。如果此日志未按预期复制到中央日志共享，请通过检查本地计算机进一步进行故障排除。脚本将两个调试日志文件放置在每台计算机的 `%temp%` 文件夹中：
  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  检查这些日志以确保脚本：
  - 按预期运行。
  - 正确检测目标操作系统。
  - 正确配置为指向 `DEPLOYSHARE` 共享的 `ROOT`（包含名为 `AutoSelect.exe` 的文件）。
  - 能够对 `DEPLOYSHARE` 和 `LOG` 共享进行身份验证。
- 有关 Citrix 如何报告组件安装结果的信息，请参阅Citrix 安装返回代码。
- 在交付组的 Studio 显示中，**详细信息**窗格中的**已安装的 VDA 版本**条目可能不是计算机上安装的版本。计算机的程序和功能显示实际的 VDA 版本。
- VDA 安装后，它无法向用户交付应用程序或桌面，直到它向 Delivery Controller 注册。

  要了解 VDA 注册方法以及如何排查注册问题，请参阅 VDA 注册。

生成自定义脚本以通过命令行安装或升级 VDA

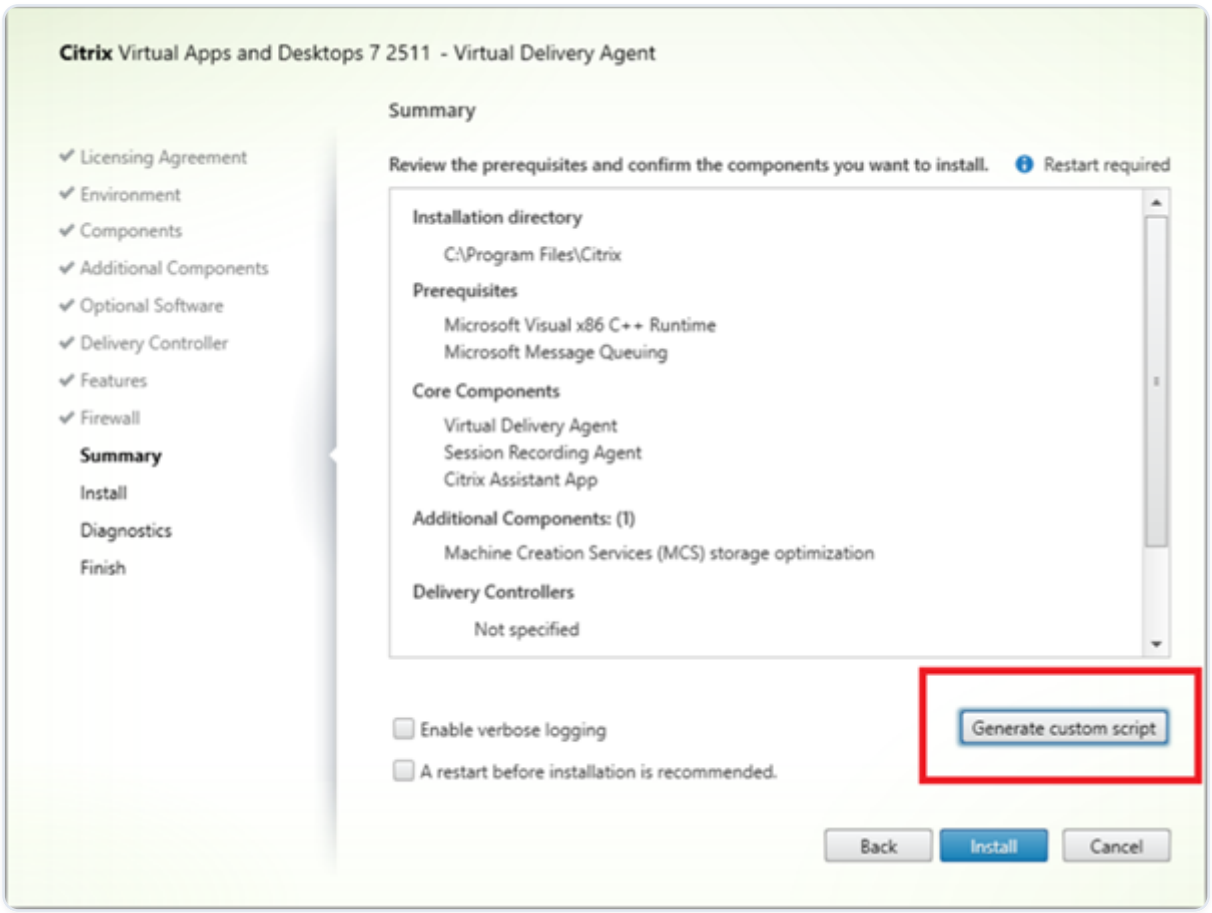
“**生成自定义脚本**”按钮允许您根据 VDA 安装 UI 中所做的配置选择创建批处理文件或脚本。生成的脚本可以导出并用于从命令行执行无人参与的安装或升级。此功能有助于自动化部署、确保配置准确性并减少手动脚本错误。

使用以下步骤从 VDA 安装 UI 生成命令行脚本。

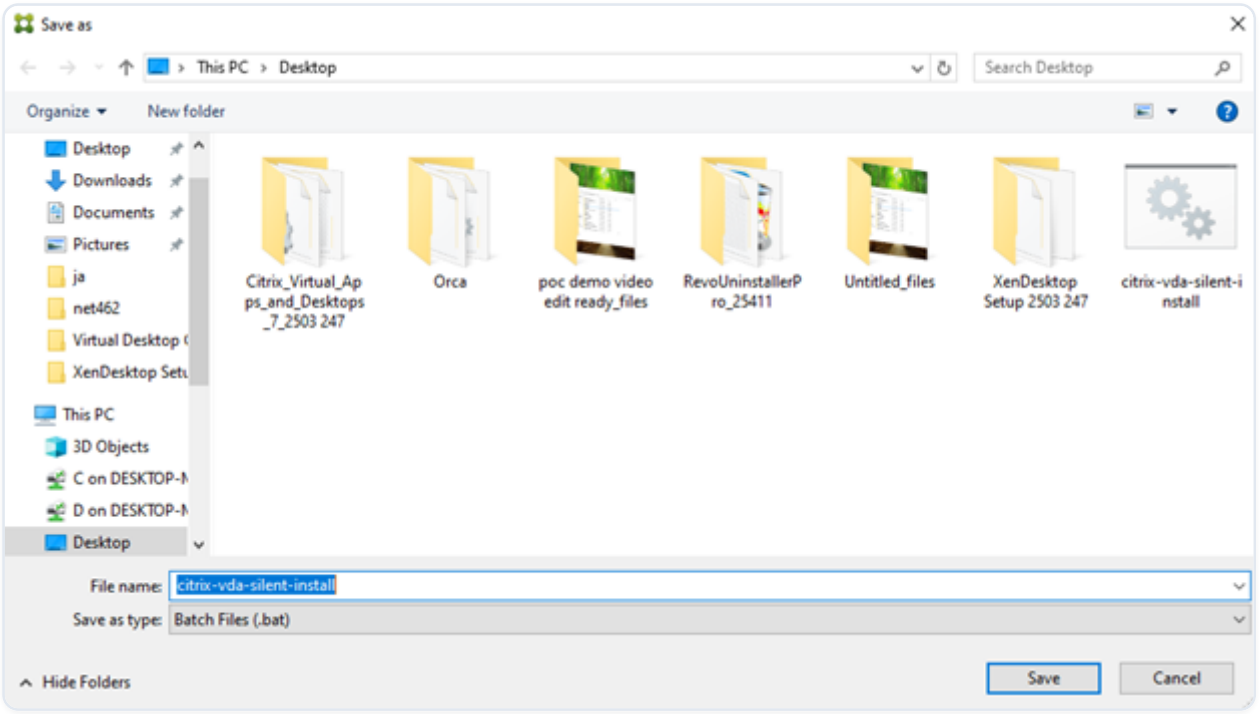
步骤 1：从安装程序 UI 生成自定义脚本

> **注意：**
>
> 此功能仅在 UI 模式下受支持。

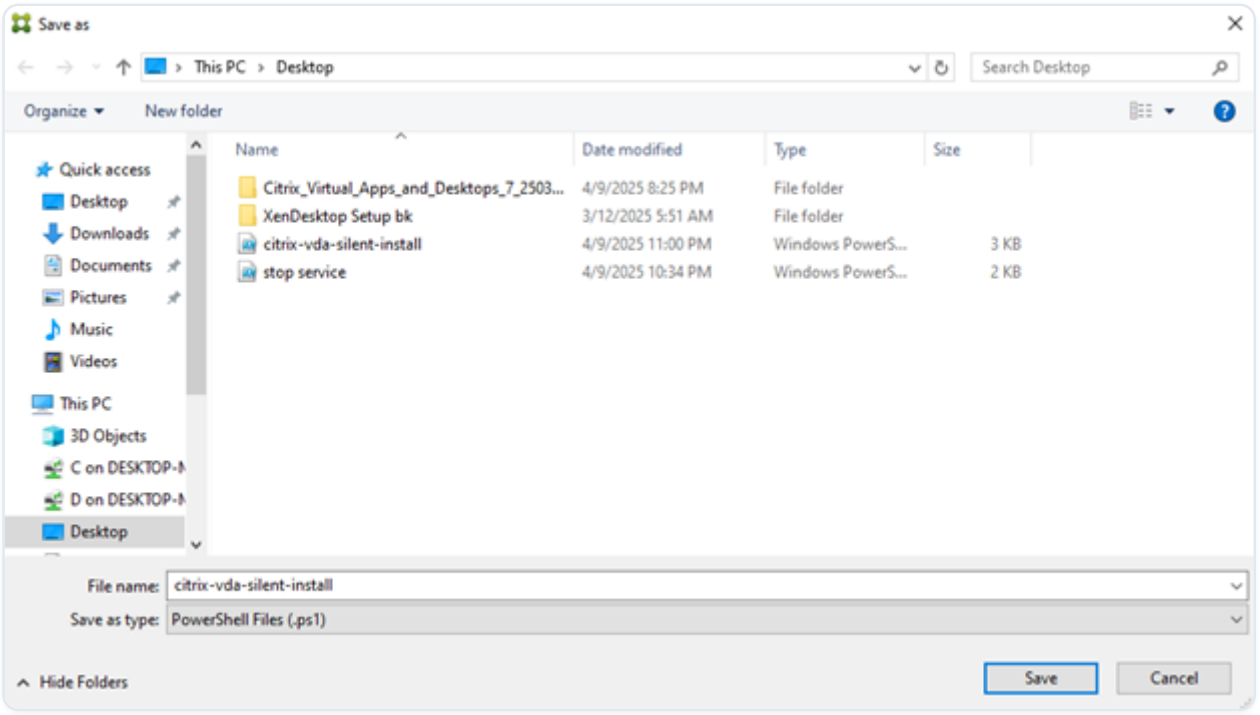
像往常一样在 UI 中配置 VDA 安装选项。在“**摘要**”页面上，选择“**生成自定义脚本**”以根据您的配置创建命令行脚本，如以下屏幕截图所示。



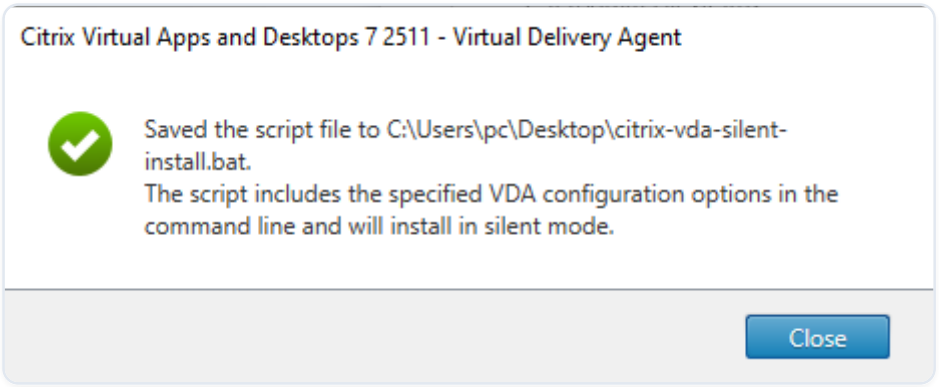
此时将出现一个对话框，提示您选择保存生成脚本的位置。您还可以在保存脚本之前选择其他目录并重命名脚本。



默认情况下，脚本另存为批处理 (.bat) 文件。您也可以选择将其另存为 PowerShell (.ps1) 脚本。



脚本生成并保存后，将出现一个确认对话框，显示文件位置并描述脚本的用途。您可以使用任何文本编辑器（例如记事本）编辑生成的脚本。运行脚本之前，请退出安装程序 UI。一次只能运行一个 VDA 安装或升级过程。



步骤 2. 使用生成的脚本安装或升级 VDA

以下屏幕截图显示了如何使用生成的批处理文件安装或升级 VDA。唯一必需的参数是 VDA 安装程序的路径。如果安装程序路径有效，脚本将运行安装或升级，并以与 VDA 安装程序相同的退出代码退出。将显示可读的结果消息以指示过程的结果。

运行生成的批处理(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/run-generated-batch.png)

以下屏幕截图显示了如何使用生成的 PowerShell 脚本安装或升级 VDA。唯一必需的参数是 VDA 安装程序的路径。如果安装程序路径有效，脚本将运行安装或升级，并以与 VDA 安装程序相同的退出代码退出。将显示一条可读的状态消息，指示该过程的结果。

运行生成的 PS1(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/run-generated-ps1.png)

> **注意：**

> 如果 Delivery Controller 配置了注册令牌，请按照以下屏幕截图所示运行脚本。

> 带 Web Socket 令牌的脚本(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/run-generated-script-with-websocket-token.png)

该脚本需要以下参数：`<Path-to-generated-script>`、`<Path-to-vda-installer>`、`<Websocket-token-value>`。

第三方 VDA 部署方法

为了使用 Microsoft System Center Configuration Manager (SCCM) 或类似的软件分发工具（例如 Ansible 和 Microsoft Intune）成功部署 Virtual Delivery Agent (VDA)，Citrix® 建议按一系列步骤使用 VDA 安装程序。

> **注意：**

> 以下文章仅描述了基于 Citrix 测试环境的建议。您可以根据自己的需求自定义这些步骤。Citrix 不对为满足客户需求而对本文档进行的任何更新或调整负责。

- 使用 SCCM 安装 VDA
- 使用 Ansible 安装 VDA
- 使用 Microsoft Intune 安装 VDA

已加入 Active Directory

Active Directory 是身份验证和授权所必需的。Active Directory 中的 Kerberos 基础结构用于保证与 Delivery Controllers 通信的真实性和机密性。有关 Kerberos 的信息，请参阅 Microsoft 文档。

《系统要求》一文列出了林和域支持的功能级别。要使用策略建模，域控制器必须在所有受支持的服务器操作系统上运行。这不影响域功能级别。

本产品支持：

- **用户帐户和计算机帐户存在于单个 Active Directory 林中的域中的部署。** 用户帐户和计算机帐户可以存在于单个林中的任意域中。在此类部署中，支持所有域功能级别和林功能级别。
- **用户帐户存在于与包含控制器和虚拟桌面计算机帐户的 Active Directory 林不同的 Active Directory 林中的部署。** 在此类部署中，包含控制器和虚拟桌面计算机帐户的域必须信任包含用户帐户的域。可以使用林信任或外部信任。在此类部署中，支持所有域功能级别和林功能级别。
- **控制器计算机帐户存在于与包含虚拟桌面计算机帐户的一个或多个其他 Active Directory 林不同的 Active Directory 林中的部署。** 在此类部署中，包含控制器计算机帐户的域与包含所有虚拟桌面计算机帐户的域之间必须存在双向信任。在此类部署中，所有包含控制器或虚拟桌面计算机帐户的域必须处于“Windows 2000 本机”功能级别或更高。支持所有林功能级别。
- **可写入的域控制器。** 不支持只读域控制器。

可选地，Virtual Delivery Agents (VDA) 可以使用 Active Directory 中发布的信息来确定它们可以向哪些控制器注册（发现）。此方法主要用于向后兼容性，并且仅当 VDA 与控制器位于同一 Active Directory 林中时才可用。有关此发现方法的信息，请参阅基于 Active Directory OU 的发现 和 CTX118976。

> **注意：**
>
> 站点配置完成后，请勿更改 Delivery Controller™ 的计算机名称或域成员身份。

在多 Active Directory 林环境中部署

在具有多个林的 Active Directory 环境中，如果存在单向或双向信任，则可以使用 DNS 转发器或条件转发器进行名称查找和注册。要允许适当的 Active Directory 用户创建计算机帐户，请使用“控制委派向导”。有关此向导的详细信息，请参阅 Microsoft 文档。

如果在林之间存在适当的 DNS 转发器，则 DNS 基础结构中不需要反向 DNS 区域。

如果 VDA 和控制器位于不同的林中，则 `SupportMultipleForest` 键是必需的，无论 Active Directory 和 NetBIOS 名称是否不同。使用以下信息将注册表项添加到 VDA 和 Delivery Controllers：

> **注意：**
>
> 不正确地编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix® 无法保证可以解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。在编辑注册表之前，请务必备份注册表。

> 在 VDA 上，配置：`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`。

- 名称: `SupportMultipleForest`
- 类型: `REG_DWORD`
- 数据: `0x00000001 (1)`

在所有 Delivery Controller 上，配置：`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest`。

- 名称: `SupportMultipleForest`
- 类型: `REG_DWORD`
- 数据: `0x00000001 (1)`

如果您的 DNS 命名空间与 Active Directory 的不同，则可能需要反向 DNS 配置。

已添加一个注册表项，以避免在 VDA 中意外启用 NTLM 身份验证，因为 NTLM 不如 Kerberos 安全。此条目可以替代 `SupportMultipleForest` 条目使用，后者仍可用于向后兼容。

在 VDA 上，配置：`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`。

- 名称: `SupportMultipleForestDdcLookup`
- 类型: `REG_DWORD`
- 数据: `0x00000001 (1)`

此注册表项在双向信任的多林环境中执行 DDC 查找，允许您在初始注册过程中删除基于 NTLM 的身份验证。

如果在设置过程中存在外部信任，则需要 `ListOfSIDs` 注册表项。如果 Active Directory FQDN 与 DNS FQDN 不同，或者包含域控制器的域的 NetBIOS 名称与 Active Directory FQDN 不同，则 `ListOfSIDs` 注册表项也是必需的。要添加注册表项，请使用以下信息：

对于 VDA，找到注册表项 `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs`。

- 名称: `ListOfSIDs`
- 类型: `REG_SZ`
- 数据：Controller 的安全标识符 (SID)。（SID 包含在 `Get-BrokerController` cmdlet 的结果中。）

如果存在外部信任，请在 VDA 上进行以下更改：

1. 找到文件 `Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config`。
2. 创建文件的备份副本。
3. 使用文本编辑程序（例如记事本）打开文件。
4. 找到文本 `allowNtlm="false"` 并将其更改为 `allowNtlm="true"`。
5. 保存文件。

添加 `ListOfSIDs` 注册表项并编辑 `brokeragent.exe.config` 文件后，重新启动 Citrix Desktop Service 以应用更改。

下表列出了支持的信任类型：

信任类型	可传递性	方向	此版本中支持
父级和子级	可传递的	双向	是

信任类型	可传递性	方向	此版本中支持
树根	可传递的	双向	是
外部	不可传递	单向或双向	是
林	可传递的	单向或双向	是
快捷方式	可传递的	单向或双向	是
领域	可传递或不可传递	单向或双向	否

有关复杂的 Active Directory 环境的更多信息，请参阅 CTX134971。

下一步操作

有关如何创建本地 Active Directory (AD) 加入的计算机身份的身份池的信息，请参阅 本地 Active Directory 加入的计算机身份的身份池。

Microsoft Entra 混合加入

本文介绍了创建 Microsoft Entra 混合加入目录以及注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录的身份池的要求，此外还包括系统要求部分中概述的要求。

Microsoft Entra 混合加入的计算机使用本地 AD 作为身份验证提供程序。您可以将它们分配给本地 AD 中的域用户或组。要启用 Microsoft Entra ID 无缝 SSO 体验，您需要将域用户同步到 Microsoft Entra ID。

> **注意：**
>
> Microsoft Entra 混合加入的 VM 在联合和托管身份基础结构中均受支持。

Microsoft Entra 混合加入的要求

- VDA 类型：单会话（仅限桌面）或多会话（应用程序和桌面）
- VDA 版本：2212 或更高版本
- 预配类型：Machine Creation Services™ (MCS)，持久和非持久
- 分配类型：专用和池化
- 托管平台：任何虚拟机管理程序或云服务

Microsoft Entra 混合加入的限制

- 如果使用 Citrix 联合身份验证服务 (FAS)，则单点登录将定向到本地 AD 而非 Microsoft Entra ID。在这种情况下，建议配置基于 Microsoft Entra 证书的身份验证，以便在用户登录时生成主刷新令牌 (PRT)，这有助于在会话内实现对 Microsoft Entra 资源的单点登录。否则，PRT 将不存在，并且对 Microsoft Entra 资源的 SSO 将不起作用。有关使用 Citrix 联合身份验证服务 (FAS) 实现对混合加入的 VDA 进行 Microsoft Entra 单点登录 (SSO) 的信息，请参阅 混合加入的 VDA。
- 在创建或更新计算机目录时，请勿跳过映像准备。如果您想跳过映像准备，请确保主 VM 不是 Microsoft Entra 或 Microsoft Entra 混合加入的。

Microsoft Entra 混合加入的注意事项

- 创建 Microsoft Entra 混合加入的计算机需要目标域中的 `Write userCertificate` 权限。请确保在目录创建期间输入具有该权限的管理员凭据。
- Microsoft Entra 混合加入过程由 Citrix 管理。您需要按如下方式在主 VM 中禁用由 Windows 控制的 `autoWorkplaceJoin`。手动禁用 `autoWorkplaceJoin` 的任务仅适用于 VDA 2212 或更早版本。

  a. 运行 `gpedit.msc`。

  b. 导航到 **计算机配置 > 管理模板 > Windows 组件 > 设备注册**。

  c. 将 **将域加入的计算机注册为设备** 设置为 **禁用**。

- 创建计算机身份时，选择配置为与 Microsoft Entra ID 同步的组织单位 (OU)。
- 对于基于 Windows 11 22H2 的主 VM，请在主 VM 中创建一个计划任务，该任务在系统启动时使用 SYSTEM 帐户执行以下命令。在主 VM 中计划任务的此任务仅适用于 VDA 2212 或更早版本。

```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'

$WorkplaceJoinKeyPath = 'HKLM:
\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin'

$MaxCount = 60



for ($count = 1; $count -le $MaxCount; $count++)

{
```

```
  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)

  {

    $provider = (Get-Item -Path
$VirtualDesktopKeyPath).GetValue("Provider", $null)

    if ($provider -eq 'Citrix')

    {

        break;

    }



    if ($provider -eq 1)

    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "Provider"
-Value "Citrix" -Force

        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name
"autoWorkplaceJoin" -Value 1 -Force

        Start-Sleep 5

        dsregcmd /join

        break

    }

  }



  Start-Sleep 1
```

```
}
```

- 默认情况下，Microsoft Entra Connect 每 30 分钟同步一次。预配的计算机在首次启动时可能需要长达 30 分钟才能加入 Microsoft Entra 混合。

已注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录

已加入 Microsoft Entra 混合的目录、持久性单会话和多会话 VM（已注册到 Microsoft Intune）使用具有共同管理功能的设备凭据。

共同管理使您能够使用 Configuration Manager 和 Microsoft Intune 同时管理 Windows 10 或更高版本的设备。有关详细信息，请参阅共同管理。

已注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录的先决条件

在启用此功能之前，请验证：

- 您的 Azure 环境符合使用 Microsoft Intune 的许可要求。有关详细信息，请参阅 Microsoft 文档。
- 您有一个已启用共同管理的有效 Configuration Manager 部署。有关详细信息，请参阅 Microsoft 文档。

已注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录的要求

- VDA 类型：单会话或多会话
- VDA 版本：2407 或更高版本
- 预配类型：Machine Creation Service (MCS)，持久性。已注册到 Microsoft Intune 的非持久性单会话和多会话 VM 的 Microsoft Entra 混合加入目录目前处于预览阶段。请参阅将混合 Entra ID 加入的非持久性 VM 注册到 Microsoft Intune。
- 分配类型：专用和池化
- 托管平台：任何虚拟机管理程序或云服务

已注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录的限制

- 在创建或更新计算机目录时，请勿跳过映像准备。
- Configuration Manager 的基于 Internet 的客户端管理 (IBCM) 不受支持。

已注册到 MICROSOFT INTUNE 的 MICROSOFT ENTRA 混合联接目录的注意事项

- 如果目录中同时启动的计算机过多，Intune 注册可能会延迟。

Microsoft 对每个租户的 Intune 注册施加了限制，该限制规定了在特定时间范围内可以注册的设备数量。允许的设备数量因与租户关联的 Microsoft Intune 许可证数量而异。请咨询您的 Microsoft 客户团队以了解您的租户的允许限制。此方法有助于 Microsoft Intune 注册更好地扩展以适应大型环境。

对于持久性计算机，所有设备完成 Intune 注册可能需要初始等待时间。

对于非持久性计算机，请考虑限制 Autoscale™ 或手动电源操作中的并发电源操作。

- 配置 Configuration Manager 的云连接。有关详细信息，请参阅 Microsoft 文档。
- 在主 VM 上手动安装 Configuration Manager 客户端，而无需使用 `.\CCMSetup.exe /mp:SCCMServer /logon FSP=SCCMServer` 分配站点代码。SCCMServer 是您环境中的 SCCM 服务器名称。有关详细信息，请参阅 Microsoft 文档。
- MCS 创建的计算机使用自动站点分配机制来查找发布到 Active Directory 域服务的站点边界组。确保在您的环境中配置了 **Configuration Manager** 的 边界和边界组。如果自动站点分配不可用，可以通过以下注册表设置在主 VM 中配置静态 Configuration Manager 站点代码：

  键：

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MachineIdentityServiceAgent\DeviceManagement
  ```

  值名称：`MdmSccmSiteCode`

  值类型：**字符串**

  值数据：`the site code to be assigned`

- 配置 Microsoft Intune 以删除陈旧设备。这可确保您的设备记录保持最新。有关删除陈旧设备的信息，请参阅 使用清理规则自动删除设备。

下一步操作

有关创建 Microsoft Entra 混合联接目录的身份池的更多信息，请参阅 Microsoft Entra 混合联接计算机身份的身份池。

非域加入

本文介绍了使用 Citrix Virtual Apps and Desktops 创建非域加入目录的要求，以及 系统要求 部分中概述的要求。

要求

- 控制平面：请参阅 支持的配置

- VDA 类型：单会话（仅限桌面）或多会话（应用程序和桌面）
- VDA 版本：2311 或更高版本
- 预配类型：Machine Creation Services™ (MCS)，持久和非持久
- 分配类型：专用和池化
- 托管平台：MCS 支持的所有平台
- 必须启用 Rendezvous V2

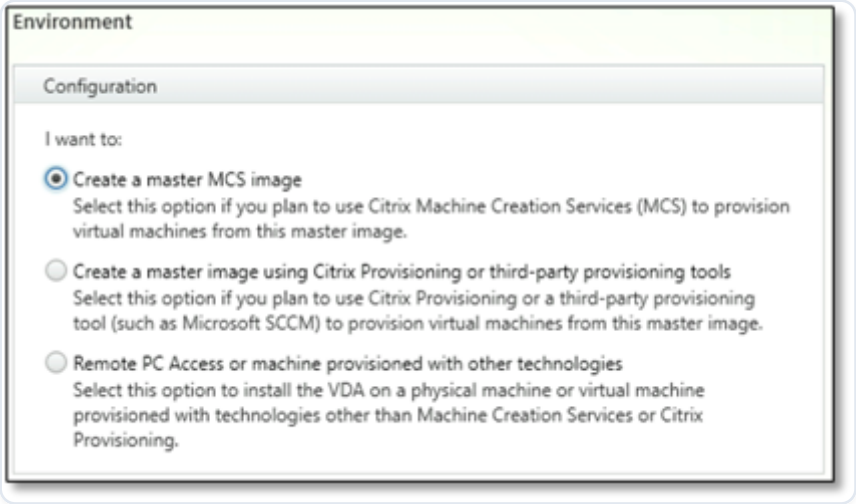
限制

- 不支持服务连续性。
- 每当我们使用多会话非域加入 VDA 时，本地用户配置文件数据将不会保留，并在注销时删除。

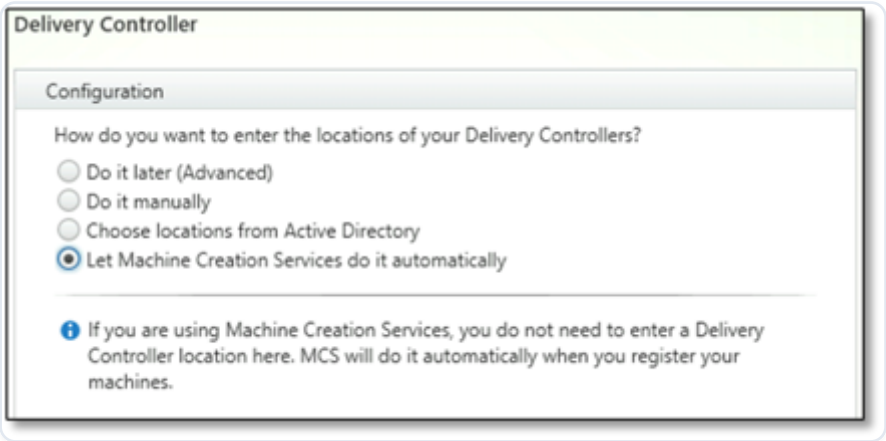
VDA 安装和配置

请按照以下步骤安装 VDA：

1. 请确保在安装向导中选择以下选项：
    - 在“环境”页面上，选择 **创建主 MCS 映像**。



    - 在“Delivery Controller™”页面上，选择 **让 Machine Creation Services 自动执行**。



下一步操作

资源位置和托管连接可用后，请继续创建身份池。有关创建非域加入计算机身份的身份池的更多信息，请参阅 非域加入计算机身份的身份池。

会话身份验证

Citrix 支持多种方法对用户进行虚拟桌面和应用程序会话身份验证。可用选项取决于您的环境配置方式；具体来说，包括用户帐户所在的目录服务（例如 Active Directory 或 Microsoft Entra ID）、会话主机加入的目录服务以及用于首次登录 Citrix 环境的身份提供程序。这些因素决定了身份验证是通过传统凭据、智能卡、联合断言还是基于证书的机制来处理。本节概述了可用的身份验证方法以及它们如何与不同的部署场景相对应。

Microsoft Entra 单点登录

当使用 Microsoft Entra ID 凭据访问 Microsoft Entra 混合加入会话主机上的虚拟应用程序和桌面时，您可以利用单点登录 (SSO)。

有关 DaaS，请参阅 Microsoft Entra 单点登录。

支持的基础设施

以下是 Microsoft Entra 单点登录支持的基础设施组件概述：

计算机身份	思杰 DAAS	CVAD 本地部署	思杰店面云	思杰店面	思杰网关服务	NETSCALER 网关
已加入 Microsoft Entra	是	否	是	否	是	是
Microsoft Entra 混合加入	是	是	是	是	是	是

注意：

在 StoreFront 中，Microsoft Entra 单点登录仅支持现代 UI 体验，不支持经典 UI 体验。

支持的访问方法

以下是 Citrix 环境中可用的访问方法：

- **本机访问**：您使用本机 Citrix Workspace 应用程序客户端访问 Citrix Storefront 并建立会话连接。
- **浏览器访问**：您通过浏览器访问 Citrix Storefront，并使用适用于 HTML5 客户端的 Citrix Workspace 应用程序连接到虚拟应用程序或桌面会话。
- **混合访问**：您通过浏览器访问 Citrix Storefront，并使用本机 Workspace 应用程序客户端连接到虚拟应用程序或桌面会话。

以下是 Microsoft Entra 单点登录支持的访问方法概述：

访问方法	视窗	林纳克斯	MAC	CHROME 操作系统	安卓	IOS
本机	是	是	是	是	是	是
浏览器	是	是	是	是	是	是
混合	是	是	是	否	否	否

注意：

您必须允许弹出窗口，以便单点登录在浏览器和混合访问中正常工作。

系统要求

以下是使用 Microsoft Entra 单点登录的系统要求：

- 控制平面：Citrix Virtual Apps and Desktops™ 2607 LTSR 或更高版本
- 访问层：StoreFront 2607 LTSR 或更高版本
- 虚拟投递代理 (VDA)
    - Windows：版本 2507 或更高版本

- Citrix Workspace 应用程序
  - Windows：版本 2508 或更高版本
  - Linux：版本 2604.10 或更高版本
  - Mac：版本 2607 或更高版本
  - HTML5：版本 2603.10 或更高版本
  - Chrome OS：版本 2603 或更高版本
  - Android：版本 2511 或更高版本
  - iOS：版本 2607 或更高版本
- 具有本机启动功能的 Web 浏览器：
  - 微软 Edge 配合 Citrix Web 扩展
  - 谷歌 Chrome 配合 Citrix Web 扩展
- 具有浏览器启动功能的 Web 浏览器：任何受支持的 Web 浏览器。
- 会话主机操作系统：
  - Windows 11，版本 24H2，并安装了 2025 年 9 月 Windows 11 累积更新 (KB5065789) 或更高版本（内部版本 26100.6725）
  - Windows Server 2025，并安装了 2026 年 1 月 Windows Server 2025 累积更新 (KB5073379) 或更高版本（内部版本 26100.32230）

> **注意：**
>
> 仅当用户将在 **Windows** 或 **Mac** 设备中利用混合访问时，才需要 Citrix Web Extension。如果用户利用本机或浏览器访问，则不需要 Citrix Web Extension。

注意事项

- 如果您的用户将利用混合访问，他们必须使用 Microsoft Edge 或 Google Chrome，并安装 Citrix Web 扩展。混合访问的 Microsoft Entra 单点登录不支持其他浏览器。
- 当使用 Microsoft Entra 单点登录登录会话时，不支持自动客户端重新连接。使用此登录方法时，此功能会自动禁用。在网络中断的情况下，会话可靠性仍可用于自动重新连接。
- 当虚拟桌面被锁定后，默认行为是显示 Windows 锁定屏幕。根据您的身份验证要求，您可能需要更改会话锁定行为。有关更多详细信息，请参阅 会话锁定行为。

- 对于 Microsoft Entra 混合加入的会话主机，默认情况下，单点登录不适用于特权组（如域管理员）的成员。要启用此功能，请将该组或用户添加到 Microsoft Entra Kerberos 访问的只读域控制器 (RODC) 允许列表中。有关详细信息，请参阅 Microsoft Entra Kerberos TGT 和 Active Directory 访问控制。
- Microsoft Entra 单一登录要求启用 Windows 设置 **允许将自定义 SSP 和 AP 加载到 LSASS 中**（默认）。请注意，如果您通过 Microsoft Intune 部署**适用于 Windows 10 及更高版本的安全基线**模板，则此设置将自动禁用并阻止 SSO，因此您必须更新 Intune 设备配置策略以使其保持启用状态。

如何配置 Microsoft Entra 单一登录

概述

Microsoft Entra 单一登录的配置包含以下步骤：

1. Azure 和 Microsoft Entra ID 的配置。
    a. 注册 Citrix 资源和客户端应用程序。
    b. 为 Citrix 资源应用程序启用 Microsoft Entra ID 远程桌面服务身份验证协议。
    c. 隐藏用户同意提示。
    d. 批准客户端应用程序。
    e. 创建 Kerberos 服务器对象（仅限 Microsoft Entra 混合联接环境）。
    f. 审查 Microsoft Entra 条件访问策略。
2. Citrix 配置。
    a. 预配具有所需操作系统版本、身份类型和 VDA 版本的会话主机。
    b. 配置 StoreFront。
    c. 在您的站点中启用 Microsoft Entra 单一登录。
    d. 在您的交付组中启用 Microsoft Entra 单一登录。

微软 AZURE 和微软 ENTRA ID 配置

为了利用 Microsoft Entra 单一登录，您必须首先在 Microsoft Entra ID 租户中为 Windows 启用 Microsoft Entra 身份验证，这将允许颁发所需的身份验证令牌，从而使用户能够登录到已加入 Microsoft Entra 和混合加入 Microsoft Entra 的会话主机。

执行 Azure 配置的人员必须至少被分配以下 Microsoft Entra 内置角色 之一或同等角色：

- 应用程序管理员
- 云应用程序管理员

配置可以通过 Azure 门户、使用 Microsoft Graph PowerShell SDK 或 Microsoft Graph API 完成。以下部分提供了通过 Azure 门户完成配置的详细信息。如果您更喜欢使用 Microsoft Graph PowerShell SDK 或 Microsoft Graph API，请参阅 Microsoft Entra 单一登录 Azure 配置。

注册 Citrix 应用程序

您必须在 Azure 租户中注册多租户 Citrix Resource 应用程序，并创建单租户 Client 应用程序。

首先，您必须注册 Citrix Resource 应用程序。为此，请使用以下同意 URL 之一：

- 美国、欧盟、亚太地区：`https://login.microsoftonline.com/common/adminconsent?client_id=3a510bb1-e334-4298-831e-3eac97f8b26c`
- 日本：`https://login.microsoftonline.com/common/adminconsent?client_id=0027603f-364b-40f2-98be-8ca4bb79bf8b`

Resource 应用程序注册后，您需要创建单租户 Client 应用程序。

创建单租户 Client 应用程序

1. 转到 Azure 门户。
2. 导航到 **Microsoft Entra ID > 企业应用程序**。
3. 选择**新建应用程序**。
4. 选择**创建自己的应用程序**。
5. 输入应用程序名称，选择**注册应用程序以与 Microsoft Entra ID 集成**，然后单击**创建**。
6. 在**支持的帐户类型**下，选择**仅限单租户**，然后单击**注册**。
7. 导航到 **Microsoft Entra ID > 应用注册**，然后选择**所有应用程序**。
8. 搜索并点击您刚刚创建的应用程序。
9. 点击 **添加重定向 URI**。
10. 您需要添加三个重定向 URI：**Web**、**单页应用程序** 和 **移动和桌面应用程序**。
    a. 对于每个 URI，选择 **添加重定向 URI**。
    b. 输入重定向 URI。有关要添加的内容的详细信息，请参阅下表。

平台类型	重定向 URI	备注
Web	客户特定的 NetScaler 登录 URI	URI 字符串是根据您特定的 NetScaler URL 计算的。
移动和桌面应用程序	`ctxaadsso://citrix.aad.redirect`	完全按原样输入此 URI。

平台类型	重定向 URI	备注
SPA 应用程序（单页应用程序）	StoreFront 应用商店 Web URL	输入您的 StoreFront 应用商店的 Web URL。例如，如果通过浏览器访问您的应用商店的 URL 是 `https://finance.acme.com/Citrix/MyStoreWeb`，则 SPA 重定向 URI 必须是 `https://finance.acme.com/Citrix/MyStoreWeb`。如果您的环境中存在多个应用商店，则必须将所有应用商店的 Web URL 输入为 SPA 重定向 URI。

c. 选择 **配置**。

11. 添加所有重定向 URI 后，您需要向客户端应用程序添加一个 API 权限。

    a. 在“管理”下的左侧窗格中，选择 **API 权限**。

    b. 选择 **添加权限**。

    c. 选择 **我的组织使用的 API**。

    d. 选择 Citrix 资源应用程序 (**Citrix-Workspace-Resource**)。

    e. 在权限列表中，选中 **user_impersonation**。

    f. 选择 **添加权限**。

12. 在左侧窗格中，选择 **概述**，并记下分配的应用程序 ID。

注册客户端应用程序
创建并配置应用程序后，您必须同意应用程序权限。

您可以在 Azure 门户中同意应用程序的权限：

1. 导航到 **微软 Entra 标识 > 企业应用程序**。
2. 搜索并选择客户端应用程序。
3. 在“安全性”下的左侧窗格中，选择 **权限**。
4. 单击 **授予管理员同意 \<tenantName\>**

5. 同意这些权限。

或者，您可以使用管理员同意 URL: `https://login.microsoftonline.com/<EntraTenantID>/adminconsent?client_id=<clientAppID>`

> **注意：**
>
> 您必须将 `<EntraTenantID>` 替换为您的 Entra 租户 ID，并将 `<clientAppID>` 替换为客户端应用程序的应用程序 ID。

Citrix 资源应用程序权限
以下是应用程序的权限：

API 名称	声明值	权限	类型
微软图形	User.Read	登录并读取用户配置文件	委派

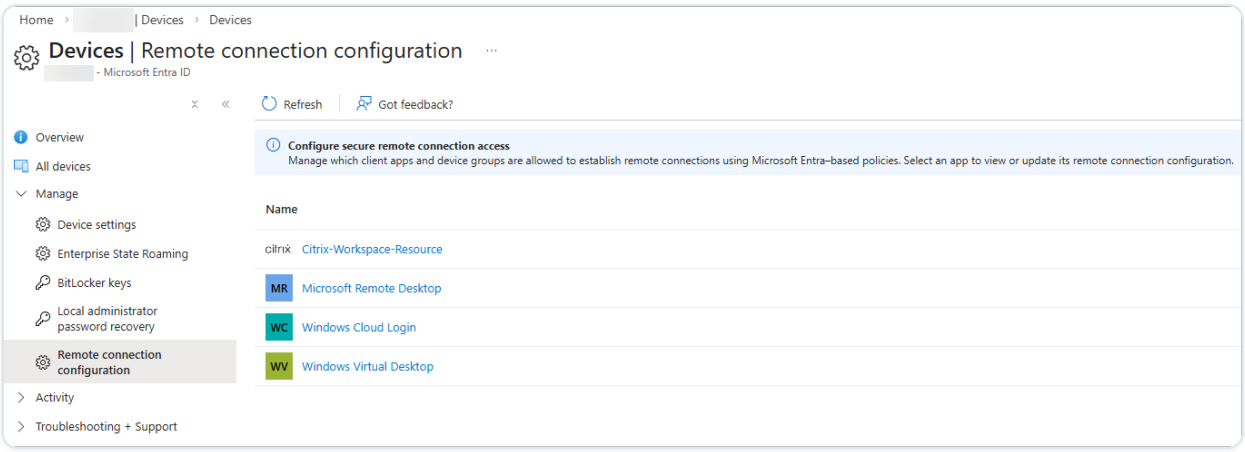
对于美国、欧盟和 APS，该应用程序称为 **Citrix-Workspace-Resource** (application ID 3a510bb1-e334-4298-831e-3eac97f8b26c)。

对于日本，该应用程序称为 **Citrix-Workspace-Resource-JP** (application ID 0027603f-364b-40f2-98be-8ca4bb79bf8b)。
Citrix 客户端应用程序权限
以下是应用程序的权限：

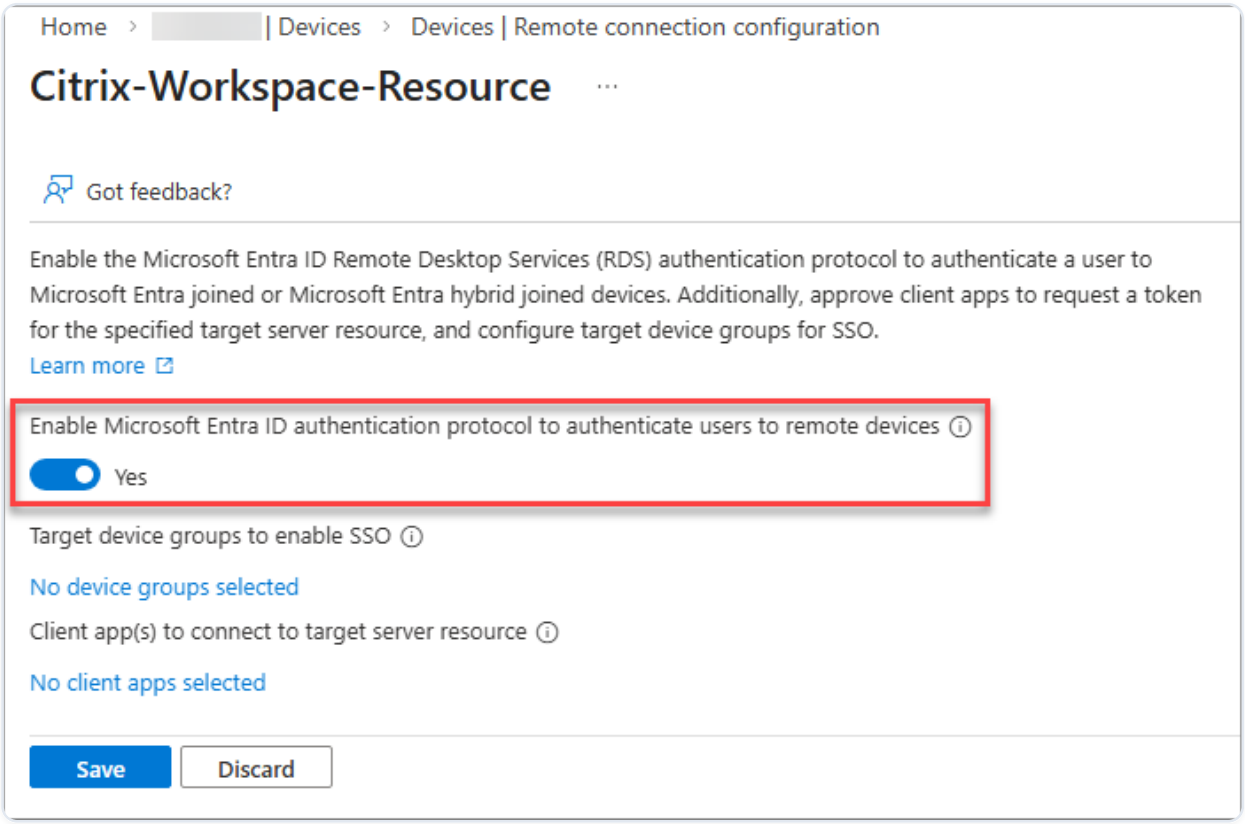
API 名称	声明值	权限	类型	
思杰-工作区-资源 Citrix-工作区-资源-JP	user_impersonation	Citrix Entra ID 单点登录	委派	
微软图形	User.Read	登录并读取用户配置文件	委派	

启用 Microsoft Entra ID 远程桌面服务身份验证协议
您必须在 Citrix Resource 应用程序中启用 Microsoft Entra ID 远程桌面服务身份验证协议。为此：

1. 在 Azure 门户 中，导航到 `Microsoft Entra ID` > `Devices` > `Manage` > `Remote connection configuration`。



2. 选择名为 **Citrix-Workspace-Resource** 的资源。
3. 启用 **Microsoft Entra ID 远程桌面服务身份验证协议**。



4. 继续隐藏用户同意提示。

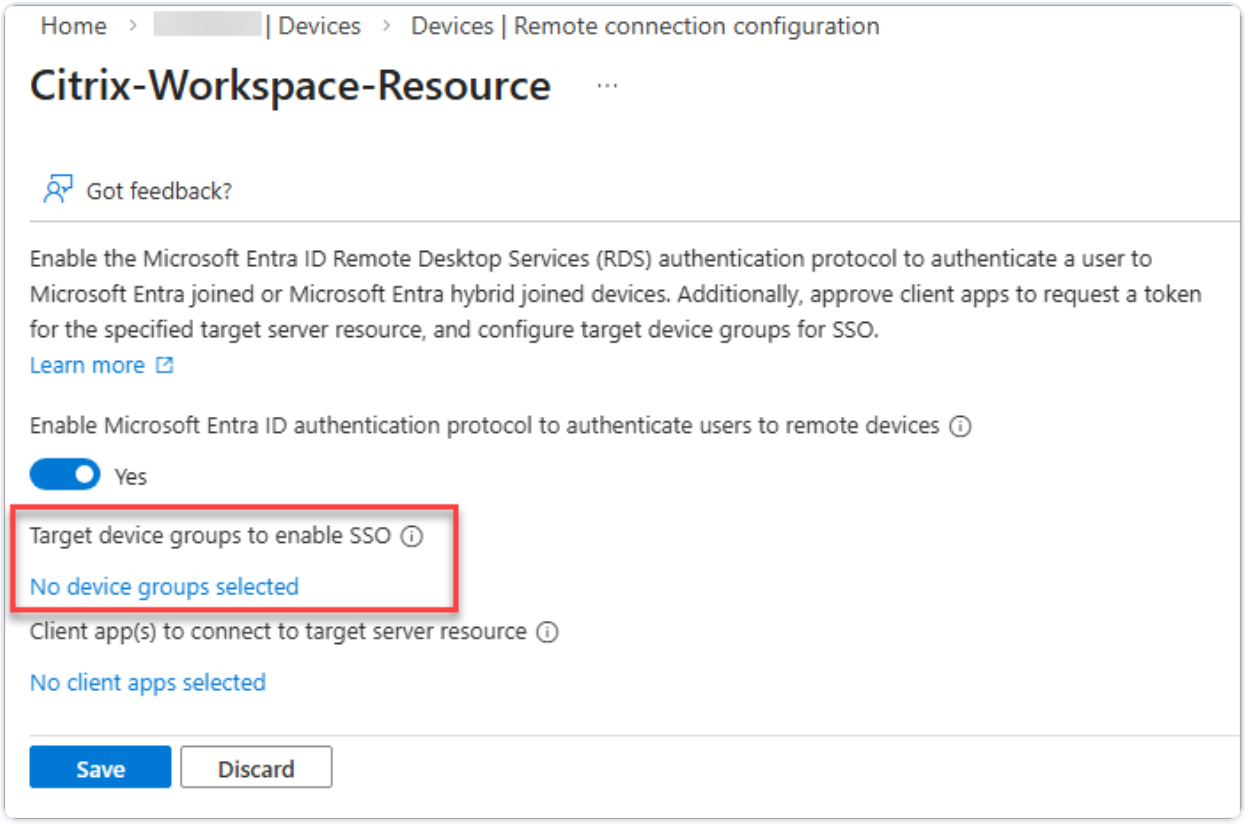
隐藏用户同意提示对话框

默认情况下，当用户连接到启用了 Microsoft Entra 单一登录的 Microsoft Entra 加入或 Microsoft Entra 混合加入会话主机时，系统会提示他们允许远程桌面连接，此时他们必须选择“**是**”以允许单一登录。Microsoft Entra 将记住最多 15 个唯一的会话主机 30 天，之后会再次提示。

您可以通过配置目标设备列表来隐藏此对话框。要配置设备列表，您必须在 Microsoft Entra ID 中创建一个或多个组，这些组包含 Microsoft Entra 加入和/或 Microsoft Entra 混合加入的会话主机，然后在资源应用程序中授权这些组，最多可授权 10 个组。

一旦您启用了 Microsoft Entra ID 远程桌面服务身份验证协议并创建了组：

1. 单击链接以添加目标设备组并选择相应的组。



注意

强烈建议创建动态组以简化组的成员资格管理。虽然动态组通常在 5-10 分钟内更新，但大型租户可能需要长达 24 小时。

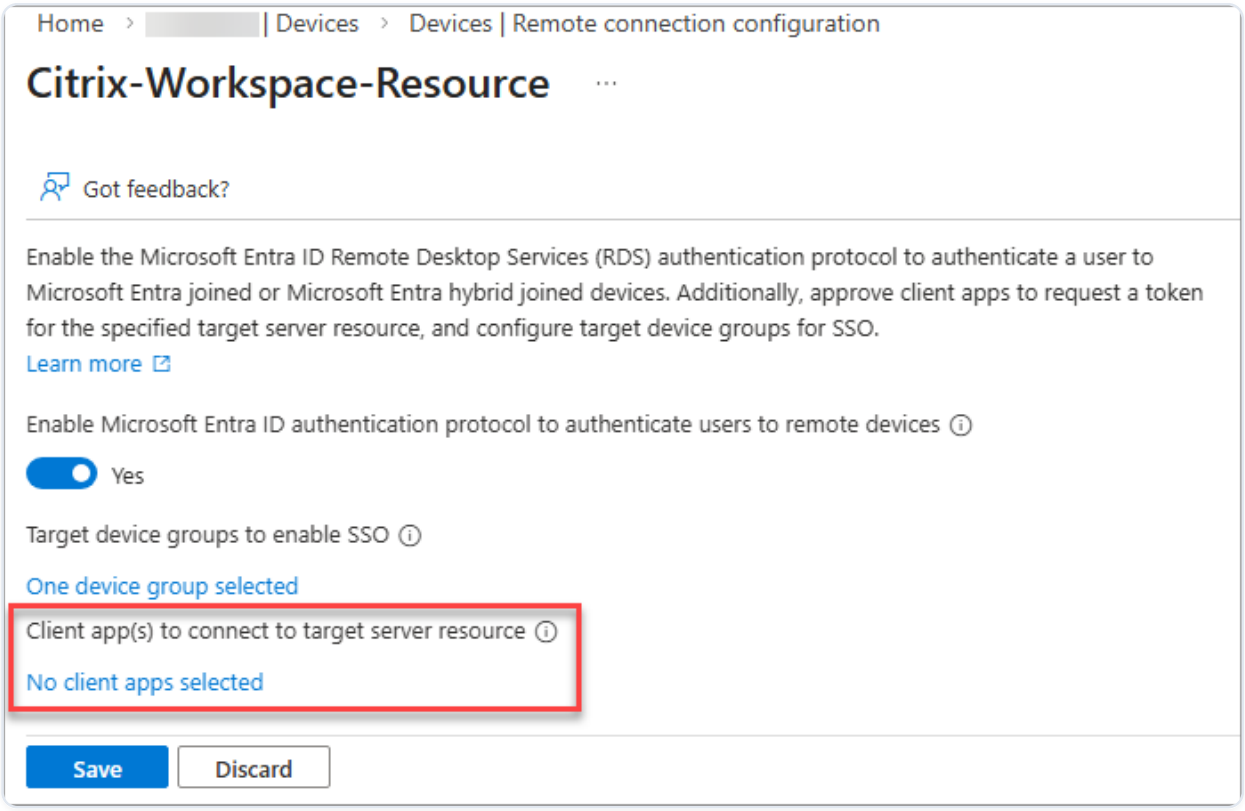
动态组需要 Microsoft Entra ID P1 许可证或 Intune for Education 许可证。有关详细信息，请参阅组的动态成员资格规则。

1. 继续批准客户端应用程序。

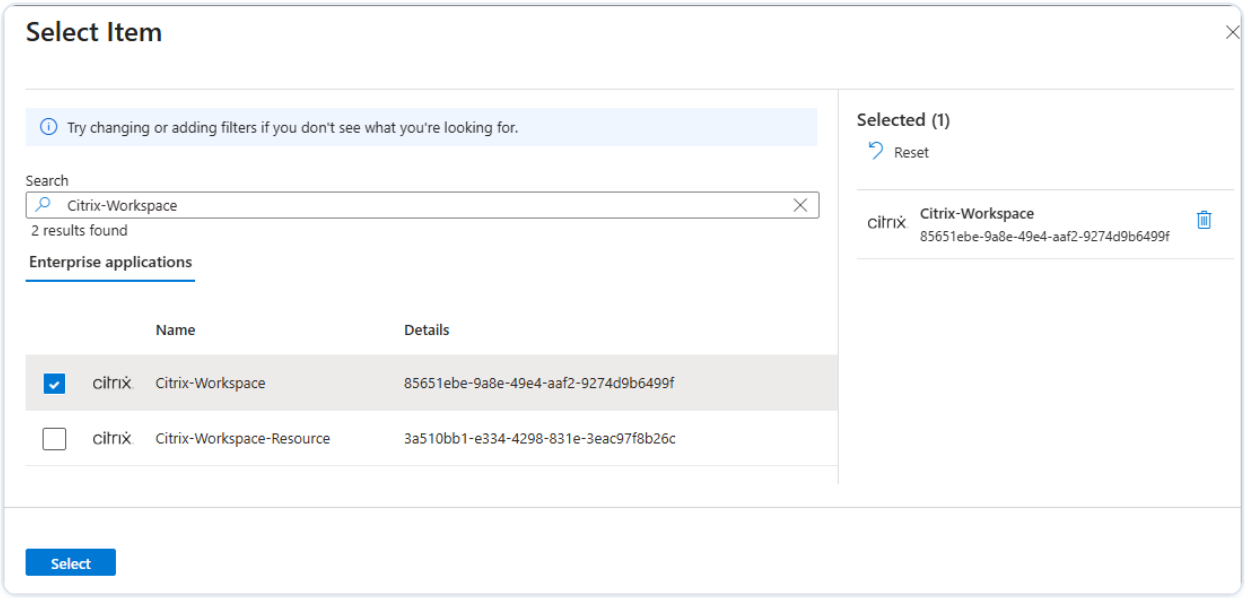
批准客户端应用程序

您必须在 Citrix 资源应用程序中将 Citrix Client 应用程序明确添加为已批准的客户端：

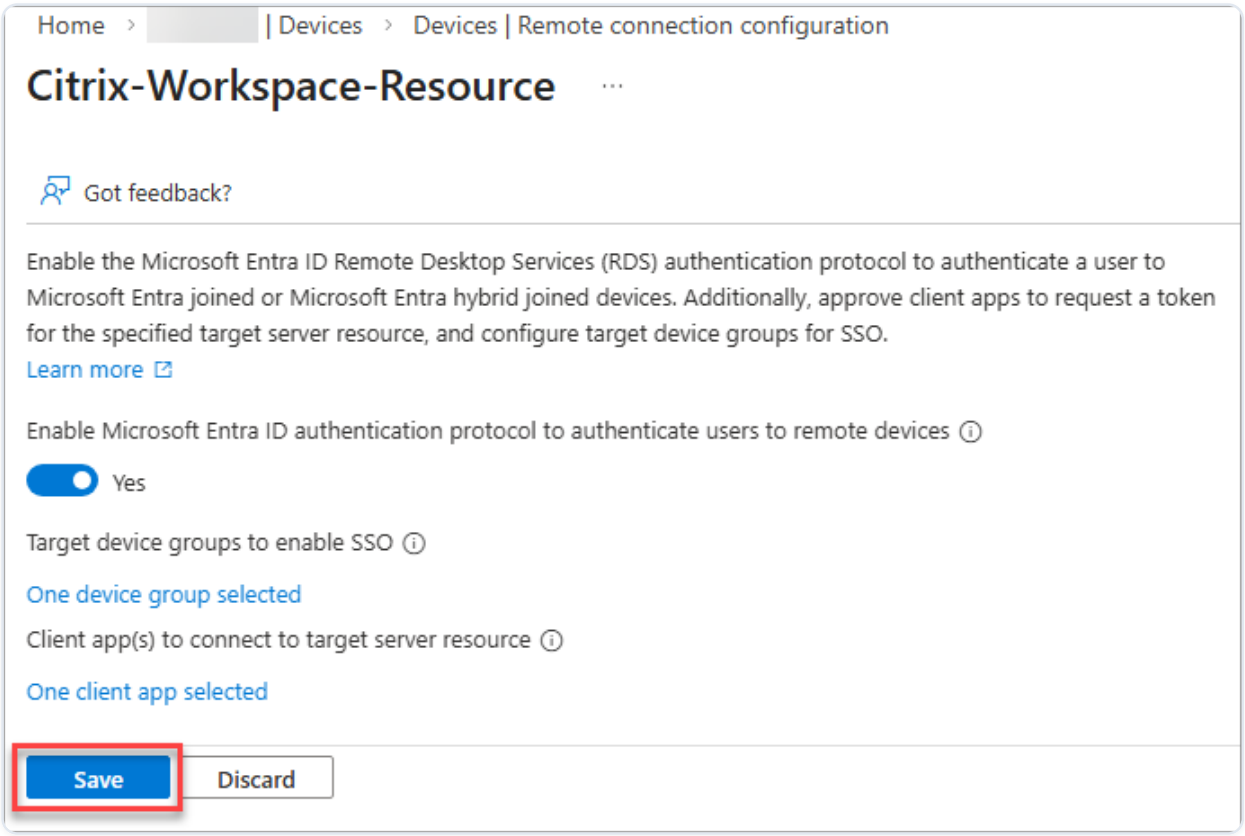
1. 单击链接以添加您的受信任客户端应用程序。



2. 选择 Citrix Client 应用程序。



3. 选择**保存**以将配置更改应用于 Citrix 资源应用程序。



4. 继续创建 Kerberos 服务器对象。

创建 Kerberos 服务器对象

如果您的会话主机是 Microsoft Entra 混合加入的，则必须在用户和计算机帐户所在的 Active Directory 域中配置 Kerberos 服务器对象。有关详细信息，请参阅创建 Kerberos 服务器对象。

查看 Microsoft Entra 条件访问策略

如果您使用或计划使用 Microsoft Entra 条件访问策略，请查看应用于 Citrix 资源应用程序 的配置，以确保用户获得预期的登录体验。

有关在使用 Microsoft Entra 单一登录时配置条件访问的详细指南，请参阅 Microsoft 文档。请记住，所需的条件访问设置必须应用于 **Citrix 资源应用程序**，而不是 Citrix 客户端应用程序或 Microsoft 应用程序。

CITRIX 会话主机

确保满足会话主机的系统要求：

1. 确保会话主机已 Microsoft Entra 混合加入。
2. 按照系统要求安装所需的操作系统版本和内部版本。
3. 按照系统要求安装所需的 VDA 版本。

Microsoft Entra 混合加入的会话主机

当使用 Citrix Machines Creation Services、Citrix Provisioning 或 Windows 365 部署 Microsoft Entra 混合加入的会话主机时，请继续下一节。如果您使用任何其他工具或方法预配 Microsoft Entra 混合加入的主机，则必须将以下注册表值添加到您的会话主机：

- 键：`HKLM\SYSTEM\CurrentControlSet\Control\Citrix`
- 值类型：**DWORD**
- 值名称：`AzureADJoinType`
- 数据: `1`

会话锁定行为
当虚拟桌面被锁定时，默认行为是显示 Windows 锁定屏幕。此时，支持的桌面解锁身份验证方法是**用户名和密码**或**智能卡**。

> **注意**
>
> Citrix Web 登录（预览版）允许您使用基于 Web 的 Entra 身份验证解锁桌面。有关详细信息，请参阅Web 登录。

> 如果您部署了无密码环境，用户不知道其密码，建议将会话锁定行为配置为断开会话连接，而不是显示锁定屏幕。

您可以通过 Intune 或组策略启用**锁定远程会话时断开 Microsoft 身份平台身份验证**设置来配置此行为。有关详细步骤，请参阅配置 Azure 虚拟桌面的会话锁定行为。

CITRIX 访问和控制平面

StoreFront 配置
要在 StoreFront 中启用 Microsoft Entra 单点登录，请参阅 StoreFront 文档中的 Entra ID single-on 。
在 Web Studio 中启用 Microsoft Entra 单点登录
要在您的站点上启用 Microsoft Entra 单点登录，您必须添加客户端和资源应用程序详细信息以及重定向 URI。有关详细信息，请参阅 Settings 文档。
为交付组启用 Microsoft Entra 单点登录
使用 Web Studio

1. 在 Web Studio 中转到交付组，然后单击 **创建交付组**。
2. 在 **用户** 页面上，选择 **Microsoft Entra 混合加入** 作为身份类型。
3. 在以下页面上完成配置。有关参考，请参阅 创建交付组。

使用 PowerShell

1. 创建新的交付组并将 VDA 添加到交付组。将用户（AD 帐户）分配给 VDA。
2. 将交付组 `MachineLogonType` 设置为 `HybridAzureAd`。例如：

```
Get-BrokerDesktopGroup -Name <dgName> | Set-BrokerDesktopGroup
-MachineLogOnType "HybridAzureAd"
```

3. 信任 Xml 服务。

```
Add-PSSnapin Citrix.Broker.Admin.V2

Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

4. 设置 SSO 参数（请参阅下表获取指导）。

```
Set-BrokerSite -AzureGlobalCloudId "B16898C6-
A148-4967-9171-64D755DA8520" -AzureSSOnAuthorizeUrl "<URL>"
-AzureSSOnClientId "<clientAppID>" -AzureSSOnRedirectUrl "<URL>"
-AzureSSOnResourceAppId "<resourceAppID>"
```

下表提供了参数及其默认值的详细信息：

参数	默认值	描述
AzureGlobalCloudId	B16898C6-A148-4967-9171-64D755DA8520	标识 Windows 中的 Entra CloudAP。
AzureSSOnAuthorizeUrl	`https://login.microsoftonline.com/common/`	初始登录 URL。这取决于 Entra 租户所在的 Azure 云（例如 Azure Commercial 与 Azure Gov）
AzureSSOnClientId	无默认值	客户端应用程序的应用程序 ID。
AzureSSOnRedirectUrl	无默认值	身份验证后重定向 URI。它必须是客户端应用程序中配置为重定向 URI 的 URL。

参数	默认值	描述
AzureSSOnResourceAppId	3a510bb1-e334-4298-831e-3eac97f8b26c	Citrix 资源应用程序的应用程序 ID。

在 VDA 上配置 Microsoft Entra 单点登录

默认情况下，VDA 上已启用 Microsoft Entra 单点登录。要为部分会话主机启用或禁用此功能，请使用Microsoft Entra 单点登录策略设置。

客户端设备

确保满足客户端设备的系统要求：

1. 安装 系统要求 中指定的 Citrix Workspace 应用程序版本。
2. 如果您的用户将利用混合访问，请确保已安装 Citrix Web Extension。如果您的用户将使用本机或浏览器访问，则不需要 Citrix Web Extension。

故障排除

> **注意**
>
> 有关 StoreFront 问题的故障排除，请参阅 诊断日志。

已知问题

- 如果 Storefront 显示错误 `There was a failure with the mapped account`，这可能是因为用户是 Entra ID 用户，但在 Active Directory 中没有匹配的用户。
- 如果会话启动在 ICA 文件发布之前失败，请确保已启用 XML 信任。
- 如果 VDA 状态停留在“正在初始化”，请确保 Active Directory 中的计算机对象位于与 Entra ID 同步的 OU 中。
- 如果在 Entra ID 中禁用了“**保持登录状态 (KMSI)**”，则 Linux 和 macOS 客户端设备上的单点登录将失败。

单点登录失败时

如果在访问虚拟桌面或应用程序时单点登录失败，请按以下步骤操作：

1. 确认 StoreFront 中已启用 Microsoft Entra 单点登录。
2. 确认您的站点中已启用 Microsoft Entra 单点登录。

3. 确认交付组中已启用 Microsoft Entra 单点登录。
4. 确认用户使用的访问方法受支持。
5. 如果用户正在使用混合访问，请确认已安装 Citrix Web Extension。
6. 确认客户端设备正在运行所需的 Citrix Workspace 应用程序版本。
7. 确认您的会话主机正在运行所需的 Windows 版本。
8. 确认您的会话主机正在运行所需的 VDA 版本。
9. 确保会话主机上未启用 Windows 设置 `Always prompt for password upon connection`。此设置默认禁用，可以通过组策略或 Intune 在 `Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security` 下进行配置。您可以通过在注册表中查找 `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services` 下的值 `fPromptForPassword` 来检查该设置是否已启用。如果该值设置为 `1`，则表示该设置已启用，单点登录将不可用。如果该值缺失或设置为 `0`，则表示该设置已禁用。
10. 确认会话主机中 `AzureADJoinType` 设置配置正确：
    - 键：`HKLM\SYSTEM\CurrentControlSet\Control\Citrix`
    - 值类型：**DWORD**
    - 值名称：`AzureADJoinType`
    - 值数据：`1` (Microsoft Entra 混合加入)
11. 确保在 Citrix Studio 中，虚拟桌面或应用程序分配给 Active Directory 身份，而不是 Entra ID 身份。
12. 确认通过运行以下 PowerShell 命令正确配置了交付组的登录类型：

    ```
    Get-BrokerDesktopGroup -Name <deliveryGroupName>
    ```

    对于 Microsoft Entra 混合加入的会话主机，`MachineLogOnType` 必须设置为 `HybridAzureAd`。
13. 确认 Citrix 资源应用程序和单租户客户端应用程序已注册到 Microsoft Entra 租户。
14. 确认 Microsoft Entra ID RDS 身份验证协议已在 Citrix 资源应用程序上启用。
15. 确认客户端应用程序已作为批准的客户端应用程序添加到 Citrix 资源应用程序中。
16. 如果您的会话主机已加入 Microsoft Entra 混合模式，请确认已在用户和计算机帐户所在的 Active Directory 域中创建了 Kerberos 服务器对象。

17. 检查您的 Microsoft Entra 条件访问策略。确保没有策略应用于 Citrix 客户端应用程序，并且应用于 Citrix 资源应用程序或会话主机的任何策略都已正确配置，以免影响单点登录体验。

联邦身份验证服务

Citrix 联邦身份验证服务 (FAS) 允许用户在通过 SAML 或 OpenID Connect (OIDC) 等不提供 Windows 密码的现代身份提供商进行身份验证的环境中，对 Citrix 虚拟桌面和应用程序进行单点登录 (SSO)，从而确保无缝访问已加入 Active Directory 域的会话主机。

有关更多详细信息，请参阅联合身份验证服务文档。

智能卡

Citrix Virtual Apps and Desktops 和 Citrix DaaS 支持智能卡登录虚拟桌面和应用程序，并在活动会话中使用。智能卡提供基于证书的双因素身份验证，通过同时要求物理卡和 PIN 码来增强安全性。这使得组织能够满足合规性要求、保护敏感数据，并为已经依赖智能卡进行 Windows 登录或安全应用程序的用户简化访问。一旦通过身份验证，用户还可以在会话中使用智能卡对文档进行数字签名、加密电子邮件或访问其他支持智能卡的应用程序，从而确保在本地和虚拟环境中获得一致且安全的体验。

有关智能卡的文档，了解更多详细信息。

Web 登录 (预览)

您可以使用 Citrix Web 登录凭据提供程序来启用基于 Entra ID 的 Windows 身份验证。这允许用户使用 Entra ID 中启用的任何身份验证方法登录或解锁其虚拟桌面。

> **重要**
>
> Web 登录目前处于预览阶段。此功能不提供支持，尚不建议在生产环境中使用。

系统要求

以下是使用 Web 登录的系统要求：

- 虚拟投递代理
  - Windows：**单会话**版本 2607 或更高版本
- Citrix Workspace 应用程序
  - Windows：版本 2607 或更高版本

- 会话主机身份：Entra 混合加入
- 会话主机操作系统：
  - Windows 11，版本 24H2，并安装了 2025 年 9 月 Windows 11 累积更新 (KB5065789) 或更高版本（内部版本 26100.6725）

如何配置 Web 登录

Citrix Web 登录默认处于禁用状态。要启用它，请按照以下步骤操作：

1. 完成 Microsoft Entra 单点登录 文档中描述的**Azure 和 Microsoft Entra ID 配置**。如果您的环境中已启用 Microsoft Entra 单点登录，则可以继续执行下一步。

   相关步骤包括：

   a. 注册 Citrix 资源和客户端应用程序。
   b. 为 Citrix 资源应用程序启用 Microsoft Entra ID 远程桌面服务身份验证协议。
   c. 隐藏用户同意提示。
   d. 批准客户端应用程序。
   e. 创建 Kerberos 服务器对象（仅限 Microsoft Entra 混合加入环境）。
   f. 审查 Microsoft Entra 条件访问策略。

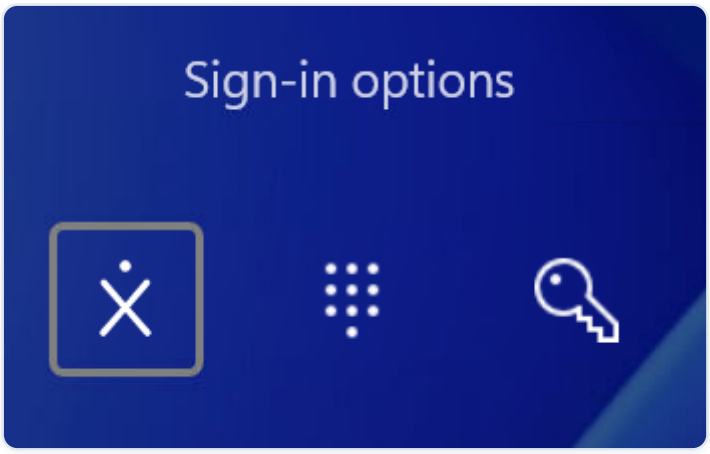
2. 在 Citrix 策略中启用 **Web 登录** 设置，并将策略应用于相应的交付组。

> **注意**
>
> - 无需使用 Microsoft Entra 单点登录即可使用 Web 登录。
> - 如果您的环境中没有此策略设置，您可以通过注册表启用 Web 登录：
>   - 键：HKLM\SOFTWARE\Policies\Citrix\ICAPolicies
>   - 值类型: DWORD
>   - 值名称：AllowWebSignIn
>   - 值数据: 1

如何使用 Web 登录

要使用 Citrix Web 登录登录或解锁您的虚拟桌面：

1. 从可用的登录方法中选择 Citrix 磁贴。



2. 单击 **Citrix Web 登录**。



3. 身份验证提示弹出后，使用所需的身份验证方法进行身份验证。

> **注意**
>
> 用户可用的身份验证方法由 Microsoft Entra ID 中启用的内容决定。

准备安装

部署 Citrix Virtual Apps and Desktops™ 始于安装以下组件。此过程为向防火墙内的用户交付应用程序和桌面做准备。

- 一个或多个 Delivery Controller
- 思杰 Director

- 思杰 StoreFront™
- Citrix 许可证服务器
- 一个或多个 Citrix Virtual Delivery Agent (VDA)
- 可选组件和技术，例如通用打印服务器、联合身份验证服务和自助密码重置

对于防火墙外的用户，请安装并配置一个额外组件，例如 Citrix Gateway。有关介绍，请参阅将 Citrix Virtual Apps and Desktops 与 Citrix Gateway 集成。

> **注意：**
>
> 请确保在服务器操作系统和工作站操作系统上满足以下 Microsoft 先决条件：
>
> - Microsoft **卷影复制**和 **Microsoft 软件卷影复制提供程序**服务正在运行。有关详细信息，请参阅卷影复制服务。
> - **MS-Defender** 版本必须高于 4.18.2105.5。有关详细信息，请参阅Microsoft Defender 防病毒安全智能和产品更新。
>
> 如果您的部署包含 Windows Server 工作负载，请配置 Microsoft RDS 许可证服务器。

您可以使用产品 ISO 上的完整产品安装程序部署许多组件和技术。您可以使用独立的 VDA 安装程序安装 VDA。独立的 VDA 安装程序可在 Citrix 下载站点上获取。所有安装程序都提供图形和命令行界面。请参阅安装程序。

产品 ISO 包含用于在 Active Directory 中安装、升级或删除计算机 VDA 的示例脚本。您还可以使用这些脚本来管理 Machine Creation Services (MCS) 和 Citrix Provisioning（以前称为 Provisioning Services）使用的映像。有关详细信息，请参阅使用脚本安装 VDA。

安装前要查看的信息

- 技术概述：熟悉产品及其组件。
- 安全性：规划部署环境时。
- 已知问题：此版本中可能遇到的问题。
- 数据库：了解系统数据库以及如何配置它们。在 Controller 安装过程中，您可以安装 SQL Server Express 作为站点数据库。在安装核心组件后创建站点时，可以配置大多数数据库信息。
- 远程电脑访问：如果您要部署一个环境，使用户能够远程访问其办公室中的物理计算机。

- 连接和资源：如果您使用虚拟机管理程序或其他服务来托管或预配用于应用程序和桌面的 VM。在创建站点时（安装核心组件后），您可以配置第一个连接。在此之前设置您的虚拟化环境。
- Microsoft System Center Configuration Manager：如果您使用 ConfigMgr 管理对应用程序和桌面的访问，或者如果您将局域网唤醒功能与远程电脑访问结合使用。
- **公有云主机连接：**如果您拥有混合权利许可证，则可以创建到公有云的主机连接。有关混合权利许可证的信息，请参阅 Hybrid Rights Renewals。有关公有云权利以及此更改原因的信息，请参阅 CTX270373。

组件安装位置

查看 System requirements 以了解支持的平台、操作系统和版本。组件必备项会自动安装，除非另有说明。有关 Citrix StoreFront 和 Citrix 许可证服务器支持的平台和必备项，请参阅其文档。

您可以将核心组件安装在同一台服务器上，也可以安装在不同的服务器上。

- 将所有核心组件安装在一台服务器上适用于评估、测试或小型生产部署。
- 为了适应未来的扩展，请考虑将组件安装在不同的服务器上。例如，将 Studio 安装在与安装 Controller 的服务器不同的计算机上，可以远程管理站点。
- 对于大多数生产部署，建议将核心组件安装在单独的服务器上。

  在其他服务器上安装其他组件之前，请先安装 Citrix 许可证服务器和许可证。
- 要在 Server CoreOS（例如交付控制器）上安装受支持的组件，您必须(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-core/install-command.html)。该操作系统类型不提供图形界面，因此请在其他位置安装 Studio 和其他工具，然后将它们指向控制器服务器。

您可以在同一台服务器上安装 Delivery Controller™ 和多会话操作系统 VDA。启动安装程序并选择 Delivery Controller（以及您希望在该计算机上安装的任何其他核心组件）。然后再次启动安装程序并选择多会话操作系统的 **Virtual Delivery Agent**。

确保每个操作系统都具有最新更新。

确保所有计算机都具有同步的系统时钟。保护计算机之间通信的 Kerberos 基础结构需要同步。

对于 XenServers，即使虚拟机显示为已注册，其电源状态也可能显示为未知。要解决此问题，请编辑注册表项 `HostTime` 值以禁用与主机的时钟同步：

```
HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\HostTime="Local"
```

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\XenTools\HostTime="Local"
```

> **提示：**

> 默认值为 `HostTime="UTC"`。将此值更改为 UTC 以外的值，例如 `Local`。此更改可有效禁用与主机的时钟同步。

> 有关 Windows 10 单会话计算机的优化指南，请参阅 CTX216252。

不应安装组件的位置：

- 不要在 Active Directory 域控制器上安装任何组件。
- 不支持在 SQL Server 群集安装、SQL Server 镜像安装中的节点上或在运行 Hyper-V 的服务器上安装控制器。

如果您尝试在当前产品版本不支持的 Windows 操作系统上安装或升级 VDA，则会显示一条消息，引导您阅读一篇介绍相关选项的文章。

权限和 Active Directory 要求

您必须是域用户，并且是安装组件的计算机上的本地管理员。

要使用独立 VDA 安装程序，您必须具有提升的管理员权限或使用“**以管理员身份运行**”。

在开始安装之前，请配置您的 Active Directory 域。

- 系统要求 列出了支持的 Active Directory 功能级别。Active Directory 加入 包含更多信息。
- 您必须至少有一个运行 Active Directory 域服务的域控制器。
- 请勿在域控制器上安装任何 Citrix Virtual Apps and Desktops™ 组件。
- 在 Studio 中指定组织单位名称时，请勿使用正斜杠 (/)。

用于安装 Citrix 许可证服务器的 Windows 用户帐户会自动配置为委派管理完全管理员。

有关详细信息：

- 安全最佳实践
- 委派管理
- 有关 Active Directory 配置的 Microsoft 文档

安装指南、注意事项和最佳实践

安装任何组件期间

- 从完整产品介质安装或升级 Delivery Controller、Studio、License Server 或 Director 时，如果 Citrix 安装程序检测到计算机上存在先前 Windows 安装导致的待处理重新启动，安装程序将停止并显示退出/返回代码 9。系统会提示您重新启动计算机。

  这不是 Citrix 强制重新启动。这是由于计算机上先前安装的其他组件引起的。如果发生这种情况，请重新启动计算机，然后再次启动 Citrix 安装程序。

  使用命令行界面时，您可以通过在命令中包含 `/no_pending_reboot_check` 选项来阻止检查待处理的重新启动。
- 通常，如果某个组件具有先决条件，则安装程序会在它们不存在时部署它们。某些先决条件可能需要重新启动计算机。
- 在安装之前、期间和之后创建对象时，请为每个对象指定唯一的名称。例如，为网络、组、目录和资源提供唯一的名称。
- 如果某个组件未能成功安装，安装将停止并显示错误消息。已成功安装的组件将保留。您无需重新安装它们。
- 安装（或升级）组件时，Citrix Analytics 会自动收集。默认情况下，安装完成后，这些数据会自动上传到 Citrix。此外，安装组件时，您会自动加入 Citrix 客户体验改善计划 (CEIP)，该计划会上传匿名数据。

  在安装过程中，您还可以选择参与其他 Citrix 技术，这些技术会收集诊断信息以用于维护和故障排除。有关这些计划的信息，请参阅 Citrix Insight Services。
- 如果 VDA 安装失败，MSI 分析器会解析失败的 MSI 日志，并显示确切的错误代码。如果这是一个已知问题，分析器会建议一篇 CTX 文章。分析器还会收集有关失败错误代码的匿名数据。此数据包含在 CEIP 收集的其他数据中。如果您终止 CEIP 注册，则收集的 MSI 分析器数据将不再发送到 Citrix。

VDA 安装期间

- 适用于 Windows 的 Citrix Workspace™ 应用程序可用，但在安装 VDA 时默认不安装。您或您的用户可以从 Citrix 网站下载、安装（和升级）适用于 Windows 的 Citrix Workspace 应用程序以及其他 Citrix Workspace 应用程序。或者，您可以从 StoreFront 服务器提供这些 Citrix Workspace 应用程序。请参阅 StoreFront 文档。
- 必须启用 Microsoft Print Spooler 服务。如果该服务被禁用，则无法成功安装 VDA。
- 必须禁用 Windows Protected Print (WPP) 模式。如果启用了 WPP 模式，则无法成功安装 VDA。

- 大多数受支持的 Windows 版本都已预装 Microsoft Media Foundation。如果计算机没有 Media Foundation（例如 N 版本），则某些多媒体功能将不会安装且无法工作。
  - Windows Media 重定向
  - HTML5 视频重定向
  - HDX™ RealTime 网络摄像头重定向

  您可以确认此限制，或者结束 VDA 安装并在安装 Media Foundation 后重新启动。在图形界面中，此选择会显示在消息中。在命令行中，您可以使用 `/no_mediafoundation_ack` 选项来确认此限制。
- 安装 VDA 时，会自动创建一个名为 **Direct Access Users** 的新本地用户组。在单会话操作系统 VDA 上，此组仅适用于 RDP 连接。在多会话操作系统 VDA 上，此组适用于 ICA® 和 RDP 连接。
- VDA 必须具有有效的 Controller 地址才能进行通信。否则，无法建立会话。您可以在安装 VDA 时或之后指定 Controller 地址。请记住，必须完成此操作。有关详细信息，请参阅 VDA 注册。

VDA 安装后和安装期间的重新启动

VDA 安装结束时需要重新启动。默认情况下，该重新启动会自动发生。

将 VDA 升级到版本 7.17（或更高支持版本）时，升级期间会发生重新启动。这是无法避免的。

要最大程度地减少 VDA 安装期间所需的重新启动次数：

- 确保在开始 VDA 安装之前已安装受支持的 .NET Framework 版本。
- 对于 Windows 多会话操作系统计算机，请在安装 VDA 之前安装并启用 RDS 角色服务。

如果您在安装 VDA 之前未安装这些必备项：

- 如果您使用的是图形界面或不带 `/noreboot` 选项的命令行界面，则计算机在安装必备项后会自动重新启动。
- 如果您使用的是带 `/noreboot` 选项的命令行界面，则必须手动启动重新启动。

升级 VDA 版本时，升级过程中会发生重启。这是无法避免的。

安装或升级失败时恢复

> **注意：**

> 此功能仅适用于工作站 VDA。为确保更可靠、更流畅的安装体验，服务器 VDA 不再支持“故障时恢复”功能。Citrix 建议在安装或升级服务器 VDA 之前手动创建备份。

> 如果工作站 VDA 安装或升级失败，并且启用了“故障时恢复”功能，则计算机将恢复到安装或升级开始之前设置的还原点。

当工作站 VDA 安装或升级在启用此功能的情况下开始时，安装程序会在实际安装或升级开始之前创建一个系统还原点。如果 VDA 安装或升级失败，计算机将恢复到还原点状态。`%temp%/Citrix` 文件夹包含部署日志和有关恢复的其他信息。

默认情况下，此功能处于禁用状态。

如果您计划启用此功能，请确保未通过 GPO 设置禁用系统还原 (`Computer Configuration > Administrative Templates > System > System Restore`)。

在安装或升级工作站 VDA 时启用此功能：

- 使用 VDA 安装程序的图形界面（例如，使用 **Autostart** 或不带任何恢复或静默选项的 `XenDesktopVDASetup.exe` 命令）时，在“**附加组件**”页面上选中 **Citrix Backup and Restore Service** 复选框。

  如果安装/升级成功完成，则还原点不会被使用，但会保留。
- 使用命令行运行 VDA 安装程序并添加以下选项之一：`/enablerestorecleanup`、`/enablerestore` 或 `/includeadditional` "Citrix Backup and Restore"。
  - 如果您使用 `/enablerestorecleanup` 选项，并且安装/升级成功完成，则还原点将自动删除。
  - 如果您使用 /enablerestore 或 /includeadditional "Citrix Backup and Restore" 选项，并且安装/升级成功完成，则还原点不会被使用，但会保留。

> **注意：**

> 如果您尝试在服务器 VDA 上使用 `/enablerestorecleanup`、`/enablerestore` 或 `/includeadditional` "Citrix Backup and Restore" 选项，安装程序将忽略这些选项并继续，而不会创建备份。

安装程序

完整产品安装程序

使用 ISO 中提供的完整产品安装程序，您可以：

- 安装、升级或删除核心组件：Delivery Controller、Studio、Director 和 License Server。
- 安装或升级 StoreFront。
- 安装或升级用于单会话或多会话操作系统的 Windows VDA。
- 在您的打印服务器上安装 Universal Print Server `UpsServer` 组件。
- 安装 联邦身份验证服务。
- 安装 会话录制。
- 安装 工作区环境管理。

> **注意：**
>
> Workspace Environment Management™ 代理安装程序未本地化。它仅提供英文版本。

要从多会话操作系统为单个用户（例如，用于 Web 开发）交付桌面，请使用完整产品安装程序的命令行界面。有关详细信息，请参阅 Server VDI。

独立 VDA 安装程序

独立 VDA 安装程序可在 Citrix 下载页面上获取。（它们不随产品安装介质提供。）独立 VDA 安装程序比完整产品 ISO 小得多。它们更容易适应以下部署：

- 使用本地暂存或复制的电子软件分发 (ESD) 软件包
- 拥有物理机
- 拥有远程办公室

默认情况下，自解压独立 VDA 中的文件会提取到 **Temp** 文件夹。与使用完整产品安装程序相比，提取到 **Temp** 文件夹时，计算机上需要更多的磁盘空间。但是，提取到 **Temp** 文件夹的文件在安装完成后会自动删除。或者，您可以使用带绝对路径的 `/extract` 命令。

有四种独立的 VDA 安装程序可供下载。

多会话操作系统虚拟投递代理 (VDAServerSetup.exe)：

为多会话操作系统安装 VDA。它支持完整产品安装程序提供的所有多会话操作系统 VDA 选项。

单会话操作系统虚拟投递代理 (VDAWorkstationSetup.exe)：

为单会话操作系统安装 VDA。它支持完整产品安装程序提供的所有单会话操作系统 VDA 选项。

单会话操作系统核心服务虚拟投递代理 (VDAWorkstationCoreSetup.exe)：

为单会话操作系统安装 VDA，该 VDA 针对远程电脑访问部署或核心 VDI 安装进行了优化。远程电脑访问使用物理机。核心 VDI 安装是未用作映像的 VM。它仅安装此类部署的 VDA 连接所需的核心服务。因此，它仅支持完整产品或 `VDAWorkstationSetup.exe` 安装程序中有效选项的子集。

此安装程序不安装或不包含用于以下目的的组件：

- 应用虚拟化。
- 配置文件管理。将 Citrix Profile Management 从安装中排除会影响 Citrix Director 显示。有关详细信息，请参阅安装 VDA。
- 计算机身份服务。
- Citrix MCS I/O 驱动程序
- Citrix 备份和还原
- deviceTRUST
- uberAgent
- WEM

`VDAWorkstationCoreSetup.exe` 安装程序不安装或不包含以下组件：适用于 Windows 的 Citrix Workspace 应用程序 (CWA)、Citrix Secure Access Client (CSA)、Citrix 用户个性化层 (UPL)、会话录制代理 (SRAGENT) 和 Citrix Assistant App (ASSISTANTAPP)。

使用 `VDAWorkstationCoreSetup.exe` 等同于使用完整产品或 `VDAWorkstationSetup` 安装程序安装单会话操作系统 VDA，并执行以下任一操作：

- 在图形界面中：在**环境**页面上选择“远程电脑访问”选项。
- 在命令行界面中：指定 `/remotepc` 选项。
- 在命令行界面中：指定 `/components vda` 以及列出所有有效附加组件名称的 `/exclude` 选项。

您可以通过运行完整产品安装程序来稍后安装省略的组件/功能。该操作使您能够安装所有缺失的组件。

`VDAWorkstationCoreSetup.exe` 安装程序会自动安装 Browser Content Redirection MSI。此自动安装适用于 VDA 2003 及更高版本支持的版本。

单会话核心服务虚拟投递代理 (VDASingleSessionCoreSetup.exe)：

适用于 Windows 365 Cloud PC 和远程电脑部署的新型轻量级单会话 VDA 元安装程序。此安装程序基于现有 VDAWorkstationCoreSetup.exe 安装程序构建，提供必要的 VDA 组件以及配置文件管理、deviceTRUST、uberAgent、WEM、备份和还原以及 VDA 升级代理。可以使用命令行选项 /enablerestore 或 /enablerestorecleanup 启用备份和还原功能。

它显著减小了程序包大小，并提高了基于云的工作负载的安装可靠性。此安装程序专为现代远程电脑场景设计，为在 Windows 365 和远程电脑上部署 Citrix 工作负载提供了简化且高性能的选项。

使用单会话 VDA 安装程序的最佳实践

对于单会话操作系统，有四种不同的安装程序可用。完整产品 VDA 安装程序和 VDAWorkstationSetup.exe 安装程序提供所有组件的安装，而 VDAWorkstationCoreSetup.exe 和 VDASingleSessionCoreSetup.exe 安装程序不包含某些默认和附加组件。

为了保持环境稳定性、一致的性能和持续的可支持性，Citrix 建议在 Citrix VDA 的整个生命周期（包括安装、升级和卸载）中，使用一致的安装程序类型。混合使用安装程序类型可能会带来某些风险。

混合安装程序类型相关的风险：

场景 1： 如果单会话 VDA 最初使用 VDAWorkstationCoreSetup.exe 或 VDASingleSessionCoreSetup.exe 安装程序安装，随后使用完整产品 VDA 安装程序或 VDAWorkstationSetup.exe 安装程序进行升级，则除非明确排除，否则以前排除的组件可能会在升级期间安装。

场景 2： 如果单会话 VDA 最初使用完整产品 VDA 安装程序或 VDAWorkstationSetup.exe 安装，随后使用 VDAWorkstationCoreSetup.exe 或 VDASingleSessionCoreSetup.exe 进行升级，则核心服务 VDA 安装程序未安装的任何组件都将从升级中排除。这些组件在升级过程中既不会升级，也不会在卸载期间删除。

场景 3： 如果单会话 VDA 最初使用 VDAWorkstationCoreSetup.exe 安装程序安装，随后使用 VDASingleSessionCoreSetup.exe 进行升级，您将体验到新功能。如果您下次使用 VDAWorkstationCoreSetup.exe 进行升级，则 VDASingleSessionCoreSetup.exe 新增的组件在升级过程中既不会升级，也不会在卸载期间删除。

解决混合安装程序类型的指南：

如果需要混合安装程序类型，则必须确保在升级过程中包含相同的组件。

如果安装程序类型不慎混用，导致安装了额外的组件或某些组件脱离了管理，并且需要恢复到以前的环境，请按以下步骤操作：

- **对于场景 1：** 从 Windows 的卸载或更改程序功能中卸载 VDA，然后使用您最初使用的安装程序（VDAWorkstationCoreSetup.exe 或 VDASingleSessionCoreSetup.exe）重新安装 VDA。
- **对于场景 2：** 使用完整产品 VDA 安装程序或 VDAWorkstationSetup.exe 安装程序升级缺失的组件。
- **对于场景 3：** 如果您打算继续利用新功能，请使用 VDASingleSessionCoreSetup.exe 安装程序升级缺失的组件。或者，如果您在通过 VDASingleSessionCoreSetup.exe 升级后不希望使用新功能，请首先从 Windows 的卸载或更改程序功能中卸载 VDA，然后使用 VDAWorkstationCoreSetup.exe 重新安装 VDA。

Citrix 安装返回代码

安装日志包含组件安装结果，其形式为 Citrix 返回代码，而非 Microsoft 值。

- 0 = 成功
- 1 = 失败
- 2 = 部分成功
- 3 = 部分成功且需要重新启动
- 4 = 失败且需要重新启动
- 5 = 用户取消
- 6 = 命令行参数错误
- 7 = 发现新版本
- 8 = 成功，需要重新启动
- 9 = 文件锁定，需要重新启动
- 10 = 已中止
- 11 = 介质失败
- 12 = 许可证失败
- 13 = 预检失败
- 14 = 已中止，待处理重新启动检查
- 15 = 预检通过 - 在使用新的 /precheckonly 命令行选项后，如果预检通过，则返回此值。
- 16 = 预检失败 - 在使用新的 /precheckonly 命令行选项后，如果预检失败，则返回此值。
- 17 = 可选软件失败 - 当新的可选软件组件之一安装失败，并且已选择“如果任何其他选定组件失败，则继续 VDA 安装或升级”时，将返回此值。

例如，当使用 Microsoft System Center Configuration Manager 等工具时，如果安装日志包含返回代码 3，则脚本化的 VDA 安装可能看似失败。这可能发生在 VDA 安装程序正在等待您必须启动的重新启动时（例如，在服务器上安装 RDS 角色先决条件之后）。只有在安装了所有先决条件和选定组件，并且安装后重新启动计算机，VDA 安装才被视为成功。

或者，您可以将安装包装在 CMD 脚本中（这些脚本返回 Microsoft 退出代码），或者更改 Configuration Manager 包中的成功代码。

为 Windows Server 工作负载配置 Microsoft RDS 许可证服务器

此产品在交付 Windows Server 工作负载（例如 Windows 2016）时访问 Windows Server 远程会话功能。这通常需要远程桌面服务客户端访问许可证 (RDS CAL)。VDA 必须能够联系 RDS 许可证服务器以请求 RDS CAL。安装并激活许可证服务器。有关详细信息，请参阅 Microsoft 文档 激活远程桌面服务许可证服务器。对于概念验证环境，您可以使用 Microsoft 提供的宽限期。

使用此方法，您可以让此服务应用许可证服务器设置。您可以在映像上的 RDS 控制台中配置许可证服务器和每用户模式。您还可以使用 Microsoft 组策略设置配置许可证服务器。有关详细信息，请参阅 Microsoft 文档 使用客户端访问许可证 (CAL) 许可 RDS 部署。

要使用组策略设置配置 RDS 许可证服务器：

1. 在可用计算机上安装远程桌面服务许可证服务器。该计算机必须始终可用。Citrix 产品工作负载必须能够访问此许可证服务器。
2. 使用 Microsoft 组策略指定许可证服务器地址和每用户许可证模式。有关详细信息，请参阅 Microsoft 文档 为 RD 会话主机服务器指定远程桌面许可模式。

Windows 10 工作负载需要适当的 Windows 10 许可证激活。我们建议您遵循 Microsoft 文档来激活 Windows 10 工作负载。

更多信息

对于特定主机类型的资源位置设置：

- AWS 云环境
- XenServer 虚拟化环境
- Google Cloud 环境
- Microsoft Azure 资源管理器云环境
- Microsoft System Center 配置管理器环境
- Microsoft System Center 虚拟机管理器虚拟化环境
- Nutanix 虚拟化环境

- Nutanix 云和合作伙伴解决方案
- VMware 虚拟化环境
- VMware 云和合作伙伴解决方案

Amulet Hotkey CoreStation 虚拟化环境

Citrix Virtual Apps and Desktops™ 通过 Citrix 管理的 Amulet Hotkey CoreStation 插件管理您的 Amulet Hotkey CoreStation 工作负载。借助此插件，您可以创建与 Amulet Hotkey CoreStation 机箱的连接、创建目录以及对目录中的计算机进行电源管理。

关键步骤

1. 设置您的 Amulet Hotkey CoreStation 环境。
2. 创建与 Amulet Hotkey CoreStation 机箱的连接。
3. 创建 Amulet Hotkey CoreStation 计算机目录。

> **注意：**
>
> 在创建目录之前，请确保拥有一台或多台 Amulet Hotkey CoreStation 节点，并在这些节点上安装 VDA。您可以将 Amulet Hotkey CoreStation 机箱视为管理程序，将节点视为虚拟机。

4. 创建交付组。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关创建和管理连接的信息，请参阅 连接到 Amulet Hotkey CoreStation。

更多信息

- 创建和管理连接与资源
- 创建计算机目录

AWS 云环境

本文将指导您如何将 AWS 账户设置为可与 Citrix Virtual Apps and Desktops 配合使用的资源位置。该资源位置用于在 AWS EC2 和 Amazon WorkSpaces Core 托管实例中预配工作负载。有关 Amazon WorkSpaces Core 托管实例支持的操作系统类型列表，请参阅 Amazon WorkSpaces Core 托管实例中的 VDA。

不同可配置资源位置的比较：适用于 AWS EC2 的 MCS、适用于 Amazon WorkSpaces Core 托管实例的 MCS 以及 适用于 Amazon WorkSpaces Core 捆绑包的快速部署。

适用于 AWS EC2 的 MCS	适用于 AMAZON WORKSPACES CORE 托管实例的 MCS	适用于 AMAZON WORKSPACES CORE 捆绑包的快速部署
Citrix® 处理您 AWS 账户中的 VM 预配	Citrix 处理您 AWS 账户中的 VM 预配	Amazon 处理 AWS 托管的 WorkSpaces 账户中的 VM 预配
用于 VM 生命周期管理的高级 MCS 工作流	用于 VM 生命周期管理的高级 MCS 工作流	5 步快速简便的工作流
EC2 实例	WorkSpaces Core 托管实例（利用直接启动到您的 AWS 账户中的按需 EC2 实例）	WorkSpaces 捆绑包，完全由 AWS 管理的容量（更高级别的抽象）
无 Microsoft 365 许可支持	BYOL Microsoft 365 支持	BYOL Microsoft 365 支持
Windows 服务器、Windows 桌面和 Linux	Windows 服务器、Windows 桌面和 Linux	Windows 服务器、Windows 桌面
持久和非持久 VM	持久和非持久 VM	仅持久 VM
仅按需付费	按需付费	仅按月固定价格
思杰 DaaS 和 思杰虚拟应用和桌面™	思杰 DaaS 和 思杰虚拟应用和桌面™	仅限 Citrix DaaS

完成本文中的任务后，您的资源位置将包含以下组件：

- 一个虚拟私有云 (VPC)，其中包含单个可用区内的公共子网和私有子网。
- 一个实例，在 VPC 的私有子网中运行，既作为 Active Directory 域控制器又作为 DNS 服务器。

- 在 VPC 的公共子网中充当堡垒主机的实例。此实例用于启动到私有子网中实例的 RDP 连接，以进行管理。完成资源位置设置后，您可以关闭此实例，使其不再易于访问。当您必须管理私有子网中的其他实例（例如 VDA 实例）时，可以重新启动堡垒主机实例。

任务概述

设置具有公共和私有子网的虚拟私有云 (VPC)。 完成此任务后，AWS 会在公共子网中部署一个带有弹性 IP 地址的 NAT 网关。此操作使私有子网中的实例能够访问 Internet。公共子网中的实例可访问入站公共流量，而私有子网中的实例则不能。

配置安全组。安全组充当虚拟防火墙，控制 VPC 中实例的流量。您将规则添加到安全组中，以允许公共子网中的实例与私有子网中的实例通信。您还将这些安全组与 VPC 中的每个实例关联。

创建 DHCP 选项集。对于 Amazon VPC，默认提供 DHCP 和 DNS 服务，这会影响您在 Active Directory 域控制器上配置 DNS 的方式。Amazon 的 DHCP 无法禁用，并且 Amazon 的 DNS 只能用于公共 DNS 解析，而不能用于 Active Directory 名称解析。要指定通过 DHCP 传递给实例的域和名称服务器，请创建 DHCP 选项集。该集会分配 Active Directory 域后缀并为 VPC 中的所有实例指定 DNS 服务器。为确保实例加入域时自动注册主机 (A) 和反向查找 (PTR) 记录，请为添加到私有子网的每个实例配置网络适配器属性。

将堡垒主机和域控制器添加到 VPC。通过堡垒主机，您可以登录到私有子网中的实例以设置域并将实例加入域。

任务 1：设置 VPC

1. 在 AWS 管理控制台中，选择 **VPC**。
2. 在 VPC 控制面板中，选择 **Create VPC**（创建 VPC）。
3. 选择 **VPC and more**。
4. 在 NAT 网关 ($) 下，选择 **In 1 AZ** 或 **1 per AZ**。
5. 在 DNS 选项下，保持选中 **Enable DNS hostnames**。
6. 选择 **Create VPC**。AWS 会创建公共和私有子网、Internet 网关、路由表和默认安全组。

任务 2：配置安全组

此任务为您的 VPC 创建并配置以下安全组：

- 一个公共安全组，用于关联公共子网中的实例。
- 一个私有安全组，用于关联私有子网中的实例。

要创建安全组：

1. 在 VPC 控制面板中，选择 **Security Groups**。

2. 为公共安全组创建一个安全组。选择 **Create Security Group**，然后输入该组的名称标签和描述。在 VPC 中，选择您之前创建的 VPC。选择 **Yes, Create**。

配置公共安全组

1. 从安全组列表中，选择公共安全组。
2. 选择“**入站规则**”选项卡并选择“**编辑**”以创建以下规则：

类型	源
所有流量	选择私有安全组。
所有流量	选择公共安全组。
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (会话可靠性)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. 完成后，选择**保存**。
4. 选择“**出站规则**”选项卡并选择“**编辑**”以创建以下规则：

类型	目标
所有流量	选择私有安全组。
所有流量	0.0.0.0/0
ICMP	0.0.0.0/0

5. 完成后，选择**保存**。

配置私有安全组

1. 从安全组列表中，选择私有安全组。

2. 如果您尚未设置来自公共安全组的流量，则必须设置 TCP 端口；选择“**入站规则**”选项卡并选择“**编辑**”以创建以下规则：

类型	源
所有流量	选择私有安全组。
所有流量	选择公共安全组。
ICMP	选择公共安全组。
TCP 53 (DNS)	选择公共安全组。
UDP 53 (DNS)	选择公共安全组。
80 (HTTP)	选择公共安全组。
TCP 135	选择公共安全组。
TCP 389	选择公共安全组。
UDP 389	选择公共安全组。
443 (HTTPS)	选择公共安全组。
TCP 1494 (ICA/HDX)	选择公共安全组。
TCP 2598 (会话可靠性)	选择公共安全组。
3389 (RDP)	选择公共安全组。
TCP 49152–65535	选择公共安全组。

3. 完成后，选择“**保存**”。
4. 选择“**出站规则**”选项卡并选择“**编辑**”以创建以下规则：

类型	目标
所有流量	选择私有安全组。
所有流量	0.0.0.0/0
ICMP	0.0.0.0/0

类型	目标
UDP 53 (DNS)	0.0.0.0/0

5. 完成后，选择**保存**。

任务 3：启动实例

执行以下步骤以创建两个 EC2 实例并解密 Amazon 生成的默认管理员密码：

1. 在 AWS 管理控制台中，选择 **EC2**。
2. 在 EC2 控制面板中，选择 **启动实例**。
3. 选择 Windows Server 计算机映像和实例类型。
4. 在“**配置实例详细信息**”页面上，为实例输入名称并选择您之前设置的 VPC。
5. 在 **子网** 中，为每个实例进行以下选择：
   - 堡垒主机：选择公共子网
   - 域控制器：选择私有子网
6. 在 **自动分配公有 IP 地址** 中，为每个实例进行以下选择：
   - 堡垒主机：选择“**启用**”。
   - 域控制器：选择“**使用默认设置**”或“**禁用**”。
7. 在 **网络接口** 中，输入您的私有子网 IP 范围内的主 IP 地址，供域控制器使用。
8. 如有必要，在 **添加存储** 页面上，修改磁盘大小。
9. 在 **标记实例** 页面上，为每个实例输入一个易记的名称。
10. 在 **配置安全组** 页面上，选择 **选择现有安全组**，然后为每个实例进行以下选择：
    - 堡垒主机：选择公有安全组。
    - 域控制器：选择私有安全组。
11. 查看您的选择，然后选择 **启动**。
12. 创建新的密钥对或选择现有密钥对。如果您创建新的密钥对，请下载您的私钥 (.pem) 文件并将其保存在安全位置。在获取实例的默认管理员密码时，您必须提供您的私钥。
13. 选择 **启动实例**。选择 **查看实例** 以显示您的实例列表。请等待新启动的实例通过所有状态检查后再访问它。
14. 获取每个实例的默认管理员密码：

a. 从实例列表中，选择实例，然后选择 **连接**。

b. 转到 **RDP 客户端** 选项卡，选择 **获取密码**，并在出现提示时上传您的私钥 (`.pem`) 文件。

c. 选择 **Decrypt Password** 以获取人类可读的密码。AWS 会显示默认密码。

15. 重复步骤 2 中的步骤，直到您创建了两个实例：

- 一个位于公共子网中的堡垒主机实例
- 您的私有子网中的一个实例，用作域控制器。

任务 4：创建 DHCP 选项集

1. 在 VPC 控制面板中，选择 **DHCP Options Sets**。
2. 输入以下信息：

- 名称标签：为该集输入一个易记的名称。
- 域名：输入配置域控制器实例时使用的完全限定域名。
- 域名服务器：输入分配给域控制器实例的私有 IP 地址和字符串 **AmazonProvidedDNS**，用逗号分隔。
- NTP 服务器：将此字段留空。
- NetBIOS 名称服务器：输入域控制器实例的私有 IP 地址。
- NetBIOS 节点类型：输入 **2**。

3. 选择 **是，创建。**
4. 将新集与您的 VPC 关联：

a. 在 VPC 控制面板中，选择 **您的 VPC**，然后选择您之前设置的 VPC。

b. 选择 **操作 > 编辑 DHCP 选项集**。

c. 出现提示时，选择您创建的新集，然后选择 **保存**。

任务 5：配置实例

1. 使用 RDP 客户端连接到堡垒主机实例的公共 IP 地址。出现提示时，输入管理员帐户的凭据。
2. 从堡垒主机实例启动远程桌面连接，并连接到您要配置的实例的私有 IP 地址。出现提示时，输入实例的管理员凭据。
3. 对于私有子网中的所有实例，配置 DNS 设置：

a. 选择 **开始 > 控制面板 > 网络和 Internet > 网络和共享中心 > 更改适配器设置**。双击显示的网络连接。

b. 选择 **属性 > Internet 协议版本 4 (TCP/IPv4) > 属性**。

c. 选择 **高级 > DNS**。确保以下设置已启用，然后选择 **确定**：

- 在 DNS 中注册此连接的地址
- 在 DNS 注册中使用此连接的 DNS 后缀

4. 要配置域控制器：

a. 使用服务器管理器，添加具有所有默认功能的 Active Directory 域服务角色。

b. 将实例提升为域控制器。在提升过程中，启用 DNS 并使用创建 DHCP 选项集时指定的域名。出现提示时，重新启动实例。

有关 AWS 权限的信息，请参阅 所需的 AWS 权限 - Amazon EC2 和 所需的 AWS 权限 - Amazon WorkSpaces Core 托管实例。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关创建和管理连接的信息，请参阅：
  - 连接到 AWS EC2
  - 连接到 Amazon WorkSpaces Core 托管实例

更多信息

- 创建和管理连接与资源
- 创建计算机目录

Azure Local 环境

Azure Local（基于 Azure Arc）是一种超融合基础设施 (HCI) 解决方案，可将本地系统连接到 Azure，以实现基于云的服务、监视和管理。

先决条件

- Azure Local 群集：2503 或更高版本
  - 已创建存储路径
  - 已创建并启用了 DHCP 的逻辑网络

- 要部署 Azure Local 群集，请参阅 Microsoft 文档 关于 Azure Local 部署。

注意事项

- 不支持 Windows 10 和 11 多会话工作负载。

主要步骤

在 Azure Local 群集中创建 MCS 目录的关键步骤如下：

1. 创建主机连接。
2. 创建目录。

下一步操作

- 有关创建到 Azure Local 的连接，请参阅 连接到 Azure Local。

更多信息

- 创建和管理连接与资源

XenServer® 虚拟化环境

XenServer 简化了您的运营管理，为密集型工作负载提供高清用户体验。

要设置 XenServer，请参阅准备安装。

下一步

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关在 XenServer 中创建和管理连接的信息，请参阅连接到 XenServer

更多信息

- 创建和管理连接和资源
- 创建计算机目录

Google Cloud 环境

Citrix Virtual Apps and Desktops™ 允许您在 Google Cloud 上预配和管理计算机。

要求

- Citrix Cloud™ 帐户。本文中描述的功能仅在 Citrix Cloud 中可用。

- 一个 Google Cloud 项目。该项目存储与计算机目录关联的所有计算资源。它可以是现有项目，也可以是新项目。
- 在您的 Google Cloud 项目中启用四个 API。有关详细信息，请参阅启用 Google Cloud API。
- Google Cloud 服务帐户。该服务帐户向 Google Cloud 进行身份验证，以启用对项目的访问。有关详细信息，请参阅 配置和更新服务帐户。
- 启用 Google 私有访问。有关详细信息，请参阅启用 Google 私有访问。

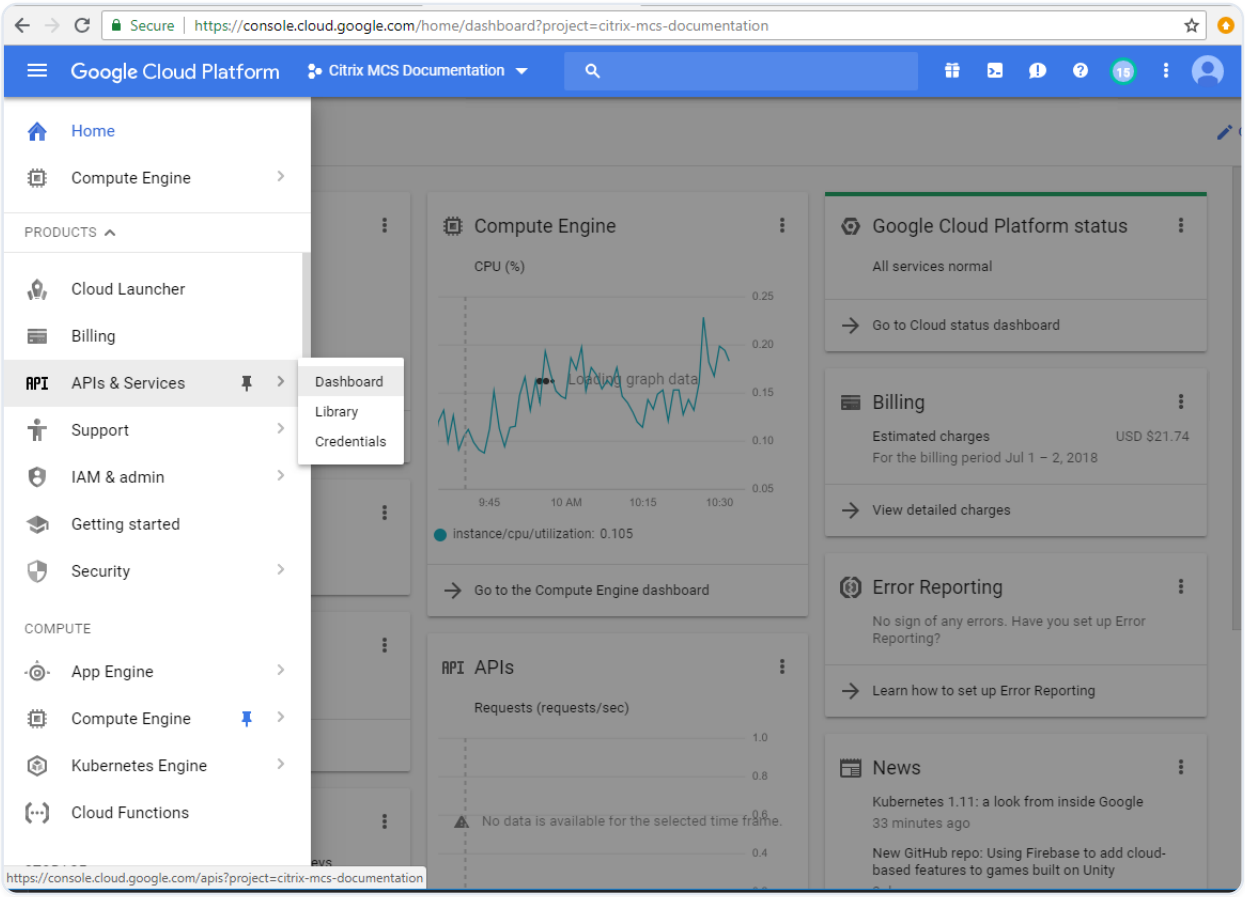
启用 Google Cloud API

要通过 Web Studio 使用 Google Cloud 功能，请在您的 Google Cloud 项目中启用以下 API：

- 计算引擎 API
- 云资源管理器 API
- 身份与访问管理 (IAM) API
- Cloud Build 接口
- Cloud 密钥管理服务 (KMS)

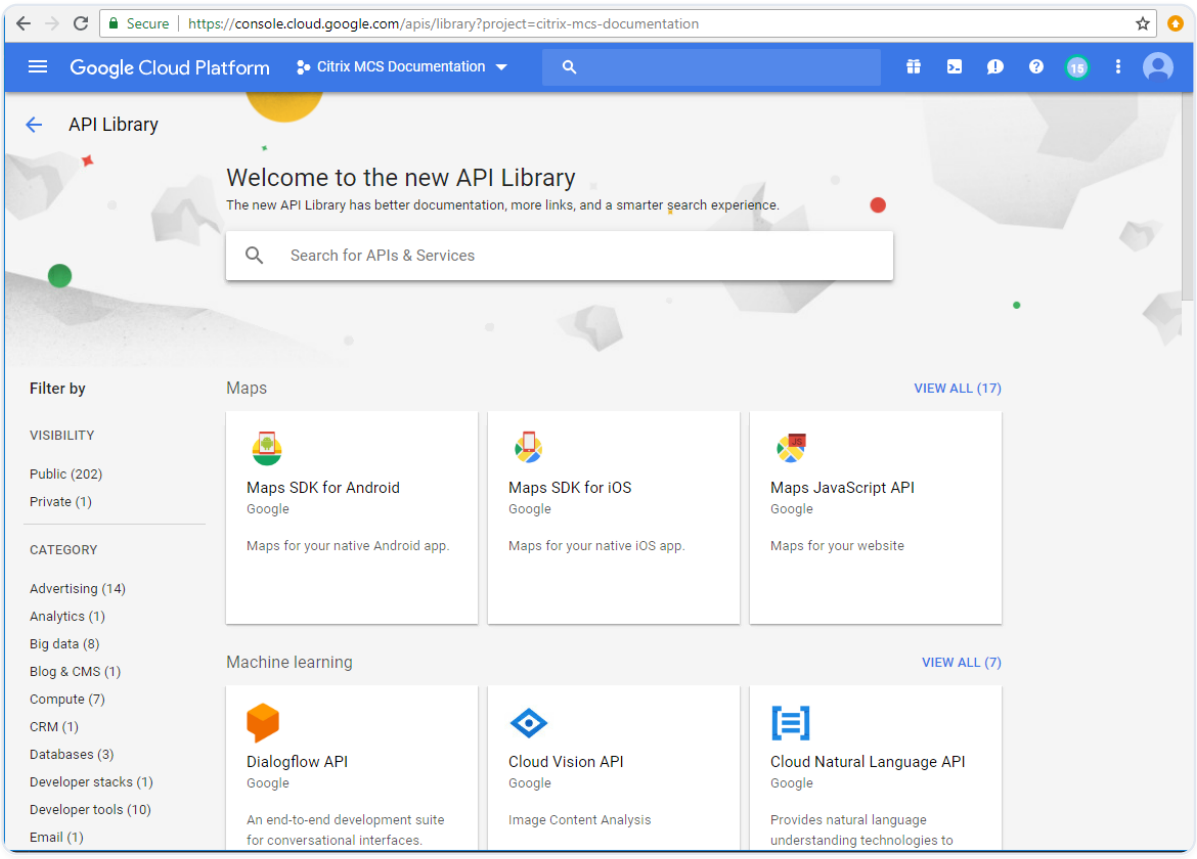
在 Google Cloud 控制台中，完成以下步骤：

1. 在左上角菜单中，选择 **API 和服务 > 控制面板**。



2. 在**控制面板**屏幕上，确保已启用 Compute Engine API。如果 未启用，请按照以下步骤操作：

   a. 导航到**API 和服务 > 库**。



   b. 在搜索框中，键入 *Compute Engine*。

   c. 从搜索结果中，选择**Compute Engine API**。

   d. 在**Compute Engine API**页面上，选择**启用**。

3. 启用云资源管理器 API。

   a. 导航到**API 和服务 > 库**。

   b. 在搜索框中，键入 *Cloud Resource Manager*。

   c. 从搜索结果中，选择**Cloud Resource Manager API**。

   d. 在**Cloud Resource Manager API**页面上，选择**启用**。API 的状态将显示。

4. 同样，启用 **身份与访问管理 (IAM) API** 和 **云构建 API**。

您还可以使用 Google Cloud Shell 启用 API。为此，请执行以下操作：

1. 打开 Google 控制台并加载 Cloud Shell。
2. 在 Cloud Shell 中运行以下四个命令：

   - 启用计算服务：gcloud services enable compute.googleapis.com

- 启用云资源管理器服务：gcloud services enable cloudresourcemanager.googleapis.com
- gcloud 服务 启用 iam.googleapis.com
- gcloud 服务 启用 cloudbuild.googleapis.com

3. 如果 Cloud Shell 提示，请单击**授权**。

配置和更新服务帐号

> **注意：**
>
> GCP 将在 April 29, 2024 之后对 Cloud Build Service 的默认行为和服务帐号的使用引入更改。有关详细信息，请参阅 Cloud Build 服务帐号更改。您在 April 29, 2024 之前启用了 Cloud Build API 的现有 Google 项目不受此更改的影响。但是，如果您希望在 April 29 之后保留现有的 Cloud Build Service 行为，则可以在启用 Cloud Build API 之前创建或应用组织策略以禁用约束实施。因此，以下内容分为两部分：April 29, 2024 之前 和 April 29, 2024 之后。如果您设置了新的组织策略，请按照 April 29, 2024 之前 部分操作。

APRIL 29, 2024 之前

Citrix Cloud 在 Google Cloud 项目中使用三个独立的服务帐户：

- *Citrix Cloud 服务帐号*：此服务帐号使 Citrix Cloud 能够访问 Google 项目、预配和管理计算机。此服务帐号使用 Google Cloud 生成的 密钥 对 Google Cloud 进行身份验证。

  您必须按照此处所述手动创建此服务帐号。有关详细信息，请参阅 创建 Citrix Cloud 服务帐号。

  您可以使用电子邮件地址识别此服务帐号。例如，`<my-service-account>@<project-id>.iam.gserviceaccount.com`。

- *Cloud Build 服务帐号*：启用 启用 Google Cloud API 中提及的所有 API 后，此服务帐号会自动预配。要查看所有自动创建的服务帐号，请在 **Google Cloud** 控制台中导航到 **IAM 和管理 > IAM**，然后选中 **包括 Google 提供的角色授予** 复选框。

  您可以通过以 **项目 ID** 和单词 **cloudbuild** 开头的电子邮件地址识别此服务帐号。例如，`<project-id>@cloudbuild.gserviceaccount.com`

  验证服务帐号是否已获得以下角色。如果必须添加角色，请按照向 Cloud Build 服务帐号添加角色中概述的步骤操作。

  - Cloud Build 服务帐户
  - 计算实例管理员

  - 服务帐号用户

- *Cloud Compute 服务帐号*：一旦 Compute API 激活，Google Cloud 就会将此服务帐号添加到在 Google Cloud 中创建的实例。此帐号具有 IAM 基本编辑者角色以执行操作。但是，如果您删除默认权限以进行更精细的控制，则必须添加一个需要以下权限的 **Storage Admin** 角色：

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

您可以通过以 **Project ID** 和单词 **compute** 开头的电子邮件地址来识别此服务帐号。例如，`<project-id>-compute@developer.gserviceaccount.com`。

创建 Citrix Cloud 服务帐号

要创建 Citrix Cloud 服务帐号，请执行以下步骤：

1. 在 Google Cloud 控制台中，导航到 **IAM & Admin > Service accounts**。
2. 在 **Service accounts** 页面上，选择 **CREATE SERVICE ACCOUNT**。
3. 在 **Create service account** 页面上，输入所需信息，然后选择 **CREATE AND CONTINUE**。
4. 在“**授予此服务帐号项目访问权限**”页面上，单击“**选择角色**”下拉菜单并选择所需的角色。如果要添加更多角色，请单击“**+添加其他角色**”。

   每个帐户（个人或服务）都具有定义项目管理的各种角色。向此服务帐户授予以下角色：

   - 计算管理员
   - Storage 管理员
   - Cloud Build 编辑者
   - 服务帐号用户
   - 云数据存储用户
   - Cloud KMS 加密操作员

   Cloud KMS 加密操作员需要以下权限：

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

> **注意：**
>
> 启用所有 API 以获取创建新服务帐户时可用的完整角色列表。

5. 单击“**继续**”
6. 在“**授予用户对此服务帐户的访问权限**”页面上，添加用户或组以授予他们在此服务帐户中执行操作的权限。
7. 单击“**完成**”。
8. 导航到 IAM 主控制台。
9. 识别已创建的服务帐户。
10. 验证角色是否已成功分配。

注意事项：

创建服务帐户时，请考虑以下事项：

- “**授予此服务帐户对项目的访问权限**”和“**授予用户对此服务帐户的访问权限**”步骤是可选的。如果选择跳过这些可选配置步骤，则新创建的服务帐户不会显示在“**IAM 和管理 > IAM**”页面中。
- 要显示与服务帐户关联的角色，请添加角色而不跳过可选步骤。此过程可确保角色显示在已配置的服务帐户中。

Citrix Cloud 服务帐户密钥
在 Citrix DaaS 中创建连接需要 Citrix Cloud 服务帐户密钥。该密钥包含在凭据文件 (.json) 中。创建密钥后，文件会自动下载并保存到 **Downloads** 文件夹。创建密钥时，请务必将密钥类型设置为 JSON。否则，Web Studio 无法解析它。

要创建服务帐户密钥，请导航到“**IAM 和管理 > 服务帐户**”，然后单击 Citrix Cloud 服务帐户的电子邮件地址。切换到“**密钥**”选项卡，然后选择“**添加密钥 > 创建新密钥**”。请务必选择 **JSON** 作为密钥类型。

> **提示：**

> 使用 Google Cloud 控制台中的“**服务帐户**”页面创建密钥。我们建议您定期更改密钥以确保安全。您可以通过编辑现有的 Google Cloud 连接，向 Citrix Virtual Apps and Desktops™ 应用程序提供新密钥。

向 Citrix Cloud 服务帐号添加角色

要向 Citrix Cloud 服务帐号添加角色，请执行以下操作：

1. 在 Google Cloud 控制台中，导航到 **IAM 和管理 > IAM**。
2. 在“**IAM > 权限**”页面上，找到您创建的服务帐号，该帐号可通过电子邮件地址识别。

   例如，`<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 选择铅笔图标以编辑服务帐号主体的访问权限。
4. 在所选主体选项的“**编辑对“project-id”的访问权限**”页面上，选择“**添加其他角色**”以逐个将所需角色添加到您的服务帐号，然后选择“**保存**”。

向 Cloud Build 服务帐号添加角色

要向 Cloud Build 服务帐号添加角色，请执行以下操作：

1. 在 Google Cloud 控制台中，导航到 **IAM 和管理 > IAM**。
2. 在“**IAM**”页面上，找到 Cloud Build 服务帐号，该帐号可通过以“**项目 ID**”和单词“**cloudbuild**”开头的电子邮件地址识别。

   例如，`<project-id>@cloudbuild.gserviceaccount.com`
3. 选择铅笔图标以编辑 Cloud Build 帐号角色。
4. 对于所选的主体选项，在**“project-id”的编辑访问权限页面**上，选择**添加其他角色**以逐个将所需角色添加到您的 Cloud Build 服务帐号，然后选择**保存**。

> **注意：**
>
> 启用所有 API 以获取完整的角色列表。

APRIL 29, 2024 之后

Citrix Cloud 在 Google Cloud 项目中使用两个独立的服务帐号：

- *Citrix Cloud 服务帐号*：此服务帐号使 Citrix Cloud 能够访问 Google 项目、预配和管理计算机。此服务帐号使用 Google Cloud 生成的 密钥 对 Google Cloud 进行身份验证。

  您必须手动创建此服务帐号。

您可以使用电子邮件地址识别此服务帐号。例如，`<my-service-account>@<project-id>.iam.gserviceaccount.com`。

- *Cloud Compute 服务帐号*：启用启用 Google Cloud API中提及的所有 API 后，此服务帐号将自动预配。要查看所有自动创建的服务帐号，请在 **Google Cloud** 控制台中导航到 **IAM 和管理 > IAM**，然后选中**包括 Google 提供的角色授予**复选框。此帐号具有 IAM 基本编辑者角色以执行操作。但是，如果您删除默认权限以获得更精细的控制，则必须添加需要以下权限的 **Storage Admin** 角色：

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

  您可以通过以**项目 ID** 和单词 **compute** 开头的电子邮件地址识别此服务帐号。例如，`<project-id>-compute@developer.gserviceaccount.com.`.

  验证是否已向服务帐号授予以下角色。

  - Cloud Build 服务帐户
  - 计算实例管理员
  - 服务帐号用户

创建 Citrix Cloud 服务帐号

要创建 Citrix Cloud 服务帐号，请执行以下步骤：

1. 在 Google Cloud 控制台中，导航到 **IAM & Admin > Service accounts**。
2. 在 **Service accounts** 页面上，选择 **CREATE SERVICE ACCOUNT**。
3. 在 **Create service account** 页面上，输入所需信息，然后选择 **CREATE AND CONTINUE**。
4. 在“**授予此服务帐号项目访问权限**”页面上，单击“**选择角色**”下拉菜单并选择所需的角色。如果要添加更多角色，请单击“**+添加其他角色**”。

   每个帐户（个人或服务）都具有定义项目管理的各种角色。向此服务帐户授予以下角色：

   - 计算管理员
   - Storage 管理员
   - Cloud Build 编辑者
   - 服务帐号用户

- 云数据存储用户
- Cloud KMS 加密操作员

Cloud KMS 加密操作员需要以下权限：

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **注意：**
>
> 启用所有 API 以获取创建新服务帐户时可用的完整角色列表。

5. 单击“**继续**”
6. 在“**授予用户对此服务帐户的访问权限**”页面上，添加用户或组以授予他们在此服务帐户中执行操作的权限。
7. 单击“**完成**”。
8. 导航到 IAM 主控制台。
9. 识别已创建的服务帐户。
10. 验证角色是否已成功分配。

注意事项：

创建服务帐户时，请考虑以下事项：

- “**授予此服务帐户对项目的访问权限**”和“**授予用户对此服务帐户的访问权限**”步骤是可选的。如果选择跳过这些可选配置步骤，则新创建的服务帐户不会显示在“**IAM 和管理 > IAM**”页面中。
- 要显示与服务帐户关联的角色，请添加角色而不跳过可选步骤。此过程可确保角色显示在已配置的服务帐户中。

Citrix Cloud 服务帐户密钥
在 Citrix DaaS 中创建连接需要 Citrix Cloud 服务帐户密钥。该密钥包含在凭据文件 (.json) 中。创建密钥后，该文件会自动下载并保存到 **Downloads** 文件夹。创建密钥时，请务必将密钥类型设置为 JSON。否则，Web Studio 无法对其进行解析。

要创建服务帐户密钥，请导航到“**IAM 和管理 > 服务帐户**”，然后单击 Citrix Cloud 服务帐户的电子邮件地址。切换到“**密钥**”选项卡，然后选择“**添加密钥 > 创建新密钥**”。请务必选择 **JSON** 作为密钥类型。

> **提示：**
>
> 在 Google Cloud 控制台的“**服务帐号**”页面中创建密钥。我们建议您定期更改密钥以确保安全。您可以通过编辑现有 Google Cloud 连接，向 Citrix Virtual Apps and Desktops 应用程序提供新密钥。

向 Citrix Cloud 服务帐号添加角色

要向 Citrix Cloud 服务帐号添加角色，请执行以下操作：

1. 在 Google Cloud 控制台中，导航到 **IAM 和管理 > IAM**。
2. 在“**IAM > 权限**”页面上，找到您创建的服务帐号，该帐号可通过电子邮件地址识别。

   例如，`<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 选择铅笔图标以编辑服务帐号主体的访问权限。
4. 在所选主体选项的“**编辑对“project-id”的访问权限**”页面上，选择“**添加其他角色**”以逐个将所需角色添加到您的服务帐号，然后选择“**保存**”。

向 Cloud Compute 服务帐号添加角色

要向 Cloud Compute 服务帐号添加角色，请执行以下操作：

1. 在 Google Cloud 控制台中，导航到 **IAM 和管理 > IAM**。
2. 在 **IAM** 页面上，找到 Cloud Compute 服务帐号，该帐号可通过以 **项目 ID** 和单词 **compute** 开头的电子邮件地址进行识别。

   例如，`<project-id>-compute@developer.gserviceaccount.com`
3. 选择铅笔图标以编辑 Cloud Build 帐号角色。
4. 对于所选的主体选项，在**“project-id”的编辑访问权限页面**上，选择**添加其他角色**以逐个将所需角色添加到您的 Cloud Build 服务帐号，然后选择**保存**。

> **注意：**
>
> 启用所有 API 以获取完整的角色列表。

存储权限和存储桶管理

Citrix Virtual Apps and Desktops 改进了 Google Cloud 服务 的云构建失败报告流程。此服务在 Google Cloud 上运行构建。Citrix Virtual Apps and Desktops 创建一个名为 `citrix-mcs-cloud-build-logs-{region}-{5 random characters}` 的存储桶，Google Cloud 服务在此存储桶中捕获构建日志信息。此存储桶上设置了一个选项，可在 30 天后删除内容。此过程要求用于连接的服务帐户具有设置为 `storage.buckets.update` 的 Google Cloud 权限。如果服务帐户没有此权限，Citrix Virtual Apps and Desktops 将忽略错误并继续执行目录创建过程。如果没有此权限，构建日志的大小会增加，并且需要手动清理。

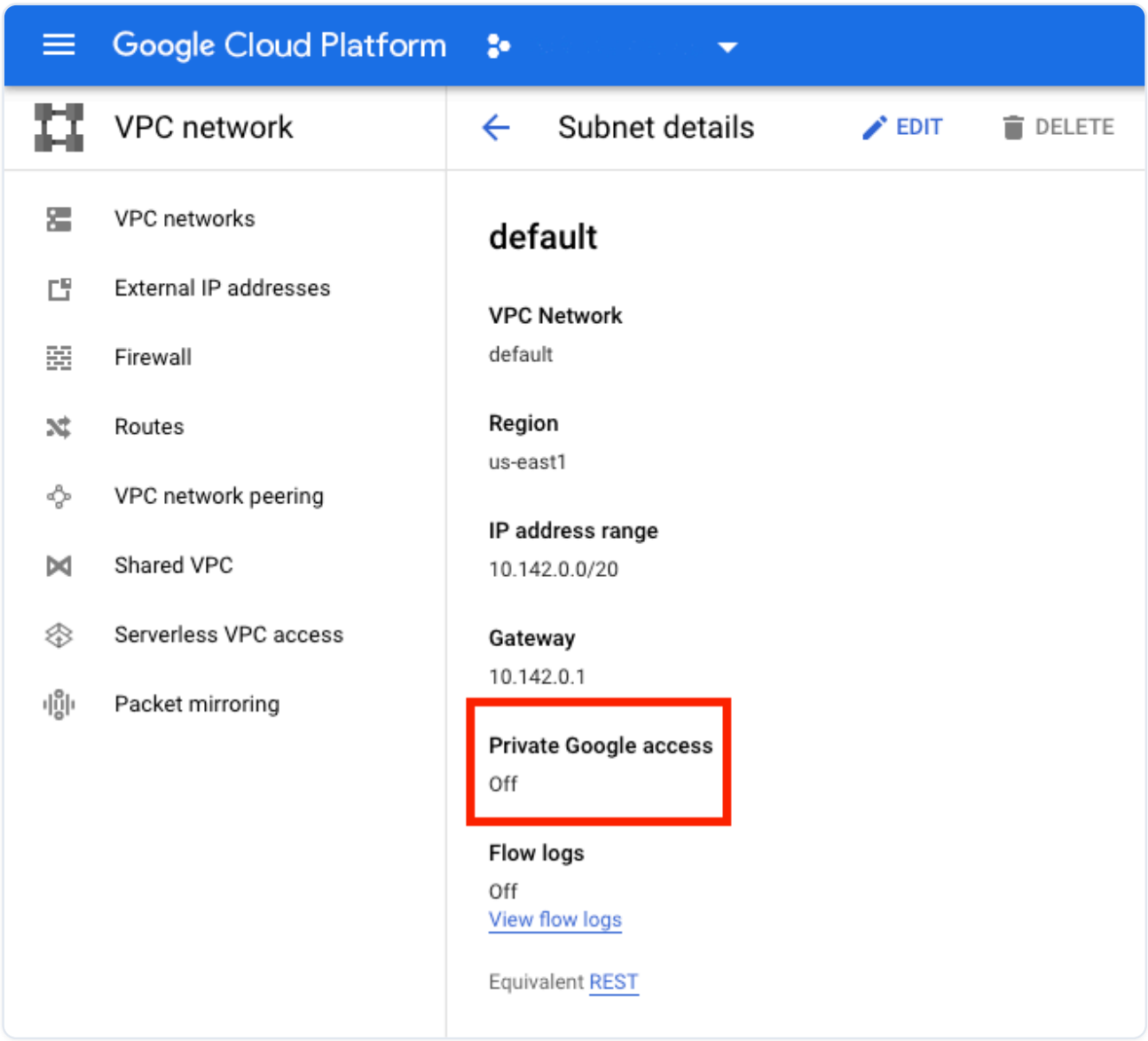
启用私有 Google 访问

当虚拟机缺少分配给其网络接口的外部 IP 地址时，数据包只会发送到其他内部 IP 地址目标。启用私有访问后，虚拟机将连接到 Google API 和相关服务使用的外部 IP 地址集。

> **注意：**
>
> 无论是否启用私有 Google 访问，所有具有和不具有公共 IP 地址的虚拟机都必须能够访问 Google 公共 API，尤其是在环境中安装了第三方网络设备的情况下。

为确保子网中的 VM 可以在没有公共 IP 地址的情况下访问 Google API 以进行 MCS 预配：

1. 在 Google Cloud 中，访问 **VPC 网络配置**。
2. 在“子网详细信息”屏幕中，启用 **Private Google access**。



有关详细信息，请参阅配置 Private Google Access。

> **重要提示：**
>
> 如果您的网络配置为阻止 VM 访问 Internet，请确保您的组织承担为 VM 连接的子网启用 Private Google access 所带来的风险。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关在 Google Cloud 环境中创建和管理连接的信息，请参阅 连接到 Google Cloud 环境

更多信息

- 创建和管理连接与资源
- 创建计算机目录

HPE Moonshot 虚拟化环境

Citrix Virtual Apps and Desktops™ 通过现有的 Citrix 管理的 HPE Moonshot 插件管理您的 HPE Moonshot 工作负载。在升级或安装 Citrix Virtual Apps and Desktops 2503 版本时，Citrix 管理的 HPE Moonshot 插件会自动安装。借助此插件，您可以创建与 HPE Moonshot 机箱的连接、创建目录以及对目录中的计算机进行电源管理。

主要步骤

1. 设置您的 HPE 环境。
2. 创建与 HPE Moonshot 机箱的连接。
3. 创建计算机目录。

> **注意：**
>
> 在创建目录之前，请确保拥有一台或多台 HPE Moonshot 刀片节点，并在这些节点上安装 VDA。您可以将 HPE Moonshot 机箱视为管理程序，将刀片节点视为虚拟机。

4. 创建交付组。
5. 将其余未受管的 HPE Moonshot 节点迁移到受管目录或交付组。

> **注意：**
>
> 使用 Web Studio 而不是基于 MMC 的 Studio。

故障排除

如果同时安装了 Citrix 管理和 HPE 管理的 HPE Moonshot 插件，并且

- 如果要使用 **HPE 管理的 Moonshot 插件**，则必须卸载 Citrix 管理的 HPE Moonshot 插件并更新 `RegisterPlugin` 缓存。为此：

  a. 以管理员身份打开 PowerShell 并运行以下命令以卸载 Citrix 管理的 HPE Moonshot 插件：

```
$CtxMnsht = Get-WmiObject -Class Win32_Product | Where-
Object{$_.Name -Contains "Citrix HPE Moonshot Plugin"}

$CtxMnsht.Uninstall()
```

b. 运行以下命令以注册 HPE 管理的 Moonshot 插件：

```
cd "C:\Program Files\Common Files\Citrix\HCLPlugins\"

.\RegisterPlugins.exe -PluginsRoot "C:\Program Files\Common
Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0\"
```

c. 插件注册成功后，从**任务管理器**重新启动以下服务：

   a. CitrixBrokerService

   b. CitrixHostService

   c. CitrixMachineCreationService

d. 运行 `Get-HypHypervisorPlugins` 以检查插件是否安装在 Delivery Controller 上。输出中的 `DisplayName` 字段必须显示为 HPE Moonshot Machine Manager。

- 如果您想再次安装 Citrix 管理的 HPE Moonshot 插件，请执行以下操作：

a. 安装 `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin.msi`。`E:\` 是 ISO。

b. 以管理员身份打开 PowerShell 并运行以下命令以注册 Citrix 管理的 HPE Moonshot 插件：

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .
\RegisterPlugins.exe -pluginsroot .\CitrixMachineCreation\v1.0.0.0\
```

c. 插件注册成功后，从任务管理器重新启动以下服务：

   a. CitrixBrokerService

   b. CitrixHostService

   c. CitrixMachineCreationService

1. 运行 `Get-HypHypervisorPlugins` 以检查插件是否安装在 Delivery Controller 上。输出中的 DisplayName 字段必须显示为 HPE Moonshot。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关在 HPE Moonshot 中创建和管理连接的信息，请参阅 连接到 HPE Moonshot

更多信息

- 创建和管理连接与资源
- 创建计算机目录

Microsoft Azure 资源管理器 云环境

在 Citrix Virtual Apps and Desktops™ 部署中使用 Microsoft Azure Resource Manager 预配虚拟机时，请熟悉以下内容：

- 微软 Entra ID: `<https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/>`
- 同意框架: `<https://docs.microsoft.com/zh-cn/azure/active-directory/manage-apps/plan-an-application-integration>`
- 服务主体: `<https://docs.microsoft.com/zh-cn/azure/active-directory/develop/app-objects-and-service-principals/>`

要设置 Microsoft Azure Resource Manager，请参阅准备安装。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关在 Azure 环境中创建和管理连接的信息，请参阅连接到 Microsoft Azure

更多信息

- 创建和管理连接与资源
- 创建计算机目录
- CTX219211：设置微软 Microsoft Entra 帐户
- CTX219243: 授予 XenApp 和 XenDesktop 访问您的 Azure 订阅的权限
- CTX219271: 使用站点到站点 VPN 部署混合云

微软系统中心配置管理器环境

使用 Microsoft System Center Configuration Manager (Configuration Manager) 管理应用程序和桌面访问的站点可以通过以下选项将该用途扩展到 Citrix Virtual Apps and Desktops™：

- 使用 SCCM 安装 VDA。
- **Configuration Manager Wake Proxy 功能：** Remote PC Access 的 Wake on LAN 功能受 Configuration Manager 支持。有关详细信息，请参阅局域网唤醒 - SCCM 集成。
- **Citrix Virtual Apps and Desktops 属性：** 属性 使您能够识别 Citrix Virtual Desktops™，以便通过 Configuration Manager 进行管理。（在某些版本中，Configuration Manager 使用 Citrix Virtual Apps and Desktops 的旧名称：XenApp and XenDesktop。）

属性

Microsoft System Center Configuration Manager 可使用属性来管理虚拟桌面。

Configuration Manager 中显示的布尔属性显示为 `1` 或 `0`，而不是 true 或 false。

这些属性适用于 `Citrix_virtualDesktopInfo` 类中的 `Root\Citrix\DesktopInformation` 命名空间。属性名称来自 Windows Management Instrumentation (WMI) 提供程序。

属性	描述
`AssignmentType`	设置 IsAssigned 的值。有效值为：`ClientIP`、`ClientName`、`None` 和 `User`（将 `IsAssigned` 设置为 `True`）
`BrokerSiteName`	返回与 `HostIdentifier` 相同的值
`DesktopCatalogName`	与桌面关联的计算机目录。
`DesktopGroupName`	与桌面关联的交付组。
`HostIdentifier`	返回与 `BrokerSiteName` 相同的值。
`IsAssigned`	`True` 用于将桌面分配给用户，设置为 `False` 以用于随机桌面
`IsMasterImage`	允许对环境做出决策。例如，在映像上而不是在预配的计算机上安装应用程序。有效值为：`True` 在用作映像的 VM 上。此值在安装期间根据选择进行设置，或者在从该映像预配的 VM 上清除。

属性	描述
`IsVirtualMachine`	`True` 用于虚拟机，`false` 用于物理机。
`OSChangesPersist`	如果桌面操作系统映像在每次重新启动时都重置为干净状态，则为 `False`；否则为 `true`。
`PersistentDataLocation`	Configuration Manager 存储持久数据的位置。用户无法访问此位置。
`BrokerSiteName`, `DesktopCatalogName`, `DesktopGroupName`, `HostIdentifier`	在桌面向控制器注册时确定。对于尚未完全注册的桌面，它们为空。

要收集属性，请在 Configuration Manager 中运行硬件清单。要查看属性，请使用 Configuration Manager 资源管理器。在这些情况下，名称包含空格或与属性名称略有不同。例如，`BrokerSiteName` 显示为 `Broker Site Name`。

- 配置 Configuration Manager 以从 Citrix VDA 收集 Citrix WMI 属性
- 使用 Citrix WMI 属性创建基于查询的设备集合
- 基于 Citrix WMI 属性创建全局条件
- 使用全局条件定义应用程序部署类型要求

您还可以在 `Root\ccm_vdi` 命名空间中的 Microsoft 类 `CCM_DesktopMachine` 中使用 Microsoft 属性。有关详细信息，请参阅 Microsoft 文档。

Microsoft System Center 虚拟机管理器 虚拟化环境

如果您使用 Hyper-V 和 Microsoft System Center Virtual Machine Manager (VMM) 来提供虚拟机，请遵循此指导。

此版本支持 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/system-requirements.html) 中列出的 VMM 版本。

> **注意：**

> 不支持混合 Hyper-V 群集（包含运行不同 Hyper-V 版本的服务器）。

> 您可以使用 Citrix Provisioning（以前称为 Provisioning Services）和 Machine Creation Services™ 来预配：

- 第 1 代支持的桌面或服务器操作系统 VM。
- 第 2 代支持的桌面或服务器操作系统 VM，包括安全启动支持。

安装和配置管理程序

> **重要提示：**
>
> 所有 Delivery Controller 必须与 VMM 服务器位于同一林中。

1. 在服务器上安装 Microsoft Hyper-V 服务器和 VMM。
2. 在所有 Controller 上安装 System Center Virtual Machine Manager 控制台。控制台版本必须与管理服务器版本匹配。尽管较早的控制台可以连接到管理服务器，但如果版本不同，则预配 VDA 将失败。
3. 验证以下帐户信息：

   您在 Studio 中指定主机时使用的帐户是相关 Hyper-V 计算机的 VMM 管理员或 VMM 委派管理员。如果此帐户在 VMM 中仅具有委派管理员角色，则在主机创建过程中，存储数据不会在 Studio 中列出。

   用于 Studio 集成的用户帐户还必须是每个 Hyper-V 服务器上管理员本地安全组的成员。此配置支持 VM 生命周期管理，例如 VM 创建、更新和删除。

   不支持在运行 Hyper-V 的服务器上安装 Controller。

在大型部署中，如果单个 SCVMM 管理不同数据中心中的多个群集，则可以限制委派管理员的主机组范围。

要限制主机组范围，请在 Microsoft System Center Virtual Machine Manager (VMM) 控制台中使用委派管理员角色：

1. 在“**创建用户角色向导**”中，选择“Fabric Administrator (Delegated Administrator)”作为用户角色。
2. 在“**成员**”中，添加您要在 Active Directory 中用作委派管理员的用户帐户。
3. 在 **范围** 中，选择您希望委派管理员访问的主机组。
4. 使用委派管理员用户凭据创建新的 **运行身份帐户**。稍后使用这些凭据创建管理程序连接。请勿使用主管理员角色帐户。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关在 SCVMM 中创建和管理连接的信息，请参阅连接到 Microsoft System Center Virtual Machine Manager

更多信息

- 创建和管理连接与资源
- 创建计算机目录

Nutanix 虚拟化环境

通过 Nutanix Prism Central 使用 Nutanix AHV Prism Central 主机连接将 Citrix Virtual Apps and Desktops 连接到 Nutanix AHV 集群。此主机连接：

- 支持包含电源管理和 MCS 预配的 VDA 的计算机目录。
- 使用模板版本在 AHV 群集之间启用 MCS 主映像共享。
- 简化主机连接上的证书信任。
- 无需在 Cloud Connector 上安装 Nutanix 插件。

请参阅 AHV 上的 Nutanix Prism Central。

您还可以使用 Nutanix Prism Element on AHV，将 Nutanix Acropolis 作为主机连接，在 Citrix Virtual Apps and Desktops 部署中提供 VM。但是，此设置过程需要在 Citrix Virtual Apps and Desktops 环境中安装并注册 Nutanix 插件。请参阅 Nutanix Prism Element on AHV。

有关 Nutanix Acropolis MCS 插件安装指南的更多信息，请参阅 Nutanix 支持门户。

适用于 AHV 的 Nutanix Prism Central

Citrix 开发并维护了一个插件，用于将 Citrix Virtual Apps and Desktops 与 Nutanix Prism Central on AHV 集成。此插件已与 Citrix Delivery Controllers 集成，无需单独安装插件。

Nutanix AHV Prism Central 插件已预安装在 Citrix 管理的 Delivery Controllers 上，无需在 Delivery Controllers 上单独安装。有关 Citrix 管理的组件和服务的信息，请参阅 技术概述。

先决条件

Nutanix AHV Prism Central 需要以下各项：

- Prism Central 版本 pc.2025.2 或更高版本。有关详细支持的 Prism Central 版本，请参阅 Citrix Virtual Apps and Desktops (MCS) 和 Citrix Provisioning (PVS) 支持的虚拟机管理程序。
- Nutanix AHV 集群的 AOS 7.3 或更高版本。
- Nutanix AHV 集群必须注册到 Prism Central。
- Citrix 管理员帐户必须具有足够的权限才能创建主机连接、计算机目录和交付组。有关详细信息，请参阅配置委派管理。
- Citrix Cloud™ 通过 Cloud Connector 与 Nutanix Prism Central 通信。因此，必须可以从 Cloud Connector 访问 Nutanix Prism Central 实例。

功能限制

由于 Nutanix Prism 和 API 的限制，针对 Windows VM 的电源操作（例如客户机重新启动或客户机关机）可能会失败。要解决此问题，我们建议按照文档 从 Prism 或 API 启动的电源操作可能对 Windows VM 失败 中的 Nutanix 说明在 VDA 上应用设置。

关键步骤

1. 设置您的 Nutanix 虚拟化环境。有关信息，请参阅 准备安装 或 激活未使用的域。
2. 创建到 Nutanix AHV Prism Central 的连接
3. 使用 Nutanix 计算机模板版本创建计算机目录。

适用于 AHV 的 Nutanix Prism Element

Nutanix Prism Element on AHV 要求在所有 Delivery Controllers 上安装 Nutanix 插件，Citrix Virtual Apps and Desktops 必须在这些 Delivery Controllers 上创建到具有 Nutanix 管理程序的资源位置的主机连接。

关键步骤

1. 安装并注册 Nutanix 插件。
2. 设置您的 Nutanix 虚拟化环境。有关信息，请参阅添加资源类型 或 激活未使用的域。
3. 创建连接。
4. 创建计算机目录。

安装并注册 NUTANIX 插件

在所有 Cloud Connector 上完成安装和注册 Nutanix 插件的步骤。有关安装 Nutanix 插件的信息，请参阅 Nutanix 文档站点。

后续步骤

- 安装核心组件

- 安装 VDA
- 创建站点
- 有关在 Nutanix 环境中创建和管理连接的信息，请参阅 连接到 Nutanix

更多信息

- (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections.html)
- (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-create.html)

Nutanix 云和合作伙伴解决方案

努坦尼克斯 AHV 棱镜中心

Citrix Virtual Apps and Desktops 支持以下云管理程序中的 Nutanix Cloud Clusters (NC2)，用于 Citrix 管理的 Nutanix AHV Prism Central 插件。

- 亚马逊云服务 (AWS)
- 微软 Azure

NUTANIX 云集群

Citrix Virtual Apps and Desktops 支持 AWS 和 Azure 上的 Nutanix 云集群。Nutanix 集群简化了应用程序在私有云或多个公有云上的运行方式。

有关设置 NC2 的更多信息，请参阅：

- AWS 上的 Nutanix 云集群部署和用户指南
- Azure 上的 Nutanix 云集群部署和用户指南。

要求

您需要以下帐户才能使用 NC2：

- Nutanix 帐户
- 对于 AWS：具有以下权限的 AWS 帐户。
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess
- 对于 Azure：
  - 有效的“Azure 上的 NC2”许可证

- 包含以下角色之一的 Azure 帐户：
  - 全局管理员
  - 云应用程序管理员
  - 应用程序管理员
  - 所有 权限

AZURE 上的 NC2 权限

```
Microsoft.Compute/register/action

Microsoft.Compute/availabilitySets/write

Microsoft.Compute/availabilitySets/delete

Microsoft.Compute/disks/read

Microsoft.Compute/disks/write

Microsoft.Compute/disks/delete

Microsoft.Compute/locations/usages/read

Microsoft.Compute/availabilitySets/read

Microsoft.Compute/virtualMachines/*

Microsoft.Compute/snapshots/*

Microsoft.Compute/images/*

Microsoft.Network/register/action

Microsoft.Network/natGateways/*

Microsoft.Network/networkInterfaces/*

Microsoft.Network/networkSecurityGroups/*

Microsoft.Network/publicIPAddresses/*

Microsoft.Network/virtualNetworks/*
```

```
Microsoft.Network/locations/usages/read

Microsoft.Storage/register/action

Microsoft.Storage/checknameavailability/read Microsoft.Storage/locations/
checknameavailability/read Microsoft.Storage/locations/usages/read

Microsoft.Storage/storageAccounts/write

Microsoft.Storage/storageAccounts/read

Microsoft.Storage/storageAccounts/delete Microsoft.Storage/
storageAccounts/blobServices/containers/clearLegalHold/action
Microsoft.Storage/storageAccounts/blobServices/containers/delete
Microsoft.Storage/storageAccounts/blobServices/containers/lease/action

Microsoft.Storage/storageAccounts/blobServices/containers/ read
Microsoft.Storage/storageAccounts/blobServices/containers/ write
Microsoft.Storage/storageAccounts/blobServices/read Microsoft.Storage/
storageAccounts/blobServices/write Microsoft.Storage/storageAccounts/
listAccountSas/action Microsoft.Storage/storageAccounts/listkeys/action
Microsoft.Storage/storageAccounts/listServiceSas/action Microsoft.Storage/
storageAccounts/regeneratekey/action Microsoft.Storage/storageAccounts/
revokeUserDelegationKeys/action Microsoft.ResourceHealth/
AvailabilityStatuses/read Microsoft.ResourceHealth/events/read

Microsoft.ResourceHealth/AvailabilityStatuses/current/read

Microsoft.ManagedIdentity/userAssignedIdentities/* Microsoft.Resources/
subscriptions/locations/read Microsoft.Resources/subscriptions/
resourceGroups/read Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourcegroups/deployments/read

Microsoft.Resources/subscriptions/resourcegroups/deployments/write
Microsoft.Resources/subscriptions/resourcegroups/resources/read
Microsoft.Resources/subscriptions/tagNames/read Microsoft.Resources/
subscriptions/tagNames/write Microsoft.Resources/subscriptions/tagNames/
delete Microsoft.Resources/subscriptions/tagNames/tagValues/write
Microsoft.Resources/subscriptions/tagNames/tagValues/read
Microsoft.Resources/subscriptions/tagNames/tagValues/delete
Microsoft.Resources/tags/read
```

```
Microsoft.Resources/tags/write

Microsoft.Resources/tags/delete

Microsoft.Resources/providers/read

Microsoft.Compute/sshPublicKeys/read

Microsoft.Compute/sshPublicKeys/write

Microsoft.Compute/sshPublicKeys/delete Microsoft.Compute/sshPublicKeys/
generateKeyPair/action Microsoft.Nutanix/Interfaces/read

Microsoft.Nutanix/Interfaces/write

Microsoft.Nutanix/Interfaces/delete

Microsoft.Nutanix/Nodes/read

Microsoft.Nutanix/Nodes/write

Microsoft.Nutanix/Nodes/delete

Microsoft.Nutanix/register/action

Microsoft.Network/virtualHubs/*

Microsoft.Network/routeTables/read

Microsoft.Network/routeTables/write

Microsoft.Network/routeTables/delete

Microsoft.Network/routeTables/join/action

Microsoft.Network/routeTables/routes/read Microsoft.Network/routeTables/
routes/write Microsoft.Network/routeTables/routes/delete
Microsoft.CostManagement/query/read

Microsoft.CostManagement/views/read Microsoft.CostManagement/
externalSubscriptions/query/read Microsoft.CostManagement/
externalSubscriptions/dimensions/read Microsoft.CostManagement/
externalSubscriptions/read Microsoft.CostManagement/
```

```
externalBillingAccounts/forecast/read

Microsoft.CostManagement/externalBillingAccounts/read

Microsoft.CostManagement/externalBillingAccounts/query/read
Microsoft.CostManagement/externalBillingAccounts/ externalSubscriptions/
read Microsoft.CostManagement/externalSubscriptions/forecast/read
Microsoft.CostManagement/operations/read Microsoft.CostManagement/
forecast/read

Microsoft.Network/virtualWans/write

Microsoft.Network/virtualWans/read

Microsoft.Network/virtualWans/delete Microsoft.Network/virtualWans/
virtualHubs/read Microsoft.Network/virtualWans/join/action
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ read
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ write
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ delete
Microsoft.Network/privateEndpoints/pushPropertiesToResource/ action
Microsoft.Network/privateEndpoints/read

Microsoft.Network/privateEndpoints/write Microsoft.Network/
privateEndpoints/delete Microsoft.Network/privateDnsZones/read
Microsoft.Network/privateDnsZones/delete Microsoft.Network/
privateDnsZones/join/action Microsoft.Network/privateDnsZones/write
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/ write

Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/delete

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
deleteBlobVersion/action

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
action Microsoft.Storage/storageAccounts/blobServices/containers/ blobs/
read Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/
read

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/write
Microsoft.Storage/storageAccounts/blobServices/containers/ blobs/write
```

```
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
action Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
modifyPermissions/action
```

创建 NUTANIX 集群

1. 登录您的 Nutanix 帐户。
2. 导航到 Nutanix 集群选项，然后单击 **启动**。**Nutanix 控制台** 将打开。有关详细信息：
   - 在 AWS 上开始使用 Nutanix 集群(https://next.nutanix.com/nutanix-cloud-clusters-nc2-149/get-started-with-nutanix-cluster-on-aws-39424)
   - Microsoft Azure 上的 Nutanix 云集群
3. 选择创建新 VPC 的选项。

集群创建完成后，检索 Nutanix Prism 的地址。
故障排除
集群创建过程可能会因以下错误而失败：

- **集群未能在给定时间内创建。正在删除集群**
- **主机 Nutanix 集群 - 节点 XXXXXXXXXXX: 实例 i-xxxxxxxxxxxxx: 禁用网络接口源/目标检查错误**。
- **主机 Nutanix 集群 - 节点 XXXXXXXXXXX: 无法获取实例 i-xxxxxxxxxxxxxx 网络接口信息**

如果集群创建失败，请尝试在其他区域重新创建一个。在重试之前，请务必删除 Nutanix CloudFormation Stack (CFS)。

注意：

除了其他资源，Nutanix CFS 还会创建：

- 一个名为 Nutanix Cluster xxxxxxxxxxxx 10.0.0.0/16 的 VPC
- 两个子网 10.0.128.0/24 和 10.0.129.0/24
- 一个 Internet 网关
- 一个 NAT 网关

检索 PRISM 服务器地址

1. 将 NC2 群集注册到 Prism Central 服务器。请参阅 将群集注册到 Prism Central。
2. 使用 Prism Central 服务器的主机名或 IP 地址作为地址。

适用于 Nutanix Prism Element 的 NC2

Citrix Virtual Apps and Desktops 支持在以下云管理程序中使用 Nutanix Cloud Clusters (NC2)，以用于 Nutanix Prism Element 插件。

- 亚马逊云服务 (AWS)

AWS 上的 NUTANIX 云集群

有关 AWS 上的 Nutanix 云群集的更多信息，请参阅 AWS 上的 Nutanix 云群集部署和用户指南。

> **提示：**
>
> 此支持提供与 Nutanix 本地群集相同的功能。仅支持单个群集，即 *Prism Element*。有关详细信息，请参阅 此处。
>
> 要在 AWS 上使用 NC2，您需要以下帐户：

- 一个 Nutanix 帐户
- 具有以下权限的 AWS 帐户：
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

有关创建 Nutanix 群集以及群集创建失败时的故障排除，请参阅 创建 Nutanix 群集 和 故障排除。

集群创建完成后，检索 **Nutanix Prism** 的地址：

检索 PRISM 服务器地址

1. 转到 **Nutanix 控制台**。
2. 在控制台的右上角，将鼠标悬停在链接 **Launch Prism Element** 上并复制 URL。

下一步操作

- 安装核心组件
- 安装 VDA

- 创建站点
- 有关创建和管理 Nutanix 云和合作伙伴解决方案连接的信息，请参阅 连接到 Nutanix 云和合作伙伴解决方案

更多信息

- 创建和管理连接与资源
- 创建计算机目录

Oracle C3 虚拟化环境 (预览版)

Citrix Virtual Apps and Desktops 通过 Citrix 管理的 Oracle C3 插件在 Citrix Virtual Apps and Desktops 控制平面中管理您的 Oracle Compute Cloud@Customer (Oracle C3) 工作负载。借助此插件，您可以创建到 Oracle C3 的连接、创建目录，并对目录中的计算机进行电源管理。

> **注意：**
>
> - 适用于 Citrix Virtual Apps and Desktops 2607 LTSR 的 Oracle C3 仅适用于拥有混合权利或通用许可证的客户。
> - 独立的 Oracle C3 环境目前不支持。

先决条件

开始之前：

- 确保您的环境可以使用 Oracle C3 REST API。Oracle C3 的 `<system_name>.<domain name>` 是 API 连接所必需的。请参阅 使用 API 管理 Compute Cloud@Customer 资源。
- 准备用于 Oracle C3 身份验证的 IAM 配置 `.ini` 文件和私钥。确保区域设置为 `<system_name>.<domain_name>`。
- 如果 Oracle C3 受私有 CA 证书保护，请获取证书指纹，以便在连接设置期间进行信任验证。

主要步骤

1. 设置您的 Oracle C3 环境。
2. 创建到 Oracle C3 端点的连接。
3. 创建计算机目录。

> **注意：**

> 在创建目录之前，请确保一台或多台 Oracle C3 计算机可用，并且这些计算机上已安装 VDA。

4. 创建交付组。
5. 将所有剩余的非托管 Oracle C3 计算机迁移到托管目录或交付组中。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关创建和管理连接的信息，请参阅 连接到 Oracle C3

更多信息

- 创建和管理连接与资源
- 创建计算机目录

Red Hat OpenShift 虚拟化环境

Citrix® 通过 Citrix 管理的 OpenShift 插件管理您的 Red Hat OpenShift 工作负载。借助此插件，您可以为 OpenShift 群集创建托管连接和托管单元、创建目录以及对目录中的计算机进行电源管理。

支持以下配置：

- **网络选项：**
  - Linux 网桥和 OVS 网桥：可用于群集网络。
- **存储选项：**
  - 本地存储：支持用于节点上的持久性存储。
  - Red Hat OpenShift Data Foundation (ODF) 块存储：支持集群范围的分布式块存储。请参阅“配置 ODF 块存储”。

> **配置 ODF 块存储**

> Citrix 支持将 ODF 块存储 `(ocs-storagecluster-ceph-rbd)` 用于计算机目录。OpenShift 插件通过容器化数据导入器 (CDI) 预配 VM 磁盘，CDI 会为每个存储类发布一个 StorageProfile。在创建托管单元之前，请配置以下内容：

- 安装 OpenShift Virtualization (CNV)，包括 CDI。确认存在与您的 ODF 块存储类同名的 StorageProfile。
- 在该 StorageProfile 中，确认已设置 `accessModes` 和 `volumeMode`。
- 确认已设置 `dataImportCronSourceFormat`。如果设置为 `snapshot`，还要确认已设置 `snapshotClass` 并且快照类使用与存储类相同的 CSI 驱动程序 — 对于 ODF 块存储，为 `openshift-storage.rbd.csi.ceph.com`。

- **NetApp 存储：** 支持企业级外部存储集成。

主要步骤

- 设置您的 Red Hat OpenShift 环境。
- 创建与 OpenShift 群集的连接和资源。
- 创建计算机目录。
- 创建交付组。

设置您的 Red Hat OpenShift 环境

1. *创建 OpenShift 群集并获取群集 API 地址*：在 OpenShift 控制台中，设置群集后，导航到 **Home > Overview > Details**，然后获取群集 API 地址。
2. *创建服务帐户并使用 OpenShift 命令行界面 (CLI) (oc 命令) 获取服务帐户令牌*: 服务帐户令牌是与服务帐户关联的身份验证凭据。服务帐户用于向 OpenShift 验证 OpenShift 插件。每个服务帐户都与一个 命名空间 关联。
3. *配置服务帐户的权限*: 一个服务帐户可以有多个角色，每个角色都包含定义 OpenShift 插件可以在哪些资源上执行哪些操作的权限。角色通过 **角色绑定** 进行绑定，**角色绑定** 有两种类型：
   a. **集群范围的角色绑定**：用于从 OpenShift 接收事件。 命名空间绑定的角色绑定：用于管理特定命名空间中的 VM。
   b. **命名空间绑定的角色绑定**：用于管理特定命名空间中的 VM。
4. *创建命名空间（项目）*: OpenShift 中的命名空间是一个隔离环境，它将 VM 或网络等资源分组，从而实现更好的组织和访问控制。**命名空间** 是 Kubernetes 术语，而 **项目** 是 OpenShift 术语。从 OpenShift 插件的角度来看，它们是相同的。部署 VM 需要命名空间。使用 OpenShift 控制台或 OpenShift Container Platform CLI 创建命名空间。
5. *在目标命名空间下创建一个网络附加定义*: 网络附加定义指定了在 OpenShift 中运行的 VM 的网络配置。在 **网络 > 网络附加定义** 下，您可以查看每个命名空间的网络附加定义。

6. *配置存储类*: 存储类定义了 VM 存储的分配方式。在 **存储 > 存储类** 下，您可以配置并查看存储提供商列表。

创建服务帐户

1. 下载并解压 oc 命令行工具。
2. 使用您的登录 ID 访问 OpenShift 控制台。
3. 单击您的用户配置文件，然后单击 **复制登录命令**。
4. 单击 **显示令牌** 并复制令牌。
5. 使用 oc 命令行运行登录命令。示例：

```
.\oc.exe login --token=<token> --server=<server address>
```

6. 创建服务帐户。
   - 如果要在默认命名空间下创建服务帐户，请运行：

```
.\oc.exe create sa <service account name>
```

   - 如果您想在自己的命名空间下创建服务帐户，请运行：

```
.\oc.exe create sa <service account name> -n mynamespace
```

7. 为密钥创建 `YAML` 文件。示例：
   - 如果您在默认命名空间下创建服务帐户：

```
apiVersion: v1

kind: Secret

metadata:

name: service account name

annotations:

kubernetes.io/service-account.name: service account name
```

```
type: kubernetes.io/service-account-token
```

- 如果您在自己的命名空间下创建服务帐户：

```
apiVersion: v1

kind: Secret

metadata:

name: service account name

namespace: mynamespace

annotations:

kubernetes.io/service-account.name: service account name

 type: kubernetes.io/service-account-token
```

8. 应用 YAML。

```
.\oc.exe apply -f <yamlFile.yaml>
```

注意：

`oc` 描述了获取令牌的密钥。该令牌用作密码。

为服务帐户创建角色和角色绑定

通过集群范围的角色绑定，服务帐户拥有读取整个集群中所有 VM 事件的权限，从而允许 OpenShift 插件为所有与 VM 相关的事件维护一个事件监视器。 通过命名空间角色绑定，服务帐户拥有管理目标命名空间中 VM 的权限。 您可以使用脚本创建角色并将其绑定到服务帐户。请参阅 `<https://github.com/citrix/citrix-mcs-sdk-samples/tree/main/OpenShift/Hosting%20Connection/Role/>`。

下一步

- 安装核心组件

- 安装 VDA
- 创建站点
- 有关创建和管理连接的信息，请参阅连接到 Red Hat OpenShift

更多信息

- 创建和管理连接和资源
- 创建计算机目录

VMware 虚拟化环境

如果您使用 VMware 提供虚拟机，请遵循此指南。

安装 vCenter Server 和相应的管理工具。（不支持 vSphere vCenter Linked Mode 操作。）

如果您计划使用 MCS，请勿禁用 vCenter Server 中的 Datastore Browser 功能（如 `<https://kb.vmware.com/s/article/2101567>` 中所述）。禁用此功能后，MCS 将无法正常工作。

下一步操作

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关在 VMware 环境中创建和管理连接的信息，请参阅 连接到 VMware

更多信息

- 创建和管理连接与资源
- 创建计算机目录

VMware 云和合作伙伴解决方案

Citrix Virtual Apps and Desktops™ 支持以下 VMware 云和合作伙伴解决方案：

- Azure VMware 解决方案 (AVS)
- 谷歌云 VMware 引擎
- 在 Amazon Web Services (AWS) 上运行的 VMware Cloud

Azure VMware 解决方案 (AVS) 集成

Citrix Virtual Apps and Desktop 服务支持 AVS。AVS 提供包含由 Azure 基础架构创建的 vSphere 群集的云基础架构。利用 Citrix Virtual Apps and Desktop 服务使用 AVS 预配 VDA 工作负载，其方式与在本地环境中使用 vSphere 相同。

设置 AVS 群集

要使 Citrix Virtual Apps™ and Desktop 服务能够使用 AVS，请在 Azure 中执行以下步骤：

- 请求主机配额
- 注册 Microsoft.AVS 资源提供程序
- 网络清单
- 创建 Azure VMware Solution 私有云
- 访问 Azure VMware Solution 私有云
- 在 Azure 中为您的 VMware 私有云配置网络
- 配置适用于 Azure VMware Solution 的 DHCP
- 在 Azure VMware Solution 中添加网络段
- 验证 Azure VMware Solution 环境

为 Azure 企业协议客户请求主机配额
在 Azure 门户的“**帮助 + 支持**”页面中，选择“**新建支持请求**”，并包含以下信息：

- 问题类型:技术
- 订阅:选择您的订阅
- 服务:所有服务 > Azure VMware Solution
- 资源:一般问题
- 摘要:需要容量
- 问题类型:容量管理问题
- 问题子类型:客户请求额外主机配额/容量

在支持票证的 **Description** 中，在 **Details** 选项卡中包含以下信息：

- POC 或生产
- 区域名称
- 主机数量
- 任何其他详细信息

> **注意：**

> AVS 最少需要三台主机，并建议您使用 N+1 主机冗余。

> 指定支持票证的详细信息后，选择 **Review + Create** 以将请求提交到 Azure。

注册 Microsoft.AVS 资源提供程序

请求主机配额后，注册资源提供程序：

1. 登录到 Azure 门户。
2. 在 Azure 门户菜单上，选择 **所有服务**。
3. 在 **所有服务** 菜单中，输入订阅，并选择 **订阅**。
4. 从订阅列表中选择订阅。
5. 选择 **资源提供程序** 并在搜索栏中输入 **Microsoft.AVS**。
6. 如果资源提供程序未注册，请选择 **注册**。

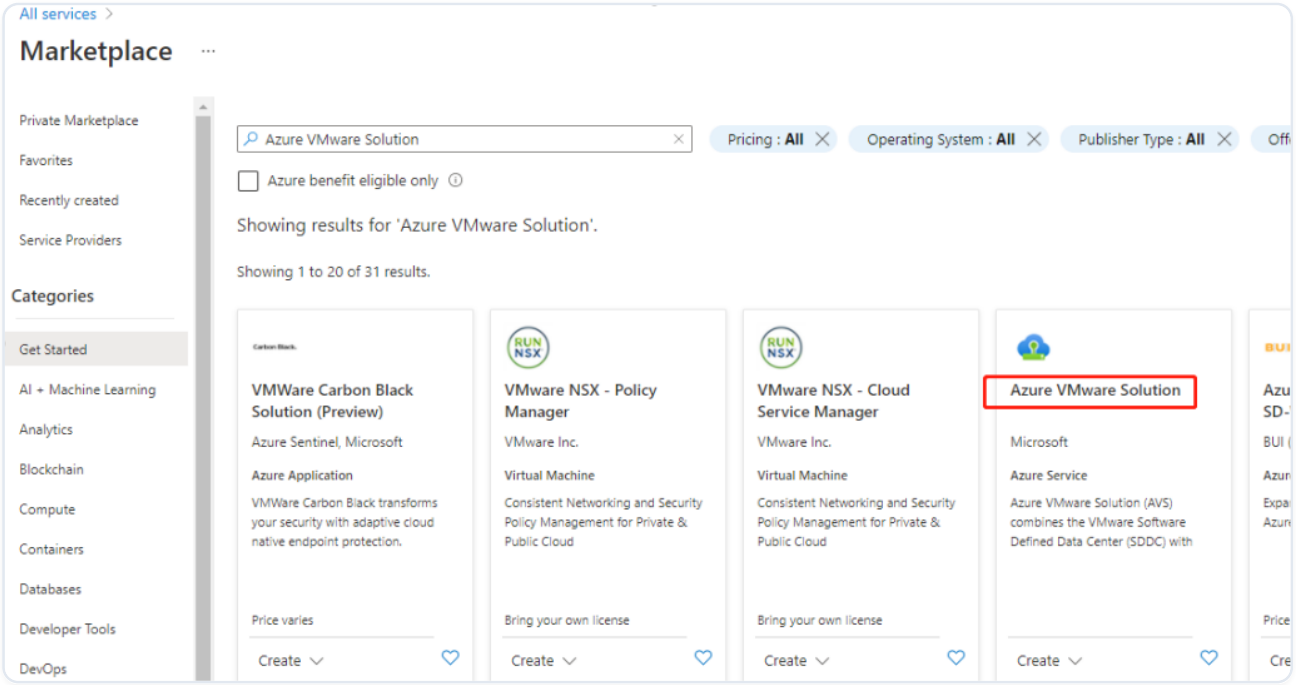
网络注意事项

AVS 提供需要特定网络地址范围和防火墙端口的网络服务。有关详细信息，请参阅 Azure VMware Solution 的网络规划清单。

创建 Azure VMware Solution 私有云

在考虑了环境的网络要求后，创建一个 ASV 私有云：

1. 登录 Azure 门户。
2. 选择 **创建新资源**。
3. 在 **搜索市场** 文本框中键入 *Azure VMware Solution*，然后从列表中选择 **Azure VMware Solution**。



图像

在 **Azure VMware Solution** 窗口中：

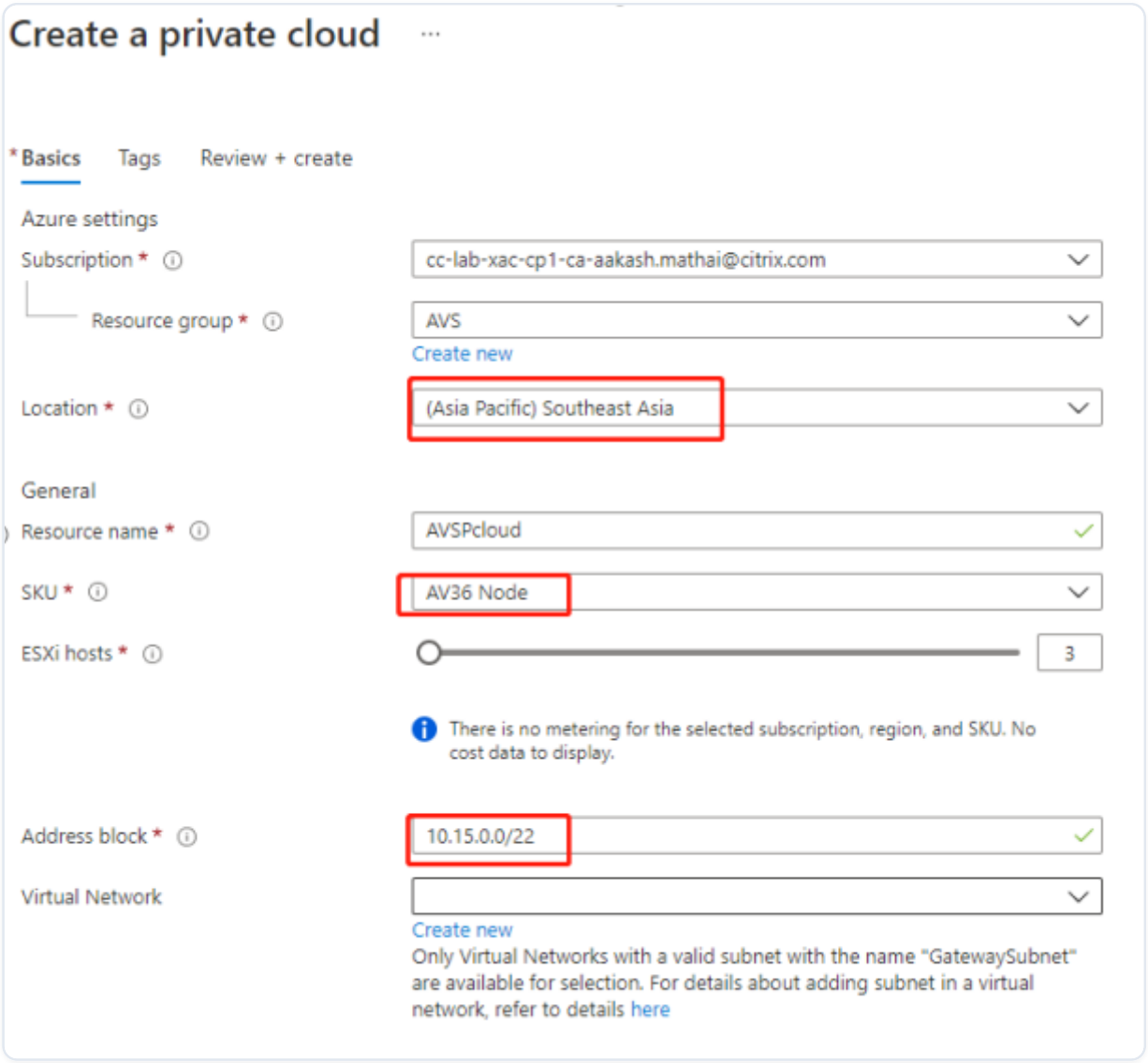
1. 选择 **创建**。
2. 单击**基本信息**选项卡。
3. 使用下表中的信息，输入字段的值：

字段	值
订阅	选择您计划用于部署的订阅。Azure 订阅中的所有资源将一起计费。
资源组	选择您的私有云的资源组。Azure 资源组是一个逻辑容器，Azure 资源部署和管理于其中。或者，您可以为您的私有云创建一个新的资源组。
位置	选择一个位置，例如美国东部。这是您在规划阶段定义的区域。
资源名称	提供您的 Azure VMware Solution 私有云的名称。
SKU	选择 AV36。
主机	显示为私有云集群分配的主机数量。默认值为 3，部署后可以增加或减少。
地址块	为私有云提供一个 IP 地址块。CIDR 代表私有云管理网络，将用于集群管理服务，例如 vCenter Server 和 NSX-T Manager。使用 /22 地址空间，例如 10.175.0.0/22。该地址应是唯一的，并且不与其他的 Azure 虚拟网络以及本地网络重叠。
虚拟网络	将其留空，因为 Azure VMware Solution ExpressRoute 线路是在部署后步骤中建立的。

在“**创建私有云**”屏幕中：

1. 在**位置**字段中，选择具有 AVS 的区域；资源组区域与 AVS 区域相同。
2. 在 **SKU** 字段中，选择 **AV36 Node**。
3. 在 **地址块** 字段中指定一个 IP 地址。例如，10.15.0.0/22。

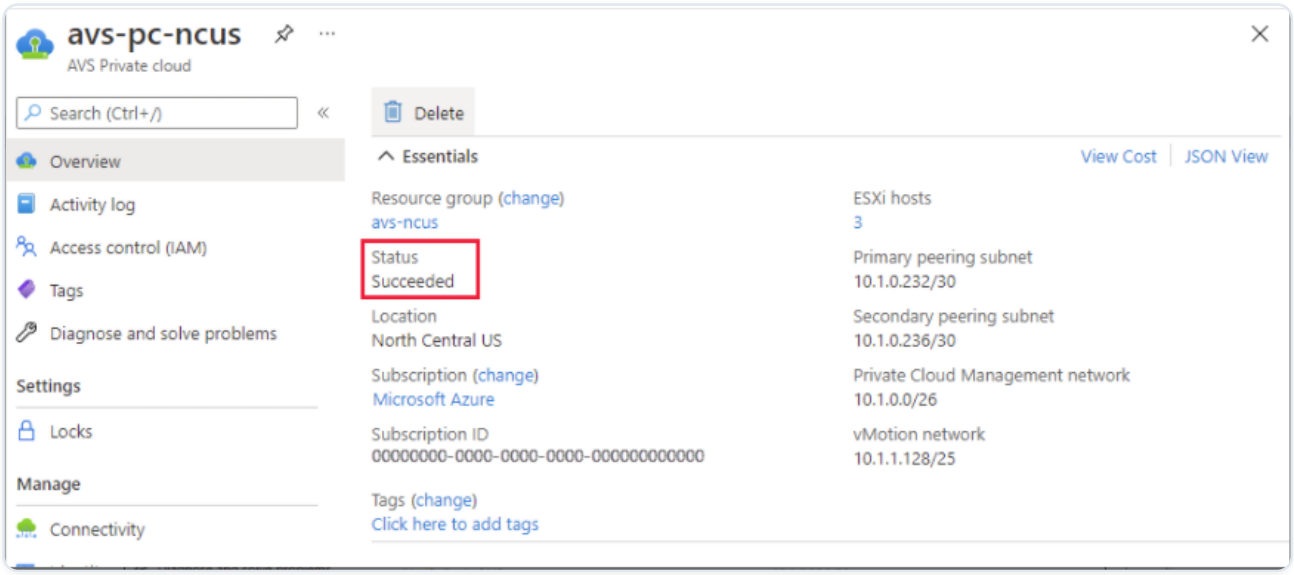
4. 选择“**审查 + 创建**”。
5. 审查信息后，单击“**创建**”。



提示：

创建私有云可能需要 3-4 小时。向集群添加单个主机可能需要 30-45 分钟。

验证部署是否成功。导航到您创建的资源组并选择您的私有云。一旦 **状态** 为 **成功**，部署即完成。



访问 Azure VMware Solution 私有云

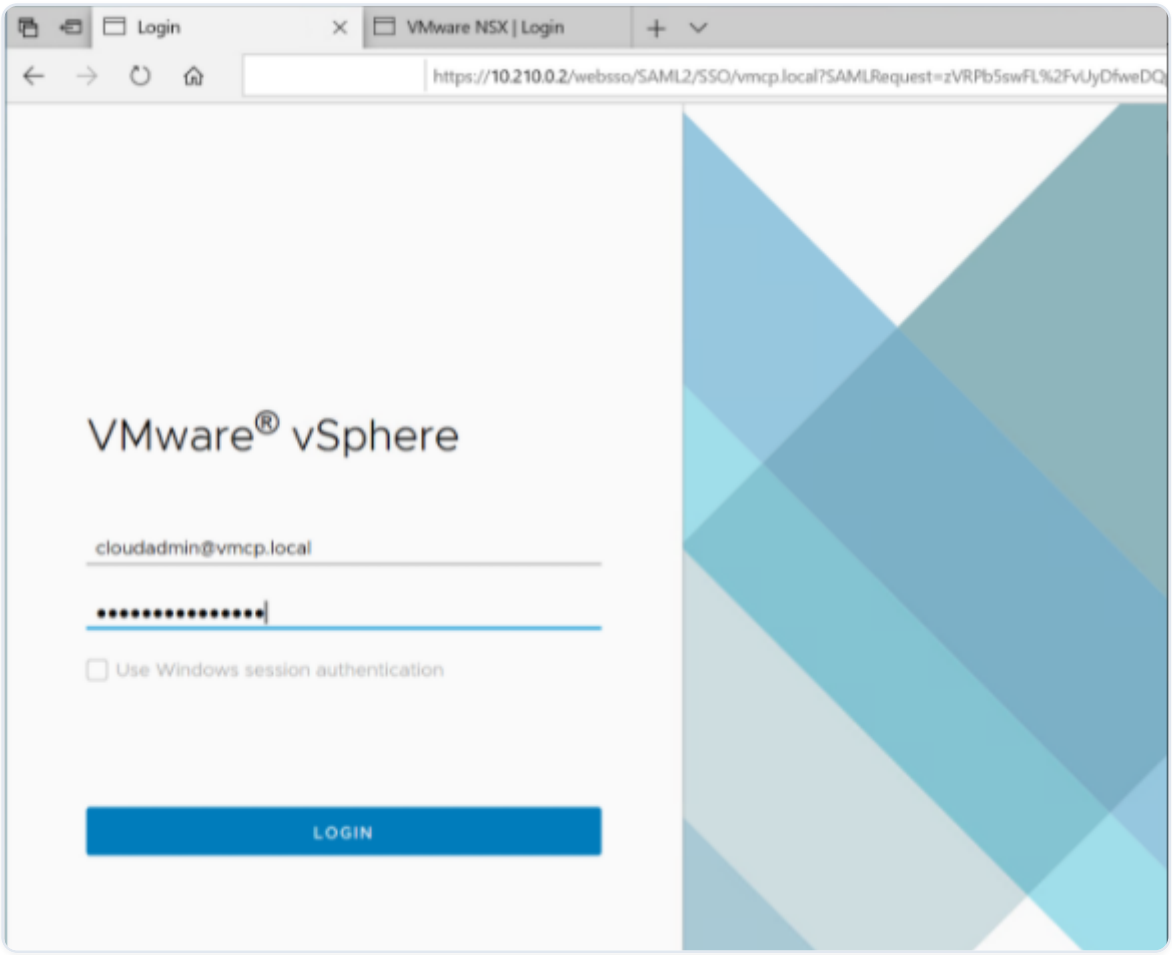
创建私有云后，创建 Windows VM 并连接到私有云的本地 vCenter。

创建新的 Windows 虚拟机

1. 在资源组中，选择 **+ 添加**，然后搜索并选择 **Microsoft Windows 10/2016/2019**。
2. 单击**创建**。
3. 输入所需信息，然后选择“**审查 + 创建**”。
4. 验证通过后，选择“**创建**”以开始虚拟机创建过程。

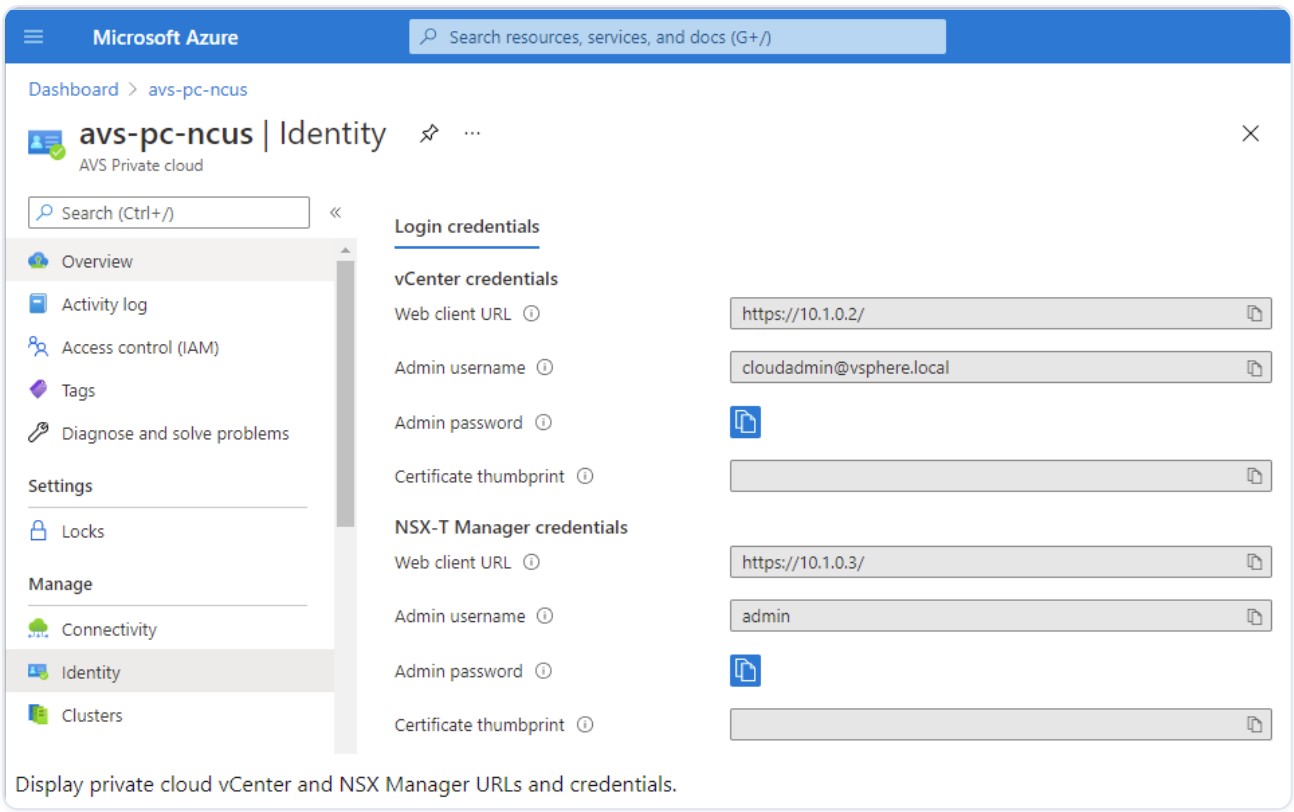
连接到私有云的本地 vCenter

1. 以云管理员身份登录 **vSphere Client with VMware vCenter SSO**。



2. 在 Azure 门户中，选择您的私有云，然后选择 **管理 > 身份**。

私有云 vCenter 和 NSX-T Manager 的 URL 和用户凭据显示如下：



确认 URL 和用户凭据后：

1. 导航到您在上一步中创建的 VM 并连接到该虚拟机。
2. 在 Windows VM 中，打开浏览器并在两个浏览器选项卡中导航到 vCenter 和 NSX-T Manager URL。在 vCenter 选项卡中，输入上一步中的 *cloudadmin@vmcp.local* 用户凭据。

在 Azure 中为您的 VMware 私有云配置网络
访问 ASV 私有云后，通过创建虚拟网络和网关来配置网络。
创建虚拟网络

1. 登录 Azure 门户。
2. 导航到之前创建的资源组。
3. 选择 **+ 添加** 以定义新资源。
4. 在 **搜索市场** 文本框中，键入 *虚拟网络*。找到虚拟网络资源并选择它。
5. 在**虚拟网络**页面上，选择**创建**以设置您的私有云的虚拟网络。
6. 在**创建虚拟网络**页面上，输入您的虚拟网络的详细信息。
7. 在**基本信息**选项卡上，输入虚拟网络的名称，选择相应的区域，然后单击**下一步：IP 地址。**
8. 在**IP 地址**选项卡上，在 IPv4 地址空间下，输入之前创建的地址。

> **重要提示：**

> 使用的地址不得与您创建私有云时使用的地址空间重叠。

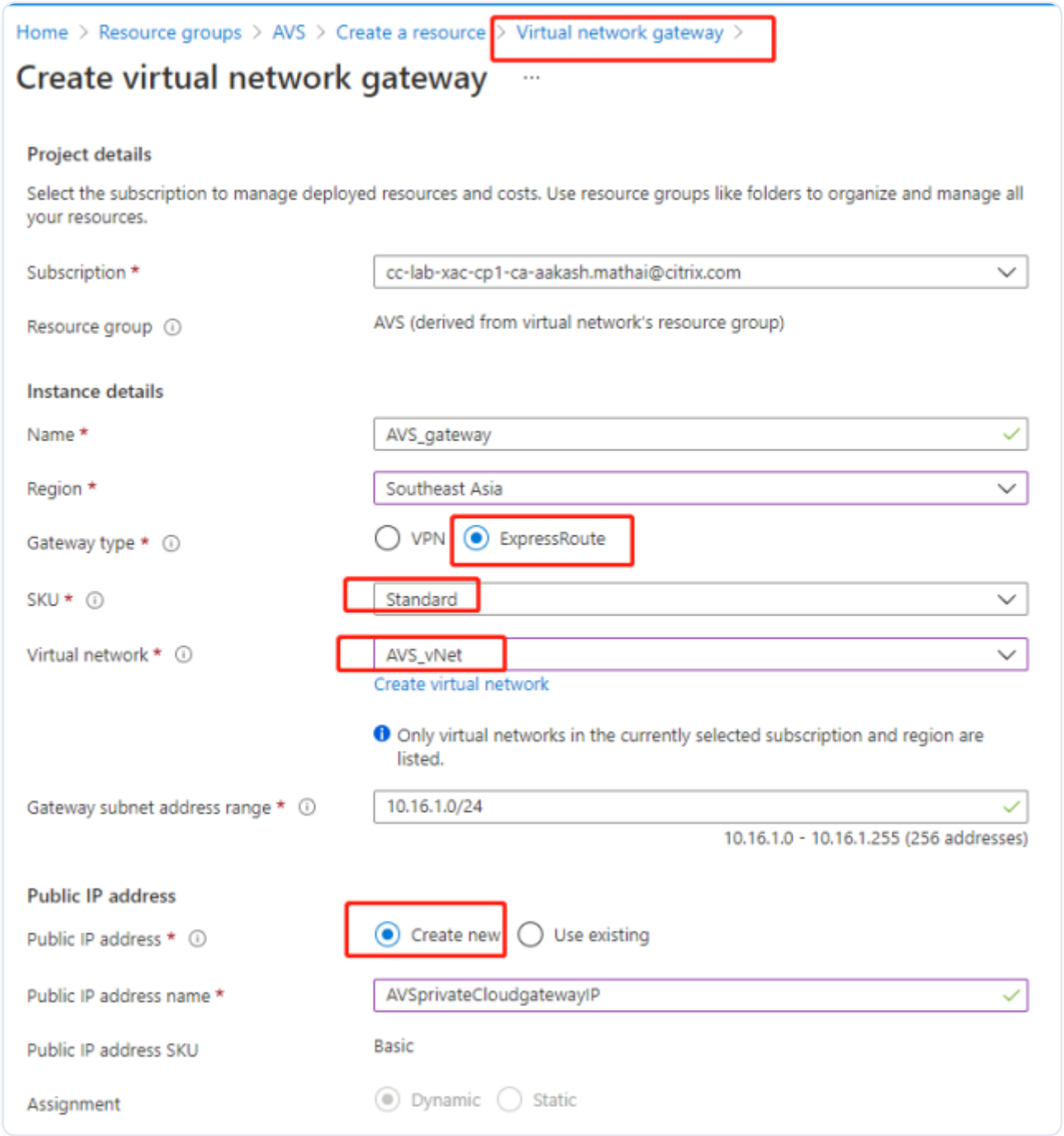
> 输入地址空间后：

1. 选择**+ 添加子网**。
2. 在**添加子网**页面上，为子网指定名称和适当的地址范围。
3. 单击**添加。**
4. 选择**审核 + 创建**。
5. 验证信息并单击**创建**。部署完成后，虚拟网络将显示在资源组中。

创建虚拟网络网关
创建虚拟网络后，创建虚拟网络网关。

1. 在您的资源组中，选择**+ 添加**以添加新资源。
2. 在“**搜索市场**”文本框中，键入 *虚拟网络网关*。找到虚拟网络资源并选择它。

3. 在“**虚拟网络网关**”页面上，单击“**创建**”。
4. 在“**创建虚拟网络网关**”页面上的“**基本信息**”选项卡中，为字段提供值。
5. 单击“**审查 + 创建**”。



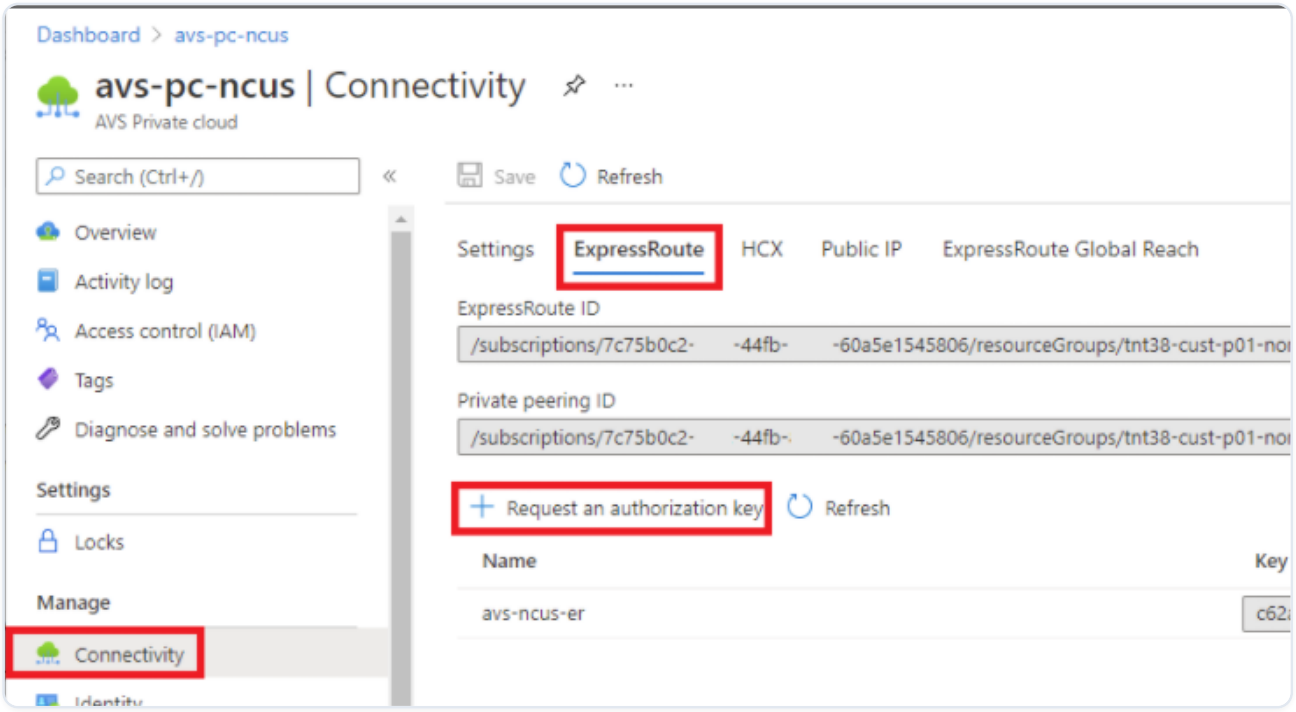
审查虚拟网络网关配置后，单击“**创建**”以部署虚拟网络网关。 部署完成后，将您的 **ExpressRoute** 连接连接到包含 Azure AVS 私有云的虚拟网络网关。

将 ExpressRoute 连接到虚拟网络网关

部署虚拟网络网关后，在其与 Azure AVS 私有云之间添加连接：

1. 请求 ExpressRoute 授权密钥。

2. 在 Azure 门户中，导航到“**Azure VMware Solution 私有云**”。选择“**管理 > 连接 > ExpressRoute**”，然后选择“**+ 请求授权密钥**”。



请求授权密钥后：

1. 输入密钥名称，然后单击“**创建**”。创建密钥可能需要大约 30 秒。创建后，新密钥将显示在私有云的授权密钥列表中。
2. 复制 **授权密钥** 和 **ExpressRoute ID**。您将需要它们来完成对等过程。授权密钥会在一段时间后消失，因此请在它出现后立即复制。
3. 导航到您计划使用的**虚拟网络网关**，并选择“**连接 > + 添加**”。
4. 在“**添加连接**”页面上，提供字段值，然后选择“**确定**”。

Azure ASV 添加连接(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-avs-add-connection-v2.png)

连接已在您的 ExpressRoute 线路和您的虚拟网络之间建立：

Azure ASV 连接成功(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-avs-connection-succeeded.png)
配置适用于 Azure VMware Solution 的 DHCP
将 ExpressRoute 连接到虚拟网关后，配置 DHCP。
使用 NSX-T 托管您的 DHCP 服务器
在 NSX-T Manager 中：

1. 选择“**网络 > DHCP**”，然后选择“**添加服务器**”。

2. 对于“**服务器类型**”，选择“**DHCP**”，提供服务器名称和 IP 地址。
3. 单击 **保存**。
4. 选择“**第 1 层网关**”，选择第 1 层网关上的垂直省略号，然后选择“**编辑**”。
5. 选择“**未设置 IP 分配**”以添加子网。
6. 对于“**类型**”，选择“**DHCP 本地服务器**”。
7. 对于“**DHCP 服务器**”，选择“**默认 DHCP**”，然后单击“**保存**”。
8. 再次点击“**保存**”，然后选择“**关闭编辑**”。

Azure ASV 添加 NSX-T 服务器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-avs-nsx-t-add-server.png)
在 Azure VMware Solution 中添加网络段
设置 DHCP 后，添加网络段。

要添加网络分段，请在 NSX-T Manager 中选择“**网络 > 分段**”，然后点击“**添加分段**”。

Azure ASV 添加 NSX-T 分段(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-avs-nsx-t-add-segment.png)

在“**分段配置文件**”屏幕中：

1. 输入该分段的**名称**。
2. 选择“**Tier-1 网关 (TNTxx-T1)**”作为“**连接的网关**”，并将“**类型**”保留为“**灵活**”。
3. 选择预配置的覆盖**传输区域 (TNTxx-OVERLAY-TZ)**。
4. 点击“**设置子网**”。

Azure ASV 添加 NSX-T 分段配置文件(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-avs-nsx-t-segment-profiles.png)

在“**子网**”部分中：

1. 输入网关 IP 地址。
2. 选择“**添加**”。

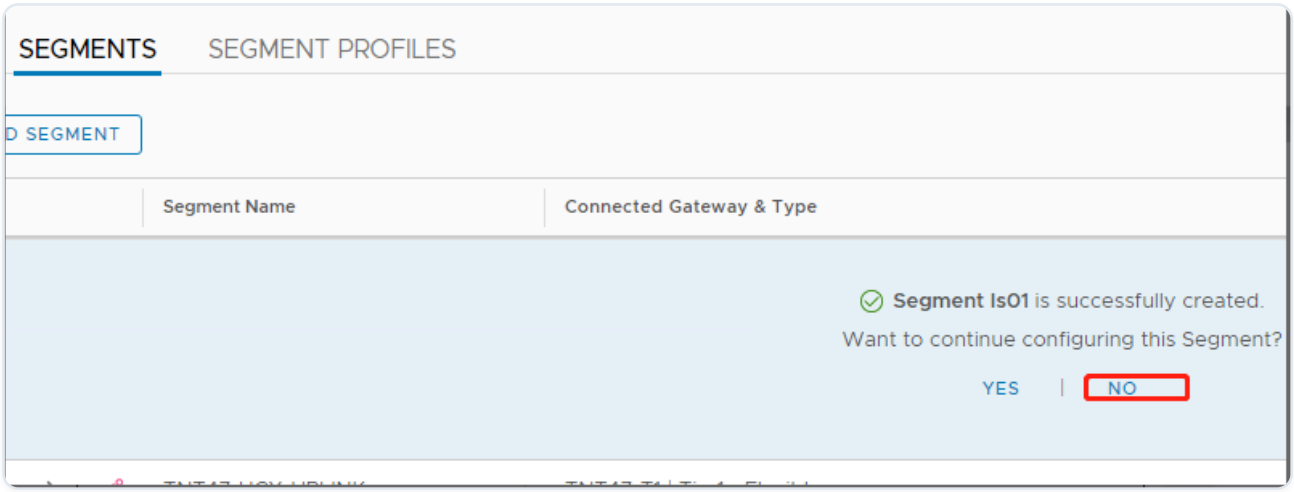
> **重要提示：**

> 此分段 IP 地址必须属于 Azure 网关 IP 地址，10.15.0.0/22。

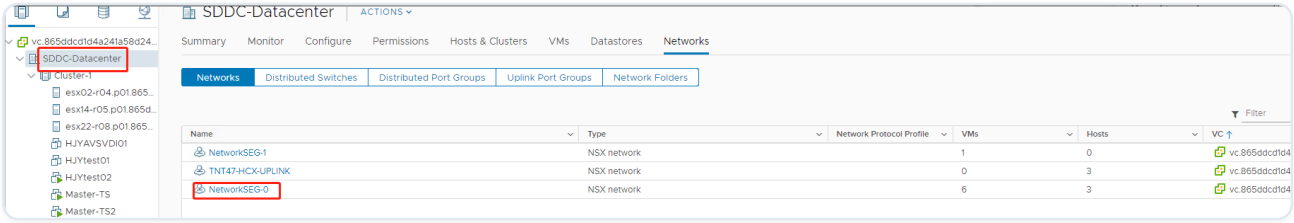
> DHCP 范围应属于网段 IP 地址：



选择 **否** 以拒绝继续配置分段的选项：



在 vCenter 中，选择 **网络 > SDDC-数据中心**：

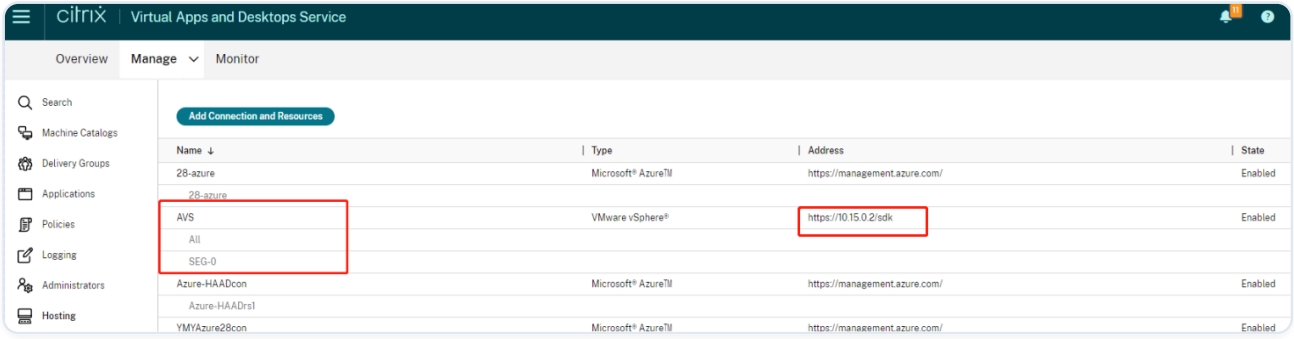


验证 Azure AVS 环境

在 Azure 资源组中设置直接连接和连接器：

Azure ASV ASV 验证连接(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-avs-verify-connection-create-dc-v2.png)

使用 vCenter 凭据验证连接：



谷歌云 VMware 引擎

Citrix Virtual Apps and Desktops 允许您将基于 VMware 的本地 Citrix 工作负载迁移到 Google Cloud VMware Engine。

配置 GOOGLE CLOUD VMWARE 引擎

以下过程介绍了如何在 Google Cloud VMware 引擎上获取和设置集群。

访问 VMware Engine 门户

1. 在 **Google Cloud Console** 中，单击导航菜单。
2. 在 **计算** 部分中，单击 **VMware Engine** 以在新浏览器选项卡中打开 VMware Engine。

创建第一个私有云的要求

您必须拥有 Google Cloud VMware Engine 的访问权限、可用的 VMware Engine 节点配额以及适当的 IAM 角色。在继续创建私有云之前，请准备以下要求：

1. 请求 API 访问权限和节点配额。有关详细信息，请参阅 请求 API 访问权限和配额。
2. 记下您要用于 VMware 管理设备和 HCX 部署网络的地址范围。有关详细信息，请参阅 网络要求。
3. 获取 VMware Engine Service 管理员 IAM 角色。

创建您的第一个私有云

1. 访问 VMware Engine 门户。
2. 在 VMware Engine 主页上，单击 **创建私有云**。将列出托管位置和硬件节点类型。
3. 选择私有云的节点数。至少需要三个节点。
4. 为 VMware 管理网络输入一个无类别域间路由 (CIDR) 范围。
5. 为 HCX 部署网络输入一个 CIDR 范围。

> **重要提示：**
>
> CIDR 范围不得与您的任何本地或云子网重叠。CIDR 范围必须为 /27 或更高。

6. 选择 **审核并创建**。
7. 查看设置。要更改任何设置，请单击 **Back**。
8. 单击 **Create** 开始创建私有云。

当 VMware Engine 创建您的新私有云时，它会部署多个 VMware 组件并为私有云中的集群设置初始 Autoscale™ 策略。私有云创建可能需要 30 分钟到 2 小时。预配完成后，您会收到一封电子邮件。

设置 谷歌云 VMware Engine VPN 网关

要与 Google Cloud VMware Engine 建立初始连接，您可以使用 VPN 网关。这是一个基于 OpenVPN 的客户端 VPN，您可以使用它连接到您的 VMware 软件定义数据中心 (SDDC) vCenter 并执行任何所需的初始配置。

在部署 VPN 网关之前，请配置部署 SDDC 的区域的 **Edge Services** 范围。为此：

1. 登录 **Google Cloud VMware Engine** 门户，然后转到 **Network > Regional Settings**。单击 **Add Region**。
2. 选择部署 SDDC 的区域，并启用 **Internet Access** 和 **Public IP Service**。
3. 提供规划期间记录的 Edge Services 范围，然后单击 **Submit**。启用这些服务需要 10-15 分钟。

   完成后，Edge Services 在“区域设置”页面上显示为 **Enabled**。启用这些设置允许将公共 IP 分配给您的 SDDC，这是部署 VPN 网关的要求。

要部署 VPN 网关：

1. 在 **Google Cloud VMware Engine** 门户中，转到 **网络 > VPN 网关**。单击 **创建新的 VPN 网关**。
2. 提供 VPN 网关的名称以及规划期间保留的客户端子网。单击“**下一步**”。
3. 选择要授予 VPN 访问权限的用户。单击“**下一步**”。
4. 指定必须通过 VPN 访问的网络。单击“**下一步**”。
5. 将显示摘要屏幕。验证选择，然后单击“**提交**”以创建 VPN 网关。将显示 VPN 网关页面，其中新 VPN 网关的状态为“**正在创建**”。
6. 状态变为“**运行中**”后，单击新的 VPN 网关。
7. 单击“**下载我的 VPN 配置**”以下载包含 VPN 网关预配置 OpenVPN 配置文件的 ZIP 文件。提供了通过 UDP/1194 和 TCP/443 连接的配置文件。选择您的首选项并将其导入 Open VPN，然后连接。
8. 转到“**资源**”并选择您的 SDDC。

连接 VPN

1. 通过 VPN 网关设置在本地网络和私有云之间建立点到站点连接。请参阅 设置 Google Cloud VMware Engine VPN 网关。
2. 上传在 设置 Google Cloud VMware Engine VPN 网关 中下载的 VPN 配置。
3. 导入到您的 VPN 客户端，例如 OpenVPN Connect。

有关详细信息，请参阅 使用 VPN 连接。

创建第一个子网

从 VMware Engine 门户访问 NSX-T Manager

创建子网的过程在 NSX-T 中进行，您可以通过 VMware Engine 访问 NSX-T。请执行以下操作以访问 NSX-T Manager。

1. 登录到 **Google Cloud VMware Engine** 门户。
2. 从主导航中，转到 **资源**。
3. 单击与要创建子网的私有云对应的 **私有云名称**。
4. 在私有云的详细信息页面上，单击 **vSphere Management Network** 选项卡。
5. 单击与 NSX-T Manager 对应的 **FQDN**。
6. 出现提示时，输入您的登录凭据。如果您已设置 vIDM 并将其连接到身份源（例如 Active Directory），请改用您的身份源凭据。

> **提醒：**
>
> 您可以从私有云详细信息页面检索生成的凭据。

为子网设置 DHCP 服务

在创建子网之前，请设置 DHCP 服务：

在 NSX-T Manager 中：

1. 转到 **网络 > DHCP**。网络仪表板显示 DHCP 服务创建了一个 Tier-0 和一个 Tier-1 网关。
2. 要开始预配 DHCP 服务器，请单击 **添加服务器**。
3. 为 **服务器类型** 选择 **DHCP**，提供服务器名称和 IP 地址。
4. 单击 **保存** 以创建 DHCP 服务。

执行以下操作以将此 DHCP 服务附加到相关的 Tier-1 网关。DHCP 服务已预配了一个默认的 Tier-1 网关：

1. 选择 **Tier 1 网关**，选择 Tier-1 网关上的垂直省略号，然后选择 **编辑**。
2. 在 **IP 地址管理** 字段中，选择 **未设置 IP 分配**。
3. 为 **类型** 选择 **DHCP 本地服务器**。
4. 为 **DHCP 服务器** 选择您创建的 DHCP 服务器。
5. 单击 **保存**。
6. 单击 **关闭编辑**。

您现在可以在 NSX-T 中创建网络分段。有关 NSX-T 中 DHCP 的更多信息，请参阅 VMware DHCP 文档。

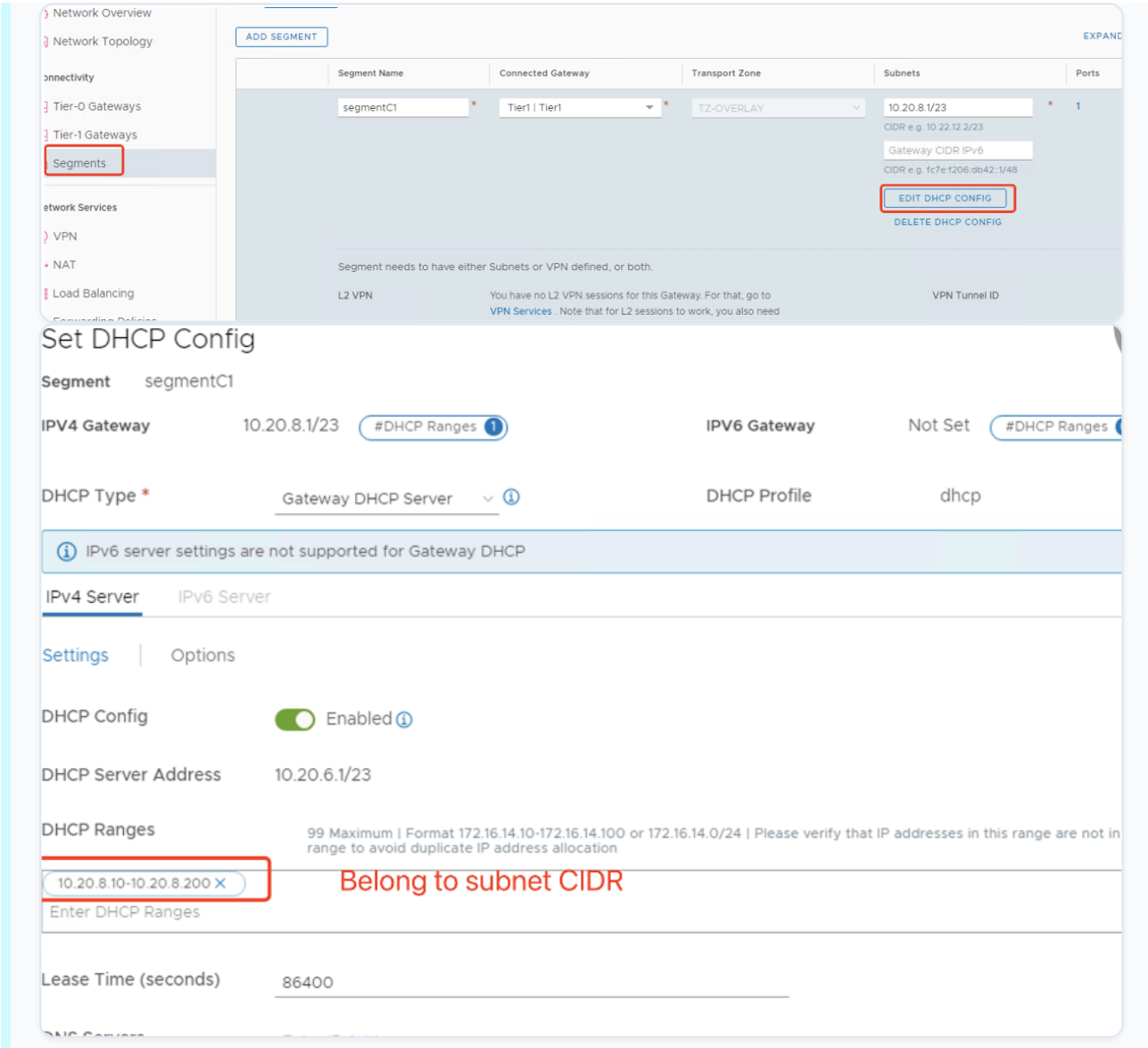
在 NSX-T 中创建网络分段

对于工作负载 VM，您可以为私有云创建作为 NSX-T 网络分段的子网：

1. 在 NSX-T Manager 中，转到 **网络 > 分段**。
2. 单击 **添加分段**。
3. 输入分段的名称。
4. 选择 **Tier-1** 作为 **连接的网关**，并将类型保留为 **灵活**。
5. 单击 **设置子网**。
6. 单击 **添加子网**。
7. 在 **网关 IP/前缀长度** 中输入子网范围。将子网范围指定为以 **.1** 作为最后一个八位字节。例如，**10.12.2.1/24**。
8. 指定 DHCP 范围，然后单击 **添加**。
9. 在 **传输区域** 中，从下拉列表中选择 **TZ-OVERLAY**。
10. 单击 **保存**。现在，您可以在 vCenter 中创建 VM 时选择此网络段。

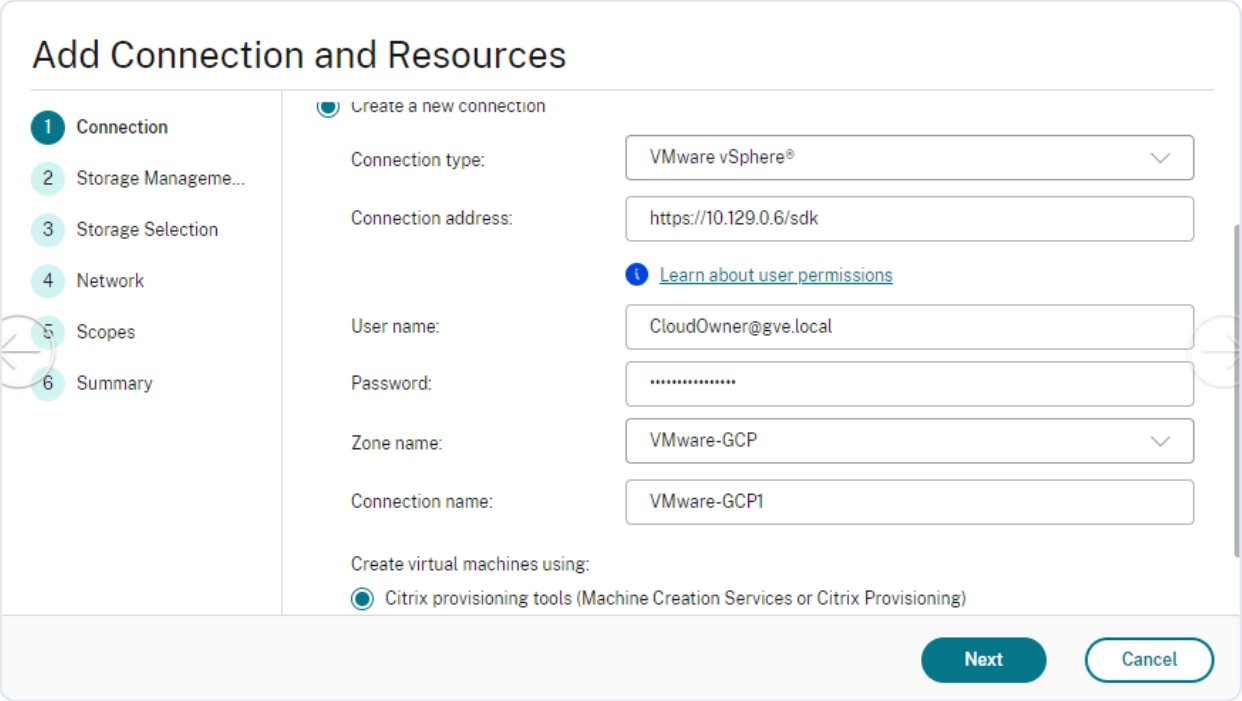
在给定区域中，您最多可以使用私有服务访问从 VMware Engine 设置 100 条到 VPC 网络的唯一路由。这包括（例如）私有云管理 IP 地址范围、NSX-T 工作负载网络段和 HCX 网络 IP 地址范围。此限制包括该区域中的所有私有云。

> **注意：**
>
> 存在一个 Google Cloud 配置问题，因此您需要多次配置 DHCP 范围设置。因此，请务必在 Google Cloud 配置后配置 DHCP 范围设置。单击 **编辑 DHCP 配置** 以配置 DHCP 范围。



在 Citrix Studio 中创建 Google Cloud VMware 连接

1. 在 vCenter 中创建计算机。
2. 启动 Citrix Studio 应用程序。
3. 选择托管节点，然后单击 **添加连接和资源**。
4. 在 **连接** 屏幕上，选择 **创建新连接**，以及以下详细信息：



a. 将 **连接类型** 选择为 **VMware vSphere**。

b. 在**连接地址**中，输入 vCenter 私有 IP 地址。

c. 输入 vCenter 凭据。

d. 输入连接名称。

e. 选择用于创建虚拟机的工具。

5. 在“**网络**”屏幕上，选择在 NSX-T 服务器中创建的子网。

6. 完成向导。

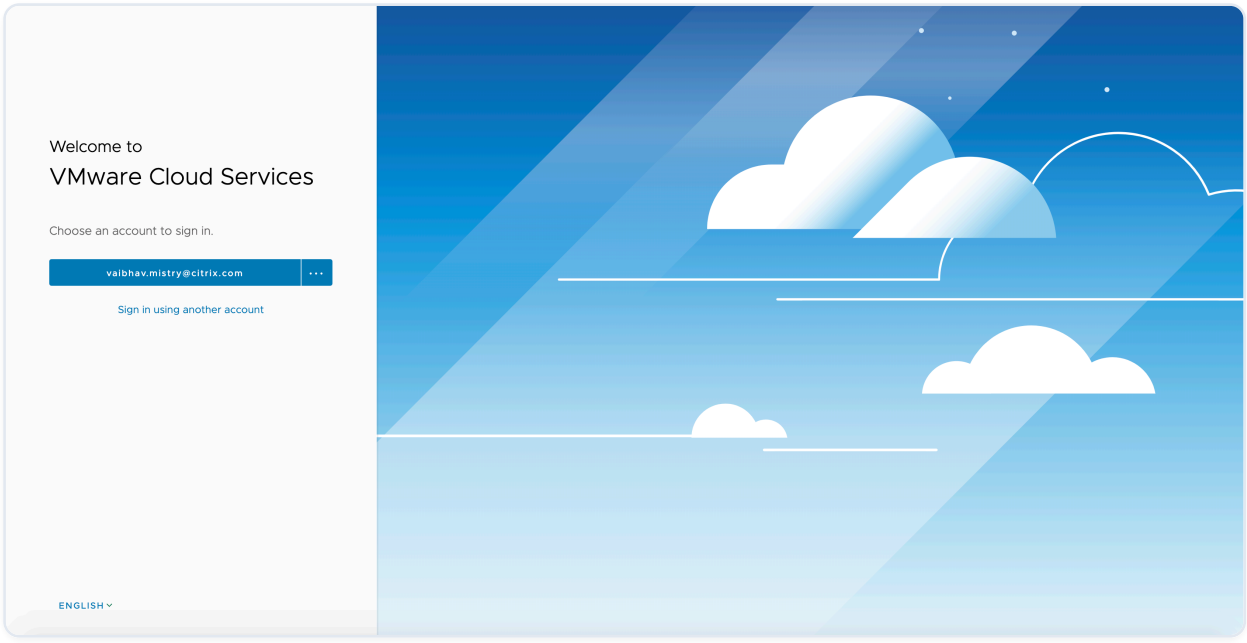
亚马逊网络服务 (AWS) 上的 VMware 云

Amazon Web Services (AWS) 上的 VMware Cloud 使您能够将基于 VMware 的本地 Citrix 工作负载迁移到 AWS Cloud。

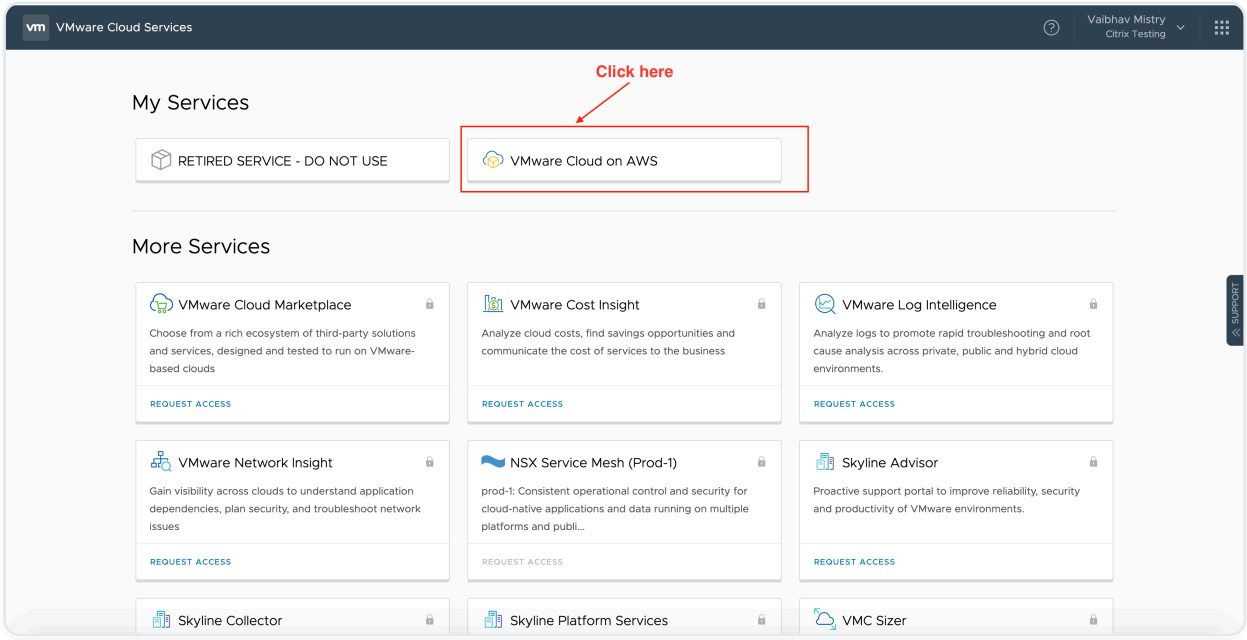
本文介绍了在 AWS 上设置 VMware Cloud 的过程。

访问 VMWARE CLOUD 环境

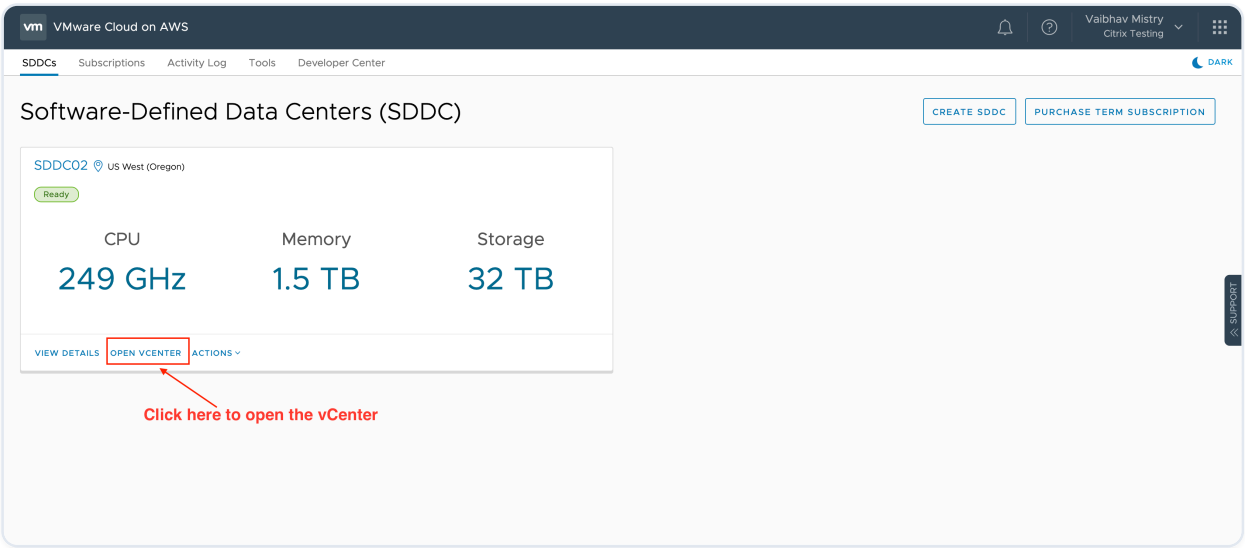
1. 使用 URL `<https://console.cloud.vmware.com/>` 登录到 VMware Cloud 服务。

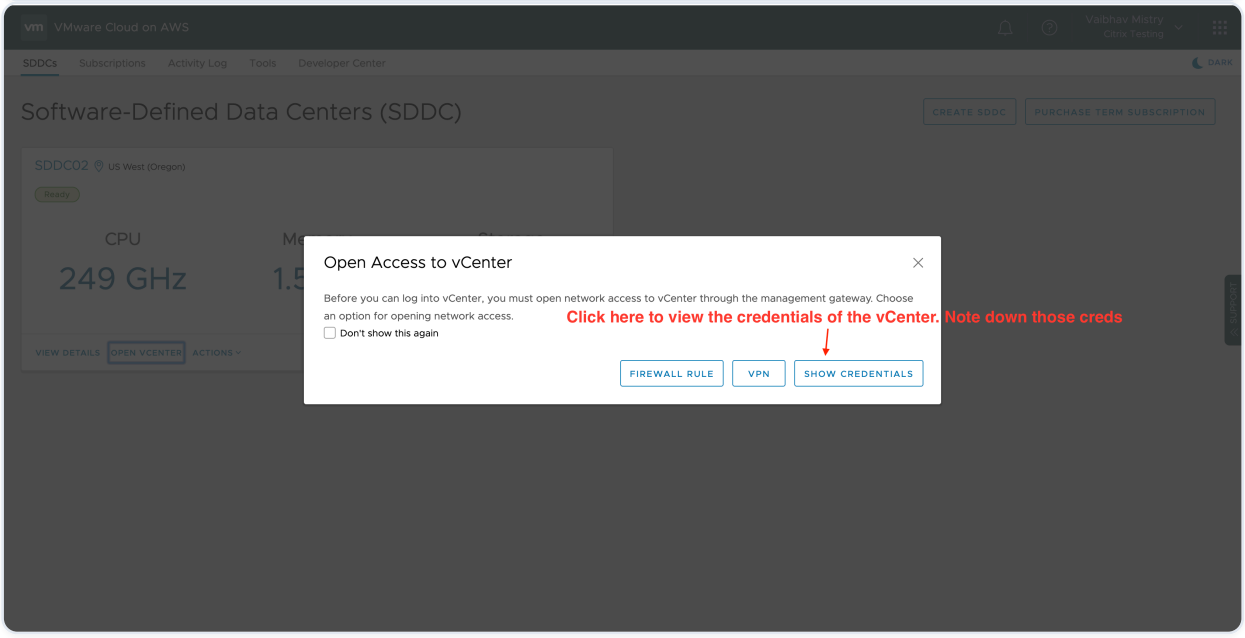


2. 单击**Amazon Web Services 上的 VMware Cloud**。将显示“软件定义数据中心 (SDDC)”页面。

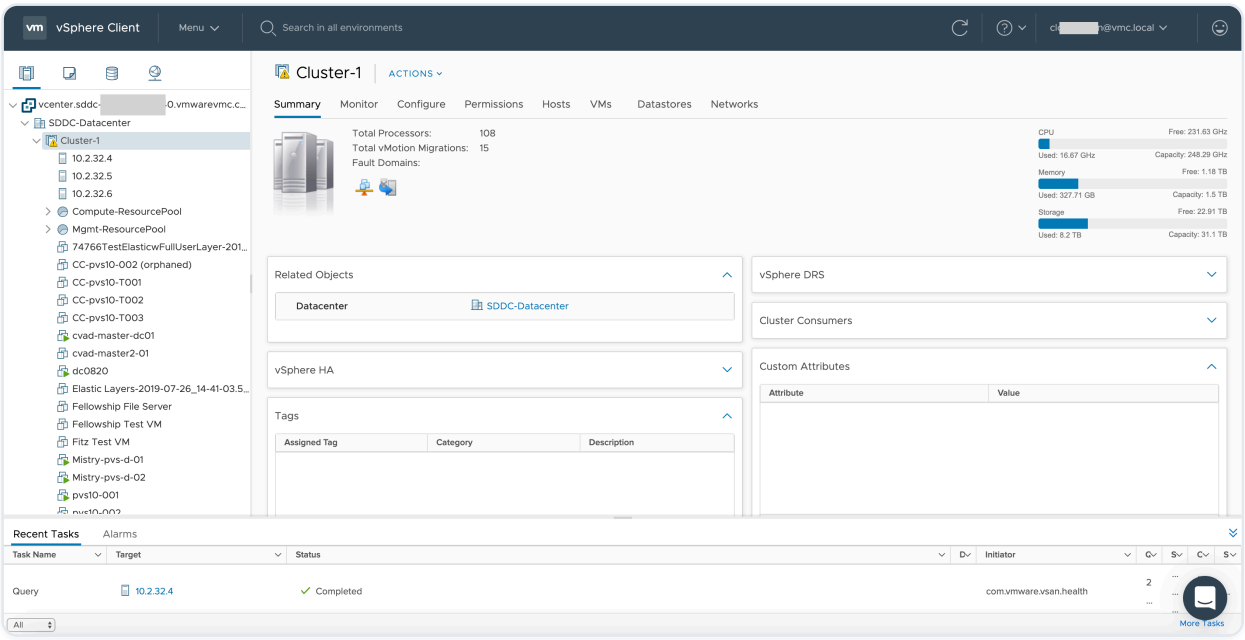


3. 单击**打开 VCENTER**，然后单击**显示凭据**。记下凭据以供以后使用。





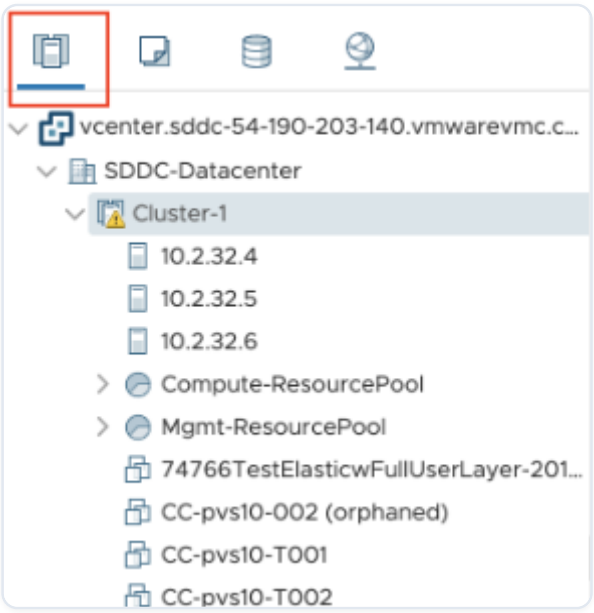
4. 打开 Web 浏览器并输入 vSphere Web Client 的 URL。
5. 输入所记录的凭据，然后单击“**登录**”。vSphere 客户端网页与本地环境类似。



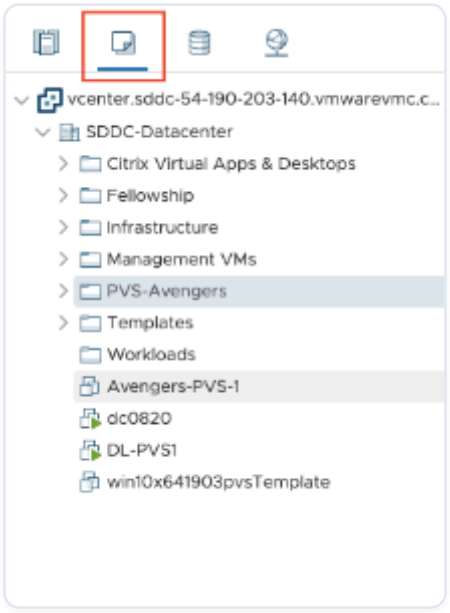
关于 VMWARE 云环境

vSphere 客户端网页上有四种视图。

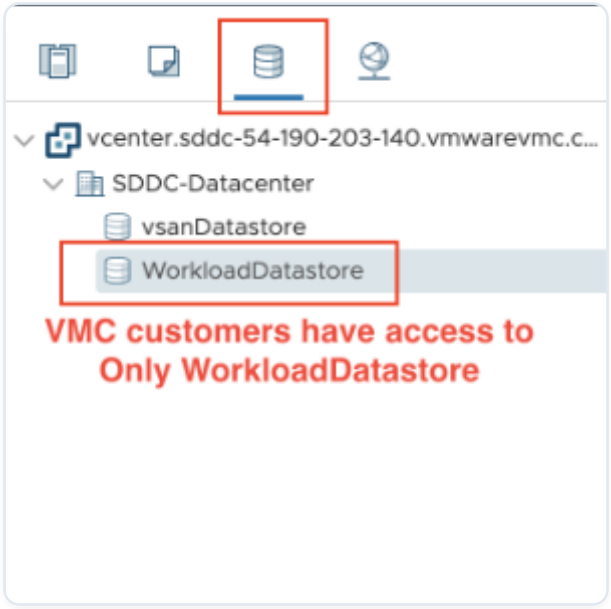
- 主机和群集视图：您无法创建新的群集，但云管理员可以创建多个资源池。



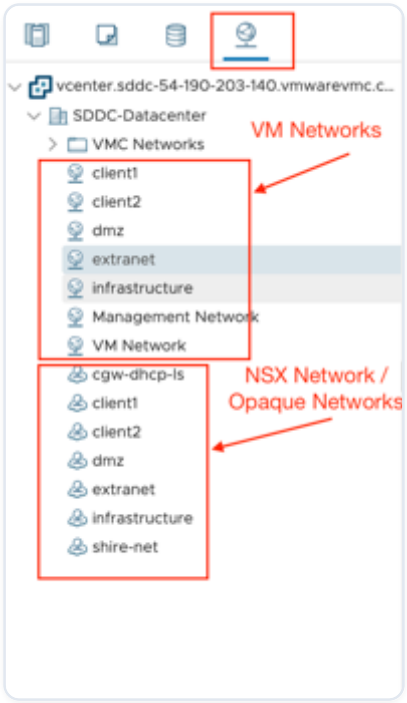
- VM 和模板视图：云管理员可以创建许多文件夹。



- 存储视图：在 Citrix Studio 中添加托管单元时，请选择 **WorkloadDatastore** 存储，因为您只能访问 Workload Datastore。



- 网络视图：VMware 云网络和不透明网络的图标不同。



设置群集后，请参阅 VMware 虚拟化环境 以添加连接和资源。

后续步骤

- 安装核心组件
- 安装 VDA
- 创建站点
- 有关创建和管理连接的信息，请参阅连接到 VMware 云和合作伙伴解决方案

更多信息

- 创建和管理连接与资源
- 创建计算机目录

安装核心组件

> **重要提示：**
>
> - Citrix 会根据其合法权益（包括许可证合规性）收集基本的许可数据。有关详细信息，请参阅 Citrix 许可数据。
> - 确保许可证服务器运行的最低版本为 11.17.2 build 53100。未能满足此必备条件将阻止 Citrix Virtual Apps and Desktops 站点升级和站点创建。

> 核心组件包括 Citrix 交付控制器™、Citrix Studio、Web Studio、Citrix Director 和 Citrix 许可证服务器。

> **注意：**

> Citrix Studio 是一个基于 Windows 的管理控制台，可用于配置和管理本地 Citrix Virtual Apps and Desktops 部署。Web Studio 是 Citrix Studio 的下一代产品，它是一个基于 Web 的管理控制台，提供与 Citrix Studio 相同的所有功能。有关 Web Studio 的详细信息，请参阅 安装 Web Studio。

> （在 2003 之前的版本中，核心组件包括 Citrix StoreFront。您仍然可以通过单击 **Citrix StoreFront** 磁贴或运行安装介质上提供的命令来安装 StoreFront。）

开始安装之前，请查看本文和 准备安装。

本文介绍了安装核心组件时的安装向导顺序。提供了命令行等效项。有关详细信息，请参阅 使用命令行安装。

步骤 1. 下载产品软件并启动向导

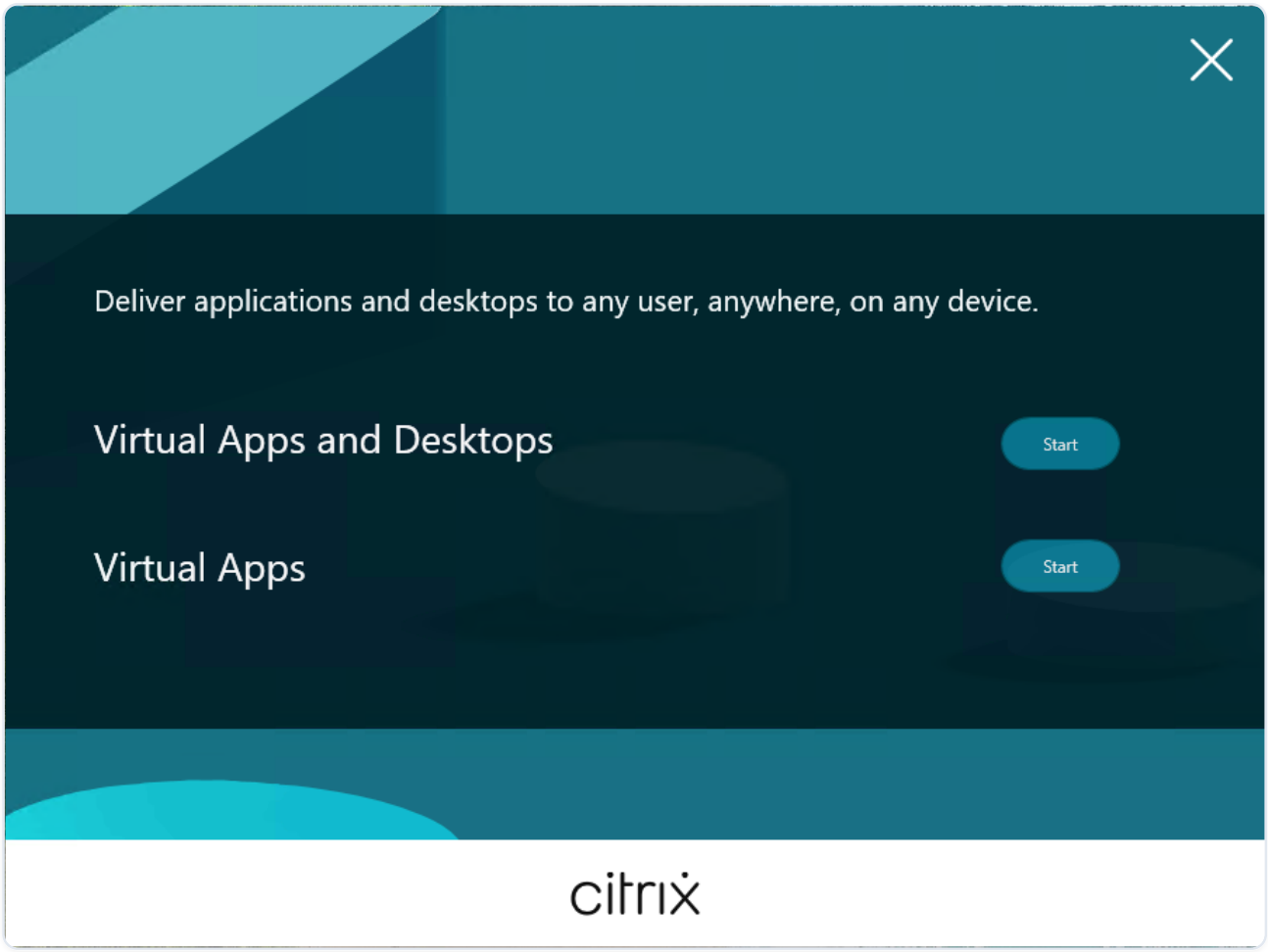
使用您的 Citrix 帐户凭据访问 Citrix Virtual Apps and Desktops™ 下载页面。下载产品 ISO 文件。

解压缩文件。或者，刻录 ISO 文件的 DVD。

使用本地管理员帐户登录到要安装核心组件的计算机。

将 DVD 插入驱动器或装载 ISO 文件。如果安装程序未自动启动，请双击 **AutoSelect** 应用程序或装载的驱动器。

步骤 2. 选择要安装的产品



点击要安装的产品旁边的“**开始**”：Virtual Apps 或 Virtual Apps and Desktops。

（如果计算机上已安装 Citrix Virtual Apps and Desktops™ 组件，则此页面不会出现。）

命令行选项：`/xenapp` 以安装 Citrix Virtual Apps。如果省略该选项，则安装 Citrix Virtual Apps and Desktops。

步骤 3. 选择要安装的内容

组件安装程序中的组件选择页面(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/what-to-install-2.png)

如果您是初次使用，请选择“**Delivery Controller**”。（在后续页面上，您将选择要在此计算机上安装的特定组件。）

如果您已安装 Controller（在此计算机上或另一台计算机上），并且想要安装其他组件，请从“**扩展部署**”部分选择该组件。

命令行选项：`/components`

步骤 4. 阅读并接受许可协议

组件安装程序中的许可协议页面(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/core-license-75.png)

在“**许可协议**”页面上，阅读许可协议后，表明您已阅读并接受该协议。然后单击“**下一步**”。

步骤 5. 选择要安装的组件和安装位置

组件安装程序中的核心组件页面(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/core-components-75.png)

在“**核心组件**”页面上：

- **位置**：默认情况下，组件安装在 `C:\Program Files\Citrix` 中。对于大多数部署，默认设置即可。如果指定其他位置，则该位置必须对网络服务具有执行权限。
- **组件**：默认情况下，所有核心组件的复选框均处于选中状态。将所有核心组件安装在一台服务器上适用于概念验证、测试或小型生产部署。对于大型生产环境，Citrix 建议将 Director、StoreFront、Secure Private Access 和许可证服务器安装在单独的服务器上。

> **注意：**
>
> 如果您要在多台服务器上安装组件，请先安装 Citrix 许可证服务器和许可证，然后再在其他服务器上安装其他组件。有关指导，请参阅 Citrix Virtual Apps and Desktops 许可指南的“自动安装”部分。

> 当您选择不在本机上安装所需的某个核心组件时，会出现一个图标提醒您。该提醒会提示您安装该组件，但并非必须在本机上安装。

单击**下一步**。

命令行选项：`/installdir`、`/components`、`/exclude`

硬件检查

安装或升级 Delivery Controller 时，会检查硬件。如果计算机的 RAM 小于建议量 (5 GB)，安装程序会发出警报，这可能会影响站点的稳定性。有关详细信息，请参阅 硬件要求。

图形界面：将出现一个对话框。

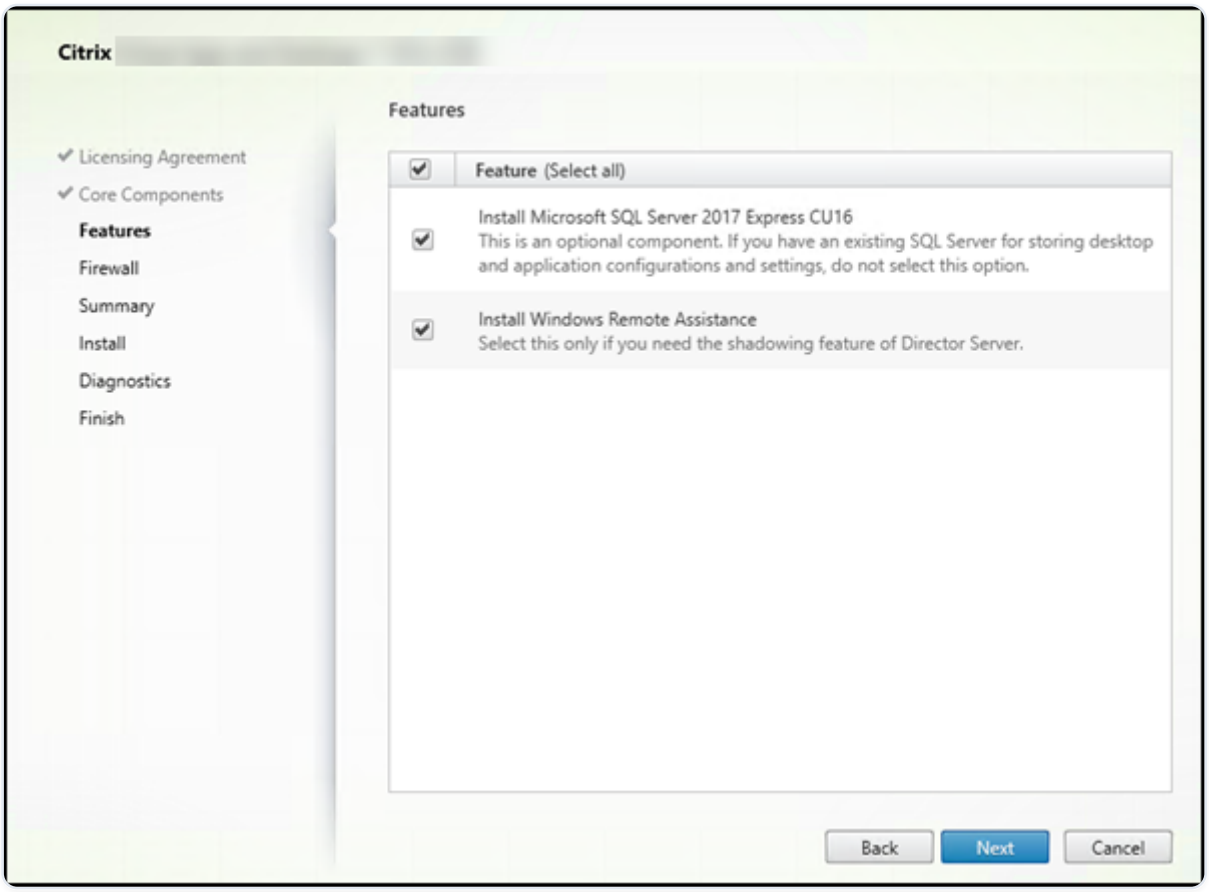
- 建议：单击“**取消**”以停止安装。向计算机添加更多 RAM，然后再次开始安装。
- 或者，单击“**下一步**”以继续安装。站点可能会出现稳定性问题。

命令行界面： 安装/升级结束。安装日志包含一条消息，描述了发现的问题和可用选项。

- 建议：向计算机添加更多 RAM，然后再次运行该命令。
- 或者，使用 `/ignore_hw_check_failure` 选项再次运行该命令以覆盖警告。您的站点可能会出现稳定性问题。

升级时，如果操作系统或 SQL Server 版本不再受支持，您也会收到通知。请参阅 升级和迁移。

步骤 6. 启用或禁用功能



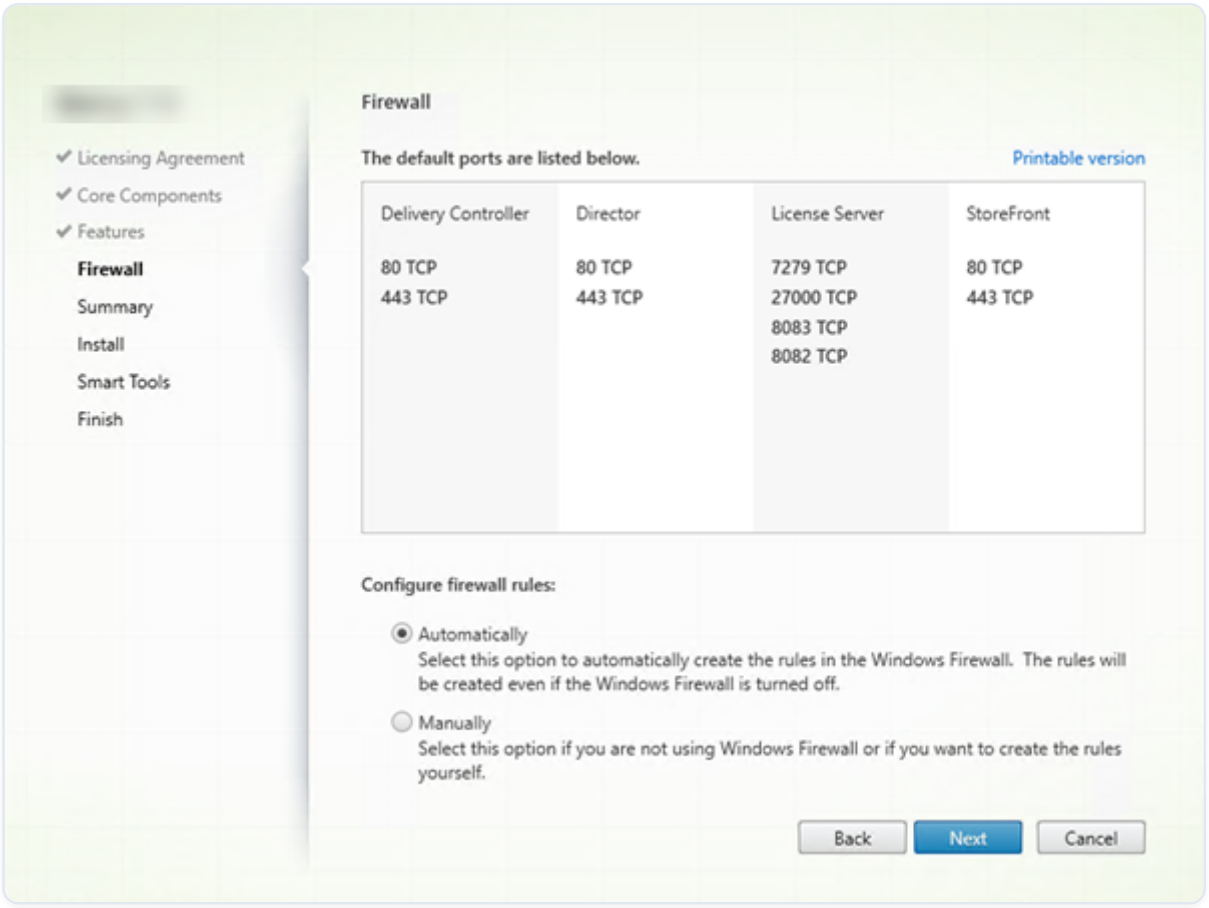
在“**功能**”页面上：

- 选择是否安装 Microsoft SQL Server Express 作为站点数据库。默认情况下，此选项处于启用状态。如果您不熟悉 Citrix Virtual Apps and Desktops 数据库，请查看数据库。
- 安装 Director 时，Windows 远程协助会自动安装。您可以选择是否在 Windows 远程协助中启用影子功能，以用于 Director 用户影子。启用影子功能会打开 TCP 端口 3389。默认情况下，此功能处于启用状态。默认设置适用于大多数部署。此功能仅在安装 Director 时显示。

单击“**下一步**”。

命令行选项：`/nosql`（阻止安装），`/no_remote_assistance`（阻止启用）

步骤 7. 打开 Windows 防火墙端口



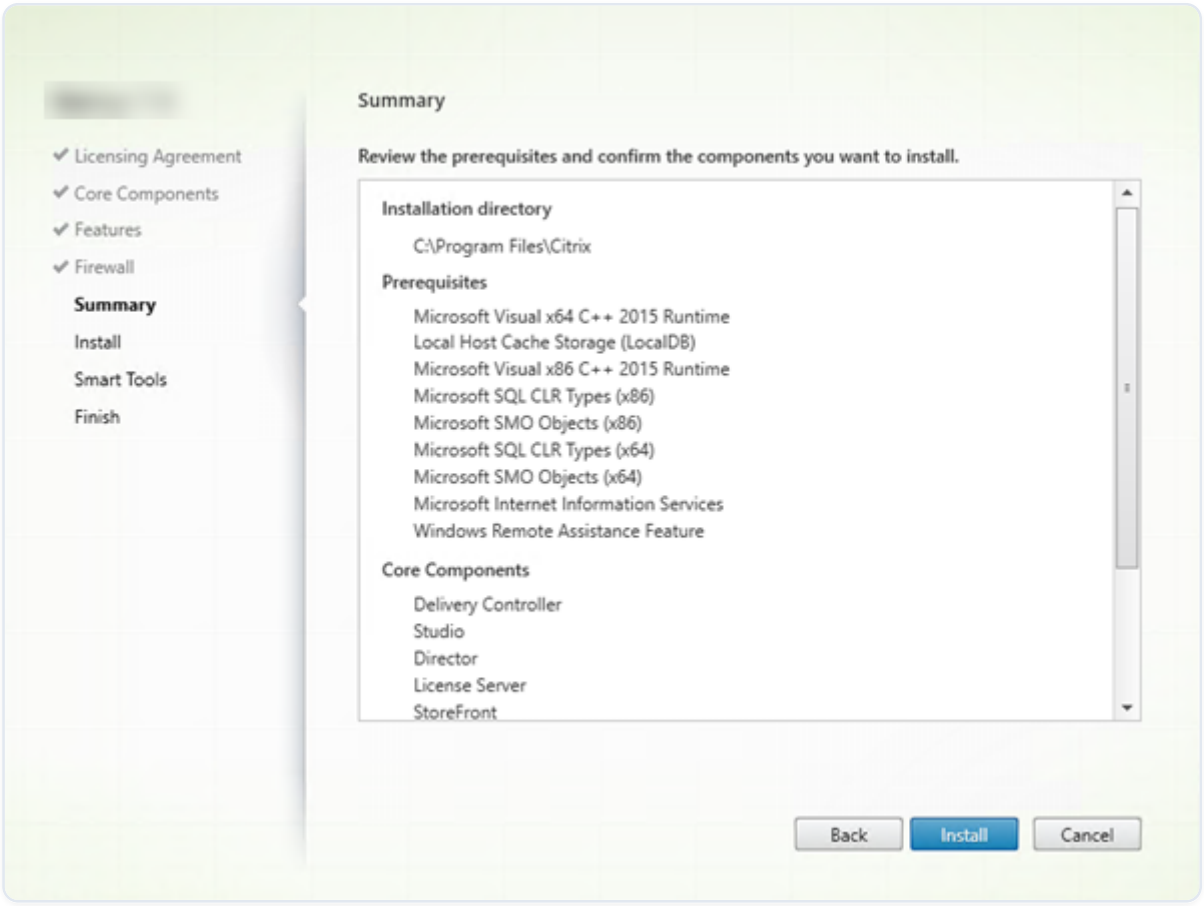
默认情况下，如果 Windows 防火墙服务正在运行，即使防火墙未启用，**防火墙**页面上的端口也会自动打开。默认设置适用于大多数部署。有关端口信息，请参阅网络端口。

单击“**下一步**”。

（该图显示了在此计算机上安装所有核心组件时的端口列表。此类安装通常仅用于测试部署。）

命令行选项：`/configure_firewall`

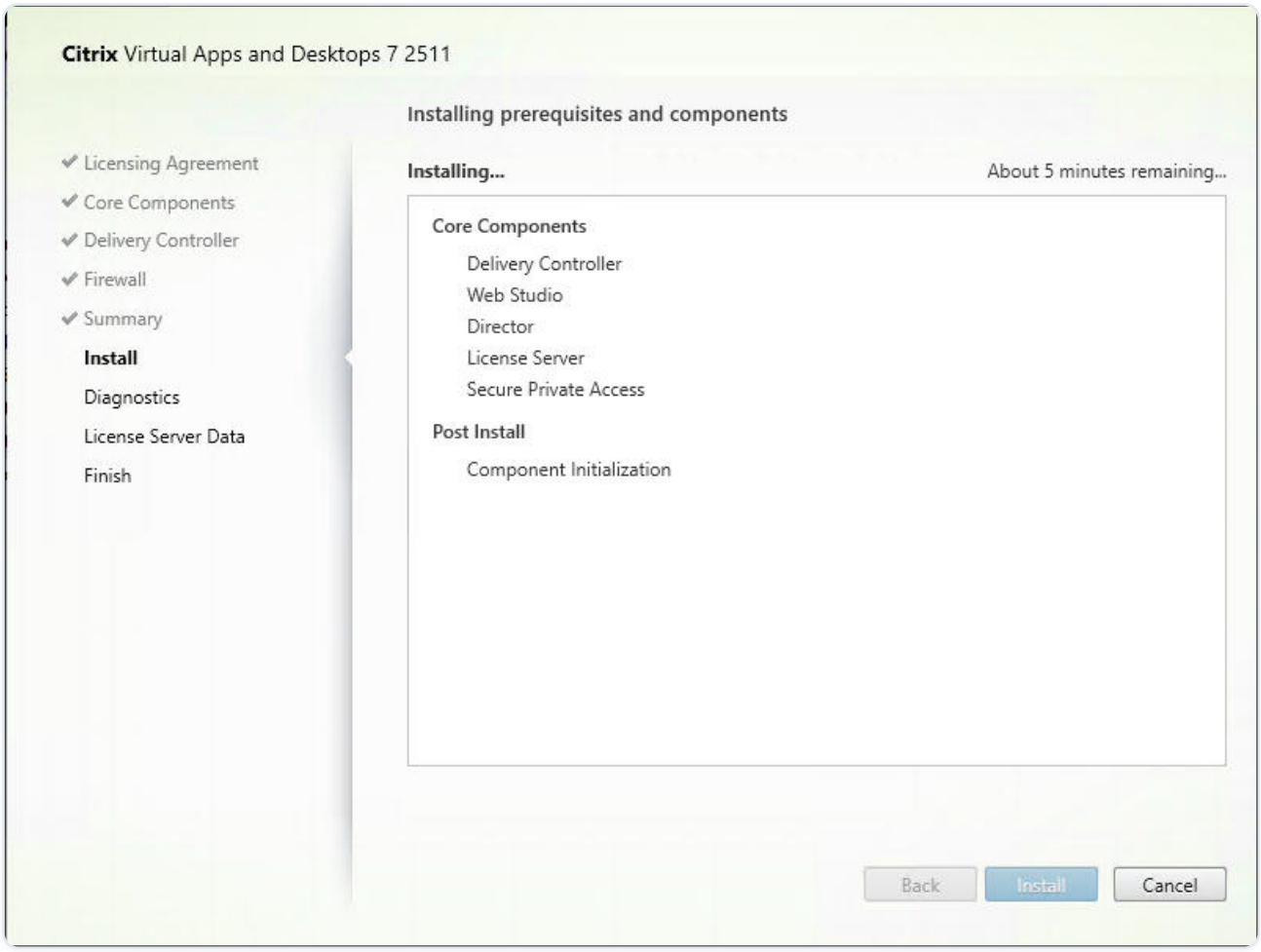
步骤 8. 查看必备条件并确认安装



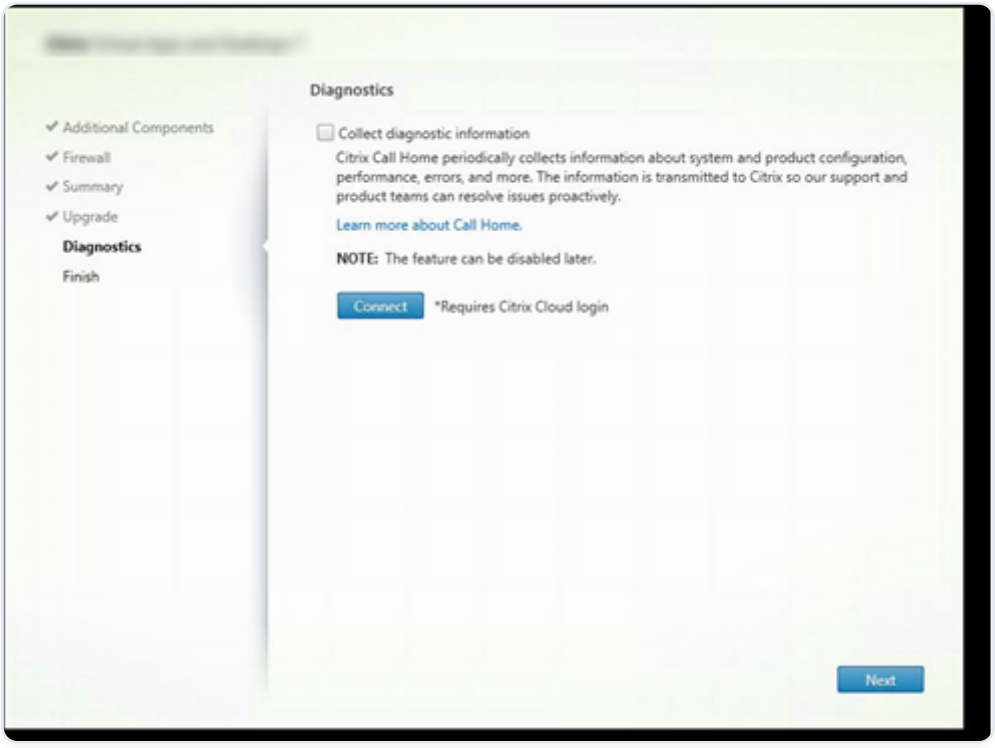
摘要页面列出了将要安装的内容。使用“**返回**”按钮返回到之前的向导页面并根据需要更改选择。

准备就绪后，单击“**安装**”。

显示屏显示安装进度：



步骤 9. 与 Cloud Software Group 共享诊断信息



在**诊断**页面上，选择是否参与 Citrix Call Home。

使用图形界面安装 Delivery Controller 时，将显示此页面。安装 StoreFront（但不是 Controller）时，向导会显示此页面。安装其他核心组件（但不是 Controller 或 StoreFront）时，向导不会显示此页面。

在升级过程中，如果 Call Home 已启用或者安装程序遇到与 Citrix Telemetry Service 相关的错误，则不会显示此页面。

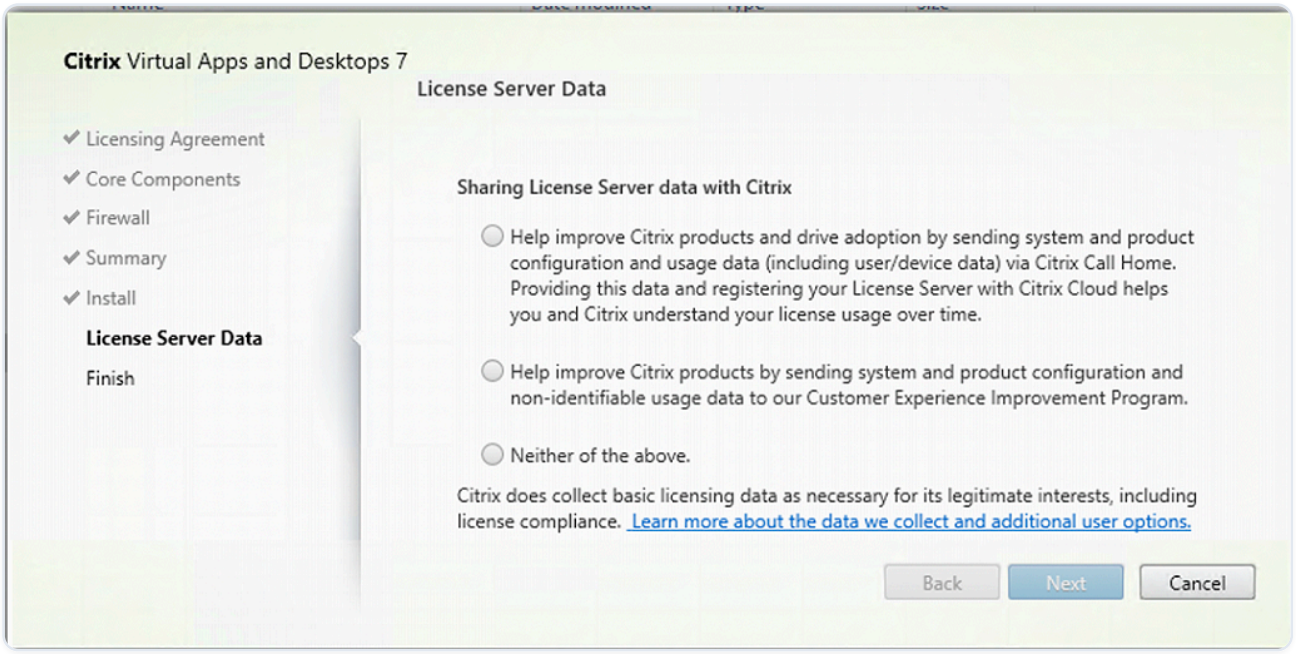
如果您选择参与（默认），请单击**连接**。出现提示时，输入您的 Citrix 帐户凭据。您可以在安装后更改您的注册选择。

凭据验证后（或者如果您选择不参与），单击**下一步**。

如果您在**诊断**页面上单击**连接**而未首先选择**收集诊断信息**，则在关闭**连接到 Citrix Insight Services** 对话框后，**下一步**按钮将禁用。您无法移动到下一页。要重新启用**下一步**按钮，请选择并立即取消选择**收集诊断信息**。

有关详细信息，请参阅 Call Home。

步骤 10. 与 Cloud Software Group 共享许可证服务器数据



在**许可证服务器数据**页面上，我们请求您共享 Call Home 数据或客户体验改善计划 (CEIP) 数据以协助我们。此外，Cloud Software Group 还要求收集基本的许可数据，包括许可证合规性，以满足其合法利益。

安装许可证服务器时，将显示**许可证服务器数据**页面：

- 作为独立组件。
- 作为核心组件，在安装 Delivery Controller 期间。

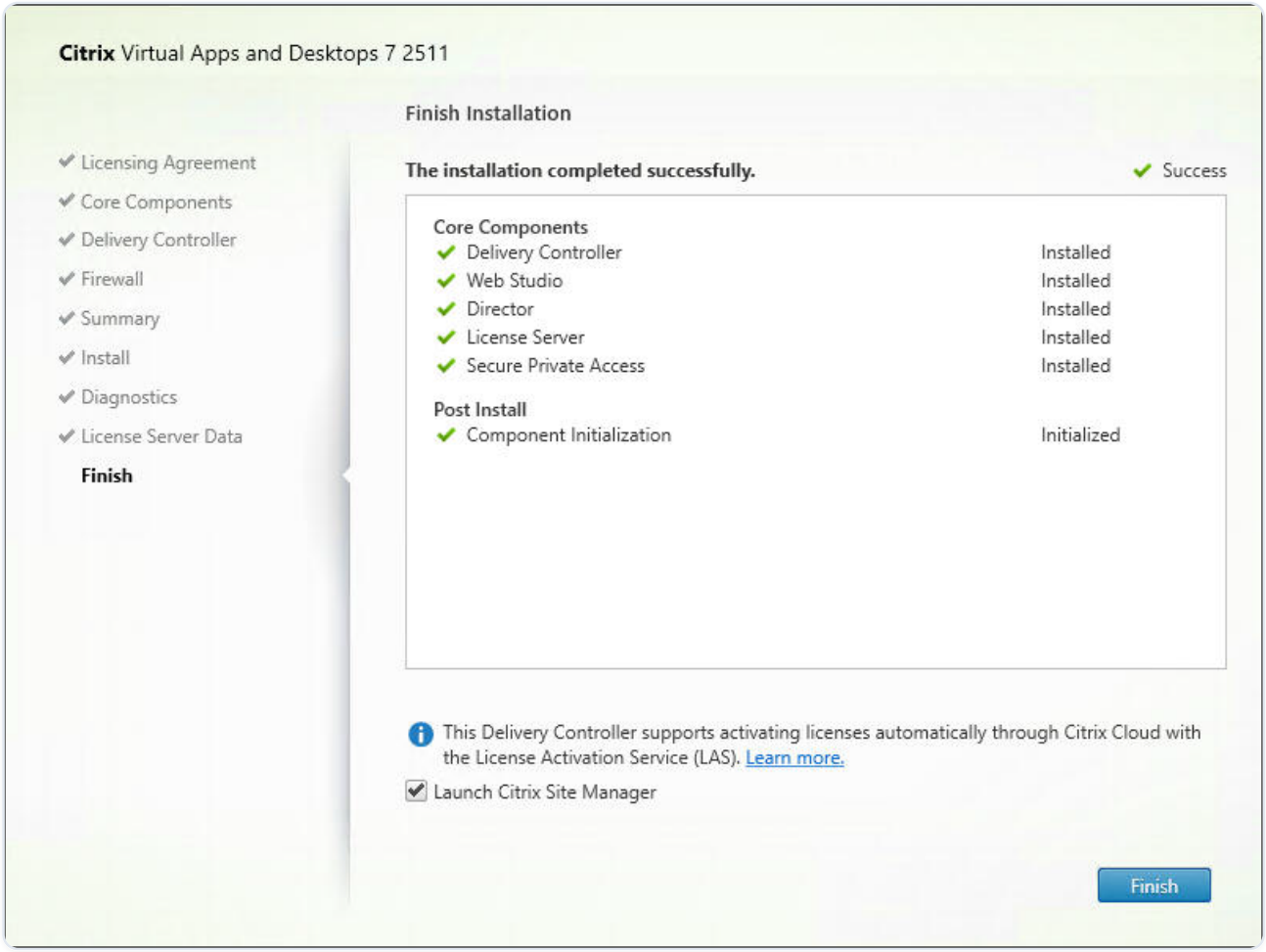
在升级期间，如果配置已在 `/CITRIX.opt:` 文件中设置，则此页面不会出现。

许可证服务器监控多种类型的用户数据，例如许可数据、Call Home 数据和 CEIP 数据。要启用 Call Home 数据和 CEIP 数据收集，您必须选择参与（选择加入）。

有关如何在使用命令行安装时启用 Call Home 和 CEIP 数据收集的更多信息，请参阅用于安装核心组件的命令行选项。

有关 Cloud Software Group 许可数据收集的更多信息，请参阅Citrix 许可数据收集程序。

步骤 11. 完成此安装



完成页面包含所有已成功安装和初始化的必备项和组件的绿色复选标记。

单击“**完成**”。

> **注意：**
>
> 当您升级到版本 2511 时，安装程序会自动卸载 Citrix Studio（基于 MMC）。您的配置数据存储在数据库中，不受自动卸载的影响。

步骤 12. 在其他计算机上安装剩余的核心组件

如果您已在一台计算机上安装了所有核心组件，请继续执行后续步骤。否则，请在其他计算机上运行安装程序以安装其他组件。您还可以在其他服务器上安装更多 Controller。

后续步骤

安装所有必需组件后，使用 Web Studio 创建站点。

创建站点后，安装 VDA。

您可以随时使用完整产品安装程序通过以下组件扩展部署：

- **Universal Print Server 服务器组件：** 在您的打印服务器上启动安装程序。

  a. 在**扩展部署**部分中选择 **Universal Print Server**。

  b. 接受许可协议。

  c. 在**防火墙**页面上，默认情况下，如果 Windows 防火墙服务正在运行，即使防火墙未启用，也会在防火墙中打开 TCP 端口 7229 和 8080。如果您想手动打开端口，可以禁用此默认操作。

  要从命令行安装此组件，请参阅用于安装通用打印服务器的命令行选项。

- 联合身份验证服务。
- 会话记录。
- 工作区环境管理。
- 安装 uberAgent
- 安装 deviceTRUST 代理
- WEM 快速入门指南

安装 Web Studio

> **注意：**
>
> Citrix Studio (MMC Studio) 已从版本 2511 开始移除，不再受支持。本文假设 Web Studio 是唯一正在使用的管理控制台。

简介

Web Studio 是一个基于 Web 的管理控制台，提供与 Citrix Studio 相同的功能。Web Studio 具有与 Citrix DaaS Studio 界面 相同的外观和体验，通过提供原生 Web 体验来现代化您的管理体验。

您可以将 Web Studio 部署到安装了 Internet Information Service (IIS) 的任何 Windows 服务器。有两种部署选项：

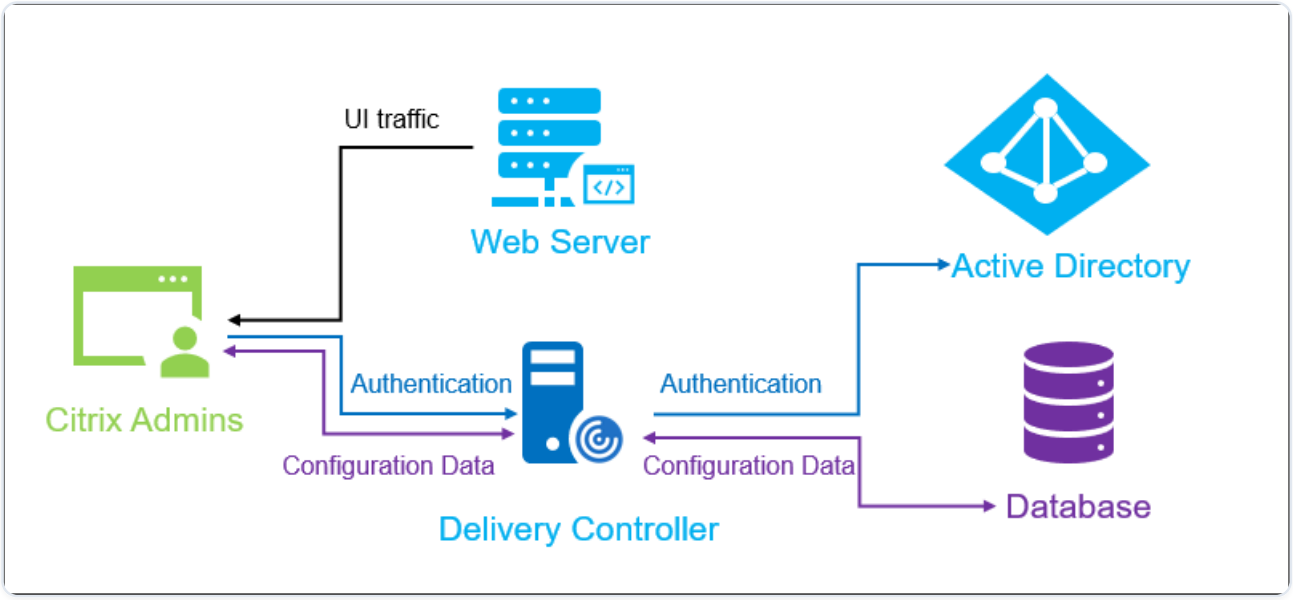
- 安装在专用服务器上：

  对于性能和可扩展性至关重要的大型环境，我们建议将 Web Studio 安装在专用服务器上。此服务器也可以选择托管 Director。

- 与交付控制器™集成：

  对于快速部署和更简单的环境，请将 Web Studio 直接安装在 Delivery Controller 上。此方法非常适合将最小化管理开销作为优先事项的小型部署。

下图显示了 Web Studio 体系结构：



启动并运行 Web Studio 的一般工作流程如下：

1. 安装 Web Studio。
2. 设置站点。
3. 将 Delivery Controller 添加到 Web Studio 进行管理。
4. (可选) 将 Web Studio 配置为 Delivery Controller 的代理
5. (可选) 禁用 Pendo。
6. Web Studio 的安全服务器配置
7. 登录 Web Studio。

要设置负载均衡的 Web Studio 部署，请参阅 本文。

Web Studio 中的新增功能

请参阅 新增功能 文章。

系统要求

下表列出了安装和使用 Studio 所支持的操作系统、浏览器、显示设置和硬件要求。

支持的操作系统

操作系统	版本	SERVER CORE 支持
Windows 服务器 2025	标准版，数据中心版	是
Windows 服务器 2022	标准版，数据中心版	是
Windows 服务器 2019	标准版，数据中心版	是
Windows 服务器 2016	标准版，数据中心版	是

支持的浏览器

浏览器	最低支持版本
微软 Edge	92
Firefox ESR（延长支持版本）	90
谷歌浏览器	92
Safari 浏览器	14

显示要求

要求	值
推荐屏幕分辨率	1440 × 1024

硬件要求

资源	最低要求
内存	1 GB RAM

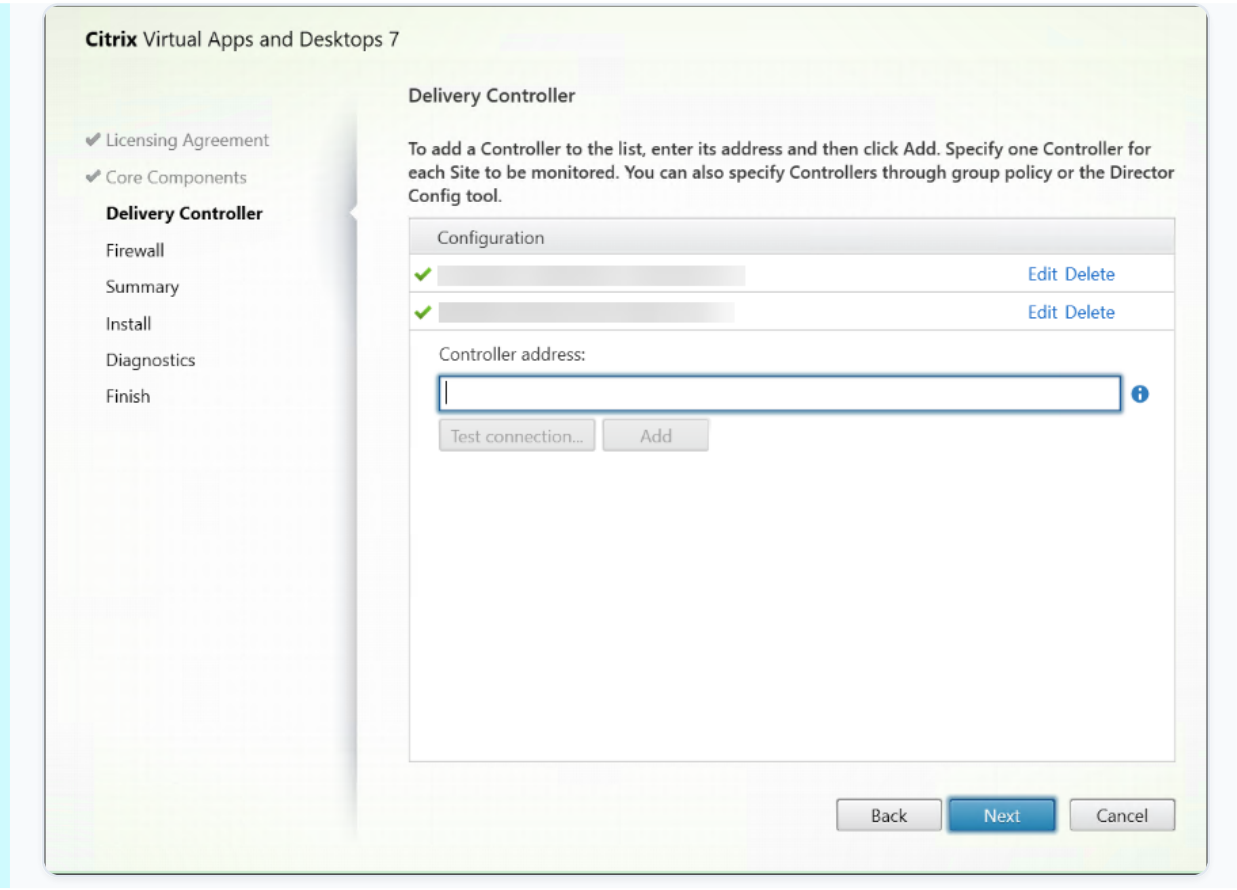
资源	最低要求
磁盘空间	100 MB

安装 Web Studio

以下信息是对 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-core-components.html) 中 指南的补充。要安装 Web Studio：

- 使用 Citrix Virtual Apps and Desktops™ 的完整产品 ISO 安装程序安装 Web Studio。ISO 安装程序会检查先决条件，安装任何缺失的组件，设置 Web Studio 网站（如果包含在 Delivery Controller 安装中，则在 Delivery Controller 上），并执行基本配置。
- 如果安装期间未包含 Web Studio，请使用安装程序添加 Web Studio。
- 安装 Web Studio 时，系统会提示您键入 Delivery Controller 的 FQDN。

> **注意：**
>
> - 我们建议在同一版本上运行 Web Studio 和 Delivery Controller，以确保完整功能。
> - 您可以添加多个 Delivery Controller。Web Studio 会尝试以随机顺序连接它们。如果 Web Studio 尝试连接的 Delivery Controller 不可达，Web Studio 会自动回退到其他 Delivery Controller。
> - 如果在**核心组件**中选择了 Director 并已安装，则您在此处添加的 Delivery Controller 将同时用于 Web Studio 和 Director。
> - 如果 Delivery Controller 配置为 TLS（推荐），则输入的 FQDN 必须与安装在 Delivery Controller 上的证书的通用名称或主题备用名称匹配。
> - Web Studio 可以安装在任何 **Site ID = 1** 的 IIS 网站上，无论网站名称如何。此功能使您可以在自定义 IIS 站点而不是**默认网站**下托管 Web Studio。
>   - 如果在运行 ISO 安装程序之前未安装 IIS，安装程序会自动配置 IIS 并在**默认网站**（Site ID = 1）下部署 Web Studio。安装后，可以根据需要重命名网站名称。
>   - 如果 IIS 已安装，您可以提前创建一个具有您首选名称和物理路径的 IIS 站点，只要其 **Site ID** 为 **1** 即可。然后 Web Studio 将直接安装在该站点下，无需进一步配置。



- 在**完成**页面上，查看已安装的组件，然后单击**完成**。

  启动站点管理器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/launch-site-manager.png)

> **注意：**
>
> 您还可以使用命令行安装 Web Studio。示例：`.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local" /configure_firewall /quiet`。有关更多信息，请参阅使用命令行安装。

配置 TLS 证书

默认情况下，如果 IIS 尚未配置 HTTPS，安装程序会使用服务器的 FQDN 作为证书的公用名创建自签名证书，并将其绑定到端口 443。此行为允许用户从本地计算机访问 Web Studio，但从其他计算机连接的用户会看到安全警告，因为该证书不受信任。我们建议将此证书替换为由企业或公共证书颁发机构 (CA) 签名的证书。有关详细信息，请参阅 在 Web Studio 和 Director 上启用 TLS。如果 IIS 中已配置 TLS 证书，则安装程序不会进行任何更改。

> **注意：**

> 要详细了解如何保护 Web Studio 部署，请参阅 保护 Web Studio 部署。

设置站点

要设置 Citrix Virtual Apps and Desktops 部署（也称为站点），请使用 Citrix Site Manager 工具。该工具随 Delivery Controller 自动安装。

要设置站点，请执行以下步骤：

1. 在 Delivery Controller 上，打开桌面“开始”菜单，然后选择 **Citrix > Citrix Site Manager**。
2. 在 Citrix Site Manager 中，选择 **Create a site**。将显示“站点设置”向导。
3. 创建站点并按如下方式配置其设置：
   - 在“**简介**”页面上，键入站点的名称。
   - “**数据库**”页面包含用于设置站点、监视和配置日志记录数据库的选项。有关详细信息，请参阅 步骤 3. 数据库。
   - 在“**许可**”页面上，指定许可证服务器地址，然后指明要使用（安装）哪个许可证。有关详细信息，请参阅 步骤 4. 许可。
4. 在“**摘要**”页面上，检查所有设置，然后单击“**提交**”。

   此 Controller 的 IP 地址会自动添加到站点。

> **注意：**
>
> 创建站点的用户将成为该站点的完全管理员。有关详细信息，请参阅 委派管理。

如果在创建站点后安装新的 Controller，则必须将该 Controller 添加到站点。详细步骤如下：

1. 在此新控制器上运行 Citrix Site Manager。
2. 选择 **加入现有站点**。
3. 键入已添加到站点的控制器的地址。
4. 单击 **提交**。

将 Delivery Controller 添加到 Web Studio 进行管理

使用 Studio 配置工具将 Delivery Controller 添加到 Web Studio 进行管理。此工具位于 Web Studio 安装文件夹中。

默认情况下，该工具安装在以下默认文件夹中。

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

假设您要为要使用 Web Studio 管理的站点配置以下两个 Delivery Controller：`ddc1.studio.local` 和 `ddc2.studio.local`。运行以下 PowerShell 命令：

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

注意：

- 该工具需要计算机管理员权限。
- 由于 IIS 服务器上的缓存设置，Delivery Controller 配置更改可能不会立即生效。要立即生效，请转到 Web Studio 服务器，打开 Internet Information Services (IIS) Manager，导航到 *Server_name* > **站点** > *安装 Web Studio 的 IIS 站点名称（站点 ID = 1）*，然后在“管理网站”窗格中选择 **重新启动**。
- 当您使用新 FQDN 重新部署 Delivery Controller 时，请使用 `StudioConfig.exe` 和 `C:\Program Files\Citrix\Web Studio\Site\assets\json\manifest.json` 文件更新其在 Web Studio 中的 FQDN。如果您不更新 `manifest.json` 文件，旧 FQDN 仍会显示在 Web Studio 登录窗口中。因此，您必须在登录时输入新的 FQDN 作为替代。
- 要查看所有支持的参数，请运行 `StudioConfig.exe --help`。

（可选）将 Web Studio 配置为 Delivery Controller 的代理

默认情况下，当您使用 Web Studio 控制台管理部署时，您通过 Web 浏览器连接到 Web Studio 服务器和 Delivery Controller。我们为您提供了一个选项，可将 Web Studio 服务器配置为 Delivery Controller 的代理。因此，在管理部署时，您只需连接到 Web Studio 服务器。

本节指导您将 Web Studio 服务器配置为 Delivery Controller 的代理。我们假设 Web Studio 和 Delivery Controller 安装在不同的服务器上。

在开始之前，请验证您的部署中是否已安装所有必需的核心组件。有关详细信息，请参阅安装核心组件。

要为 Web Studio 启用代理模式，请执行以下步骤：

1. 在 Web Studio 服务器上，以管理员身份运行 Windows PowerShell。
2. 运行以下命令，其中将 `fqdn_of_webstudio_machine` 替换为 Web Studio 服务器的 FQDN。

`& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enableproxy --proxyserver "fqdn_of_webstudio_machine"`

> **注意：**
>
> 如果您有负载平衡的 Web Studio 部署，请将 `fqdn_of_webstudio_machine` 替换为负载平衡器服务器（也称为虚拟服务器）的 FQDN。有关详细信息，请参阅设置负载平衡的 Web Studio 部署。

要为 Web Studio 禁用代理模式，请运行此 PowerShell 命令：

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy
```

（可选）启用或禁用 Pendo

从版本 2411 开始，Web Studio 集成了 Pendo，默认情况下已启用。Pendo 按照Citrix 隐私策略 收集您的使用数据。它还在 Web Studio 的右下角添加了一个图标，为您提供上下文功能信息和反馈选项。如果您不想共享使用数据，可以使用 Studio 配置工具禁用 Pendo。

此工具位于 Web Studio 安装文件夹中。默认情况下，该工具安装在以下文件夹中：`C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`。

要禁用 Pendo，请执行以下步骤：

1. 登录 Web Studio。如果右下角出现图标，则表示 Pendo 已启用。
2. 在 Web Studio 服务器上，以管理员身份运行 Windows PowerShell。 运行此 PowerShell 命令：

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disablependo
```

要启用 Pendo，请运行此命令：

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enablependo
```

Web Studio 的安全服务器配置

将以下安全配置应用于托管 Web Studio 的服务器，以提高安全性。这些设置在服务器级别应用，而不是在 Web Studio 本身中应用。

禁用中等强度 SSL 密码 (SWEET32)

Web Studio 服务器可能使用中等强度密码 `TLS_RSA_WITH_3DES_EDE_CBC_SHA`，该密码容易受到 SWEET32 攻击。 要禁用该密码，请在 Web Studio 服务器上运行以下 PowerShell 命令：

```
Disable-TlsCipherSuite -Name TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

禁用已弃用的 TLS 1.0 和 1.1 协议

TLS 1.0 和 TLS 1.1 已弃用，不应在 Web Studio 服务器上启用。 要禁用它们：

1. 打开注册表编辑器 (`regedit.exe`)。
2. 转到 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocol`。
3. 如果以下子项不存在，请创建它们：
   - `TLS 1.0\Client`
   - `TLS 1.0\Server`
   - `TLS 1.1\Client`
   - `TLS 1.1\Server`
4. 在每个 `Client` 和 `Server` 键中，创建以下 `DWORD (32-bit)` 值：
   - `Enabled` = `0`
   - `DisabledByDefault` = `1`（可选但建议）
5. 重新启动服务器以应用更改。

登录 Web Studio

1. 如果使用默认端口号 443，请在 `https://<address of the server hosting Web Studio>/Citrix/Studio` 访问 Web Studio。如果配置了不同的端口，请使用 `https://<address of the server hosting Web Studio>:<port number>/Citrix/Studio`。

   如果您已将 Delivery Controller 添加到 Web Studio 并且它们可访问，则会出现登录页面。

   > **注意：**

> 在以下情况下，将显示**无法登录**页面：
>
> - 尚未为站点指定任何 Delivery Controller。系统会提示您添加一个以进行连接。
> - 指定的 Delivery Controller 不可达。单击 **测试** 以检查连接。或者，输入备用 Delivery Controller，然后单击 **连接**。

2. 输入 **用户名**、**密码** 和 **域**。
3. 单击 **登录**。

后续步骤

1. 安装 VDA
2. 使用 Web Studio 向用户交付虚拟应用程序和桌面，方法是：
   a. 创建计算机目录
   b. 创建交付组
   c. 创建应用程序组（可选）

保护 Web Studio 部署

本文重点介绍在部署 Web Studio 时可能影响系统安全性的配置区域。

> **注意：**
>
> 为了保护用户 Web 浏览器与 Web Studio 之间的通信安全，请参阅在 Web Studio 和 Director 上启用 TLS。

配置 IIS 设置

作为安全最佳实践，请使用受限的 IIS 配置来配置 Web Studio：

1. 限制请求筛选：
   - 如果您将 Web Studio 与 Director 一起安装，IIS 会自动配置以下筛选规则。
   - 如果您将 Web Studio 作为独立组件安装，请手动配置 IIS，如下所示：
     - 仅允许以下文件扩展名：

       `.`, `.aspx`, `.css`, `.eot`, `.html`, `.ico`, `.js`, `.png`, `.svc`, `.svg`, `.jpg`, `.gif`, `.j`

有关详细信息，请参阅这篇 Microsoft 文章。

- 仅允许以下 HTTP 谓词：

  `GET`, `POST`, `HEAD`

  有关详细信息，请参阅这篇 Microsoft 文章。

2. 删除不需要的处理程序映射。

   Web Studio 只需要 `StaticFile` 处理程序映射。删除所有其他映射。有关详细信息，请参阅这篇 Microsoft 文章。

3. 删除未使用的 ISAPI 筛选器。

   Web Studio 不需要任何 ISAPI 筛选器。您可以删除所有筛选器。有关详细信息，请参阅 这篇 Microsoft 文章。

   > **注意：**
   >
   > ASP.NET 需要 ISAPI Windows 功能。

4. 从 `C:\inetpub\wwwroot` 中删除以下默认 IIS 登录页面文件：

   - `iisstart.htm`
   - `welcome.png`

5. 确保 **.NET 信任级别** 保持设置为 **完全信任**。此设置在安装过程中自动配置，是 Web Studio 正常运行所必需的。请勿更改此设置。

删除未使用的应用程序池权限

在安装过程中，Web Studio 应用程序池被授予以下用户权限：

- **作为服务登录**
- **调整进程的内存配额**
- **生成安全审核**
- **替换进程级别令牌**

这些权限是 IIS 应用程序池的标准权限。Web Studio 不使用它们，您可以将其删除。

隔离 WEB STUDIO 部署

您可以在与 Web Studio 相同的 Web 域（域名和端口）中部署任何 Web 应用程序。但是，这些 Web 应用程序中的任何安全风险都可能降低 Web Studio 部署的安全性。如果需要更高程度的安全隔离，我们建议您将 Web Studio 部署在与任何其他*第三方*应用程序不同的 Web 域中。

为 Web Studio 设置智能卡身份验证

本文概述了为 Web Studio 设置和启用智能卡身份验证所需的步骤：

步骤 1：安装智能卡驱动程序

步骤 2：为智能卡用户颁发证书

步骤 3：为智能卡用户注册证书

步骤 4：配置 Web Studio IIS 服务器

步骤 5（可选）：为 Web Studio 配置身份验证委派

步骤 6：为 Web Studio 启用智能卡身份验证

> **注意：**

> 智能卡身份验证仅支持与 Web Studio 服务器位于同一 Active Directory 域中的用户。

步骤 1：安装智能卡驱动程序

在以下计算机上安装智能卡驱动程序：

- 安装了证书服务的域控制器。
- Web Studio 服务器
- 最终用户用于访问 Web Studio 的计算机
- 用于为智能卡用户注册证书的计算机

智能卡驱动程序因供应商而异。例如，如果使用 ITS 提供的智能卡硬件，请从 `<https://support.globalsign.com/ssl/ssl-certificates-installation/safenet-drivers>` 下载 SaftNet 驱动程序。

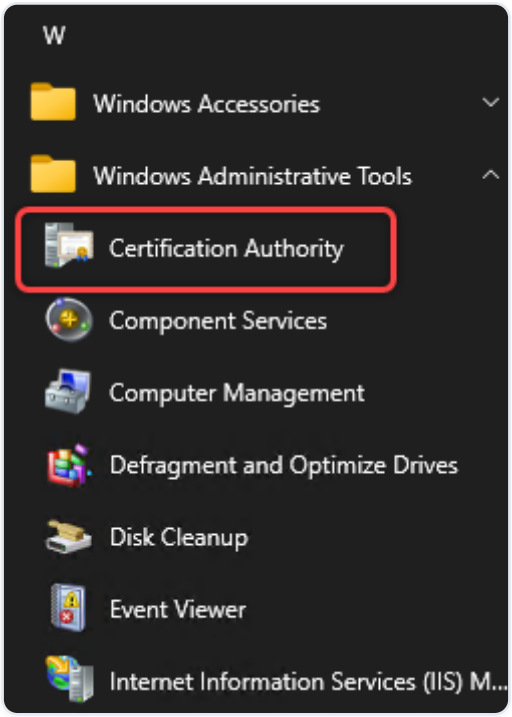
步骤 2：为智能卡用户颁发证书

> **注意：**

> 以下步骤作为示例提供，以指导您完成此过程。

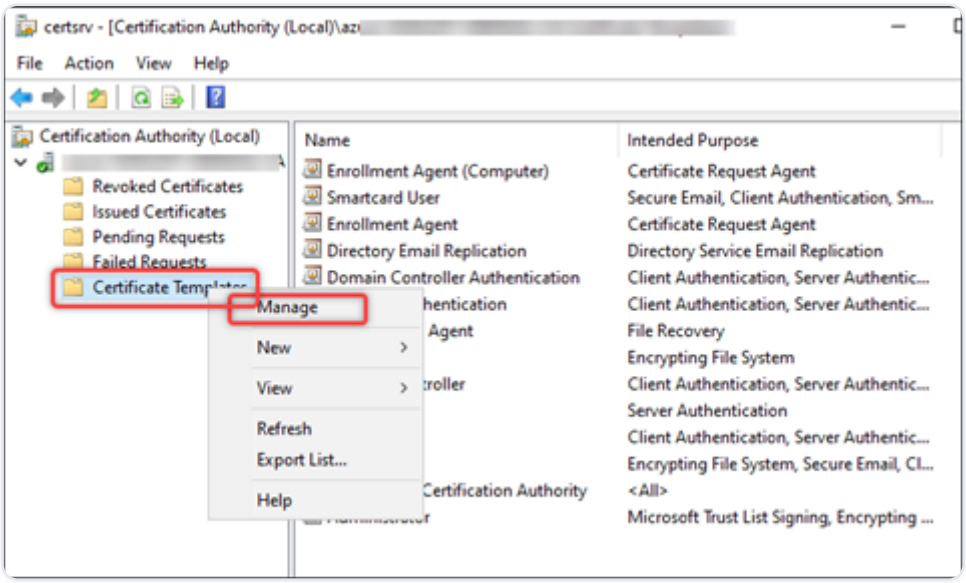
> 在您的域控制器上，请按照以下步骤完成任务：

1. 访问您的域控制器并打开“**证书颁发机构**”。



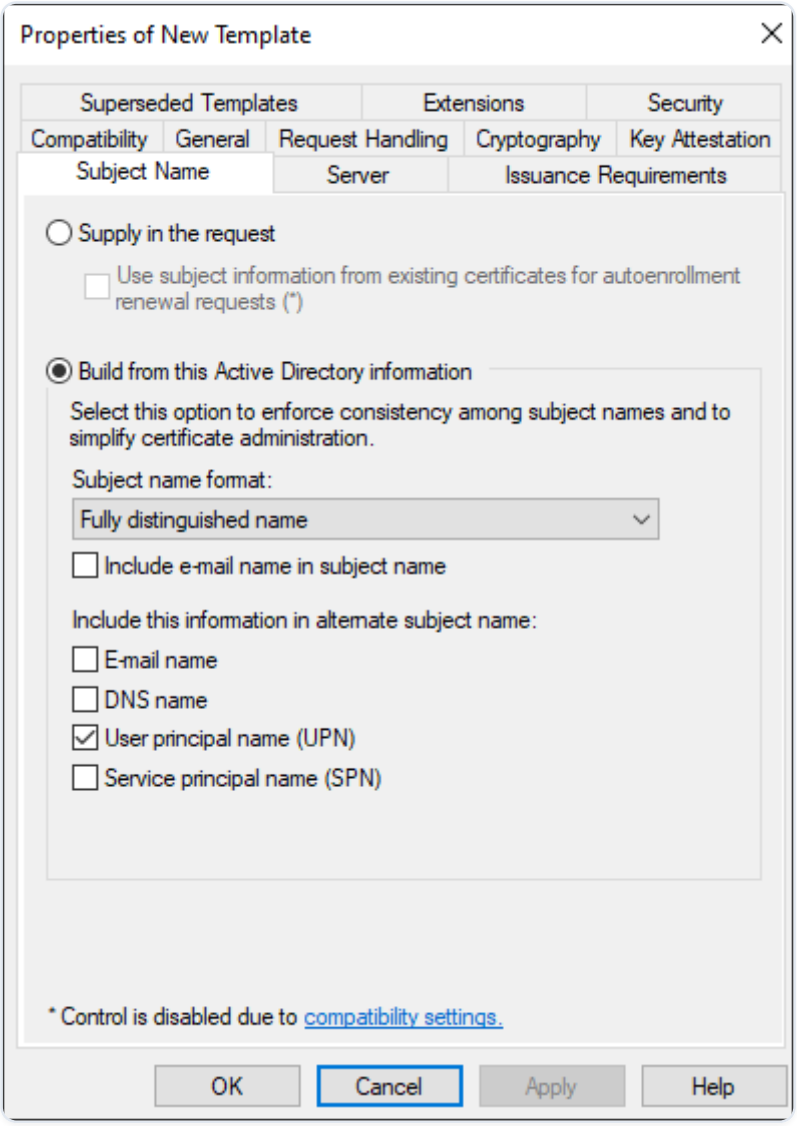
2. 复制“**注册代理**”模板。详细步骤如下：

   a. 右键单击“**证书模板**”并选择“**管理**”。

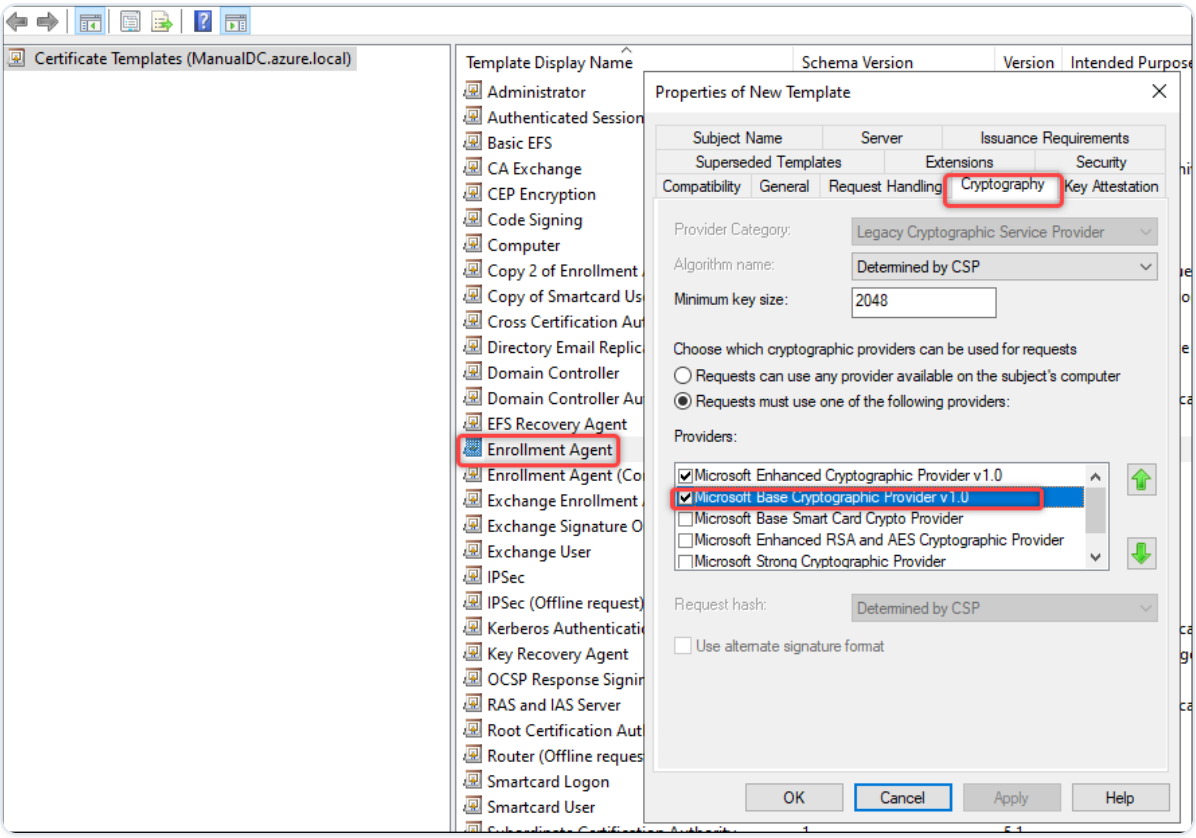


   b. 右键单击“**注册代理**”并选择“**复制模板**”。

   c. 在“**使用者名称**”选项卡上，确保未选中“**在使用者名称中包含电子邮件**”。



d. 在“**加密**”选项卡上，选择“**Microsoft 基本智能卡加密服务提供程序**”，然后单击“**确定**”。名为“**注册代理副本**”的模板将显示在“**证书模板**”列表中。



3. 为智能卡颁发证书。详细步骤如下：

   a. 右键单击 **证书模板**，然后选择 **新建 > 要颁发的模板**。

   b. 选择 **注册代理副本** 和 **智能卡用户**。

   c. 单击 **确定**。

步骤 3：为智能卡用户注册证书

> **注意：**
>
> 以下步骤作为示例提供，以指导您完成此过程。

> 在已加入域的物理 Windows 计算机上，请按照以下步骤为每张智能卡注册证书：

1. 准备一台已加入域的物理 Windows 计算机以用于注册：

   a. 确保智能卡驱动程序已安装。

   b. 将智能卡插入计算机。

   c. 使用您要分配给智能卡的用户帐户登录到计算机。

2. 将 **证书** 管理单元添加到您在步骤 1 中准备的计算机上。详细步骤如下：

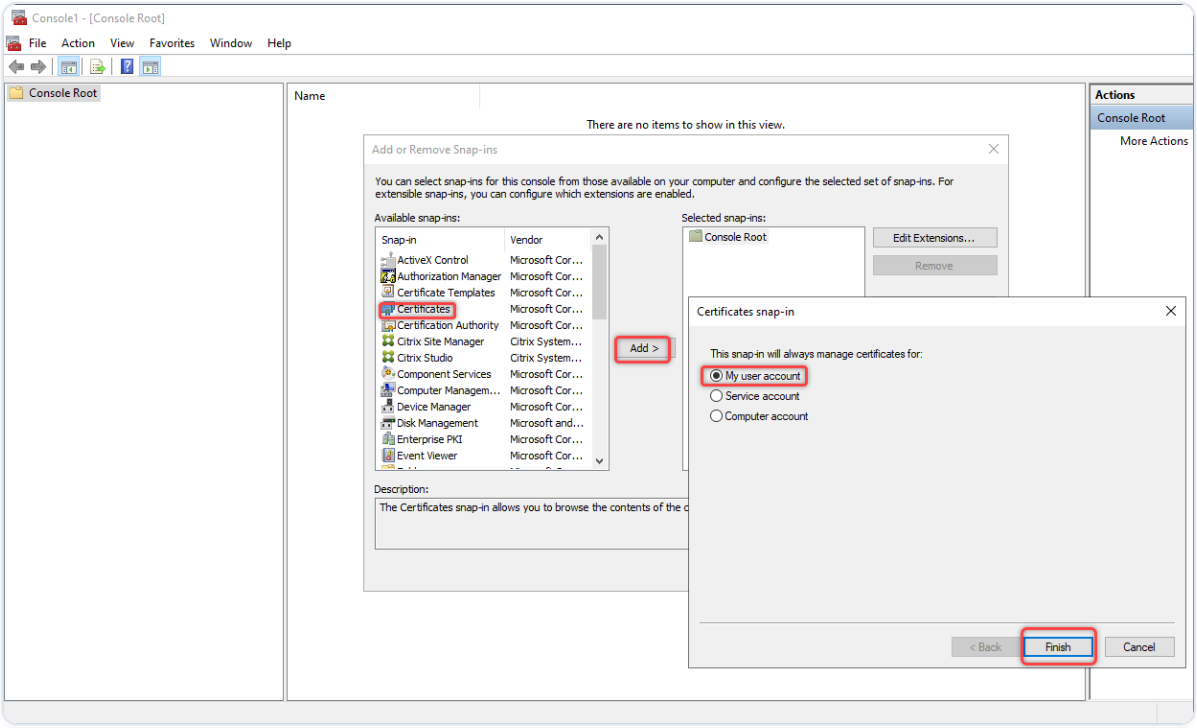
a. 打开 **mmc**。

b. 单击 **文件**，然后单击 **添加/删除管理单元**。

c. 在出现的 **添加或删除管理单元** 窗口中，选择 **证书**，然后单击 **添加 >**。

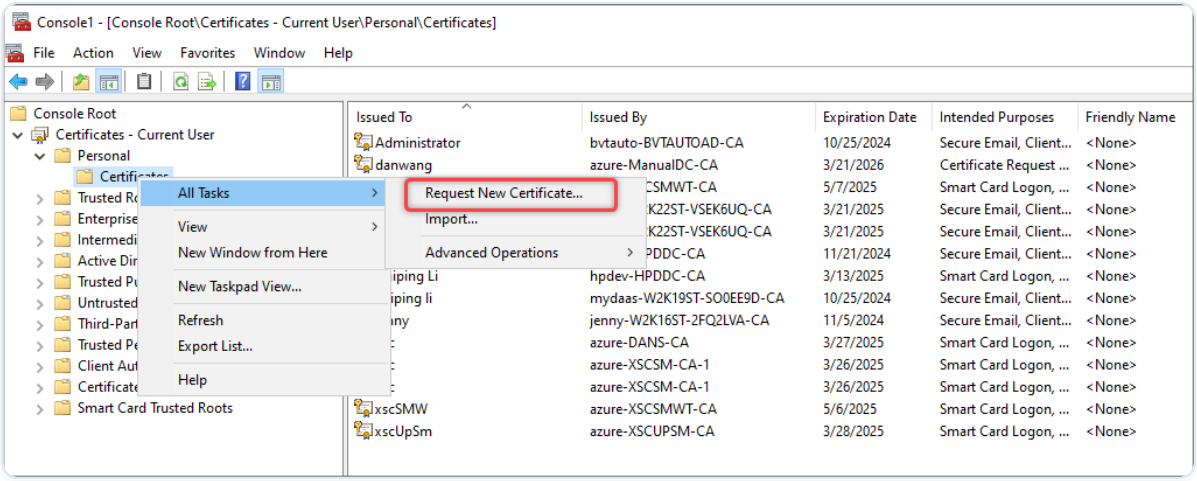
d. 在出现的对话框中，选择 **我的用户帐户**，然后单击 **完成**。

e. 单击 **确定**。

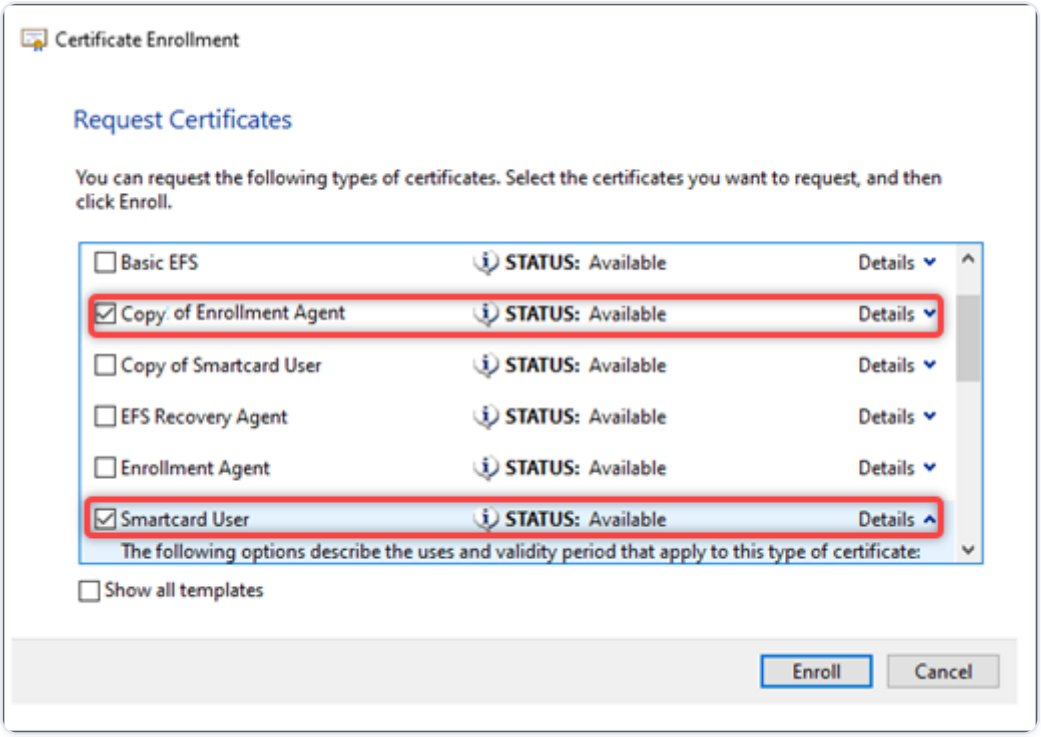


3. 为 **Certificates** 管理单元请求新证书。详细步骤如下：

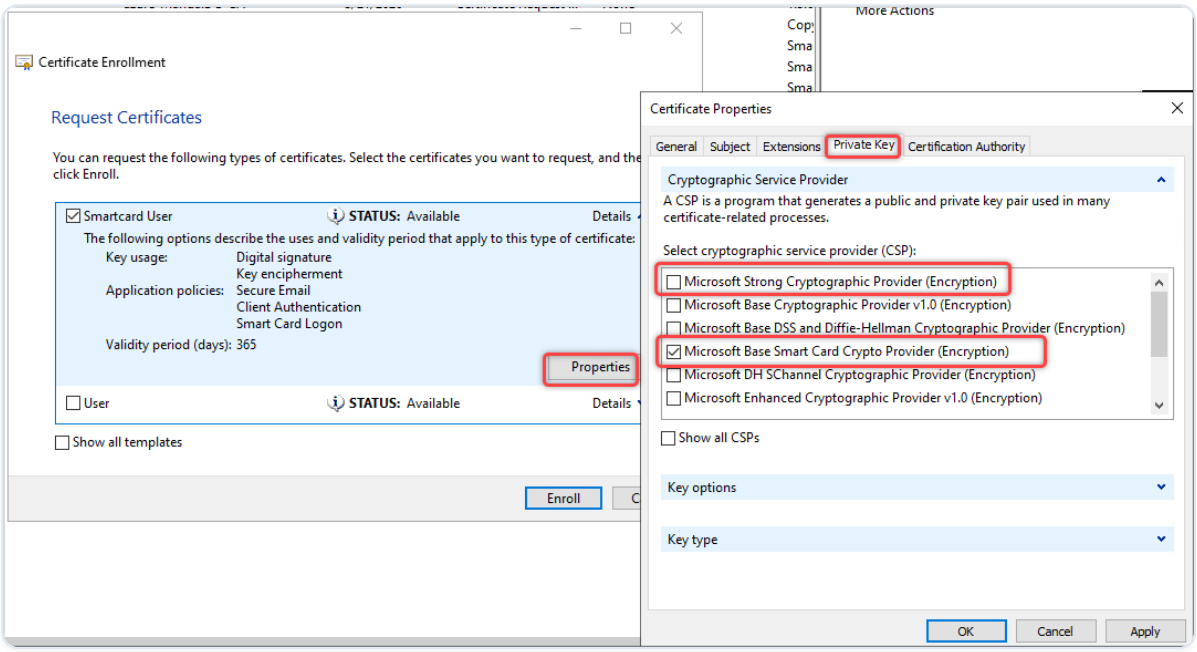
a. 转到 **证书 - 当前用户 > 个人**，右键单击 **证书**，然后选择 **所有任务 > 请求新证书**。



b. 在出现的 **Request Certificates** 对话框中，选择 **Copy of Enrollment Agent** 和 **Smartcard User**。



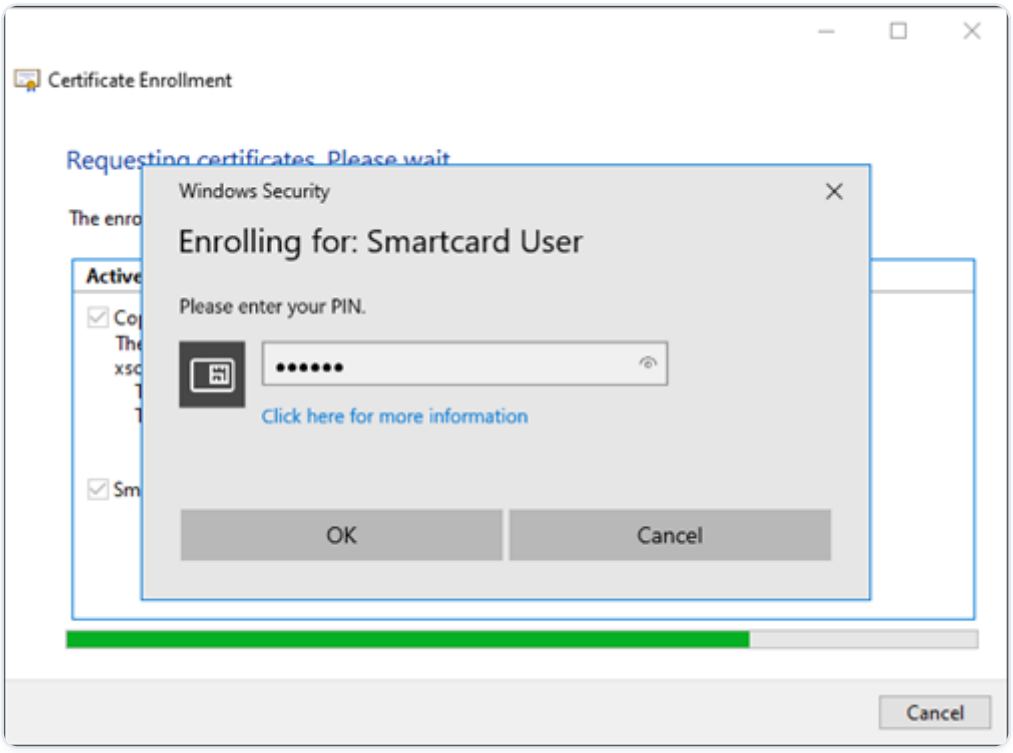
c. 在上述对话框中，单击“**Smartcard User**”的“**详细信息**”，然后单击“**属性**”。此时将显示“**证书属性**”对话框。



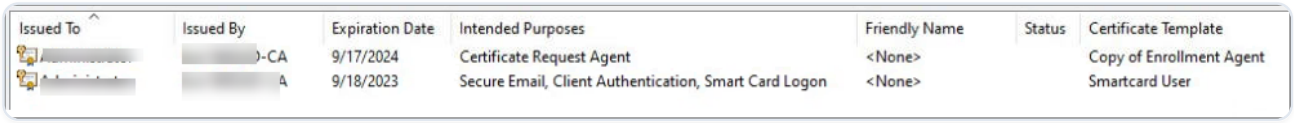
d. 在 **私钥** 选项卡上，展开 **加密服务提供程序**，清除 **Microsoft 增强型加密服务提供程序 (加密)**，仅选择 **Microsoft 基本智能卡加密服务提供程序 (加密)**，然后单击 **确定**。

e. 单击 **Enroll**。

f. 在显示的“**Windows 安全中心**”对话框中，输入智能卡 PIN 码，然后单击“**确定**”。注册完成后，单击“**完成**”。



成功注册后，在 **Certificates - Current User -> Personal -> Certificates** 下会出现两个证书，如以下屏幕截图所示。



步骤 4：配置 WEB STUDIO IIS 服务器

在每个 Web Studio 服务器上，按照以下步骤配置 IIS 以进行智能卡身份验证：

1. 为 Web Studio 计算机启用 **客户端证书映射身份验证**。

   在 IIS 7 及更高版本的默认安装中，`<clientCertificateMappingAuthentication>` 元素不可用。有关安装和启用的更多信息，请参阅这篇 Microsoft 文章。

2. 在 Web Studio 计算机上启动 **IIS Manager**。
3. 为计算机启用 **Active Directory 客户端证书身份验证**。详细步骤如下：

   a. 在左窗格中选择计算机，然后双击 **Authentication**。

   IIS > 身份验证(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/ad-client-auth-1.png)

   b. 启用 **Active Directory 客户端证书身份验证**。

   IIS > 启用 AD 客户端证书身份验证(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/ad-client-auth-2.png)

4. 为 Web Studio 后端模块配置更安全的 HTTPS 协议以及客户端证书身份验证：

a. 转至“**站点 >** `the IIS site name where Web Studio is installed (site ID = 1, by default, Default Web Site)` **> Studio > Backend > Smartcard**”，然后在“**IIS**”部分双击“**SSL 设置**”。

IIS 后端模块智能卡 SSL(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/iis-server-backend-smartcard-ssl.png)

b. 为 **客户端证书** 选择 **要求**。

IIS 服务器后端智能卡 SSL 必需(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/iis-server-backend-smartcard-ssl-required.png)

c. 返回“**站点 >** `the IIS site name where Web Studio is installed (site ID = 1, by default, Default Web Site)` **> Studio > Backend > Smartcard**”，然后在“**IIS**”部分双击“**配置编辑器**”。

IIS > 配置编辑器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/iis-server-backend-smartcard-config.png)

d. 确保 **/clientCertificateMappingAuthentication** 已**启用**。

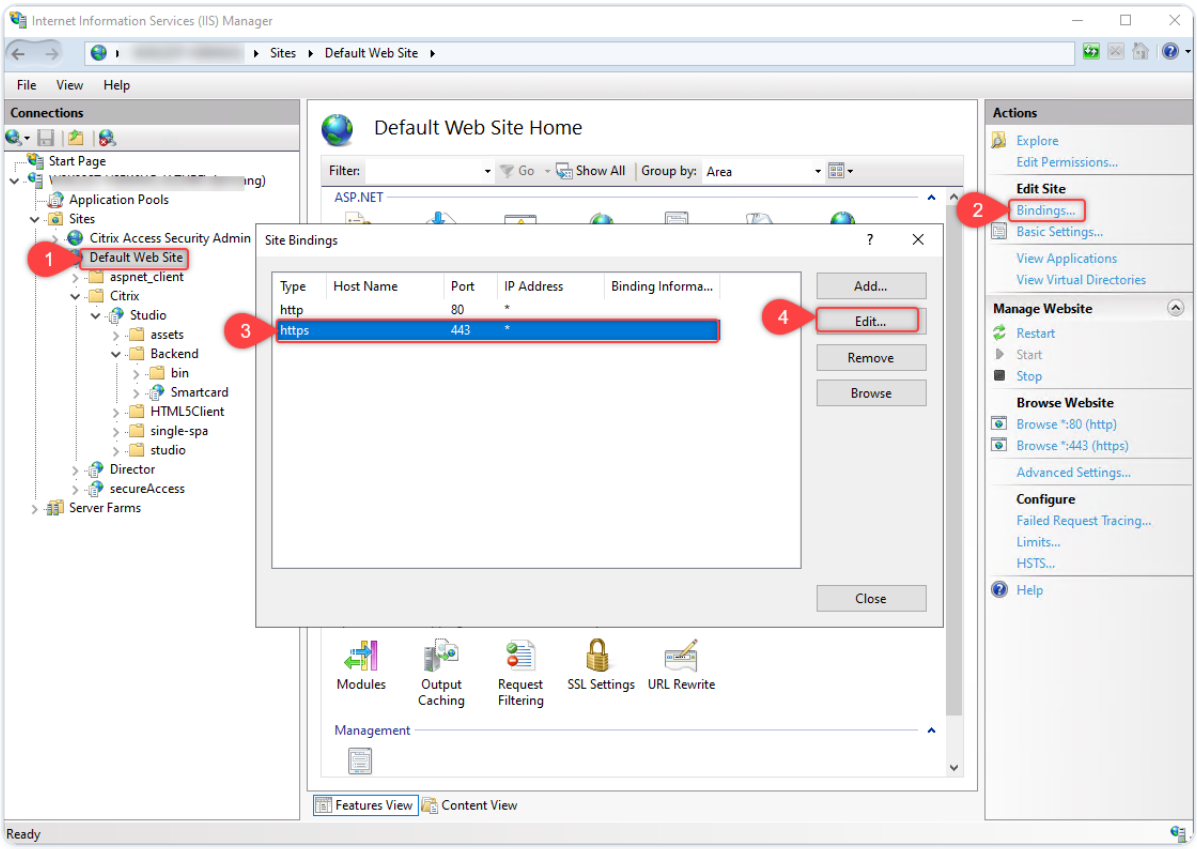
启用客户端身份验证(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/iis-server-backend-smartcard-config-enabled.png)

5. (仅限 Windows 2022) 禁用通过 TCP 的 TLS 3.1。详细步骤如下：

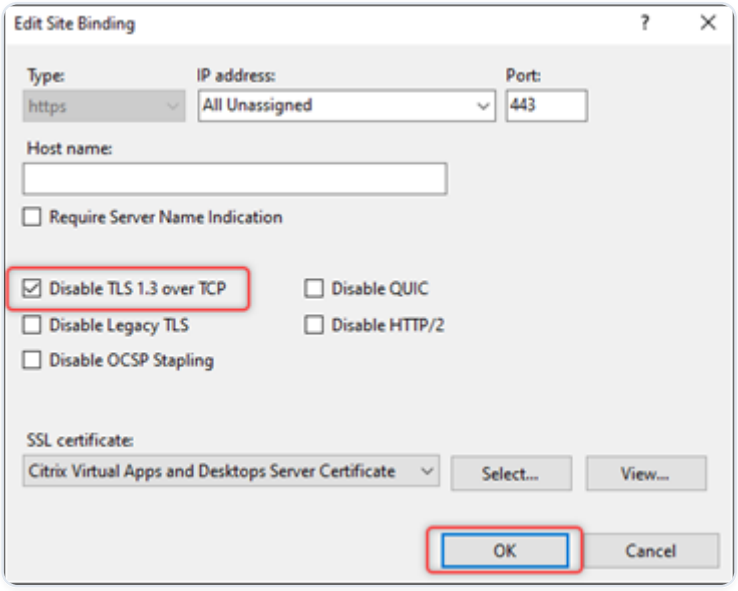
a. 转至“**站点 >** `the IIS site name where Web Studio is installed (site ID = 1, by default, Default Web Site)` ”。

b. 单击 **编辑站点 > 绑定**。

c. 在出现的“**站点绑定**”对话框中，选择 **https** 记录，然后单击“**编辑**”。



d. 在出现的“**编辑站点绑定**”对话框中，选择“**禁用 TLS 1.3 over TCP**”，然后单击“**确定**”。



须知：

Web Studio Backend 是 Web Studio 中的一个模块，提供以下功能：

- 智能卡身份验证。
- 使用集成 Windows 身份验证从编排服务检索 FMA 持有者令牌。

步骤 5 (可选) 为 WEB STUDIO 配置身份验证委派

当 Web Studio 和 Delivery Controller 安装在不同的服务器上时，您必须为每个 Web Studio 服务器向 Delivery Controller 配置用于 HOST 和 HTTPS 服务的委派。

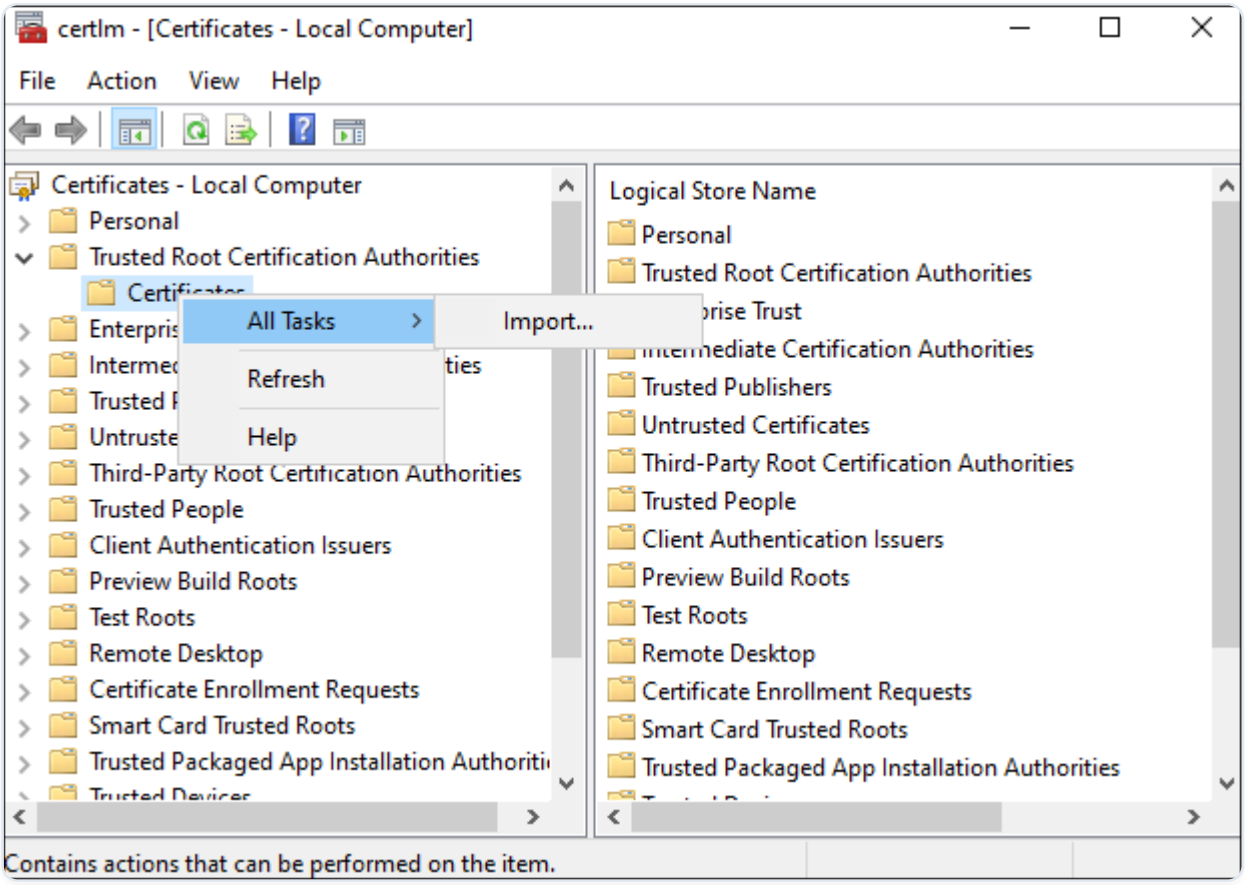
请按照以下步骤为每个 Web Studio 服务器完成此任务：

1. 导入 Delivery Controller™ 编排 HTTPS 证书
2. 为 Web Studio 服务器配置委派
3. （可选）为 Web Studio IIS 服务器的服务帐户配置委派

导入 Delivery Controller 编排 HTTPS 证书

在 Web Studio 服务器上，将 **Delivery Controller 编排 HTTPS** 证书导入到 **受信任的根证书颁发机构**。详细步骤如下：

1. 启动 **设置 > 管理计算机证书**。
2. 右键单击 **受信任的根证书颁发机构 > 证书**，然后选择 **所有任务 > 导入**。

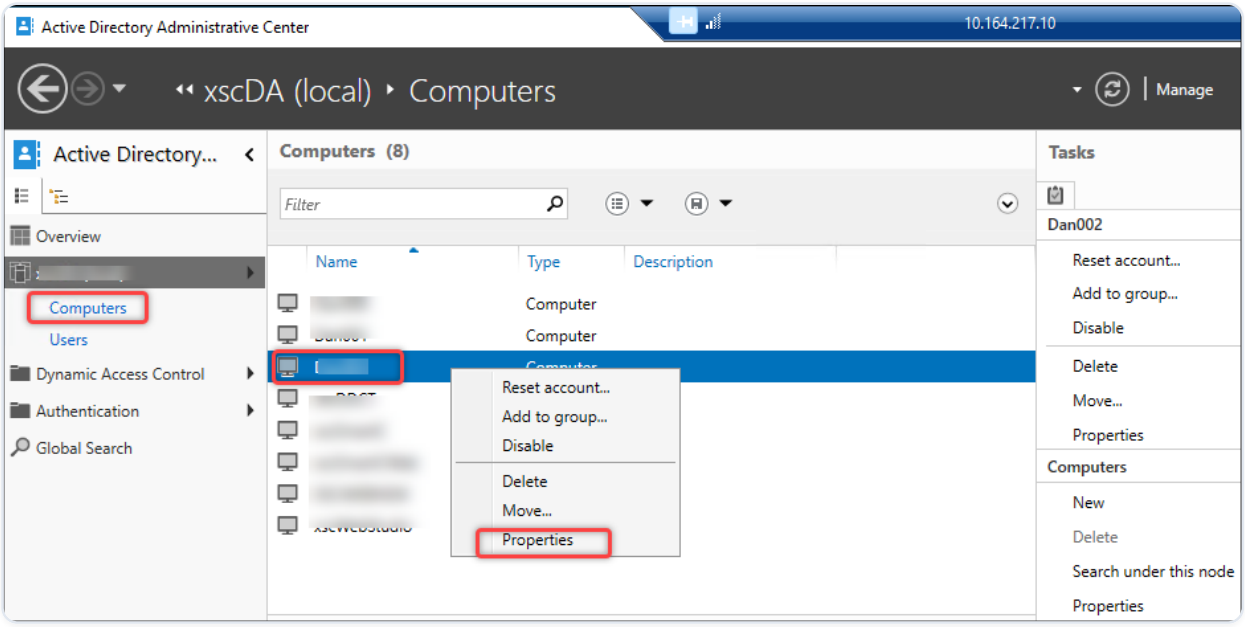


3. 按照屏幕上的说明导入 **Delivery Controller 编排 HTTPS** 证书。

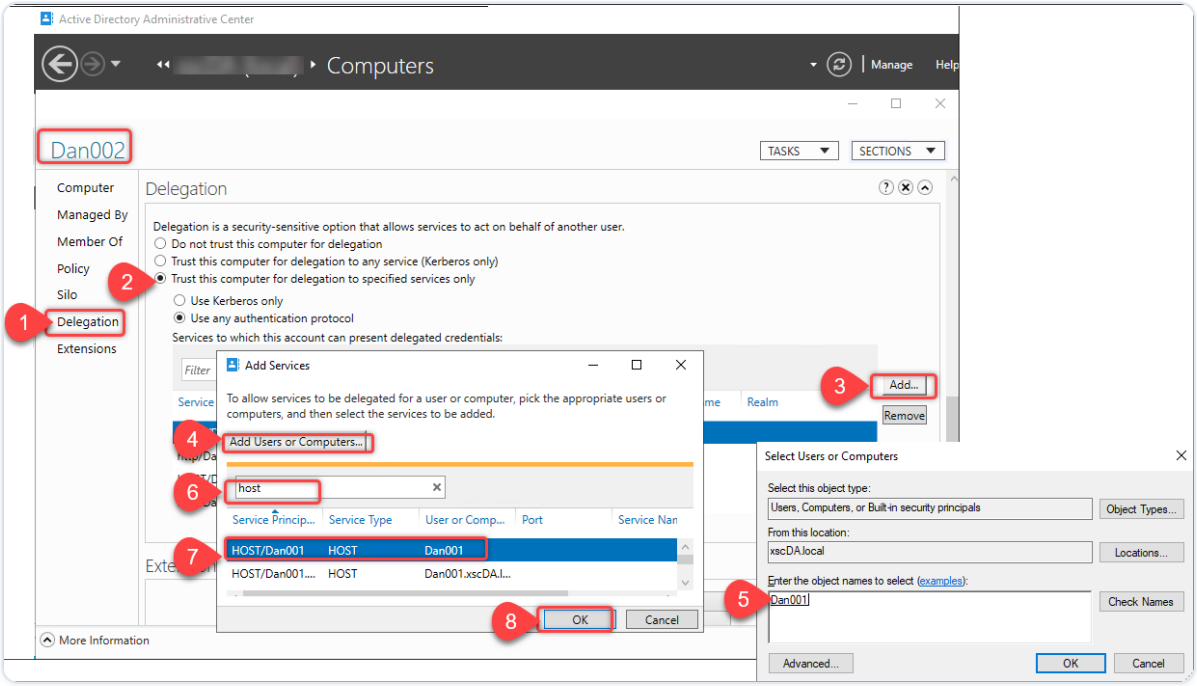
配置 Web Studio 服务器的委派

在域控制器上，为 Web Studio 服务器配置到 Delivery Controller 的 HOST 和 HTTP 服务的委派。请按照以下步骤完成此任务：

1. 在域控制器上，启动 **Active Directory 管理中心**。
2. 找到要为其配置委派的 Web Studio 服务器的**计算机**帐户（*例如，Dan002*）。
3. 右键单击该帐户，选择“**属性**”，然后完成以下步骤：



a. 转到**委派**选项卡。



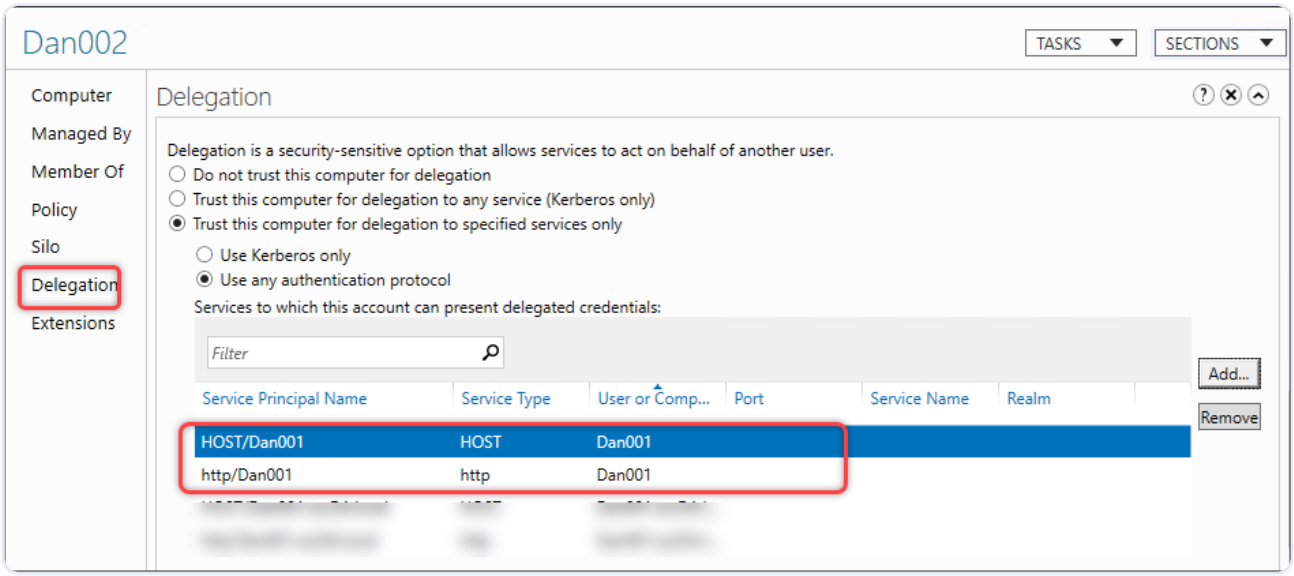
b. 选择 **仅信任此用户作为委派对象 > 使用任何身份验证协议**。

c. 单击 **添加** 以指定此计算机帐户可委派到的服务。

d. 在出现的 **添加服务** 对话框中，单击 **添加用户或计算机** 以查找 Delivery Controller 的计算机名称（*例如，Dan001*）。

e. 选择 **HOST** 和 **HTTP** 服务，然后单击 **确定**。

配置结果显示在以下屏幕截图中。

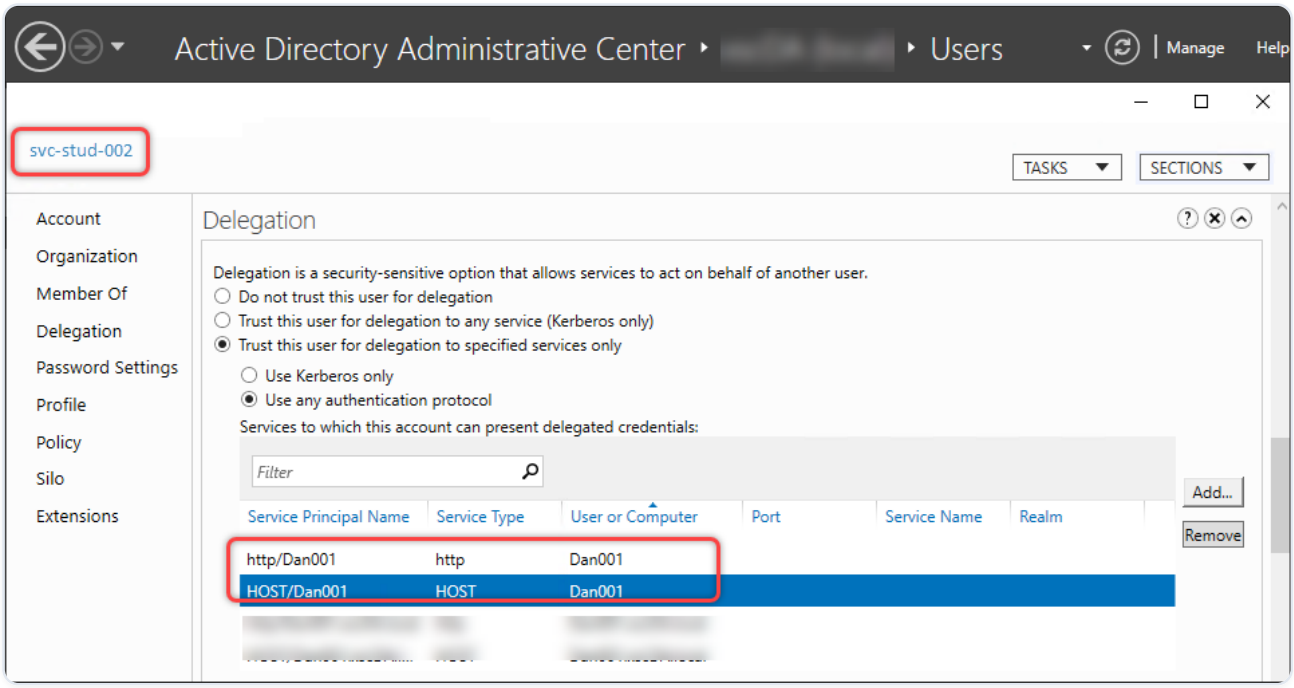


（可选）为 Web Studio IIS 服务器的服务帐户配置委派

如果您已为 Web Studio IIS 服务器配置了服务帐户，则还需要为该服务帐户配置委派，以使其能够访问 Delivery Controller 的 HOST 和 HTTP 服务。建立此委派后，Web Studio 服务器可以使用其服务帐户模拟当前智能卡用户，以访问 Delivery Controller 的 HOST 和 HTTP 服务。请按照以下步骤完成配置：

1. 在域控制器上，启动 **Active Directory 管理中心**。
2. 找到要为其配置委派的 Web Studio IIS 服务器的**用户**帐户（服务帐户）（*例如，svr-stud-002*）。
3. 右键单击该帐户并选择**属性**。
4. 按照 配置 Web Studio 服务器的委派 的第 3 步中描述的步骤，将 Web Studio IIS 服务器的服务帐户委派给 Delivery Controller，用于 HOST 和 HTTP 服务。

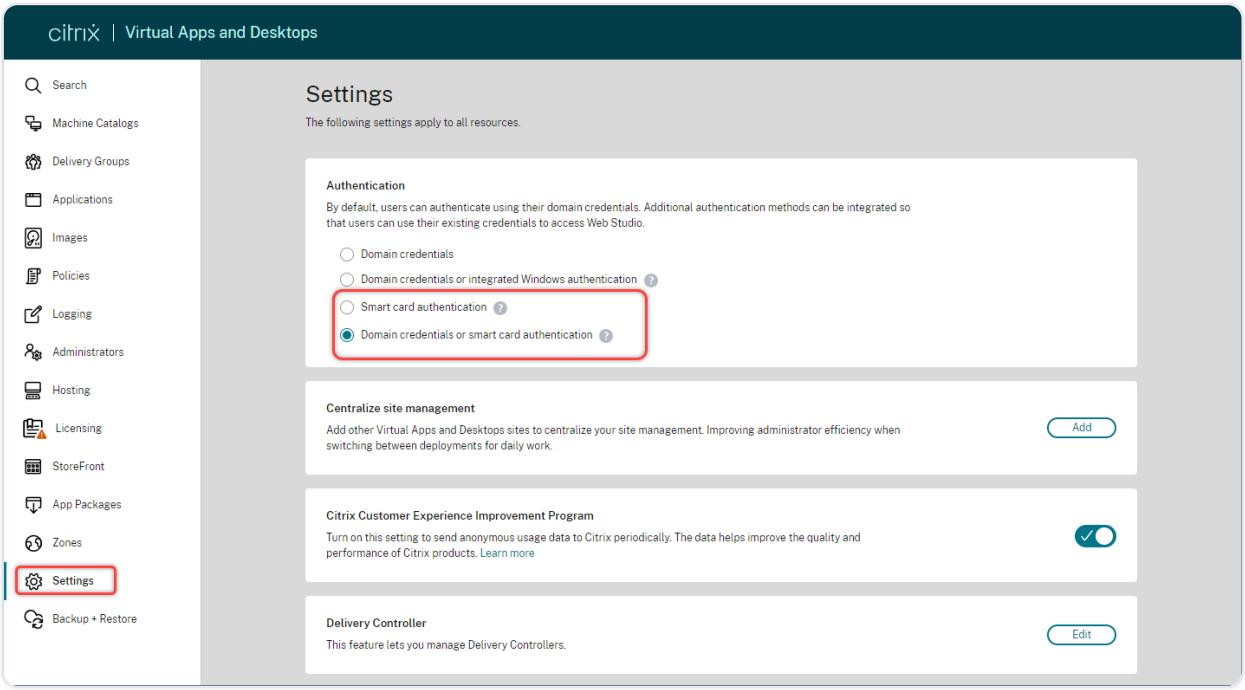
配置结果显示在以下屏幕截图中。



步骤 6：为 WEB STUDIO 启用智能卡身份验证

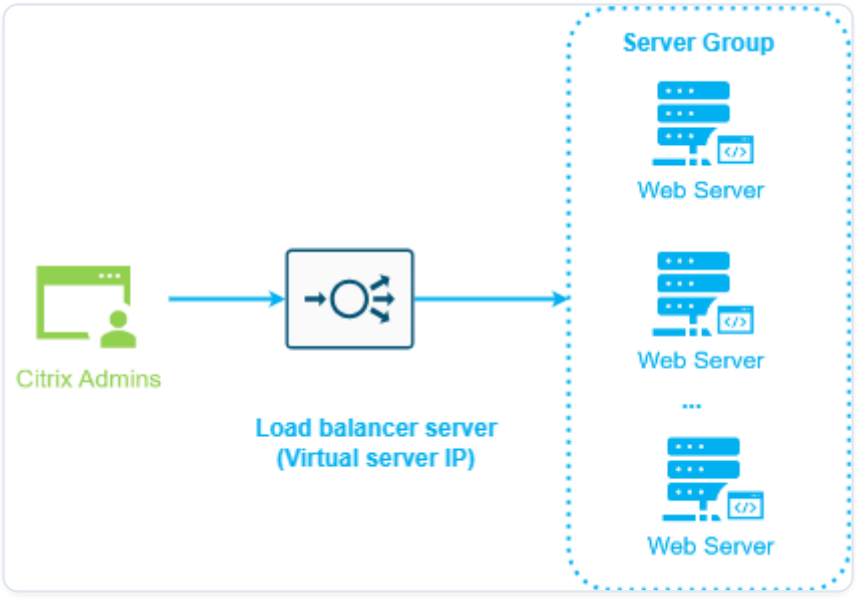
请按照以下步骤为 Web Studio 启用智能卡身份验证：

1. 登录 **Web Studio** 并在左侧窗格中选择 **设置**。
2. 根据需要选择 **智能卡身份验证** 或 **域凭据或智能卡身份验证**。
3. 单击**应用**。



设置负载均衡的 Web Studio 部署

要设置高可用性 Web Studio 部署，您可以选择 NetScaler® ADC 或 Windows 网络负载均衡等工具。本文提供了使用 NetScaler ADC 设备设置负载均衡 Web Studio 部署的分步指南。



证书要求

在从商业证书颁发机构购买证书或从您的企业证书颁发机构颁发证书之前，请根据您的需求考虑以下选项：

选项	优点	缺点
选项 1：在 NetScaler ADC 设备负载均衡器服务器和 Web Studio 服务器上使用 *.example.com 通配符证书。	• 简化配置 • 更易于管理 (单个证书) • 可以添加新的子域而无需更新证书	• 如果通配符证书遭到泄露，所有子域都将面临风险 • 并非所有应用程序都支持通配符证书 • 可能比单个证书更昂贵
选项 2：在 NetScaler ADC 设备负载均衡器服务器和 Web Studio 服务器上使用带有主题备用名称 (SAN) 的证书。	• 灵活，可以包含多个特定域和子域 集中管理多个域	• 随着域数量的增加，管理 SAN 条目可能会变得复杂 添加新域需要重新颁发证书

选项	优点	缺点
	支持多个不同的名称，提供比通配符更大的灵活性	受 CA 支持的 SAN 条目数量限制
选项 3：为每个 Web Studio 服务器和 NetScaler ADC 设备负载均衡器服务器使用一个证书	• 每个服务器都是独立安全的	• 管理开销更高，因为每个证书都必须单独管理
	一个证书的泄露不会影响其他证书	需要续订的证书更多，成本可能更高
	可以使用针对每个服务器需求量身定制的特定证书	必须确保所有证书都配置一致

在负载均衡器上配置服务器证书

1. 登录到 NetScaler ADC 设备管理 GUI。
2. 选择 **流量管理 > SSL > 证书 > 服务器证书**
3. 单击“**安装**”。
4. 在**安装服务器证书**页面上，输入证书-密钥对名称，单击**选择文件**，然后浏览证书文件。如果证书文件不包含私钥，请选择**密钥文件**。

   证书安装屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/cert-install.png)

步骤 1: 添加 WEB STUDIO 服务器节点

将所有 Web Studio 服务器节点（例如，`Studio-eu-1` 和 `Studio-eu-2`）添加到负载均衡器。

1. 登录到 NetScaler ADC 管理 GUI。
2. 导航到 **Traffic Management > Load Balancing > Servers**。单击“**添加**”。
3. 输入 Web Studio 服务器节点的服务器 IP 地址。
4. 重复步骤 2–3 以添加其他 Web Studio 服务器。

   包含两个服务器的“服务器”屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/server-nodes.png)

步骤 2: 为 WEB STUDIO 服务器节点添加监视器

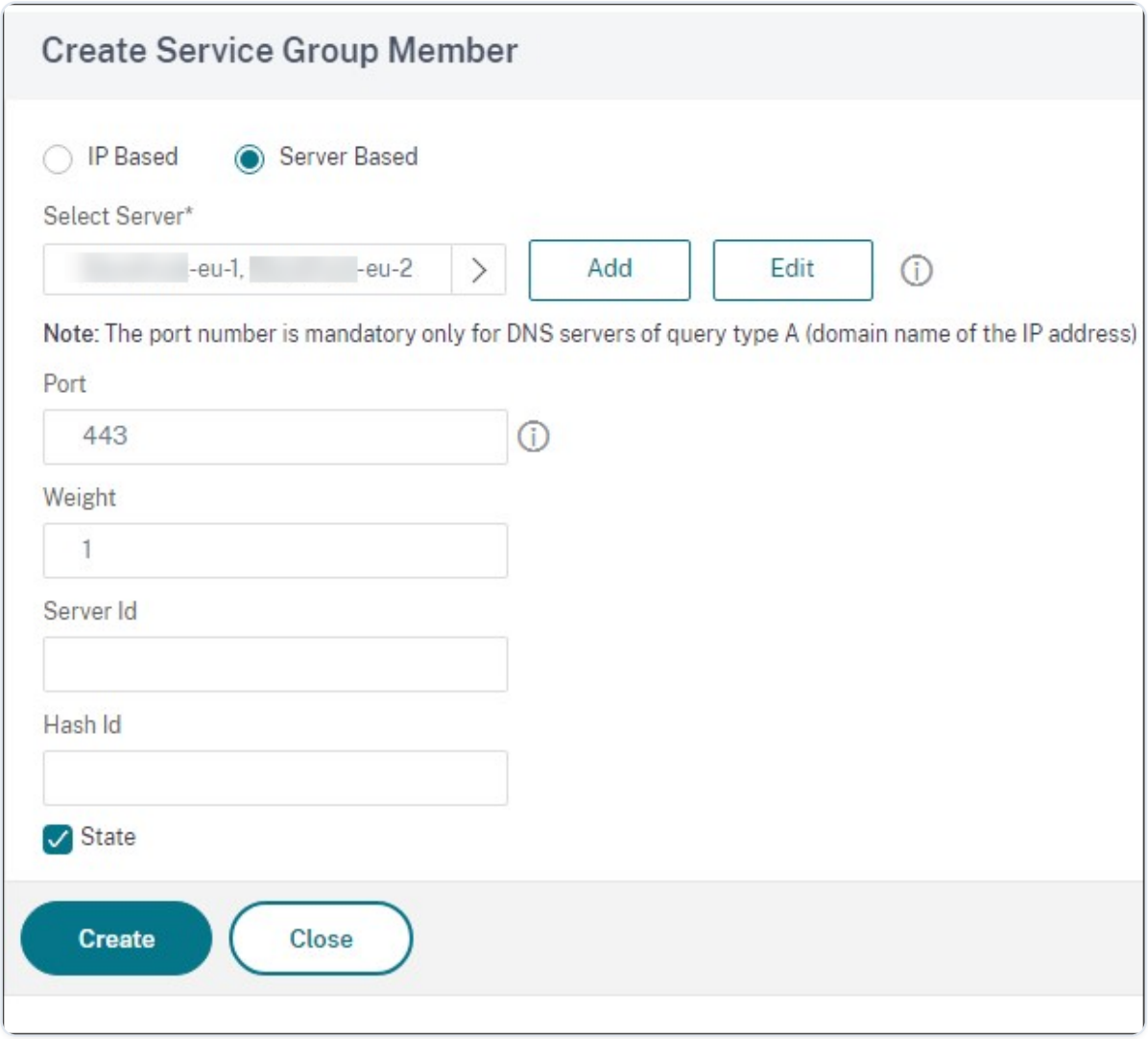
在负载均衡器中设置监视器，以检查所有 Web Studio 服务器节点的状态。

1. 选择 **流量管理 > 负载平衡 > 监视器 > 添加**。
2. 在“**配置**”选项卡上，完成以下设置并保留其他默认值：
   - 为“**名称**”输入 **Web Studio**。
   - 为“**类型**”选择 **HTTP** 或 **SSL**。
   - 选择“**安全**”选项。
   - 为“**HTTP 请求**”输入 **HEAD/citrix/studio/**。

   包含两个服务器的“服务器”屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/netscaler-monitor-for-studio.png)

步骤 3: 为 WEB STUDIO 服务器节点创建服务组

1. 选择 **Traffic Management > Load Balancing > Service Groups > Add**。要通过 HTTPS 连接到 Web Studio 服务器，请选择 SSL 协议，保留其他设置作为默认值，然后单击“**确定**”。
2. 在您的服务组中，在“**服务组成员**”下，单击“**无服务组成员**”，然后按照以下步骤添加成员：
   a. 单击 **基于服务**。
   b. 选择之前添加的所有服务器。
   c. 端口输入 **443**。



3. 添加“**监视器**”部分，然后选择您之前创建的 Web Studio 监视器。

   监视器屏幕截图，其中列出了一个监视器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/monitors.png)

4. 添加“**证书**”部分并完成以下设置：

   a. 绑定客户端证书。

   b. 绑定用于签署您之前导入的服务器证书的 CA 证书，以及可能属于 PKI 信任链的任何其他 CA。

      添加绑定屏幕(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/add-binding.png)

5. 添加“**设置**”部分，选择“**插入客户端 IP 标头**”，然后输入标头名称 **X-Forwarded-For**。此设置允许在策略中使用客户端 IP 地址。

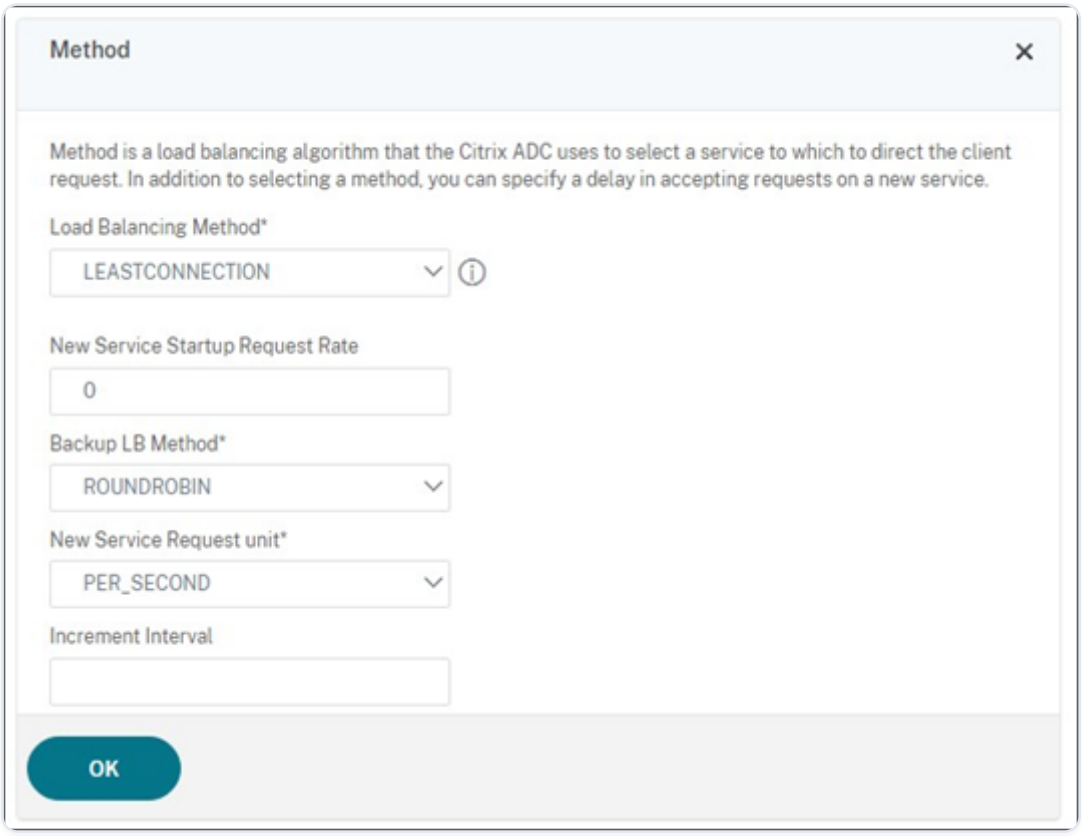
步骤 4：创建虚拟服务器

创建一个负载平衡虚拟服务器，供用户访问 Web Studio 服务器组。

1. 导航到“**流量管理 > 负载平衡 > 虚拟服务器**”，然后单击“**添加**”。
2. 输入名称，为“**协议**”选择 **SSL**，为“**端口**”输入 **443**，然后单击“**确定**”。



3. 将您之前创建的“**服务组**”绑定到负载平衡虚拟服务器。
4. 绑定您在步骤 3：为 Web Studio 服务器节点创建服务组中绑定到服务组的 CA 证书。
5. 添加“**方法**”部分并选择负载平衡方法。Web Studio 负载平衡的常见选择是 **ROUNDROBIN** 或 **LEASTCONNECTION**。



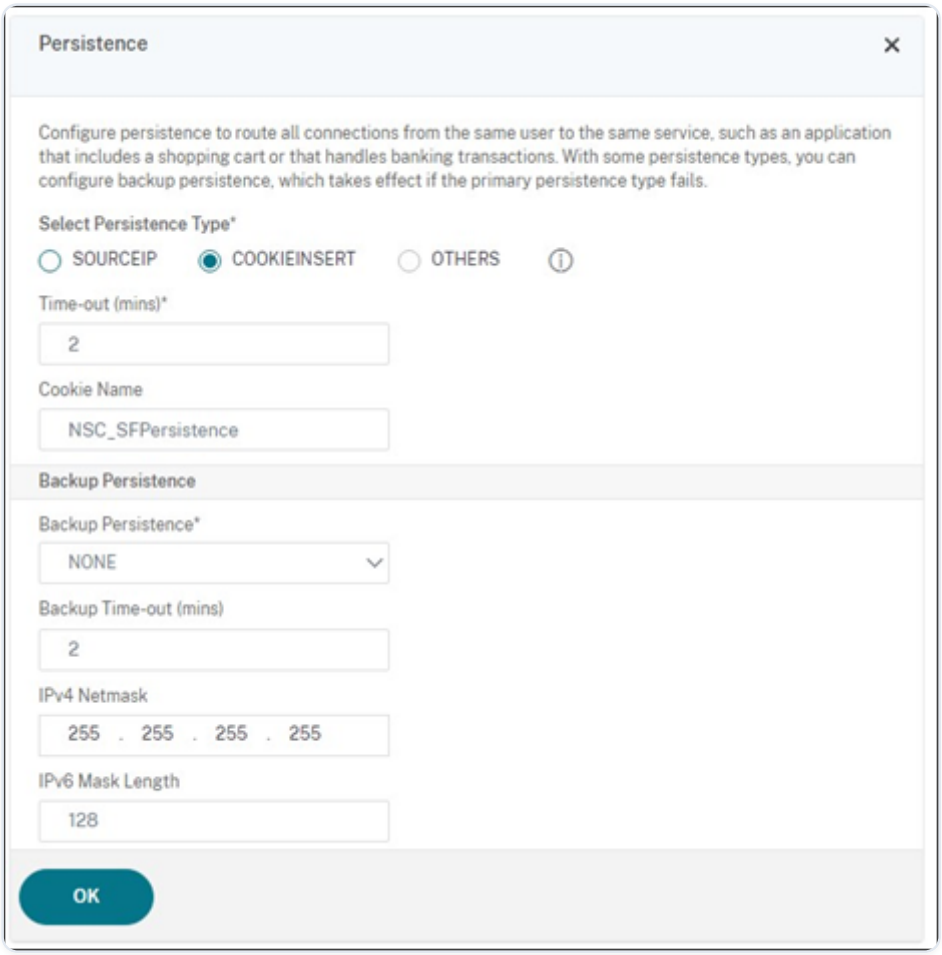
6. 添加 **持久性** 部分并完成以下设置:

   a. 将持久性方法设置为 **COOKIEINSERT**。

   b. 将超时设置为与 Web Studio 中的会话超时相同（默认情况下为 20 分钟）。

   c. 为会话 Cookie 命名，以便于将来调试。例如，**NSC_SFPersistence**。

   d. 将备份持久性设置为 **NONE**。

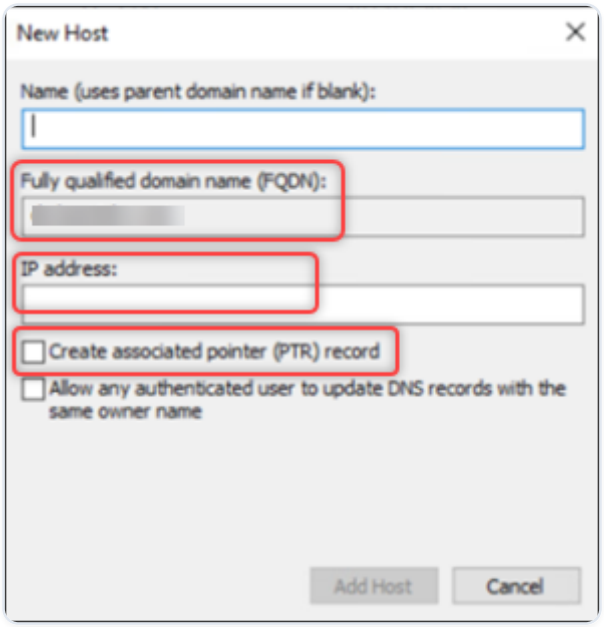


注意：

如果客户端不允许存储 HTTP Cookie，则后续请求不包含 HTTP Cookie，并且不使用持久性。

步骤 5: 为虚拟服务器创建 DNS 记录

在域控制器上，创建 DNS 和 PTR 记录，将虚拟服务器的 IP 地址映射到 FQDN。网络中的 Web Studio 用户使用此 FQDN 访问 Web Studio 服务器组。例如，webstudio.example.com 解析为负载均衡器虚拟服务器 IP 地址 (VIP)。

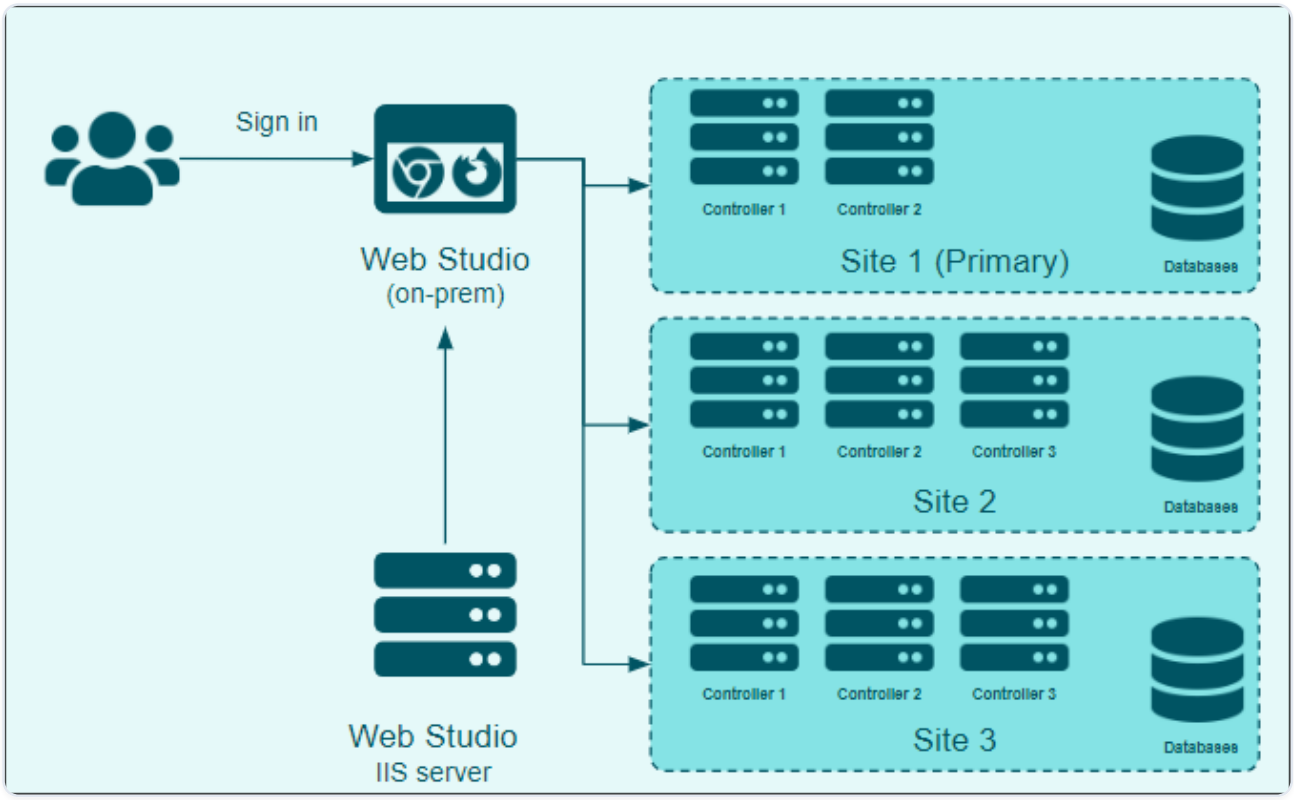


为用户提供此 URL 以访问 Web Studio 服务器: `https://<FQDN of the virtual server>/<text you entered in the HTTP Request field when creating a monitor>`。示例: `https://webstudio.example.com/citrix/studio`

启用多站点管理

默认情况下，一个 Web Studio 控制台映射到一个 Citrix Virtual Apps and Desktops™ 站点，必要时，您可以配置一个 Web Studio 控制台来管理多个站点。这样，您只需安装一个 Web Studio 即可配置和管理所有站点。

下图说明了多站点体系结构，其中单个 Web Studio 部署管理多个独立的 Citrix Virtual Apps and Desktops™ 站点。



> **注意：**
>
> 多站点部署支持 Web Studio 连接到比其早一个版本的 Delivery Controller。这种向后兼容性允许分阶段升级。但是，建议所有组件都在同一版本上运行，以确保完整的功能。

优势

- 通过统一的单一登录体验，提高了管理多个站点的效率。
- 所有配置都可从一个控制台访问，从而简化了故障排除。

注意事项

配置和部署站点时，请记住以下事项：

- 所需版本：
  - Citrix Virtual Apps and Desktops 2311 及更高版本。
  - Delivery Controller™ 版本必须与 Web Studio 版本匹配或早于 Web Studio 版本，最低要求为 2311 或更高版本。
  - 此功能仅适用于 Web Studio（基于 Web），不适用于 Citrix Studio（基于 Windows）。
- 为了支持单一登录，请在受信任的域上部署所有站点。
- 您可以使用统一的 Web Studio 控制台管理最多 10 个 Citrix Virtual Apps and Desktops 站点。

工作流程

开始之前

- 确定主站点，并确保 Web Studio 控制台可用于主站点管理。

> **注意：**
>
> - 设计主站点时，请注意，所添加站点的可访问性取决于主站点的可用性。主站点的性能问题可能会影响对所添加站点的访问。
> - 如果未安装 Web Studio，请参阅安装 Web Studio。

- 确保您打算使用 Web Studio 管理的站点已就绪。
  - 要创建新站点，请参阅创建站点。
- （推荐）要在控制台上在站点之间切换时启用单点登录，请在所有站点上启用集成 Windows 身份验证 (IWA)。对于未启用 IWA 的站点，您也可以使用登录凭据登录。

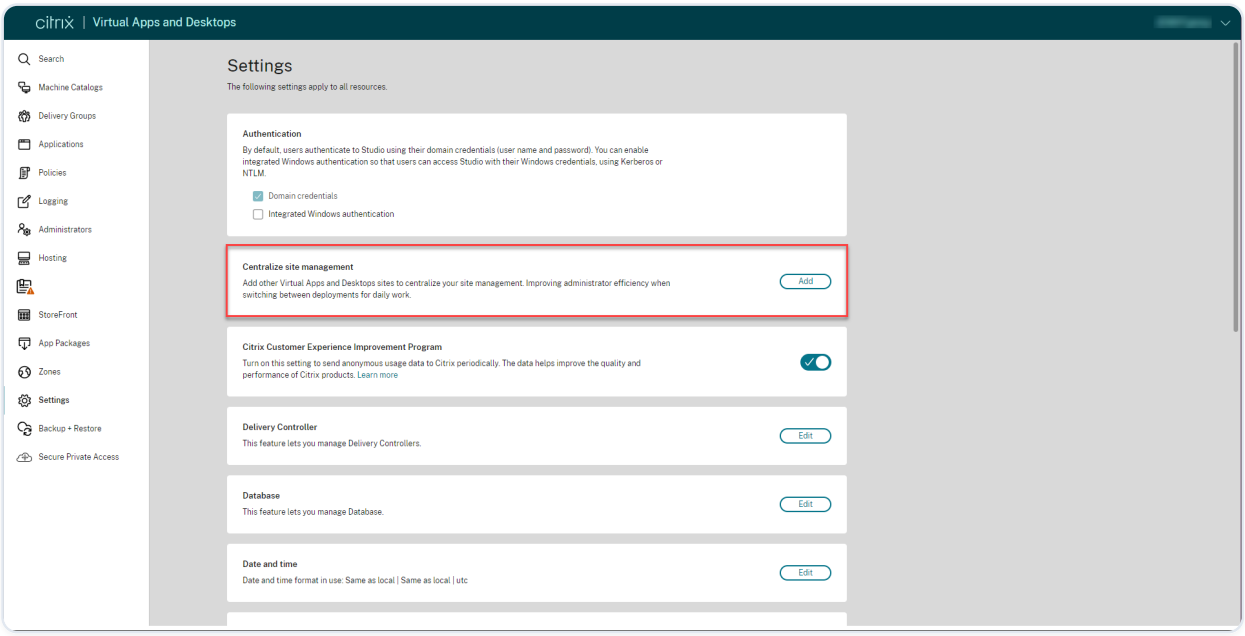
步骤 1：登录到 Web Studio 控制台

1. 打开 Web 浏览器。输入 `https://<address of the server hosting Web Studio>/Citrix/Studio`。
2. 登录到 Web Studio 以管理主站点。

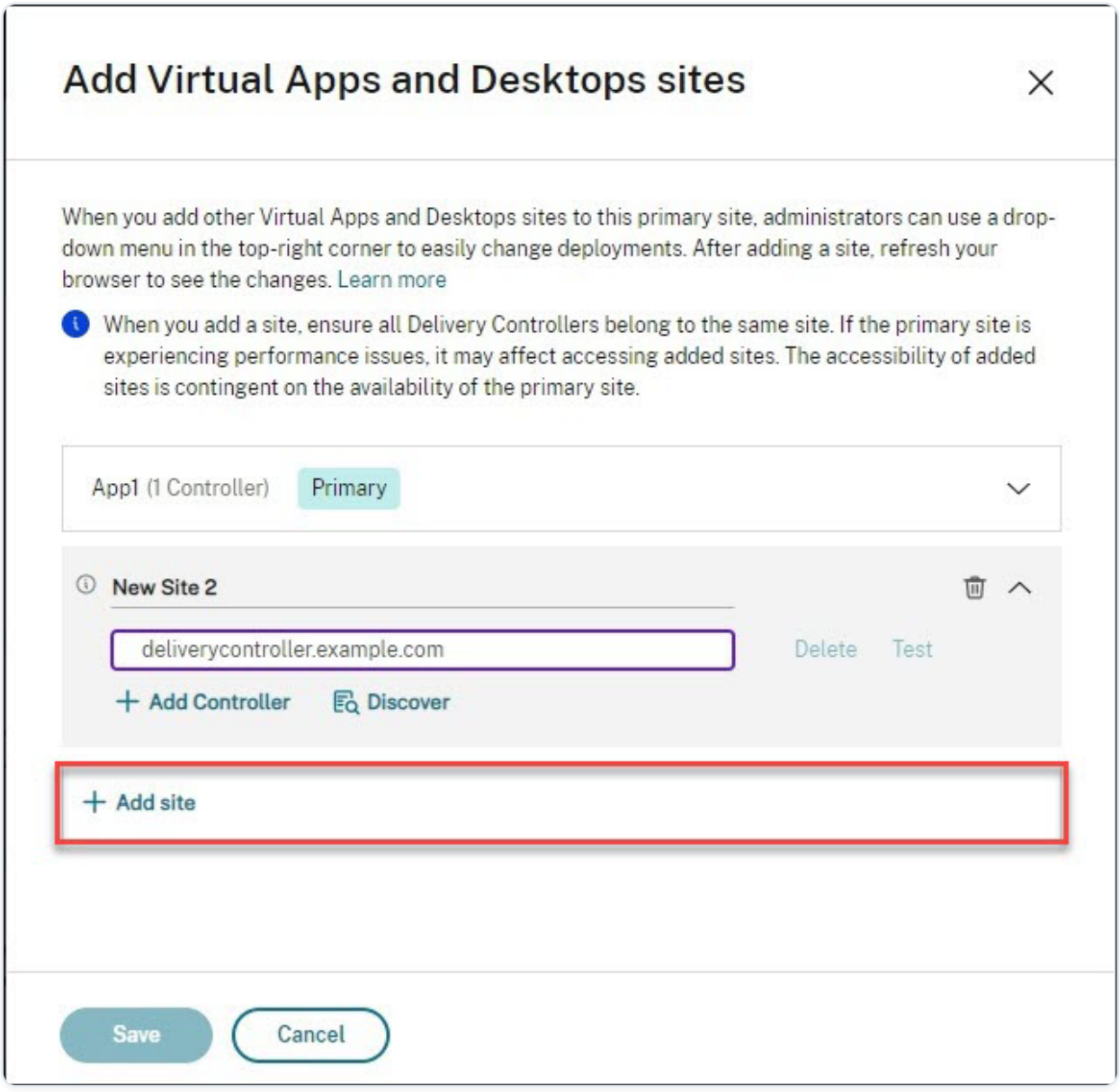
> **注意：**
>
> 您在安装期间使用的 Delivery Controller 地址用于标识站点。如果 Delivery Controller 来自主站点，您将登录到该站点。

步骤 2：使用 Web Studio 添加站点

1. 转至**设置** > **集中站点管理**，然后单击**添加**。



2. 在**添加 Virtual Apps and Desktops 站点**页面上，单击**添加站点**。



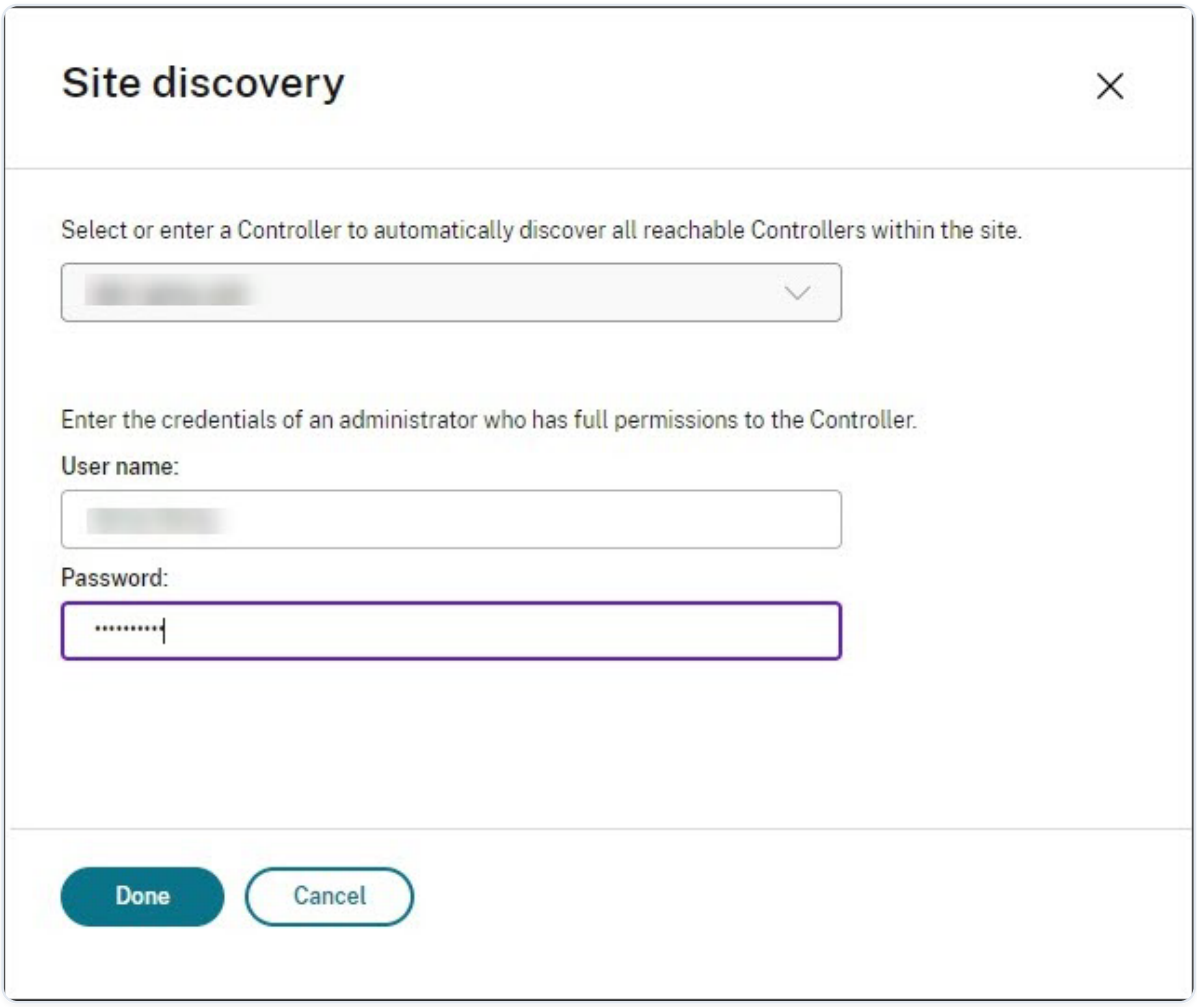
3. 执行以下任一操作以添加交付控制器：

   - 单击“**添加控制器**”，然后输入 FQDN。单击“**测试**”以测试其连接性。
   - 单击“**发现**”。

     a. 在“**站点发现**”页面上，选择或输入站点中存在的控制器的地址。

     b. 在“**用户名**”和“**密码**”字段中输入对控制器具有完全权限的管理员凭据。

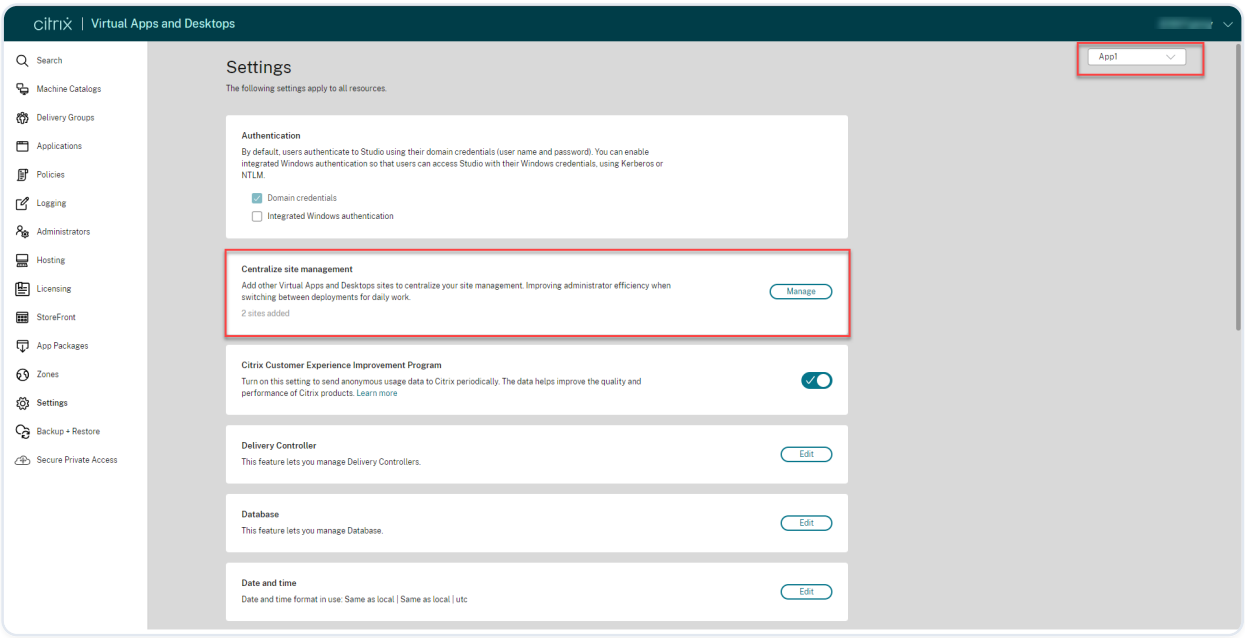
     c. 单击“**完成**”。



> **注意：**
>
> “发现”功能会根据您输入的交付控制器地址，自动添加站点内可访问的交付控制器。

4. 单击 **保存**。

   要管理或编辑站点配置，请转至“**设置**”>“**集中站点管理**”，然后单击“**管理**”。 “**管理**”选项仅对主站点启用。



步骤 3：管理站点设置

刷新浏览器以显示站点配置更改。站点选择框显示在控制台的右上角。

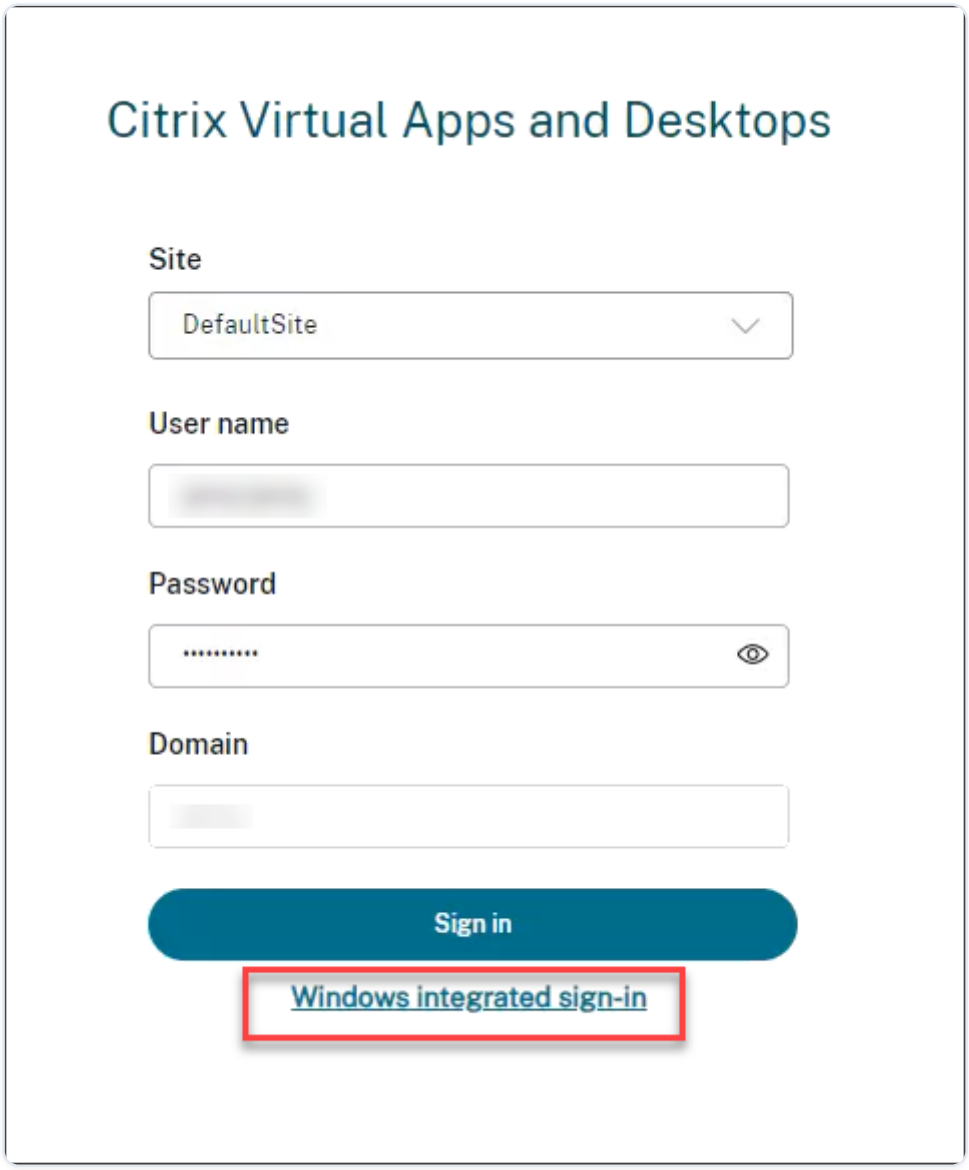
在“**设置**”页面上，从右侧角落“**刷新**”图标旁边的下拉菜单中选择站点。 控制台将显示所选站点的配置。

> **注意：**
>
> - 当主站点不可访问时，您无法访问与其关联的其他站点。
> - 切换到其他站点时，请确保您具有登录所需的权限或访问凭据。

站点配置后的登录体验

1. 打开 Web 浏览器。输入 `https://<address of the server hosting Web Studio>/Citrix/Studio`。
2. 从“**站点**”字段中选择一个站点。
3. 选择“**Windows 集成登录**”或输入“**用户名**”和“**密码**”进行登录。

> **注意：**
>
> 仅当所选站点启用了 Windows 集成登录时，此功能才可用。有关集成 Windows 身份验证的更多信息，请参阅管理身份验证。



使用 REST API 自动管理

借助 Citrix Virtual Apps and Desktops™ REST API，您可以自动管理 Citrix Virtual Apps and Desktops 部署中的资源。

Citrix Virtual Apps and Desktops REST API 可在 `<https://developer.cloud.com/citrixworkspace/citrix-daas/citrix-daas-rest-apis/docs/overview>` 获取。不适用于 Citrix Virtual Apps and Desktops 的 API 已相应标记。请遵循其中的指导来配置对 API 服务的访问，并使用 API 管理和优化您的资源。

安全私有访问与 Web Studio 的集成

简介

从 2407 开始，当您在 Web Studio 中单击“安全私有访问”链接时，“安全私有访问”控制台会在 Web Studio 控制台中打开。

以前，从 Web Studio 访问“安全私有访问”控制台时，它会在不同的选项卡中打开。

要在 Web Studio 中查看“安全私有访问”控制台，您必须执行以下两个步骤：

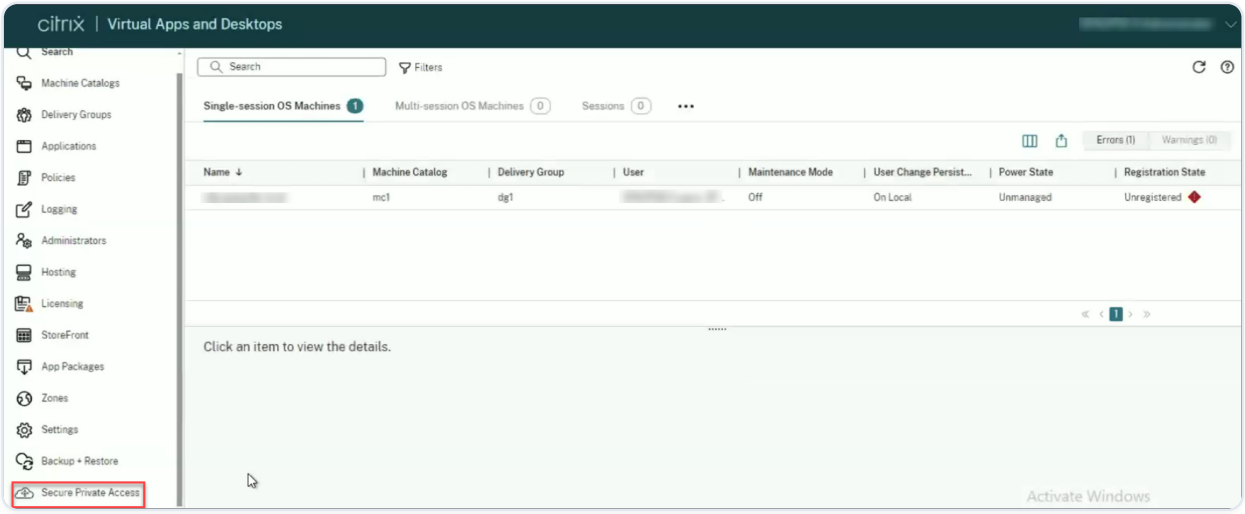
- 编辑 spa-config 文件以添加安全私有访问服务器
- 为安全私有访问控制台启用单点登录

编辑 spa-config 文件

1. 导航到 `C:\Program Files\Citrix\Web Studio\Sites\studio\assets\json` 并修改 `spa-config.json` 文件的内容。
2. 在 `<SpaServer>` 中，添加您的安全私有访问服务器 URL 并添加 `<“styleIsolation”: false>`，然后保存文件。



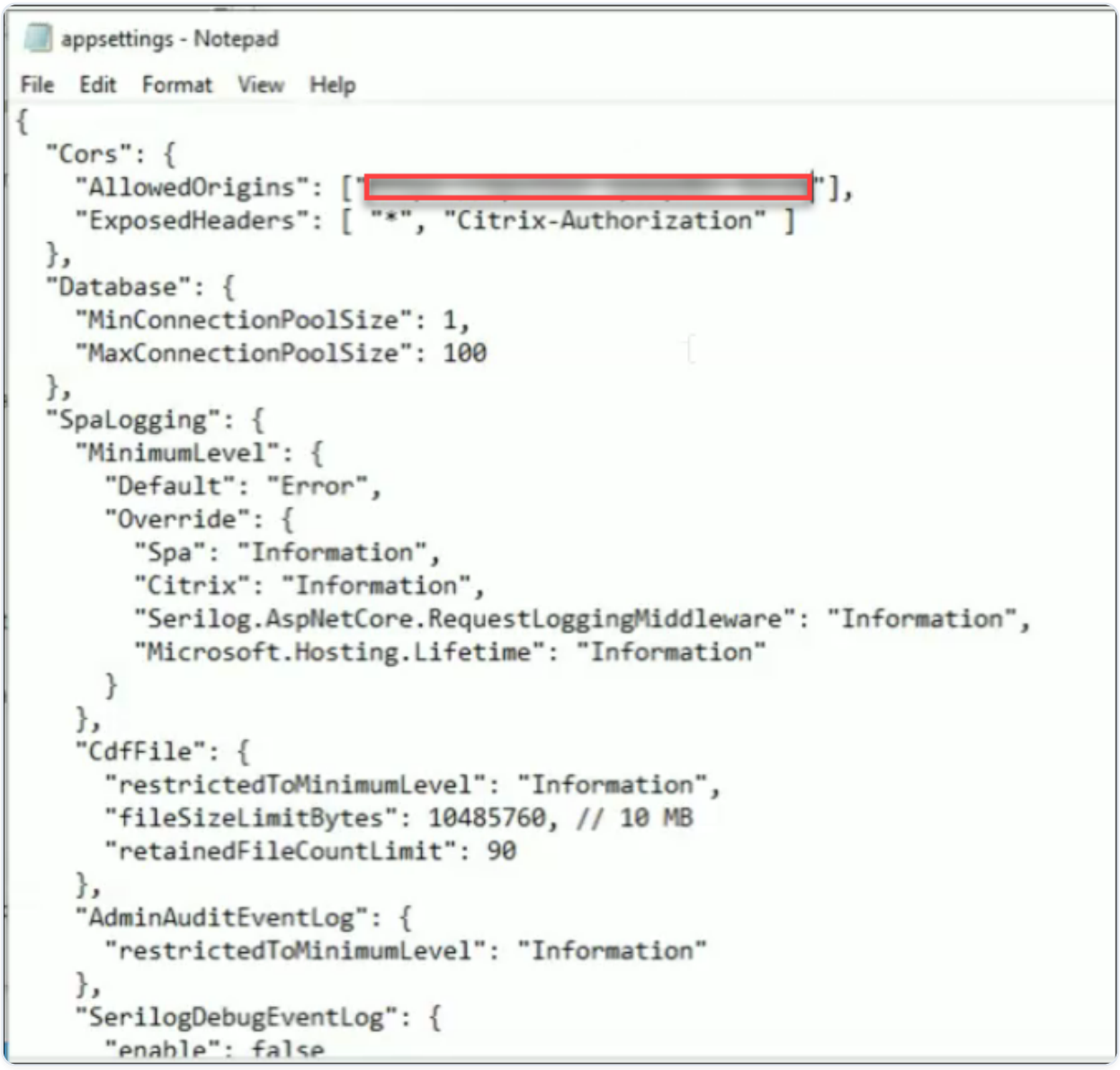
3. 刷新 Web Studio 控制台。
4. **安全私有访问**选项卡显示在 Web Studio 中。



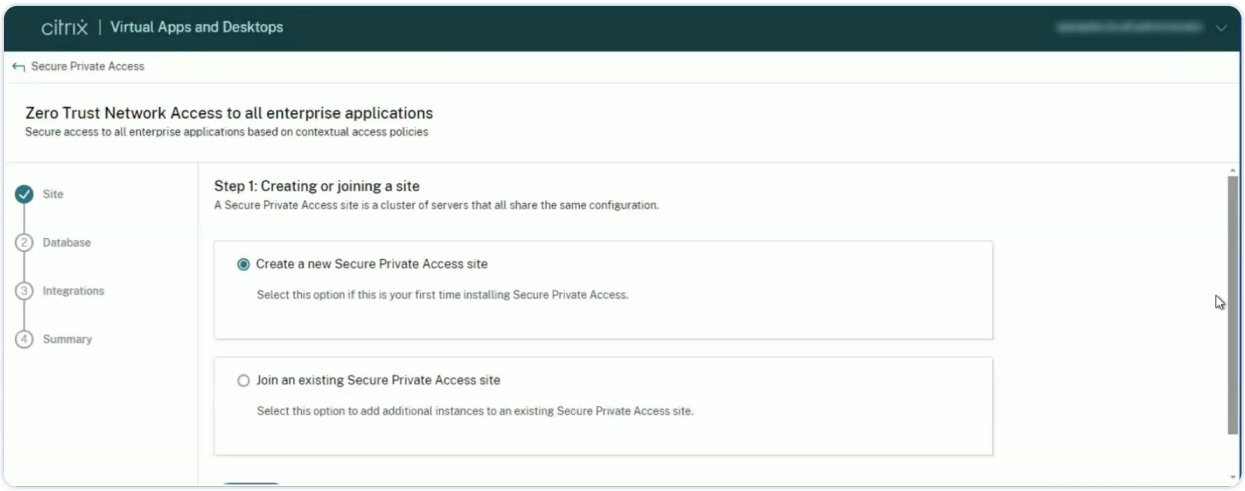
为安全私有访问控制台启用单点登录

当您单击 Web Studio UI 中的“安全私有访问”选项卡时，“安全私有访问”控制台必须直接打开。相反，它会将用户导航到登录页面。为避免这种情况并启用单点登录，请执行以下步骤：

1. 转到 `C:\Program Files\Citrix\Citrix Access Security\Admin\AdminService` 并修改 appsettings 文件中的内容。
2. 在 `<AllowedOrigins>` 参数中，提供 Web Studio URL 以允许来自 Web Studio 的所有流量进入 Secure Private Access，然后保存文件。



3. 在 Internet Information Services (IIS) 中，重新启动 Secure Private Access 服务器。
4. 在 Web Studio 中单击 Secure Private Access。Secure Private Access 将在 Web Studio 控制台中打开。



使用命令行安装

重要提示：

- 如果您正在升级，并且当前版本使用或安装了 Personal vDisk 或 AppDisks 软件，请参阅删除 PvD、AppDisks 和不受支持的主机。
- Citrix 会根据其合法权益（包括许可合规性）收集基本的许可数据。有关详细信息，请参阅 Citrix 许可数据。

简介

本文适用于在 Windows 操作系统计算机上安装组件。有关适用于 Linux 操作系统的 VDA 的信息，请参阅Linux Virtual Delivery Agent。

本文介绍了如何发出产品安装命令。在开始任何安装之前，请查看准备安装。该文章包含对可用安装程序的说明。

要查看命令执行进度和返回值，您必须是原始管理员或使用**以管理员身份运行**。有关详细信息，请参阅 Microsoft 命令文档。

作为直接使用安装命令的补充，产品 ISO 上提供了示例脚本，用于在 Active Directory 中的计算机上安装、升级或删除 VDA。有关详细信息，请参阅使用脚本安装 VDA。

如果您尝试在不受此 Citrix Virtual Apps and Desktops 版本支持的 Windows 操作系统版本上安装或升级，则会显示一条消息，引导您了解有关选项的信息。请参阅早期操作系统。

有关 Citrix 如何报告组件安装结果的信息，请参阅Citrix 安装返回代码。

使用完整产品安装程序

要访问完整产品安装程序的命令行界面：

1. 从 Citrix 下载产品包。访问下载站点需要 Citrix 帐户凭据。
2. 解压缩文件。或者，刻录 ISO 文件的 DVD。
3. 使用本地管理员帐户登录到要安装组件的服务器。
4. 将 DVD 插入驱动器或装载 ISO 文件。
5. 从介质上的 `\x64\XenDesktop Setup` 目录中，运行相应的命令。

   安装核心组件： 运行 `XenDesktopServerSetup.exe`，并使用 安装核心组件的命令行选项 中列出的选项。

   安装 VDA： 运行 `XenDesktopVDASetup.exe`，并使用 安装 VDA 的命令行选项 中列出的选项。

   安装 StoreFront： 在安装介质的 `x64 > StoreFront` 文件夹中运行 `CitrixStoreFront-x64.exe`。

   安装通用打印服务器： 请遵循 安装通用打印服务器的命令行选项 中的指导。

   安装联合身份验证服务： Citrix 建议使用图形界面。

   安装会话录制： 请遵循 会话录制 中的指导。

   安装工作区环境管理： 请遵循 工作区环境管理 中的指导。

   安装 Secure Private Access： 在安装介质的 `x64 > XenDesktop` Setup 文件夹中运行 `XenDesktopSPASetup.exe`。请遵循 安装 Secure Private Access 的命令行选项 中的指导。

安装核心组件的命令行选项

使用 `XenDesktopServerSetup.exe` 命令安装核心组件时，以下参数选项有效。有关选项的更多详细信息，请参阅 安装核心组件。

> **注意：**
>
> - 在使用用于安装核心组件的命令行选项时，请勿使用 `/exclude`。
> - 如果您使用 `/components` 升级一个组件，则其他组件也可能会升级。这是为了避免不同组件之间潜在的兼容性问题。

- 如果您只想升级一个组件，请使用该组件的独立安装程序。请参阅 升级和迁移。

- **/ceipoptin** *ceipoptin* 等等.

  启用 Call Home 数据和客户体验改善计划 (CEIP) 数据的收集。有效值为：

  - `DIAGNOSTIC`：选择此值以启用 Citrix 许可收集 Call Home 数据。
  - `ANONYMOUS`：选择此值以启用 Citrix 许可收集未识别的 CEIP 数据（不识别用户）。
  - `NONE`：选择此值以禁用 Citrix 许可收集 CEIP 数据。

  有关 Call Home 数据收集的详细信息，请参阅 Citrix Licensing Call Home。

  有关 CEIP 数据收集的更多详细信息，请参阅 Citrix Licensing Customer Experience Improvement Program。

  有关 CEIP 数据的更多详细信息，请参阅 Citrix Licensing CEIP data elements。

  有关许可证服务器许可数据的更多详细信息，请参阅 Citrix Licensing Data。

- **/components** *组件 ...*

  逗号分隔的用于安装或删除的组件列表。有效值为：

  - `CONTROLLER`：控制器
  - `WEBSTUDIO`：工作室
  - `DESKTOPDIRECTOR`: 导向器
  - `LICENSESERVER`：Citrix 许可证服务器
  - `SECUREPRIVATEACCESS`: 安全专用访问

要仅安装 VDA 并排除其他 Citrix 组件的安装，请指定 /components vda。

使用 VDAWorkstationCoreSetup_xxxx.exe 安装程序时，此选项无效。该安装程序无法安装 Citrix Workspace 应用程序或其他 Citrix 组件。

如果省略此选项，则会安装所有组件（如果还指定了 `/remove` 选项，则会删除所有组件）。

（在 2003 之前的版本中，有效值包括 `STOREFRONT™`。对于 2003 及更高版本，请使用使用完整产品安装程序 中提到的专用 StoreFront 安装命令）。

- **/仅限先决条件**

  将仅安装所选组件的必备项。不会安装任何 Citrix 产品组件。

- **/configure_firewall**

  如果 Windows 防火墙服务正在运行，即使防火墙未启用，也会打开正在安装的组件使用的 Windows 防火墙中的所有端口。如果您使用的是第三方防火墙或没有防火墙，则必须手动打开端口。

- **禁用体验指标**

  阻止在安装、升级或删除过程中收集的分析数据自动上传到 Citrix。

- **/help** 或 **/h**

  显示命令帮助。

- **/ignore_hw_check_failure**

  允许 Delivery Controller 安装或升级继续，即使硬件检查失败（例如，由于 RAM 不足）。有关详细信息，请参阅硬件检查。

- **/ignore_site_test_failure**

  仅在 Controller 升级期间有效。通常，任何站点测试失败都会被忽略，升级会继续进行。如果省略（或设置为 false），任何站点测试失败都会导致安装程序失败，而不会执行升级。默认值 = false

  在升级期间，如果检测到不受支持的 SQL Server 版本，则此选项将被忽略。有关详细信息，请参阅检查 SQL Server 版本。

- **/installdir** ***目录***

  现有空目录，组件将安装在此处。默认值 = `c:\Program Files\Citrix`。

- **/日志路径** ***路径***

  日志文件位置。指定的文件夹必须存在。安装程序不会创建它。默认值 = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  仅在安装 Director 时有效。禁用使用 Windows 远程协助的用户影子功能。

- **/noreboot**（禁止重新启动）

  防止安装后重新启动。（对于大多数核心组件，默认情况下不启用重新启动。）

- **/noresume**（禁止恢复）

默认情况下，如果在安装过程中需要重新启动计算机，安装程序会在重新启动完成后自动恢复。要覆盖默认设置，请指定 `/noresume`。如果您必须重新装载介质或希望在自动化安装期间捕获信息，这会很有帮助。

- **/无SQL**

  防止在安装 Controller 的服务器上安装 Microsoft SQL Server Express。如果省略此选项，则会安装 SQL Server Express 作为站点数据库。

  此选项不影响用于本地主机缓存的 SQL Server Express LocalDB 的安装。

- **/quiet** 或 **/passive**

  安装期间不显示用户界面。安装过程的唯一证据在 Windows 任务管理器中。如果省略此选项，则会启动图形界面。

- **/删除**

  删除使用 `/components` 选项指定的核心组件。

- **/删除所有**

  删除所有已安装的核心组件。

- **/发送体验指标**

  自动将安装、升级或删除期间收集的分析数据发送给 Citrix。如果省略此选项（或指定了 `/disableexperiencemetrics`），则分析数据将在本地收集，但不会自动发送。

- **/临时目录** *目录*

  安装期间用于存放临时文件的目录。默认值 = `c:\Windows\Temp`。

- **/Xen应用**

  安装 Citrix Virtual Apps。如果省略此选项，则安装 Citrix Virtual Apps and Desktops™。

安装核心组件的示例

以下命令在服务器上安装 Delivery Controller™、Studio、Citrix Licensing 和 SQL Server Express。组件通信所需的防火墙端口将自动打开。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,webstudio,licenseserver /configure_firewall
```

以下命令在服务器上安装 Citrix Virtual Apps™ Controller、Studio 和 SQL Server Express。组件通信所需的防火墙端口将自动打开。

`\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components controller,webstudio /configure_firewall`

以下命令在服务器上安装 Delivery Controller、Secure Private Access 和 SQL Server Express。组件通信所需的防火墙端口将自动打开。

`\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall`

如果您从 Citrix Virtual Apps and Desktops 2407 版升级到 2411 或更高版本，或者执行 2411 或更高版本的新安装，请首先将许可证服务器更新到最新版本（版本 11.2.17 build 51000）。然后，升级 Delivery Controller。否则将导致命令行安装和升级失败。运行以下命令以升级许可证服务器和 Delivery Controller、Studio 和 Citrix Director 等组件（假设您位于已装载 ISO 中的 \x64 文件夹内）。

1. 运行以下命令：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   如果您已将许可二进制文件复制到任何本地驱动器，请运行以下命令：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. 运行以下命令：

   ```
   \x64\XenDesktop Setup\XenDesktopServerSetup.exe /components
   "CONTROLLER,WEBSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
   ```

使用独立 VDA 安装程序

访问下载站点需要 Citrix 帐户凭据。您必须在开始安装之前拥有提升的管理权限，或者使用**以管理员身份运行**。

1. 从 Citrix 下载相应的软件包：
   - 多会话操作系统虚拟投递代理：`VDAServerSetup_xxxx.exe`
   - 单会话操作系统虚拟投递代理：`VDAWorkstationSetup_xxxx.exe`
   - 单会话操作系统核心服务虚拟投递代理：`VDAWorkstationCoreSetup_xxxx.exe`
2. 要么先将文件从包中提取到现有目录，然后运行安装命令，要么直接运行包。

要在安装文件之前提取它们，请使用 `/extract` 和绝对路径，例如 `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`。目录必须存在。否则，提取将失败。然后，在单独的命令中，使用本文中列出的有效选项运行相应的命令。

- 对于 `VDAServerSetup_XXXX.exe`，运行 `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
- 对于 `VDAWorkstationCoreSetup_XXXX.exe`，运行 `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
- 对于 `VDAWorkstationSetup_XXXX.exe`，运行 `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

要运行下载的包，请运行其名称：`VDAServerSetup.exe`、`VDAWorkstationSetup.exe` 或 `VDAWorkstationCoreSetup.exe`。使用本文中列出的有效选项。

如果您熟悉完整产品安装程序：

- 运行独立的 `VDAServerSetup.exe` 或 `VDAWorkstationSetup.exe` 安装程序，就像它是 `XenDesktopVdaSetup.exe` 命令一样，除了名称不同。
- `VDAWorkstationCoreSetup.exe` 安装程序有所不同，因为它支持其他安装程序可用选项的子集。

逗号分隔的用于安装或删除的组件列表。有效值为：

- `VDA`: 虚拟投递代理
- `CSA`: Citrix 安全访问™ 客户端
- `PLUGINS`: 适用于 Windows 的 Citrix Workspace™ 应用程序
- `UPL`: Citrix 用户个性化层（仅适用于 WS VDA）
- `SRAGENT`: 会话录制代理
- `ASSISTANTAPP`: Citrix Assistant App（仅适用于 WS VDA）
- `CEAL`: Citrix 弹性应用分层（仅适用于 TS VDA）

要安装 VDA 和适用于 Windows 的 Citrix Workspace 应用程序，请指定 /components vda,plugins 或根本不指定任何组件。

从该版本开始，Citrix Device Trust、Citrix uberAgent 和 Citrix Workspace Environment Management™ (WEM) Agent 已集成到默认 VDA 安装中。这些组件作为 VDA 设置的一部分静默安装，不再作为单独的组件进行管理。

> **注意：**
>
> 如果在环境中检测到现有独立版本的 Citrix uberAgent®，安装程序将不会安装、升级或卸载它。
>
> 要仅安装 VDA 并排除安装其他 Citrix 组件，请指定 `/components vda`。

使用 VDAWorkstationCoreSetup_xxxx.exe 安装程序时，此选项无效。该安装程序无法安装 Citrix Workspace 应用程序或其他 Citrix 组件。

用于安装 VDA 的命令行选项

以下选项适用于以下一个或多个命令（安装程序）：`VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe` 和 `VDAWorkstationCoreSetup_xxxx.exe`。

有关选项的更多详细信息，请参阅 安装 VDA。

- **/components** *组件*\[,*组件*\]

  逗号分隔的用于安装或删除的组件列表。有效值为：

  - `VDA`：虚拟投递代理
  - `PLUGINS`：适用于 Windows 的 Citrix Workspace 应用程序
  - `CSA`：Citrix 安全访问客户端
  - `UPL`：Citrix 用户个性化层（仅适用于 WS VDA）
  - `SRAGENT`：会话录制代理
  - `ASSISTANTAPP`：Citrix Assistant App（仅适用于 WS VDA）
  - `CEAL`：Citrix 弹性应用分层（仅适用于 TS VDA）

要安装 VDA 和适用于 Windows 的 Citrix Workspace 应用程序，请指定 `/components vda,plugins, CSA, UPL` 或根本不指定任何组件。如果未指定任何组件，则默认仅安装 VDA、SRAGENT 和 ASSISTANTAPP。

要仅安装 VDA 并排除安装 Citrix Workspace 应用程序和其他组件，请指定 `/components vda`。

此选项在使用 `VDAWorkstationCoreSetup_xxxx.exe` 安装程序时无效。该安装程序无法安装 Citrix Workspace 应用程序。

- **仅限先决条件**

  将仅安装所选组件的必备项。不会安装任何 Citrix 产品组件。

- **controllers** "*控制器* \[*控制器*\]"

  VDA 可以与之通信的 Controller 的 FQDN，以空格分隔，并用直引号括起来。请勿同时指定 `/site_guid` 和 `/controllers` 选项。

- **禁用体验指标**

  阻止自动上传在安装、升级或删除期间收集到 Citrix 的分析数据。

- **/enable_hdx_ports**

  如果检测到 Windows 防火墙服务，即使防火墙未启用，也会打开 VDA 和已启用功能（Windows 远程协助除外）所需的 Windows 防火墙中的端口。如果您使用的是其他防火墙或没有防火墙，则必须手动配置防火墙。有关端口信息，请参阅网络端口。

  要打开 HDX 自适应传输使用的 UDP 端口，除了此 `/enable_hdx_ports` 选项外，还请指定 `/enable_hdx_udp_ports` 选项。

- **/enable_hdx_udp_ports**

  如果检测到 Windows 防火墙服务，即使防火墙未启用，也会在 Windows 防火墙中打开 HDX 自适应传输使用的 UDP 端口。如果您使用不同的防火墙或不使用防火墙，则必须手动配置防火墙。有关端口信息，请参阅网络端口。

  要打开 VDA 使用的额外端口，除了此 `/enable_hdx_udp_ports` 选项外，还请指定 `/enable_hdx_ports` 选项。

- **/enable_hdx_tls_dtls**

  为 HDX™ Direct V1 打开 TCP 和 UDP 端口 443。

- **/enable_real_time_transport**

  启用或禁用将 UDP 用于音频数据包（用于音频的实时音频传输）。启用此功能可以提高音频性能。如果希望在检测到 Windows 防火墙服务时自动打开 UDP 端口，请包含 `/enable_hdx_ports` 选项。

- **/enable_remote_assistance**

启用 Windows 远程协助中的影子功能，以便与 Director 结合使用。如果指定此选项，Windows 远程协助将在防火墙中打开动态端口。

- **/enablerestore 或 /enablerestorecleanup**

  （仅适用于单会话 VDA）如果 VDA 安装或升级失败，则启用自动返回到还原点。

  如果安装/升级成功完成：

  - `/enablerestorecleanup` 指示安装程序删除还原点。
  - `/enablerestore` 指示安装程序保留还原点，即使未使用该还原点。

  有关详细信息，请参阅安装或升级失败时恢复。

- **/ENABLE_SECURE_DEFAULTS**

  将各种功能的默认设置从启用更改为禁用，以实现更安全的开箱即用配置。相关功能包括：客户端驱动器重定向、特殊文件夹重定向、拖放、客户端 TWAIN 设备重定向、客户端 USB 即插即用设备重定向、客户端打印机重定向、客户端剪贴板重定向和客户端麦克风重定向。

- **/enable_ss_ports**

  如果在检测到 Windows 防火墙服务时，即使防火墙未启用，也会打开 Windows 防火墙中屏幕共享所需的端口。如果您使用不同的防火墙或不使用防火墙，则必须手动配置防火墙。

- **/SKIPHDXDRIVERCHECK**

  跳过对 VDA 元安装程序中 HDX™ 驱动程序的检查。

- **/排除** “*组件*”

  阻止安装一个或多个用逗号分隔的可选组件，每个组件都用直引号括起来。例如，在不受 MCS 管理的映像上安装或升级 VDA 不需要计算机身份服务组件。有效值如下：

多会话操作系统	单会话操作系统	单会话操作系统核心服务
`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`
`Citrix Backup and Restore`	`Citrix Backup and Restore`	`Citrix Browser Content Redirection`
`Citrix deviceTRUST®`	`Citrix deviceTRUST`	`Citrix deviceTRUST`
`uberAgent®`	`uberAgent`	`uberAgent`

多会话操作系统	单会话操作系统	单会话操作系统核心服务
Citrix Secure Access Client	Citrix Secure Access Client	Citrix Secure Access Client
Citrix Workspace Environment Management™ Agent	Citrix Workspace Environment Management Agent	Citrix Workspace Environment Management Agent
Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Personalization for App-V - VDA
Citrix MCS IODriver	Citrix MCS IODriver	Citrix Telemetry Service
Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA	Citrix Universal™ Print Client
Citrix Profile Management	Citrix Profile Management	Citrix Vda Log Capture Service
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in	CSE Component
Citrix Rendezvous V2	Citrix Rendezvous V2	Director VDA Plug-in
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in
Citrix Vda Log Capture Service	Citrix Vda Log Capture Service	VDA WMI Proxy Plug-in
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
CSE Component	CSE Component	
Director VDA Plug-in	Director VDA Plug-in	

多会话操作系统	单会话操作系统	单会话操作系统核心服务
`Machine Identity Service`	`Machine Identity Service`	
`Machine Management Provider`	`Machine Management Provider`	
`VDA Monitor Plug-in`	`User Personalization Layer`	
`VDA WMI Proxy Plug-in`	`VDA Monitor Plug-in`	
	`VDA WMI Proxy Plug-in`	
`Citrix App Protection Component`	`Citrix App Protection Component`	`Citrix App Protection Component`
`Citrix HyperV Filter Driver`	`Citrix HyperV Filter Driver`	
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Session Recording Agent`	`Session Recording Agent`	
`Elastic App Layering`	`Citrix Assistant App`	

将 Citrix Profile Management 从安装中排除 (`/exclude "Citrix Profile Management"`) 会影响使用 Citrix Director 对 VDA 进行监视和故障排除。在“**用户详细信息**”和“**端点**”页面上，“个性化”面板和“登录持续时间”面板将失败。在“**控制板**”和“**趋势**”页面上，“平均登录持续时间”面板仅显示已安装 Profile Management 的计算机的数据。

即使您使用的是第三方用户配置文件管理解决方案，Citrix 仍建议您安装并运行 Citrix Profile Management Service。不需要启用 Citrix Profile Management Service。

如果同时指定 `/exclude` 和 `/includeadditional` 且组件名称相同，则不会安装该组件。

使用 `VDAWorkstationCoreSetup.exe` 安装程序时，此选项无效。该安装程序会自动排除其中许多项目。

- **/h 或 /help**

显示命令帮助。

- **/includeadditional** "*组件*"\[,"*组件*"\]

  包括安装一个或多个用直引号括起来的逗号分隔的可选组件。当您创建远程电脑访问部署并希望安装默认情况下不包含的其他组件时，此选项会很有帮助。有效值如下：

多会话操作系统	单会话操作系统
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

  如果同时指定 `/exclude` 和 `/includeadditional` 且组件名称相同，则不会安装该组件。

- **/installdir** *目录*

  将安装组件的现有空目录。默认值 = `c:\Program Files\Citrix`。

- **/install_mcsio_driver**

  请勿使用。请改用 `/includeadditional "Citrix MCS IODriver"` 或 `/exclude "Citrix MCS IODriver"`。

- **/logpath** *路径*

日志文件位置。指定的文件夹必须存在。安装程序不会创建它。默认值 = "`%TEMP%\Citrix\XenDesktop Installer`"

此选项在图形界面中不可用。

- **/主映像**

  仅在虚拟机上安装 VDA 时有效。将 VDA 设置为用于创建其他计算机的映像。此选项等同于 `/mastermcsimage`。

  使用 `VDAWorkstationCoreSetup_xxxx.exe` 安装程序时，此选项无效。

- **/MCS主映像**

  指定此计算机将用作 Machine Creation Services 的映像。此选项等同于 `/masterimage`。

- **/PVS主映像**

  指定此计算机将用作映像，通过 Citrix Provisioning™ 或第三方预配工具（例如 Microsoft System Center Configuration Manager）来预配 VM。

- **/websocket令牌** *WebSocket令牌*

  创建 Web Socket VDA。WebSocketToken 用于所需的令牌。

- **/websockettokenfile** *包含 WebSocket 令牌的文件*

  创建 Web Socket VDA。*FileContainingWebSockToken* 用于包含所需令牌的文件。

- **/websocket令牌stdin** <*WebSocket令牌*

  创建 Web Socket VDA。<*WebSocketToken* 用于通过 STDIN 传入的所需令牌。

- **/no_mediafoundation_ack**

  确认未安装 Microsoft Media Foundation，并且多个 HDX 多媒体功能将不会安装且无法工作。如果省略此选项且未安装 Media Foundation，则 VDA 安装将退出，因为未满足先决条件。大多数受支持的 Windows 版本都已安装 Media Foundation，N 版本除外。如果*手动*启用“Windows 功能”>“媒体功能”，则 Citrix Meta Installer 查找的注册表项可能没有设置值。在开始安装过程之前，请检查 `SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` 注册表项以确认该值存在且不为空。

- **/nodesktopexperience**（不安装桌面体验）

  增强桌面体验功能不再可用。如果指定此选项（和策略设置），则会将其忽略。

  仅在为多会话操作系统安装 VDA 时有效。阻止启用增强桌面体验功能。此功能也通过增强桌面体验 Citrix 策略设置进行控制。

- **/noreboot**（禁止重新启动）

  阻止安装后重新启动。VDA 必须在重新启动后才能使用。

- **/noresume**（禁止恢复）

  默认情况下，如果在安装过程中需要重新启动计算机，安装程序会在重新启动完成后自动恢复。要覆盖默认设置，请指定 `/noresume`。如果您必须重新装载介质或希望在自动化安装期间捕获信息，这会很有帮助。

- **/物理机**

  将此参数与 `/remotepc` 一起用于 RemotePC 安装。否则，VDA 在某些用户场景中可能无法按预期运行。

- **/portnumber** *端口*

  仅当指定了 `/reconfig` 选项时有效。用于启用 VDA 与 Controller 之间通信的端口号。除非是端口 80，否则以前配置的端口将被禁用。

- **/proxyconfig** "*地址或 PAC 文件路径*"

  如果您计划在您的环境中使用 Rendezvous V2 协议以及 Gateway Service 等服务，并且您的网络中存在用于出站连接的非透明代理，请在此处指定代理。仅支持 HTTP 代理。用于 Rendezvous 协议的代理地址或 PAC 文件路径。此命令行会自动安装 Citrix Rendezvous V2，如同使用了 /includeadditional "Citrix Rendezvous V2"。有关功能详细信息，请参阅 Rendezvous 协议。

  - 代理地址格式：`http://<url-or-ip>:<port>`
  - PAC 文件格式：`http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** 或 **/passive**

  安装期间不会出现用户界面。安装和配置过程的唯一证据在 Windows 任务管理器中。如果省略此选项，则会启动图形界面。

- **/重新配置**

  与 `/portnumber`、`/controllers` 或 `/enable_hdx_ports` 选项一起使用时，自定义以前配置的 VDA 设置。如果指定此选项但未同时指定 `/quiet` 选项，则会启动用于自定义 VDA 的图形界面。

- **/远程电脑**

  仅适用于远程 PC 访问部署（单会话操作系统）或代理连接（多会话操作系统）。不包括安装任何附加组件（请参阅带有 `/exclude` 和 `/includeadditional` 选项的组件列表）。

使用 `VDAWorkstationCoreSetup.exe` 安装程序时，此选项无效。该安装程序会自动排除这些组件的安装。

`/remotepc` 与 `/servervdi` 选项不兼容。

- **/删除**

  删除使用 `/components` 选项指定的组件。

- **/remove_appdisk_ack**

  授权 VDA 安装程序卸载 AppDisks™ VDA 插件（如果已安装）。

- **/remove_pvd_ack**

  授权 VDA 安装程序卸载 Personal vDisk（如果已安装）。

- **/删除所有**

  删除 VDA。它不会删除 Citrix Workspace 应用程序（如果已安装）。

- **/REMOVEALLWITHCWA**

  删除 CWA 以及 VDA。

- **/发送体验指标**

  在安装、升级或删除过程中自动将收集到的分析数据发送给 Citrix。如果省略此选项（或指定了 `/disableexperiencemetrics` 选项），则分析数据将在本地收集，但不会自动发送。

- **/服务器VDI**

  在受支持的 Windows 多会话计算机上安装用于单会话操作系统的 VDA。在 Windows 多会话计算机上安装用于多会话操作系统的 VDA 时，请省略此选项。

  使用此选项之前，请参阅 Server VDI。

  仅将此选项与完整产品 VDA 安装程序一起使用。

- **/站点GUID** *GUID*

  站点的 Active Directory 组织单位 (OU) 的全局唯一标识符。当您使用 Active Directory 进行发现时（自动更新是推荐的默认发现方法），这会将虚拟桌面与站点关联。站点 GUID 是 Studio 中显示的站点属性。请勿同时指定 `/site_guid` 和 `/controllers` 选项。

- **/临时目录** *目录*

  安装期间用于存放临时文件的目录。默认值 = `c:\Windows\Temp`。

此选项在图形界面中不可用。

- **/虚拟机**

  仅在 VM 上安装 VDA 时有效。覆盖安装程序对物理机的检测，因为传递给 VM 的 BIOS 信息使其显示为物理机。

  此选项在图形界面中不可用。

- **/XenDesktop云**

  指示 VDA 安装在 Citrix DaaS (Citrix Cloud™) 部署中。

安装 VDA 的示例

使用完整产品安装程序安装 VDA：

以下命令将为单会话操作系统和 Citrix Workspace 应用程序安装 VDA 到 VM 上的默认位置。此 VDA 将用作映像并使用 MCS 预配 VM。VDA 将首先在域 `mydomain` 中名为 `Contr-Main` 的服务器上向 Controller 注册。VDA 将使用用户个性化层和 Windows 远程协助。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /
controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional
"user personalization layer" /mastermcsimage /enable_remote_assistance
```

使用 VDAWorkstationCoreSetup 独立安装程序安装单会话操作系统 VDA：

以下命令在单会话操作系统上安装核心服务 VDA，用于远程 PC 访问或 VDI 部署。Citrix Workspace 应用程序和其他非核心服务未安装。指定了 Controller 的地址，Windows 防火墙服务中的端口将自动打开。管理员将处理重新启动。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /
enable_hdx_ports /noreboot
```

自定义 VDA

安装 VDA 后，您可以自定义多项设置。从产品介质上的 `\x64\XenDesktop Setup` 目录中，运行 `XenDesktopVdaSetup.exe`，使用以下一个或多个选项，这些选项在 安装 VDA 的命令行选项 中进行了描述。

- `/reconfigure`（自定义 VDA 时必需）
- `/h` 或 `/help`
- `/quiet`
- `/noreboot`

- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

排除 VDA 故障

- 在交付组的 Studio 显示中，**详细信息**窗格中的**已安装 VDA 版本**条目可能不是计算机上安装的版本。计算机的 Windows 程序和功能显示屏会显示实际的 VDA 版本。
- VDA 安装后，必须先向 Delivery Controller 注册，然后才能向用户交付应用程序或桌面。

  要了解 VDA 注册方法以及如何排查注册问题，请参阅 VDA 注册。

安装 Universal Print Server 的命令行选项

以下选项对 `XenDesktopPrintServerSetup.exe` 命令有效。

- **/enable_upsserver_port**

如果未指定此选项，安装程序将从图形界面显示**防火墙**页面。选择**自动**让安装程序自动添加 Windows 防火墙规则，或选择**手动**让管理员手动配置防火墙。

在打印服务器上安装软件后，请按照 Citrix Universal Print Server (UPS) 中的指导配置 Universal Print Server。

安装 Secure Private Access 的命令行选项

以下选项对两者均有效：

1. CVAD 安装程序：`XenDesktopSPASetup.exe`
2. SPA 本地安装程序：`SecurePrivateAccessSetup_XXXX.exe`

- **/enable_spa_ports**

  如果检测到 Windows 防火墙服务，即使防火墙未启用，也会打开 Secure Private Access 所需的 Windows 防火墙端口。如果您使用的是其他防火墙或没有防火墙，则必须手动配置防火墙。有关端口信息，请参阅 网络端口。

- **/无 SQL**

  阻止在安装 Secure Private Access 的服务器上安装 Microsoft SQL Server Express。如果省略此选项，则会安装 SQL Server Express 作为站点数据库使用。

- **/help 或 /h 或 /?**

  显示命令帮助

- **/noreboot**（禁止重新启动）

  阻止安装后重新启动。Secure Private Access 必须在重新启动后才能使用。

- **/quiet 或 /passive**

  安装期间不会出现用户界面。安装和配置过程的唯一证据在 Windows 任务管理器中。如果省略此选项，则会启动图形界面。

- **/删除**

  删除安全私有访问。

有关这些选项的更多详细信息，请参阅 Secure Private Access 安装程序。

更多信息

有关 Citrix 如何报告组件安装结果的信息，请参阅 Citrix 安装返回代码。

安装 VDA

> **重要提示：**
>
> - 如果您正在升级，并且当前版本安装了 Personal vDisk 或 AppDisks 软件，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/upgrade-migrate/preparation.html#remove-pvd-appdisks-and-unsupported-hosts)。
> - Citrix® 分发的二进制文件现已签名。签名二进制文件表示它们已通过 Citrix 生成的证书或真实的第三方证书进行验证。

> 适用于 Windows 计算机的 VDA 有两种类型：适用于多会话操作系统的 VDA 和适用于单会话操作系统的 VDA。（有关适用于 Linux 计算机的 VDA 的信息，请参阅 (/zh-cn/linux-virtual-delivery-agent.html) 文档。）

在开始安装之前，请查看 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-prepare.html) 并完成所有准备任务。

在安装 VDA 之前，请安装核心组件。您也可以在安装 VDA 之前创建站点。

本文介绍了安装 VDA 时的安装向导序列。提供了命令行等效项。有关详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-core/install-command.html)。

步骤 1. 下载产品软件并启动向导

如果您使用的是完整产品安装程序：

1. 如果您尚未下载产品 ISO：
   - 使用您的 Citrix 帐户凭据访问 Citrix Virtual Apps and Desktops™ 下载页面。下载产品 ISO 文件。
   - 解压缩文件。或者，刻录 ISO 文件的 DVD。
2. 在要安装 VDA 的映像或计算机上使用本地管理员帐户。将 DVD 插入驱动器或装载 ISO 文件。如果安装程序未自动启动，请双击装载驱动器上的 **AutoSelect** 应用程序。

   安装向导启动。

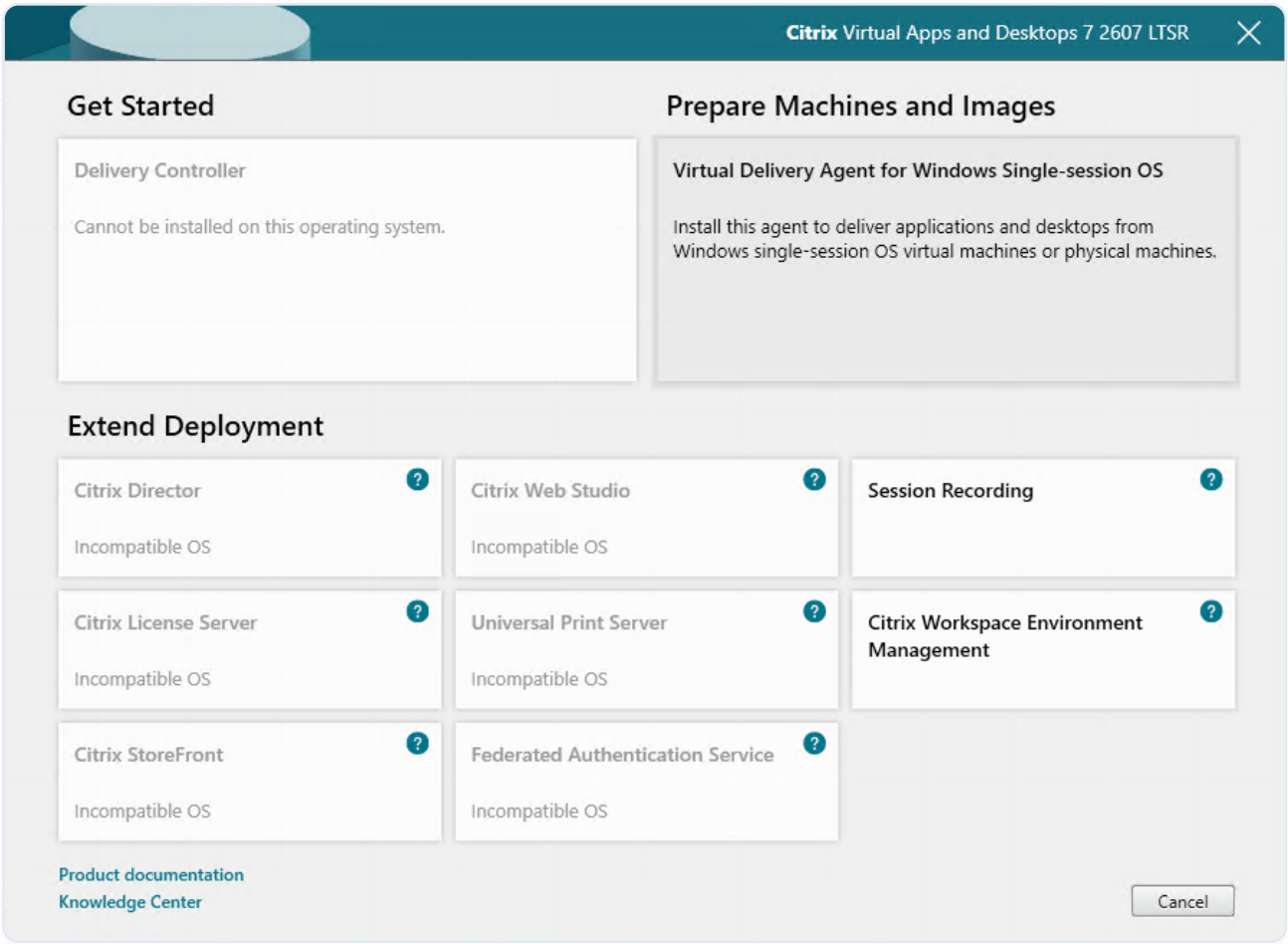
步骤 2. 选择要安装的产品

组件安装程序中的产品安装页面 (/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/product-selector2-75.png)

在要安装的产品（Citrix Virtual Apps 或 Citrix Virtual Desktops）旁边单击“**开始**”。（如果计算机已安装 Citrix Virtual Apps 或 Citrix Virtual Desktops 组件，则此页面不会出现。）

命令行选项：`/xenapp` 以安装 Citrix Virtual Apps。如果省略此选项，则安装 Citrix Virtual Desktops。

步骤 3. 选择 VDA



选择“**Virtual Delivery Agent**”条目。安装程序知道它是在单会话还是多会话操作系统上运行，因此它只提供适当的 VDA 类型。

例如，当您在 Windows Server 2019 计算机上运行安装程序时，适用于多会话操作系统的 VDA 选项可用。不提供适用于单会话操作系统的 VDA 选项。

如果您尝试在不受此 Citrix Virtual Apps and Desktops™ 版本支持的操作系统上安装（或升级到）Windows VDA，将显示一条消息，引导您了解有关选项的信息。

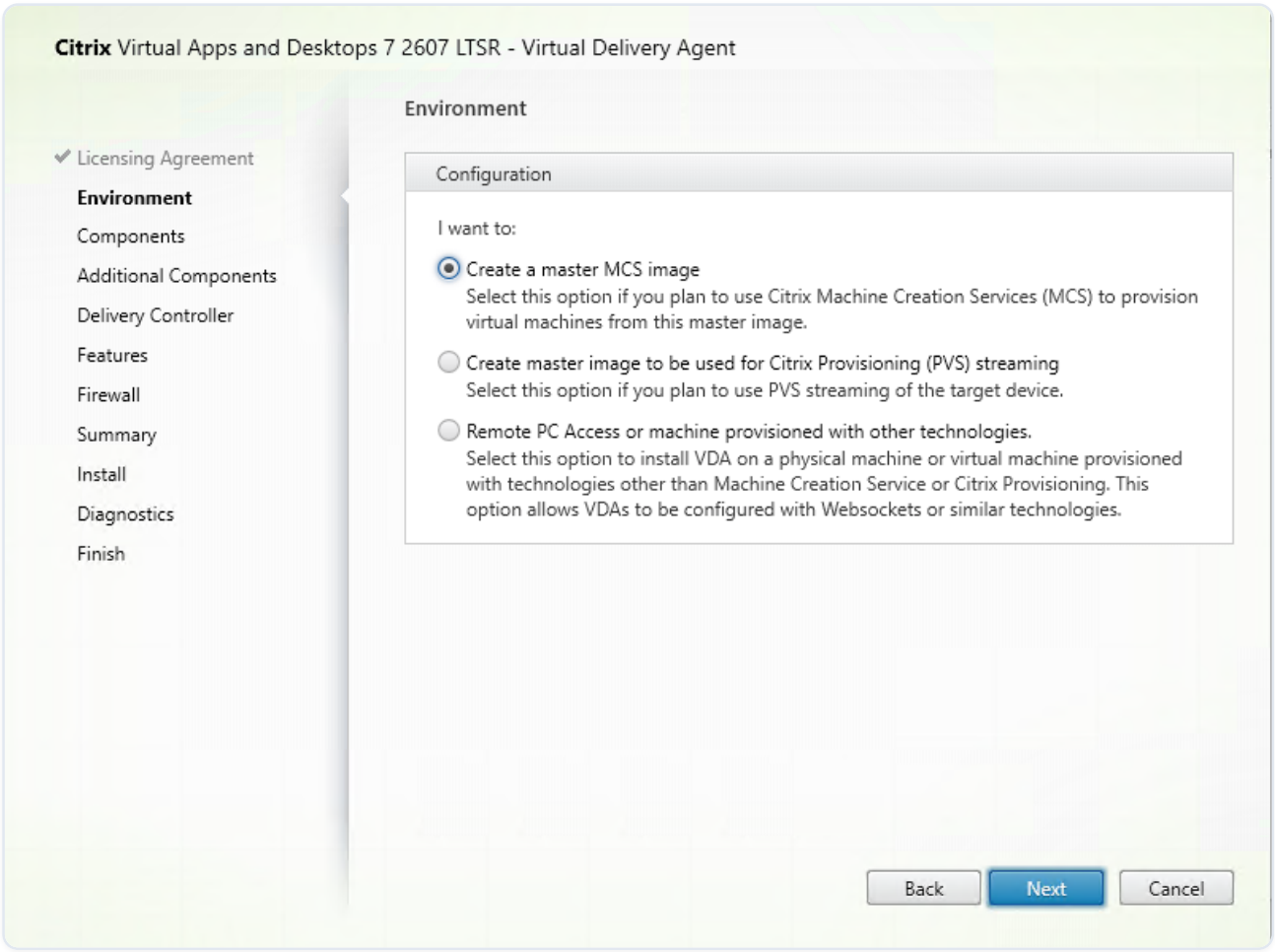
如果您使用的是独立软件包：

1. 使用您的 Citrix 帐户凭据访问 Citrix Virtual Apps and Desktops™ 下载页面。下载相应的软件包：
   - `VDAServerSetup_2607.exe`：多会话操作系统 VDA *版本*
   - `VDAWorkstationSetup_2607.exe`：单会话操作系统 VDA *版本*
   - `VDAWorkstationCoreSetup_2607.exe`：单会话操作系统核心服务 VDA *版本*
   - `VDASingleSessionCoreSetup_2607.exe`：新的单会话操作系统核心服务 VDA 版本

2. 右键单击软件包并选择“**以管理员身份运行**”。

   安装向导启动。

步骤 4. 指定 VDA 的使用方式



在“**环境**”页面上，指定您计划如何使用 VDA，并指明您是否将此计算机用作预配更多计算机的映像。

您选择的选项会影响自动安装哪些 Citrix Provisioning™ 工具（如果有），以及 VDA 安装程序“附加组件”页面上的默认值。

安装 VDA 时，会自动安装多个 MSI（预配及其他）。防止其安装的唯一方法是在命令行安装中使用 `/exclude` 选项。

选择以下选项之一：

- **创建主 MCS 映像：** 如果您计划使用 Machine Creation Services™ 预配 VM，请选择此选项以在 VM 映像上安装 VDA。此选项将安装 Machine Identity Service。这是默认选项。

  命令行选项：`/mastermcsimage` 或 `/masterimage`

> **重要提示：**
>
> 安装介质或 ISO 映像必须在本地装载。不支持从网络驱动器装载 ISO 映像以安装软件。

- **使用 Citrix Provisioning 或第三方预配工具创建主映像：** 如果您计划使用 Citrix Provisioning 或第三方预配工具（例如 Microsoft System Center Configuration Manager）预配 VM，请选择此选项以在 VM 映像上安装 VDA。

  命令行选项：`/masterpvsimage`

- （仅在多会话操作系统计算机上显示）**启用与服务器的代理连接：** 选择此选项可在物理或虚拟机上安装 VDA，该虚拟机不会用作预配其他计算机的映像。

  命令行选项：`/remotepc`

- （仅在单会话操作系统计算机上显示）**启用远程电脑访问：** 选择此选项可在物理计算机上安装 VDA，以用于远程电脑访问。

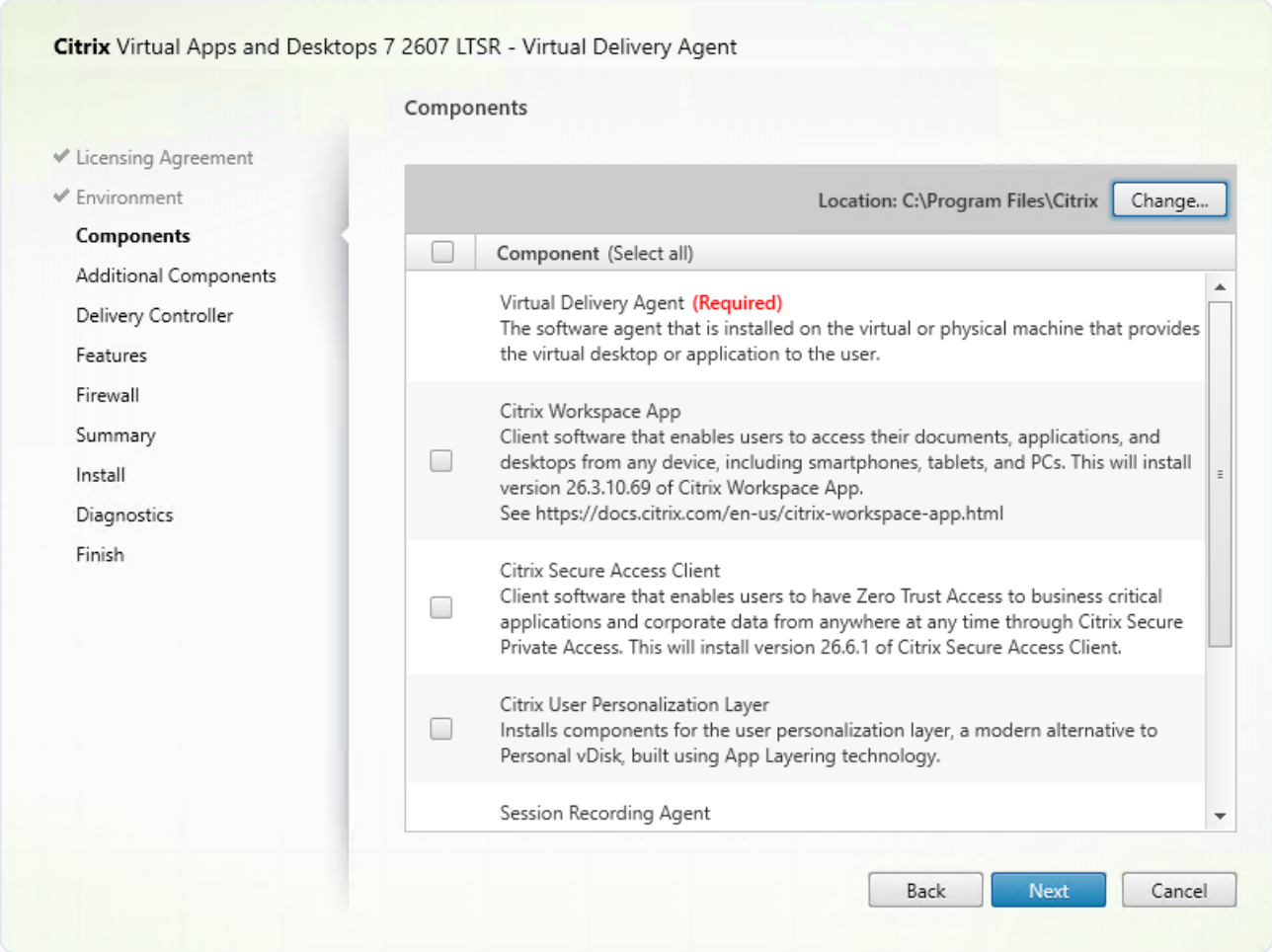
  命令行选项：`/remotepc`

单击“**下一步**”。

此页面不显示：

- 如果您正在升级 VDA
- 如果您使用的是 `VDAWorkstationCoreSetup_xxxx.exe`、`VDASingleSessionCoreSetup_xxxx.exe`、`VDAServerSetup_xxxx.exe` 或 `VDAWorkstationSetup_xxxx.exe` 安装程序

步骤 5. 选择要安装的组件和安装位置



> **注意：**
>
> 从版本 2603 开始，以前在“可选软件”页面上列出的组件已移至“组件”页面。

> 在**组件**页面上：

- **位置：** 默认情况下，VDA 安装在 `C:\Program Files\Citrix` 中。此默认设置适用于大多数部署。如果您指定不同的位置，则该位置必须具有网络服务的 `execute` 权限。
- **组件：** 默认情况下，会话录制代理和 Citrix Virtual Desktop Assistant 与 VDA 一起安装。如果您使用的是 `VDAWorkstationCoreSetup.exe` 安装程序或 `VDASingleSessionCoreSetup.exe` 安装程序，则只会安装 VDA，并且不会显示其他组件。

单击“**下一步**”。

命令行选项：`/installdir "C:\Program Files\VDA" /components "VDA","CSA","PLUGINS"`

用于将 Virtual Delivery Agent、Citrix Workspace Environment Management™ 代理、Citrix

deviceTRUST、Citrix uberAgent、Citrix Secure Access Client 和 Citrix Workspace 应用程序安装到指定目录中。

注意：

在以下情况下，您可以在 VDA 安装、升级或卸载期间选择安装、升级或卸载 Citrix Workspace 应用程序和其他组件：

- 在 VDA 安装和升级到 2607 期间，您可以选择包含或排除组件和 CWA 插件。
  - 默认情况下，**Citrix Workspace 应用程序 (CWA)**、**Citrix Secure Access Client (CSA)**、**Citrix 用户个性化层 (UPL)（仅适用于 WS VDA）**和 **Citrix Elastic App Layering (CEAL)（仅适用于 TS VDA）**未选择安装，如果需要，您可以在安装期间选择它们。 **会话录制代理 (SRAGENT)** 和 **Citrix Virtual Desktop Assistant (ASSISTANTAPP)（现在在 TS VDA 和 WS VDA 上均可用）**默认选择安装，如果需要，您可以在安装期间取消选择它们。
  - **Citrix Device Trust**、**Citrix uberAgent** 和 **Citrix Workspace Environment Management™ 代理**现已与 VDA 集成并始终安装。为防止其安装，管理员必须使用受支持的 `/exclude` 命令行选项。**uberAgent** 也默认安装，从 VDA 2511 开始，以及在 2603 中，它无法通过 GUI 或命令行 (CLI) 从安装中排除。
  - 默认情况下，**Citrix Workspace Environment Management™ 代理**在**基本部署**中运行，这是一种功能有限的单机模式，不连接到 WEM 基础结构。要通过将代理连接到 Citrix Cloud 中的 WEM 服务或本地部署来启用完整的 WEM 功能，请通过组策略配置设置。有关详细信息，请参阅这篇 WEM 文章。
  - **Citrix 用户个性化层：** 安装用户个性化层的 MSI。有关详细信息，请参阅用户个性化层。
  - **命令行更改**

    `/components VDA,CSA`：此命令将安装 **VDA** 和 **CSA**（已选择），以及 **Citrix Device Trust**、**Citrix uberAgent** 和 **Citrix Workspace Environment Management agent**（默认集成）。

    `/components VDA`：此命令将安装 **VDA**，以及 **Citrix Device Trust**、**Citrix uberAgent** 和 **Citrix Workspace Environment Management agent**，因为这些组件现已集成到 VDA 本身中。如果您将 Citrix Device Trust、Citrix uberAgent 和 Citrix

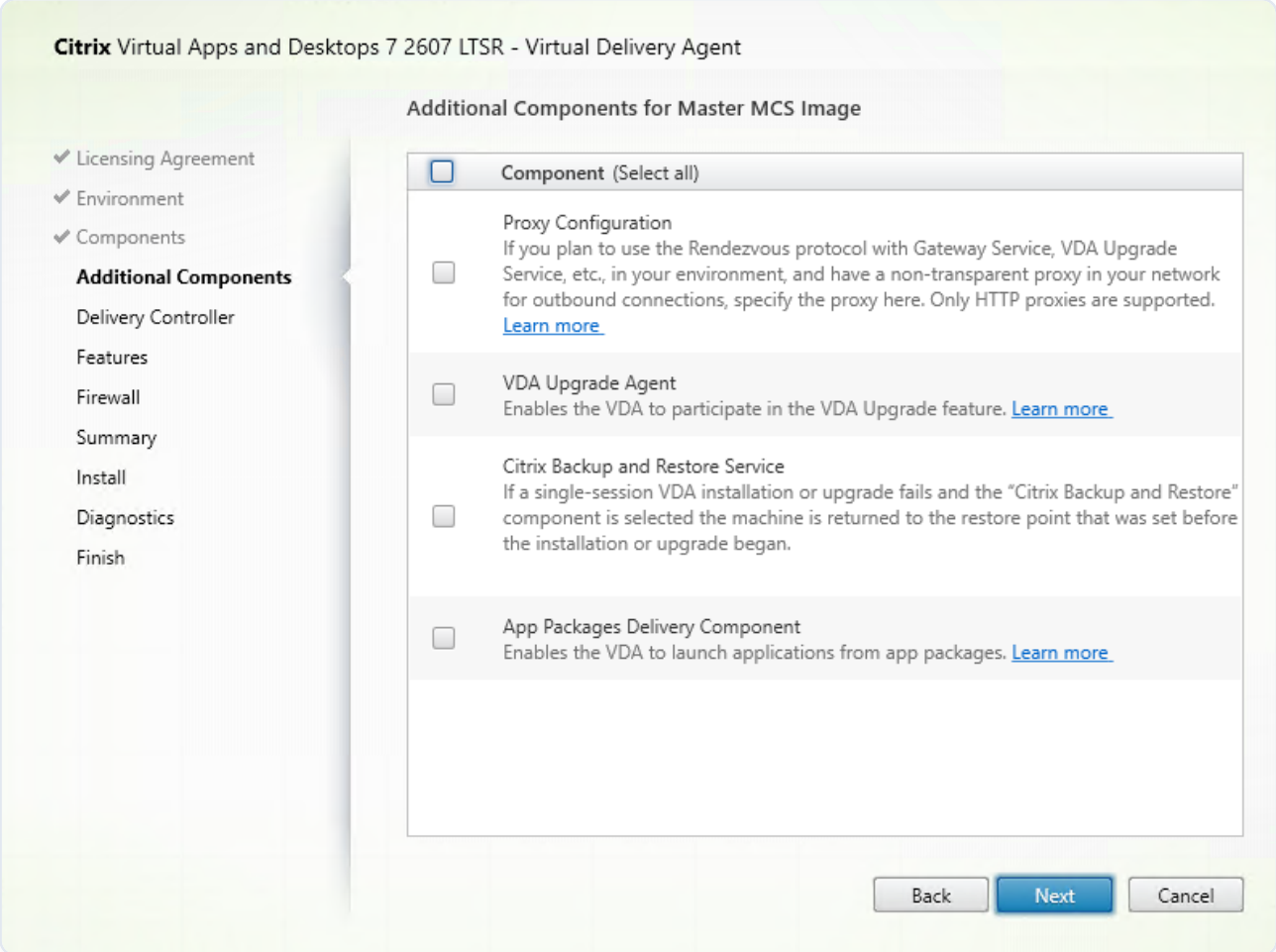
Workspace Environment Management agent 指定为与 `/components` 选项一起使用的参数，则 VDA 元安装程序会记录一条通知，指示从 `/components` 选项中删除了这些参数。随后，VDA 元安装程序将继续安装或升级 VDA。

`/components`：此命令是无效命令，它必须始终包含 VDA。可以根据需要添加其他组件进行安装。

将 `/exclude` 命令用于默认集成组件：`/exclude` 选项始终优先。它可用于阻止安装默认集成组件。示例：`/exclude "Citrix Device Trust","Citrix Universal Print Client"`。此命令将安装包含 Citrix Workspace Environment Management agent 的 VDA，但不安装 Citrix Device Trust 和 Citrix Universal Print Client。

- 在 VDA 升级期间，如果 VDA 中尚未安装 Citrix Workspace app、Citrix Secure Access Client 和 Citrix 用户个性化层（仅适用于 WS VDA）、Session Recording Agent、Citrix Virtual Desktop Assistant 和 Elastic App Layering（仅适用于 TS VDA），则可以选择安装它们。
- 在 VDA 升级期间，如果已安装用户个性化层或 Elastic App Layering，则会将其选为“**必需**”，并升级该组件。
- 在 VDA 升级期间，如果 Citrix Workspace app 和其他已安装插件的版本可以升级，则会显示升级它们的选项。
- 在 VDA 卸载期间，您可以选择是否卸载 Citrix Workspace app (CWA) 和任何其他已安装的组件。默认情况下，除 CWA 之外的所有组件都会自动卸载。CWA 的处理方式不同，除非明确选择，否则不会将其删除。

步骤 6. 安装其他组件



"其他组件"页面包含用于启用或禁用随 VDA 安装其他功能和技术的复选框。在命令行安装中，可以使用 `/exclude` 或 `/includeadditional` 选项明确省略或包含一个或多个可用组件：

- **/includeadditional** "*组件*"\[,"*组件*"\] ...
- **排除** "*组件*"\[,"*组件*"\] ...

下表指示此页面上各项的默认设置。默认设置取决于您在**"环境"**页面上选择的选项。

附加组件页面	环境页面："带 MCS 的主映像"或"带 CITRIX PROVISIONING 的主映像"已选定	环境页面："启用与服务器的代理连接"（适用于多会话操作系统）或"远程电脑访问"（适用于单会话操作系统）已选定
应用程序包交付组件	未选定	未选定
Citrix VDA 升级代理	未选定	未选定
Citrix 备份和还原	未选定	未选定
Citrix 会合 V2	未选定	未选定

如果出现以下情况，此页面将不显示：

- 您正在使用 `VDAWorkstationCoreSetup.exe` 安装程序或 `VDASingleSessionCoreSetup.exe`。此外，附加组件的命令行选项不适用于该安装程序。
- 您正在升级 VDA，并且所有附加组件都已安装。如果某些附加组件已安装，则页面仅列出未安装的组件。

选中或清除以下复选框。（这些组件在安装程序中可能以不同的顺序显示。）

- **应用程序包交付组件**：如果您使用 Microsoft App-V 包中的应用程序，请安装此组件。有关详细信息，请参阅部署和交付 App-V 应用程序。

  命令行选项：`/includeadditional "App Packages Delivery Component"` 启用组件安装，`/exclude "App Packages Delivery Component"` 阻止组件安装。

- **Citrix Profile Management**：此组件管理用户配置文件中的用户个性化设置。有关详细信息，请参阅Profile Management。

  将 Citrix Profile Management 从安装中排除会影响使用 Citrix Director 对 VDA 进行的监视和故障排除。在**用户详细信息**和**端点**页面上，**个性化**面板和**登录持续时间**面板将失败。在**控制板**和**趋势**页面上，**平均登录持续时间**面板仅显示已安装 Profile Management 的计算机的数据。

  即使您正在使用第三方用户配置文件管理解决方案，Citrix 仍建议您安装并运行 Citrix Profile Management Service。不需要启用 Citrix Profile Management Service。

  命令行选项：`/includeadditional "Citrix Profile Management"` 启用组件安装，`/exclude "Citrix Profile Management"` 阻止组件安装。

- **Citrix Profile Management WMI 插件**：此插件在 WMI（Windows Management Instrumentation）对象中提供 Profile Management 运行时信息（例如，配置文件提供程序、配置文件类型、大小和磁盘使用情况）。WMI 对象向 Director 提供会话信息。

  命令行选项：`/includeadditional "Citrix Profile Management WMI Plug-in"` 启用组件安装，`/exclude "Citrix Profile Management WMI Plug-in"` 阻止组件安装。

> **注意：**

> 从 2507 LTSR 开始，**Citrix Profile Management** 和 **Citrix Profile Management WMI 插件**现在是 VDA 的一部分，并针对**主映像/MCS/PVS** 用例自动安装。对于**远程 PC** 用例，这些组件**默认不安装**。在所有情况下，已安装的组件都会自动升级。命令行行为与以前的版本保持不变。

- **VDA 升级代理**：仅适用于 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops service）部署。使 VDA 能够参与 VDA 升级功能。您可以使用该功能从管理控制台立即或在计划时间升级目录的 VDA。如果未安装此代理，您可以通过在计算机上运行 VDA 安装程序来升级 VDA。

  命令行选项：`/includeadditional "Citrix VDA Upgrade Agent"` 启用组件安装，`/exclude "Citrix VDA Upgrade Agent"` 阻止组件安装。

- **MCSIO 存储优化写入缓存**：安装 Citrix MCS I/O 驱动程序。有关详细信息，请参阅管理程序共享存储 和配置临时数据缓存。

  命令行选项：`/includeadditional "Citrix MCS IODriver"` 启用组件安装，`/exclude "Citrix MCS IODriver"` 阻止组件安装。

  > **注意：**
  >
  > 从版本 2607 开始，**用于存储优化的 MCSIO 写入缓存**现在是 VDA 的一部分，并针对 **Master Image/MCS** 用例自动安装。对于 **Remote PC** 用例，此组件**默认不安装**。在所有情况下，已安装的组件都会自动升级。命令行行为与以前的版本保持不变。

- **代理配置：** 如果您计划在环境中使用 Rendezvous 协议以及 Gateway Service、VDA 升级服务等，并且您的网络中存在用于出站连接的非透明代理，请在此处指定代理。仅支持 HTTP 代理。

  如果安装此组件，请在“**Rendezvous 代理配置**”页面上指定代理地址或 PAC 文件路径。有关功能详细信息，请参阅Rendezvous 协议。

  命令行选项：`/includeadditional "Citrix Rendezvous V2"` 启用组件安装，`/exclude "Citrix Rendezvous V2"` 阻止组件安装。

- **Citrix 备份和还原：** 如果 VDA 安装或升级失败，此组件可以将计算机恢复到安装或升级之前完成的备份。

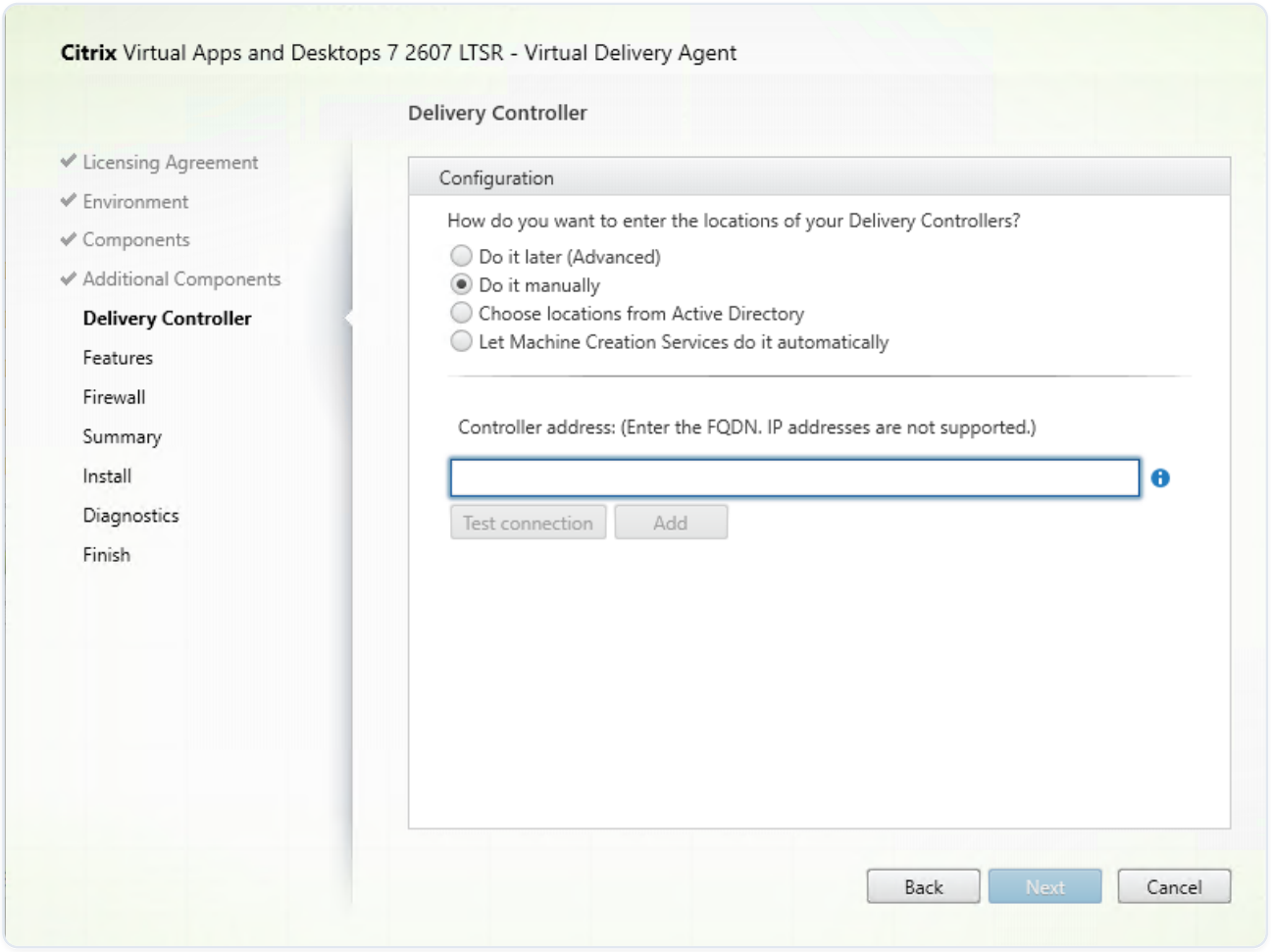
  确保满足 准备安装 中提到的 Microsoft 先决条件。

  命令行选项：`/includeadditional "Citrix Backup and Restore"` 启用组件安装，`/exclude "Citrix Backup and Restore"` 阻止组件安装。

  > **注意：**

> 从版本 2603 开始，Citrix 备份和还原组件仅适用于工作站 VDA。如果启用了 MCS 存储优化，则桌面操作系统的备份或还原可能会失败。要解决此问题，请在元安装程序中禁用 MCS 存储优化选项。

步骤 7. Delivery Controller™ 地址



在“**Delivery Controller**”页面上，选择输入已安装 Controller 地址的方式。Citrix 建议您在安装 VDA 时指定地址（**手动执行**）。VDA 必须拥有此信息才能向 Controller 注册。如果 VDA 无法注册，用户将无法访问该 VDA 上的应用程序和桌面。

- **手动执行：**（默认）输入已安装 Controller 的 FQDN，然后单击“**添加**”。如果您安装了更多 Controller，请添加它们的地址。
- **稍后执行（高级）：**如果选择此选项，向导会要求您在继续之前确认是否要执行此操作。要稍后指定地址，您可以重新运行安装程序或使用 Citrix 组策略。向导还会在“**摘要**”页面上提醒您。
- **从 Active Directory 中选择位置：**仅当计算机已加入域且用户是域用户时有效。
- **使用 WebSocket 令牌：**创建 WebSocket VDA。WebSocketToken 用于所需的令牌。
- **让 Machine Creation Services 自动执行：**仅在使用 MCS 预配计算机时有效。

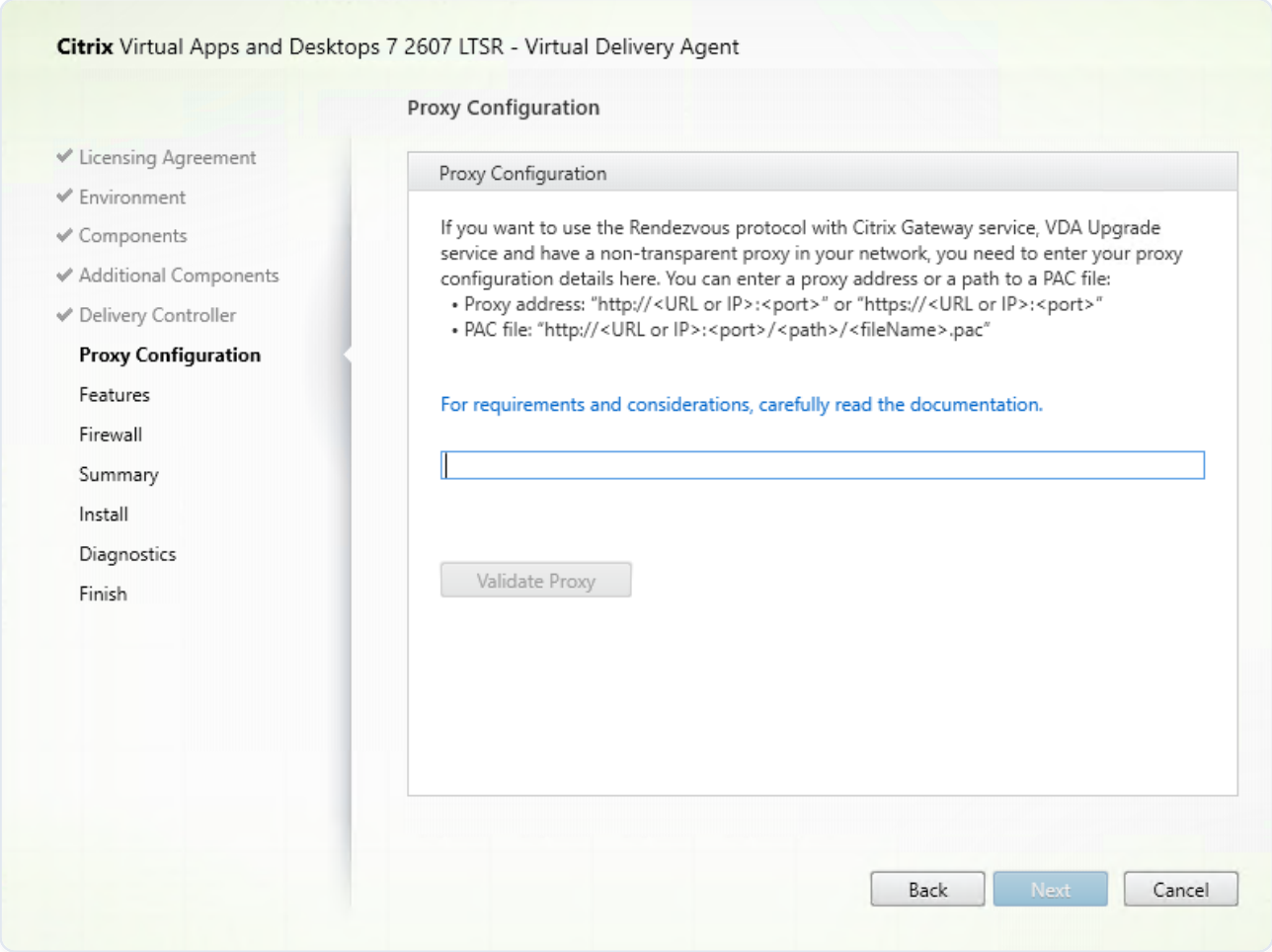
单击**下一步**。如果您选择了**稍后执行 (高级)**，系统会提示您确认稍后指定 Controller 地址。

其他注意事项：

- 地址不能包含非字母数字字符。
- 如果在 VDA 安装期间和组策略中指定地址，则策略设置将覆盖安装期间提供的设置。
- VDA 成功注册要求用于与 Controller 通信的防火墙端口处于打开状态。此操作在向导的**防火墙**页面上默认启用。
- 指定 Controller 位置（在 VDA 安装期间或之后）后，您可以使用自动更新功能在添加或删除 Controller 时更新 VDA。有关 VDA 如何发现 Controller 并向其注册的详细信息，请参阅VDA 注册。

命令行选项：`/controllers`

步骤 8. 代理配置



代理配置页面仅在您在**附加组件**页面上启用了**代理配置**复选框时显示。

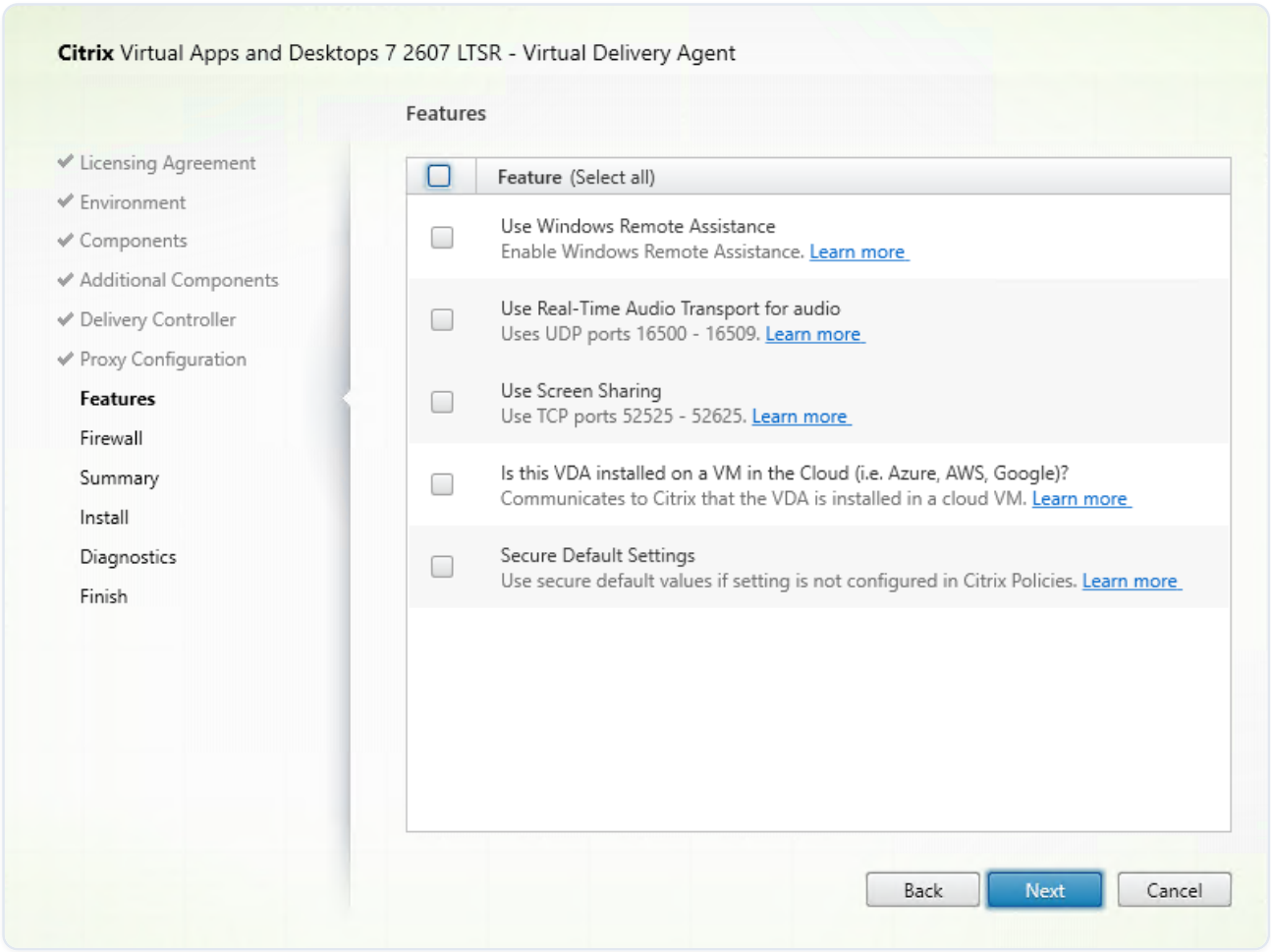
1. 选择是按代理地址还是 PAC 文件路径指定代理源。
2. 指定代理地址或 PAC 文件路径。
    - 代理地址格式：`http://<url-or-ip>:<port>`

- PAC 文件格式：`http://<url-or-ip>:<port>/<path>/<filename>.pac`

代理端口的防火墙必须打开，连接测试才能成功。如果无法连接到代理，您可以选择是否继续 VDA 安装。

命令行选项：`/proxyconfig`

步骤 9. 启用或禁用功能



在**功能**页面上，使用复选框启用或禁用要使用的功能。

- **使用 Windows 远程协助：** 启用此功能后，Windows 远程协助将与 Director 的用户影子功能一起使用。Windows 远程协助会在防火墙中打开动态端口。（默认 = 禁用）

  命令行选项：`/enable_remote_assistance`

- **使用实时音频传输进行音频传输：** 如果您的网络中广泛使用 IP 语音，请启用此功能。此功能可降低延迟并提高音频在有损网络上的弹性。它允许使用 RTP over UDP 传输音频数据。（默认 = 禁用）

  命令行选项：`/enable_real_time_transport`

- **使用屏幕共享：** 启用后，屏幕共享使用的端口将在 Windows 防火墙中打开。（默认 = 禁用）

命令行选项：`/enable_ss_ports`

- **此 VDA 是否安装在云中的 VM 上：** 此设置有助于 Citrix 正确识别本地和服务 (Citrix Cloud™) VDA 部署的资源位置，以用于遥测目的。此功能对客户侧利用率没有影响。如果您的部署使用 Citrix DaaS，请启用此设置（默认 = 禁用）。

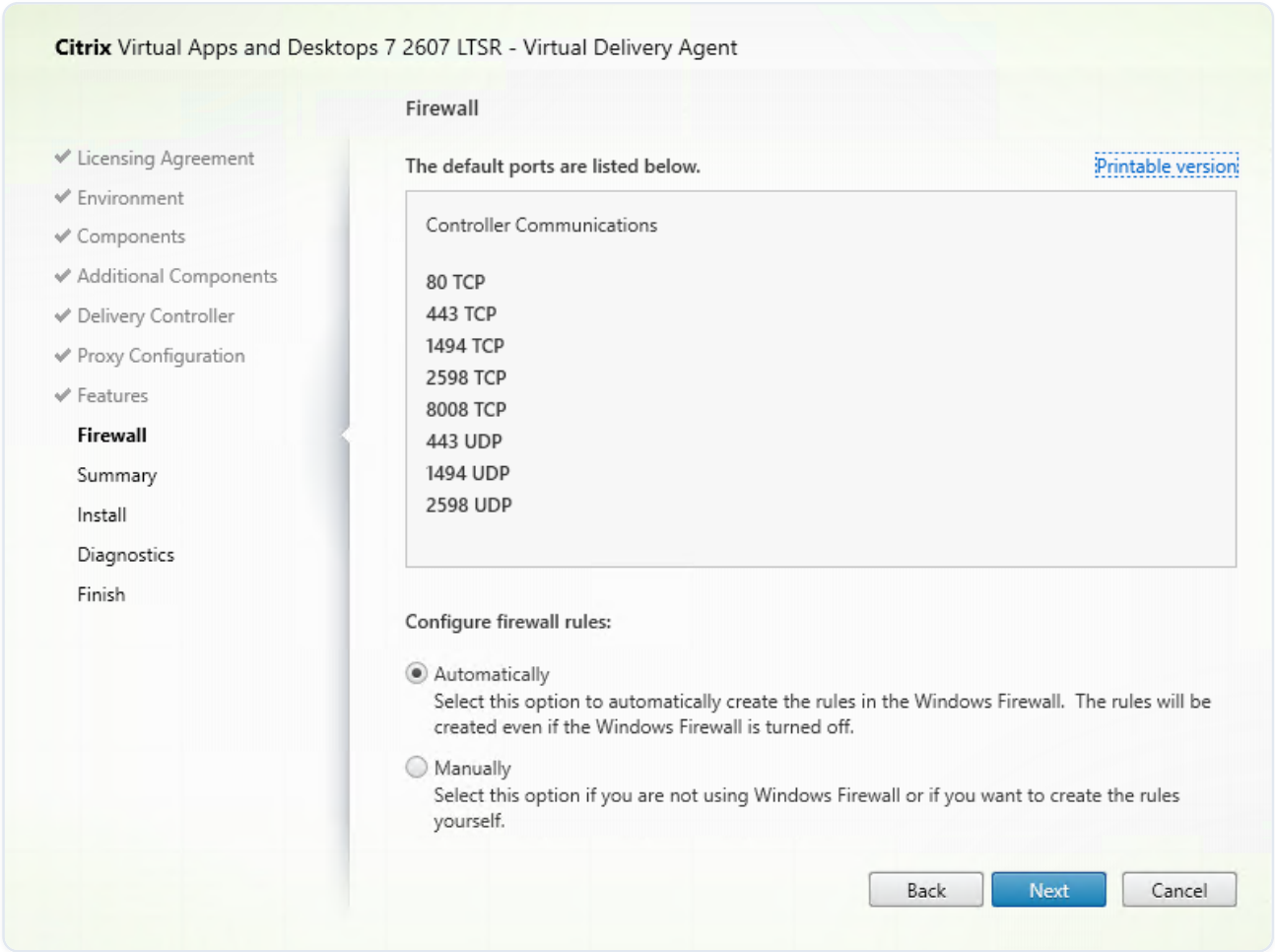
  命令行选项：`/xendesktopcloud`

- **安全默认设置：** 此选项将各种功能的默认设置从启用更改为禁用，以实现更安全的开箱即用配置。相关功能包括：客户端驱动器重定向、特殊文件夹重定向、拖放、客户端 TWAIN 设备重定向、客户端 USB 即插即用设备重定向、客户端打印机重定向、客户端剪贴板重定向和客户端麦克风重定向。

命令行选项：`/ENABLE_SECURE_DEFAULTS`

单击**下一步**。

步骤 10. 防火墙端口

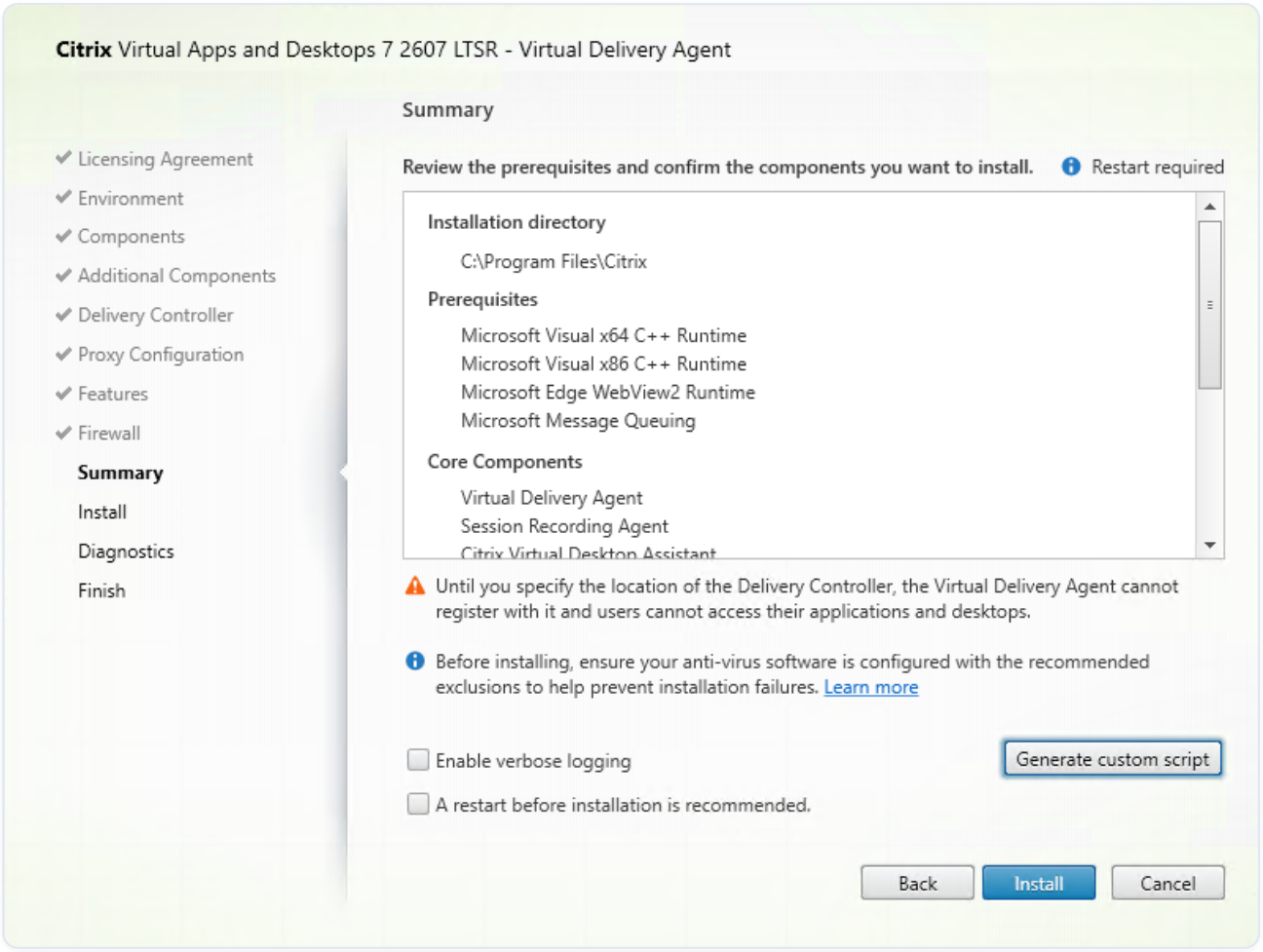


在“**防火墙**”页面上，默认情况下，如果 Windows 防火墙服务正在运行，即使防火墙未启用，端口也会自动打开。此默认设置适用于大多数部署。有关端口信息，请参阅网络端口。

单击**下一步**。

命令行选项：`/enable_hdx_ports`

步骤 11. 查看必备条件并确认安装



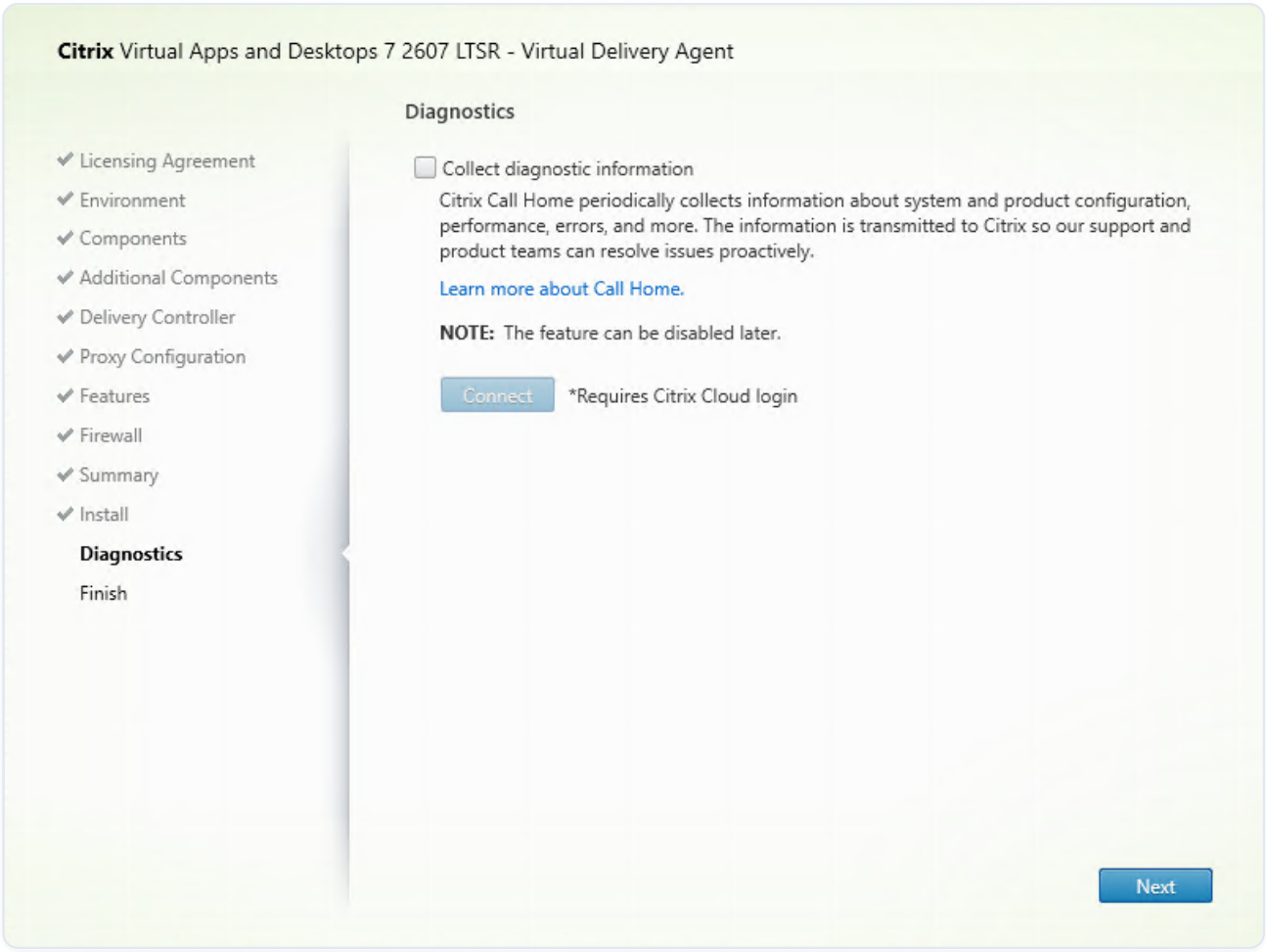
“**摘要**”页面列出了将要安装的内容。使用“**返回**”按钮返回到之前的向导页面并更改选择。

准备就绪后，单击“**安装**”。

如果尚未安装或启用必备条件，计算机可能会重启一次或多次。请参阅准备安装。

> **注意：**
>
> 此时，您还可以单击“**摘要**”页面上的“**生成自定义脚本**”按钮，根据您当前的安装选择创建命令行脚本。此脚本可以重复用于以无人参与模式安装或升级 VDA。

步骤 12. 诊断



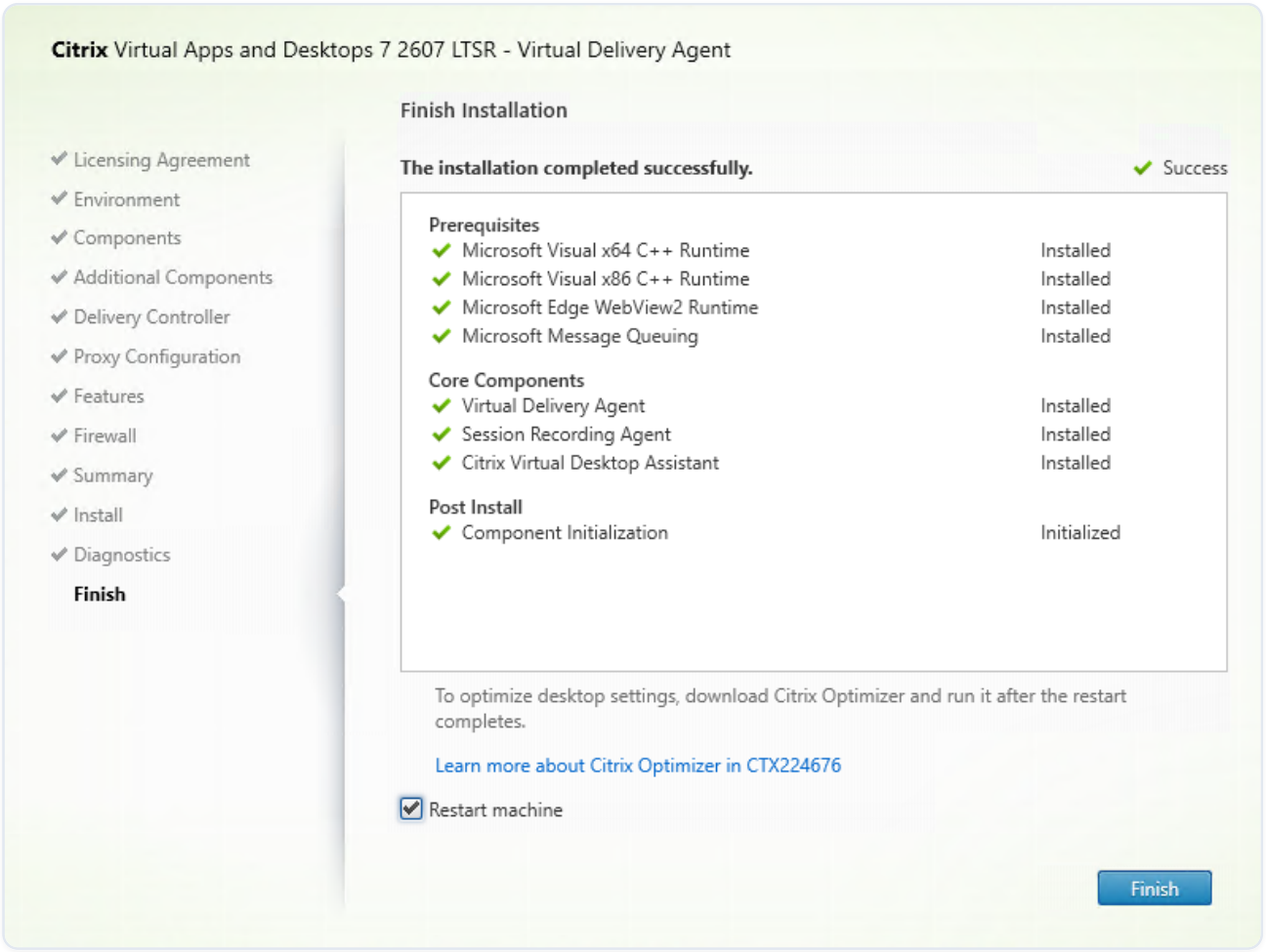
在“**诊断**”页面上，选择是否参与 Citrix Call Home。如果您选择参与（默认），请单击“**连接**”。出现提示时，输入您的 Citrix 帐户凭据。

凭据验证后（或者如果您选择不参与），单击“**下一步**”。

使用完整产品安装程序时，如果您在“**诊断**”页面上单击“**连接**”而未首先选择“**收集诊断信息**”，则在关闭“**连接到 Citrix Insight Services**”对话框后，“**下一步**”按钮将禁用。您无法移动到下一页。要重新启用“**下一步**”按钮，请选择并立即取消选择“**收集诊断信息**”。

有关详细信息，请参阅Call Home。

步骤 13. 完成此安装



完成页面包含所有已成功安装和初始化的先决条件和组件的绿色复选标记。

单击**完成**。默认情况下，计算机将自动重新启动。尽管您可以禁用此自动重新启动，但在计算机重新启动之前，VDA 无法使用。

后续步骤

如有需要，请重复上述步骤在其他计算机或映像上安装 VDA。

安装所有 VDA 后，启动 Studio。如果您尚未创建站点，Studio 会自动引导您完成该任务。完成该任务后，Studio 会引导您创建计算机目录，然后创建交付组。请参阅：

- 创建站点
- 创建计算机目录
- 创建交付组

Citrix 优化器

Citrix Optimizer 是一款适用于 Windows 操作系统的工具，可帮助 Citrix 管理员通过删除和优化各种组件来优化 VDA。

安装 VDA 并完成最终重新启动后，下载并安装 Citrix Optimizer。请参阅 CTX224676。该 CTX 文章包含下载包以及有关安装和使用 Citrix Optimizer 的说明。

自定义 VDA

要自定义已安装的 VDA：

1. 在 Windows 的“删除或更改程序”功能中，选择“**Citrix Virtual Delivery Agent**”或“**Citrix Remote PC Access/VDI Core Services VDA**”。然后右键单击并选择“**更改**”。
2. 选择**自定义 Virtual Delivery Agent 设置**。安装程序启动后，您可以更改：
   - Controller 地址
   - 用于向 Controller 注册的 TCP/IP 端口（默认值 = 80）
   - 是否自动打开 Windows 防火墙端口

故障排除

- 有关 Citrix 如何报告组件安装结果的信息，请参阅 Citrix 安装返回代码。
- 在交付组的 Studio 显示中，**详细信息**窗格中的**已安装的 VDA 版本**条目可能不是计算机上安装的版本。计算机的 Windows 程序和功能显示屏会显示实际的 VDA 版本。
- VDA 安装完成后，它无法向用户交付应用程序或桌面，直到它向 Delivery Controller 注册。

  要了解 VDA 注册方法以及如何排查注册问题，请参阅 VDA 注册。

已知限制

当您使用适用于 Windows 的 Citrix Workspace 应用程序 1912 或更早版本时，会话会在一段时间后断开。此问题已在较新的 LTSR 和 CR 版本的 Citrix Workspace 应用程序中修复。 有关支持的版本信息，请参阅 适用于 Windows 的 Citrix Workspace 应用程序 / 适用于 Windows 的 Citrix Receiver 长期服务版本。

配置与 VDA 安装相关的 Windows Defender 访问控制

客户配置 Windows Defender 访问控制 (WDAC) 设置以禁止加载未签名的二进制文件。因此，通过 VDA 安装程序分发的未签名二进制文件将被禁止，这会限制 VDA 安装。

Citrix® 现在使用 Citrix 代码签名证书对所有 Citrix 生成的二进制文件进行签名。此外，Citrix 还使用证书对随产品分发的第三方二进制文件进行签名，该证书将这些第三方二进制文件认证为受信任的二进制文件。

> **重要提示：**

从包含未签名第三方二进制文件的旧 VDA 升级到包含已签名二进制文件的新 VDA 版本时，可能不会始终将已签名二进制文件放置在升级后的计算机上。 这是由于操作系统中的一种机制，即系统升级不会替换相同版本的二进制文件。 尽管第三方二进制文件已签名，但其版本由第三方控制，Citrix 无法更新，导致这些二进制文件未更新。为避免此限制：

1. 将二进制文件包含在允许列表中。这消除了对二进制文件进行签名的需要。
2. 卸载旧 VDA 并安装新 VDA。这类似于全新 VDA 安装，并且将安装已签名版本。

使用向导创建新基本策略

WDAC 允许您添加受信任的二进制文件以在您的系统上运行。安装 WDAC 后，**Windows Defender 应用程序控制策略向导**会自动打开。

要添加二进制文件，必须创建新的基本 WDAC 策略。本节提供了 Citrix 推荐的创建基本策略的指南。

- 选择**签名和信誉模式**作为基本模板，因为它授权 Windows 操作系统组件、从 Microsoft Store 安装的应用程序、所有 Microsoft 签名的软件以及第三方 Windows 硬件兼容驱动程序。
- **启用审核模式**，因为它允许您在强制实施新的 Windows Defender 应用程序控制策略之前对其进行测试。
- 为**文件规则**添加**自定义规则**，以指定识别和信任应用程序的级别并提供参考文件。通过选择“发布者”作为规则类型，可以选择由 Citrix 证书之一签名的参考文件。
- 添加规则后，导航到保存 `.XML` 和 `.CIP` 文件的文件夹。`.XML` 文件包含策略中定义的所有规则。可以对其进行配置以更改、添加或删除任何规则。
- 在部署 WDAC 策略之前，必须将 `.XML` 文件转换为其二进制形式。WDAC 文件将 `.XML` 文件转换为 `.CIP` 文件。
- 将 `.CIP` 文件复制并粘贴到：C:\WINDOWS\System32\CodeIntegrity\CiPolicies\Active 并重新启动计算机。生成的策略将以审核模式应用。
- 有关创建基本策略的分步过程，请参阅使用向导创建新基本策略。

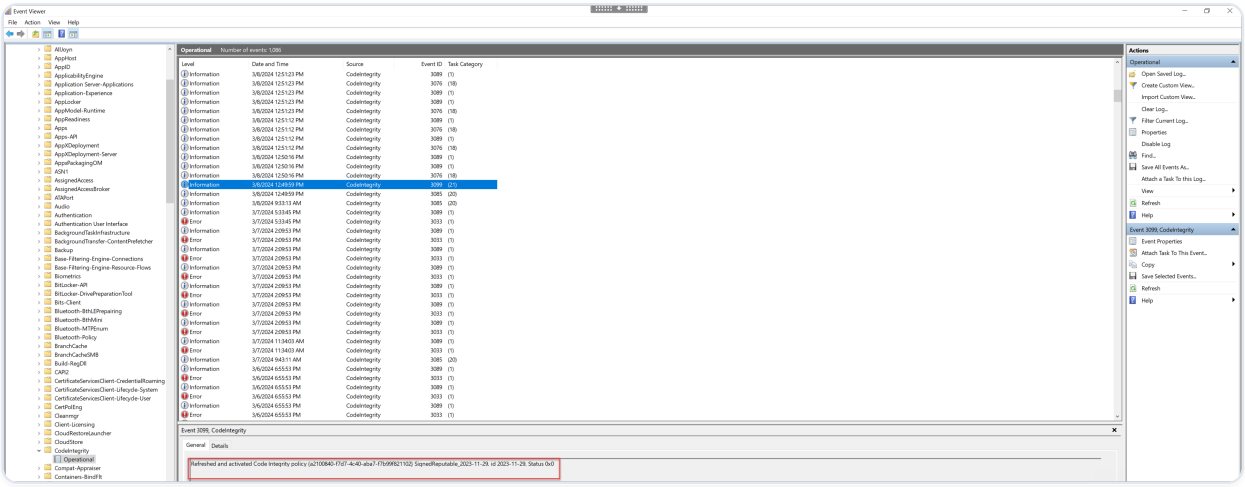
应用此策略后，WDAC 不会就由指定发布者/CA 机构签名的任何 Citrix 文件发出警告。

同样，我们可以为由第三方签名的文件创建发布者级别规则。

验证已应用的策略

1. 计算机重新启动后，打开**事件查看器**，然后转到**应用程序和服务日志 > Microsoft > Windows > CodeIntegrity > Operational**。

2. 确保已应用的策略已激活。



3. 查找违反策略的日志并检查该文件的属性。首先，确认它已签名。如果未签名且此计算机已进行 VDA 升级，则很可能是上述限制中描述的情况。如果已签名，则此文件可能已使用备用证书签名，如前所述。

使用 Citrix 证书签名的 Citrix 生成文件的示例如下：`C:\Windows\System32\drivers\picadm.sys`。 使用 Citrix 第三方证书签名的第三方二进制文件的示例如下：`C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`。

VDA 安装和升级预检查

引入了一项解耦的 VDA 安装和升级预检，使客户能够在继续操作之前主动识别潜在问题。此检查会验证所有依赖项和先决条件，为每个条件提供明确的通过/失败状态。如果发生任何故障，将提供包含具体建议的详细补救指南。实际的安装或升级过程是独立的，并且必须在预检查完成后手动启动。

本文概述了执行 VDA 安装和升级预检查的步骤。

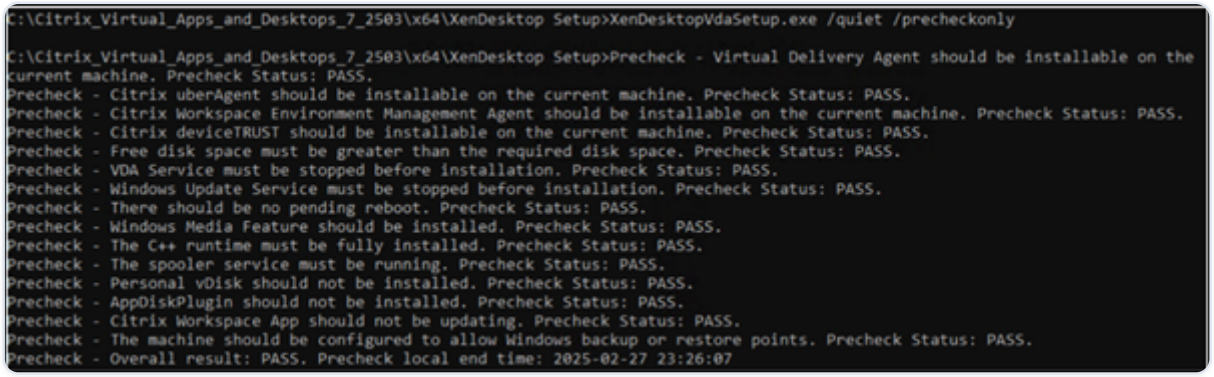
步骤 1. 运行命令行

> **注意：**
>
> - 预检查仅支持命令行模式。
> - 运行此命令时不会启动安装或升级。

> 要执行预检查，请将 `/precheckonly` 选项添加到您常用的安装或升级命令中。将检查 VDA 安装或升级的所有预检查条件。

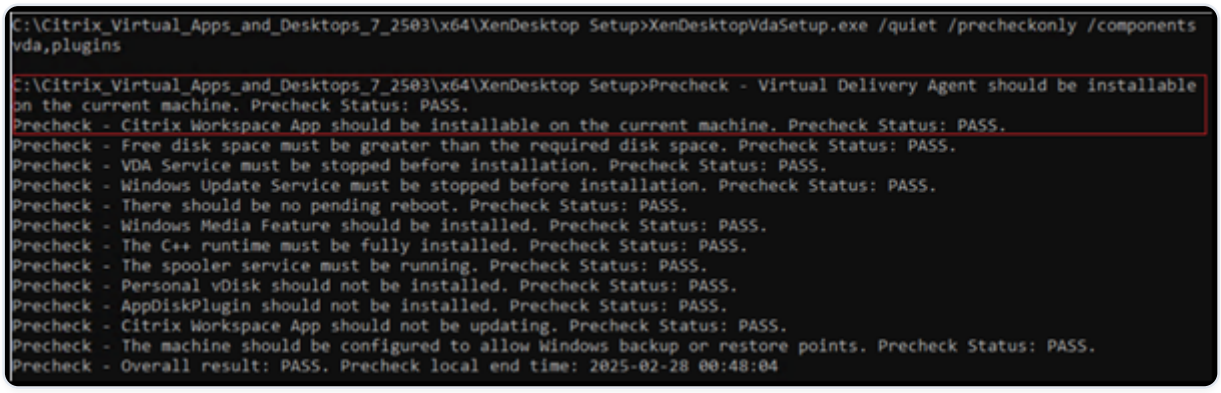
执行默认安装和升级的预检查

运行以下命令以执行预检查并确保计算机状态处于可接受状态：`\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly`



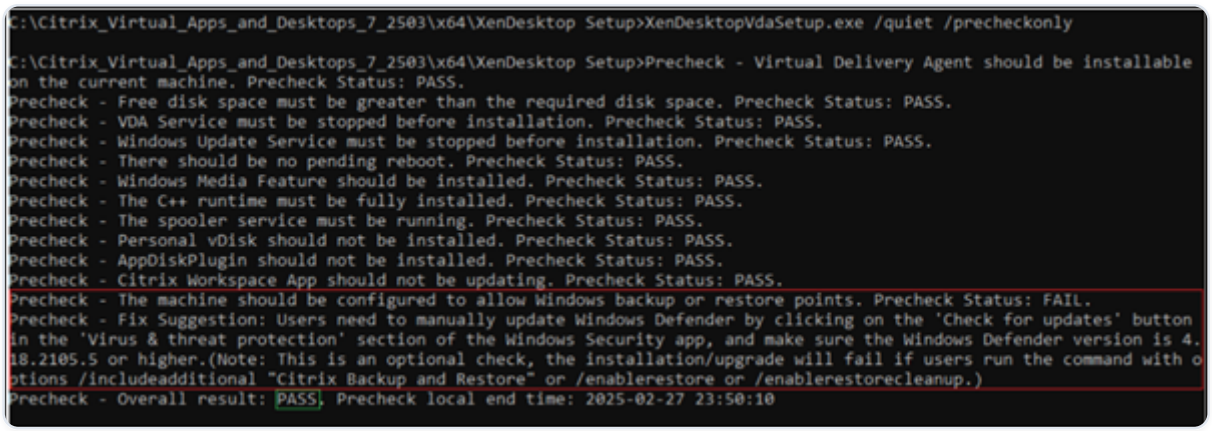
执行指定组件的安装和升级预检查

要在安装或升级之前检查特定组件的先决条件，请将 `/precheckonly` 添加到您的命令中。`\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /components vda,plugins`



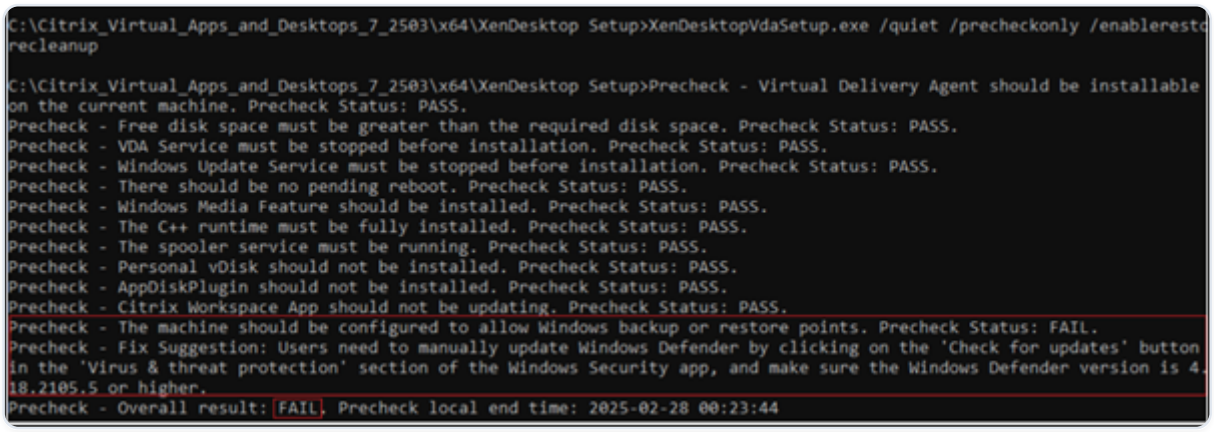
执行附加组件（CITRIX 备份和还原）的安装和升级预检查

命令 `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly` 检查 Citrix 备份和还原组件的先决条件，作为可选检查。如果所有预检查都通过（可选检查除外），则总体结果为“通过”。



以下命令检查 Citrix Backup and Restore 组件的必备条件，作为强制检查的一部分：

- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /includeadditional "Citrix Backup and Restore"`
- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /enablerestore`
- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /enablerestorecleanup`



步骤 2. 查看预检查结果

预检查结果显示在命令行中，记录在 `%temp%/Citrix/XenDesktop Installer/XenDesktop Installation.log` 中并保存在 `%temp%/Citrix/XenDesktop Installer/PrecheckResult_{yyyyMMddHHmmss}.json` 中。如果预检查失败，则总体结果为 `FAIL`，并为每个问题提供建议的修复措施。

命令行输出

命令行中的预检查结果包括：

- 预检查标准
- 预检查状态
- 失败修复建议
- 总体结果
- 结束时间。

如果结果为 `FAIL`，则修复建议可在以 **Precheck - Fix Suggestion:** 开头的行中找到。

```
C:\Citrix_Virtual_Apps_and_Desktops_7_2503\x64\XenDesktop Setup>XenDesktopVdaSetup.exe /quiet /precheckonly

C:\Citrix_Virtual_Apps_and_Desktops_7_2503\x64\XenDesktop Setup>Precheck - Virtual Delivery Agent should be installable on the
 current machine. Precheck Status: PASS.
Precheck - Citrix uberAgent should be installable on the current machine. Precheck Status: PASS.
Precheck - Citrix Workspace Environment Management Agent should be installable on the current machine. Precheck Status: PASS.
Precheck - Citrix deviceTRUST should be installable on the current machine. Precheck Status: PASS.
Precheck - Free disk space must be greater than the required disk space. Precheck Status: PASS.
Precheck - VDA Service must be stopped before installation. Precheck Status: PASS.
Precheck - Windows Update Service must be stopped before installation. Precheck Status: PASS.
Precheck - There should be no pending reboot. Precheck Status: PASS.
Precheck - Windows Media Feature should be installed. Precheck Status: PASS.
Precheck - The C++ runtime must be fully installed. Precheck Status: PASS.
Precheck - The spooler service must be running. Precheck Status: FAIL.
Precheck - Fix Suggestion: Users can start 'Print Spooler' service manually, it is recommended to set the startup type of 'Pri
nt Spooler' service to Automatic, then re-run the installer.
Precheck - Personal vDisk should not be installed. Precheck Status: PASS.
Precheck - AppDiskPlugin should not be installed. Precheck Status: PASS.
Precheck - Citrix Workspace App should not be updating. Precheck Status: PASS.
Precheck - The machine should be configured to allow Windows backup or restore points. Precheck Status: PASS.
Precheck - Overall result: FAIL. Precheck local end time: 2025-02-28 00:32:40
```

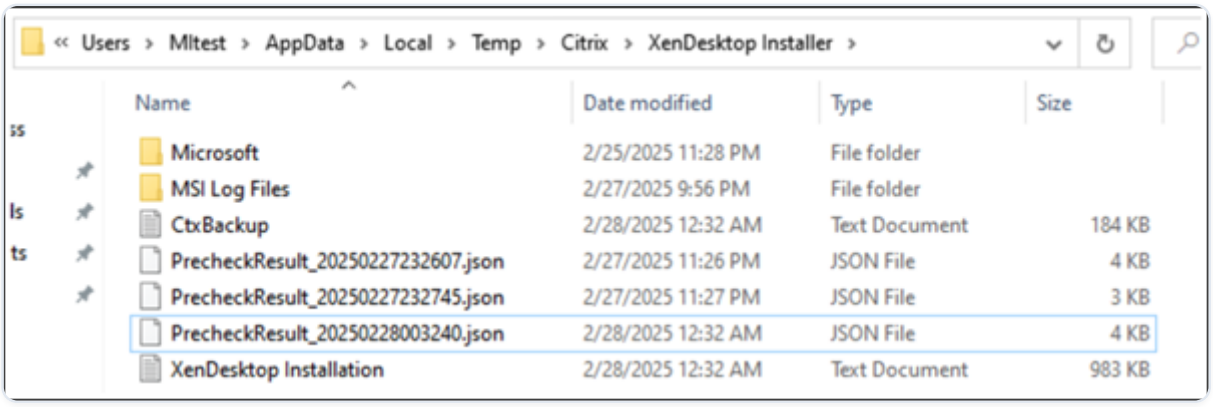
日志输出

`XenDesktop Installation.log` 中的预检查结果与命令行中显示的结果一致。要找到它们，请在日志文件中搜索 `Precheck -`。 如果总体结果为 `FAIL`，则修复建议可在包含 `Precheck - Fix Suggestion:` 的行中找到。

```
Line 8838: 00:32:18.9367       : XenDesktopSetup:Precheck - Virtual Delivery Agent should be installable on the current machine. Precheck Status: PASS.
Line 8839: 00:32:18.9367       : XenDesktopSetup:Precheck - Citrix uberAgent should be installable on the current machine. Precheck Status: PASS.
Line 8840: 00:32:18.9367       : XenDesktopSetup:Precheck - Citrix Workspace Environment Management Agent should be installable on the current machine.
    Precheck Status: PASS.
Line 8841: 00:32:18.9367       : XenDesktopSetup:Precheck - Citrix deviceTRUST should be installable on the current machine. Precheck Status: PASS.
Line 8842: 00:32:18.9367       : XenDesktopSetup:Precheck - Free disk space must be greater than the required disk space. Precheck Status: PASS.
Line 8913: 00:32:29.3433       : XenDesktopSetup:Precheck - VDA Service must be stopped before installation. Precheck Status: PASS.
Line 8914: 00:32:30.6715       : XenDesktopSetup:Precheck - Windows Update Service must be stopped before installation. Precheck Status: PASS.
Line 8918: 00:32:30.6715       : XenDesktopSetup:Precheck - There should be no pending reboot. Precheck Status: PASS.
Line 8921: 00:32:30.7178       : XenDesktopSetup:Precheck - Windows Media Feature should be installed. Precheck Status: PASS.
Line 8927: 00:32:30.7959       : XenDesktopSetup:Precheck - The C++ runtime must be fully installed. Precheck Status: PASS.
Line 8930: 00:32:35.8281       : XenDesktopSetup:Precheck - The spooler service must be running. Precheck Status: FAIL.
Line 8931: 00:32:35.8281       : XenDesktopSetup:Precheck - Fix Suggestion: Users can start 'Print Spooler' service manually, it is recommended to set the
    startup type of 'Print Spooler' service to Automatic, then re-run the installer.
Line 8933: 00:32:35.8298       : XenDesktopSetup:Precheck - Personal vDisk should not be installed. Precheck Status: PASS.
Line 8935: 00:32:35.8298       : XenDesktopSetup:Precheck - AppDiskPlugin should not be installed. Precheck Status: PASS.
Line 8938: 00:32:35.8298       : XenDesktopSetup:Precheck - Citrix Workspace App should not be updating. Precheck Status: PASS.
Line 8981: 00:32:40.3025       : XenDesktopSetup:Precheck - The machine should be configured to allow Windows backup or restore points. Precheck Status: PASS.
Line 9128: 00:32:49.0153       : XenDesktopSetup:Precheck - Overall result: FAIL. Precheck local end time: 2025-02-28 00:32:40
```

JSON 输出

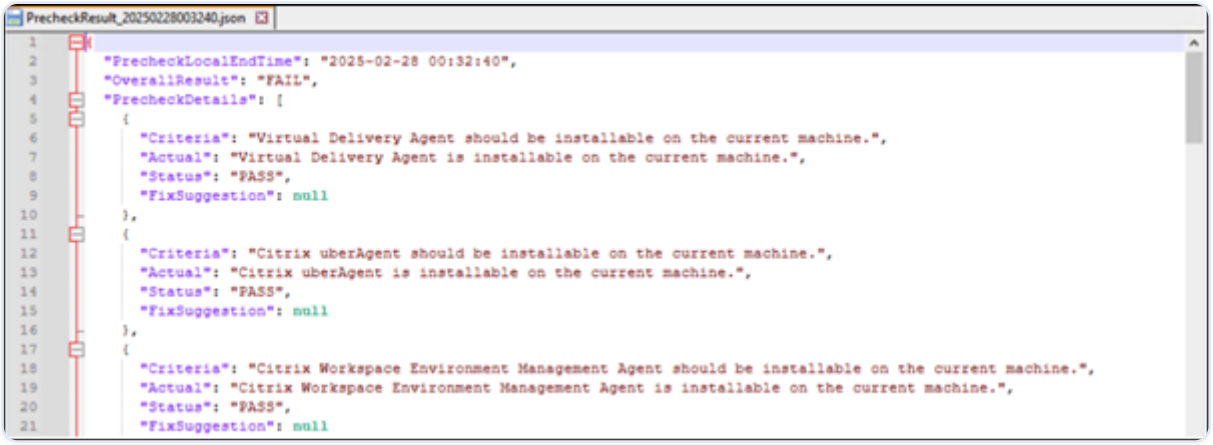
每次运行带有 `/quiet /precheckonly` 的命令时，都会生成一个 `.json` 文件。该文件名为 `PrecheckResult_{yyyyMMddHHmmss}.json`，并带有时间戳后缀。



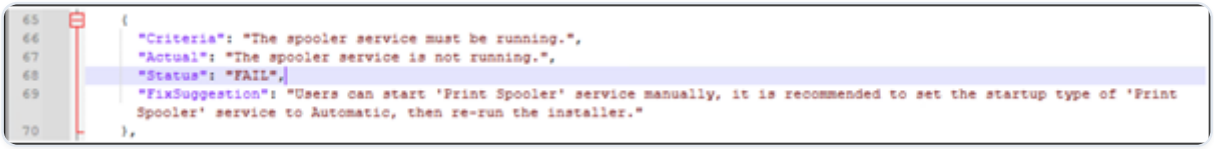
`.json` 文件包括：

- 预检查本地结束时间
- 总体结果
- 预检查详细信息

- 标准
- 实际值
- 状态
- 修复建议



状态为 `FAIL` 的每个预检查项目的修复建议可以在 `.json` 文件中的预检查详细信息部分下找到。



VDA 元安装程序助手工具

1. 简介

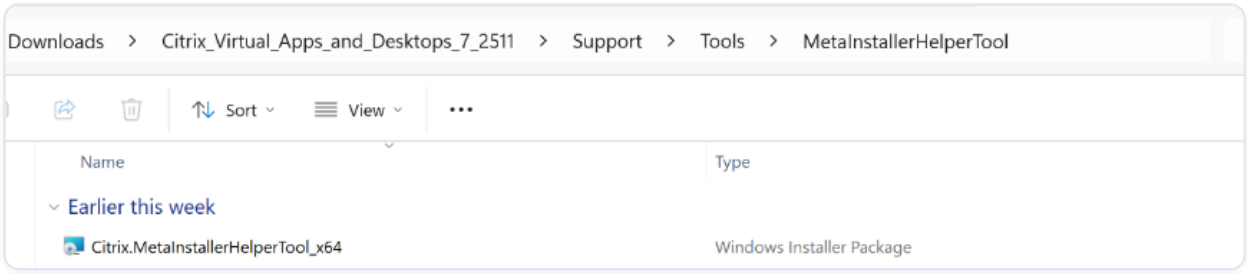
VDA 元安装程序助手工具包含一套工具，可协助通过 SCCM 任务序列进行 VDA 安装，以及一个用于分析安装日志和识别潜在问题的实用程序。

凭借简单的 MSI 安装和直观的用户界面，元安装程序助手工具提供了多项基本功能：

- **检查 SCCM 任务序列：** 此工具可帮助审查和验证现有 SCCM 任务序列，以确保其与 VDA 安装要求兼容。
- **生成任务序列参考：** 此工具自动创建参考任务序列，以帮助将 VDA 安装集成到 SCCM 部署工作流中，同时最大限度地减少手动配置。
- **VDA 安装日志分析器：** 此工具可帮助审查安装日志以识别错误、警告或故障。该工具会生成一份报告，突出显示根本原因、可能的解决方案以及成功部署的建议。

2. 安装

1. 从 Citrix 虚拟应用和桌面 下载页面 下载 Citrix 虚拟应用和桌面 产品 ISO。
2. 从 `\Support\Tools\MetaInstallerHelperTool` 文件夹中找到 Citrix.MetaInstallerHelperTool_x64.msi。



3. 双击 Citrix.MetaInstallerHelperTool_x64.msi 以安装该工具。

> **注意：**
>
> 此工具不是 VDA 的一部分。您可以将其安装在 VDA 上或任何本地设备上。

4. 安装后，在“开始”菜单中搜索“MetaInstallerHelperTool”，以管理员身份启动应用程序。

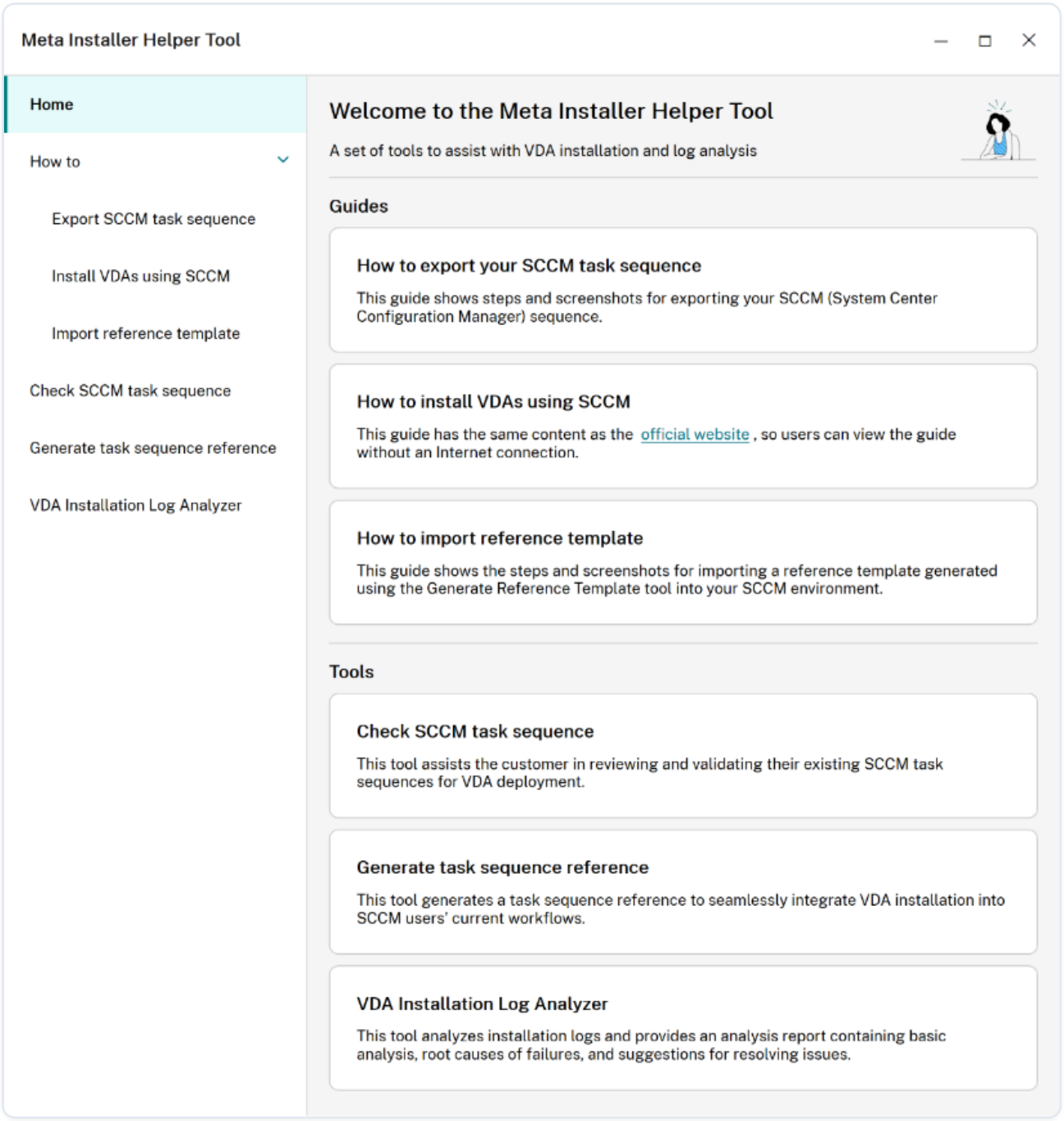


3. 用户界面 (UI) 概述

启动应用程序“MetaInstallerHelperTool”后，将出现主用户界面，该界面设计直观，易于导航和使用。

“**主页**”部分提供了“操作方法”部分中的指南说明，以及用于检查 SCCM 序列、生成任务序列模板和分析 VDA 安装日志的工具的功能说明。

您可以通过从左侧导航面板中选择相应的选项卡来访问这些指南和工具。



"**操作方法**"部分提供了导出任务序列、使用 SCCM 安装 VDA 以及导入带有屏幕截图和步骤的参考模板的指南。

- 请参阅"如何导出任务序列"以获取 SCCM 任务序列，供"检查 SCCM 任务序列"工具使用。
- 请参阅"如何使用 SCCM 安装 VDA"以安装 VDA。"检查 SCCM 任务序列"工具和"生成任务序列模板"工具也将参考本指南。
- 请参阅"如何导入参考模板"，将"生成任务序列模板"工具生成的模板作为参考模板导入到您的 SCCM 环境中。

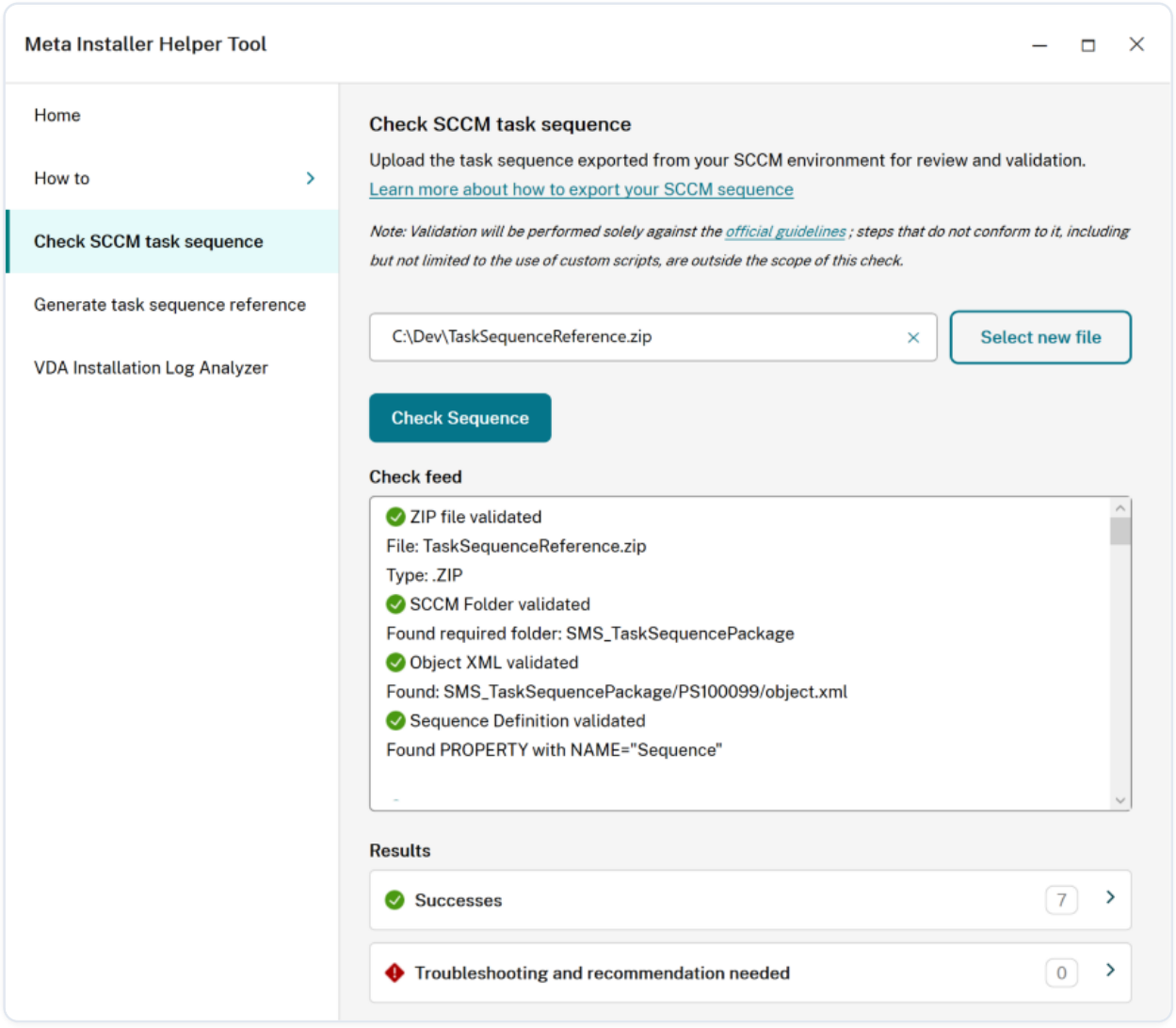
"**检查 SCCM 任务序列**"、"**生成任务序列模板**"和"**VDA 安装日志分析器**"部分可让您执行 Meta Installer Helper Tool 的核心任务。

4. 工具

1. 检查 SCCM 任务序列

   上传从 SCCM 环境导出的任务序列以进行审查和验证。

   该工具将检查上传的文件是否为 zip 文件，以及是否包含所需的 SCCM 任务序列文件夹结构、所需的 .xml 对象文件和有效的任务序列定义。它还将根据任务序列进行命令行参数分析和安装条件分析。



2. 生成任务序列参考

   此工具根据 Citrix 官方指南 生成任务序列模板，用于通过 SCCM 安装 VDA。

   您可以将其导入到 SCCM 环境中，作为将 VDA 安装集成到任务序列中的参考模板。

   Meta 安装程序生成任务序列(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/metainstaller-generate-task-sequence.png)

3. VDA 安装日志分析器

使用自动模式直接在 VDA 上分析安装日志，或者手动上传包含 VDA 安装日志的 .zip 文件进行分析。

Meta 安装程序日志分析器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/metainstaller-vda-log-analyzer.png)

在 VDA 上以**自动模式**运行时，该工具会自动检测日志存储路径并在本地分析安装日志。分析结果将保存，所有日志文件和报告都将打包成一个 ZIP 文件。

Meta 安装程序日志分析器 1(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/metainstaller-vda-log-analyzer1.png)

在**手动模式**下，您必须上传一个包含 VDA 安装日志的 .zip 文件进行分析。默认情况下，日志文件存储在以下位置：`%TEMP%\Citrix\XenDesktop Installer`

如果默认日志路径已修改，您可以在 Windows 注册表的以下位置验证当前位置：`Computer\HKLM\Software\Citrix\MetaInstall\LogPath`

该工具会提取上传的 .zip 文件，分析其内容，并保存分析结果以供查看。

Meta 安装程序日志分析器 2(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/metainstaller-vda-log-analyzer2.png)

使用脚本安装 VDA

> **注意：**
>
> Citrix 不对因适应客户生产环境而修改的脚本引起的问题负责。对于任何与安装相关的 Citrix 问题，请使用 Citrix 支持门户 提交技术支持案例并附上相关安装日志。

> 本文适用于在 Windows 操作系统计算机上安装 VDA。有关适用于 Linux 操作系统的 VDA 的信息，请参阅 Linux Virtual Delivery Agent 文档。

安装介质包含用于在 Active Directory 中为计算机安装、升级或删除 Virtual Delivery Agent (VDA) 的示例脚本。您还可以使用这些脚本来维护 Machine Creation Services™ 和 Citrix Provisioning（以前称为 Provisioning Services）使用的主映像。

所需访问权限：

- 脚本需要对 VDA 安装命令所在的网络共享具有“所有人读取”访问权限。安装命令在完整产品 ISO 中为 `XenDesktopVdaSetup.exe`，在独立安装程序中为 `VDAWorkstationSetup.exe` 或 `VDAServerSetup.exe`。
- 日志记录详细信息存储在每台本地计算机上。为了集中记录结果以供审查和分析，脚本需要对相应的网络共享具有“所有人读取和写入”访问权限。

要检查脚本运行结果，请检查中央日志共享。捕获的日志包括脚本日志、安装程序日志和 MSI 安装日志。每次安装或删除尝试都记录在一个带时间戳的文件夹中。文件夹标题以 PASS 或 FAIL 前缀指示操作结果。您可以使用标准目录搜索工具在中央日志共享中查找失败的安装或删除。这些工具提供了在目标计算机上本地搜索的替代方法。

在开始任何安装之前，请阅读并完成 准备安装 中的任务。

使用脚本安装或升级 VDA

1. 从安装介质上的 `\Support\AdDeploy\` 获取示例脚本 **InstallVDA.bat**。Citrix 建议您在自定义脚本之前备份原始脚本。
2. 编辑脚本：
   - 指定要安装的 VDA 版本：`SET DESIREDVERSION`。完整值可在安装介质的 ProductVersion.txt 文件中找到。但是，不要求完全匹配。
   - 指定将调用安装程序的网络共享。指向布局的根目录（树的最高点）。脚本运行时会自动调用相应版本的安装程序（32 位或 64 位）。例如：`SET DEPLOYSHARE=\\fileserver1\share1`。
   - （可选）指定用于存储集中式日志的网络共享位置。例如：`SET LOGSHARE=\\fileserver1\log1)`。
   - 按照使用命令行安装中所述指定 VDA 配置选项。`/quiet` 和 `/noreboot` 选项默认包含在脚本中，并且是必需的：`SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT /NORESUME`。
3. 使用组策略启动脚本，将脚本分配给包含您的计算机的 OU。此 OU 应仅包含要安装 VDA 的计算机。当该 OU 中的计算机重新启动时，脚本将在所有计算机上运行。VDA 将安装在每台具有受支持操作系统的计算机上。

使用脚本删除 VDA

1. 从安装介质上的 `\Support\AdDeploy\` 获取示例脚本 UninstallVDA.bat。Citrix 建议您在自定义脚本之前备份原始脚本。
2. 编辑脚本。

- 指定要删除的 VDA 版本：`SET CHECK\_VDA\_VERSION`。完整值可在安装介质的 ProductVersion.txt 文件中找到（例如 7.0.0.3018）。但是，不需要完全匹配。
- （可选）指定用于存储集中式日志的网络共享位置。

3. 使用组策略启动脚本，将脚本分配给包含您的计算机的 OU。此 OU 应仅包含要从中删除 VDA 的计算机。当 OU 中的计算机重新启动时，脚本将在所有计算机上运行。VDA 将从每台计算机中删除。

故障排除

- 脚本会生成内部日志文件，描述脚本执行进度。脚本在开始部署后的几秒钟内将 `Kickoff_VDA_Startup_Script` 日志复制到中央日志共享。您可以验证整个过程是否正常运行。如果此日志未按预期复制到中央日志共享，请通过检查本地计算机进一步进行故障排除。脚本将两个调试日志文件放置在每台计算机的 `%temp%` 文件夹中：
  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  检查这些日志以确保脚本：
  - 按预期运行。
  - 正确检测目标操作系统。
  - 正确配置为指向 `DEPLOYSHARE` 共享的 `ROOT`（包含名为 `AutoSelect.exe` 的文件）。
  - 能够对 `DEPLOYSHARE` 和 `LOG` 共享进行身份验证。
- 有关 Citrix 如何报告组件安装结果的信息，请参阅Citrix 安装返回代码。
- 在交付组的 Studio 显示中，**详细信息**窗格中的**已安装的 VDA 版本**条目可能不是计算机上安装的版本。计算机的程序和功能显示实际的 VDA 版本。
- VDA 安装后，它无法向用户交付应用程序或桌面，直到它向 Delivery Controller 注册。

  要了解 VDA 注册方法以及如何排查注册问题，请参阅 VDA 注册。

生成自定义脚本以通过命令行安装或升级 VDA

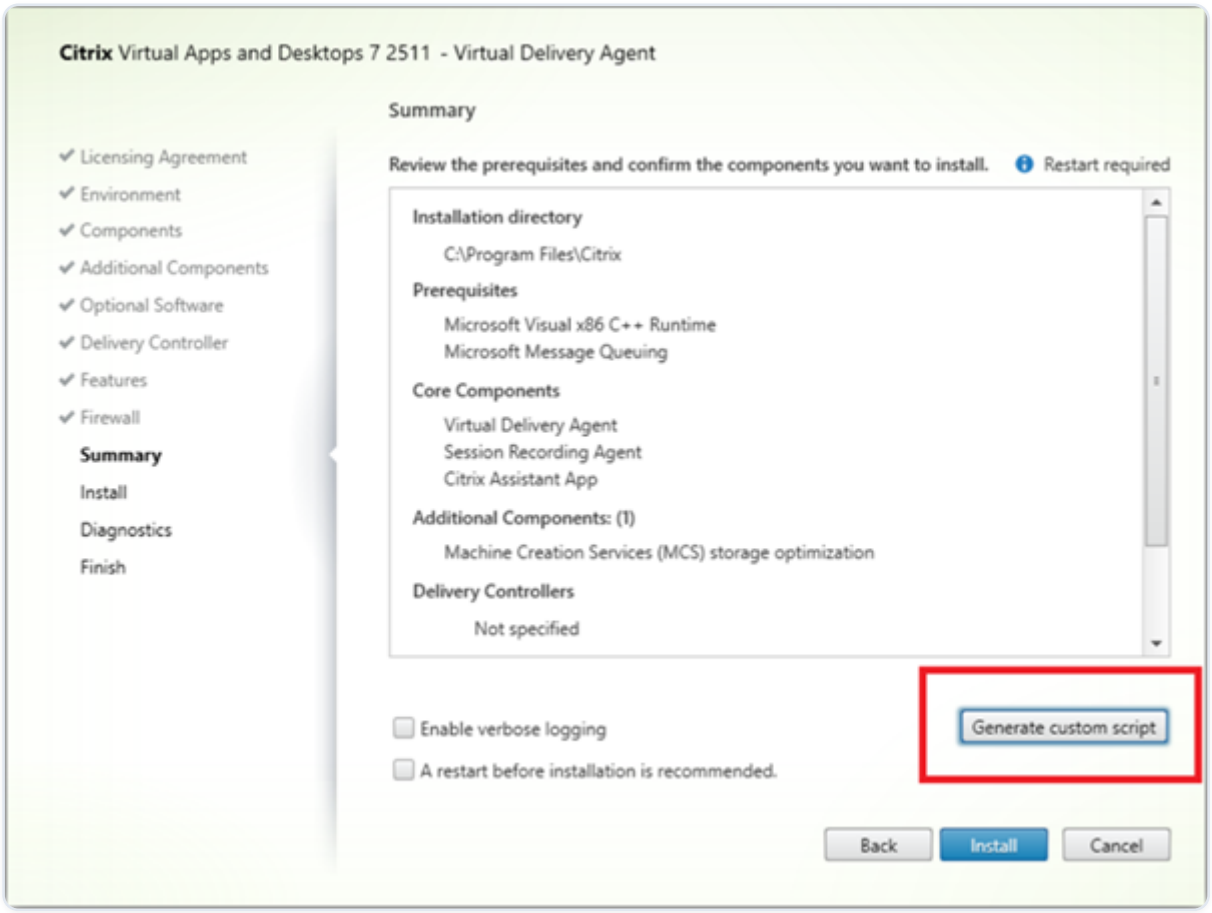
“**生成自定义脚本**”按钮允许您根据 VDA 安装 UI 中所做的配置选择创建批处理文件或脚本。生成的脚本可以导出并用于从命令行执行无人参与的安装或升级。此功能有助于自动化部署、确保配置准确性并减少手动脚本错误。

使用以下步骤从 VDA 安装 UI 生成命令行脚本。

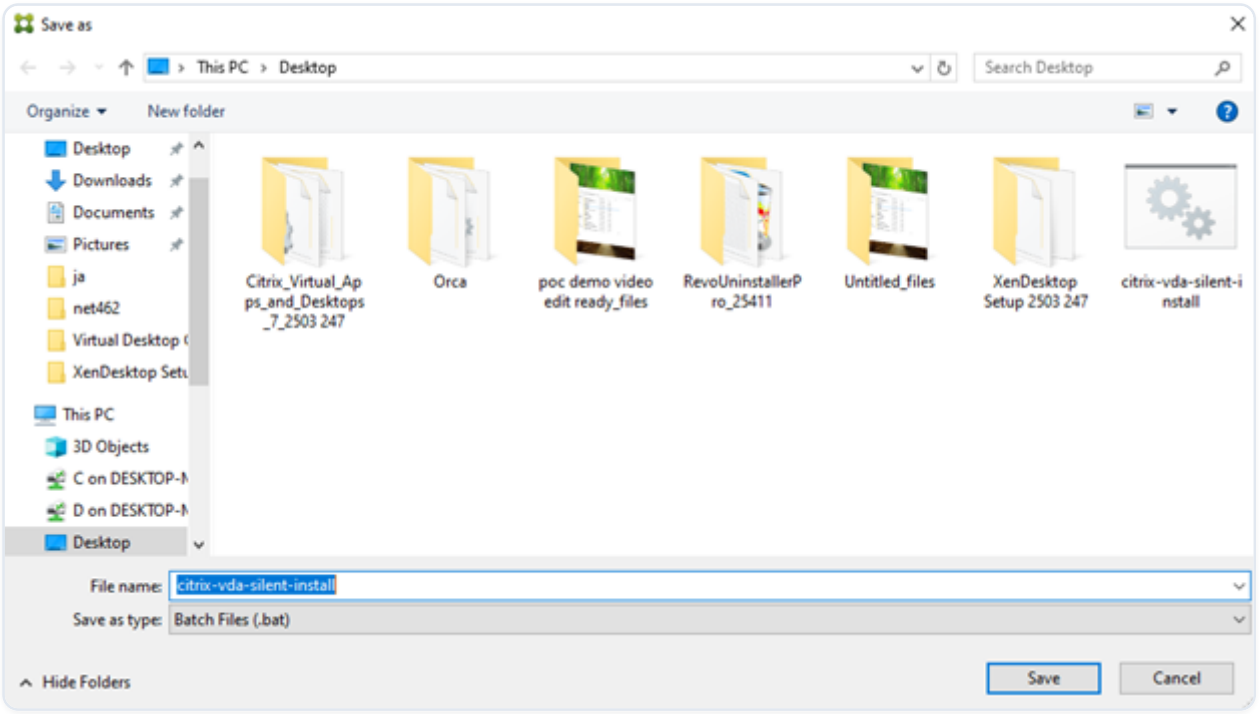
步骤 1：从安装程序 UI 生成自定义脚本

> **注意：**
>
> 此功能仅在 UI 模式下受支持。

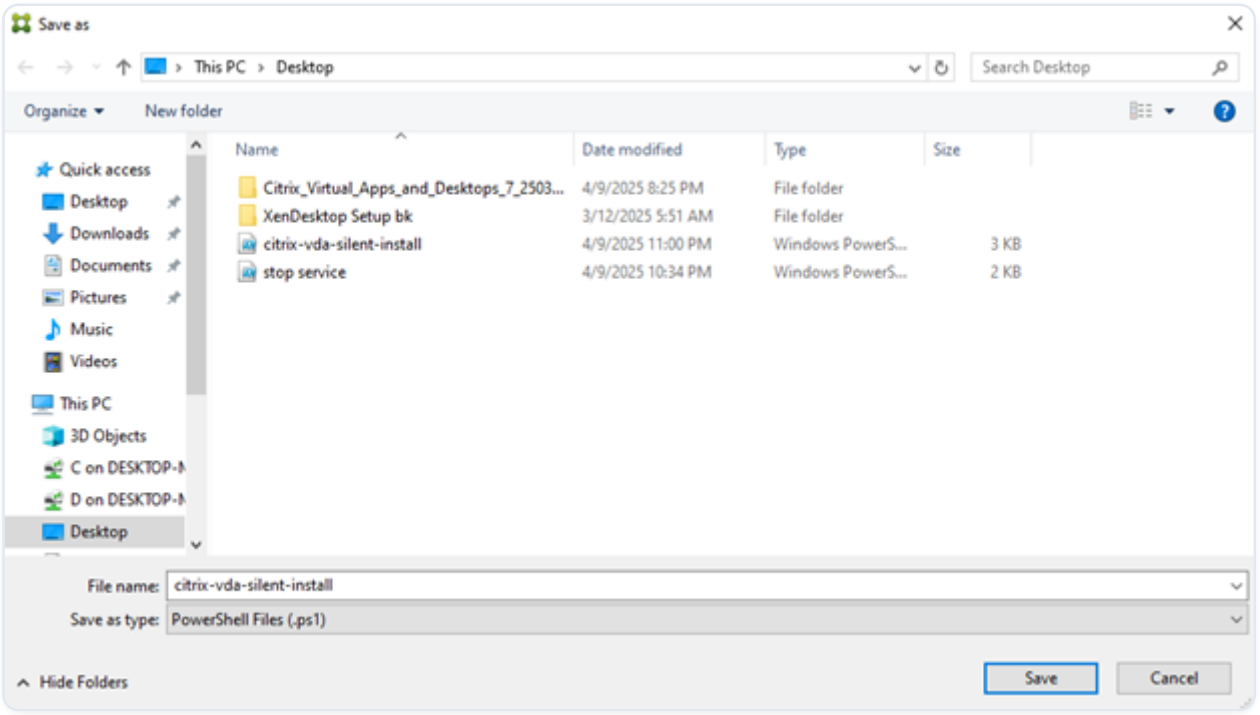
像往常一样在 UI 中配置 VDA 安装选项。在“**摘要**”页面上，选择“**生成自定义脚本**”以根据您的配置创建命令行脚本，如以下屏幕截图所示。



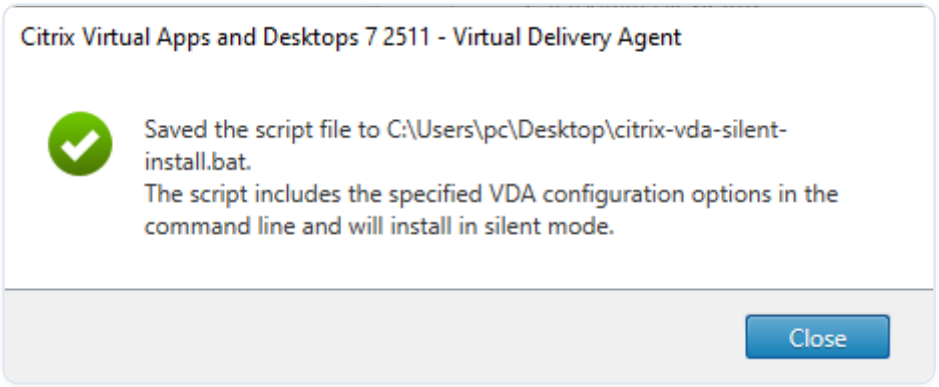
此时将出现一个对话框，提示您选择保存生成脚本的位置。您还可以在保存脚本之前选择其他目录并重命名脚本。



默认情况下，脚本另存为批处理 (.bat) 文件。您也可以选择将其另存为 PowerShell (.ps1) 脚本。



脚本生成并保存后，将出现一个确认对话框，显示文件位置并描述脚本的用途。您可以使用任何文本编辑器（例如记事本）编辑生成的脚本。运行脚本之前，请退出安装程序 UI。一次只能运行一个 VDA 安装或升级过程。



步骤 2. 使用生成的脚本安装或升级 VDA

以下屏幕截图显示了如何使用生成的批处理文件安装或升级 VDA。唯一必需的参数是 VDA 安装程序的路径。如果安装程序路径有效，脚本将运行安装或升级，并以与 VDA 安装程序相同的退出代码退出。将显示可读的结果消息以指示过程的结果。

运行生成的批处理(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/run-generated-batch.png)

以下屏幕截图显示了如何使用生成的 PowerShell 脚本安装或升级 VDA。唯一必需的参数是 VDA 安装程序的路径。如果安装程序路径有效，脚本将运行安装或升级，并以与 VDA 安装程序相同的退出代码退出。将显示一条可读的状态消息，指示该过程的结果。

运行生成的 PS1(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/run-generated-ps1.png)

> **注意：**

> 如果 Delivery Controller 配置了注册令牌，请按照以下屏幕截图所示运行脚本。

> 带 Web Socket 令牌的脚本(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/run-generated-script-with-websocket-token.png)

该脚本需要以下参数：`<Path-to-generated-script>`、`<Path-to-vda-installer>`、`<Websocket-token-value>`。

第三方 VDA 部署方法

为了使用 Microsoft System Center Configuration Manager (SCCM) 或类似的软件分发工具（例如 Ansible 和 Microsoft Intune）成功部署 Virtual Delivery Agent (VDA)，Citrix® 建议按一系列步骤使用 VDA 安装程序。

> **注意：**

> 以下文章仅描述了基于 Citrix 测试环境的建议。您可以根据自己的需求自定义这些步骤。Citrix 不对为满足客户需求而对本文档进行的任何更新或调整负责。

- 使用 SCCM 安装 VDA
- 使用 Ansible 安装 VDA
- 使用 Microsoft Intune 安装 VDA

使用 SCCM 安装 VDA

概述

Microsoft Endpoint Configuration Manager，前身为 System Center Configuration Manager (SCCM)，是一款 Windows 产品，可实现企业范围内设备和应用程序的管理、部署和安全。

> **注意：**
>
> 以下文章仅描述了基于 Citrix® 测试环境的建议。您可以根据自己的需求自定义这些步骤。Citrix 不对为满足客户需求而进行的任何更新或调整负责。

建议

- 为了成功部署 Virtual Delivery Agent (VDA) 使用 SCCM 或类似的软件分发工具，Citrix 建议使用按步骤安装 VDA 安装程序。
- Citrix 不建议在 VDA 安装或升级过程中使用 VDA 清理实用程序。仅当 VDA 安装程序之前失败时，才在有限情况下使用 VDA 清理实用程序。

开始之前

VDA 安装期间所需的重新启动次数取决于环境。例如：

- 挂起的更新或早期软件安装导致的重新启动可能需要重新启动。
- 以前被其他进程锁定的文件可能需要更新，从而强制进行额外重新启动。
- VDA 安装程序中的某些可选组件（例如 Citrix Profile Management 和 Citrix Files）可能需要重新启动。
- 升级 VDA 时，安装 VDA 的计算机必须处于维护模式，且没有会话。
- 当 VDA 首次在计算机上运行时，所使用的 VDA 安装程序会复制到该计算机上。 有关 VDA 安装的更多信息，请参阅(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-prepare.html#installers)。

SCCM 任务序列器管理所有必需的重新启动。

使用 SCCM 部署 VDA 的关键步骤

以下步骤描述了如何使用 SCCM 在虚拟机上部署 VDA。

1. (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-vdas/third-party-vda-deployment-methods/install-vdas-sccm.html#step-1-install-the-vda)。
2. 创建组织单位 (OU)。
3. 验证计算机。
4. 使用 VDA 分发内容。

步骤 1：安装 VDA
确定所有必备条件后，使用 **SCCM 任务序列器**完成以下任务：

1. 从安装介质的可访问副本或从某个 VDA 独立安装程序安装 VDA：
   - `VDAWorkstationSetup_XXXX.exe`
   - `VDAServerSetup_XXXX.exe`
   - `VDAWorkstationCoreSetup_XXXX.exe`

   有关 VDA 安装程序的详细信息，请参阅安装程序。

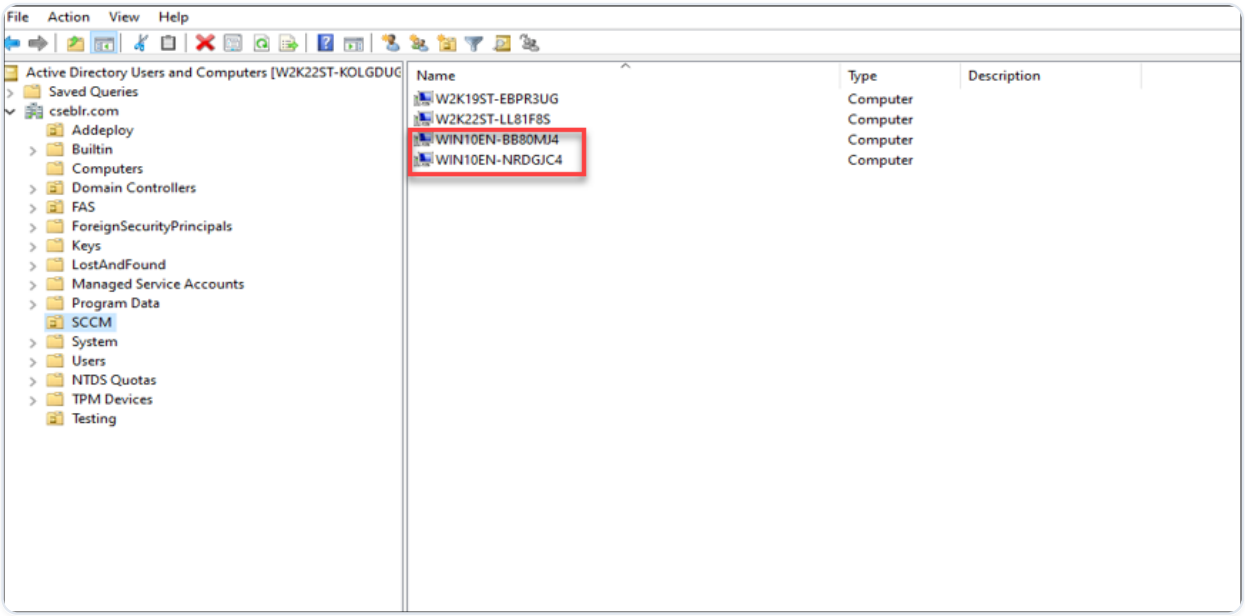
   > **注意：**
   >
   > 升级 VDA 时，安装 VDA 的计算机必须处于维护模式，且没有会话。

2. 当 VDA 首次在计算机上运行时，所使用的 VDA 安装程序会复制到该计算机上。
   - 当您使用 `VDAWorkstationCoreSetup_XXXX.exe` 以外的 VDA 安装程序时，VDA 安装程序将复制到 `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`。
   - 当您使用 `VDAWorkstationCoreSetup_XXXX.exe` 时，VDA 安装程序将复制到 `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe.`.
3. VDA 安装程序的目录位置也存储在注册表 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall”` `“MetaInstallerInstallLocation”` 中。
4. 将命令行选项 `/NOREBOOT`、`/NORESUME` 和 `/QUIET` 添加到您的命令行选项中。

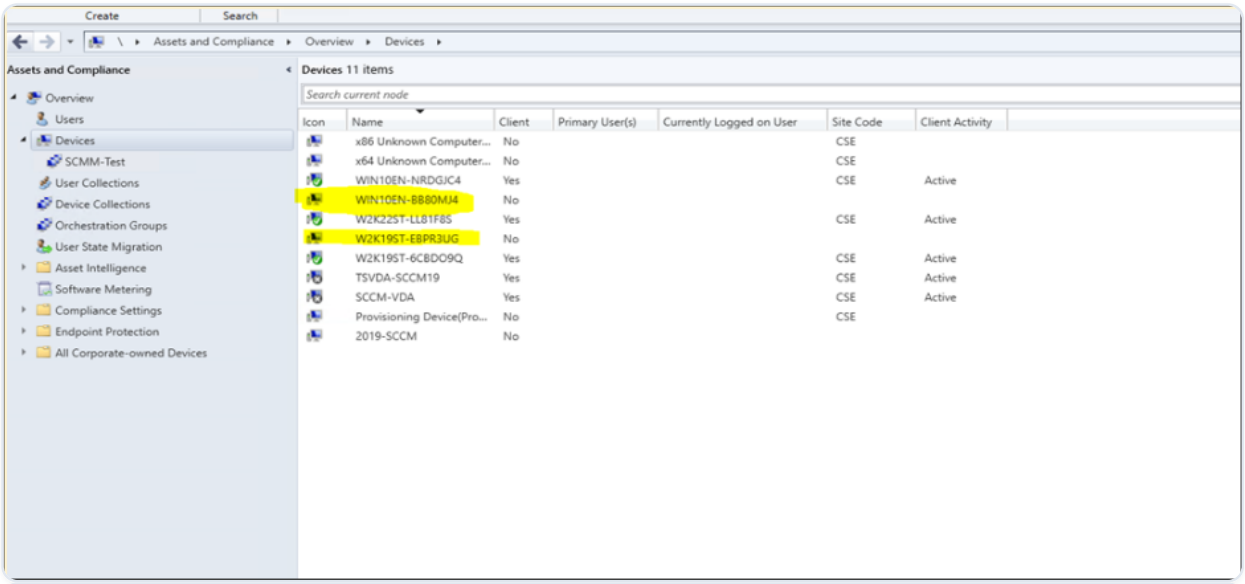
- `/QUIET`：安装期间不显示用户界面，以便 SCCM 控制安装过程。
- `/NOREBOOT`：禁止 VDA 安装程序自动重新启动。SCCM 会在需要时触发重新启动。
- `/NORESUME`：通常，当安装期间需要重新启动时，VDA 安装程序会设置一个 runonce 注册表项（`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`）。Windows 使用该项在计算机重新启动时打开 VDA 安装程序。这对于 SCCM 来说是一个问题，因为 SCCM 无法监视安装并捕获退出代码。

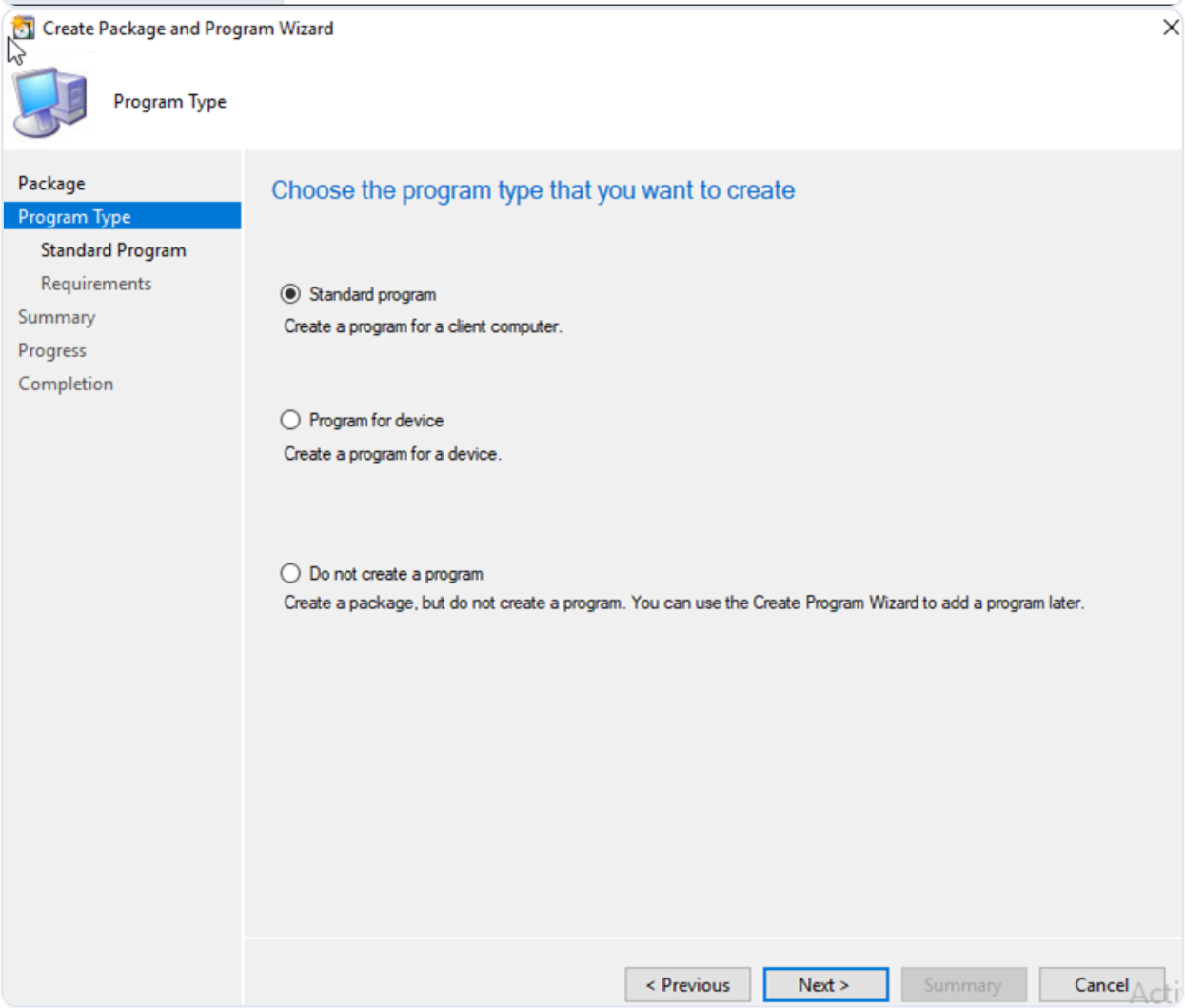
步骤 2：创建组织单位 (OU)

1. 创建要添加到 OU 的两台已加入域的虚拟机。虚拟机最初创建时位于 **Computers** 文件夹中。将虚拟机移动到 **SCCM** 文件夹。 示例：WIN10EN-BB80MJ4.cseblr.com W2K19ST-EBPR3UG.cseblr.com

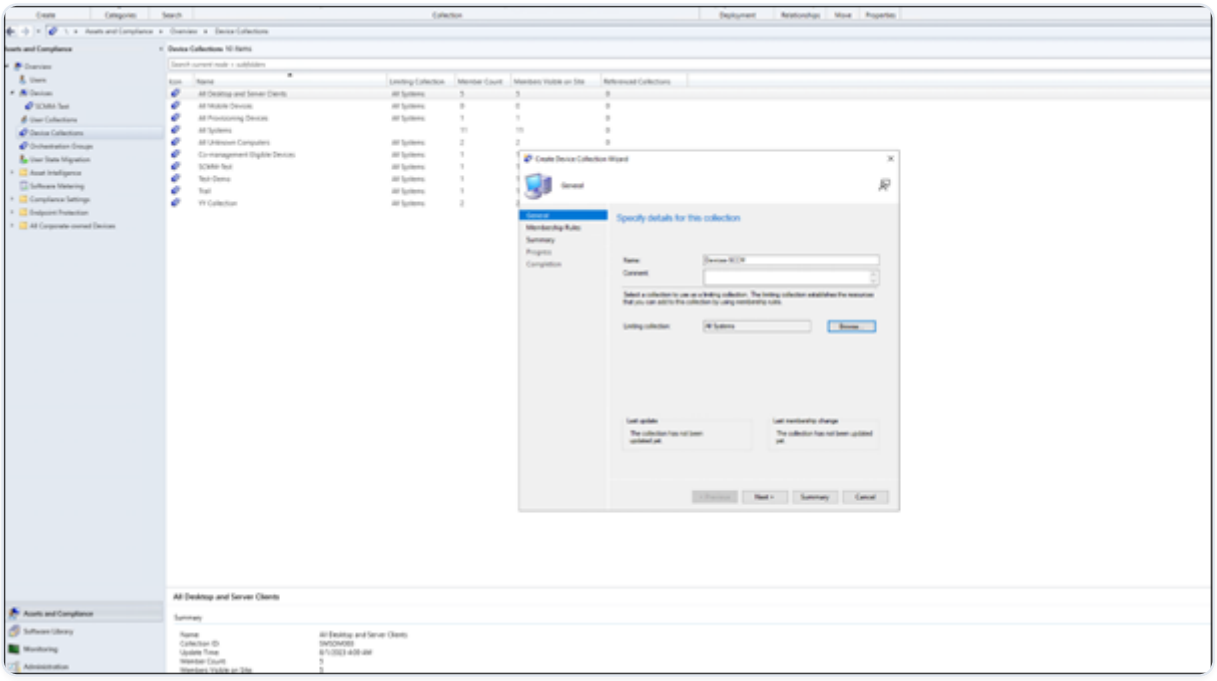


2. 在 微软配置管理器 中，转到 `\Administration\Overview\Hierarchy Configuration\Discovery Methods\`。
3. 单击 **Active Directory 系统发现**，然后选中 **启用 Active Directory 系统发现** 复选框以启用新创建虚拟机的自动发现。
4. 单击  图标以选择新容器。
5. 在**位置**部分中，添加 SCCM 虚拟机所在的**路径**。
6. 转到 `\Administration\Overview\Site Configuration\Sites` 并右键单击 SCCM VDA。
7. 选择**客户端安装设置 > 客户端推送安装**。此时将打开**客户端推送安装属性**窗口。
8. 将 VM 设置为 `Enabled` 后，您可以看到 VM 列表，如以下图像所示。





9. 创建**设备集合**以创建 OU。输入集合名称的**名称**。



10. 遵循向导说明。

    成员资格规则(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/sccm-membership-rules.png)

    OU 已创建。

    OU 创建(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/sccm-create-device-collection-wizard.png)

11. 将创建的 VM 添加到新创建的设备集合中。

    a. 右键单击 VM。选择 **添加选定项目 > 将选定项目添加到现有设备集合**。

       添加项目(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/sccm-add-item-to-device-collection.png)

    b. 在 **选择集合** 窗口中，选择所需的设备名称。在此示例中，它是 `Devices-SCCM`。

       设备列表(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/sccm-list.png)

    `Devices-SCCM` 列在 **资产和合规性 > 概述 > 设备集合** 中。

    列出的设备(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/devices-sccm.png)

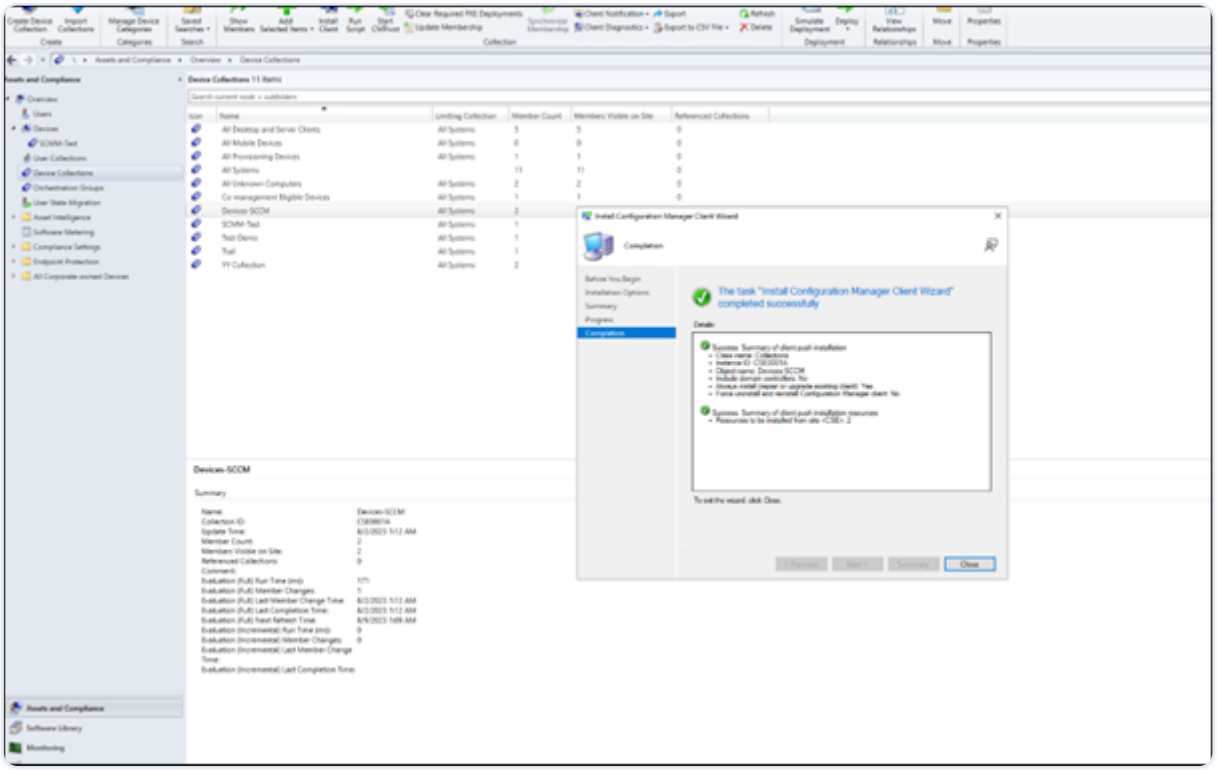
12. 在设备收集器上选择 **安装客户端**。

    安装客户端(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/sccm-install-client.png)

13. 选择所需的安装 **站点**。

    安装站点(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/sccm-install-client-1.png)

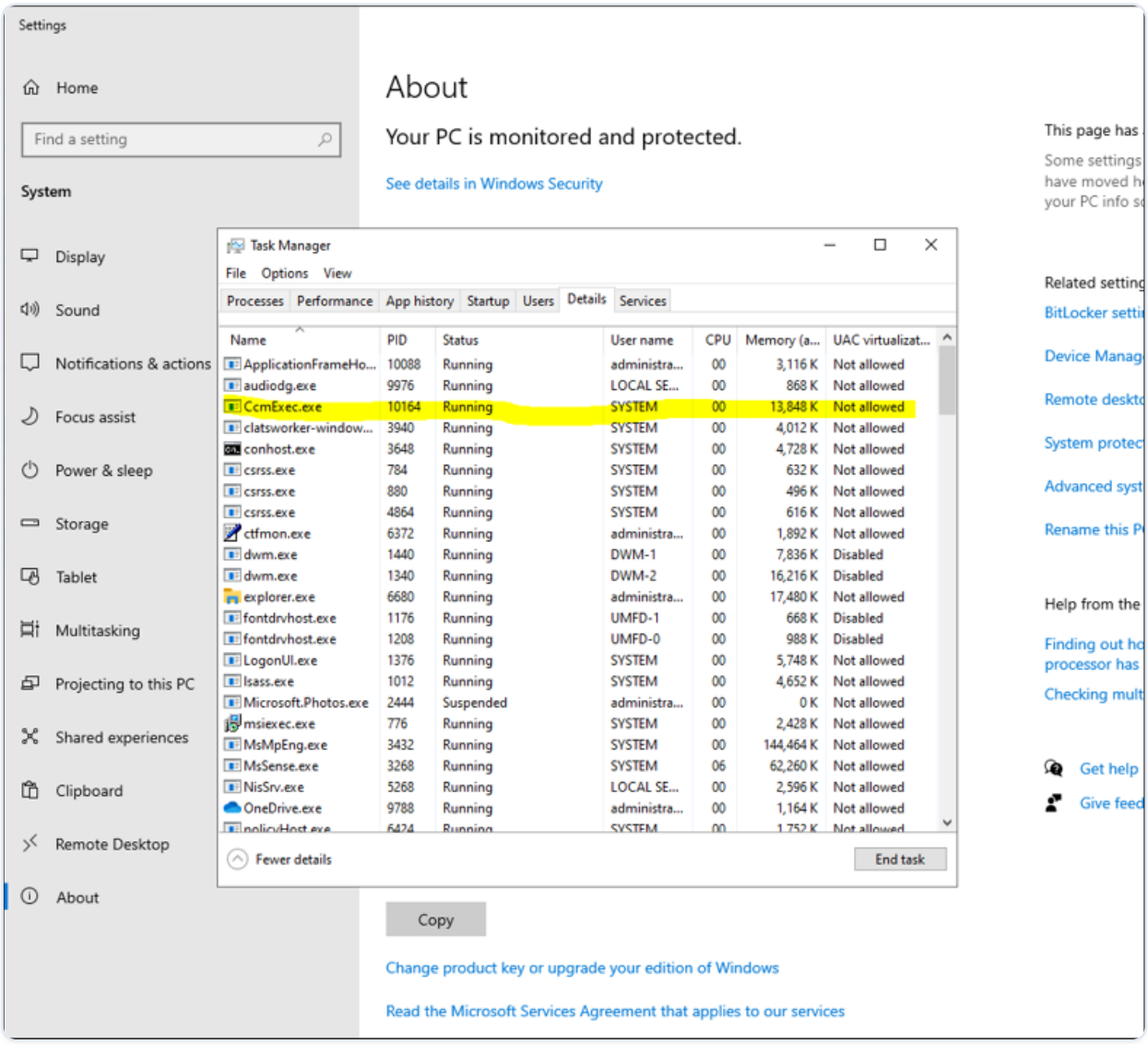
14. 按照向导说明操作。**安装 Configuration Manager 客户端向导**已成功完成。



有关详细信息，请参阅 Microsoft 文档中的管理集合。

步骤 3：验证计算机

1. 在客户端计算机上，通过检查 `CCMExec` 进程是否正在运行来验证客户端是否已安装。



2. 验证 SCCM 上虚拟机的客户端是否正在运行。

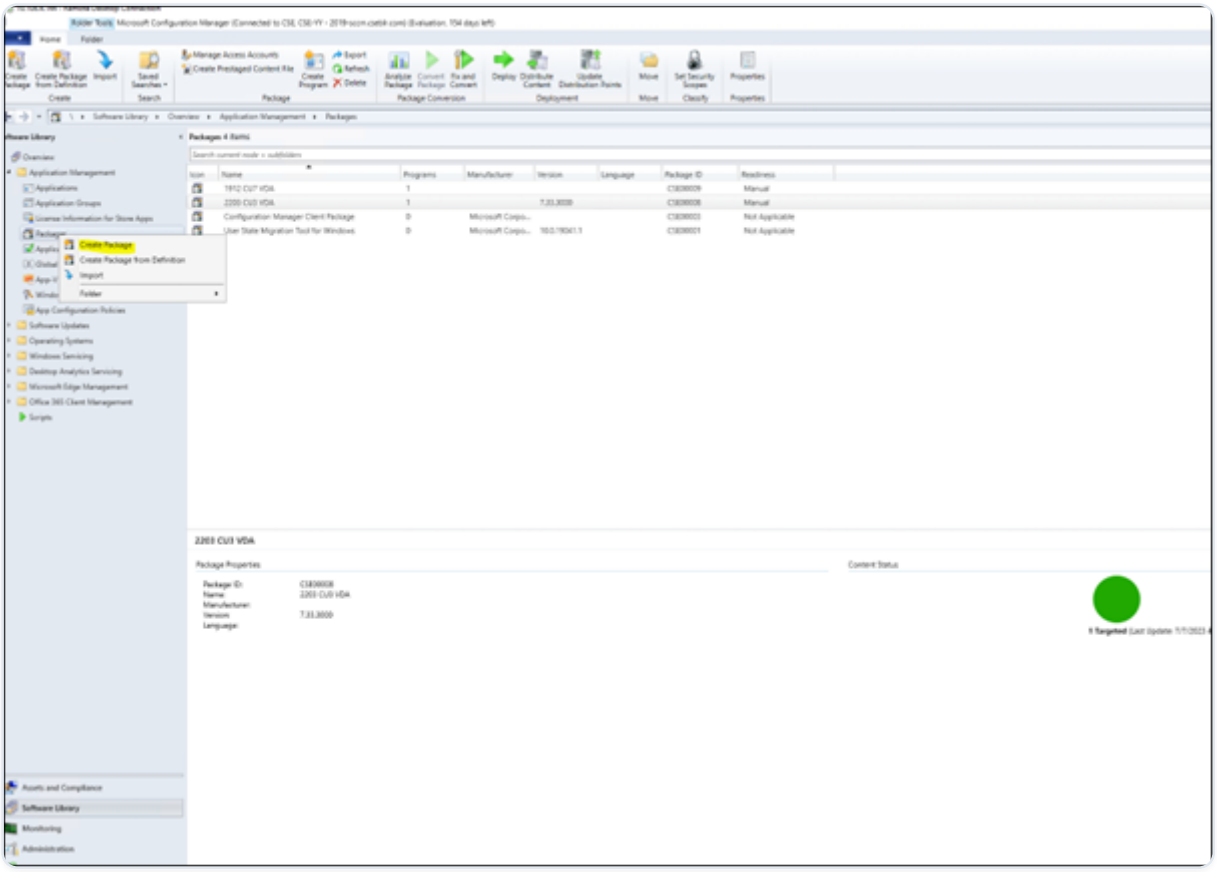
步骤 4：使用 VDA 分发内容

以下步骤介绍了如何使用已部署的 VDA 在关联的虚拟机上分发内容。

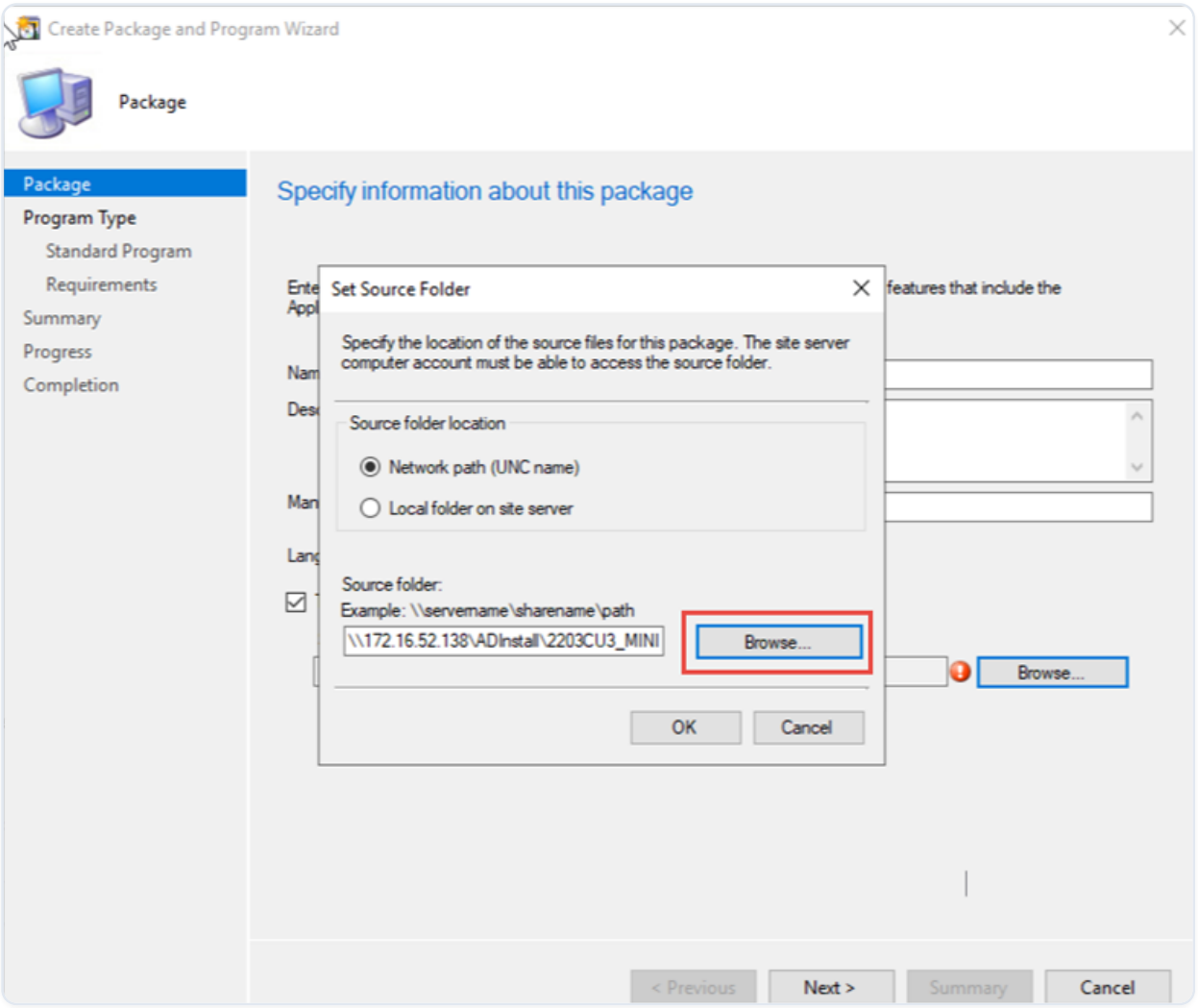
1. 创建程序包
2. 分发内容

创建程序包

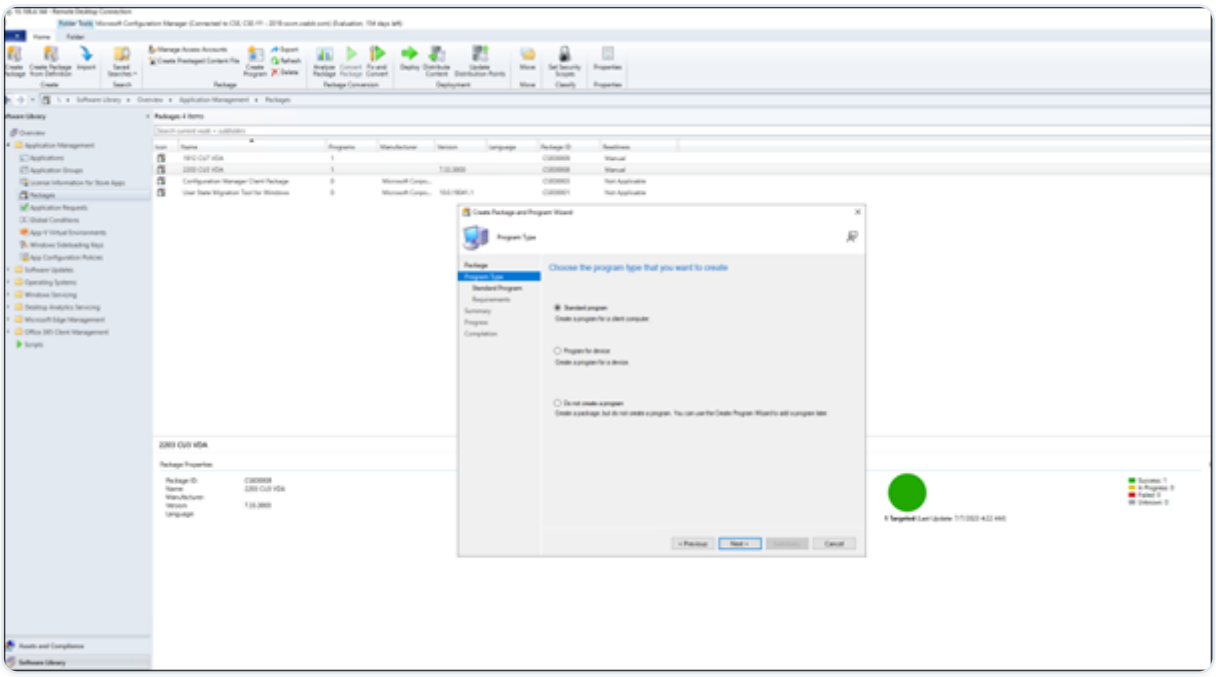
1. 要创建程序包，请右键单击所需的 VDA，然后单击**创建程序包**。



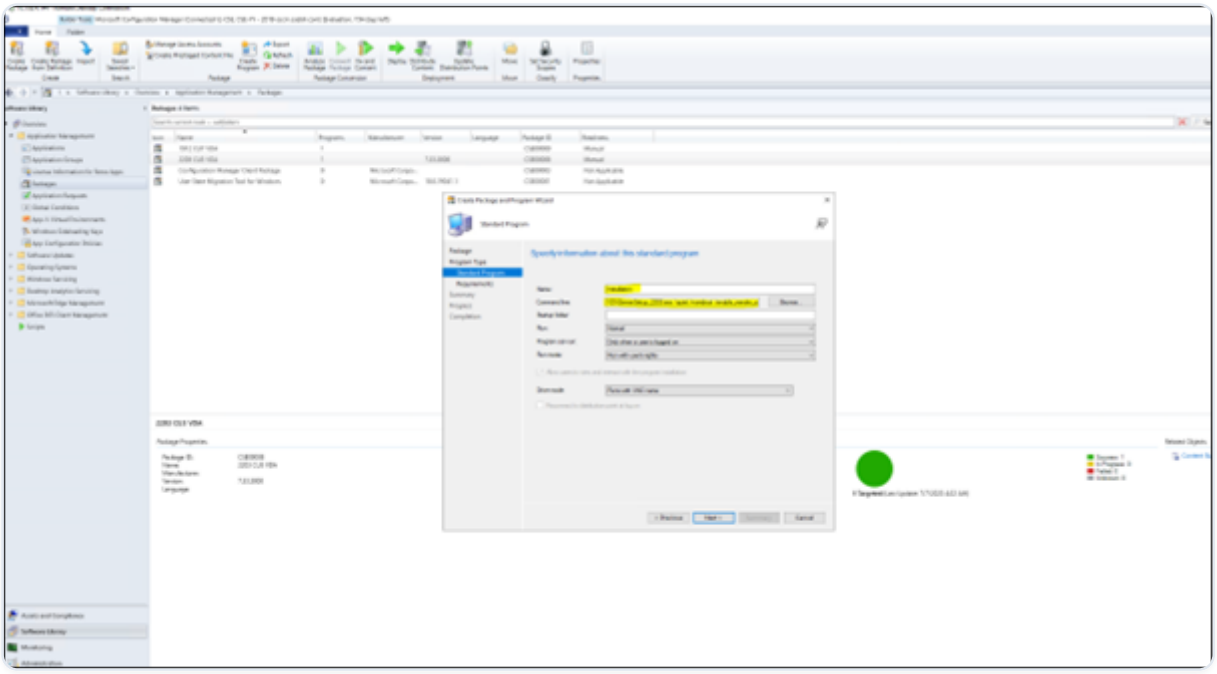
2. 通过单击**浏览**指定此程序包的源文件位置。



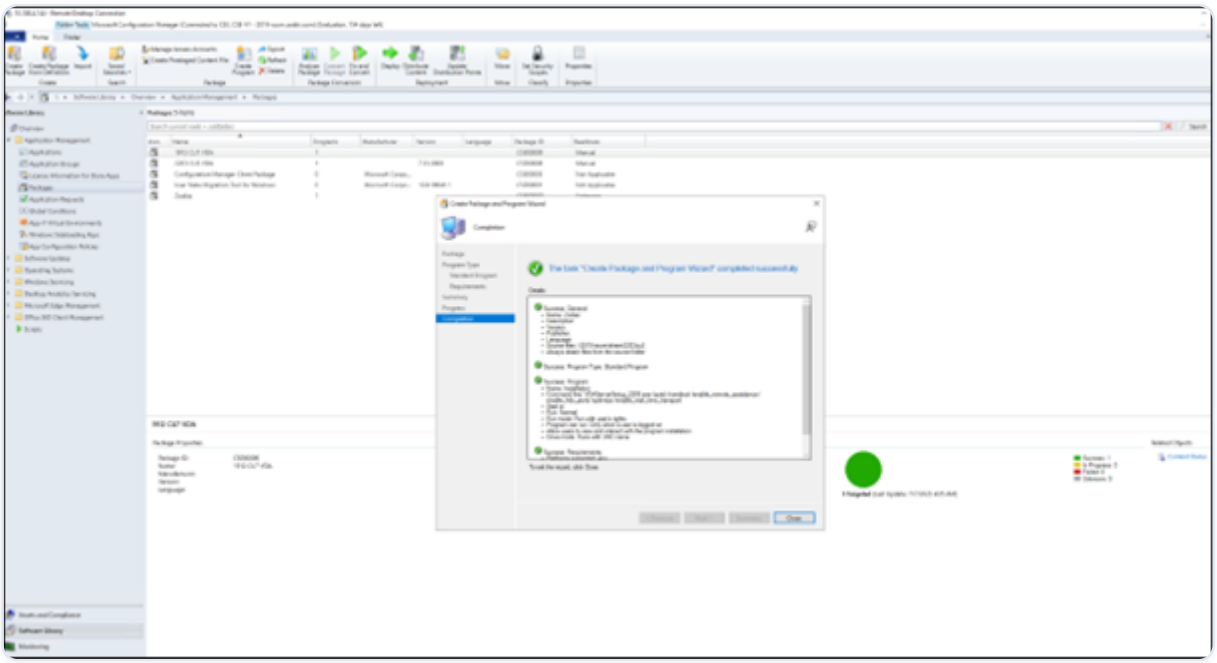
3. 选择所需的程序包类型。



4. 输入程序包的**名称**和**命令行**。



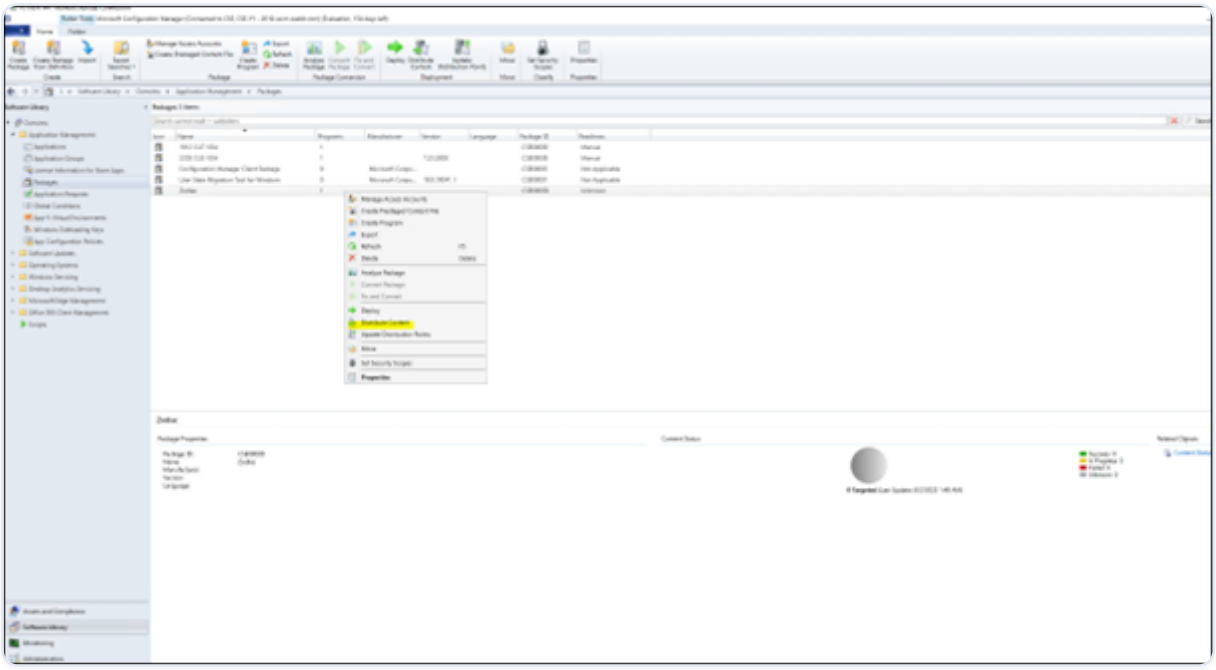
5. 单击“**下一步**”。



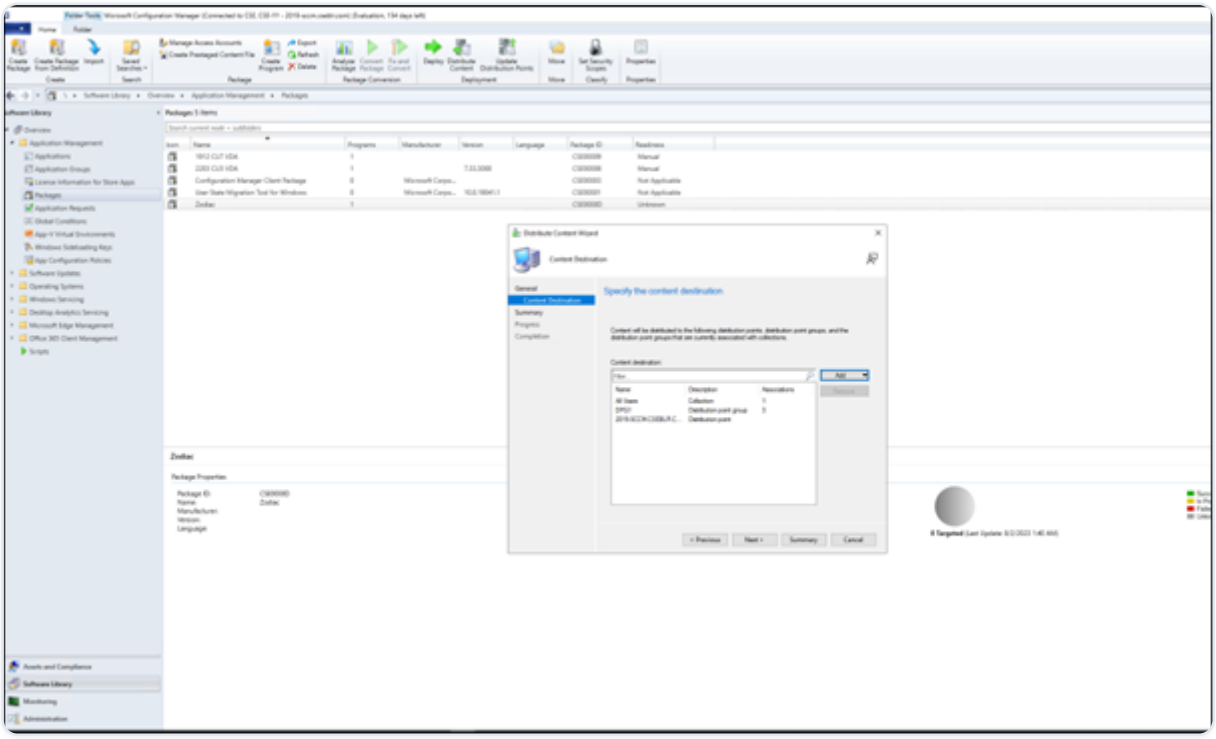
有关详细信息，请参阅 Microsoft 文档中的Configuration Manager 中的程序包和程序。

分发内容

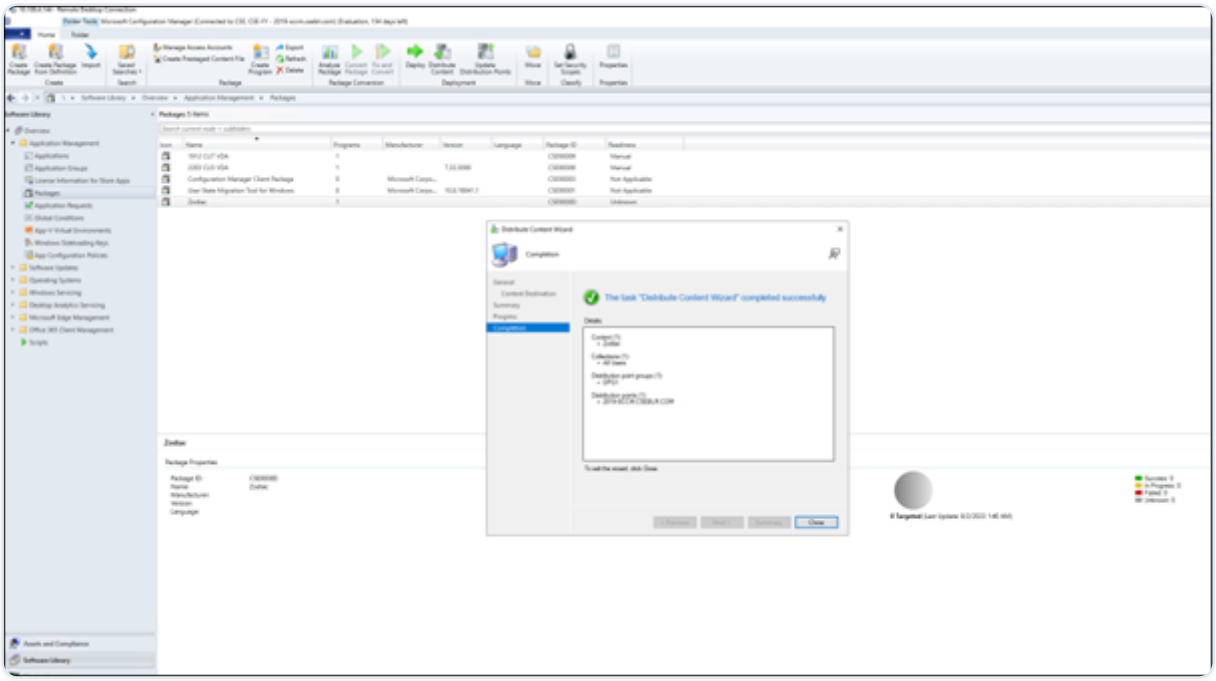
1. 右键单击您已创建的程序包名称。
2. 选择**分发内容**。



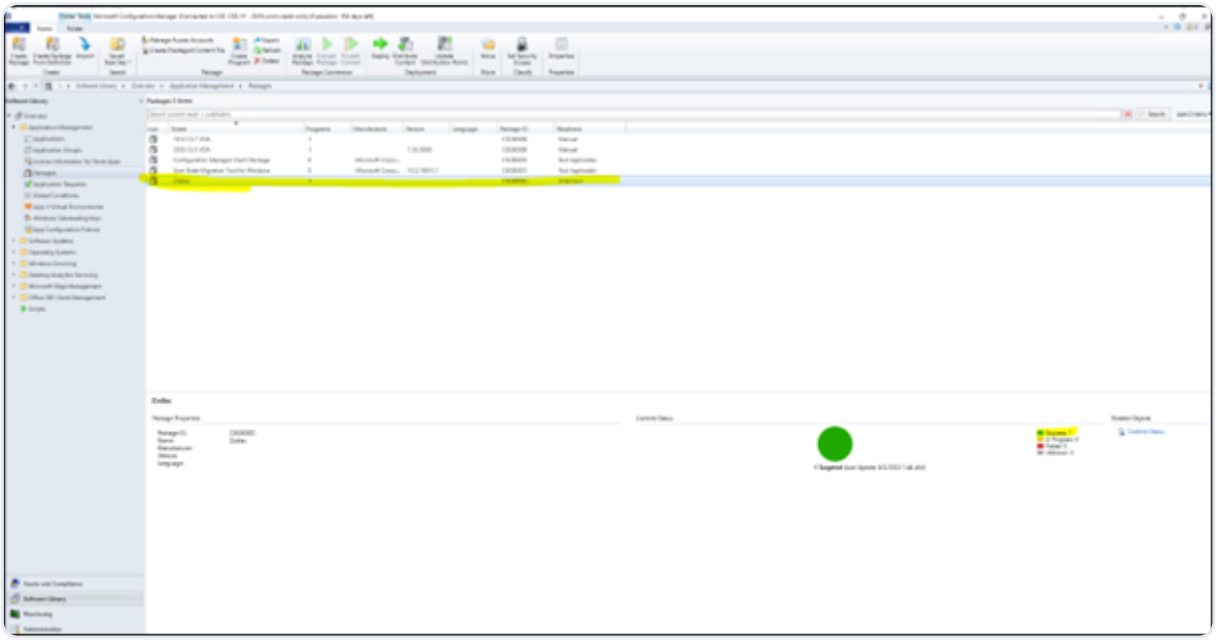
3. 在**分发内容向导**窗口中，选择您已创建的程序包的源文件位置。在此示例中，它是 `2019-SCCM` 。单击**下一步**。



4. 验证程序包（在此示例中为 `Zodiac` ）是否可用于部署。



下图显示了可用于部署的软件包。

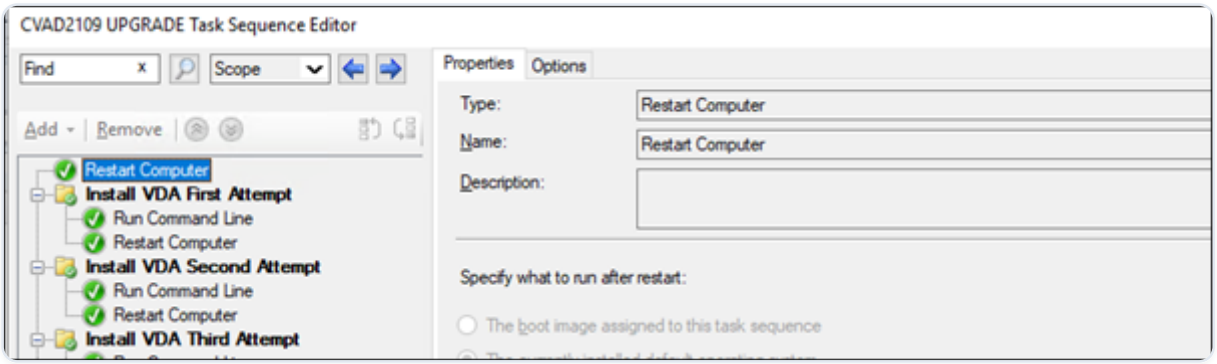


有关详细信息，请参阅 Microsoft 文档中的 部署和管理 Configuration Manager 的内容。

使用 SCCM 的安装序列示例

以下示例显示了安装序列。

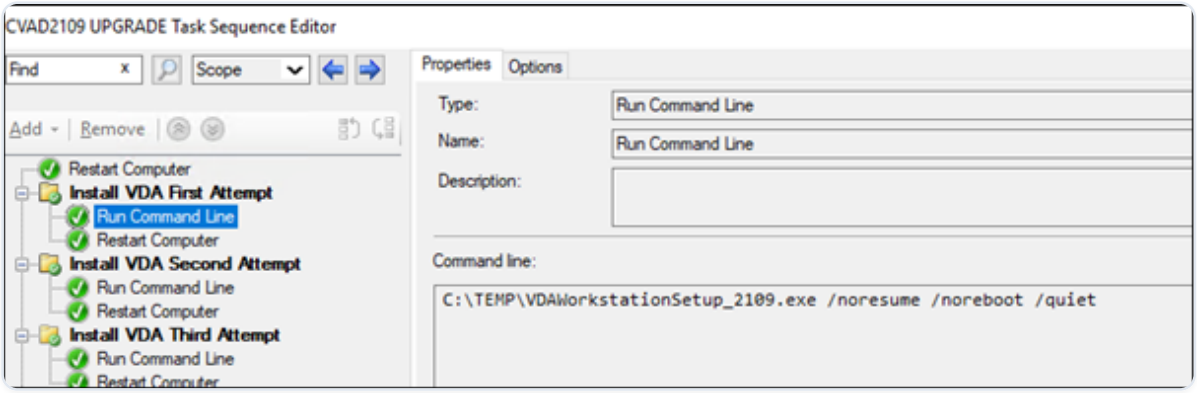
1. **重新启动计算机：** 通过重新启动计算机来准备计算机。



2. **首次尝试安装 VDA：** 开始 VDA 安装。

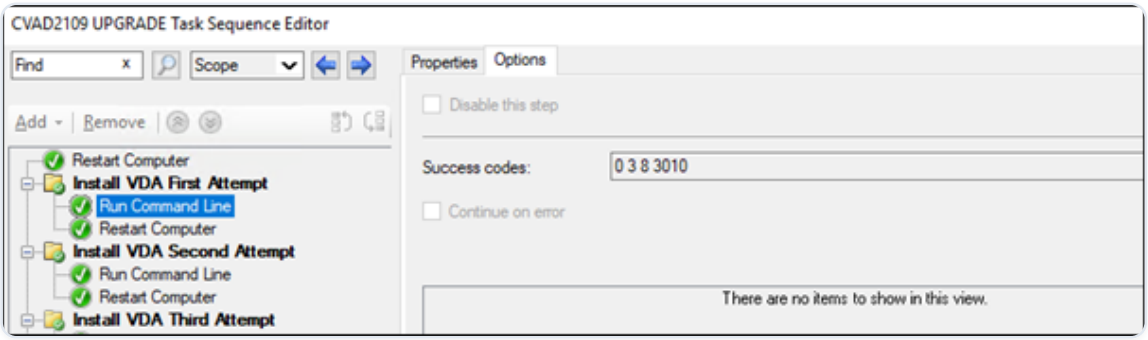
   a. 将 `/quiet`、`/noreboot` 和 `/noresume` 选项添加到命令行选项中。

   b. 运行您选择的 VDA 安装程序（本地映像或其中一个最小安装程序）。

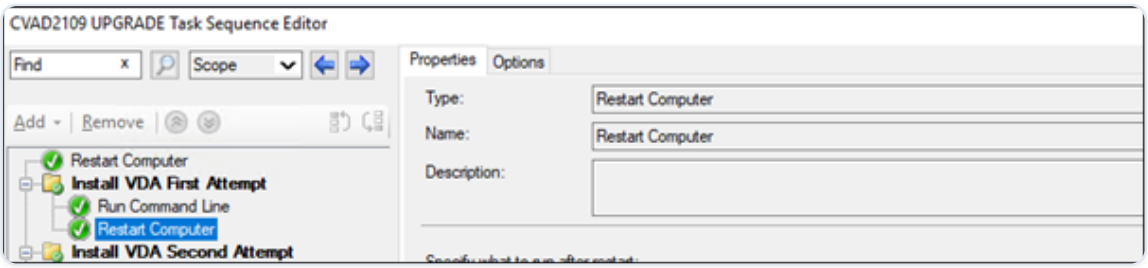


   c. SCCM 必须捕获返回代码。

   - 如果返回代码为 0 或 8，则安装完成，需要重新启动。

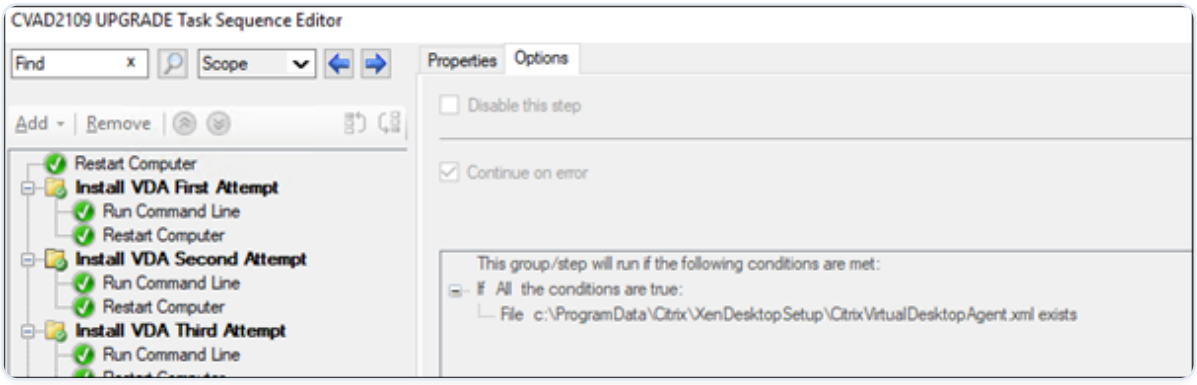


   - 如果返回代码为 3，请重新启动计算机，然后将控制权传递给**第二次尝试安装 VDA**。



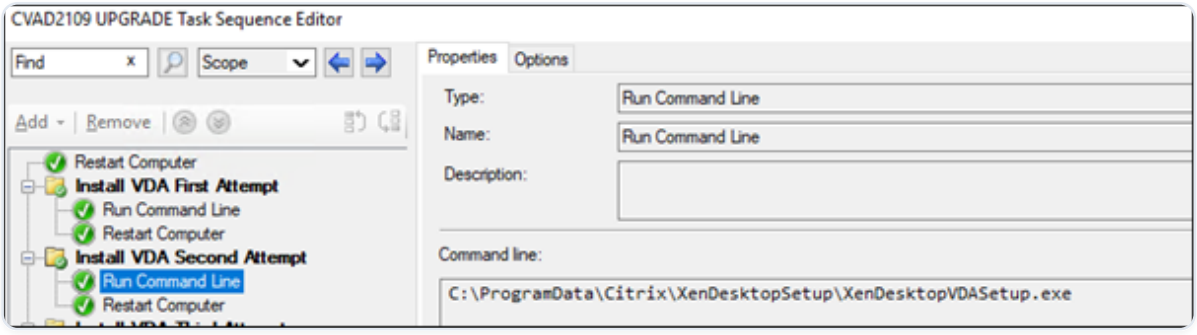
3. **VDA 第二次安装尝试：** 继续 VDA 安装。

a. 在**VDA 第一次安装尝试**之后，如果文件 `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` 存在，则表示安装未完成，必须在重新启动完成后继续安装。



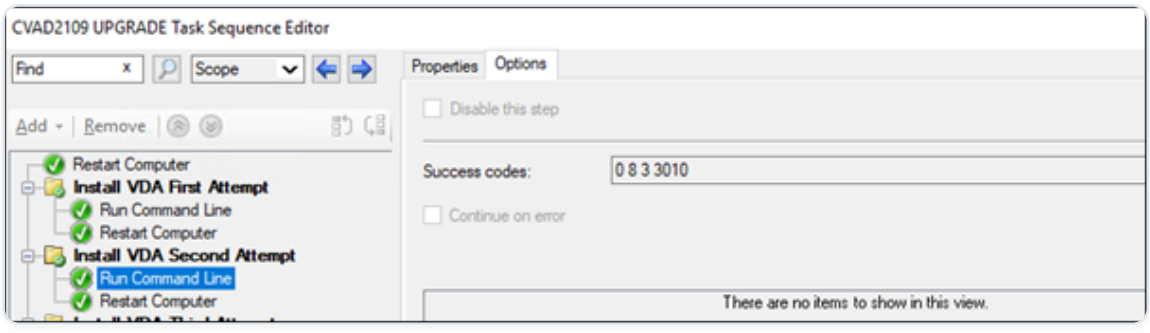
b. **VDA 第二次安装尝试**会重复，直到文件 `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` 不存在或返回除 0 或 8 之外的返回代码。将任何其他返回代码视为错误，并且 VDA 第二次安装尝试应报告错误并停止。

c. 通过从文件 `%programdata%\ Citrix\XenDesktopSetup\` 目录运行相应的 VDA 安装程序（大多数情况下为 `XenDesktopVdaSetup.exe`，如果使用了 `VDAWorkstationCoreSetup_XXXX.exe` 则为 `XenDesktopRemotePCSetup.exe`），且不带任何命令行参数，来恢复 VDA 安装。（VDA 安装程序会使用其在首次运行安装程序时保存的参数。）



d. 注意 VDA 安装程序返回的代码。

- 0 或 8：成功，安装完成，需要重新启动。



- 3：安装未完成。重新启动计算机并重复 VDA 第二次安装尝试，直到文件 `%programdata%\ Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` 不存在或返回 0 或 8。将任何其他返回代码视为错误，并且 VDA 第二次安装尝试应报告错误并结束。

有关返回代码的详细信息，请参阅Citrix 安装返回代码。

VDA 安装命令示例

可用的安装选项因所使用的安装程序而异。有关命令行选项的详细信息，请参阅以下文章。

- 安装 VDA
- 使用命令行安装

远程电脑访问的安装命令

- 以下命令使用单会话核心 VDA 安装程序 (`VDAWorkstationCoreSetup.exe`)：

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- 以下命令使用单会话完整 VDA 安装程序 (`VDAWorkstationSetup.exe`)：

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

专用 VDI 的安装命令

- 以下命令使用单会话完整 VDA 安装程序 (`VDAWorkstationSetup.exe`)：

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
  ```

使用 Ansible 安装 VDA

概述

本文介绍了如何使用 Ansible 部署 VDA。有关更多信息，请参阅 Ansible 文档。

> **注意：**
>
> 本文仅介绍基于 Citrix® 测试环境的建议。您可以根据自己的需求自定义这些步骤。Citrix 不对为满足客户需求而对本文进行的任何更新或调整负责。

使用 ANSIBLE 部署 VDA 的关键步骤

1. 配置虚拟机环境。
2. 安装 Ansible
3. Kerberos 配置
    a. 安装 Kerberos
    b. 配置 Kerberos
4. 配置 Ansible

步骤 1：配置虚拟机环境
在 Windows 服务器上运行以下命令。

1. 设置 PS RemoteSigned。 `Set-ExecutionPolicy RemoteSigned`
2. 将 WinRM 设置为使用未加密连接： `winrm set winrm/config/service '@{AllowUnencrypted="true"}'`

> **注意：**
>
> 如果此步骤中发生错误，请使用以下命令： `Enable-PSRemoting -Force`

3. 打开防火墙端口 5985。 `New-NetFirewallRule -DisplayName "Allow WinRm port 5985" -Direction Inbound -Profile Any -Action Allow -LocalPort 5985 -Protocol tcp`

步骤 2：安装 Ansible
要在 Ubuntu 20.4 或更高版本上安装 Ansible，请运行以下命令：

- `sudo apt update`
- `sudo apt install software-properties-common`
- `sudo add-apt-repository --yes --update ppa:ansible/ansible`
- `sudo apt install ansible`
- `sudo apt install python3-pip`

步骤 2i：安装 Kerberos
要安装 Kerberos，请运行以下命令。

`sudo apt install python3-dev libkrb5-dev krb5-user`

步骤 2ii：配置 Kerberos

要配置 Kerberos，请运行以下命令：

`Edit /etc/krb5.conf`

```
[libdefaults]
        default_realm = [redacted]

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented.  In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

#       default_tgs_enctypes = des3-hmac-sha1
#       default_tkt_enctypes = des3-hmac-sha1
#       permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true

[realms]
        LTSRLAB.NET = {
                kdc = [redacted]
                admin_server = [redacted]
        }
        ATHENA.MIT.EDU = {
                kdc = [redacted]
```

注意：

Kerberos 领域名称请使用大写字母。

```
[domain_realm]
        .mit.edu = ATHENA.MIT.EDU
        mit.edu = ATHENA.MIT.EDU
        .media.mit.edu = MEDIA-LAB.MIT.EDU
        media.mit.edu = MEDIA-LAB.MIT.EDU
        .csail.mit.edu = CSAIL.MIT.EDU
        csail.mit.edu = CSAIL.MIT.EDU
        .whoi.edu = ATHENA.MIT.EDU
        whoi.edu = ATHENA.MIT.EDU
        .stanford.edu = stanford.edu
        .slac.stanford.edu = SLAC.STANFORD.EDU
        .toronto.edu = UTORONTO.CA
        .utoronto.ca = UTORONTO.CA
```

步骤 3：配置 Ansible

要配置 Ansible 主机，请完成以下步骤：

1. 运行以下命令：

   `Edit /etc/ansible/hosts`

2. 配置 Delivery Controller `Install.yaml` 文件

   `/QUIET /NOREBOOT /NORESUME /OPTIMIZE /VERBOSELOG /COMPONENTS VDA /CONTROLLERS 'MyDDC.xd.local' /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT`

```
- name: Install multi-session VDA using network share path
  hosts: TSVDA

  tasks:

  - name: mount a cvad iso
    community.windows.win_disk_image:
      image_path: \\            \Ansible\Citrix_Virtual_Apps_and_Desktops_7_1912_9000.iso
      state: present
    become: true
    become_method: runas
    become_flags: logon_type=new_credentials logon_flags=netcredentials_only
    vars:
      ansible_become_user:
      ansible_become_password:
    register: disk_image_out

  - name: copy iso file to c drive temp folder
    ansible.windows.win_copy:
      src: "{{disk_image_out.mount_paths[0]}}"
      dest: C:\Temp\
      remote_src: yes

  - name: unmount iso
    community.windows.win_disk_image:
      image_path: \\            \Ansible\Citrix_Virtual_Apps_and_Desktops_7_1912_9000.iso
      state: absent
    become: true
    become_method: runas
    become_flags: logon_type=new_credentials logon_flags=netcredentials_only
    vars:
      ansible_become_user:
      ansible_become_password:
-- INSERT --                                                                    26,83         Top
```

```
- name: unmount iso
  community.windows.win_disk_image:
    image_path: \\                \Ansible\Citrix_Virtual_Apps_and_Desktops_7_1912_9000.iso
    state: absent
  become: true
  become_method: runas
  become_flags: logon_type=new_credentials logon_flags=netcredentials_only
  vars:
    ansible_become_user:
    ansible_become_password:

- name: stop windows upgrade service
  ansible.windows.win_service:
    name: wuauserv
    start_mode: disabled
    state: stopped

- name: Restart server before install
  ansible.windows.win_reboot:

- name: Install vda from exe
  win_package:
    path: C:\Temp\X64\Xendesktop Setup\XendesktopVdaSetup.exe
    arguments: /quiet /verboselog /PORTNUMBER    /logpath 'C:\CitrixInstallationLogs\TSVDA' /components "VDA,PLUGINS"  /CONT
ROLLERS '                    '  /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT /NOREBOOT /NORESUME
    expected_return_code: [0, 3,3010]
  register: install_vda

- name: debug 1
  debug:
    msg: "{{install_vda}}"

- name: Restart server
```

```
  register: install_vda

- name: debug 1
  debug:
    msg: "{{install_vda}}"

- name: Restart server
  win_reboot:
  when: install_vda.changed

- name: Resume VDA install
  win_package:
    path: C:\Temp\X64\Xendesktop Setup\XendesktopVdaSetup.exe
    expected_return_code: [0,3,3010]
  when: install_vda.changed
  register: vda_resume

- name: debug 2
  debug:
    msg: "{{vda_resume}}"

- name: Restart server after VDA install
  win_reboot:
  when: vda_resume.changed

- name: find files
  win_find:
    paths: C:\ProgramData\Citrix\XendesktopSetup\XendesktopVdaSetup.exe
  register: vda_install_find
```

```
- name: Resume VDA install
  win_package:
    path: C:\Temp\X64\Xendesktop Setup\XendesktopVdaSetup.exe
    expected_return_code: [0,3,3010]
  when: install_vda.changed
  register: vda_resume

- name: debug 2
  debug:
    msg: "{{vda_resume}}"

- name: Restart server after VDA install
  win_reboot:
  when: vda_resume.changed

- name: find files
  win_find:
    paths: C:\ProgramData\Citrix\XendesktopSetup\XendesktopVdaSetup.exe
  register: vda_install_find

- name: Restart server after VDA install
  win_reboot:
  when: vda_install_find.matched == 0

- name: remove temp folder
  win_file:
    path: C:\Temp\
    state: absent
```

3. 使用以下命令运行 yaml 文件： `sudo ansible-playbook install.yml -vvv` （详细模式）
4. 您可以在配置文件中配置多个主机以及其他附加配置。

`Edit /etc/ansible/hosts`

```
[WSVDA]

[TSVDA]

[WSVDA:vars]
ansible_port=
ansible_user =
ansible_password =
ansible_connection = winrm
ansible_winrm_transport = kerberos
ansible_winrm_server_cert_validation = ignore

[TSVDA:vars]
ansible_port=
ansible_user =
ansible_password =
ansible_connection = winrm
ansible_winrm_transport = kerberos
ansible_winrm_server_cert_validation = ignore
```

使用 Microsoft Intune 安装 VDA

概述

本文介绍如何使用 Microsoft Intune 部署 VDA。有关详细信息，请参阅 Microsoft 文档。

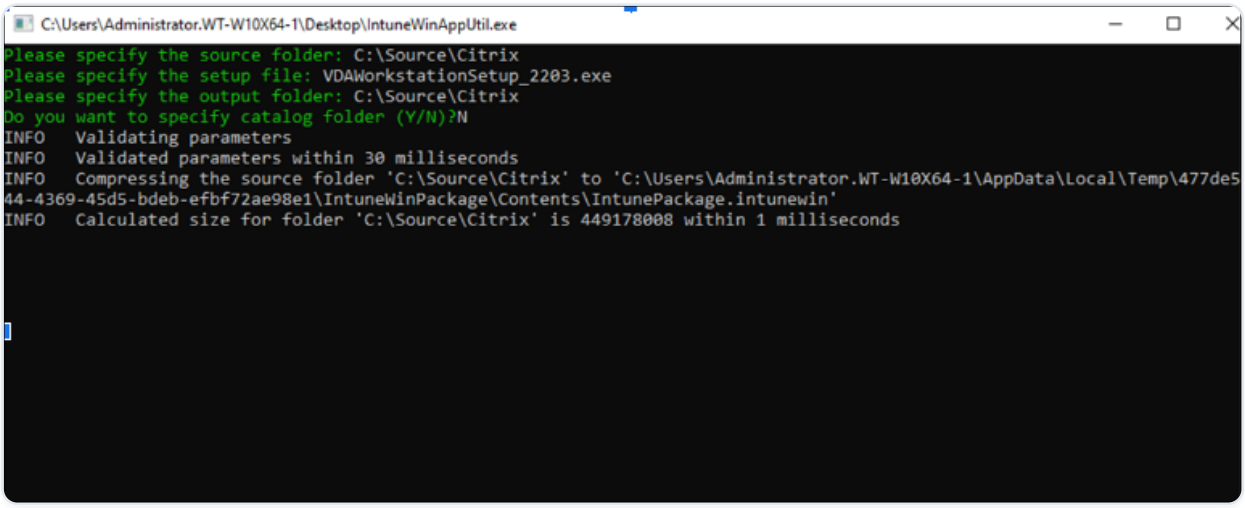
> **注意：**
>
> 以下文章仅描述了基于 Citrix® 测试环境的建议。您可以根据需要自定义这些步骤。Citrix 不对为满足客户需求而进行的任何更新或调整负责。

使用 MICROSOFT INTUNE 部署 VDA 的关键步骤

1. 准备 Citrix VDA 的安装。
2. 设置 Microsoft 365 开发人员计划订阅者。
3. 添加和分配应用程序。
4. 在已注册设备上安装应用程序。

步骤 1：准备 Citrix VDA 的安装

1. 从 GitHub 下载更新的 IntuneWinAppUtil.exe。
2. 使用**以管理员身份运行**来运行 `IntuneWinAppUtil.exe` 文件。
3. 输入以下数据：



a. **请指定源文件夹**：输入包含应用程序安装文件的文件夹。例如，C:\source\Citrix。

b. **请指定安装文件**：输入安装文件名称（例如 setup.exe 或 setup.msi）。例如，VDAWorkstationSetup_2203.exe。

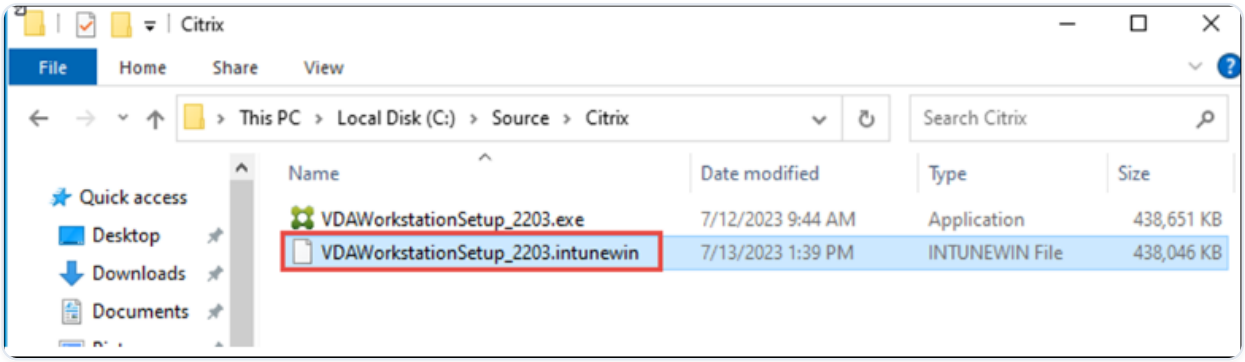
c. **请指定输出文件夹**：输入输出文件夹的路径以生成 .intunewin 文件。例如，C:\source\Citrix。

d. **是否要指定目录文件夹 (Y/N)**：键入 N。

> **注意：**
>
> 请稍候几分钟，直到 **Win32 Content Prep Tool** 运行完毕。一旦它生成了 `.intunewin` 文件，命令提示符底部会显示 100% 的状态。

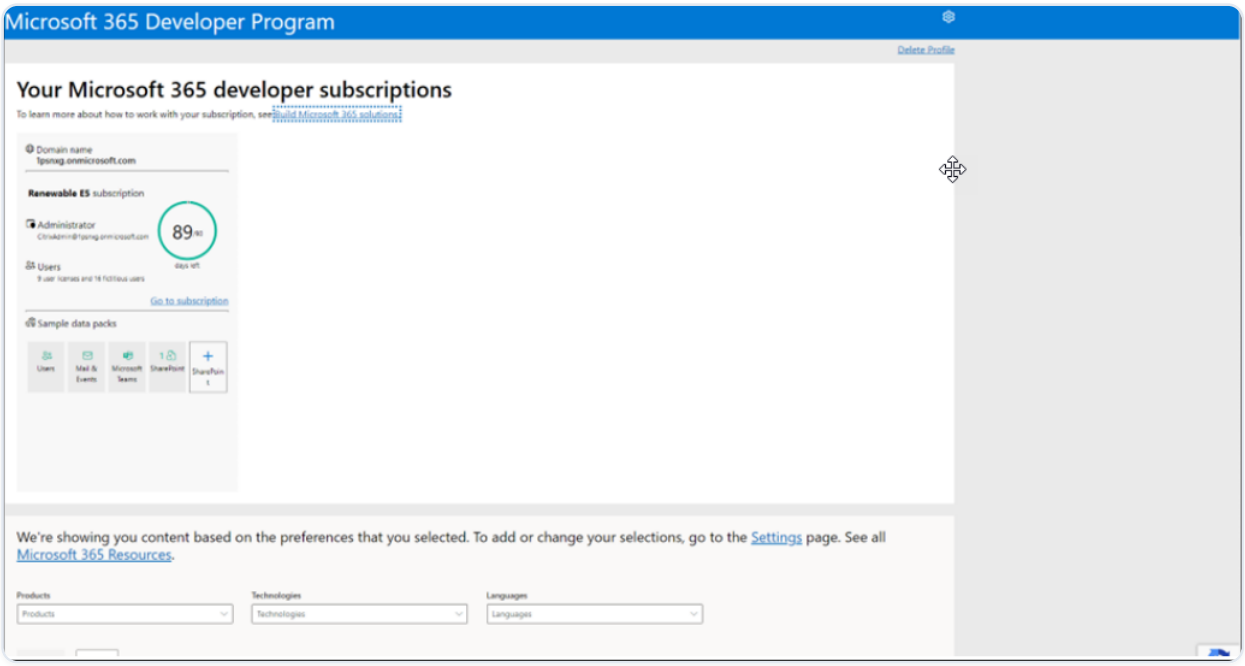
4. 进程完成后，转到输出文件夹（在此示例中为 `C:\source\Citrix`）以获取 Microsoft Intune 部署文件。

5. 注册 Microsoft Intune 免费试用版。

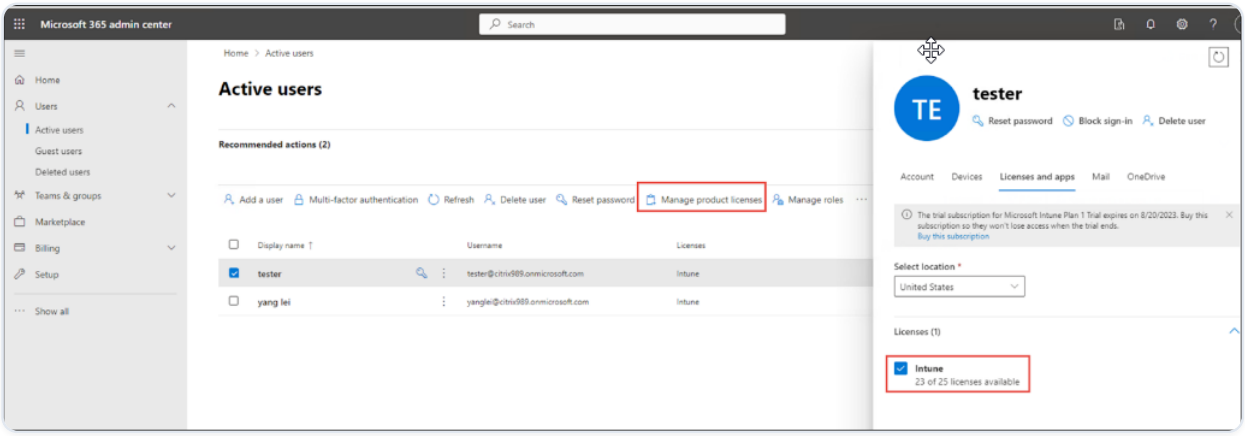


步骤 2：设置 Microsoft 365 开发人员计划订阅者

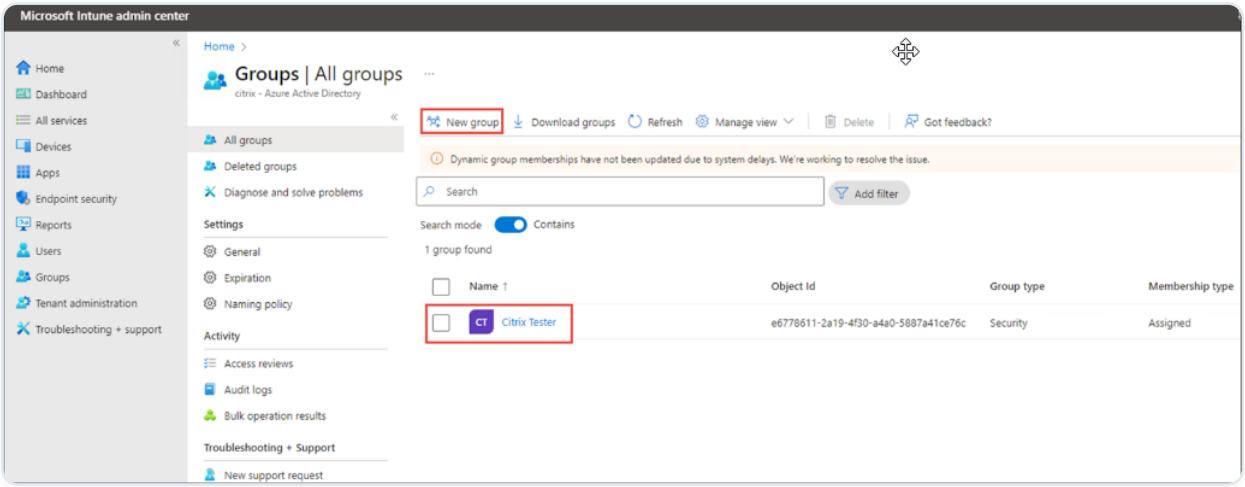
1. 创建即时沙盒以激活您的订阅。 要获取您的开发人员沙盒，请转到您的 Microsoft 365 开发人员计划仪表板 并选择 **添加新订阅**。



2. 在 Microsoft 365 管理中心创建用户并为该用户分配许可证。



3. 创建组。



4. 创建组后，您必须向该组提供 MDM 权限。设置自动注册。这可能需要一分钟才能激活。 或者，您可以通过完成以下步骤手动将 MDM 权限添加到组中：

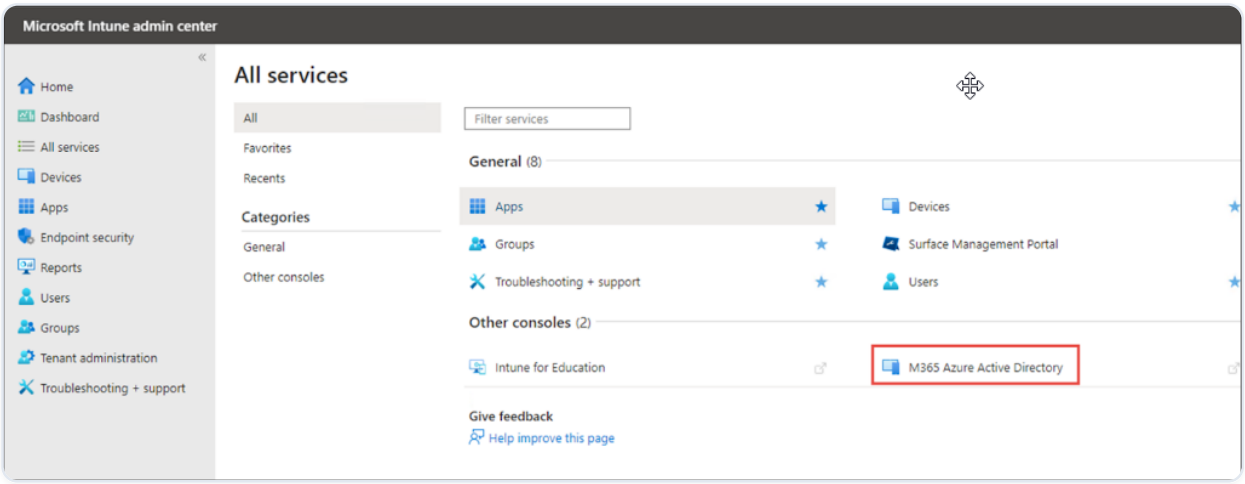
   a. 转到 **所有服务 > Microsoft Entra**。

   b. 转到 **设置 > 移动性** 并选择 **Microsoft Intune**。

   c. 选择您刚刚创建的组。这将打开一个包含 MDM 用户范围的页面。

   d. 点击 **保存**。

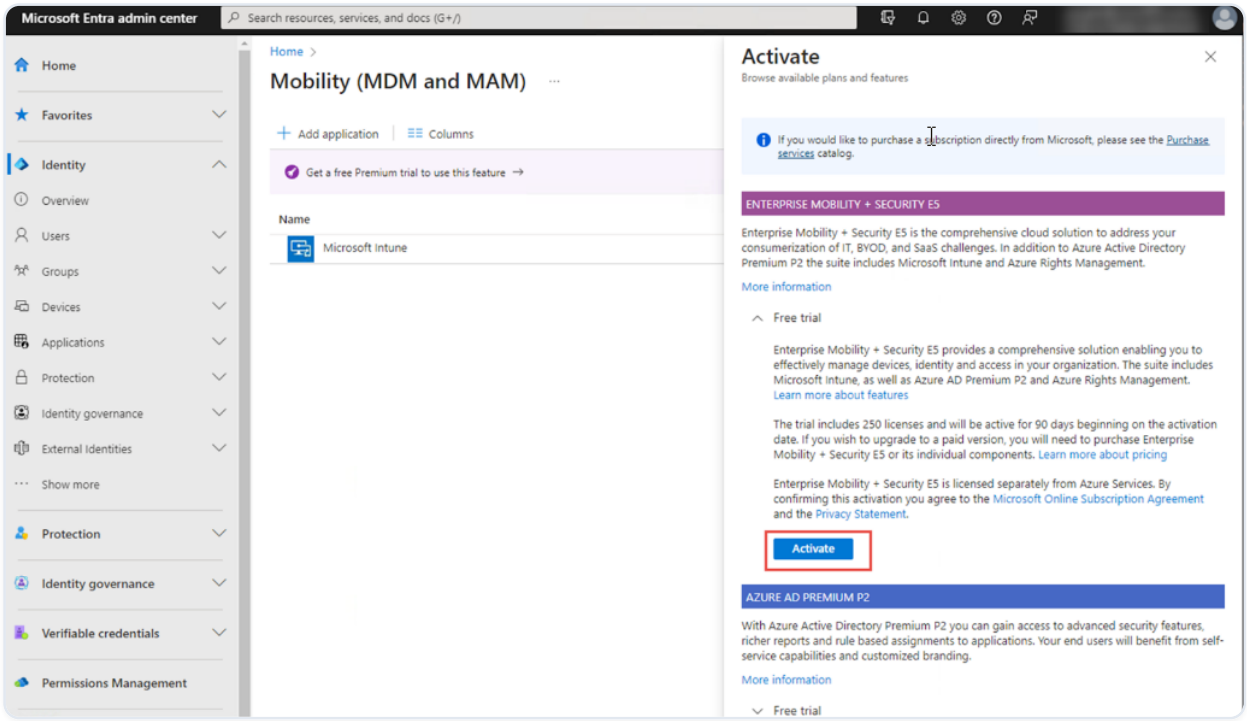
5. 在“**所有服务**”选项卡中，单击“**M365 Microsoft Entra ID**”。



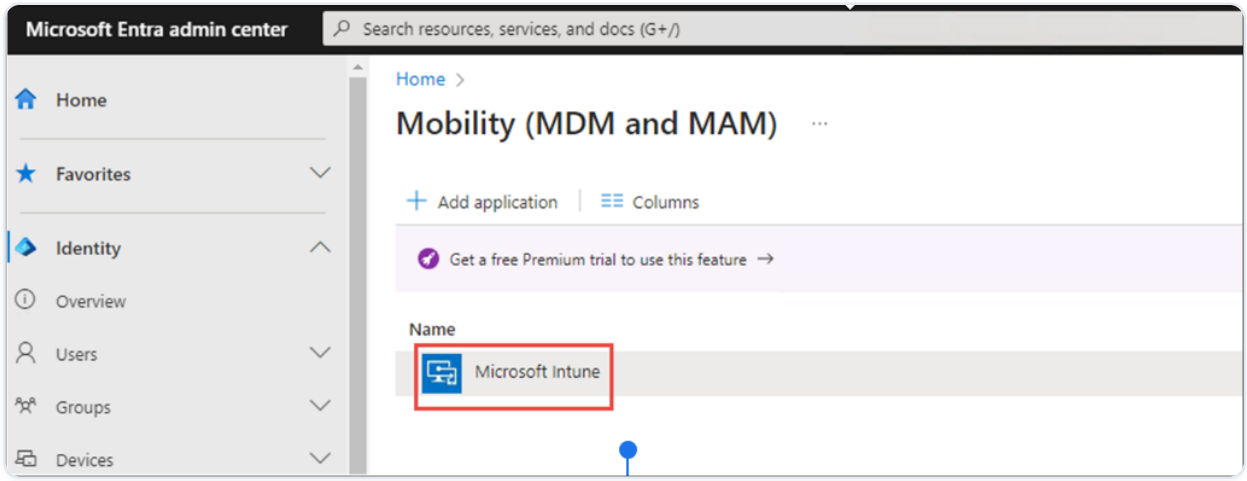
6. 单击“**获取免费高级试用版以使用此功能**”。



7. 单击“**激活**”。



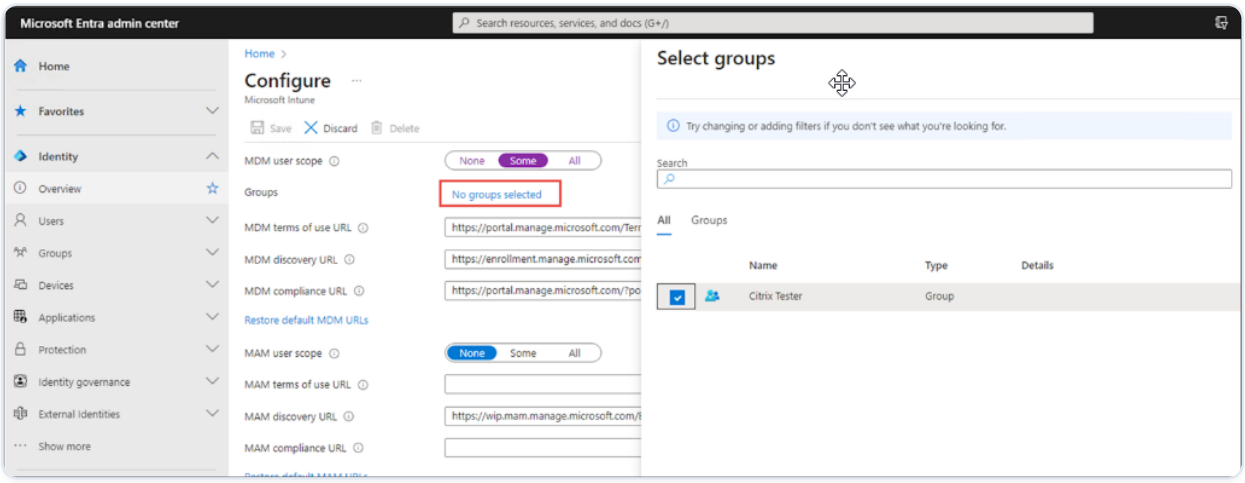
8. 现在，单击“**Microsoft Intune**”。



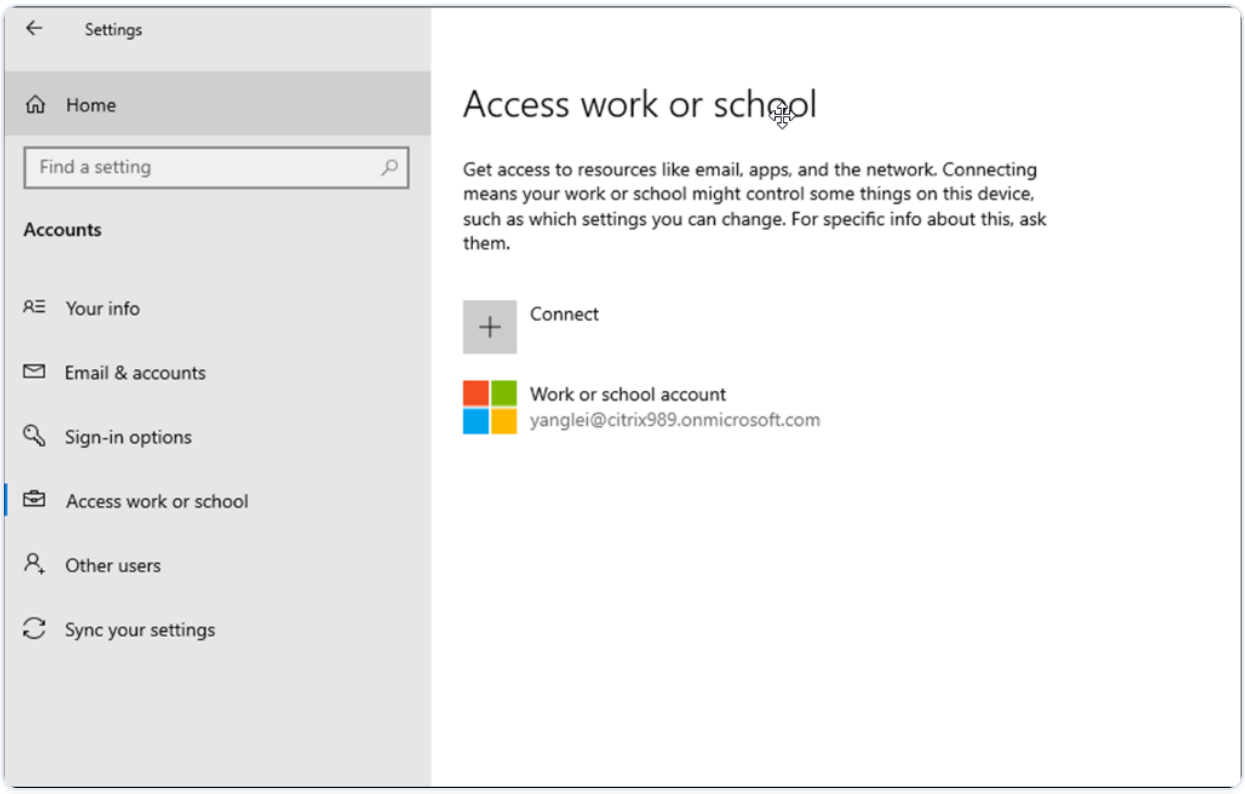
9. 在“**配置**”选项卡中，输入所需的配置。

   配置(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/ms-entra-configuration.png)

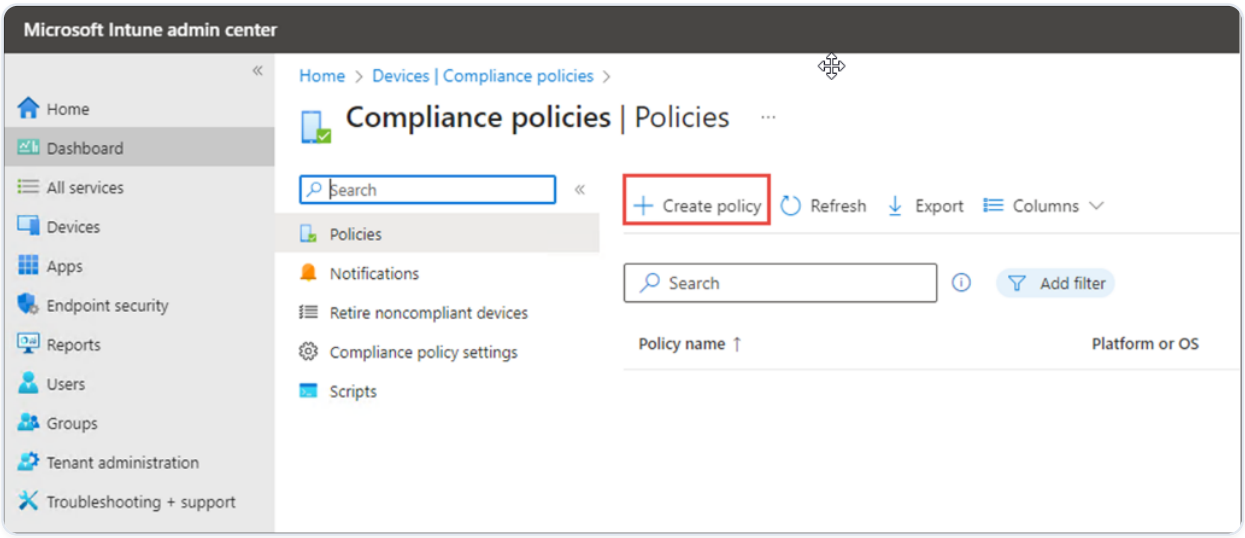
10. 要添加组，请单击“**未选择任何组**”。



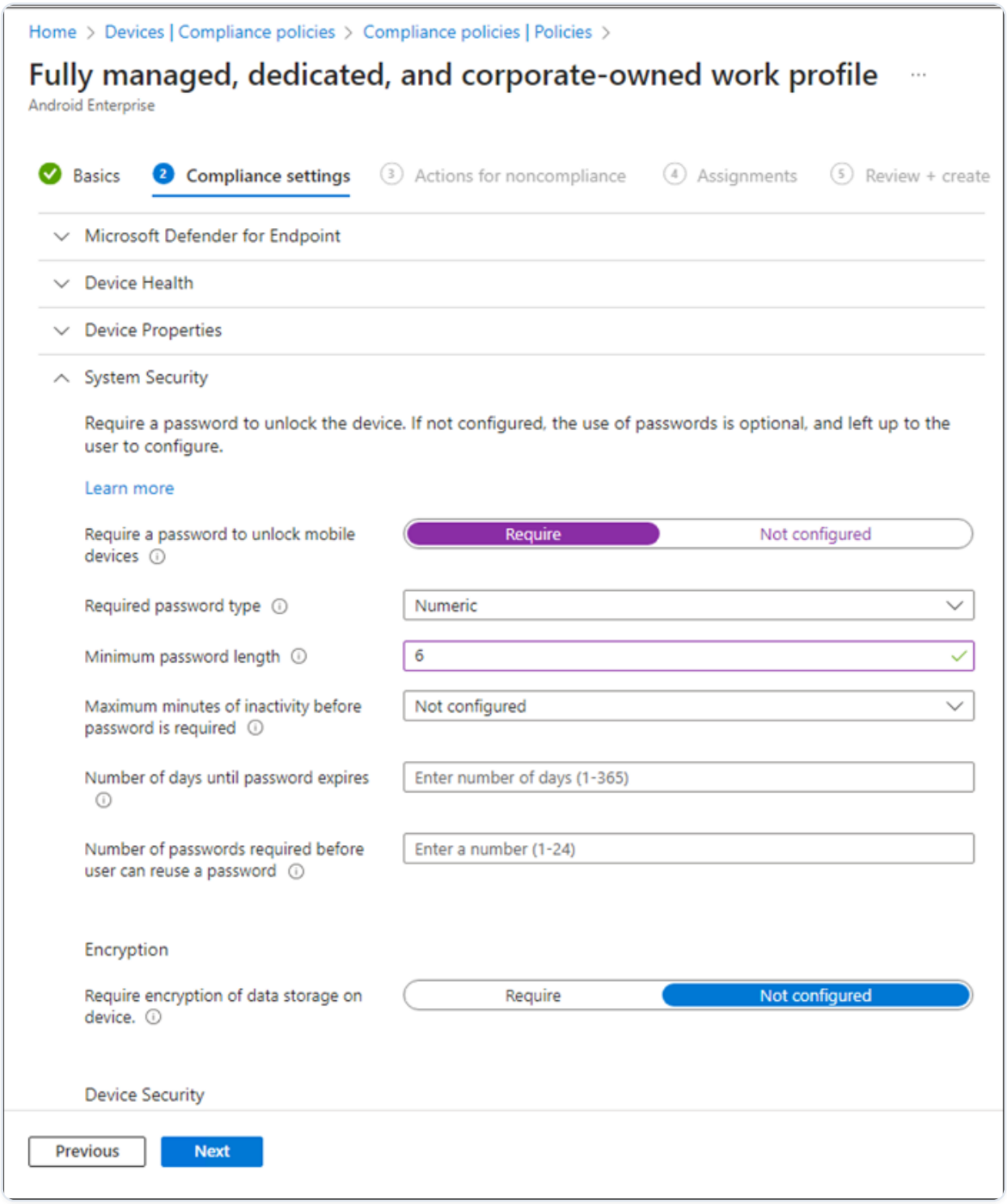
11. 注册您的设备。



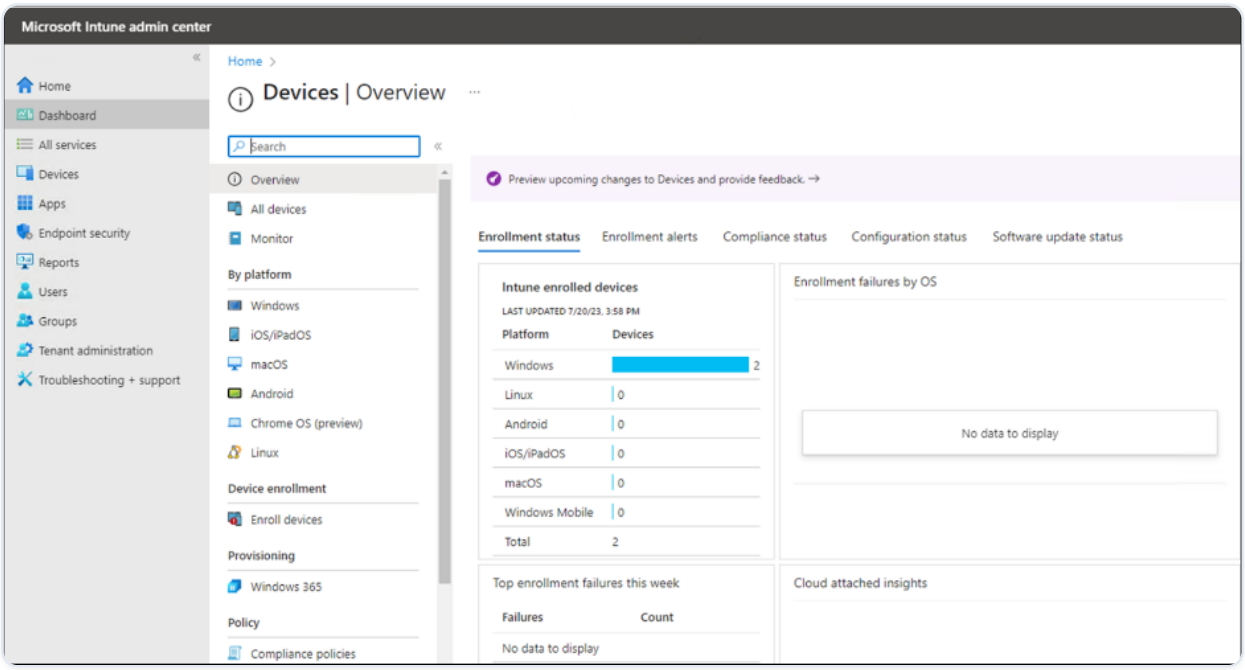
12. 创建设备合规性策略以将新创建的设备的合规性更改为 `Compliant`。



13. 转到“**分配**”选项卡以添加新创建的组。


Home > Devices | Compliance policies > Compliance policies | Policies >
Fully managed, dedicated, and corporate-owned work profile
Android Enterprise
Basics
2 Compliance settings
3 Actions for noncompliance
4 Assignments
5 Review + create
Microsoft Defender for Endpoint
Device Health
Device Properties
System Security
Require a password to unlock the device. If not configured, the use of passwords is optional, and left up to the user to configure.
Learn more
Require a password to unlock mobile devices
Require
Not configured
Required password type
Numeric
Minimum password length
6
Maximum minutes of inactivity before password is required
Not configured
Number of days until password expires
Enter number of days (1-365)
Number of passwords required before user can reuse a password
Enter a number (1-24)
Encryption
Require encryption of data storage on device.
Require
Not configured
Device Security
Previous
Next

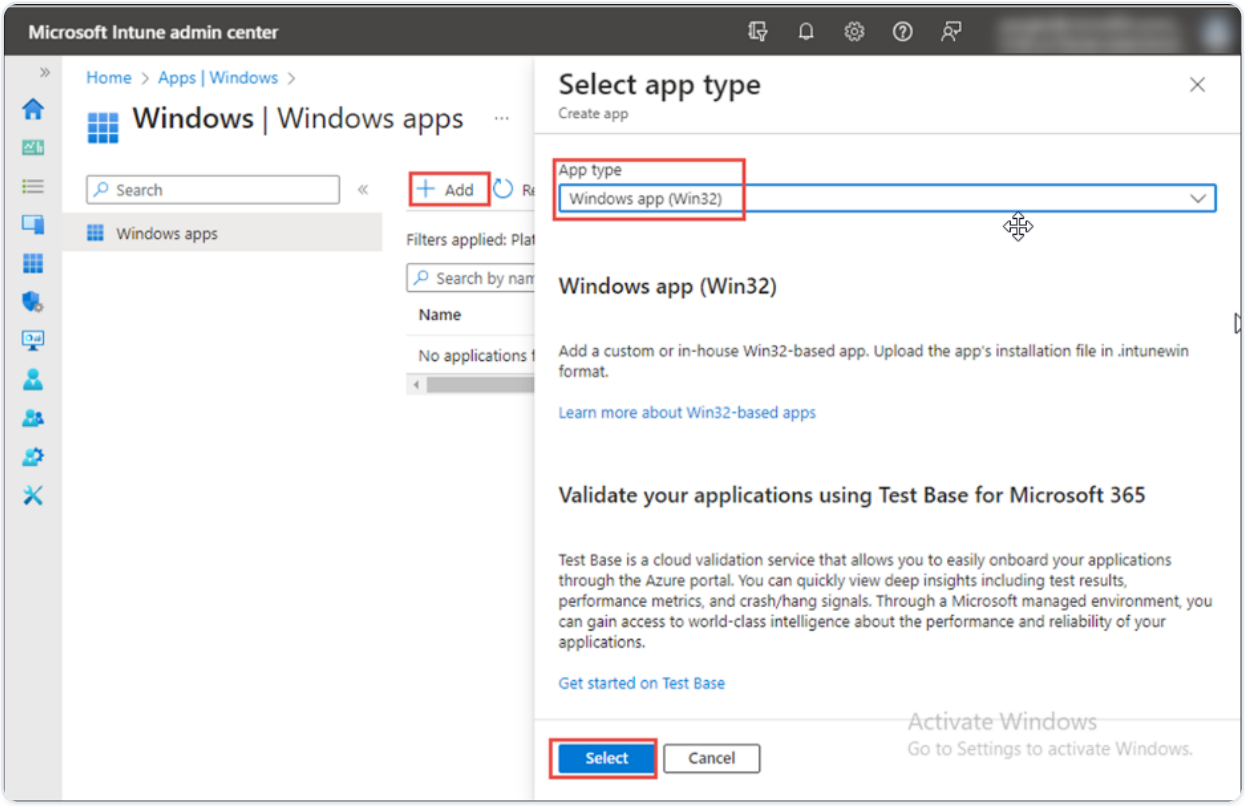
14. 确认设备注册。



有关详细信息，请参阅 Microsoft 365 developer program。

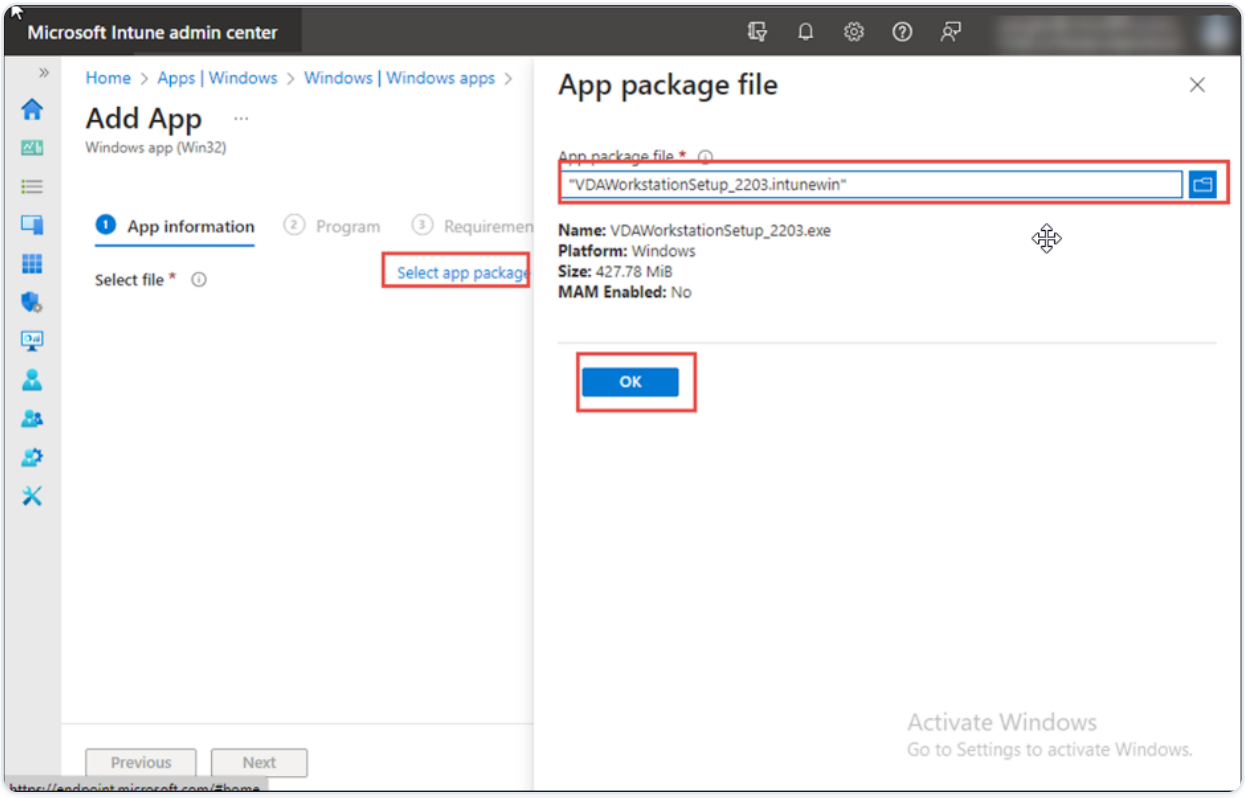
步骤 3：添加和分配应用程序

1. 登录到 Microsoft Intune 管理中心。
2. 选择“**应用 > 所有应用 > 添加**”或转到“**应用 > Windows > Windows 应用**”。



3. 在“**选择应用类型**”窗格中，选择“**其他应用类型 > Windows 应用 (Win32)**”，然后单击“**选择**”。
4. 在“**添加应用**”窗格中，单击“**选择应用包文件**”。单击“**浏览**”。

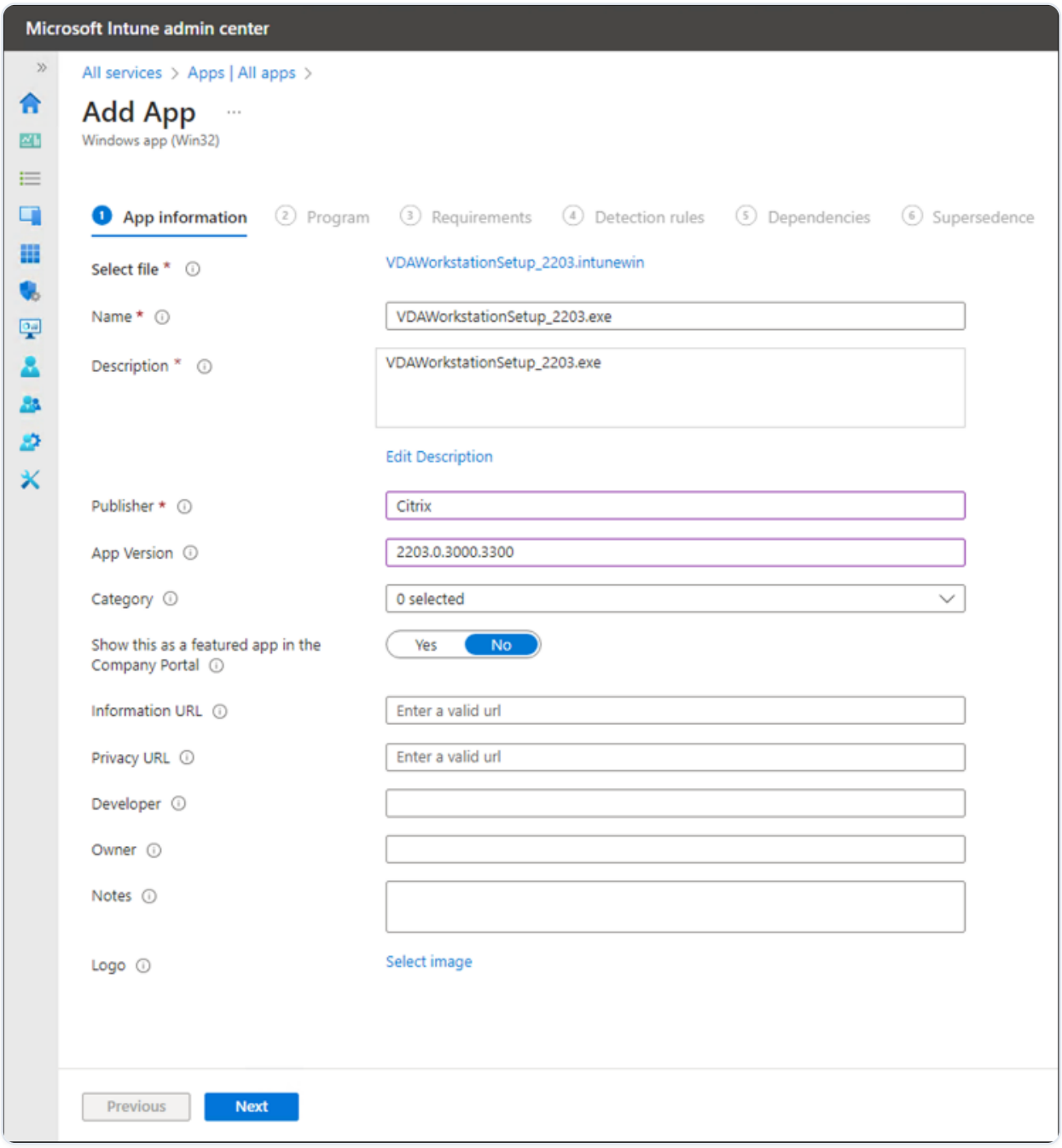
5. 选择扩展名为 `.intunewin` 的准备好的文件。准备好的文件是在 为 Citrix VDA 准备安装 步骤中创建的。将显示一个包含有关该应用程序的详细信息的页面。



注意：

- 如果您使用的是服务器核心计算机，则必须使用 VDA 工作站核心。
- 如果您使用的是 Windows 10 桌面操作系统，则必须使用 VDA 工作站。
- 如果您使用的是服务器操作系统（例如 Windows 2022），则必须使用 VDA 服务器安装程序。
- 在此示例中，我们使用的是 2203 版本，但它适用于所有版本。

6. 在“**应用包文件**”窗格上单击“**确定**”。
7. 在以下屏幕中，在“**应用信息**”选项卡下，输入应用的“**名称**”，并输入 Windows 应用的“**描述**”。将“**发布者**”名称输入为 `Citrix`，您可以在此处指定其他应用信息。单击“**下一步**”。



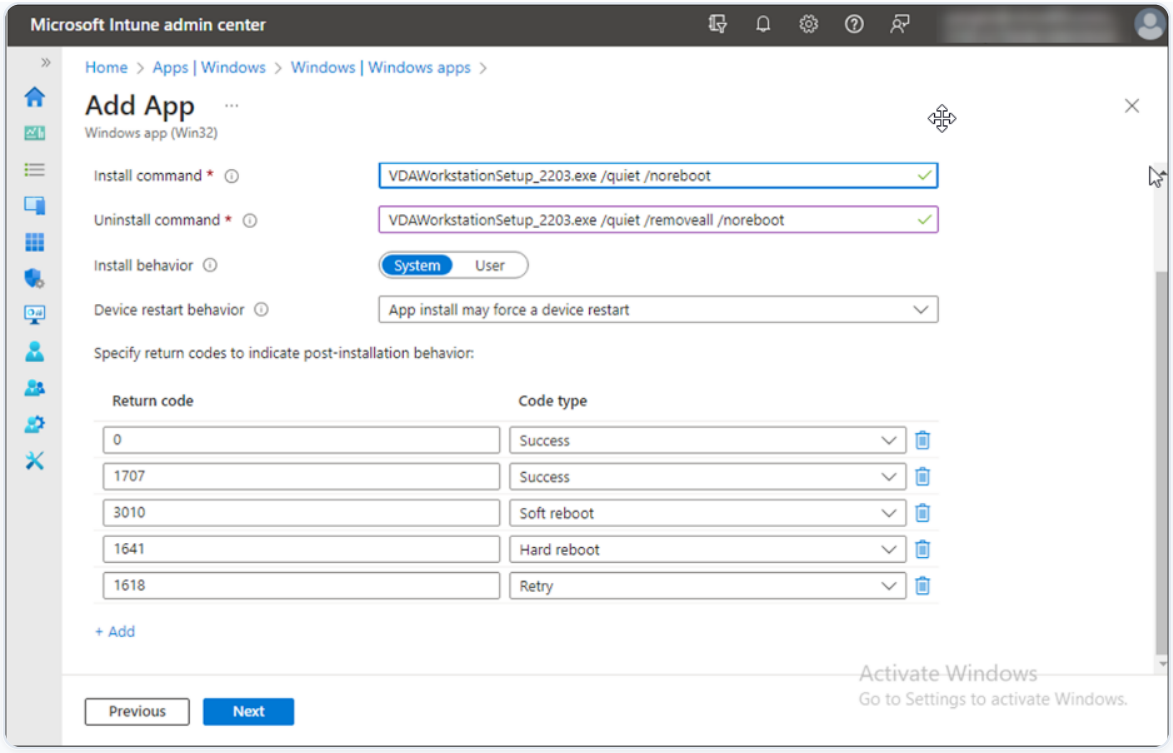
8. 在下一个屏幕上，输入以下值：

   - **安装命令**：`VDAWorkstationSetup_2203.exe /quiet /noreboot`
   - **卸载命令**：`VDAWorkstationSetup_2203.exe /quiet /removeall /noreboot`
   - **安装行为**：
     - **系统**：选择此选项可在组中的所有设备上安装应用。
     - **用户**：选择此选项可在组中仅在特定用户设备上安装应用。

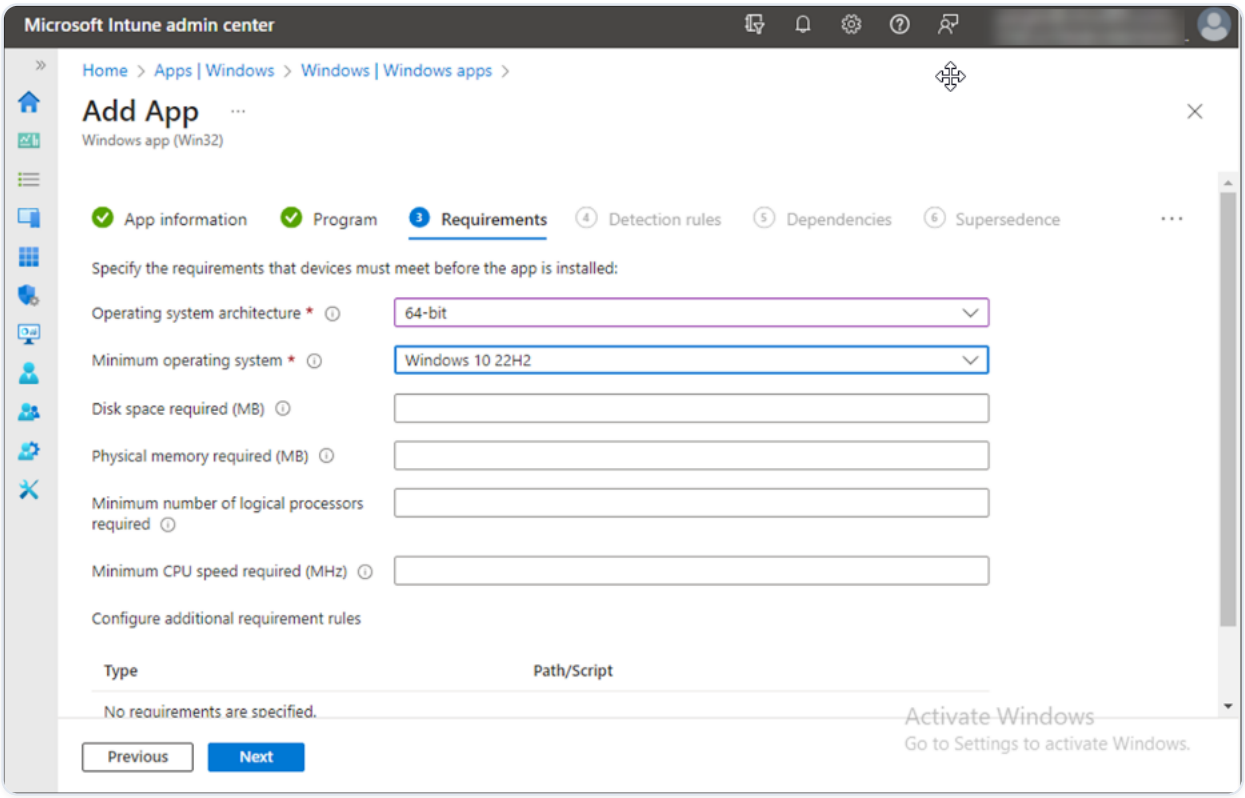
9. 单击“**下一步**”。

注意：

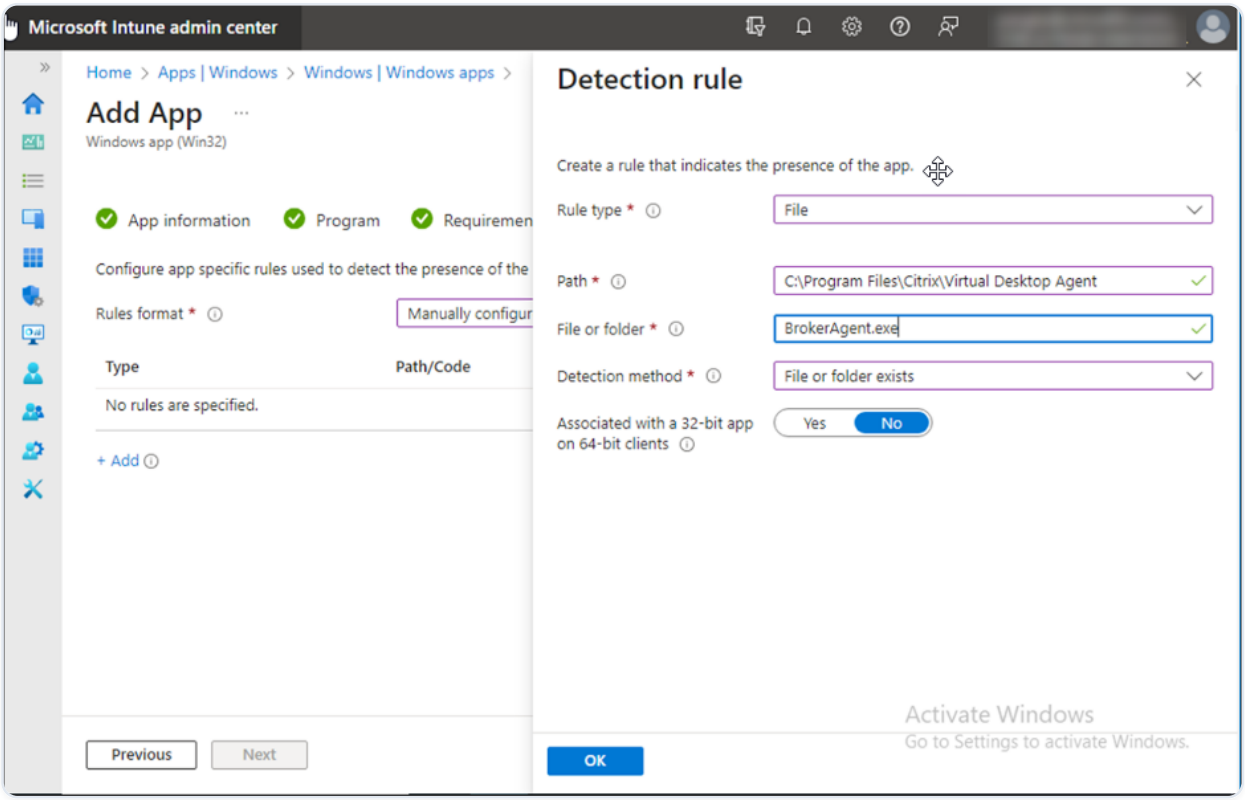
- 此示例使用 2203 版本，但您可以将其与任何版本一起使用。
- 将 `/noreboot` 添加到命令中并不意味着在安装或部署期间不会有任何重新启动，而只是强制执行强制重新启动。 有关脚本的更多信息，请参阅用于安装 VDA 的命令行选项。
- 对于“**设备重新启动行为**”，选择“**Intune 将强制执行强制设备重新启动**”。
- 在“**返回代码**”文本框中，输入 `0`、`3` 和 `8` 以表示安装后成功。 有关其他返回代码的信息，请参阅Citrix 安装返回代码。



10. 在以下屏幕中，在“**要求**”选项卡下，输入所需值。单击“**下一步**”。

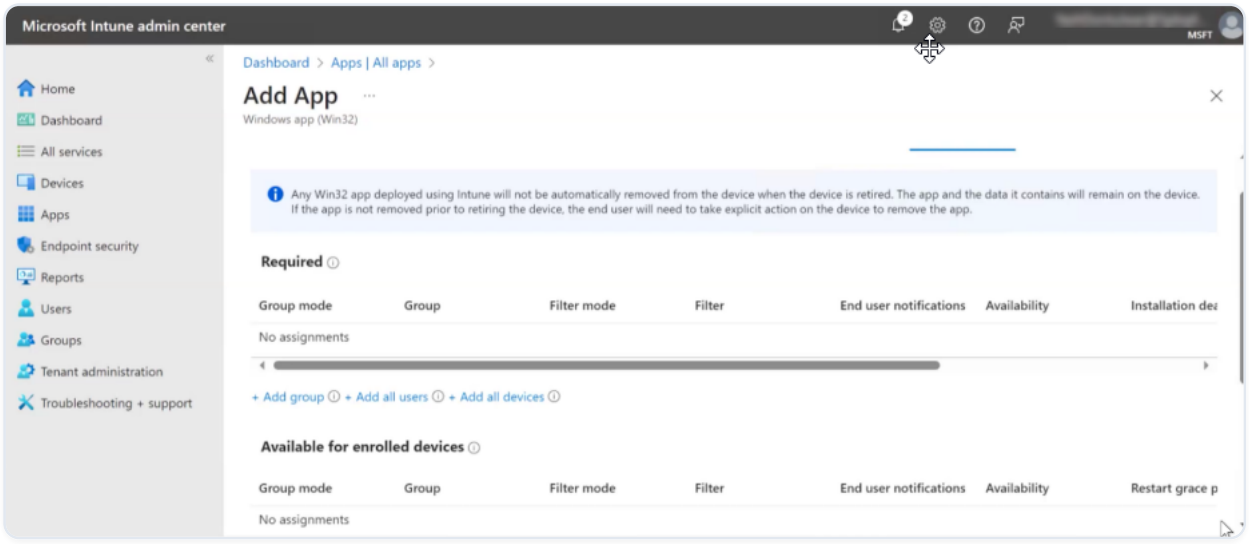


11. 在以下屏幕中，在“**检测规则**”选项卡下，添加“**检测规则**”以添加 Broker 代理。单击“**确定**”。

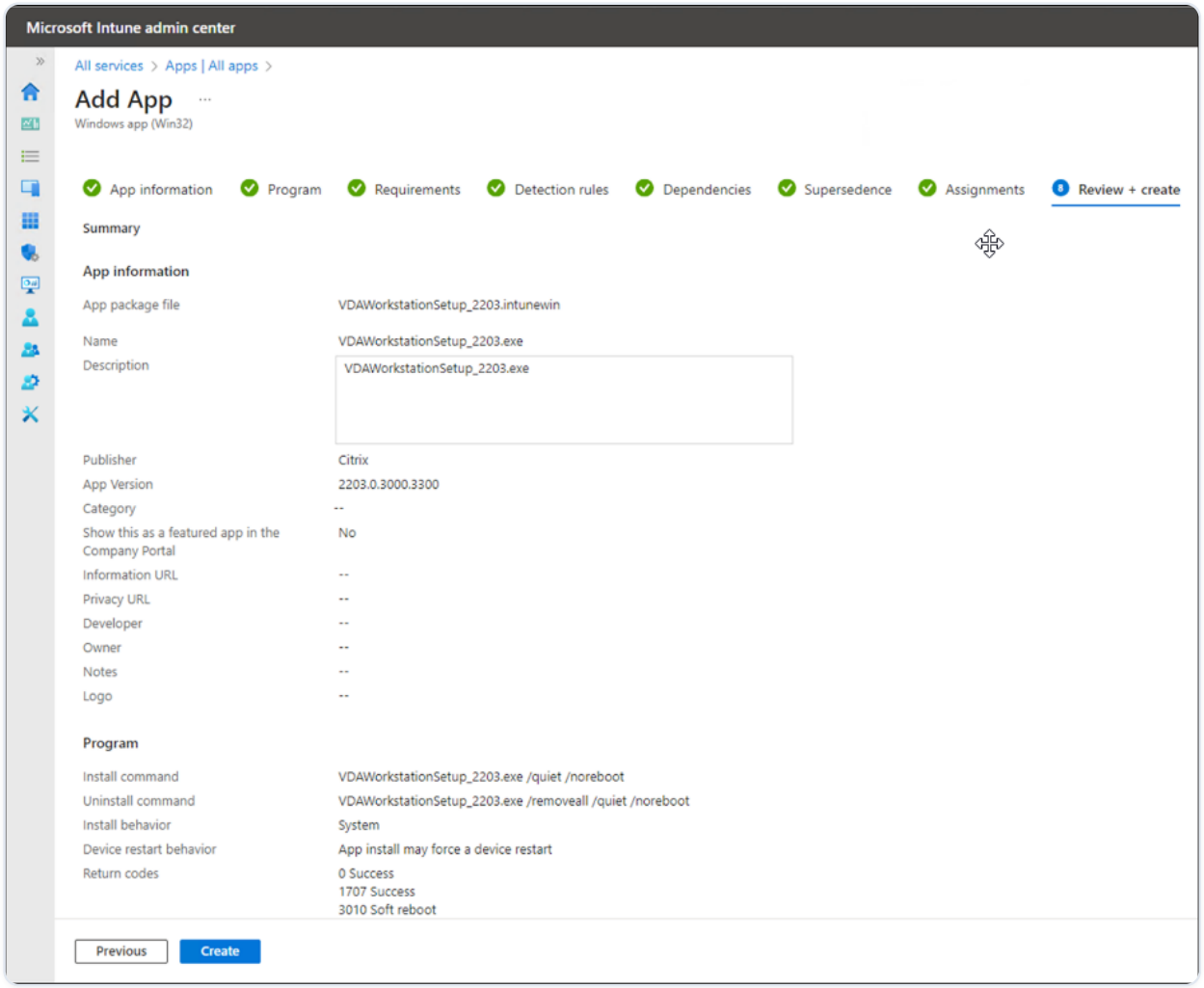


12. 在“**分配**”选项卡中，您可以按以下方式添加设备：

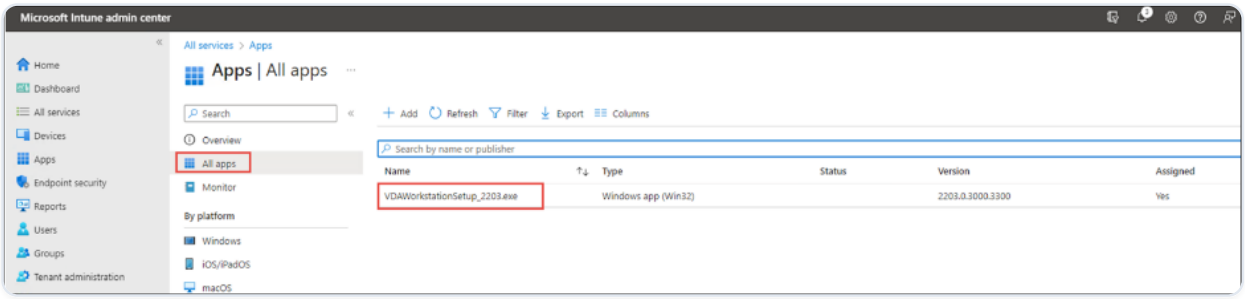
- **必需**：自动更新的设备。
- **适用于已注册的设备**：手动更新的设备。



13. 查看详细信息，然后单击“**创建**”。



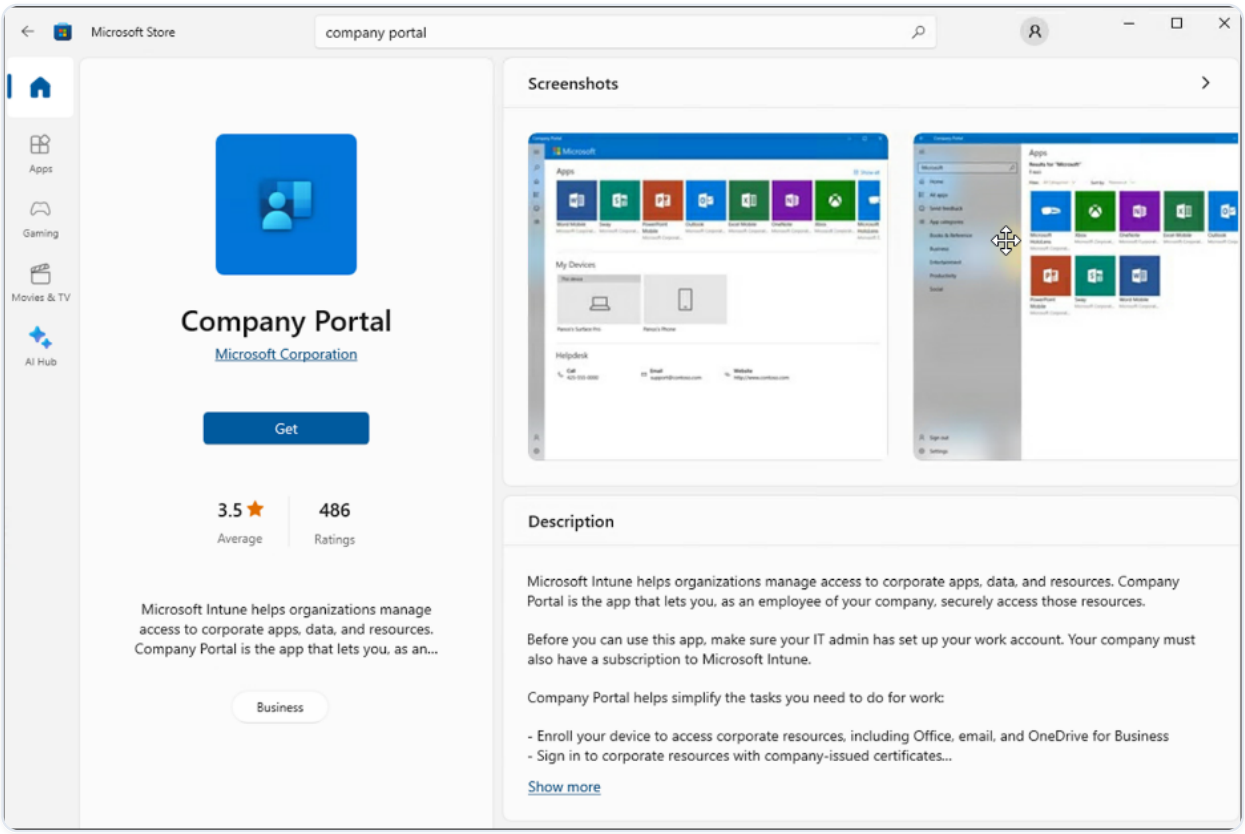
应用已成功分配。



有关详细信息，请参阅添加和分配应用。

步骤 4：在已注册的设备上安装应用程序

1. 登录到已注册的 Windows 10 桌面设备。 设备必须已注册到 Microsoft Intune。此外，您必须使用分配给应用程序的组中包含的帐户登录到设备。有关详细信息，请参阅 Microsoft 文档。
2. 从“**开始**”菜单中，打开“**Microsoft Store**”。
3. 浏览并找到“**公司门户**”应用程序，然后安装它。



4. 运行“**公司门户**”应用程序。
5. 单击您使用 Microsoft Intune 添加的应用程序。 如果您未成功将任何应用程序分配给 Intune 用户，则会显示以下消息： `Your IT administrator did not make any apps available to you.`
6. 单击“**安装**”。

创建站点

注意：

- 在站点创建过程中，添加许可证以启用混合权利许可证后，公共云主机（例如 Microsoft Azure、Google Cloud Platform 和 Amazon Web Services）不会出现在连接类型列表中，直到站点创建完成。
- 在启用许可证激活服务期间或之后，请勿手动更改产品版本或许可模型。

站点是您为 Citrix Virtual Apps and Desktops™ 部署指定的名称。它包括 Delivery Controller 和其他核心组件、Virtual Delivery Agent (VDA)、到主机的连接、计算机目录和交付组。您在安装核心组件之后、创建第一个计算机目录和交付组之前创建站点。

如果您的 Controller 安装在 Server Core 上，请使用 Citrix Virtual Apps and Desktops SDK 中的 PowerShell cmdlet 创建站点。

创建站点时，您将自动加入 Citrix 客户体验改善计划 (CEIP)。CEIP 收集匿名统计信息和使用情况信息，然后将其发送给 Citrix。第一个数据包将在您创建站点后大约七天发送给 Citrix。您可以在站点创建后的任何时间更改您的注册。在 Web Studio 左窗格中选择**设置**，然后找到**Citrix 客户体验改善计划**设置。有关详细信息，请参阅 `<http://more.citrix.com/XD-CEIP>`。

创建站点的用户将成为完全管理员。有关详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/manage-deployment/delegated-administration.html)。

在创建站点之前，请查看本文，以便了解预期情况。

步骤 1. 打开站点创建向导 - Citrix Site Manager

使用工具 Citrix Site Manager 设置您的 Citrix Virtual Apps and Desktops™ 部署（也称为站点）。当您安装 Delivery Controller 时，该工具会自动安装。

要运行此工具，请在 Delivery Controller 上打开桌面“开始”菜单，然后选择 **Citrix > Citrix Site Manager**。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-core/install-web-studio.html#set-up-a-site)。

步骤 2. 站点名称

在**简介**页面上，键入站点的名称。

步骤 3. 数据库

> **注意：**
>
> 从版本 2411 开始，您可以将 Azure SQL 托管实例用于数据库。

> “**数据库**”页面包含用于设置站点、监视和配置日志记录数据库的选项。有关数据库设置选择和要求的详细信息，请参阅数据库。

> **注意：**
>
> 如果 SQL Server Always On 侦听器配置为 TLS 加密，系统可能会提示您输入具有数据库创建权限的凭据。即使输入有效的管理员凭据，创建数据库的尝试仍会失败。请验证 SQL Server 证书是否在主题备用名称 (SAN) 中包含侦听器 DNS 名称。有关详细信息，请参阅 `<https://docs.microsoft.com/zh-cn/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates>` 。

> 如果您选择安装 SQL Server Express 作为站点数据库（默认），则该软件安装后会重新启动。如果您选择不安装 SQL Server Express 软件作为站点数据库，则不会发生此重新启动。

如果您不使用默认的 SQL Server Express，请确保在创建站点之前已在计算机上安装 SQL Server 软件。系统要求列出了支持的版本。

如果您想向站点添加更多 Delivery Controller，并且已在其他服务器上安装了 Controller 软件，则可以从此页面添加这些 Controller。如果您还计划生成用于设置数据库的脚本，请在生成脚本之前添加 Controller。

步骤 4. 许可

在“**许可**”页面上，指定 License Server 地址，然后指明要使用的（安装的）许可证。

> **注意：**

- 确保 License Server 运行的最低版本为 11.17.2 build 53100 或更高版本。未能满足此先决条件将阻止 Citrix Virtual Apps and Desktops 站点升级和站点创建。
- License Activation Service (LAS) 是一种基于云的许可解决方案，可替代传统的 Citrix 旧版许可。有关详细信息，请参阅：
  - Citrix 虚拟应用和桌面文档：License Activation Service
  - 许可文档：许可证激活服务
- 在启用 License Activation Service 期间或之后，请勿手动更改产品版本或许可模型。

- 以 `name:[port]` 形式指定 License Server 地址。*名称*必须是 FQDN、NetBIOS 或 IP 地址。建议使用 FQDN。如果省略端口号，则默认值为 27000。单击“**连接**”。在成功连接到 License Server 之前，您无法继续到下一页。
- 建立连接后，“**使用现有许可证**”默认处于选中状态。显示屏列出了根据当前安装的许可证，此产品可以配置为的兼容产品。
  - 如果 License Server 配置为使用 License Activation Service (LAS)，则 Metainstaller 会显示权利。权利及其相应的许可证到期日期会一并提供。如果您想使用其中一个许可证将此产品配置为所列产品之一，请选择该条目。
  - 如果您已分配并下载了用于此产品的许可证（使用 Citrix 许可证管理工具），但尚未安装该许可证：
    - 单击 **浏览许可证文件**。
    - 在文件资源管理器中，找到并选择您下载的许可证。关联的产品现在显示在站点创建向导的**许可**页面上。选择要使用的条目。
  - 如果未显示所需产品，或者您没有已分配和下载的许可证，您可以分配、下载并安装许可证。为此，许可证服务器必须具有 Internet 访问权限。您必须拥有所需产品的许可证访问代码。Citrix 会通过电子邮件将该代码发送给您。
    - 单击 **分配并下载**。
    - 在**分配许可证**对话框中，输入 Citrix 发送的许可证访问代码。单击 **分配许可证**。
    - 与新许可证关联的产品将显示在站点创建向导的**许可**页面上。选择要使用的条目。
- 或者，选择 **使用免费 30 天试用版**，稍后安装许可证。有关详细信息，请参阅许可文档。

步骤 5. 摘要

“**摘要**”页面列出了您指定的信息。如果要更改任何内容，请使用“**返回**”按钮。完成后，单击“**完成**”。

更多信息

主机连接、网络和存储

如果您正在使用虚拟机管理程序或其他服务上的 VM 来交付应用程序和桌面，您可以选择创建与该主机的第一个连接。您还可以为该连接指定存储和网络资源。创建站点后，您可以修改此连接和资源，并创建更多连接。有关详细信息，请参阅连接和资源。

- 有关**连接**页面上指定的信息，请参阅连接和资源。
  - 如果您不使用虚拟机管理程序或其他服务上的 VM（或者如果您使用 Web Studio 管理专用刀片式 PC 上的桌面），请选择连接类型**无**。
  - 如果您正在配置远程电脑访问站点并计划使用局域网唤醒功能，请选择 **Microsoft System Center Virtual Machine Manager** 或 **远程电脑局域网唤醒** 类型。有关详细信息，请参阅局域网唤醒。

  除了连接类型之外，请指定您将使用 Citrix 工具（例如 Machine Creation Services™）还是其他工具来创建 VM。
- 有关**存储**和**网络**页面上指定的信息，请参阅主机存储、存储管理和存储选择。
- 如果您拥有混合权利许可证并已添加公共云主机连接（例如 AWS），则这些连接将在此处列出。要查看这些公共云主机连接，请在添加它们几分钟后刷新 Web Studio。

远程电脑访问

有关远程电脑访问部署的信息，请参阅远程电脑访问。

如果您使用局域网唤醒功能，请在创建站点之前完成 Microsoft System Center Configuration Manager 上的配置步骤。有关详细信息，请参阅Configuration Manager 和远程电脑访问局域网唤醒。

创建和管理连接与资源

> **重要提示：**
>
> 自 Citrix Virtual Apps and Desktops™ 7 2006 起，如果您的当前部署使用以下任何技术，则只有在删除使用这些技术的生命周期结束 (EOL) 项目后，才能将部署升级到当前版本。
>
> - 个人虚拟磁盘 (PvD)
> - AppDisks™

- 公有云主机类型：Citrix CloudPlatform、Microsoft Azure Classic

有关详细信息，请参阅删除 PVD、AppDisks 和不受支持的主机。

注意：

从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

如果要将公有云主机连接用于部署，则需要混合权利许可证才能完成全新安装或升级到当前版本。

当安装程序检测到一个或多个不受支持的技术或没有混合权利许可证的主机连接时，升级会暂停或停止，并显示一条解释性消息。安装程序日志包含详细信息。有关详细信息，请参阅升级和迁移。

混合权利许可证对主机连接的影响

根据混合权利许可证的授权，主机与公有云主机的连接会受到影响，共有三种情况：

- 要创建与公有云主机的新主机连接，您必须拥有混合权利许可证。
- 如果您拥有混合权利许可证但许可证已过期，则与公有云主机的现有连接将被标记为无权，并进入维护模式。当现有主机连接处于维护模式时，您无法执行以下操作：
  - 添加或修改主机连接
  - 创建目录和更新映像
  - 执行电源操作
- 当未授权的主机连接变为授权时，现有托管连接将重新启用。

简介

您可以在创建站点时选择性地创建与托管资源的第一个连接。之后，您可以更改该连接并创建其他连接。配置连接包括从支持的管理程序中选择连接类型，以及从该连接的资源中选择存储和网络。

只读管理员可以查看连接和资源详细信息。您必须是完全管理员才能执行连接和资源管理任务。有关详细信息，请参阅委派管理。

在何处查找有关连接类型的信息

您可以使用受支持的虚拟化平台在您的 Citrix Virtual Apps 或 Citrix Virtual Desktops 环境中托管和管理计算机。系统要求文章列出了支持的类型。

有关详细信息，请参阅以下信息源：

- **XenServer（以前称为 Citrix Hypervisor™）：**
  - XenServer 虚拟化环境。
  - XenServer® 文档。
- **能腾 Acropolis：**
  - Nutanix 虚拟化环境。
  - Nutanix 文档。
- **威睿：**
  - VMware 虚拟化环境。
  - VMware 产品文档。
- **微软 Hyper-V：**
  - Microsoft System Center 虚拟机管理器虚拟化环境文章。
  - Microsoft 文档。
- **公共云主机连接（AWS、Google Cloud、Microsoft Azure、Nutanix 云和合作伙伴解决方案以及 VMware 云和合作伙伴解决方案）：**有关公共云主机的信息，请参阅设置资源类型。

> **注意：**
>
> 这些信息源将引导您查阅 Citrix DaaS™ 文档。如果您熟悉 Citrix DaaS 产品中的公共云主机，则本地版本存在一些差异。在本地 Virtual Apps and Desktops 中，管理界面称为 Web Studio。更新大约每四周发布到服务中。因此，您可能会发现服务中提供的某些功能在本地版本中不可用。

主机存储

当存储产品由受支持的管理程序管理时，该产品将受到支持。Citrix 支持部门会协助这些存储产品供应商解决问题，并根据需要将这些问题记录在知识中心。

预配计算机时，数据按类型分类：

- 操作系统 (OS) 数据，其中包括主映像。
- 临时数据。此数据包括写入到 MCS 预配的计算机的所有非持久性数据、Windows 页面文件、用户配置文件数据以及与 ShareFile 同步的任何数据。每次计算机重新启动时，此数据都会被丢弃。

为每种数据类型提供单独的存储可以减少每个存储设备的负载并提高其性能，从而充分利用主机的可用资源。它还允许为不同的数据类型使用适当的存储 – 对于某些数据而言，持久性和弹性比其他数据更重要。

存储可以是共享的（集中放置，独立于任何主机，由所有主机使用），也可以是管理程序本地的。例如，中央共享存储可以是一个或多个 Windows Server 2012 群集存储卷（带或不带附加存储），也可以是存储供应商提供的设备。中央存储还可能提供其自身的优化，例如管理程序存储控制路径以及通过合作伙伴插件进行的直接访问。

在本地存储临时数据可避免通过网络访问共享存储。它还可以减少共享存储设备的负载。共享存储可能更昂贵，因此在本地存储数据可以降低成本。必须权衡这些优势与管理程序服务器上可用存储的充足性。

创建连接时，您可以选择两种存储管理方法之一：管理程序共享的存储，或管理程序本地的存储。

当在一个或多个 XenServer 主机上使用本地存储进行临时数据存储时，请确保池中的每个存储位置都具有唯一的名称。（要在 XenCenter® 中更改名称，请右键单击存储并编辑名称属性。）

管理程序共享的存储

管理程序共享的存储方法集中存储需要长期持久性的数据，提供集中备份和管理。该存储保存操作系统磁盘。

选择此方法时，您可以选择是否使用本地存储（在同一管理程序池中的服务器上）来存储临时计算机数据。此方法不需要像共享存储中的数据那样具有持久性或弹性，共享存储中的数据被称为*临时数据缓存*。本地磁盘有助于减少到主操作系统存储的流量。每次计算机重新启动后，此磁盘都会被清除。通过直写式内存缓存访问此磁盘。如果将本地存储用于临时数据，则预配的 VDA 将绑定到特定的管理程序主机。如果该主机发生故障，则 VM 无法启动。

例外：使用群集共享卷 (CSV) 时，Microsoft System Center Virtual Machine Manager 不允许在本地存储上使用临时数据缓存磁盘。

创建连接以在本地存储临时数据，然后为每个 VM 的缓存磁盘大小和内存大小启用并配置非默认值。默认值根据连接类型量身定制，并且在大多数情况下都足够。有关详细信息，请参阅创建计算机目录。

管理程序还可以通过在本地读取缓存磁盘映像来提供优化技术。例如，XenServer 提供 IntelliCache™，这可以减少到中央存储的网络流量。

管理程序本地存储

管理程序本地存储方法在管理程序上本地存储数据。使用此方法，主映像和其他操作系统数据会传输到站点中的管理程序。此过程用于初始计算机创建和将来的映像更新。此过程会导致管理网络上出现大量流量。映像传输也耗时，并且映像在不同时间对每个主机可用。

创建连接和资源

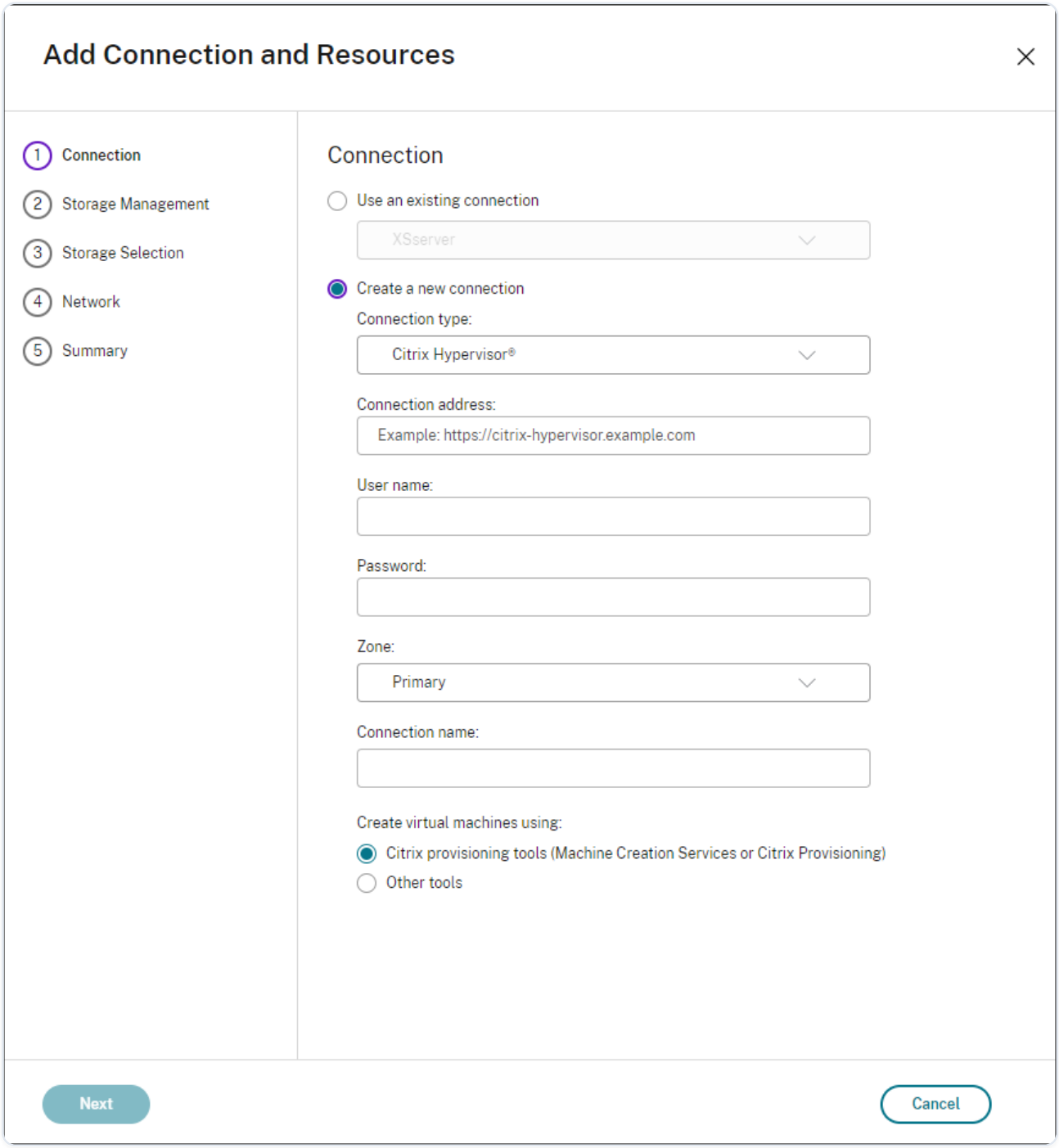
您可以在创建站点时选择创建第一个连接。站点创建向导包含如下面各节所述的连接相关页面。

如果您在创建站点后创建连接，请从步骤 1 开始。

> **重要提示：**
>
> 主机资源（存储和网络）必须在创建连接之前可用。

1. 登录 Web Studio。
2. 在左侧窗格中选择**托管**。
3. 在操作栏中选择 **添加连接和资源**。
4. 向导将引导您完成以下页面（具体页面内容取决于所选的连接类型）。完成每个页面后，单击 **下一步**，直到到达 **摘要** 页面。

连接



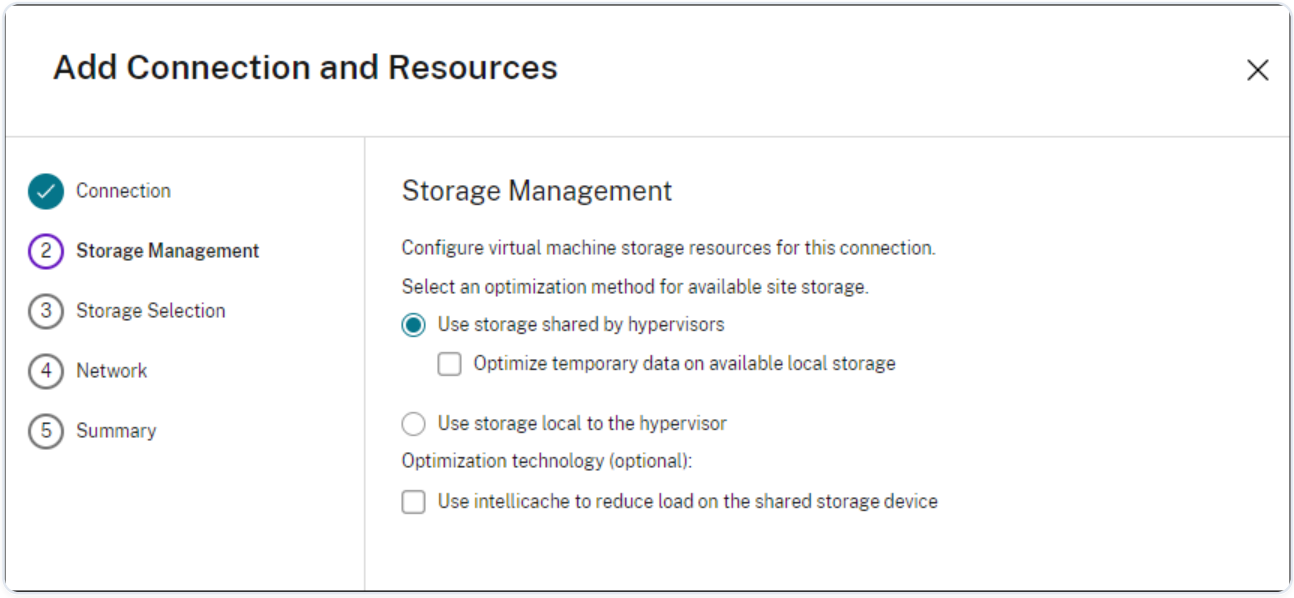
在 **Connection** 页面上：

- 要创建连接，请选择 **创建新连接**。要基于与现有连接相同的主机配置创建连接，请选择 **使用现有连接**，然后选择相关连接。
- 在 **连接类型** 字段中选择您正在使用的管理程序。仅当您使用混合权利许可证时，公共云主机连接才会显示在下拉列表中。或者，您可以使用 PowerShell 命令 `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/true 来获取以下信息：
  - 所有 Citrix 支持的管理程序插件列表，包括第三方插件。

  - 管理程序插件的可用性。如果可用性状态为 **false**，可能的原因是管理程序插件未正确安装，或者您没有混合权利许可证。

- 连接地址和凭据字段有所不同，具体取决于所选的连接类型。输入请求的信息。
- 输入连接名称。此名称显示在 Web Studio 中。
- 选择用于创建虚拟机的工具：Web Studio 工具（例如 Machine Creation Services™ 或 Citrix Provisioning）或其他工具。

存储管理



有关存储管理类型和方法的信息，请参阅 主机存储。

如果正在配置与 Hyper-V 或 VMware 主机的连接，请浏览并选择群集名称。其他连接类型不要求提供群集名称。

选择存储管理方法：虚拟机管理程序共享存储或虚拟机管理程序本地存储。

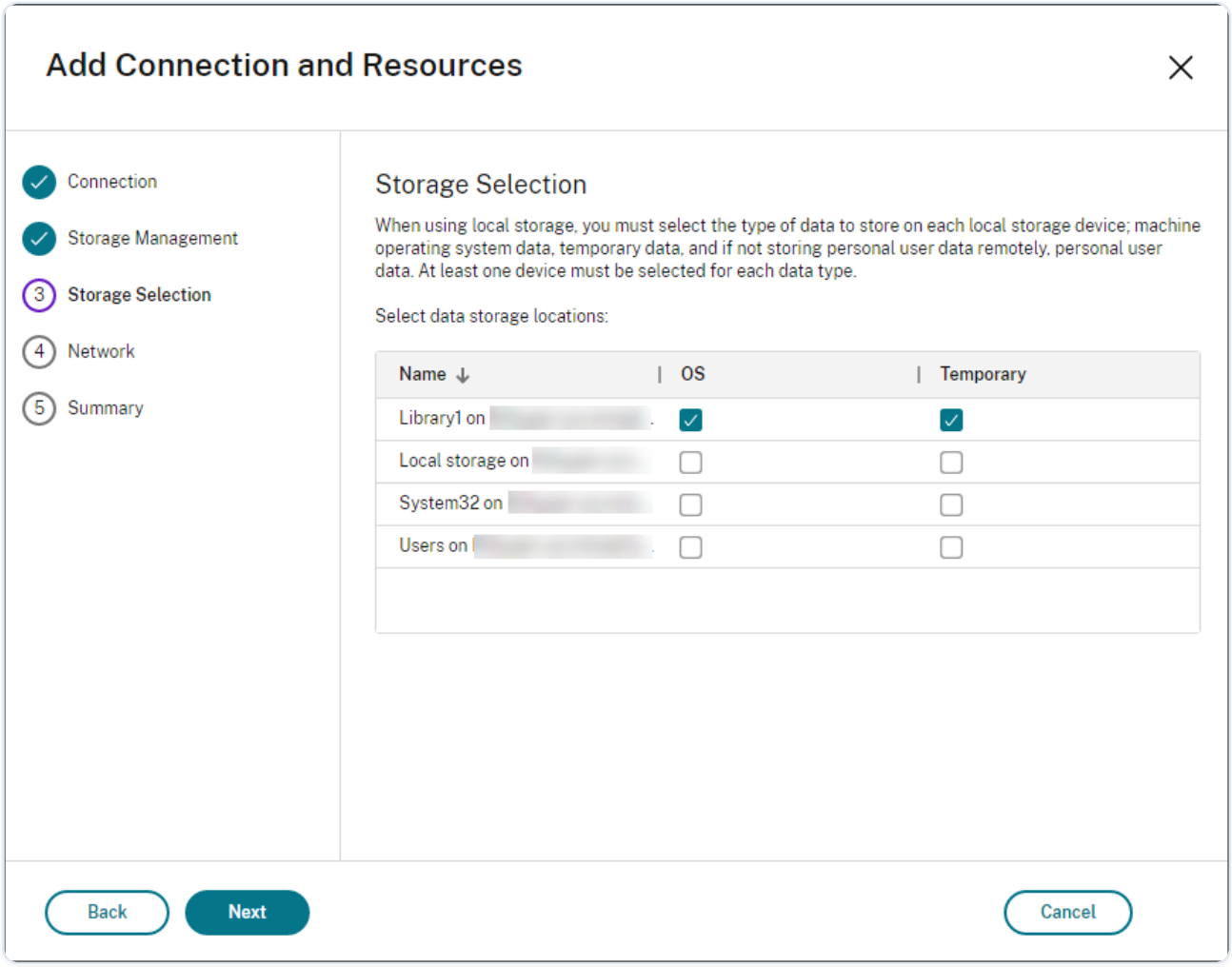
- 如果选择由虚拟机管理程序共享的存储，请指示是否要将临时数据保留在可用的本地存储上。（您可以在使用此连接的计算机目录中指定非默认的临时存储大小。）**例外：**使用群集共享卷 (CSV) 时，Microsoft System Center Virtual Machine Manager 不允许在本地存储上使用临时数据缓存磁盘。在 Web Studio 中配置该存储管理设置将失败。

如果在 XenServer 池中使用共享存储，请指示是否要使用 IntelliCache 来减少共享存储设备上的负载。请参阅将 IntelliCache 用于 XenServer 连接。

> **注意：**

在 XenServer、VMware 和 SCVMM 虚拟化环境中，您可以将回写缓存 (WBC) 磁盘与操作系统磁盘放在同一存储位置。为此，请勿选择**优化可用本地存储上的临时数据**。

存储选择



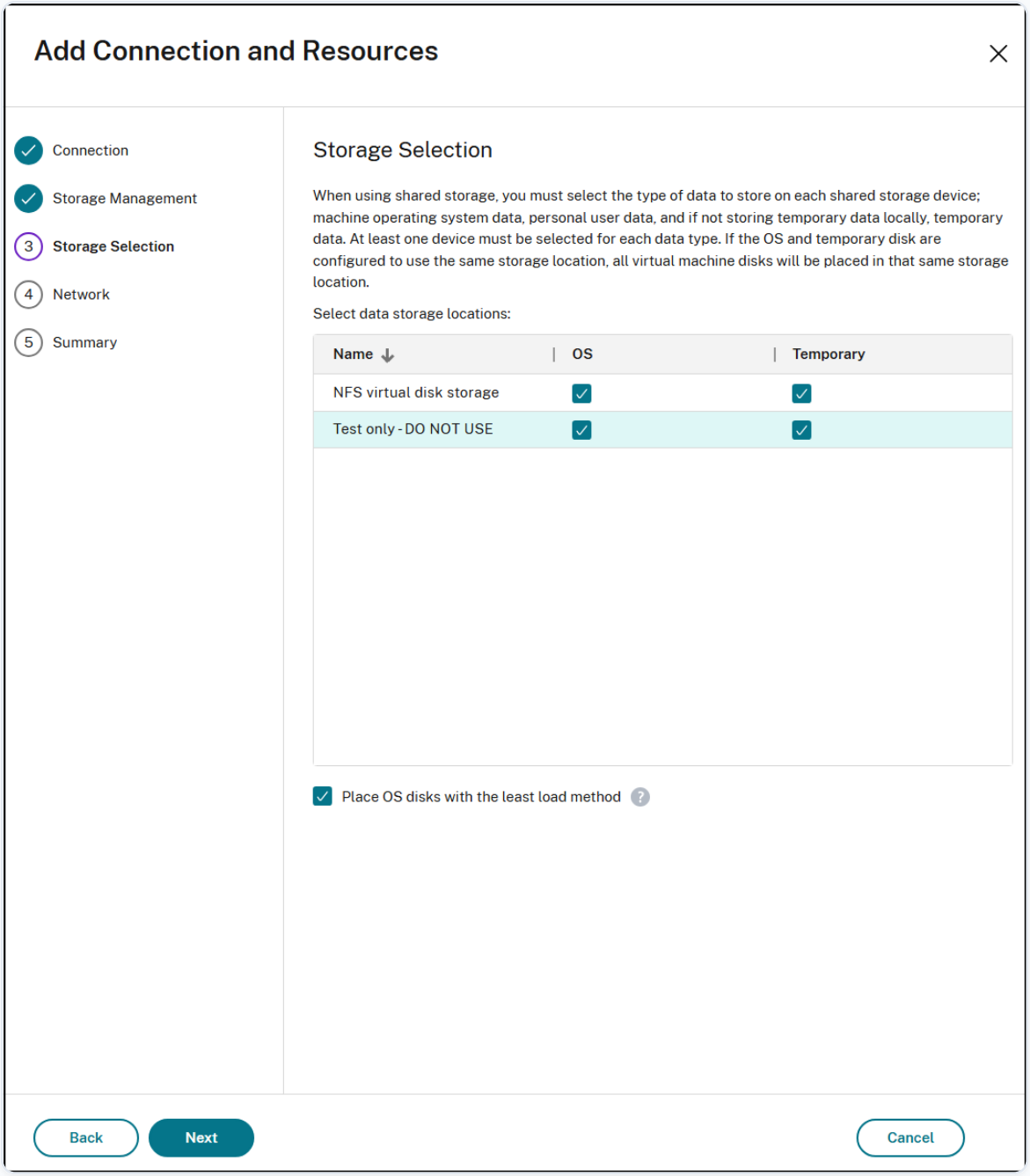
有关存储选择的详细信息，请参阅 主机存储。

为每种可用数据类型选择至少一个主机存储设备。您在上一页上选择的存储管理方法会影响此页面上可供选择的数据类型。在向导中继续到下一页之前，请为每种支持的数据类型选择至少一个存储设备。

注意：

- 在 XenServer、VMware 和 SCVMM 虚拟化环境中，如果您将可用 OS 存储列表配置为与可用临时存储列表相同，则 MCS 会将回写缓存 (WBC) 磁盘放置在与 OS 磁盘相同的存储位置。

- 如果选择至少两个或更多操作系统数据存储位置，将显示**使用最少负载方法优化存储负载平衡**选项。此选项允许您选择负载最低的存储库进行磁盘分配。



- **摘要**页面会根据您的选择指示该选项是**已启用**还是**已禁用**。**详细信息**面板显示存储分配方法的更改。您可以使用**操作系统存储**页面上的**编辑存储**选项进行调整。或者，您可以使用 PowerShell 实现相同的目标。请参阅适用于 VM 的灵活存储位置选项。

如果您在“**存储管理**”页面上选择“**使用管理程序共享的存储**”并选择“**优化可用本地存储上的临时数据**”，则可以在“**存储选择**”页面上获得更多配置选项。例如，您可以选择要用于临时数据的本地存储设备（在同一管理程序池中）。

显示当前选定的存储设备数量（在前面的图中，“已选择 1 个存储设备”）。将鼠标悬停在该条目上时，将显示选定的设备名称。

1. 单击**选择**以更改要使用的存储设备。
2. 在**选择存储**对话框中，选中或清除存储设备复选框，然后单击**确定**。

网络

在“**网络**”页面上，输入资源的名称。此名称将显示在 Web Studio 中，用于标识与连接关联的存储和网络组合。

选择虚拟机使用的一个或多个网络。

摘要

在“**摘要**”页面上，查看您的选择。完成后，单击“**完成**”。

请记住：在本地存储临时数据允许您在创建包含使用此连接的计算机的计算机目录时，为临时数据存储配置非默认值。请参阅创建计算机目录。

编辑连接设置

请勿使用此过程重命名连接或创建连接。这些连接是不同的操作。仅当当前主机具有新地址时才更改地址。输入不同计算机的地址会中断连接的计算机目录。

您无法更改连接的 **GPU** 设置，因为访问此资源的计算机目录必须使用适当的 GPU 专用主映像。请创建连接。

1. 登录 Web Studio。
2. 在左侧窗格中选择**托管**。
3. 选择连接，然后在操作栏中选择**编辑连接**。
4. 按照编辑连接时可用设置的指导进行操作。
5. 完成后，单击“**应用**”以应用所做的任何更改并保持窗口打开，或者单击“**保存**”以应用更改并关闭窗口。

连接属性”页面：

- 要更改连接地址和凭据，请选择“**编辑设置...**”，然后输入新信息。
- 要为 XenServer 连接指定高可用性服务器，请选择 **编辑服务器...** 并选择服务器。Citrix 建议您选择池中的所有服务器，以便在池主服务器出现故障时允许与 XenServer 通信。

> **注意：**

> 如果您正在使用 HTTPS 并希望配置高可用性服务器，请勿为池中的所有服务器安装通配符证书。每个服务器都需要一个单独的证书。

高级”页面：

- 对于 Microsoft System Center Configuration Manager (ConfMgr) 局域网唤醒连接类型（与远程电脑访问结合使用），请输入 **ConfMgr 唤醒代理**、幻数据包和数据包传输信息。
- 限制阈值设置使您能够指定连接上允许的最大电源操作数。当电源管理设置允许同时启动过多或过少的计算机时，这些设置会有所帮助。每种连接类型都有特定的默认值，这些默认值适用于大多数情况，并且不得更改。
- “**同时操作（所有类型）**”设置指定两个值：此连接上可同时发生的最大绝对数量，以及使用此连接的所有计算机的最大百分比。您必须同时指定绝对值和百分比值。实际应用的限制是这两个值中较低的一个。

  例如，在包含 34 台计算机的部署中，如果“**同时操作（所有类型）**”设置为绝对值 10 和百分比值 10，则实际应用的限制为 3（即 34 的 10% 四舍五入到最接近的整数，小于 10 台计算机的绝对值）。
- “**每分钟最大新操作数**”是一个绝对数字。没有百分比值。
- 仅在 Citrix 支持代表的指导或明确的文档说明下，才可在**连接选项**字段中输入信息。

共享租户页面：

添加与此连接的订阅共享 Azure 计算库的租户和订阅。因此，在创建或更新目录时，您可以从这些租户和订阅中选择共享映像。

- 输入与此连接关联的应用程序的**应用程序 ID** 和**应用程序密钥**。利用此信息，您可以向 Azure 进行身份验证。我们建议您定期更改密钥以确保安全。
- 指定共享租户和订阅。您最多可以添加八个共享租户。对于每个租户，您最多可以添加八个订阅。
- 完成后，单击**保存**和**应用**。

仅在 Citrix 支持代表的指导下，才可在**连接选项**字段中输入信息。

编辑网络

您可以更改连接的网络。请执行以下操作：

1. 转至**托管**。

2. 在连接下选择目标资源，然后在操作栏中选择**编辑网络**。
3. 为虚拟机选择一个或多个要使用的网络。
4. 单击**保存**以保存更改并退出。

开启或关闭连接的维护模式

为连接开启维护模式可防止任何新的电源操作影响连接上存储的任何计算机。当计算机处于维护模式时，用户无法连接到该计算机。如果用户已连接，则维护模式将在他们注销时生效。

1. 登录到 Web Studio。
2. 在左侧窗格中选择**托管**。
3. 选择连接。要开启维护模式，请在操作栏中选择 **Turn On Maintenance Mode**（开启维护模式）。要关闭维护模式，请选择 **Turn Off Maintenance Mode**（关闭维护模式）。

您还可以为单个计算机启用或禁用维护模式。此外，您还可以为计算机目录或交付组中的计算机启用或禁用维护模式。

删除连接

删除连接可能会导致大量计算机被删除和数据丢失。请确保受影响计算机上的用户数据已备份或不再需要。

删除连接之前，请确保：

- 所有用户均已从连接上存储的计算机注销。
- 没有正在运行的已断开连接的用户会话。
- 已为共用和专用计算机开启维护模式。
- 连接使用的计算机目录中的所有计算机都已关闭电源。

当您删除某个目录引用的连接时，该计算机目录将变得不可用。如果此连接被某个目录引用，您可以选择删除该目录。在删除目录之前，请确保它未被其他连接使用。

1. 登录到 Web Studio。
2. 在左侧窗格中选择**托管**。
3. 选择连接，然后在操作栏中选择 **删除连接**。
4. 如果此连接上存储有计算机，系统会询问您是否必须删除这些计算机。如果要删除它们，请指定如何处理关联的 Active Directory 计算机帐户。

重命名或测试连接

1. 登录到 Web Studio。
2. 在左侧窗格中选择**托管**。
3. 选择连接，然后在操作栏中选择 **重命名连接** 或 **测试连接**。

测试 TLS 证书信任

如果由于不受信任的证书导致主机连接中断，您可以在 Web Studio 中重新信任该证书。要重新信任：

1. 在左侧窗格中选择**托管**。
2. 右键单击要重新信任证书的连接，然后选择 **测试 TLS 证书信任**。
3. 在后续窗口中输入密码，然后单击 **保存**。
    - 如果必须重新信任证书，将弹出一个警告对话框，其中包含信任证书的选项。
    - 如果证书已受信任，将弹出一个成功对话框，显示证书已受信任。

查看连接上的计算机详细信息

1. 登录到 Web Studio。
2. 在左侧窗格中选择**托管**。
3. 选择连接，然后在操作栏中选择**查看计算机**。

上方窗格列出了通过连接访问的计算机。选择一台计算机可在下方窗格中查看其详细信息。还提供了开放会话的会话详细信息。

使用搜索功能快速查找计算机。您可以从窗口顶部的列表中选择一个已保存的搜索，也可以创建一个搜索。您可以通过键入计算机名称的全部或部分进行搜索，也可以构建一个表达式用于高级搜索。要构建表达式，请单击 **展开**，然后从属性和运算符列表中进行选择。

管理连接上的计算机

1. 登录到 Web Studio。
2. 在左侧窗格中选择**托管**。
3. 选择一个连接，然后在 **操作** 窗格中选择 **查看计算机**。
4. 在操作栏中选择以下选项之一。某些操作可能不可用，具体取决于计算机状态和连接主机类型。

操作	描述
启动	如果计算机已关机或挂起，则启动计算机。
挂起	暂停计算机而不将其关闭，并刷新计算机列表。
关机	请求操作系统关机。
强制关机	强制关闭计算机电源，并刷新计算机列表。
重新启动	请求操作系统关机，然后再次启动计算机。如果操作系统无法执行此操作，则桌面将保持其当前状态。
启用维护模式	暂时停止与计算机的连接。用户无法连接到处于此状态的计算机。如果用户已连接，则维护模式将在他们注销时生效。（您还可以为通过连接访问的所有计算机启用或禁用维护模式，如上所述。）
从交付组中删除	从交付组中删除计算机不会将其从交付组使用的计算机目录中删除。只有在没有用户连接到计算机时，才能删除计算机。启用维护模式可暂时阻止用户在您删除计算机时进行连接。
删除	删除计算机后，用户将无法再访问该计算机，并且该计算机将从计算机目录中删除。在删除计算机之前，请确保所有用户数据都已备份或不再需要。只有在没有用户连接到计算机时，才能删除计算机。启用维护模式可暂时阻止用户在您删除计算机时进行连接。

对于涉及计算机关机的操作，如果计算机在 10 分钟内未关机，则会将其断电。如果 Windows 在关机期间尝试安装更新，则存在在更新完成之前计算机断电的风险。

编辑存储

您可以显示用于存储使用连接的 VM 的操作系统和临时数据的服务器状态。您还可以指定要用于存储每种数据类型的服务器。

1. 登录 Web Studio。
2. 在左侧窗格中选择**托管**。

3. 选择连接，然后在操作栏中选择“**编辑存储**”。
4. 在左侧窗格中，选择数据类型：操作系统或临时。
5. 选中或清除所选数据类型的一个或多个存储设备的复选框。
6. 单击 **确定**。

列表中的每个存储设备都包含其名称和存储状态。有效的存储状态值为：

- **正在使用：** 存储正在用于创建计算机。
- **已取代：** 存储仅用于现有计算机。此存储中不添加新计算机。
- **未使用：** 存储未用于创建计算机。

如果您清除当前**正在使用**的设备的复选框，其状态将更改为**已取代**。现有计算机将继续使用该存储设备（并且可以向其写入数据），因此即使该位置停止用于创建计算机，它也可能变满。

删除、重命名或测试资源

1. 登录 Web Studio。
2. 在左侧窗格中选择**托管**。
3. 选择资源，然后在操作栏中选择相应的条目：**删除资源**、**重命名资源**或**测试资源**。

VM 的灵活存储位置选项

计算机目录中的 VM 分配有各种存储服务 (SR)。为了平衡不同存储中的 VM 分配，您有两种选择：

- **增强型当前轮询分配方法**：MCS 不再总是从相同的固定 SR 开始分配，而是从上次使用的 SR 之后的 SR 开始分配。
- **基于最低负载的分配方法**：根据同一计算机目录中每个 SR 上的虚拟机总数进行比较，将虚拟机放置在当前负载最低的 SR 上。例如，如果一个计算机目录包含 100 个虚拟机，分布如下：SR1 上有 20 个虚拟机，SR2 上有 30 个虚拟机，SR3 上有 50 个虚拟机，则新虚拟机将首先分配给 SR1。此方法可确保 SR1、SR2 和 SR3 之间的负载均衡。

此功能具有以下特点：

- 适用于所有本地管理程序（VMware、XenServer 和 Hyper-V）
- 仅适用于操作系统磁盘存储。
- 不适用于现有虚拟机

要实施基于负载的分配选项，请在创建或更新主机连接时添加自定义属性 `Name="StorageBalanceType"` `Value="VMCountBasedLeastLoad`。如果您不使用此自定义属性和值，则默认应用增强型轮询方法。

例如：

- 创建主机连接时：

```
New-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"StorageBalanceType`"
Value=`"VMCountBasedLeastLoad`" /></CustomProperties>"
-HypervisorConnectionName "Xen-Connection" -NetworkPath @("XDHyp:
\Connections\Xen-Connection\Network 0.network") -Path @("XDHyp:
\HostingUnits\XS-Network") -PersonalvDiskStoragePath @() -RootPath
"XDHyp:\Connections\Xen-Connection\" -StoragePath @("XDHyp:
\Connections\Xen-Connection\NFS virtual disk storage.storage")
```

- 更新主机连接时：

```
Set-Item  -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"StorageBalanceType`"
Value=`"VMCountBasedLeastLoad`" /></CustomProperties>" -Path @("XDHyp:
\HostingUnits\XS-Network")
```

检测孤立的 Azure 资源

孤立资源是系统中存在的未使用的资源，它们可能导致不必要的开销。

除了云管理员之外，在**主机**下具有**使用主机连接检测虚拟机管理程序中的孤立资源**权限的任何新创建的角色都将能够检测孤立资源。

此功能允许您检测 Citrix Virtual Apps and Desktops 站点上主机中的孤立 Azure 资源。

请按照 Web Studio 上的步骤操作：

1. 在**管理**中，选择左侧窗格中的**托管**。
2. 选择一个连接，然后选择操作栏中的**检测孤立资源**。**检测孤立资源**对话框显示孤立资源报告。
3. 要查看孤立资源报告，请选择**查看报告**。

或者，您可以使用 PowerShell 检测孤立的 Azure 资源。有关详细信息，请参阅检索孤立资源列表。

要了解孤立资源背后的原因，并了解如何进一步操作，请参阅使用 Citrix 有效管理孤立的 Azure 资源。

连接计时器

您可以使用策略设置配置三个连接计时器：

- **最长连接计时器：** 确定用户设备与虚拟桌面之间不间断连接的最长持续时间。使用**会话连接计时器**和**会话连接计时器间隔**策略设置。
- **连接空闲计时器：** 确定在用户没有输入的情况下，用户设备与虚拟桌面之间的不间断连接保持多长时间。使用**会话空闲计时器**和**会话空闲计时器间隔**策略设置。
- **断开连接计时器：** 确定断开连接的锁定虚拟桌面在会话注销之前可以保持锁定的时间。使用**断开连接会话计时器**和**断开连接会话计时器间隔**策略设置。

当您更新任何这些设置时，请确保它们在您的部署中保持一致。

有关详细信息，请参阅策略设置文档。

检索孤立资源列表

您可以获取由 MCS 创建但不再由 MCS 跟踪的孤立资源列表。此功能目前适用于 Azure 环境。要获取列表，您可以使用 PowerShell 命令。您可以使用连接进行筛选。

默认情况下，**完全管理员**和**云管理员**角色已分配此权限。要允许其他角色执行此操作，请在**主机**下为其分配**使用主机连接检测管理程序中的孤立资源**权限。有关详细信息，请参阅创建和管理角色。

> **注意：**
>
> - 如果正在进行任何预配或映像更新，PowerShell 命令将被拒绝。
> - 标记了所有 Citrix 标签的客户管理资源被检测为孤立资源。但是，如果您向该资源添加另一个标签 CitrixDetectIgnore，并将其值设置为 true，则在检测孤立资源时将忽略该资源。

限制

- 只有内置的完全管理员或云管理员角色管理员用户才能运行 PowerShell 命令并获取孤立资源列表。
- 为避免错误识别孤立资源，请勿在筛选孤立资源时打开 VM 的电源。
- 在可能出现繁重工作负载的情况下，大约 2,000 条记录会显示为孤立记录。

要显示孤立资源列表：

1. 打开 **PowerShell** 窗口。
2. 运行以下命令：
    a. 获取连接 uid。连接 uid 是 HypervisorConnectionUid 属性的值。

    ```
    Get-ChildItem xdhyp:\connections | where { $_.PluginId -like
    'Azure*' }"
    ```

    b. 获取孤立资源列表。

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

要从订阅 ID 显示孤立资源列表：

1. 打开 **PowerShell** 窗口。
2. 运行以下命令：
    a. 使用订阅 ID 查找连接 uid。连接 uid 是 HypervisorConnectionUid 属性的值。

    ```
    Get-ChildItem xdhyp:\connections | where { $_.CustomProperties
    -match '<subscriptionId>' }
    ```

    b. 获取孤立资源列表：

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

注意：

删除前请仔细检查资源。

将 WinHttp (netsh) 代理服务器设置用于托管连接

此功能增强允许托管连接使用 WinHttp (netsh) 代理服务器设置与托管连接一起使用。这使得代理设置更简单，并且与用于其他 Citrix 服务的代理设置配置保持一致。

此功能适用于以下虚拟化环境：

- XenServer

- 谷歌云
- 微软 Azure
- 努坦尼克斯
- 红帽 OpenShift
- 威睿

要将 Delivery Controller 上配置的 WinHttp (netsh) 代理服务器用于托管连接，您可以在托管连接中包含此自定义属性。

```
<Property xsi:type="StringProperty"
Name="UseWinHttpProxyForHypervisorTraffic" Value="True" />
```

- 当此自定义属性设置为 `True` 时，如果通过 `netsh winhttp set proxy` 命令在计算机上设置了 WinHttp 代理服务器，则对管理程序的 API 调用将通过该代理服务器路由。
- 当此自定义属性设置为 `False` 时，API 调用将忽略在 DDC 上配置的所有代理服务器（包括 WinINet 代理和 .net 代理）。
- 如果托管连接中不存在此自定义属性，则使用计算机的 `WinINet` 或 `.net` 代理服务器配置。这是现有行为。

用例

- 示例 1：托管连接上未设置自定义属性

  托管连接将读取 WinINet 代理配置，然后读取 .net 代理配置，如果已配置，则使用代理设置。如果未配置任何代理，则创建直接连接。这是现有行为，并将继续按原样工作。

- 示例 2：托管连接上设置了自定义属性，值为 True

  托管连接将仅读取 WinHttp 代理设置，如果存在，则使用这些代理设置。如果不存在，则托管连接将不使用任何代理设置。

- 示例 3：托管连接上设置了自定义属性，值为 False

  托管连接将不会读取计算机上的任何代理配置设置，并将尝试在没有代理的情况下连接到管理程序。

先决条件

在使用 PowerShell 创建主机连接时设置自定义属性之前，请确保在所有桌面交付控制器上配置 WinHTTP 代理。

配置步骤

通过 CLI 创建新的托管连接以使用 WinHttp 代理设置：

```
$CustomProperties = "<CustomProperties  xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<!-- Include any other hypervisor specific custom properties here -->

<Property xsi:type=`"StringProperty`"
Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />

</CustomProperties>"



New-Item -ConnectionType $ConnectionType -HypervisorAddress @('https://
hypervisorhost1.example.com') -Path @('XDHyp:\Connections\
$ConnectionName') -Password $Password -UserName $User -CustomProperties
$CustomProperties
```

在现有托管连接上设置自定义属性：

1. 如果存在，请从托管连接复制现有自定义属性。

   ```
   dir XDHyp:\Connections
   ```

2. 复制托管连接的自定义属性并添加以下内容，然后将其保存到变量中。

   ```
   $CustomProperties

   <Property xsi:type=`"StringProperty`"
   Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />
   ```

   示例：

   ```
   Example:

   $CustomProperties = "<CustomProperties xmlns=`"http://
   schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
   www.w3.org/2001/XMLSchema-instance`">
   ```

```
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`"
Value=`"123abc`" />

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` /
><Property xsi:type=`"StringProperty`"
Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />

</CustomProperties>"
```

如果现有自定义属性为空，请设置自定义属性：

```
$CustomProperties = "<CustomProperties  xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`"
Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />

</CustomProperties>"
```

3. 运行 `Set-Item` 命令以更新现有托管连接。

```
Set-Item -CustomProperties $CustomProperties -LiteralPath @("XDHyp:
\Connections\$ConnectionName") -PassThru -UserName $User
-SecurePassword $Password
```

下一步操作

有关连接到特定主机类型的信息，请参阅：

- 连接到 AWS
- 连接到 XenServer
- 连接到 Google Cloud 环境
- 连接到 Microsoft Azure
- 连接到 微软系统中心虚拟机管理器
- 连接到 Nutanix
- 连接到 Nutanix 云和合作伙伴解决方案
- 连接到 VMware
- 连接到 VMware 云和合作伙伴解决方案

如果您处于初始部署过程中，请创建计算机目录。

连接到 Amulet Hotkey CoreStation

(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections.html)介绍了创建连接的通用向导。以下信息涵盖了 Amulet Hotkey CoreStation 的具体细节。您目前可以使用 PowerShell 命令创建到 Amulet Hotkey CoreStation 的连接。

> **注意：**
>
> 在创建到 Amulet Hotkey CoreStation 的连接之前，您需要先完成 Amulet Hotkey CoreStation 帐户的设置。

创建连接

您可以使用以下方式创建到 Amulet Hotkey CoreStation 的连接：

- 工作室
- PowerShell 命令

使用 STUDIO 创建连接

1. 在**添加连接和资源**页面中，选择 **Amulet Hotkey CoreStation** 作为连接类型。
2. 输入您的 Amulet Hotkey CoreStation 机箱管理器连接地址。您可以将 IP 地址、主机名或 FQDN 用作地址。

3. 输入您的机箱管理凭据和易记的连接名称。

   出现以下任一情况时，连接设置将停止：

   - DaaS 收到带有错误的公共 CA 签名证书：将显示错误消息。按照屏幕上的说明修复问题。否则，您无法继续创建连接。
   - DaaS 收到私有 CA 签名证书：将显示警告页面。将收到的指纹与服务器的指纹进行比较，以验证证书的有效性。如果有效，请选择“信任证书”并单击“确定”以继续创建连接。DaaS 将信任该证书并存储指纹以供将来验证。

使用 POWERSHELL 命令创建连接

使用 PowerShell 命令创建连接时，请提供以下信息：

- IP 地址：Amulet Hotkey CoreStation 的 IP地址
- 用户名: Amulet Hotkey CoreStation 用户名
- 密码: Amulet Hotkey CoreStation 密码

示例：

```
Get-ConfigZone

Get-HypHypervisorPlugin

New-Item `

    -ConnectionType "Custom" `

    -HypervisorAddress $IP `

    -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} `

    -Path @("XDHyp:\Connections\$connectionName") `

    -Persist `

    -PluginId "AmuletHotkeyCoreStationFactory" `

    -Scope @() `

    -SecurePassword $Password `
```

```
    -UserName $UserName `
    -ZoneUid $ZoneUid `
    -SslThumbprint $SslThumbprint
New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$HypervisorConnectionID
```

注意：

`-SslThumbprint` 参数仅适用于私有 CA 签名的证书。

证书和指纹验证

要成功连接到 Amulet Hotkey CoreStation，证书不得有错误，并且指纹必须具有正确的值。以下是与证书和指纹验证相关的用例：

- 公共 CA 签名证书存在错误。连接创建失败。请查看错误详细信息并解决问题。
- 公共 CA 签名证书无错误。连接创建成功，`SslThumbprints` 值为 `Null`。
- 私有 CA 签名证书无错误且具有 `sslthumbprint` 值。连接成功创建，`SslThumbprints` 值正确。
- 私有 CA 签名证书的指纹值不正确。连接创建失败。
- 私有 CA 签名证书无错误。连接创建成功。创建连接时，`SSlThumbprints` 为 `Null`。`SSlThumbprints` 值由站点服务更新为某个值。

管理连接

修复证书问题

当出现证书问题时，Citrix Virtual Apps and Desktops 会阻止 Amulet Hotkey CoreStation 连接，从而阻止您在关联的 Amulet Hotkey CoreStation 节点上交付和管理工作负载。您将在“主机连接”列表中看到连接旁边显示一个错误图标。

有关具体问题和解决方案，请参阅下表。

问题	解决方案
公共 CA 签名的证书出现证书错误。	单击连接并选择“**故障排除**”选项卡。查看错误详细信息并解决问题。
收到的证书是私有 CA 签名的或已过期。	编辑主机连接以更新证书指纹。详细步骤： 1. 选择连接，然后单击 **编辑连接**。 2. 在 **连接属性** 页面上，单击 **编辑设置**。 3. 输入密码以连接到 Amulet Hotkey CoreStation 机箱，然后单击 **保存**。 4. 在出现的 **警告** 页面上，将收到的指纹与服务器的指纹进行比较，以验证证书的有效性。 5. 如果它们相同，请选择 **信任证书**，然后单击 **确定**。

更新指纹值

创建连接后，可以使用 `Set-Item` PowerShell 命令更新连接的指纹值。请按照以下步骤更新指纹值。

1. 获取连接的连接详细信息。例如：

```
Get-Item -LiteralPath xdhyp:\connections\AmuletCon-101
```

2. 更新指纹值。例如：

```
Set-Item -LiteralPath xdhyp:\connections\AmuletCon-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. 检查更新后的指纹值。例如：

```
Get-Item -LiteralPath xdhyp:\connections\AmuletCon-101
```

注意：

如果您在 `Set-Item` 命令中提供了不正确的指纹值，则更新将失败。

后续步骤

- 如果您处于初始部署过程中，请参阅创建计算机目录。
- 有关 Amulet Hotkey CoreStation 的信息，请参阅创建 Amulet Hotkey CoreStation 计算机目录。

更多信息

- 创建和管理连接与资源
- Amulet Hotkey CoreStation 虚拟化环境

连接到 AWS EC2

创建和管理连接和资源 描述了创建连接的向导。以下信息涵盖了 AWS 云环境特有的详细信息。

先决条件

在创建到 AWS EC2 的连接之前，请执行以下操作：

- 完成将 AWS 设置为资源位置。请参阅 AWS 虚拟化环境。
- 定义 IAM 权限 策略，用于 Citrix 代表您管理 AWS 资源的 IAM 用户或角色。

定义 IAM 权限

在创建主机连接之前，需要为 IAM 用户或角色正确定义 IAM 权限策略，该策略授予 Citrix 适当的权限，以代表您在 AWS 账户中预配和管理资源。使用本节中的信息为 AWS 上的 Citrix Virtual Apps and Desktops 定义 IAM 权限。Amazon 的 IAM 服务允许账户拥有多个用户，这些用户可以进一步组织成组。这些用户可以拥有不同的权限来控制其执行与账户相关的操作的能力。有关 IAM 权限的更多信息，请参阅IAM JSON 策略参考。

要将 IAM 权限策略应用于新的用户组：

1. 登录 AWS 管理控制台，然后从下拉列表中选择 **IAM 服务**。
2. 选择 **创建新用户组**。
3. 为新用户组键入名称，然后选择 **继续**。
4. 在 **权限** 页面上，选择 **自定义策略**，然后选择 **选择**。
5. 为 **权限策略** 键入名称。
6. 在 **策略文档** 部分中，输入相关权限。

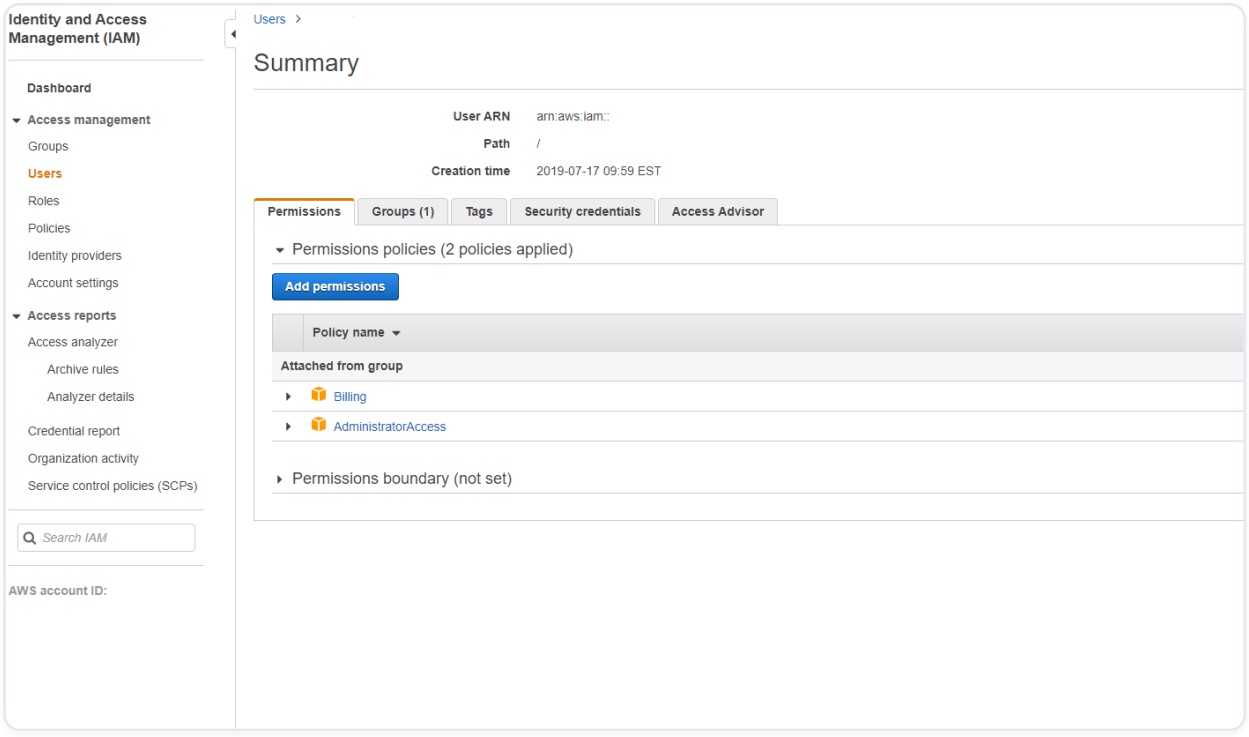
输入策略信息后，选择**继续**以完成将 IAM 权限策略应用于用户组。组中的用户被授予执行 Citrix Virtual Apps and Desktops 所需操作的权限。

> **重要提示：**
>
> 使用本文提供的示例中的策略文本，列出 Citrix Virtual Apps and Desktops 在 AWS 账户中执行操作时使用的操作，而不将这些操作限制为特定资源。Citrix 建议您将此示例用于测试目的。对于生产环境，您可能需要对资源添加进一步的限制。

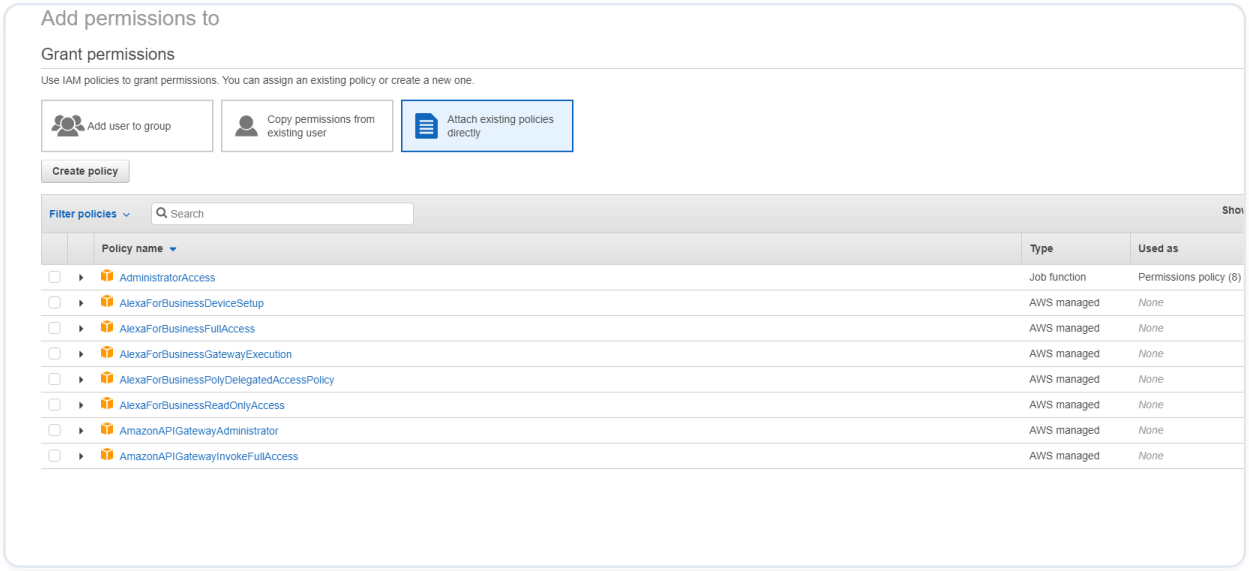
添加 IAM 权限

在 AWS 管理控制台的 **IAM** 部分添加权限：

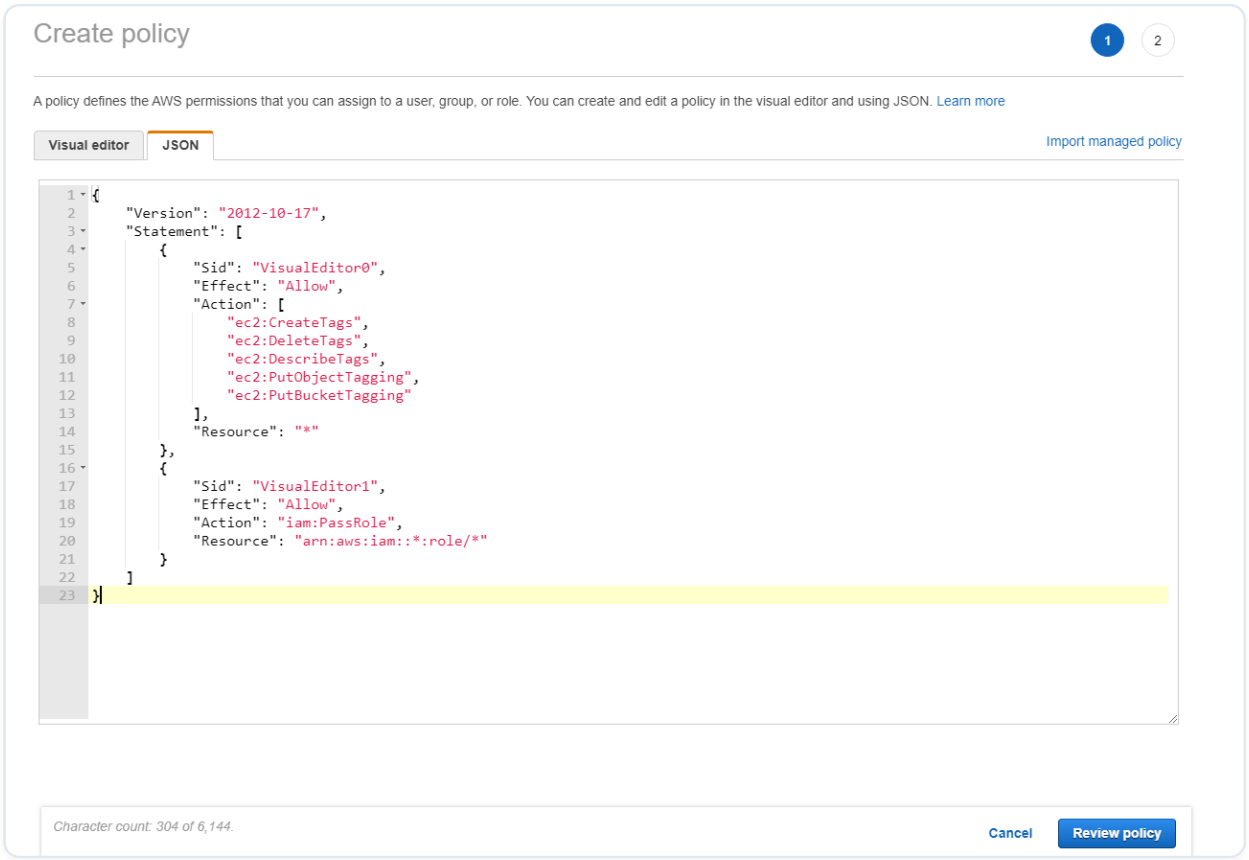
1. 在 **摘要** 面板中，选择 **权限** 选项卡。
2. 选择 **添加权限**。



3. 在 **添加权限到** 屏幕中，授予权限：



4. 在 JSON 部分，为您的环境包含所需的 AWS 权限。



创建连接

您可以使用以下方式创建到 Amazon EC2 的连接：

- Web 控制台
- PowerShell 命令

> **注意：**
>
> 检查您的代理服务器或防火墙限制，并确保以下地址可访问：`https://*.amazonaws.com`。此外，请确保 Citrix Gateway 服务连接 中提及的所有地址均可访问。
>
> 如果这些地址无法访问，则在创建或更新主机连接时可能会导致失败。

使用 WEB STUDIO 创建连接

1. 导航到 **托管 > 添加连接和资源** 页面。
2. 在“**连接**”页面上，按照以下步骤配置连接：
   a. 选择“**创建新连接**”。
   b. 在 **Zone** 中，选择您为 AWS 环境设置的资源位置。
   c. 选择 **Amazon EC2** 作为连接类型。
   d. 选择以下方法之一来预配资源：
      - 如果选择**使用此 AWS 账户预配资源**，则选择**使用 IAM 用户访问密钥**或**使用 IAM 角色**。对于 IAM 用户访问密钥，请提供具有适当 IAM 权限策略的 IAM 用户的 **API 密钥**和**秘密密钥**，以便 Citrix 管理您的 AWS 账户中的资源。对于 IAM 角色，请确保您已为 Delivery Controller 实例分配 IAM 角色，并具有适当的 IAM 权限策略，以便 Citrix 管理您的 AWS 账户中的资源。有关详细信息，请参阅基于角色的身份验证指南。
      - 如果选择**使用跨账户访问预配资源**，则提供账户 B 中 IAM 角色的 **ARN**，账户 A 中的 Delivery Controller 必须承担该角色才能执行预配操作。
   e. 输入连接名称，然后单击 **下一步**。
3. 在**虚拟机位置**页面上，指定必须预配 VM 的位置。选择用于创建新 VM 的云区域、VPC 和可用区。
4. 在 **网络** 页面上：
   a. 为之前在可用区或本地区域中选择的资源输入名称。
   b. 在您在上一个菜单中配置的 VPC 中选择一个或多个子网。
5. 依次单击其余页面，直到 **摘要** 页面。
6. 单击“**完成**”以创建到 Amazon EC2 的主机连接。

重要注意事项

使用 Studio 创建连接时：

- 为 Citrix 定义适当的 IAM 权限以管理您的 AWS 资源。
- 如果您使用 IAM 用户访问密钥让 Citrix 管理您的 AWS 资源，则必须提供 API 密钥和秘密密钥值。您可以从 AWS 导出包含这些值的密钥文件，然后将其导入。您还必须提供区域、可用区、VPC 名称、子网地址、域名、安全组名称和凭据。
- 如果您使用 IAM 角色让 Citrix 管理您的 AWS 资源，则必须确保为所有 Delivery Controller 分配具有适当 IAM 权限的角色。有关详细信息，请参阅基于角色的身份验证指南。
- 根 AWS 账户的凭据文件（从 AWS 控制台检索）的格式与为标准 AWS 用户下载的凭据文件不同。因此，Citrix Virtual Apps and Desktops 无法使用该文件填充 API 密钥和秘密密钥字段。请确保您使用的是 AWS Identity Access Management (IAM) 凭据文件。
- 区域可以是可用区或本地区域。

使用 POWERSHELL 创建连接

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行以下命令。以下是一个示例：

```
$connectionName = "demo-hostingconnection"

$cloudRegion = "us-east-1"

$apiKey = "aaaaaaaaaaaaaaaaaaaa"

$apiSecret = “bbbbb”

$secureKey = ConvertTo-SecureString -String $apiSecret

$zoneUid = "00000000-0000-0000-0000-000000000000"

$connectionPath = "XDHyp:\Connections\" + $connectionName



$connection = New-Item -Path $connectionPath -ConnectionType "<name of
the connection>" -HypervisorAddress " "@("https://ec2.cn-
north-1.amazonaws.com.cn") -Persist -Scope @() -UserName $apiKey
-SecurePassword $secureKey -ZoneUid $zoneUid
```

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid



$hostingUnitName = "demo-hostingunit"

$availabilityzone = "us-east-1a"

$vpcName = "Default VPC"

$jobGroup = [Guid]::NewGuid()

$hostingUnitPath = "XDHyp:\HostingUnits\" + $HostingUnitName

$rootPath = $connectionPath + "\" + $vpcName + ".virtualprivatecloud\"

$availabilityZonePath = @($rootPath + $availabilityzone +
".availabilityzone")

$networkPaths = (Get-ChildItem $availabilityZonePath[0] | Where
ObjectType -eq "Network") | Select-Object -ExpandProperty FullPath #
will select all the networks in the availability zone



New-Item -Path $hostingUnitPath -AvailabilityZonePath
$availabilityZonePath -HypervisorConnectionName $connectionName
-JobGroup $jobGroup -PersonalvDiskStoragePath @() -RootPath $rootPath
-NetworkPath $networkPaths
```

注意：

要使用基于角色的身份验证创建连接，请将 apiKey 和 apiSecret 指定为 `role_based_auth`。

限制

如果在 AWS 控制台中更改 AWS 虚拟私有云 (VPC) 的名称，则 Citrix Cloud™ 中现有的托管单元将中断。托管单元中断后，您将无法创建目录或向现有目录添加计算机。要解决此问题，请将 AWS VPC 的名称改回原始名称。

跨账户预配

在某些用例中，Delivery Controller 希望放置在单独的 AWS 账户（共享服务账户或站点组件账户）中，并具有跨账户访问权限的 IAM 角色（跨账户 IAM 角色），而 MCS 预配的计算机目录则放置在单独的辅助 AWS 账户（工作负载账户）中，而无需在单独的账户中部署额外的 Delivery Controller。为了支持此类场景，此功能使用 VPC 对等和通过 IAM 角色进行的跨账户访问，使管理多个 AWS 账户的企业能够实现跨不同 AWS 账户的预配。

通过VPC 对等，您可以让您的 Delivery Controller 和预配的 VM 位于不同区域或账户中，并能够相互通信。

通过使用 IAM 角色进行跨账户访问，您可以允许主账户（Delivery Controller 账户）承担 IAM 角色以访问辅助账户（计算机目录 VM）中的 AWS 资源。

要允许 Delivery Controller 访问辅助账户的资源，请在承担辅助账户的 IAM 角色后创建主机连接。

先决条件

在为跨账户预配创建主机连接之前，请设置以下内容：

- 设置 VPC 对等连接，并配置两个区域或账户中的安全组。请参阅 设置 VPC 对等连接。
- 使用 IAM 角色委派跨账户访问。请参阅 使用 IAM 角色委派跨账户访问。

设置 VPC 对等连接

假设 VPC A 位于主账户（账户 A）中，并且包含 Delivery Controller 和 Active Directory。VPC B 位于辅助账户（账户 B）中，您希望在此处预配 VM。

要在账户 A 和账户 B 之间设置 VPC 对等连接，请执行以下操作：

1. 创建 VPC 对等连接。请参阅：
    - 不同账户，相同区域
    - 不同账户，不同区域
2. 转到您的 VPC A 和与公共子网关联的路由表。
3. 单击 **编辑路由 > 添加路由**。在**目标**列中添加 VPC B 的 CIDR 块，并在**目标**列中添加您创建的 VPC 对等连接。

4. 重复步骤 2 和 3，但使用 VPC A 和 VPC B 的私有子网（添加 VPC A 的 CIDR 块）。请参阅 更新 VPC 对等连接的路由表。
5. 转到与 VPC A 关联的私有安全组。
6. 选择 **操作**，然后选择 **编辑入站规则**。
7. 选择 **添加规则**。对于类型，选择 **所有流量**，然后在**源列**中添加：
   - 如果是不同区域，添加 VPC B 的 CIDR 块。
   - 如果是不同账户但相同区域，添加 VPC B 的账户 ID 和私有安全组 ID，用斜杠分隔（例如，123456789012/sg-1a2b3c4d）。
8. 重复步骤 5 到 7，但使用 VPC B 的私有安全组（但添加 VPC A 的 CIDR 块或 VPC A 的账户 ID 和相同区域但不同账户的私有安全组 ID）。请参阅更新您的安全组以引用对等安全组。

> **注意：**
>
> 创建 VPC 对等连接不收取费用。但是，虽然可用区内的 VPC 对等是免费的，但当数据通过 VPC 对等连接跨多个可用区和区域传输时，会收取费用。请参阅VPC 对等连接定价。

使用 IAM 角色委派跨账户访问

设置跨账户 VPC 对等连接后，您可以使用 IAM 角色委派跨账户访问。

通过使用 IAM 角色进行跨账户访问，您可以允许主账户（交付控制器账户）承担 IAM 角色，以访问辅助账户（计算机目录 VM）中的 AWS 资源。

要访问跨账户资源，请执行以下操作：

> **请记住：**
>
> 假设 VPC A 位于主账户（账户 A）中，并且它具有交付控制器和 Active Directory。VPC B 位于辅助账户（账户 B）中，您希望在此处预配 VM

1. 按照前面提到的步骤设置跨账户 VPC 对等连接。
2. 在账户 B 中创建具有最少 Citrix IAM 权限的 IAM 角色和策略。请参阅 IAM 教程：使用 IAM 角色委派跨 AWS 账户访问权限。假设此角色的 ARN 为“arn:aws:iam::5678:role/citrix-role”。

3. 将信任策略添加到角色“arn:aws:iam::5678:role/citrix-role”，以便账户 A 角色“arn:aws:iam::1234:role/primary-account-citrix-role”可以访问它，如 IAM 中的跨账户资源访问中所述。
4. 在账户 A 中创建之前提到的名为“primary-account-citrix role”的 IAM 角色和策略，该角色和策略可以承担 IAM 角色并从账户 B 传递 IAM 角色 (arn:aws:iam::5678:role/citrix-role)。
5. 将角色“arn:aws:iam::1234:role/primary-account-citrix-role”分配给账户 A 中的所有交付控制器。

交付控制器现在可以从账户 B 承担角色（“arn:aws:iam::5678:role/citrix-role”）。

为跨账户预配创建主机连接

在辅助账户（账户 B）中创建主机连接，您希望在此处预配 VM。这允许账户 A 的交付控制器在承担账户 B 中的角色后访问账户 B 中的资源。

使用 PowerShell 命令创建主机连接并添加以下两个自定义属性：

- `CrossAccountRoleArn`：如果您不提供 `CrossAccountRoleArn` 属性，则会创建常规主机连接。在这种情况下，即使提供了 `MaximumAssumeRoleDurationInSeconds`，也会被忽略。
- `MaximumAssumeRoleDurationInSeconds`：`DurationInSeconds` 必须介于 900 秒到 3600 秒之间。默认值为 900 秒。如果您提供的值超过 3600，则 `DurationInSeconds` 将设置为 3600。

示例：

```
$connectionName = "cross-account-conn"

$cloudRegion = "us-east-1"

$apiKey = "role_based_auth"

$secretKey = "role_based_auth"

$zoneUid = "xxxxxx"

$secureKey = (ConvertTo-SecureString -String $secretKey -AsPlainText
-Force)

$connectionPath = "XDHyp:\Connections\" + $connectionName

$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
```

```
<Property xsi:type="StringProperty" Name="CrossAccountRoleArn"
Value="arn:aws:iam::5678:role/citrix-role" /><Property
xsi:type="StringProperty" Name="MaximumAssumeRoleDurationInSeconds"
Value="3600" />

"</CustomProperties>'



$connection = New-Item -Path $connectionPath -ConnectionType "AWS"
-HypervisorAddress "https://ec2.$($cloudRegion).amazonaws.com" -Persist
-Scope @() -UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid
-CustomProperties $customProperties



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

创建主机连接后，使用 Studio 或 PowerShell 创建托管单元。但是，请选择 VPC 和网络。

编辑连接

您可以编辑现有主机连接以：

- 修改为 Citrix 提供 IAM 权限以管理资源的选项
- 修改每个托管连接的最大同时操作数（或并发计算机数）
- 修改范围。
- 使用 PowerShell 命令配置每个弹性网络接口 (ENI) 允许的最大安全组数

编辑选项以提供 IAM 权限

1. 右键单击现有 Amazon EC2 连接。
2. 在“**连接属性**”页面上，单击“**编辑设置**”。
3. 选择其中一个选项以提供 IAM 权限，供 Citrix 管理资源。输入所需详细信息，然后单击“**保存**”。

修改最大并发操作数

在 Studio 中为 Amazon EC2 创建主机连接时，将显示以下默认值：

选项	绝对值	百分比
并发操作（所有类型）	125	100
每分钟最大新增操作数	150	不适用
最大并发预配操作数	100	不适用

MCS 默认支持 100 个最大并发预配操作。

通过访问 **Edit Connection**（编辑连接）屏幕上的 Citrix Studio **Advanced**（高级）部分来配置这些值。

或者，您可以使用远程 PowerShell SDK 设置最大并发操作数，以根据您的环境获得最佳设置。

使用 PowerShell 自定义属性 `MaximumConcurrentProvisioningOperations` 来指定最大并发 AWS 预配操作数。

配置前：

- 确保您已安装适用于 Cloud 的 PowerShell SDK。
- 请注意，`MaximumConcurrentProvisioningOperations` 的默认值为 100。

执行以下步骤来自定义 `MaximumConcurrentProvisioningOperations` 值：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 输入 `cd xdhyp:\Connections\`。
4. 输入 `dir` 以列出连接。
5. 更改或初始化自定义属性字符串：
    - 如果自定义属性字符串有值，请将自定义属性复制到记事本中。接下来，将 `MaximumConcurrentProvisioningOperations` 属性更改为首选值。您可以输入 1-1000 范围内的值。 例如，`<Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="xyz"/>`。
    - 如果自定义属性字符串为空或为 null，则必须通过输入架构和 `MaximumConcurrentProvisioningOperations` 属性的正确语法来初始化该字符串。
6. 在 **PowerShell** 窗口中，从记事本粘贴修改后的自定义属性，并将变量分配给修改后的自定义属性。如果已初始化自定义属性，请在语法后添加以下行：

`$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="100"/></CustomProperties>'`。

此字符串将 `MaximumConcurrentProvisioningOperations` 属性设置为 100。在自定义属性字符串中，您必须将 `MaximumConcurrentProvisioningOperations` 属性设置为符合您需求的值。

7. 输入 `Get-XDAuthentication`，系统将提示您输入凭据。
8. 运行 `$cred = Get-Credential`，系统可能会提示您仅输入密码（或用户名和密码）。系统还可能提示您输入应用程序 ID 和关联的密钥。对于使用基于角色的身份验证的连接，**role_based_auth** 既是用户名也是密码。否则，请输入 AWS API ID 和密钥。
9. 运行 `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`。您必须将 *<connection-name>* 设置为连接的名称。
10. 输入 `dir` 以验证更新的 CustomProperties 字符串。

配置每个网络接口的安全组

编辑主机连接时，您现在可以使用 PowerShell 命令配置每个弹性网络接口 (ENI) 允许的最大安全组数量。有关 AWS 安全组配额值的信息，请参阅安全组。

要配置每个网络接口的安全组：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行 `cd xdhyp:\Connections\`。
4. 运行 `dir` 以列出连接。
5. 运行以下 PowerShell 命令以配置每个网络接口的安全组：

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws -Name "Citrix_MachineManagement_Options" -Value "AwsMaxENISecurityGroupLimit=<number>"
```

> **注意：**

> 如果您未设置 `AwsMaxENISecurityGroupLimit` 的值，则它将采用默认值 5。

服务终结点 URL

标准区域服务端点 URL

使用 MCS 时，将添加一个包含 API 密钥和 API 秘密的新 AWS 连接。借助此信息以及经过身份验证的帐户，MCS 使用 AWS DescribeRegions EC2 API 调用查询 AWS 以获取支持的区域。查询是使用通用 EC2 服务端点 URL `https://ec2.amazonaws.com/` 进行的。使用 MCS 从支持的区域列表中为连接选择区域。首选的 AWS 服务端点 URL 会自动为该区域选择。但是，创建服务端点 URL 后，您将无法再设置或修改该 URL。

所需的 AWS 权限

本节包含 AWS 权限的完整列表。使用本节中提供的完整权限集，以确保功能正常运行。

> **注意：**
>
> `iam:PassRole` 权限仅用于 **role_based_auth**。

创建主机连接

使用从 AWS 获取的信息添加新的主机连接。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

虚拟机电源管理

虚拟机开机或关机。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances",
                "ec2:DescribeInstanceStatus"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
```

```
    ]
}
```

创建、更新或删除虚拟机

已创建、更新或删除计算机目录，其中虚拟机作为 AWS 实例进行预配。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
```

```
                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:CancelSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",



                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",
```

```
            "ec2:DisassociateIamInstanceProfile",
            "ec2:RunInstances",
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances"
        ],
        "Effect": "Allow",
        "Resource": "*"
    },
    {
        "Action": [
            "ec2:CreateSecurityGroup",
            "ec2:DeleteSecurityGroup"
        ],
        "Effect": "Allow",
        "Resource": "*"
    },
    {
        "Action": [
            "ebs:StartSnapshot",
            "ebs:GetSnapshotBlock",
            "ebs:PutSnapshotBlock",
```

```
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

注意：

- 仅在目录创建期间必须为准备虚拟机创建隔离安全组时，才需要与 SecurityGroups 相关的 EC2 部分。完成此操作后，不再需要这些权限。

导入虚拟机

通过导入虚拟机创建计算机目录。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
```

```
                "ec2:DescribeSecurityGroups",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeSubnets",

                "ec2:DescribeVolumes",

                "ec2:DescribeSpotInstanceRequests"

            ],

            "Effect": "Allow",

            "Resource": "*"

        }

    ]

}
```

注意：

仅当将从 AWS 区域导入虚拟机且该区域中存在竞价型实例时，才需要 `ec2:DescribeSpotInstanceRequests`。

直接磁盘上传和下载

直接磁盘上传消除了计算机目录预配对卷工作程序的要求，而是使用 AWS 提供的公共 API。此功能降低了与额外存储帐户相关的成本以及维护卷工作程序操作的复杂性。

注意：

已移除对卷工作程序的支持。计算机目录预配需要直接磁盘上传和下载权限。

必须将以下权限添加到策略中：

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

重要提示：

- 您可以将新的 VM 添加到现有计算机目录中，而无需任何卷工作程序资源，例如卷工作程序 AMI 和卷工作程序 VM。
- 如果您删除了之前使用过任何卷工作程序的现有目录，则所有与卷工作程序相关的工件都将被删除。

已创建卷的 EBS 加密

如果 AMI 已加密，或者 EBS 配置为加密所有新卷，则 EBS 可以自动加密新创建的卷。但是，要实现此功能，IAM 策略中必须包含以下权限。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",
```

```
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
    ]
}
```

注意：

权限可以通过在用户酌情决定下包含资源和条件块来限制为特定密钥。例如，**带条件的 KMS 权限：**

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "kms:CreateGrant",

                "kms:Decrypt",

                "kms:DescribeKey",

                "kms:GenerateDataKeyWithoutPlainText",

                "kms:GenerateDataKey",

                "kms:ReEncryptTo",

                "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"

            ],

            "Condition": {

                "Bool": {

                    "kms:GrantIsForAWSResource": true

                }

            }

        }

    ]

}
```

以下密钥策略语句是 KMS 密钥的整个默认密钥策略，它允许帐户使用 IAM 策略委托 KMS 密钥上的所有操作 (kms:*) 权限。

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",

"Resource": ""

}
```

有关更多信息，请参阅 AWS Key Management Service 官方文档。

基于 IAM 角色的身份验证

添加以下权限以支持基于角色的身份验证。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]
```

```
}
```

最低 IAM 权限策略

以下 JSON 可用于所有当前支持的功能。您可以使用此策略创建主机连接、创建、更新或删除 VM 以及执行电源管理。 该策略可以按照 定义 IAM 权限 部分中的说明应用于用户，或者您也可以使用 **role_based_auth** 安全密钥和秘密密钥进行基于角色的身份验证。

重要提示：

要使用 **role_based_auth**，请在设置交付控制器时，首先在交付控制器 ec2 实例上配置所需的 IAM 角色。使用 Web Studio，添加托管连接并为身份验证密钥和机密提供 role_based_auth。具有这些设置的托管连接随后使用基于角色的身份验证。

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:AttachVolume",

                "ec2:AssociateIamInstanceProfile",

                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:RevokeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateNetworkInterface",
```

```
                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteLaunchTemplate",

                "ec2:DeleteNetworkInterface",

                "ec2:DeleteSecurityGroup",

                "ec2:DeleteSnapshot",

                "ec2:DeleteTags",

                "ec2:DeleteVolume",

                "ec2:DeregisterImage",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:CancelSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
```

```
            "ec2:CreateSecurityGroup",
            "ec2:DeleteSecurityGroup"
        ],
        "Effect": "Allow",
        "Resource": "*"
    },
    {
        "Action": [
            "ebs:StartSnapshot",
            "ebs:GetSnapshotBlock",
            "ebs:PutSnapshotBlock",
            "ebs:CompleteSnapshot",
            "ebs:ListSnapshotBlocks",
            "ebs:ListChangedBlocks",
            "ec2:CreateSnapshot"
        ],
        "Effect": "Allow",
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
```

```
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
    ]
}
```

注意：

- 仅当在目录创建期间必须为准备 VM 创建隔离安全组时，才需要与 SecurityGroups 相关的 EC2 部分。完成此操作后，不再需要这些权限。
- KMS 部分仅在使用 EBS 卷加密时才需要。

- `iam:PassRole` 权限部分仅在 **role_based_auth** 时才需要。
- 可以根据您的要求和环境添加特定的资源级权限，而不是完全访问权限。有关更多详细信息，请参阅 AWS 文档 Demystifying EC2 Resource-Level Permissions 和 Access management for AWS resources。
- 仅当您使用卷工作程序方法时，才使用 `ec2:CreateNetworkInterface` 和 `ec2:DeleteNetworkInterface` 权限。

验证主机连接上的权限

您可以验证主机连接上的权限，以执行与创建和管理 MCS 计算机目录相关的任务。此实现可帮助您提前找出在不同场景（例如创建、删除和更新 VM、VM 的电源管理和 EBS 加密）中所需的缺失权限，从而避免在关键时刻受阻。

您可以使用 PowerShell 命令 `Test-HypHypervisorConnection` 验证主机连接上的权限。该命令的结果将捕获为一个列表，列表中的每个项目都分为三个部分。

- 类别：用户可以执行的用于创建和管理 MCS 计算机目录的操作或任务。
- 纠正措施：管理员必须执行的步骤，以解决用户缺失权限的差异。
- 缺失权限：某个类别的缺失权限列表。

要验证权限，请执行以下操作：

1. 创建到 AWS 的主机连接。
2. 从 Delivery Controller™ 主机打开 PowerShell 窗口。
3. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
4. 运行以下命令以验证您是否具有查找权限所需的权限。

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AWSCon"
```

5. 在添加了查找权限所需的缺失权限后，运行以下命令以验证您是否在以下类别中拥有权限：
   - 创建 更新 删除
   - 电源管理
   - EBS 加密

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:
\Connections\AWSCon" [-SecurePassword -Password] "password" -UserName
"" -CustomProperties ""
```

有关添加权限的更多信息，请参阅 添加 IAM 权限。

下一步

- 如果您处于初始部署过程中，请参阅 创建计算机目录。
- 有关 AWS 特定信息，请参阅 创建 AWS EC2 目录。

更多信息

- 创建和管理连接与资源
- AWS 虚拟化环境

连接到 Amazon WorkSpaces Core 托管实例

创建和管理连接和资源 描述了创建连接的向导。以下信息涵盖了 Amazon WorkSpaces Core 托管实例的特定详细信息。

先决条件

在创建到 Amazon WorkSpaces Core 托管实例的连接之前，请执行以下操作：

- 完成将 AWS 设置为资源位置。请参阅 AWS 虚拟化环境。
- 定义 IAM 权限 策略，用于 IAM 用户或角色，以便 Citrix® 代表您管理 AWS 资源。
- 创建服务相关角色。

定义 IAM 权限

在创建主机连接之前，需要为 IAM 用户或角色正确定义 IAM 权限策略，以便 Citrix 获得代表您在 AWS 账户中预配和管理资源的适当权限。使用本节中的信息为 Amazon WorkSpaces Core 托管实例上的 Citrix Virtual Apps and Desktops 定义 IAM 权限。Amazon 的 IAM 服务允许账户拥有多个用户，这些用户可以进一步组织成组。这些用户可以拥有不同的权限，以控制其执行与账户关联的操作的能力。有关 IAM 权限的更多信息，请参阅IAM JSON 策略参考。

> **注意：**
>
> 由于 Citrix 代表您在 AWS 账户中预置和管理资源和自动化，因此不支持基于特定标签或资源命名约定配置 IAM 权限策略。

> 要将 IAM 权限策略应用于新的用户组：

1. 登录 AWS 管理控制台，并从下拉列表中选择 **IAM 服务**。
2. 选择 **创建新的用户组**。
3. 为新的用户组键入名称，然后选择 **继续**。
4. 在“**权限**”页面上，选择“**自定义策略**”。
5. 为“**权限策略**”键入名称。
6. 在“**策略文档**”部分中，输入相关权限。

输入策略信息后，选择“**继续**”以完成将 IAM 权限策略应用于用户组。组中的用户被授予仅执行 Citrix Virtual Apps and Desktops 所需操作的权限。

> **重要提示：**
>
> 使用本文提供的示例中的策略文本列出 Citrix Virtual Apps and Desktops 用于在 AWS 账户中执行操作的操作，而不将这些操作限制到特定资源。Citrix 建议您将该示例用于测试目的。对于生产环境，您可能需要对资源添加进一步的限制。

添加 IAM 权限

在 AWS 管理控制台的“**IAM**”部分中添加权限：

1. 在“**摘要**”面板中，选择“**权限**”选项卡。
2. 选择“**添加权限**”。
3. 在“**添加权限到**”屏幕中，授予权限。
4. 在 JSON 部分中，包含适用于您的环境的所需 AWS 权限。

创建服务相关角色

对于 Citrix 将调用 Core V2 API 的每个 AWS 账户，创建一个服务相关角色 (SLR)。

创建角色的步骤：

- 在 AWS 管理控制台中打开命令行界面 (CLI)。
- 在 CLI 中运行以下命令：

```
aws iam create-service-linked-role --aws-service-name workspaces-instances.amazonaws.com
```

您还可以使用 Amazon WorkSpaces Core 管理控制台配置服务相关角色。请参阅创建服务相关角色（控制台）。

创建连接

您可以使用以下方式创建到 Amazon WorkSpaces Core 托管实例的连接：

- Web 工作室
- PowerShell 命令

> **注意：**
>
> 检查您的代理服务器或防火墙限制，并确保以下地址可访问：`https://*.amazonaws.com` 和 `https://*.api.aws`。此外，请确保 Citrix Gateway 服务连接 中提及的所有地址均可访问。
>
> 如果这些地址不可访问，则在创建或更新主机连接时可能会导致失败。

使用 WEB STUDIO 创建连接

1. 导航到 **托管 > 添加连接和资源** 页面。
2. 在“**连接**”页面上，按照以下步骤配置连接：
   a. 选择“**创建新连接**”。
   b. 在 **Zone** 中，选择您为 AWS 环境设置的资源位置。
   c. 选择 **Amazon WorkSpaces Core** 作为连接类型。
   d. 选择 **使用 IAM 用户访问密钥** 或 **使用 IAM 角色**。

      对于 IAM 用户访问密钥，请提供具有适当 IAM 权限策略的 IAM 用户的 **API 密钥** 和 **秘密密钥**，以便 Citrix 管理您的 AWS 账户中的资源。

      对于 IAM 角色，请确保您已为 Delivery Controller 实例分配 IAM 角色，并具有适当的 IAM 权限策略，以便 Citrix 管理您的 AWS 账户中的资源。有关详细信息，请参阅基于角色的身份验证指南。
   e. 输入连接名称，然后单击 **下一步**。
3. 在“**虚拟机位置**”页面上，指定必须预配 VM 的位置。选择用于创建新 VM 的云区域、VPC 和可用区。

4. 在 **网络** 页面上：
    a. 为之前在可用区或本地区域中选择的资源输入名称。
    b. 在您在上一个菜单中配置的 VPC 中选择一个或多个子网。
5. 依次单击其余页面，直到 **摘要** 页面。
6. 单击 **完成** 以创建到 Amazon WorkSpaces Core 托管实例的主机连接。

重要注意事项
使用 Web Studio 创建连接时：

- 为 Citrix 定义适当的 IAM 权限以管理您的 AWS 资源。
- 如果您使用 IAM 用户访问密钥让 Citrix 管理您的 AWS 资源，则必须提供 API 密钥和秘密密钥值。您可以从 AWS 导出包含这些值的密钥文件，然后将其导入。您还必须提供区域、可用区、VPC 名称、子网地址、域名、安全组名称和凭据。
- 如果您使用 IAM 角色供 Citrix 管理您的 AWS 资源，则必须确保为所有 Delivery Controller 分配具有适当 IAM 权限的角色。有关详细信息，请参阅基于角色的身份验证指南。
- 根 AWS 账户的凭据文件（从 AWS 控制台检索）的格式与为标准 AWS 用户下载的凭据文件不同。因此，Citrix Virtual Apps and Desktops 无法使用该文件填充 API 密钥和秘密密钥字段。请确保您使用的是 AWS Identity Access Management (IAM) 凭据文件。
- 区域可以是可用区或本地区域。

使用 POWERSHELL 创建连接

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行以下命令。示例如下：

```
$connectionName = "demo-hostingconnection"

$cloudRegion = "us-east-1"

$apiKey = "aaaaaaaaaaaaaaaaaaaa"

$apiSecret = “bbbbb”

$secureKey = ConvertTo-SecureString -String $apiSecret

$zoneUid = "00000000-0000-0000-0000-000000000000"
```

```
$connectionPath = "XDHyp:\Connections\" + $connectionName



$connection = New-Item -Path $connectionPath -ConnectionType
"AmazonWorkSpacesCoreMachineManagerFactory" -HypervisorAddress "
"https://workspaces-instances.$($cloudRegion).api.aws"" -Persist -Scope
@() -UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid



$hostingUnitName = "demo-hostingunit"

$availabilityzone = "us-east-1a"

$vpcName = "Default VPC"

$jobGroup = [Guid]::NewGuid()

$hostingUnitPath = "XDHyp:\HostingUnits\" + $HostingUnitName

$rootPath = $connectionPath + "\" + $vpcName + ".virtualprivatecloud\"

$availabilityZonePath = @($rootPath + $availabilityzone +
".availabilityzone")

$networkPaths = (Get-ChildItem $availabilityZonePath[0] | Where
ObjectType -eq "Network") | Select-Object -ExpandProperty FullPath #
will select all the networks in the availability zone



New-Item -Path $hostingUnitPath -AvailabilityZonePath
$availabilityZonePath -HypervisorConnectionName $connectionName
-JobGroup $jobGroup -PersonalvDiskStoragePath @() -RootPath $rootPath
-NetworkPath $networkPaths
```

> **注意：**
>
> 要使用基于角色的身份验证创建连接，请将 apiKey 和 apiSecret 指定为 `role_based_auth`。

限制

如果您在 AWS 控制台中更改 AWS 虚拟私有云 (VPC) 的名称，则 Citrix Cloud™ 中现有的托管单元将中断。当托管单元中断时，您无法创建目录或向现有目录添加计算机。要解决此问题，请将 AWS VPC 的名称改回原始名称。

跨账户预配

在某些用例中，Cloud Connector 希望部署在单独的 AWS 账户（共享服务账户或站点组件账户）中，并具有跨账户访问权限的 IAM 角色（跨账户 IAM 角色），而 MCS 预配的计算机目录则位于单独的辅助 AWS 账户（工作负载账户）中，而无需在这些单独的账户中部署额外的 Cloud Connector。为了支持此类场景，此功能使用 VPC 对等和通过 IAM 角色进行的跨账户访问，从而使管理多个 AWS 账户的企业能够跨不同 AWS 账户进行预配。

通过VPC 对等，您可以让您的 Cloud Connector 和位于不同区域或账户中的预配 VM 能够相互通信。

通过使用 IAM 角色进行跨账户访问，您可以允许主账户（Cloud Connector 账户）承担 IAM 角色，以访问辅助账户（计算机目录 VM）中的 AWS 资源。

要允许 Cloud Connector 访问辅助账户的资源，请在承担辅助账户中的 IAM 角色后创建主机连接。

先决条件

在为跨账户预配创建主机连接之前，请设置以下各项：

- 设置 VPC 对等连接并在两个区域或账户中配置安全组。请参阅 设置 VPC 对等连接。
- 使用 IAM 角色委派跨账户访问权限。请参阅 使用 IAM 角色委派跨账户访问权限。

设置 VPC 对等连接

假设 VPC A 位于主账户（账户 A）中，并且包含 Cloud Connector 和 Active Directory。VPC B 位于辅助账户（账户 B）中，您希望在此处预配 VM。

要在账户 A 和账户 B 之间设置 VPC 对等连接，请执行以下操作：

1. 创建 VPC 对等连接。请参阅：
    - 不同账户，相同区域

- 不同账户，不同区域

2. 转到您的 VPC A 以及与公共子网关联的路由表。
3. 单击 **Edit Routes > Add route**。在“**目标地址**”列中添加 VPC B 的 CIDR 块，并在“**目标**”列中添加您创建的 VPC 对等连接。
4. 重复步骤 2 和 3，但使用 VPC A 和 VPC B 的私有子网（添加 VPC A 的 CIDR 块）。请参阅 更新 VPC 对等连接的路由表。
5. 转到与 VPC A 关联的私有安全组。
6. 选择“**操作**”，然后选择“**编辑入站规则**”。
7. 选择“**添加规则**”。对于类型，选择“**所有流量**”，然后在“**源列**”中添加：
   - 如果它是不同的区域，请添加 VPC B 的 CIDR 块。
   - 如果它是不同的账户但属于同一区域，请添加 VPC B 的账户 ID 和私有安全组 ID，并用斜杠分隔（例如，123456789012/sg-1a2b3c4d）
8. 重复步骤 5 到 7，但使用 VPC B 的私有安全组（但添加 VPC A 的 CIDR 块或 VPC A 的账户 ID 和同一区域但不同账户的私有安全组 ID）。请参阅更新安全组以引用对等安全组。

> **注意：**
>
> 创建 VPC 对等连接不收取费用。但是，虽然可用区内的 VPC 对等是免费的，但当数据通过 VPC 对等连接跨多个可用区和区域传输时，会产生费用。请参阅 VPC 对等连接定价。

使用 IAM 角色委派跨账户访问

在设置跨账户 VPC 对等后，您可以使用 IAM 角色委派跨账户访问。

通过使用 IAM 角色进行跨账户访问，您可以允许主账户（Cloud Connector 账户）承担 IAM 角色，以访问辅助账户（计算机目录 VM）中的 AWS 资源。

要访问跨账户资源，请执行以下操作：

> **请记住：**
>
> 假设 VPC A 位于主账户（账户 A）中，并且它具有 Cloud Connector 和 Active Directory。VPC B 位于辅助账户（账户 B）中，您希望在此处预配 VM

1. 按照前面提到的步骤设置跨账户 VPC 对等。
2. 在账户 B 中创建具有最少 Citrix IAM 权限的 IAM 角色和策略。请参阅IAM 教程：使用 IAM 角色委派跨 AWS 账户访问。假设此角色的 ARN 为“arn:aws:iam::5678:role/citrix-role”。
3. 将信任策略添加到角色“arn:aws:iam::5678:role/citrix-role”，以便账户 A 角色“arn:aws:iam::1234:role/primary-account-citrix-role”可以访问它，按照 - IAM 中的跨账户资源访问。
4. 在账户 A 中创建 IAM 角色和策略，名称如前所述“primary-account-citrix role”，该角色可以承担 IAM 角色并从账户 B 传递 IAM 角色 (arn:aws:iam::5678:role/citrix-role)。
5. 将角色“arn:aws:iam::1234:role/primary-account-citrix-role”分配给账户 A 中的所有 Cloud Connector。

云连接器现在可以从账户 B（"arn:aws:iam::5678:role/citrix-role"）承担角色。

为跨账户预配创建主机连接

在辅助账户（账户 B）中创建主机连接，您希望在此账户中预配虚拟机。这允许账户 A 的云连接器在从账户 B 承担角色后访问账户 B 中的资源。

使用 PowerShell 命令创建主机连接并添加以下两个自定义属性：

- `CrossAccountRoleArn`：如果您不提供 `CrossAccountRoleArn` 属性，则会创建常规主机连接。在这种情况下，即使提供了 `MaximumAssumeRoleDurationInSeconds`，也会被忽略。
- `MaximumAssumeRoleDurationInSeconds`：`DurationInSeconds` 必须介于 900 秒到 3600 秒之间。默认值为 900 秒。如果您提供的值超过 3600，则 `DurationInSeconds` 将设置为 3600。

示例：

```
$connectionName = "cross-account-conn"

$cloudRegion = "us-east-1"

$apiKey = "role_based_auth"

$secretKey = "role_based_auth"

$zoneUid = "xxxxxx"

$secureKey = (ConvertTo-SecureString -String $secretKey -AsPlainText
-Force)
```

```
$connectionPath = "XDHyp:\Connections\" + $connectionName

$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CrossAccountRoleArn"
Value="arn:aws:iam::5678:role/citrix-role" /><Property
xsi:type="StringProperty" Name="MaximumAssumeRoleDurationInSeconds"
Value="3600" />

"</CustomProperties>'



$connection = New-Item -Path $connectionPath -ConnectionType
"AmazonWorkSpacesCoreMachineManagerFactory" -HypervisorAddress "https://
workspaces-instances.$($cloudRegion).api.aws" -Persist -Scope @()
-UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid
-CustomProperties $customProperties



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

创建主机连接后，使用 Web Studio 或 PowerShell 创建托管单元。但是，请选择 VPC 和网络。

编辑连接

您可以编辑现有主机连接以：

- 修改为 Citrix 提供 IAM 权限以管理资源的选项
- 修改每个托管连接的最大同时操作数（或并发计算机数）
- 修改范围。
- 使用 PowerShell 命令配置每个弹性网络接口 (ENI) 允许的最大安全组数

编辑选项以提供 IAM 权限

1. 右键单击现有 Amazon WorkSpaces Core 连接。
2. 在“**连接属性**”页面上，单击“**编辑设置**”。
3. 选择其中一个选项以提供 Citrix 管理资源的 IAM 权限。输入所需详细信息，然后单击“**保存**”。

修改最大并发操作数

在 Studio 中为 Amazon WorkSpaces Core 托管实例创建主机连接时，将显示以下默认值：

选项	绝对值	百分比
并发操作（所有类型）	125	100
每分钟最大新增操作数	150	不适用
最大并发预配操作数	150	不适用

MCS 默认支持 150 个最大并发预配操作。

您可以通过在 **Edit Connection**（编辑连接）屏幕上访问 Citrix Studio 的 **Advanced**（高级）部分来配置这些值：

或者，您可以使用远程 PowerShell SDK 设置最大并发操作数，以根据您的环境获得最佳设置。

使用 PowerShell 自定义属性 `MaximumConcurrentProvisioningOperations` 来指定最大并发 AWS 预配操作数。

配置前：

- 确保您已安装适用于 Cloud 的 PowerShell SDK。
- 请注意，`MaximumConcurrentProvisioningOperations` 的默认值为 150。

执行以下步骤来自定义 `MaximumConcurrentProvisioningOperations` 值：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 输入 `cd xdhyp:\Connections\`。
4. 输入 `dir` 以列出连接。
5. 更改或初始化自定义属性字符串：
    - 如果自定义属性字符串有值，请将自定义属性复制到记事本中。然后，将 `MaximumConcurrentProvisioningOperations` 属性更改为首选值。您可以输入 1-1000 范围内的值。 例如，`<Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="xyz"/>`。
    - 如果自定义属性字符串为空或为 null，则必须通过为架构和 `MaximumConcurrentProvisioningOperations` 属性输入正确的语法来初始化该字符串。

6. 在 **PowerShell** 窗口中，从记事本粘贴修改后的自定义属性，并将变量分配给修改后的自定义属性。如果已初始化自定义属性，请在语法后添加以下行：

   ```
   $customProperties = '<CustomProperties xmlns="http://
   schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
   www.w3.org/2001/XMLSchema-instance"><Property xsi:type="IntProperty"
   Name="MaximumConcurrentProvisioningOperations" Value="100"/></
   CustomProperties>'
   ```

   此字符串将 `MaximumConcurrentProvisioningOperations` 属性设置为 100。在自定义属性字符串中，您必须将 `MaximumConcurrentProvisioningOperations` 属性设置为符合您需求的值。

7. 输入 `Get-XDAuthentication`，系统将提示您输入凭据。
8. 运行 `$cred = Get-Credential`，系统可能会提示您仅输入密码（或用户名和密码）。系统还可能提示您输入应用程序 ID 和关联的密钥。对于使用基于角色的身份验证的连接，**role_based_auth** 既是用户名也是密码。否则，请输入 AWS API ID 和密钥。
9. 运行 `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`。您必须将 *<connection-name>* 设置为连接的名称。
10. 输入 `dir` 以验证更新后的 CustomProperties 字符串。

配置每个网络接口的安全组

编辑主机连接时，您现在可以使用 PowerShell 命令配置每个弹性网络接口 (ENI) 允许的最大安全组数量。有关 AWS 安全组配额值的信息，请参阅 安全组。

要配置每个网络接口的安全组：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行 `cd xdhyp:\Connections\`。
4. 运行 `dir` 以列出连接。
5. 运行以下 PowerShell 命令以配置每个网络接口的安全组:

   ```
   Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws -Name
   "Citrix_MachineManagement_Options" -Value "
   AwsMaxENISecurityGroupLimit=<number>"
   ```

> **注意：**
>
> 如果您未设置 `AwsMaxENISecurityGroupLimit` 的值，则它将采用默认值 5。

服务终结点 URL

标准区域服务终端节点 URL

当您使用 MCS 时，将添加一个新的 Amazon WorkSpaces Core 托管实例连接，其中包含 API 密钥和 API 秘密。利用此信息以及经过身份验证的帐户，MCS 使用 AWS EC2 和 Amazon WorkSpaces Core 托管实例 API 调用查询 AWS 以获取支持的区域和可用区。查询是使用 Workspace Instances 服务终端节点 URL `<https://workspaces-instances.us-east-1.api.aws/>` 和 EC2 服务终端节点 https:/ec2.us-east-1.api.aws/ 进行的。

> **注意：**
>
> 确保 `<https://workspaces-instances.us-east-1.api.aws/>` 可联系。

所需的 AWS 权限

本节包含 AWS 权限的完整列表。使用本节中提供的完整权限集，以确保功能正常运行。

> **注意：**
>
> 仅当 Citrix 使用 IAM 角色管理资源时才需要 `iam:PassRole` 权限。

创建主机连接

使用从 AWS 获取的信息添加新的主机连接。

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [
```

```
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "workspaces-instances:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

VM 的电源管理

VM 已开机或关机。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",,
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances",
```

```
                "ec2:DescribeInstanceStatus"

            ],

            "Effect": "Allow",

            "Resource": "*"

        },

        {

           "Action": [

               "workspaces-instances:*"

           ],

           "Effect": "Allow",

            "Resource": "*"

       }


    ]


}
```

创建、更新或删除 VM

创建、更新或删除计算机目录，其中 VM 作为 AWS 实例进行预配。

```
{

    "Version": "2012-10-17",

    "Statement": [

        {
```

```
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
```

```
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
```

```
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
```

```
                "workspaces-instances:*"

            ],

            "Effect": "Allow",

            "Resource": "*"

        }


    ]

}
```

注意：

- 仅当在目录创建期间必须为准备 VM 创建隔离安全组时，才需要与 SecurityGroups 相关的 EC2 部分。完成此操作后，不再需要这些权限。

直接磁盘上传和下载

必须将以下权限添加到策略中：

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

EBS 加密已创建的卷

如果 AMI 已加密，或者 EBS 配置为加密所有新卷，则 EBS 可以自动加密新创建的卷。但是，要实现此功能，IAM 策略中必须包含以下权限。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:GenerateDataKey",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": "*"

        }

    ]

}
```

注意：

用户可以自行决定通过包含资源和条件块来将权限限制为特定密钥。例如，**带条件的 KMS 权限**：

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:GenerateDataKey",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"

            ],

            "Condition": {

                "Bool": {
```

```
                    "kms:GrantIsForAWSResource": true

                }

            }

        }

    ]

}
```

以下密钥策略语句是 KMS 密钥的整个默认密钥策略，它允许帐户使用 IAM 策略委托 KMS 密钥上的所有操作 (kms:*) 权限。

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",

"Resource": ""

}
```

有关详细信息，请参阅 AWS Key Management Service 官方文档。

基于 IAM 角色的身份验证

添加以下权限以支持基于角色的身份验证。

```
{

     "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
    ]
}
```

最小 IAM 权限策略

以下 JSON 可用于所有当前支持的功能。您可以使用此策略创建主机连接、创建、更新或删除 VM 以及执行电源管理。 该策略可以按照 定义 IAM 权限 部分中的说明应用于用户，或者您也可以在配置主机连接时通过选择**使用 IAM 角色**来使用基于角色的身份验证。

重要提示：

要使用**IAM 角色供 Citrix 管理资源**，请在设置 Delivery Controller 时，首先在 Delivery Controller ec2 实例上配置所需的 IAM 角色。使用 Citrix Studio，添加托管连接并选择“**使用 IAM 角色**”选项。具有这些设置的托管连接随后将使用基于角色的身份验证。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
```

```
                "ec2:AssociateIamInstanceProfile",

                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:RevokeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateNetworkInterface",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteLaunchTemplate",

                "ec2:DeleteNetworkInterface",

                "ec2:DeleteSecurityGroup",

                "ec2:DeleteSnapshot",

                "ec2:DeleteTags",

                "ec2:DeleteVolume",

                "ec2:DeregisterImage",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",
```

```
                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",

                "ec2:RebootInstances",

                "ec2:RunInstances",

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:TerminateInstances"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "workspaces-instances:*"
            ],
            "Resource": "*"
        }


    ]
}
```

注意：

- 仅当在目录创建期间必须为准备虚拟机创建隔离安全组时，才需要与安全组相关的 EC2 部分。完成此操作后，不再需要这些权限。
- 仅在使用 EBS 卷加密时才需要 KMS 部分。
- 仅当使用 Citrix 用于管理资源的 IAM 角色时，才需要 `iam:PassRole` 权限部分。
- 可以根据您的要求和环境添加特定的资源级权限，而不是完全访问权限。有关更多详细信息，请参阅 AWS 文档 揭秘 EC2 资源级权限 和 AWS 资源访问管理。
- 仅当您使用卷工作器方法时，才使用 `ec2:CreateNetworkInterface` 和 `ec2:DeleteNetworkInterface` 权限。

下一步操作

- 有关创建准备好的映像，请参阅 为 Amazon WorkSpaces Core 托管实例创建准备好的映像

更多信息

- 创建和管理连接及资源
- AWS 虚拟化环境

- 有关 Amazon WorkSpaces Core GitHub PowerShell 示例，请参阅 citrix-mcs-sdk-samples-Amazon WorkSpaces Core。

连接到 Azure Local

创建和管理连接和资源 介绍了创建连接的向导。以下信息涵盖了 Azure Local 环境特有的详细信息。

创建托管连接

您可以使用以下方式创建主机连接：

- Web 工作室
- (#use-powershell)

使用 WEB STUDIO

1. 在 Web 工作室中，打开 **托管 > 添加连接和资源**。
2. 在“**连接**”页面上，按照以下步骤配置连接：
   a. 选择“**创建新连接**”。
   b. 选择 **Microsoft® Azure™ Arc** 作为连接类型。
   c. 选择 Azure 环境。
   d. 选择一个区域。选项是您配置的所有资源位置。
   e. 选择**其他工具**以创建虚拟机。

   > **注意：**
   >
   > 选择**其他工具**仅创建托管连接，而不创建托管单元。

   f. 单击“**下一步**”。
3. 在**连接详细信息**页面上，按照向导中的指导输入连接详细信息。如果您使用现有 SPN，请确保该 SPN 已被授予订阅的参与者角色。有关详细信息，请查看所需的 Azure Local 权限。
4. 在**范围**页面上，为此连接选择一个或多个范围。
5. 在“**摘要**”页面上，检查配置，然后单击“**完成**”。

使用 POWERSHELL

脚本的标头
请确保提供脚本标头中定义的正确参数值。

```
$azureSubscription = "" # Azure Subscription ID


$azureTenantId = "" # Microsoft Entra Tenant ID


$appClientId = "" # Client ID of an Microsoft Entra application which is
grant with sufficient permissions


$appClientSecret = "" # Client secret of above client ID


$appClientSecretExpirationDateTimestamp = "" # Client secret expiration
date in epoch timestamp format


$region = "" # Azure region of your Azure Local cluster


$resourceGroupName = "" # Azure resource group of your Azure Local cluster


$zoneUid = "" # Zone UID of your resource location


$hostingConnectionName = "" # Name of the created hosting connection
```

创建托管连接

```
asnp citrix*


[SecureString]$appClientSecretSecureString = $appClientSecret | ConvertTo-
```

```
SecureString -AsPlainText -Force



$conn = New-Item -ConnectionType "Custom" -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"$azureSubscription`" /><Property xsi:type=`"StringProperty`"
Name=`"ManagementEndpoint`" Value=`"https://management.azure.com/`" /
><Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" /><Property
xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"$azureTenantId`" /
></CustomProperties>" -HypervisorAddress @("https://
management.azure.com/") -Path @("XDHyp:\Connections\
$hostingConnectionName") -Persist -PluginId "AzureArcFactory" -Scope @()
-SecurePassword $appClientSecretSecureString -UserName $appClientId
-ZoneUid $zoneUid



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$conn.HypervisorConnectionUid



Set-HypHypervisorConnectionMetadata -HypervisorConnectionUid
$conn.HypervisorConnectionUid -Name
Citrix_Orchestration_Hypervisor_Secret_Allow_Edit -Value true



Set-HypHypervisorConnectionMetadata -HypervisorConnectionUid
$conn.HypervisorConnectionUid -Name
Citrix_Orchestration_Hypervisor_Secret_Expiration_Date -Value
$appClientSecretExpirationDateTimestamp
```

创建托管单元

您可以使用以下方式创建托管单元：

- Web 工作室
- (#create-a-hosting-unit-using-powershell)

创建托管单元 使用 WEB STUDIO

1. 在 Web Studio 中，打开 **托管 > 添加连接和资源**。
2. 在 **Connection** 页面上：
   - 要创建新的托管连接以及托管单元，请选择 **创建新连接**，然后执行以下操作：
     a. 选择“**创建新连接**”。
     b. 选择 **Microsoft® Azure™ Arc** 作为连接类型。
     c. 选择 Azure 环境。
     d. 选择一个区域。选项是您配置的所有资源位置。
     e. 选择 **Citrix 预配工具（Machine Creation Services™ 或 Citrix Provisioning）**以创建虚拟机。
     f. 单击**下一步**。
   - 要从现有主机连接创建托管单元，请选择 **使用现有连接**，然后选择相关连接。
3. 在**连接详细信息**页面上，按照向导中的指导输入连接详细信息。如果您使用现有 SPN，请确保该 SPN 已被授予订阅的参与者角色。
4. 在**群集选择**页面上，浏览资源组并选择目标 Azure Local 群集。
5. 在**存储选择**页面上，为每种支持的数据类型至少选择一个存储设备，然后才能继续向导中的下一页。有关存储选择的更多信息，请参阅 主机存储。
6. 在 **网络** 页面上，输入资源的名称。此名称将显示在 Studio 中，用于标识与连接关联的存储和网络组合。选择虚拟机使用的一个或多个网络。
7. 在 **摘要** 页面上，检查详细信息，然后单击 **完成**。

使用 POWERSHELL 创建托管单元

脚本标题

确保提供脚本头中定义的正确参数值。

```
$resourceGroupName = "" # Azure resource group of your Azure Local cluster



$clusterName = "" # Name of your Azure Local cluster
```

```
$storagePathName = "" # Storage path in your Azure Local cluster that
wants to be used in this hosting unit



$logicalNetworkName = "" # Logical network in your Azure Local cluster
that wants to be used in this hosting unit



$zoneUid = "" # Zone UID of your resource location



$hostingConnectionName = "" # Name of the created hosting connection



$hostingUnitName = "" # Name of the created hosting unit
```

创建托管单元

```
asnp citrix*



$guid = (New-Guid).Guid



New-HypStorage -StoragePath @("XDHyp:\Connections\$hostingConnectionName\
$region.region\$resourceGroupName.resourcegroup\cluster.folder\
$clusterName.cluster\storage.folder\$storagePathName.storage")
-StorageType "TemporaryStorage" -JobGroup $guid



New-Item -Path XDHyp:\HostingUnits -Name $hostingUnitName
-HypervisorConnectionName $hostingConnectionName -RootPath "XDHyp:
\Connections\$hostingConnectionName\$region.region\
$resourceGroupName.resourcegroup\cluster.folder\$clusterName.cluster"
-NetworkPath "XDHyp:\Connections\$hostingConnectionName\$region.region\
$resourceGroupName.resourcegroup\cluster.folder\
```

```
$clusterName.cluster\network.folder\$logicalNetworkName.network"
-StoragePath "XDHyp:\Connections\$hostingConnectionName\$region.region\
$resourceGroupName.resourcegroup\cluster.folder\
$clusterName.cluster\storage.folder\$storagePathName.storage" -JobGroup
$guid
```

所需的 Azure Local 权限

参与者角色拥有管理所有资源的完全访问权限，并提供最佳的未来兼容性，尽管它包含的权限超出了当前功能集所需。本节详细介绍了 Azure Local 所需的最低权限。

最低权限

电源管理虚拟机

```
"Microsoft.Resources/tenants/read",



"Microsoft.Resources/subscriptions/read",



"Microsoft.Resources/subscriptions/locations/read",



"Microsoft.Resources/subscriptions/resourceGroups/read",



"Microsoft.AzureStackHCI/VirtualMachines/Read",



"Microsoft.AzureStackHCI/virtualMachineInstances/Read",



"Microsoft.AzureStackHCI/LogicalNetworks/Read",



"Microsoft.AzureStackHCI/StorageContainers/Read",
```

```
"Microsoft.AzureStackHCI/Clusters/Read",

"Microsoft.AzureStackHCI/VirtualMachineInstances/start/action",

"Microsoft.AzureStackHCI/VirtualMachineInstances/stop/action",

"Microsoft.AzureStackHCI/VirtualMachineInstances/restart/action"

"Microsoft.ExtendedLocation/CustomLocations/Read",

"Microsoft.KubernetesConfiguration/extensions/read",

"Microsoft.HybridCompute/machines/read"
```

创建、更新或删除虚拟机

```
"Microsoft.Resources/tenants/read",

"Microsoft.Resources/subscriptions/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",
```

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.HybridCompute/machines/read",

"Microsoft.HybridCompute/machines/write",

"Microsoft.HybridCompute/machines/delete",

"Microsoft.AzureStackHCI/Clusters/Read",

"Microsoft.AzureStackHCI/VirtualMachines/Read",

"Microsoft.AzureStackHCI/VirtualMachines/Write",

"Microsoft.AzureStackHCI/VirtualMachines/Delete",

"Microsoft.AzureStackHCI/virtualMachineInstances/Read",

"Microsoft.AzureStackHCI/virtualMachineInstances/Write",
```

```
"Microsoft.AzureStackHCI/virtualMachineInstances/Delete",

"Microsoft.AzureStackHCI/VirtualMachineInstances/start/action",

"Microsoft.AzureStackHCI/VirtualMachineInstances/stop/action",

"Microsoft.AzureStackHCI/VirtualMachineInstances/restart/action",

"Microsoft.AzureStackHCI/LogicalNetworks/Read",

"Microsoft.AzureStackHCI/LogicalNetworks/join/action",

"Microsoft.AzureStackHCI/StorageContainers/Read",

"Microsoft.AzureStackHCI/StorageContainers/deploy/action",

"Microsoft.AzureStackHCI/GalleryImages/Read",

"Microsoft.AzureStackHCI/GalleryImages/Write",

"Microsoft.AzureStackHCI/GalleryImages/Delete",
```

```
"Microsoft.AzureStackHCI/GalleryImages/deploy/action",

"Microsoft.AzureStackHCI/NetworkInterfaces/Read",

"Microsoft.AzureStackHCI/NetworkInterfaces/Write",

"Microsoft.AzureStackHCI/NetworkInterfaces/Delete",

"Microsoft.AzureStackHCI/networkInterfaces/join/action",

"Microsoft.AzureStackHCI/VirtualHardDisks/Read",

"Microsoft.AzureStackHCI/VirtualHardDisks/Write",

"Microsoft.AzureStackHCI/VirtualHardDisks/Delete",

"Microsoft.AzureStackHCI/VirtualHardDisks/upload/action",

"Microsoft.AzureStackHCI/VirtualHardDisks/join/action",

"Microsoft.AzureStackHCI/marketplaceGalleryImages/deploy/action",
```

```
"Microsoft.ExtendedLocation/CustomLocations/Read",

"Microsoft.ExtendedLocation/customLocations/deploy/action",

"Microsoft.KubernetesConfiguration/extensions/read",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",
```

```
"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action"
```

下一步操作

- 有关创建 Azure Local 计算机目录的信息，请参阅创建 Azure Local 计算机目录。

更多信息

- 连接和资源
- 创建计算机目录

连接到 XenServer®

创建和管理连接和资源 介绍了创建连接的向导。以下信息涵盖了 XenServer 虚拟化环境的特定详细信息。

> **注意：**
>
> 在创建到 XenServer 的连接之前，您需要首先将 XenServer 帐户设置为资源位置。请参阅 XenServer 虚拟化环境。

创建与 XenServer 的连接

创建到 XenServer（以前称为 Citrix Hypervisor™）的连接时，必须提供 VM Power Admin 或更高级别用户的凭据。

Citrix 建议使用 HTTPS 来保护与 XenServer 的通信。要使用 HTTPS，必须替换 XenServer 上安装的默认 SSL 证书。

如果 XenServer 服务器上启用了高可用性，则可以对其进行配置。对于 Citrix Virtual Apps and Desktops 2507 LTSR 及更高版本，如果您使用 HTTPS 并希望配置高可用性服务器，则可以为池中的所有服务器安装通配符证书。但是，对于 2507 LTSR 之前的版本，每个服务器都需要单独的证书。

如果 XenServer 支持 vGPU，则可以选择 GPU 类型和组，或直通。显示屏会指示所选内容是否具有专用 GPU 资源。

当在一个或多个 XenServer 主机上使用本地存储进行临时数据存储时，请确保池中的每个存储位置都具有唯一的名称。（要在 XenCenter® 中更改名称，请右键单击存储并编辑名称属性。）

您可以使用 Citrix Provisioning（以前称为 Provisioning Services）和 Machine Creation Services™ (MCS) 来预配：

- 支持的桌面或服务器操作系统 VM 的传统 BIOS。
- 支持的桌面或服务器操作系统 VM 的 UEFI，包括安全启动。

> **注意：**
>
> 配置 MCS 时需要池操作员权限或更高级别的权限。

将 INTELLICACHE™ 用于 XENSERVER 连接

使用 IntelliCache，托管 VDI 部署更具成本效益，因为您可以结合使用共享存储和本地存储。这可以提高性能并减少网络流量。本地存储会缓存共享存储中的主映像，从而减少对共享存储的读取次数。对于共享桌面，对差异磁盘的写入会写入到主机上的本地存储，而不是共享存储。

- 使用 IntelliCache 时，共享存储必须是 NFS。
- Citrix 建议您使用高性能本地存储设备，以确保最快的数据传输速度。

要使用 IntelliCache，必须在此产品和 XenServer 中都启用它。

- 安装 XenServer 时，选择 **Enable thin provisioning (Optimized storage for Virtual Desktops)**。Citrix 不支持混合池，即同时包含启用 IntelliCache 的服务器和未启用 IntelliCache 的服务器的池。有关详细信息，请参阅 XenServer 文档。
- 在 Citrix Virtual Apps and Desktops™ 中，IntelliCache 默认处于禁用状态。您只能在创建 XenServer 连接时更改此设置；之后无法禁用 IntelliCache。添加 XenServer 连接时：
  - 选择**共享**作为存储类型。
  - 选择**使用 IntelliCache** 复选框。

所需的 XenServer 权限

XenServer 权限是基于角色的 (RBAC)。XenServer 中的基于角色的访问控制 (RBAC) 功能允许您分配用户、角色和权限，以控制谁可以访问您的 XenServer 以及他们可以执行哪些操作。XenServer RBAC 系统将用户（或用户组）映射到定义的角色（一组命名的权限）。这些角色具有关联的 XenServer 权限以执行特定操作。

有关详细信息，请参阅 基于角色的访问控制。

角色层次结构（按权限递增顺序）为：只读 → VM 操作员 → VM 管理员 → VM 电源管理员 → 池操作员 → 池管理员。

以下部分总结了每个预配任务所需的最低角色。

创建主机连接

任务	所需的最低角色
使用从 XenServer 获取的信息添加主机连接	只读
查看用户及其分配的角色	只读

虚拟机电源管理

任务	所需的最低角色
启动或关闭虚拟机	虚拟机操作员

创建、更新或删除虚拟机

任务	所需的最低角色
将虚拟机添加到现有快照计划或从中删除虚拟机	虚拟机电源管理员
添加、修改、删除快照计划	池操作员
发布主映像	池操作员（需要交换机端口锁定）
创建计算机目录	池操作员：需要交换机端口锁定
添加或删除 VM（非 GPU 启用的 VM）	VM 管理员
添加或删除 VM（GPU 启用的 VM）	池操作员
添加、删除或配置虚拟磁盘或 CD 设备	VM 管理员
管理标签	VM 操作员

有关 RBAC 角色和权限的更多信息，请参阅 RBAC 角色和权限。

有关交换机端口锁定的信息，请参阅 使用交换机端口锁定。

后续步骤

- 如果您处于初始部署过程中，请参阅创建计算机目录
- 有关 XenServer 的特定信息，请参阅创建 XenServer 目录

更多信息

- 连接和资源
- 创建计算机目录

连接到 Google 云环境

(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections.html) 介绍了创建连接的向导。以下信息涵盖了 Google 云环境特有的详细信息。

> **注意：**
>
> 在创建与 Google 云环境的连接之前，您需要先将 Google 云帐户设置为资源位置。请参阅 Google Cloud 环境。

添加连接

请遵循 创建连接和资源 中的指导。以下说明将指导您设置托管连接：

1. 在左侧窗格中，从 **管理 > 配置** 中选择 **托管**。
2. 在操作栏中选择 **Add Connection and Resources**。
3. 在 **Connection** 页面上，选择 **Create a new Connection** 和 **Citrix provisioning™ tools**，然后选择 **Next**。
   - **连接类型**。从菜单中选择 **Google Cloud**。
   - **连接名称**。键入连接的名称。
4. 在**区域**页面上，从菜单中选择一个项目名称，选择包含要使用的资源的区域，然后选择**下一步**。
5. 在**网络**页面上，键入资源的名称，从菜单中选择一个虚拟网络，选择一个子集，然后选择**下一步**。资源名称有助于识别区域和网络组合。名称后附加 *(Shared)* 后缀的虚拟网络表示共享 VPC。如果您为共享 VPC 配置了子网级 IAM 角色，则共享 VPC 的特定子网才会显示在子网列表中。

   > **注意：**

- 资源名称可以包含 1–64 个字符，并且不能只包含空格或字符 `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`。

6. 在**摘要**页面上，确认信息，然后选择**完成**以退出**添加连接和资源**窗口。

创建连接和资源后，您创建的连接和资源将列出。要配置连接，请选择该连接，然后在操作栏中选择适用的选项。

同样，您可以删除、重命名或测试在连接下创建的资源。为此，请选择连接下的资源，然后在操作栏中选择适用的选项。

服务端点 URL

您必须有权访问以下 URL：

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Google Cloud 项目

Google Cloud 项目主要有两种类型：

- 预配项目：在这种情况下，当前管理员帐户拥有项目中预配的计算机。此项目也称为本地项目。
- 共享 VPC 项目：预配项目中创建的计算机使用共享 VPC 项目中的 VPC 的项目。用于预配项目的管理员帐户在此项目中具有有限的权限，具体来说，只有使用 VPC 的权限。

为 GCP 托管流量创建安全环境

您可以允许私有 Google 访问您的 Google Cloud 项目。此实施可增强安全性以处理敏感数据。为此，您可以执行以下操作之一：

- 为 Cloud Build Service Account 包含 VPC 服务控制的以下入站规则。如果执行此步骤，则无需遵循以下步骤为 GCP 托管流量创建安全环境。

```
Ingress Rule 1

From:
```

```
Identities:

<ProjectID>@cloudbuild.gserviceaccount.com

Source > All sources allowed

To:

Projects =

All projects

Services =

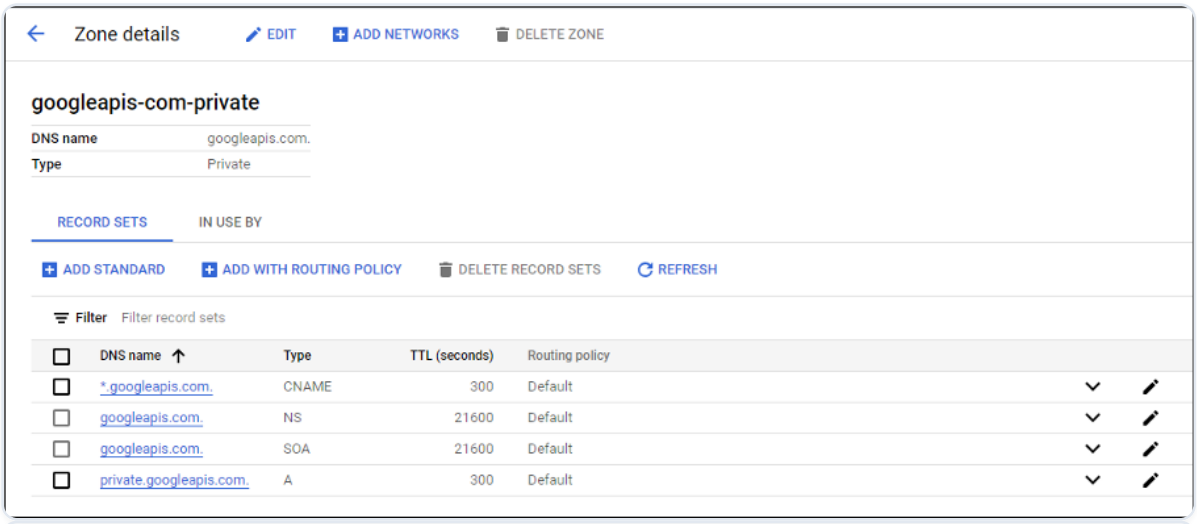
Service name: All services
```

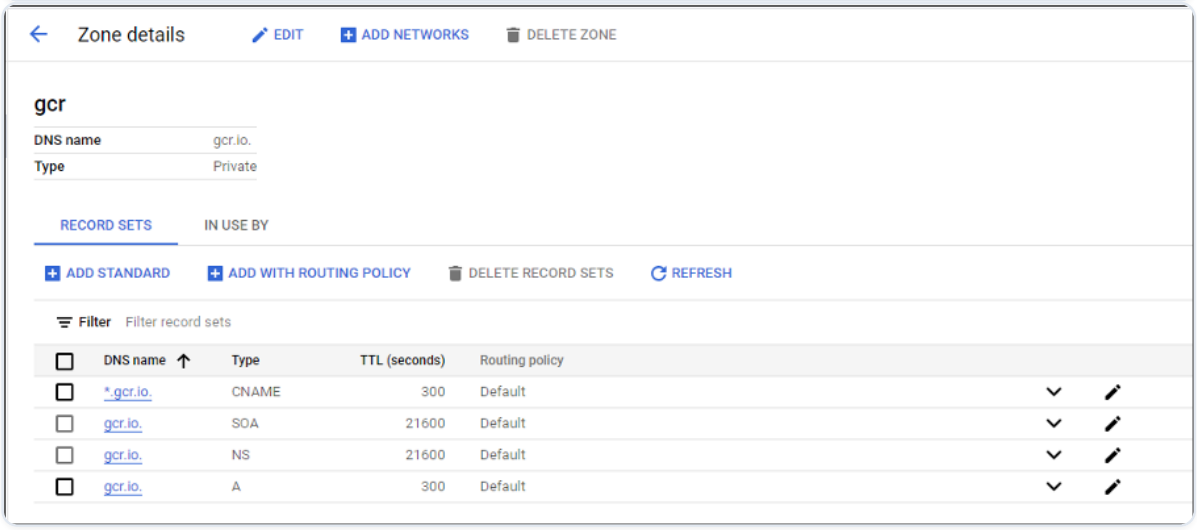
- 如果您正在使用私有工作池，请在 `CustomProperties` 中添加 `UsePrivateWorkerPool`。有关私有工作池的信息，请参阅 私有池概述。

为 GCP 托管流量创建安全环境的要求

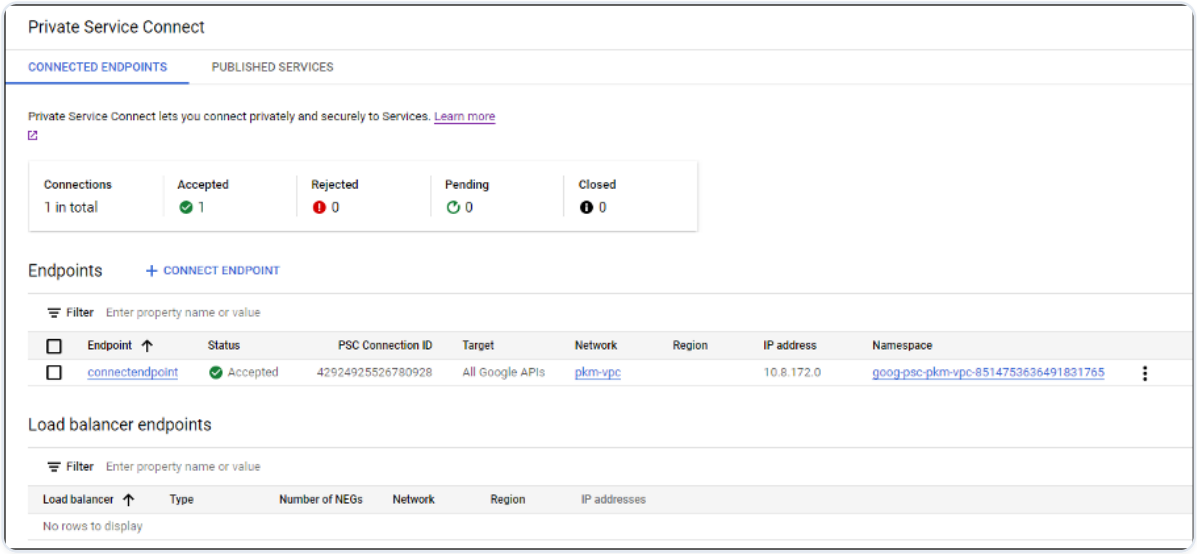
为 GCP 托管流量创建安全环境的要求如下：

- 更新自定义属性时，请确保托管连接处于维护模式。
- 要使用私有工作池，需要进行以下更改：
  - 对于 Citrix Cloud™ 服务帐户，添加以下 IAM 角色：
    - Cloud Build 服务帐户
    - 计算实例管理员
    - 服务帐号用户
    - 服务帐号令牌创建者
    - Cloud Build WorkerPool 所有者
  - 在用于创建托管连接的同一项目中创建 Citrix Cloud 服务帐户。
  - 为 `private.googleapis.com` 和 `gcr.io` 设置 DNS 区域，如 DNS 配置 中所述。

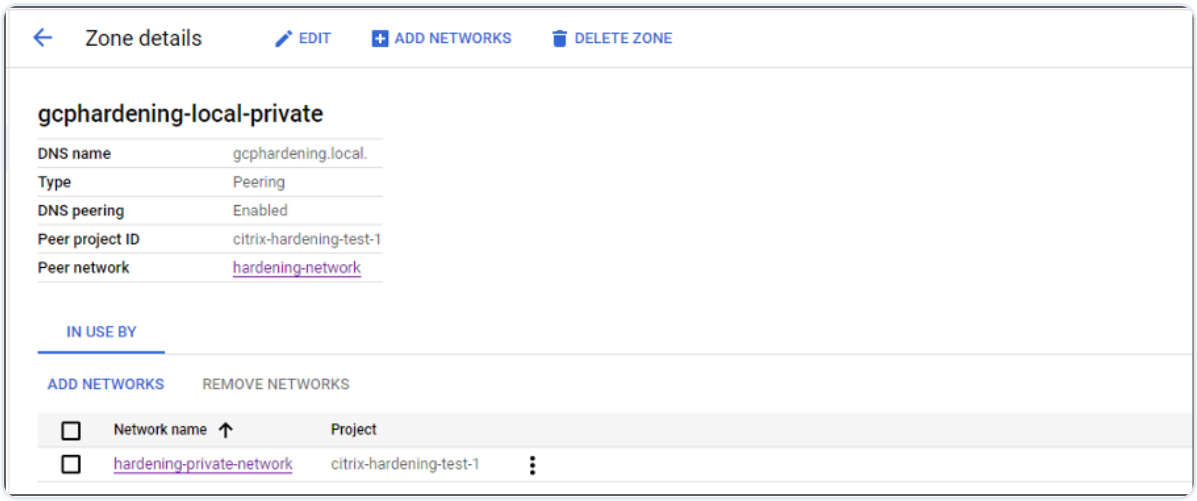




- 设置专用网络地址转换 (NAT) 或使用专用服务连接。有关详细信息，请参阅 通过端点访问 Google API。



- 如果使用对等 VPC，请创建到对等 VPC 的 Cloud DNS 区域对等互连。有关详细信息，请参阅 创建对等区域。



- 在 VPC 服务控制中，设置出站规则，以便 API 和 VM 可以与 Internet 通信。入站规则是可选的。例如：

```
Egress Rule 1

From:

Identities:ANY_IDENTITY

To:

Projects =

All projects

Service =

Service name: All services
```

启用私有工作池

要启用私有工作池，请在主机连接上按如下方式设置自定义属性：

1. 从 Delivery Controller 主机打开 PowerShell 窗口或使用远程 PowerShell SDK。有关远程 PowerShell SDK 的详细信息，请参阅 SDK 和 API。
2. 运行以下命令：
   a. `Add-PSSnapin citrix®*`
   b. `cd XDHyp:\Connections\`
   c. `dir`

3. 将连接中的 `CustomProperties` 复制到记事本。
4. 追加属性设置 `<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>`。例如：

   ```
   ```

   <CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

   <Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
   Value="True"/>

   </CustomProperties>

   ```
   ```

5. 在 PowerShell 窗口中，为修改后的自定义属性分配一个变量。例如：`$customProperty = '<CustomProperties…</CustomProperties>'`。
6. 运行 `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`。
7. 运行 `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`。
8. 运行 `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`。
9. 运行以下命令以更新现有主机连接：

   ```
   Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR CONNECTION
   NAME HERE>') -SecurePassword $securePassword -UserName
   $gcpServiceAccount -CustomProperties $customProperty
   ```

指定 CMEK 全局和区域密钥

> **注意：**

> GCP 中对 CMEK 的支持目前处于预览阶段。

> GCP 中有两种类型的客户管理的加密密钥 (CMEK)：

- 区域：只能由同一区域中的资源使用的加密密钥。
- 全局：可由来自多个区域的资源使用的加密密钥。

您可以浏览和使用服务帐户可访问的所有项目中的全局或区域客户管理的加密密钥 (CMEK)。然后，您可以使用该密钥创建启用 CMEK 的 MCS 计算机目录，并使用 `Set-ProvScheme` 命令更新现有的启用 CMEK 的 MCS 计算机目录。有关使用 PowerShell 创建启用 CMEK 的目录的信息，请参阅使用自定义属性创建启用 CMEK 的目录。

对于此功能，您需要为以下两个服务帐户提供额外的权限：

- 当前项目的服务帐户，用于创建托管连接。
- 当前项目的 Compute Engine 服务代理（其电子邮件为：`service-PROJECT_NUMBER@compute-system.iam.gserviceaccount.com`）。有关详细信息，请参阅 Compute Engine 服务代理。

在服务帐户中，您必须在包含要使用的加密密钥的项目中分配以下角色（例如，共享项目）：

- Cloud KMS 查看者
- 云 KMS 加密密钥 加密器/解密器

如果您未分配到这些角色，请确保您拥有以下权限：

- resourcemanager.projects.get
- cloudkms.keyRings.list
- cloudkms.keyRings.get
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

列出加密密钥

您可以使用 PowerShell 命令列出同一项目和所有其他可访问项目中的全局和区域加密密钥。为此，请执行以下操作：

1. 从 Delivery Controller™ 主机或远程 PowerShell 打开 PowerShell 窗口。
2. 运行命令 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行以下命令以列出加密密钥。示例：
    - 要列出 `encryptionKeys` 文件夹的内容：

```
Get-ChildItem XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder
```

- 要在同一项目中获取全局加密密钥：

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\myglobalkeyring.globalkeyring\mygl
obalkey.cryptokey
```

- 要在同一项目中获取区域加密密钥：

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\regional-ring.keyring\shared-
key.cryptokey
```

- 要从另一个可访问的项目（例如：myanotherproject）获取全局加密密钥：

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\myanotherproject.project\shared-
global-ring.globalkeyring\shared-key.cryptokey
```

- 要从另一个可访问的项目（例如：myanotherproject）获取区域加密密钥：

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\myanotherproject .project.project\
shared-uscentral.keyring\shared-uscentral-key.cryptokey
```

注意：

- 全局密钥环的密钥环清单项的扩展名为 `.globalkeyring`。
- 全局密钥环的 ID 中包含单词 `global`。

所需的 GCP 权限

本节包含 GCP 权限的完整列表。请使用本节中提供的完整权限集，以确保功能正常运行。

> **注意：**
>
> GCP 将在 April 29, 2024 之后对 Cloud Build Services 的默认行为和服务账户的使用引入更改。有关详细信息，请参阅 Cloud Build Service Account Change。您在 April 29, 2024 之前启用了 Cloud Build API 的现有 Google 项目不受此更改影响。但是，如果您希望在 April 29 之后仍保留现有的 Cloud Build Service 行为，则可以在启用 API 之前创建或应用组织策略以禁用约束强制执行。如果您设置了新的组织策略，则仍可以遵循本节中现有的权限以及标记为 **Before Cloud Build Service Account Change** 的项目。否则，请遵循标记为 **After Cloud Build Service Account Change** 的现有权限和项目。

创建主机连接

- 预配项目中 Citrix Cloud 服务账户所需的最低权限：

  ```
  compute.instanceTemplates.list

  compute.instances.list

  compute.networks.list

  compute.projects.get

  compute.regions.list

  compute.subnetworks.list

  compute.zones.list

  resourcemanager.projects.get
  ```

  以下 Google 定义的角色具有上述权限：

  - 计算管理员
  - 云数据存储用户

- Citrix Cloud 服务帐户在共享 VPC 项目中共享 VPC 所需的额外权限：

  ```
  compute.networks.list

  compute.subnetworks.list
  ```

```
resourcemanager.projects.get
```

以下 Google 定义的角色具有上述权限：

- 计算网络用户

- 在服务帐户中，您必须在包含要使用的加密密钥的项目（例如，共享项目）中分配以下角色：
  - Cloud KMS 查看者
  - 云密钥管理服务加密密钥加密器/解密器

  如果您未分配到这些角色，请确保您具有以下权限：
  - resourcemanager.projects.get
  - cloudkms.keyRings.list
  - cloudkms.keyRings.get
  - cloudkms.cryptoKeys.get
  - cloudkms.cryptoKeys.list
  - cloudkms.cryptoKeyVersions.useToDecrypt
  - cloudkms.cryptoKeyVersions.useToEncrypt

虚拟机的电源管理

在仅电源管理的目录中，Citrix Cloud 服务帐户在预配项目中所需的最低权限：

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop

compute.instances.suspend
```

```
compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

以下 Google 定义的角色具有上述权限：

- Compute 管理员
- 云数据存储用户

创建、更新或删除虚拟机

- Citrix Cloud 服务帐户在预配项目中所需的最低权限：

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get
```

```
compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete
```

```
compute.instances.detachDisk

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list
```

```
compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete
```

```
storage.objects.get

storage.objects.list

compute.networks.get

compute.resourcePolicies.use
```

以下 Google 定义的角色具有上述权限：

- Compute 管理员
- Storage 管理员
- Cloud Build 编辑者
- 服务帐户用户
- 云数据存储用户

- Citrix Cloud 服务帐户在共享 VPC 项目中创建托管单元时，使用共享 VPC 项目中的 VPC 和子网所需的共享 VPC 附加权限：

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

以下 Google 定义的角色具有上述权限：

- 计算网络用户
- 云数据存储用户

将准备说明磁盘下载到 MCS 时所需的最低权限：

- (在 Cloud Build 服务帐户更改之前)：将这些权限分配给预配项目中的 Cloud Build 服务帐户。
- (在 Cloud Build 服务帐户更改之后)：将这些权限分配给预配项目中的 Cloud Compute 服务帐户。

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels
```

```
compute.instances.setMetadata

compute.instances.setServiceAccount

compute.machineTypes.list

compute.networks.get

compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete
```

```
storage.objects.get

storage.objects.list
```

以下 Google 定义的角色具有上述权限：

- Cloud Build 服务帐户（在 Cloud Build 服务帐户更改后，它是 Cloud Compute 服务帐户）
- 计算实例管理员
- 服务帐户用户

- 将准备说明磁盘下载到 MCS 时，Google Cloud Build 服务在预配项目中为 Cloud Compute 服务帐户所需的最低权限：

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get

storage.objects.list
```

以下 Google 定义的角色具有上述权限：

- 计算网络用户
- 存储账户用户
- 云数据存储用户

将准备说明磁盘下载到 MCS 时，共享 VPC 所需的额外权限：

- (在 Cloud Build 服务帐户更改之前)：将这些权限分配给预配项目中的 Cloud Build 服务帐户。
- (在 Cloud Build 服务帐户更改之后)：将这些权限分配给预配项目中的 Cloud Compute 服务帐户。

```
compute.firewalls.list

compute.networks.list

compute.subnetworks.list
```

```
compute.subnetworks.use

resourcemanager.projects.get
```

以下 Google 定义的角色具有上述权限：

- 计算网络用户
- 存储账户用户
- 云数据存储用户

- 预配项目中 Citrix Cloud 服务帐户的 Cloud Key Management Service (KMS) 所需的额外权限：

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

以下 Google 定义的角色具有上述权限：

- 计算 KMS 查看者

一般权限

以下是预配项目中 Citrix Cloud 服务帐户在 MCS 中支持的所有功能的权限。这些权限可提供最佳的未来兼容性：

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list
```

```
compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly
```

```
compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig

compute.instances.updateShieldedVmConfig
```

```
compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list
```

```
resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs

compute.resourcePolicies.use

cloudkms.cryptoKeyVersions.useToDecrypt
```

```
cloudkms.cryptoKeyVersions.useToEncrypt
```

下一步

- 如果您处于初始部署过程中，请参阅创建计算机目录
- 有关 Google Cloud Platform (GCP) 的特定信息，请参阅 创建 Google Cloud Platform 目录

更多信息

- 连接和资源
- 创建计算机目录

连接到 HPE Moonshot

(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections.html)介绍了创建连接的向导。以下信息涵盖了 HPE Moonshot 的具体细节。

> **注意：**
>
> 在创建到 HPE Moonshot 的连接之前，您需要先完成 HPE 帐户的设置。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-prepare/hpe-moonshot.html)。

创建连接

您可以使用以下方式创建到 HPE Moonshot 的连接：

- 网页工作室
- PowerShell 命令

使用 WEB STUDIO 创建连接

1. 在“**添加连接和资源**”页面上，选择“**HPE Moonshot**”作为连接类型。
2. 输入 Moonshot iLO 机箱管理器的连接地址。您可以将 IP 地址、主机名或 FQDN 用作地址。
3. 输入您的机箱管理凭据和易记的连接名称。

出现以下任一情况时，连接设置将停止：

- Citrix Virtual Apps and Desktops™ 收到带有错误的公共 CA 签名证书：将显示错误消息。按照屏幕上的说明修复问题。否则，您无法继续创建连接。

- Citrix Virtual Apps and Desktops™ 收到私有 CA 签名证书。将显示警告页面。将收到的指纹与服务器的指纹进行比较，以验证证书的有效性。如果有效，请选择“**信任证书**”，然后单击“**确定**”以继续创建连接。Citrix Virtual Apps and Desktops 将信任该证书并存储指纹以供将来验证。

使用 POWERSHELL 命令创建连接

使用 PowerShell 命令创建连接时，请提供以下信息：

- IP：HPE 服务器 IP 地址
- 用户名：HPE 用户名
- 密码：HPE 密码

例如：

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} -Path
@("XDHyp:\Connections\$connectionName") -Persist -PluginId
"HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
$UserName -sslthumbprint $SslThumbprint New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $HypervisorConnectionID
```

注意：

`sslthumbprint` 参数仅适用于私有 CA 签名证书。

证书和指纹验证

为了成功连接到 **HPE Moonshot**，证书不得有错误，并且指纹必须具有正确的值。以下是与证书和指纹验证相关的用例：

- 公共 CA 签名的证书存在错误。连接未成功创建。请查看错误详细信息并解决问题。
- 公共 CA 签名的证书无错误。连接成功创建，并且 `SslThumbprints` 值为 **Null**。
- 私有 CA 签名的证书无错误且具有 `sslthumbprint` 值。连接成功创建，并具有正确的 `SslThumbprints` 值。
- 私有 CA 签名的证书指纹值不正确。连接未成功创建。
- 私有 CA 签名的证书无错误。连接成功创建。创建连接时，`SSlThumbprints` 为 **Null**。`SSlThumbprints` 值由站点服务更新为某个值。

> **注意：**
>
> Citrix 数据库与 Moonshot 服务器之间证书指纹不匹配会在 Web Studio 中触发警告。但是，此警告不会出现在基于 MMC 的 Studio 中。

管理连接

本节详细介绍了如何管理连接：

- 使用 Web Studio 修复证书问题
- 使用 PowerShell 命令更新指纹值

修复证书问题

当出现证书问题时，Citrix Virtual Apps and Desktops 会阻止 HPE Moonshot 连接，从而阻止您在关联的 HPE Moonshot 节点上交付和管理工作负载。您将在“**主机连接**”列表中看到连接旁边有一个错误图标。有关具体问题和解决方案，请参阅下表。

问题	解决方案
公共 CA 签名的证书出现错误	单击连接并选择“**故障排除**”选项卡。查看错误详细信息并解决问题。
收到的证书是私有 CA 签名的或已过期。	编辑主机连接以更新证书指纹。详细步骤： 1. 选择连接，然后单击 **编辑连接**。 2. 在 **连接属性** 页面上，单击 **编辑设置**。 3. 输入连接到 HPE Moonshot 机箱的密码，然后单击“**保存**”。 4. 在出现的 **警告** 页面上，将收到的指纹与服务器的指纹进行比较，以验证证书的有效性。

问题	解决方案	
	5. 如果它们相同，请选择**信任证书**，然后单击**确定**。	

更新指纹值

创建连接后，可以使用 `Set-Item` PowerShell 命令更新连接的指纹值。例如，运行以下命令：

1. 获取连接的连接详细信息。例如：

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. 更新指纹值。例如：

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. 检查更新后的指纹值。例如：

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

注意：

如果您在 `Set-Item` 命令中提供了不正确的指纹值，则更新将失败。

下一步操作

- 如果您处于初始部署过程中，请参阅创建计算机目录
- 有关 AWS 特定信息，请参阅 创建 HPE Moonshot 计算机目录

更多信息

- 连接和资源
- 创建计算机目录

连接到 Microsoft Azure

创建和管理连接和资源 介绍了创建连接的向导。以下信息涵盖了 Azure Resource Manager 云环境特有的详细信息。

> **注意：**
>
> 在创建到 Microsoft Azure 的连接之前，您必须完成将 Azure 帐户设置为资源位置的设置。请参阅 Microsoft Azure Resource Manager 云环境。

创建服务主体和连接

在创建连接之前，必须设置连接用于访问 Azure 资源的服务主体。可以通过两种方式创建连接：

- 使用 Web Studio 同时创建服务主体和连接
- 使用以前创建的服务主体创建连接

本节介绍如何完成以下任务：

- 使用 Web Studio 创建服务主体和连接
- 使用 PowerShell 创建服务主体
- 在 Azure 中获取应用程序机密
- 使用现有服务主体创建连接

注意事项

- Citrix® 建议使用具有贡献者角色的服务主体。但是，请参阅 最低权限 部分以获取最低权限列表。
- 首次创建连接时，Azure 会提示您授予其必要的权限。对于将来的连接，您仍然需要进行身份验证，但 Azure 会记住您之前的同意，并且不会再次显示提示。
- 用于身份验证的帐户必须具有使用 Azure RBAC 在订阅中分配角色的权限。例如，订阅的 Owner、Role Based Access Control Administrator 或 User Access Administrator。
- 用于身份验证的帐户必须是订阅目录的成员。需要注意两种类型的帐户：“工作或学校”帐户和“个人 Microsoft 帐户”。有关详细信息，请参阅 CTX219211。
- 尽管您可以通过将现有 Microsoft 帐户添加为订阅目录的成员来使用它，但如果用户之前被授予对目录某个资源的来宾访问权限，则可能会出现并发症。在这种情况下，他们可能在目录中有一个占位符条目，该条目未授予他们必要的权限，并且会返回错误。

通过从目录中删除资源并将其显式添加回来来纠正此问题。但是，请谨慎使用此选项，因为它会对帐户可以访问的其他资源产生意外影响。

- 存在一个已知问题，即某些帐户在实际是成员时被检测为目录访客。此类配置通常发生在较旧的已建立的目录帐户中。解决方法：向目录添加一个帐户，该帐户将采用正确的成员身份值。
- 资源组只是资源的容器，它们可以包含来自其自身区域以外区域的资源。如果您期望资源组区域中显示的资源可用，这可能会造成混淆。
- 确保您的网络和子网足够大，可以容纳您所需的计算机数量。这需要一些远见，但 Microsoft 会帮助您指定正确的值，并提供有关地址空间容量的指导。

使用 WEB STUDIO 创建服务主体和连接

> **重要提示：**
>
> 此功能尚不适用于 Azure 中国订阅。
>
> 借助 Web Studio，您可以在单个工作流中同时创建服务主体和连接。服务主体授予连接访问 Azure 资源的权限。当您向 Azure 进行身份验证以创建服务主体时，会在 Azure 中注册一个应用程序。为注册的应用程序创建一个密钥（称为客户端密钥或应用程序密钥）。注册的应用程序（在本例中为连接）使用客户端密钥向 Microsoft Entra ID 进行身份验证。

在开始之前，请确保您已满足以下先决条件：

- 您在订阅的 Microsoft Entra 租户中拥有一个用户帐户。
- 用于身份验证的帐户必须具有使用 Azure RBAC 在订阅中分配角色的权限。例如，订阅的 Owner、Role Based Access Control Administrator 或 User Access Administrator。
- 您拥有用于身份验证的全局管理员、应用程序管理员或应用程序开发人员权限。创建主机连接后，可以撤销这些权限。有关角色的更多信息，请参阅 Microsoft Entra 内置角色。

使用“**添加连接和资源**”向导一起创建服务主体和连接：

1. 在“**连接**”页面上，选择“**创建新连接**”、“**Microsoft Azure**”连接类型和您的 Azure 环境。
2. 选择用于创建虚拟机的工具，然后选择“**下一步**”。
3. 在“**连接详细信息**”页面上，输入您的 Azure 订阅 ID 和连接名称。输入订阅 ID 后，“**新建**”按钮将启用。

> **注意：**

> 连接名称可以包含 1–64 个字符，并且不能只包含空格或字符 `\/;:#.*?=<>|[]{}"'()'`。

4. 选择“**创建新项**”，然后输入 Microsoft Entra 帐户用户名和密码。
5. 选择“**登录**”。
6. 选择“**接受**”以授予 Citrix Virtual Apps and Desktops™ 列出的权限。Citrix Virtual Apps and Desktops 会创建一个服务主体，允许它代表指定用户管理 Azure 资源。
7. 选择“**接受**”后，您将返回向导中的“**连接**”页面。

> **注意：**
>
> 成功通过 Azure 身份验证后，**创建新连接**和**使用现有连接**按钮将消失。**连接成功**文本将显示，并带有一个绿色复选标记，表示已成功连接到您的 Azure 订阅。

8. 在**连接详细信息**页面上，选择**下一步**。

> **注意：**
>
> 在成功向 Azure 进行身份验证并同意授予所需权限之前，您无法继续访问下一页。

9. 配置连接的资源。资源包括区域和网络。
   - 在**区域**页面上，选择一个区域。
   - 在**网络**页面上，执行以下操作：
     - 键入 1–64 个字符的资源名称，以帮助识别区域和网络组合。资源名称不能只包含空格，也不能包含字符 `\/;:#.*?=<>|[]{}"'()'`。
     - 选择一个虚拟网络/资源组对。（如果存在多个同名虚拟网络，将网络名称与资源组配对可提供唯一组合。）如果您在上一页选择的区域没有任何虚拟网络，请返回该页面并选择一个具有虚拟网络的区域。
10. 在**摘要**页面上，查看设置摘要，然后选择**完成**以完成设置。

查看应用程序 ID

创建连接后，您可以查看该连接用于访问 Azure 资源的应用程序 ID。

在**添加连接和资源**列表中，选择连接以查看详细信息。**详细信息**选项卡显示应用程序 ID。

使用 POWERSHELL 创建服务主体

要使用 PowerShell 创建服务主体，请连接到您的 Azure Resource Manager 订阅，并使用以下部分中提供的 PowerShell cmdlet。

请确保您已准备好以下各项：

- **SubscriptionId：** Azure Resource Manager `SubscriptionID` 用于要预配 VDA 的订阅。
- **ActiveDirectoryID：** 您已在 Microsoft Entra ID 中注册的应用程序的租户 ID。
- **ApplicationName：** 将在 Microsoft Entra ID 中创建的应用程序的名称。

详细步骤如下：

连接到您的 Azure Resource Manager 订阅。

```
`Connect-AzAccount`
```

1. 选择要在其中创建服务主体的 Azure Resource Manager 订阅。

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
   ```

2. 在您的 AD 租户中创建应用程序。

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. 创建服务主体。

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. 为服务主体分配角色。

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
   $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. 从 PowerShell 控制台的输出窗口中，记下 ApplicationId。在创建主机连接时提供该 ID。

在 AZURE 中获取应用程序机密

要使用现有服务主体创建连接，必须首先在 Azure 门户中获取服务主体的应用程序 ID 和密钥。

详细步骤如下：

1. 从 Web Studio 或使用 PowerShell 获取**应用程序 ID**。
2. 登录 Azure 门户。

3. 在 Azure 中，选择 **Microsoft Entra ID**。
4. 在 Microsoft Entra ID 的 **应用注册** 中，选择您的应用程序。
5. 转到 **证书和机密**。
6. 单击 **客户端机密**。

使用现有服务主体创建连接

如果您已有服务主体，则可以使用它通过 Web Studio 创建连接。

确保您已准备好以下各项：

- SubscriptionId
- ActiveDirectoryID (租户 ID)
- 应用程序 ID
- 应用程序密钥

  有关详细信息，请参阅 获取应用程序机密。
- 密钥过期日期

详细步骤如下：

在 **添加连接和资源** 向导中：

1. 在“**连接**”页面上，选择“**创建新连接**”、“**Microsoft Azure**”连接类型和您的 Azure 环境。
2. 选择用于创建虚拟机的工具，然后选择“**下一步**”。
3. 在**连接详细信息**页面上，输入您的 Azure 订阅 ID 和连接名称。

   > **注意：**
   >
   > 连接名称可以包含 1–64 个字符，不能只包含空格，也不能包含字符 `\/;:#.*?=<>|[]{}"'()'`。

4. 选择 **使用现有**。在 **现有服务主体详细信息** 窗口中，输入现有服务主体的以下设置。输入详细信息后，**保存** 按钮将启用。选择 **保存**。在提供有效详细信息之前，您无法继续此页面。

   - **订阅 ID**。输入您的 Azure 订阅 ID。要获取您的订阅 ID，请登录 Azure 门户并导航到 **订阅 > 概述**。

- **Active Directory ID**（租户 ID）。输入您在 Azure AD 中注册的应用程序的目录（租户）ID。
- **应用程序 ID**。输入您在 Azure AD 中注册的应用程序的应用程序（客户端）ID。
- **应用程序密钥**。创建密钥（客户端密钥）。注册的应用程序使用该密钥向 Azure AD 进行身份验证。我们建议您定期更改密钥以确保安全。请务必保存密钥，因为以后无法检索该密钥。
- **密钥过期日期**。输入应用程序密钥的过期日期。在密钥过期前 14 天，您将在**托管**节点中的特定主机连接上看到警告图标。但是，如果密钥过期，您将收到错误。

> **注意：**
>
> 出于安全考虑，过期期限不能超过两年。

- **身份验证 URL**。此字段自动填充且不可编辑。
- **管理 URL**。此字段自动填充且不可编辑。
- **存储后缀**。此字段自动填充且不可编辑。
- **用于上传或下载磁盘或快照的 Azure Blob 存储终结点**。此字段自动填充且不可编辑。
- **Key Vault 服务**。此字段自动填充且不可编辑。
- **服务总线后缀**。此字段自动填充且不可编辑。

  在 Azure 中创建 MCS 目录需要访问以下终结点。访问这些终结点可优化您的网络与 Azure 门户及其服务之间的连接。

  - 身份验证 URL: `https://login.microsoftonline.com`
  - 管理 URL: `https://management.azure.com`。这是 Azure Resource Manager 提供程序 API 的请求 URL。管理终结点取决于环境。例如，对于 Azure Global，它是 `https://management.azure.com`；对于 Azure US Government，它是 `https://management.usgovcloudapi.net`。
  - 存储后缀: `https://*.core.windows.net`。此 (*) 是存储后缀的通配符。例如，`https://demo.table.core.windows.net`。
  - 用于上传或下载磁盘或快照的 Azure Blob 存储终结点: `https://*.storage.azure.net`。此 (*) 是 Blob 存储导入和导出操作的通配符。例如，`https://md-impexp-xxxxx.z[00-50].blob.storage.azure.net`。

- Key Vault 服务: `https://*.vault.azure.net`。此 (*) 是密钥保管库名称的通配符。例如，`https://<your-key-vault-name>.vault.azure.net`。
- 服务总线后缀: `https://*.servicebus.windows.net`。此 (*) 是在全局 Azure 云中创建的命名空间的通配符。例如，`https://{serviceNamespace}.servicebus.windows.net/{path}`。

5. 选择**保存**后，您将返回到**连接详细信息**页面。选择**下一步**以继续到下一页。
6. 配置连接的资源。资源包括区域和网络。
   - 在**区域**页面上，选择一个区域。
   - 在**网络**页面上，执行以下操作：
     - 键入 1–64 个字符的资源名称，以帮助识别区域和网络组合。资源名称不能只包含空格或字符 `\/;:#.*?=<>|[]{}"'()'`。
     - 选择一个虚拟网络/资源组对。（如果存在多个同名虚拟网络，将网络名称与资源组配对可提供唯一组合。）如果您在上一页选择的区域没有任何虚拟网络，请返回该页面并选择一个具有虚拟网络的区域。
7. 在**摘要**页面上，查看设置摘要，然后选择**完成**以完成设置。

管理服务主体和连接

本节详细介绍了如何管理服务主体和连接：

- 配置 Azure 限制设置
- 在 Azure 中启用映像共享
- 使用 Web Studio 将共享租户添加到连接
- 使用 PowerShell 实现映像共享
- 管理应用程序机密和机密过期日期

配置 AZURE 限制设置

Azure Resource Manager 会限制对订阅和租户的请求，根据定义的限制路由流量，这些限制是根据提供商的特定需求量身定制的。有关详细信息，请参阅 Microsoft 网站上的限制 Resource Manager 请求。订阅和租户存在限制，管理大量计算机可能会出现问题。例如，包含许多计算机的订阅可能会遇到与电源操作相关的性能问题。

> **提示：**

> 有关详细信息，请参阅使用 Machine Creation Services 提高 Azure 性能。

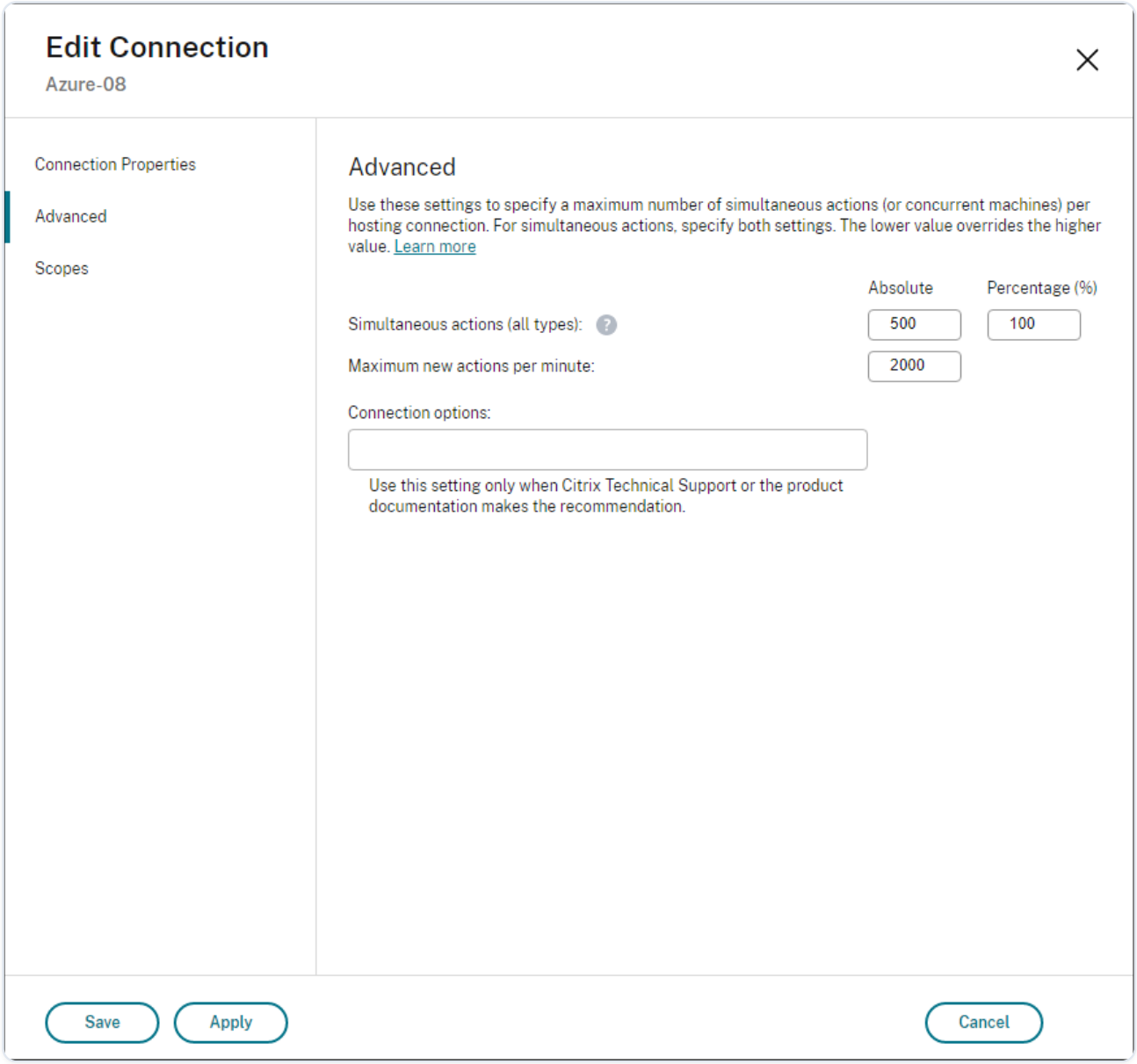
> 为了帮助缓解这些问题，您可以删除 MCS 内部限制，以使用更多 Azure 提供的可用请求配额。

在大型订阅（例如包含 1,000 个 VM 的订阅）中打开或关闭 VM 时，我们建议使用以下最佳设置：

- 绝对同时操作数：500
- 每分钟最大新操作数：2000
- 最大并发操作数：500

使用 Web Studio 为给定的 Azure 连接配置 Azure 操作：

1. 在 Web Studio 中，选择左侧窗格中的**托管**。
2. 选择连接。
3. 在**编辑连接**向导中，选择**高级**。
4. 在**高级**页面上，使用配置选项指定同时操作数和每分钟最大新操作数，以及任何其他连接选项。



MCS 默认支持 500 个最大并发操作。或者，您可以使用远程 PowerShell SDK 设置最大并发操作数。

使用 **PowerShell** 属性 `MaximumConcurrentProvisioningOperations` 指定 Azure 预配操作的最大并发数。使用此属性时，请考虑：

- `MaximumConcurrentProvisioningOperations` 的默认值为 500。
- 使用 PowerShell 命令 `Set-item` 配置 `MaximumConcurrentProvisioningOperations` 参数。

在 AZURE 中启用映像共享

创建或更新计算机目录时，可以从不同的 Azure 租户和订阅中选择共享映像（通过 Azure 计算库共享）。要在租户内部或跨租户启用映像共享，必须在 Azure 中进行必要的设置：

- 在租户内共享映像（跨订阅）

- 跨租户共享映像

在租户内共享映像（跨订阅）
要在 Azure 计算库中选择属于不同订阅的映像，必须将该映像与该订阅的服务主体 (SPN) 共享。

例如，如果存在一个服务主体 (SPN 1)，其在 Studio 中的配置如下：

服务主体: SPN 1

订阅: 订阅 1

租户: tenant 1

映像位于不同的订阅中，在 Studio 中配置为：

订阅: 订阅 2

租户: tenant 1

如果要将订阅 2 中的映像与订阅 1 (SPN 1) 共享，请转到订阅 2，并将资源组与 SPN1 共享。

必须使用 Azure 基于角色的访问控制 (RBAC) 与另一个 SPN 共享映像。Azure RBAC 是用于管理对 Azure 资源访问的授权系统。有关 Azure RBAC 的更多信息，请参阅 Microsoft 文档什么是 Azure 基于角色的访问控制 (Azure RBAC)。要授予访问权限，您需要以“参与者”角色在资源组范围为服务主体分配角色。要分配 Azure 角色，您必须具有 `Microsoft.Authorization/roleAssignments/write` 权限，例如“用户访问管理员”或“所有者”。有关与另一个 SPN 共享映像的更多信息，请参阅 Microsoft 文档使用 Azure 门户分配 Azure 角色。

有关使用 PowerShell 命令从不同订阅中选择映像的信息，请参阅从不同订阅中选择映像。
跨租户共享映像
为了使用 Azure Compute Gallery 在租户之间共享映像，请创建应用程序注册。

例如，如果有两个租户（租户 1 和租户 2），并且您想与租户 1 共享映像库，则：

1. 为租户 1 创建应用程序注册。有关详细信息，请参阅创建应用程序注册。
2. 通过使用浏览器请求登录，授予租户 2 对应用程序的访问权限。将 `Tenant2 ID` 替换为租户 1 的租户 ID。将 `Application (client) ID` 替换为您创建的应用程序注册的应用程序 ID。完成替换后，将 URL 粘贴到浏览器中，然后按照登录提示登录到租户 2。例如：

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
   client_id=<Application (client)
   ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

有关详细信息，请参阅授予租户 2 访问权限。

3. 授予应用程序访问租户 2 资源组的权限。以租户 2 身份登录，并授予应用程序注册访问包含库映像的资源组的权限。有关详细信息，请参阅跨租户验证请求。

要使用 PowerShell 命令从不同租户的映像创建目录：

1. 使用共享租户 ID 更新托管连接自定义属性。
2. 从不同租户选择映像。

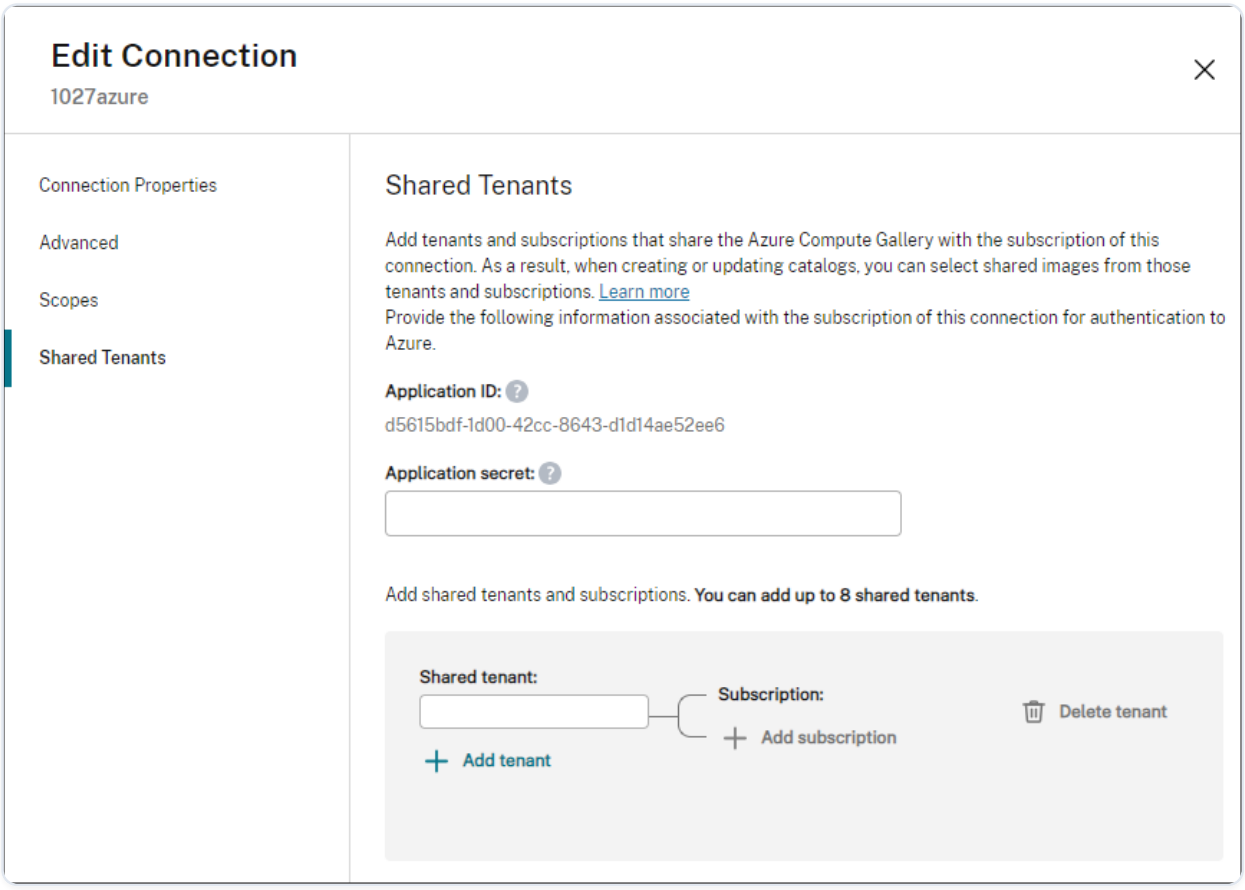
使用 WEB STUDIO 将共享租户添加到连接

在 Web Studio 中创建或更新计算机目录时，您可以从不同的 Azure 租户和订阅中选择共享映像（通过 Azure Compute Gallery 共享）。此功能要求您为关联的主机连接提供共享租户和订阅信息。

> **注意：**
>
> 请确保您已在 Azure 中配置了必要的设置，以启用跨租户映像共享。有关详细信息，请参阅跨租户共享映像。

完成连接的以下步骤：

1. 在 Web Studio 中，在左侧窗格中选择**托管**。
2. 选择连接，然后在操作栏中选择**编辑连接**。



3. 在 **共享租户** 中，执行以下操作：

   - 提供与连接订阅关联的应用程序 ID 和应用程序密钥。Citrix Virtual Apps and Desktops™ 使用此信息向 Microsoft Entra ID 进行身份验证。
   - 添加与连接订阅共享 Azure Compute Gallery 的租户和订阅。每个租户最多可以添加 8 个共享租户和 8 个订阅。

4. 完成后，选择 **应用** 以应用所做的更改并保持窗口打开，或者选择 **确定** 以应用更改并关闭窗口。

使用 POWERSHELL 实施映像共享

本节将引导您完成使用 PowerShell 共享映像的过程：

- 从其他订阅中选择映像
- 使用共享租户 ID 更新托管连接自定义属性
- 从其他租户中选择映像

从其他订阅中选择映像

您可以在同一 Azure 租户中选择属于其他共享订阅的 Azure 计算库中的映像，以使用 PowerShell 命令创建和更新 MCS 目录。

1. 在托管单元根文件夹中，Citrix 创建一个名为 `sharedsubscription` 的新共享订阅文件夹。

2. 列出租户中的所有共享订阅。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\sharedsubscription.folder"
```

3. 选择一个共享订阅，然后列出该共享订阅的所有共享资源组。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription"
```

4. 选择一个资源组，然后列出该资源组的所有库。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup"
```

5. 选择一个图库，然后列出该图库的所有映像定义。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\testgallery.gallery"
```

6. 选择一个映像定义，然后列出该映像定义的所有映像版本。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\sigtestdef.imagedefinition"
```

7. 使用以下元素创建和更新 MCS 目录：

   - 资源组
   - 图库
   - 图库映像定义
   - 图库映像版本

   有关如何使用远程 PowerShell SDK 创建目录的信息，请参阅 `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`。

使用共享租户 ID 更新托管连接自定义属性

使用 `Set-Item` 更新具有共享租户 ID 和订阅 ID 的托管连接自定义属性。在 `CustomProperties` 中添加属性 `SharedTenants`。`Shared Tenants` 的格式为：

```
[{"Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":
["7bb42f40-8d7f-4230-a920-be2781f6d5d9"]},{"Tenant":"50e83564-c4e5-4209-
b43d-815c45659564","Subscriptions":["06ab8944-6a88-47ee-
a975-43dd491a37d0"]}]
```

例如：

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`" /
>

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` />

</CustomProperties>"

-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "advc345"
-SecurePassword

$psd
```

注意：

> 您可以添加多个租户。每个租户可以有多个订阅。

从其他租户选择映像

您可以使用 PowerShell 命令选择属于不同 Azure 租户的 Azure 计算库中的映像，以创建和更新 MCS 目录。

1. 在托管单元根文件夹中，Citrix 创建一个名为 `sharedsubscription` 的新共享订阅文件夹。
2. 列出所有共享订阅。

```
Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
```

3. 选择一个共享订阅，然后列出该共享订阅的所有共享资源组。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription
```

4. 选择一个资源组，然后列出该资源组的所有库。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup
```

5. 选择一个图库，然后列出该图库的所有映像定义。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery
```

6. 选择一个映像定义，然后列出该映像定义的所有映像版本。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery\hij.imagedefinition
```

7. 使用以下元素创建和更新 MCS 目录：

   - 资源组

- 图库
- 图库映像定义
- 图库映像版本

有关如何使用远程 PowerShell SDK 创建目录的信息，请参阅 `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`。

管理应用程序密钥和密钥过期日期

请务必在密钥过期之前更改连接的应用程序密钥。在密钥过期前 14 天，您会在**托管**节点中特定主机连接上看到一个警告图标。但是，如果密钥过期，您将收到错误。

在 Azure 中创建应用程序密钥

您可以通过 Azure 门户为连接创建应用程序密钥。

1. 选择 **微软 Entra ID**。
2. 在 Microsoft Entra ID 的 **应用注册** 中，选择您的应用程序。
3. 转到 **证书和机密**。
4. 单击“**客户端机密 > 新建客户端机密**”。
5. 提供密钥的描述并指定持续时间。完成后，选择**添加**。

> **注意：**
>
> 请务必保存客户端机密，因为以后无法检索它。

6. 复制客户端机密值和过期日期。
7. 在 Web Studio 中，编辑相应的连接，并将**应用程序密钥**和**密钥过期日期**字段中的内容替换为您复制的值。

更改机密过期日期

您可以使用 Web Studio 添加或修改正在使用的应用程序机密的到期日期。

> **注意：**
>
> 在机密密钥到期前 14 天，您会在**托管**节点中特定主机连接上看到一个警告图标。

1. 在“**添加连接和资源**”向导中，右键单击一个连接，然后单击“**编辑连接**”。

2. 在“**连接属性**”页面上，单击“**机密过期日期**”以添加或修改正在使用的应用程序机密的过期日期。

Azure 扩展区域

Azure 扩展区域是现有 Azure 区域的小型扩展，使组织能够将工作负载运行得更靠近其用户，从而提高性能和合规性。Azure 上的 MCS 现在支持扩展区域中 VM 的预配和电源管理。

要了解有关 Azure 扩展区域的更多信息，请参阅 Microsoft 文档：Azure 扩展区域文档。

用例

此功能适用于持久和非持久目录：

- 仅限电源管理的 VM：您可以将现有的扩展区域 VM 导入到仅限电源管理的目录中，并使用 Citrix MCS 对其进行电源管理。
- MCS 预配的 VM：您可以将新的 VM 预配到扩展区域中，并使用 MCS 对其进行管理。此功能还包括对映像管理工作流的支持。

限制

目前，使用 Azure 扩展区域存在一些限制。其中许多限制是由于当前的 Azure 约束造成的：

- 不支持专用主机。
- 不支持容量预留。
- 不支持邻近放置组。
- 不支持 Spot VM。
- 扩展区域不支持可用性区域。
- 仅支持 **StandardSSD_LRS** 和 **Premium_LRS** 存储类型。
- 当前无法使用 **UseSharedImageGallery** 功能将主映像保存到扩展区域中的 Azure 计算库（或共享映像库）。因此，也不支持临时 OS 磁盘。
- 如果您使用 Azure 计算库映像版本作为主映像，请确保在尝试使用之前，复制已在扩展区域中完全完成。在复制完成之前尝试使用映像版本可能会导致部署失败。

先决条件

使用扩展区域之前，请确保已完成以下先决条件步骤：

1. 在 Azure 中注册：
    a. 扩展区域默认未启用。
    b. 在 Azure 订阅中注册 `Microsoft.EdgeZones` 资源提供程序：为资源提供程序 Microsoft.EdgeZones 注册订阅。

c. 分别注册每个所需的扩展区域（例如：LosAngeles、Perth）：注册 Azure 扩展区域。

2. 准备 Citrix 资源：

a. 在扩展区域中创建虚拟网络。

b. 根据需要创建主映像和快照。

所需权限

要在扩展区域中创建目录，您的服务主体必须具有以下权限：`Microsoft.EdgeZones/extendedZones/read`。

有关最低所需权限的更多信息，请参阅最低权限。

配置步骤

1. 在扩展区域中创建托管单元

使用 `.extendedzone` 类型的扩展区域与区域一起列在 Citrix MCS 清单中。要预配到扩展区域，您必须创建与该扩展区域关联的新托管单元。

示例：在洛杉矶扩展区域中创建托管单元

```
$RootPath = "XDHyp:\Connections\MyConnectionName\Los
Angeles.extendedzone"



$NetworkPath = "XDHyp:\Connections\MyConnectionName\Los
Angeles.extendedzone\virtualprivatecloud.folder\MyResourceGroup.resourc
egroup\MyExtendedZoneNetwork.virtualprivatecloud\MyExtendedZoneSubnet.n
etwork"



$HostingUnitPath = "XDHyp:\HostingUnits\MyHostingUnitName"



New-Item -HypervisorConnectionName MyConnectionName -NetworkPath
@($NetworkPath) -Path @($HostingUnitPath) -RootPath $RootPath
-StoragePath @()
```

2. 在扩展区域中创建 MCS 目录

创建托管单元后，使用 Studio 或 PowerShell 继续创建目录。确保您的目录引用了扩展区域托管单元。

故障排除

如果遇到问题，请检查以下各项：

1. 确保您的订阅已注册扩展区域。
   a. 确认您的订阅已在 Microsoft.EdgeZones 资源提供程序中注册。
   b. 确保每个扩展区域都已单独注册。
2. 验证您的服务主体是否具有新权限。
   a. 您的服务主体必须具有 `Microsoft.EdgeZones/extendedZones/read` 权限。

扩展区域中的清单项在缺少注册或权限时可能显示为“未知扩展区域”。

> **注意：**
>
> 如果在父区域中使用来自扩展区域的主映像创建目录，则仍需要扩展区域的注册和权限。

使用预创建的网络安全组

创建一个“全部拒绝”网络安全组用于映像准备，而不是请求 Citrix 创建和修改 NSG。使用 PowerShell 命令 `Set-Item` 编辑托管单元的自定义属性，以包含参数 `NsgForPreparation` 来提供“全部拒绝”网络安全组。

先决条件

配置服务主体所需的以下权限：

- `Microsoft.Network/networkSecurityGroups/join/action`：将网络安全组关联到子网或网络接口
- `Microsoft.Network/networkSecurityGroups/read`：获取网络安全组
- `Microsoft.Network/networkSecurityGroups/securityRules/read`：获取规则

添加预创建的“全部拒绝”网络安全组

要添加预创建的“全部拒绝”网络安全组，请在托管单元上按如下方式设置自定义属性：

1. 使用远程 PowerShell SDK 打开 PowerShell 窗口。
2. 运行以下命令：

```
Add-PSSnapin citrix*.

cd XDHyp:\HostingUnits\

Dir
```

3. 选择一个托管单元以检索详细信息：

```
Get-Item "XDHyp:\HostingUnits\<hostingunitname>"
```

4. 将 CustomProperties 复制到记事本，并附加属性设置 `<Property xsi:type="StringProperty` " Name= `"NsgForPreparation` " Value= `"{ResourceGroupName}/{NetworkSecurityGroupName}"/>` 。例如：

```
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>
```

5. 在 PowerShell 窗口中，为修改后的自定义属性分配一个变量。例如：

```
$customProperty = "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`"{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>"
```

6. 运行 `$cred = Get-Credential` 。如果出现提示，请提供连接凭据。凭据是 Azure 应用程序 ID 和密钥。

7. 运行以下命令。

```
Set-Item -PSPath XDHyp:\HostingUnits\<hostingunitname>
-CustomProperties $customProperty -username $cred.username
-Securepassword $cred.password
```

重要提示：

> 如果收到提示 SubscriptionId 缺失的消息，请将自定义属性中的所有双引号 (“) 替换为反引号后跟双引号 (`”)。

8. 运行 `dir` 以验证更新的 `CustomProperties` 设置。

> **注意：**
>
> 更新需要一分钟以上才能反映。

检索网络安全组详细信息

要检索网络安全组详细信息，首先检索包含网络安全组的资源组，然后根据资源组名称检索网络安全组。

1. 检索包含网络安全组的资源组。例如：

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes":
["networksecuritygroup"]}'
```

2. 根据资源组名称检索网络安全组。例如：

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType securitygroup -MaxRecords
5 -AdditionalDataFilter '{"location": ["eastus", "westus"],
"resourcegroup":["resourcegroupname"]}'
```

筛选空资源组

在创建计算机目录期间选择主映像、计算机配置文件或准备好的映像时，使用 PowerShell 命令 `Get-HypInventoryItem` 筛选空资源组。

示例：

- 检索页面中的最大记录数：

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- 检索页面中的最大记录数，并进行筛选以查找具有特定资源的资源容器。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- 通过跳过直接指示页面进行检索，并进行筛选以查找具有特定资源的资源容器。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -skip 20 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- 使用令牌检索下一页，并进行筛选以查找具有特定资源的资源容器。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
-ContinuationToken
'ew0KICAiJGlkIjogIjEiLA0KICAiTWF4Um93cyI6IDUsDQogICJSb3dzVG9Ta2lwIjogMj
UsDQogICJLdXN0b0NsdXN0ZXJVcmwiOiAiaHR0cHM6Ly9hcmctbmV1LTEzLXNmLmFyZy5jb
3JlLndpbmRvd3MubmV0Ig0KfQ=='
```

- 检索所有带有 Citrix 内部标签的资源组，并使用 `MaxRecords` 限制最大记录数。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- 筛选带有 Citrix 内部标签的计算机配置文件（主映像），并使用 `MaxRecords` 限制最大记录数。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- 筛选带有 Citrix 内部标签的准备好的映像，并使用 `MaxRecords` 限制最大记录数。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion"]}'
```

- 筛选带有 Citrix 内部标签的计算机配置文件（准备好的映像），并使用 `MaxRecords` 限制最大记录数。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- 筛选带有 Citrix 内部标签的映像，并使用 `MaxRecords` 和位置限制最大记录数。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"], "location": ["eastus",
"westus"]}'
```

- 检索所有资源组，不考虑标签 `CitrixResource`。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
50 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"]}' -Force $true
```

连接到 Azure Sovereign Airgap 云环境

Azure Sovereign Airgap 云环境适用于必须位于隔离网络域中的绝密工作负载。您可以在创建主机连接时使用自定义属性 `DisableInstanceDiscovery` 连接到 Azure Sovereign Airgap 云环境。

```
<Property xsi:type="StringProperty" Name="DisableInstanceDiscovery"
Value="true" />
```

有关创建 Azure 主机连接的更多信息，请参阅 Create-HostingConnection.ps1。

所需的 Azure 权限

本部分包含 Azure 所需的最低和一般权限。

最低权限

最低权限可提供更好的安全控制。但是，由于仅使用最低权限，需要额外权限的新功能将无法运行。

创建主机连接

使用从 Azure 获取的信息添加新的主机连接。

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/disks/read",

"Microsoft.Resources/providers/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/tenants/read",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read"
```

虚拟机电源管理

启动或关闭计算机实例。

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",
```

```
"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",
```

创建、更新或删除虚拟机
创建计算机目录，然后添加、删除、更新计算机，并删除计算机目录。

以下是当主映像是托管磁盘或快照与托管连接位于同一区域时所需的最低权限列表。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",
```

```
"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Features/providers/features/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/locations/usages/read",
```

```
"Microsoft.Compute/capacityReservationGroups/capacityReservations/read"
```

对于以下功能，您需要在最低权限的基础上额外授予以下权限：

- 如果主映像是位于与托管连接相同区域的存储帐户中的 VHD：

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",
```

- 如果主映像是共享映像库中的 ImageVersion：

```
"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",
```

- 如果主映像是托管磁盘，则快照或 VHD 位于与托管连接区域不同的区域：

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

- 如果您使用 Citrix 管理的资源组：

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- 如果您将主映像放置在共享租户或订阅中的 Azure 计算库（以前称为共享映像库）中：

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Resources/subscriptions/read",
```

- 如果您使用 Azure 专用主机支持：

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

- 如果您将服务器端加密 (SSE) 与客户管理密钥 (CMK) 结合使用：

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- 如果您使用 ARM 模板（计算机配置文件）部署 VM：

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/delete",

"Microsoft.Insights/DataCollectionRuleAssociations/Read",

"Microsoft.Insights/dataCollectionRules/read",
```

- 如果您使用 Azure 模板规范作为计算机配置文件：

```
"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

创建、更新和删除具有非托管磁盘的计算机
以下是主映像为 VHD 且使用管理员提供的资源组时所需的最低权限列表：

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

```
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
```

成本管理

以下是检索 VM 定价所需的最低权限：

```
"Microsoft.Consumption/pricesheets/read"
```

以下是检索 VM 成本所需的最低权限：

```
"Microsoft.CostManagement/query/read"
```

注意：

要查看 Azure 计算机目录的“**成本洞察**”选项卡，您必须具有“**成本管理 > 管理 > 读取成本**”权限（云管理员的默认权限）。有关“**成本洞察**”选项卡的信息，请参阅查看目录详细信息。

一般权限

参与者角色拥有管理所有资源的完全访问权限。这组权限不会阻止您获取新功能。

以下权限集提供了最佳的未来兼容性，尽管它包含的权限比当前功能集所需的权限更多：

```
"Microsoft.Compute/diskEncryptionSets/read",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/read",
```

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/hostGroups/hosts/read",

"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",
```

```
"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/locations/usages/read",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Resources/providers/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/read",

"Microsoft.Resources/tags/read",
```

```
"Microsoft.Resources/tags/write",

"Microsoft.Resources/tenants/read",

"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",

"Microsoft.Features/providers/features/read",

"Microsoft.Insights/DataCollectionRuleAssociations/Read",

"Microsoft.Insights/dataCollectionRules/read",

"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read",

"Microsoft.Compute/capacityReservationGroups/capacityReservations/read"
```

在 Azure 非机密环境中验证主机连接

您可以验证主机连接上的权限，以执行与创建和管理 MCS 计算机目录相关的任务。此实现可帮助您提前找出不同场景（例如创建、删除和更新 VM、VM 的电源管理）所需的缺失权限，从而避免在关键时刻受阻。

您可以使用 PowerShell 命令 `Test-HypHypervisorConnection` 验证主机连接上的权限。该命令的结果将捕获为一个列表，其中列表中的每个项目都分为三个部分。

- 类别：用户可以执行的用于创建和管理 MCS 计算机目录的操作或任务。
- 纠正措施：管理员必须执行的步骤，以解决用户缺少权限的差异。
- 缺失权限：某个类别缺失权限的列表。

要验证权限，请执行以下操作：

1. 创建到 Azure 的主机连接。
2. 从 Delivery Controller™ 主机打开 PowerShell 窗口。
3. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
4. 运行以下命令以验证您是否具有测试连接所需的权限。

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AzureCon"
   ```

   SPN 所需的角色级别权限：

   - Microsoft.Authorization/roleDefinitions/read（在订阅级别或资源组级别，如果提供了资源组）
   - Microsoft.Authorization/roleAssignments/read（在订阅级别，如果提供了资源组，则在资源组级别）

   SPN 所需的 API 级别权限：

   Microsoft.Graph：

   - Application.Read.All
   - Directory.Read.All
   - ServicePrincipalEndpoint.Read.All

5. 添加查找权限所需的缺失权限后，运行以下命令以验证您是否在各个类别中拥有权限。

   示例：

要在需要更高级别授权的订阅级别测试连接：

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\ AzureCon
-SecurePassword $password -UserName 922e65d5-38ae-4cf5-xxxx-xxxxxxxxx
```

示例：

要在不需要高级别授权的资源组级别测试连接：

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
-CustomProperties $customProperties | Format-List
```

注意：

CustomProperties 参数用于提供资源组级别，因为资源组是连接的特定信息。

示例：

要在资源组级别测试具有更高级别授权的连接：

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
-SecurePassword $password -UserName
922e65d5-38ae-4cf5-832b-54122196b7dd -CustomProperties
$customProperties
```

有关权限的信息，请参阅 所需的 Azure 权限。

在 Azure 机密环境中验证主机连接

您可以使用 PowerShell 命令 `Test-HypHypervisorConnection` 验证主机连接在 Azure 机密环境中是否具有所需的权限。

但是，要成功获取验证结果，请创建或更新现有主机连接以具有自定义属性 `AuthenticationObjectId`。此属性存储与托管连接关联的服务主体的对象 ID。

注意：

从 Azure 门户获取服务主体的对象 ID。请勿使用应用程序的 ID。

创建或更新主机连接以包含 AUTHENTICATIONOBJECTID

使用 `New-Item` 创建主机连接并将 `AuthenticationObjectId` 添加为自定义属性。示例：

```
New-Item -ConnectionType 'Azure' -HypervisorAddress @('http://
hypervisorhost1.example.com','http://hypervisorhost2.example.com')`

    -LoggingId $loggingId -Path @('XDHyp:\\Connections\\Example') -Persist
-Scope @() `

    -Password 'Password' -UserName 'root' -CustomProperties <Property
xsi:type="StringProperty" Name="AuthenticationObjectId" Value="Object ID
of the service principal"/>
```

使用 `Set-Item` 更新现有主机连接以将 `AuthenticationObjectId` 添加为自定义属性。执行此操作的步骤如下：

1. 使用远程 PowerShell SDK 打开 PowerShell 窗口。
2. 运行以下命令：

   ```
   Add-PSSnapin citrix*.

   cd XDHyp:\Connections\

   dir
   ```

3. 将连接中的 `CustomProperties` 复制到记事本，并将属性设置 `<Property xsi:type="StringProperty" Name="AuthenticationObjectId" Value="Object ID of the service principal"/>` 附加到 `CustomProperties`。
4. 在 PowerShell 窗口中，为修改后的自定义属性分配一个变量。
5. 运行 `$cred = Get-Credential`。如果出现提示，请提供连接凭据。凭据是 Azure 应用程序 ID 和密钥。
6. 运行 `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password`。
7. 运行 `dir` 以验证更新的 `CustomProperties` 设置。

```
Set-Item -PSPath XDHyp:\Connections\$connName -CustomProperties
<Property xsi:type="StringProperty" Name="AuthenticationObjectId"
Value="Object ID of the service principal"/> -username $cred.username
-Securepassword $cred.password
```

验证主机连接的权限

为了验证所需角色和权限的主机连接，请运行以下命令：

- 如果您在订阅级别分配了角色和权限：

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\<Your-
HostingConnection>
```

- 如果您在资源组级别分配了角色和权限：

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\<Your-
HostingConnection>  -CustomProperties $CustomProperties



$CustomProperties = '<CustomProperties xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/
machinecreation">'`

+ '<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="ExampleResourceGroup" />'`

+ '</CustomProperties>'
```

下一步操作

- 如果您处于初始部署过程中，请参阅创建计算机目录
- 有关 Azure 特定信息，请参阅 创建 Microsoft Azure 目录

更多信息

- 连接和资源
- 创建计算机目录

连接到微软系统中心虚拟机管理器

(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections.html)介绍了创建连接的向导。以下信息涵盖了 Microsoft System Center Virtual Machine Manager (VMM) 的具体详细信息。

> **注意：**
>
> 在创建到 VMM 的连接之前，您需要首先将 VMM 帐户设置为资源位置。请参阅 Microsoft System Center Virtual Machine Manager 虚拟化环境。

创建连接

如果您使用 MCS 预配 VM，请在连接创建向导中执行以下操作：

- 以主机服务器的完全限定域名形式输入地址。
- 输入您之前设置的管理员帐户的凭据。此帐户必须具有创建新 VM 的权限。
- 在“主机详细信息”对话框中，选择创建 VM 时要使用的群集或独立主机。

> **重要提示**
>
> 即使您使用的是单个 Hyper-V 主机部署，也要浏览群集或独立主机。

下一步操作

- 如果您处于初始部署过程中，请参阅创建计算机目录
- 有关使用 MCS 在 SMB 3 文件共享上创建计算机目录的信息，请参阅 创建 Microsoft System Center Virtual Machine Manager 目录

更多信息

- 连接和资源
- 创建计算机目录

连接到 Nutanix

(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections.html) 描述了创建连接的向导。以下信息涵盖了 Nutanix 特有的详细信息。

> **注意：**

> 在创建到 Nutanix 的连接之前，您需要首先将您的 Nutanix 帐户设置为资源位置。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-prepare/nutanix.html)。

Nutanix AHV Prism Central 主机连接

在创建 Nutanix AHV Prism Central 主机连接之前，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-prepare/nutanix.html#prerequisites)。

您可以使用以下任一方式创建连接：

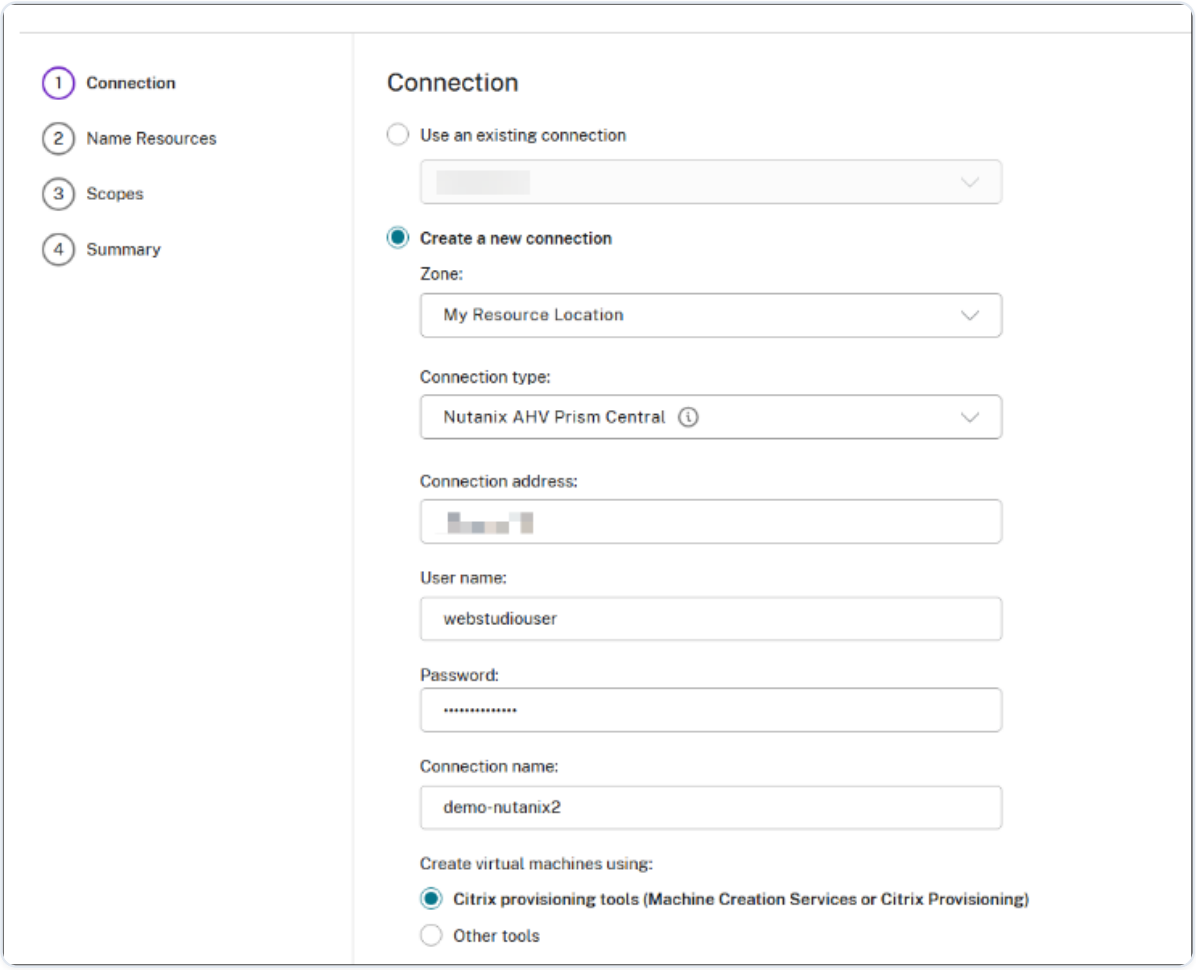
- Web 控制台
- (#create-a-connection-using-powershell)

限制

- Nutanix AHV Prism Central 主机连接不支持模板和网络等项目的重复对象名称。为目录创建选择此类项目可能会导致意外行为。

使用 WEB STUDIO 创建连接

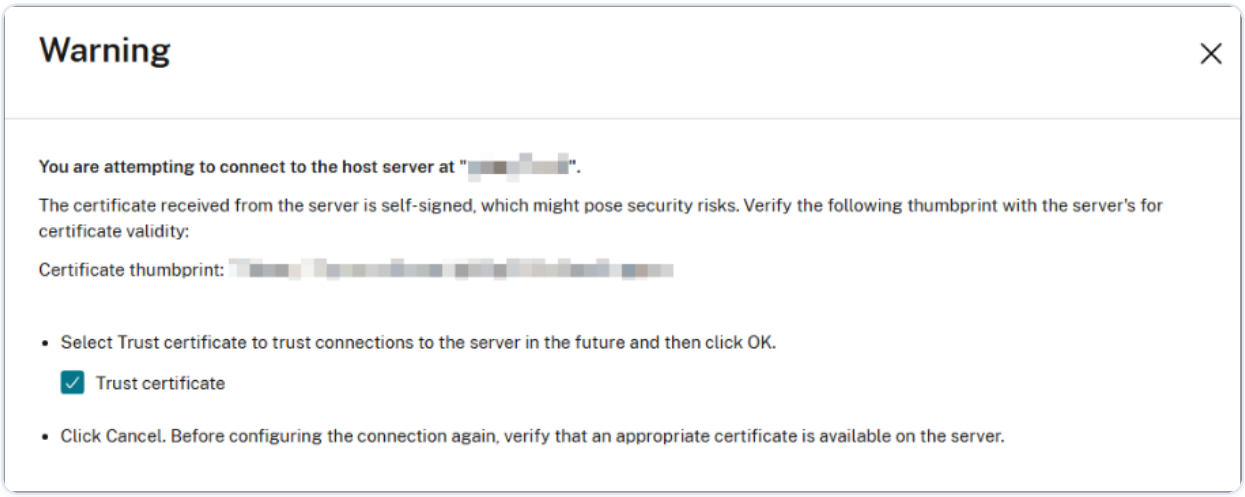
1. 登录到 Citrix Cloud。
2. 单击**管理**。
3. 在左侧窗格中选择**托管**。
4. 在操作栏中单击**添加连接和资源**。
5. 在 **Connection** 页面上：
    a. 选择“**创建新连接**”。
    b. 选择 **Nutanix AHV Prism Central** 作为连接类型。
    c. 输入您的 Nutanix AHV Prism Central 的 IP 地址作为连接地址。
    d. 输入您的管理凭据和易记的连接名称。
    e. 选择 **Citrix 预配工具 (机器创建服务™ 或 Citrix 预配)**。
    f. 单击**下一步**。



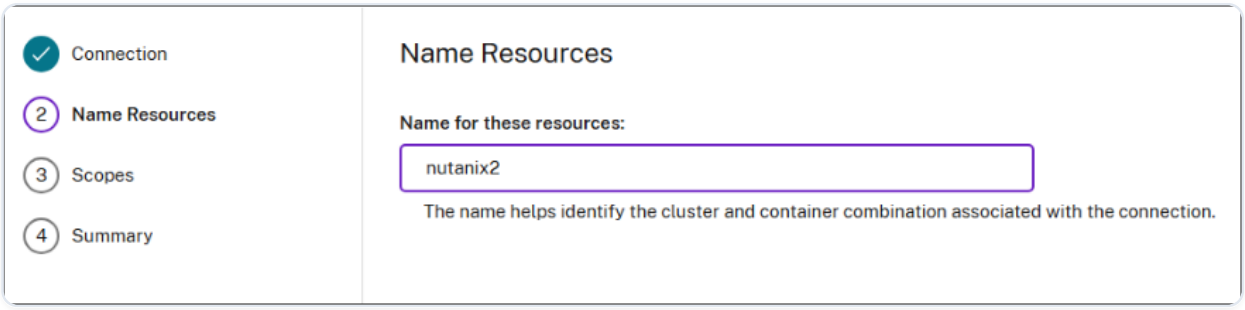
> **注意：**
>
> 创建主机连接时，不需要选择网络或群集。只需要一个托管单元名称。在创建计算机目录时选择网络和群集。

6. 单击 **Next** 后，Citrix Virtual Apps and Desktops 会收到私有 CA 签名的证书，您会看到一个 **Warning** 页面。有关信息，请参阅 Secure connections to the Nutanix Prism Central。

   将收到的指纹与服务器的指纹进行比较，以验证证书的有效性。如果有效，请选择 **Trust certificate**，然后单击 **OK** 以继续创建连接。Citrix Virtual Apps and Desktops 随后会信任该证书并存储指纹以供将来验证。



7. 在“**命名资源**”页面上，添加资源的唯一名称。点击“**下一步**”。



8. 在“**范围**”页面上，为此主机选择一个或多个范围。
9. 在“**摘要**”页面上，检查配置，然后单击“**完成**”。

> **注意：**
>
> Nutanix AHV Prism Central 连接可以与其他类型的 Nutanix 连接共存。

保护到 NUTANIX PRISM CENTRAL 的连接

Nutanix SSL 指纹功能简化了在与 Nutanix Prism Central 虚拟机管理程序建立主机连接时的证书信任。此功能允许将不受信任证书的指纹存储在站点数据库中，从而确保 Citrix Virtual Apps and Desktops 始终将虚拟机管理程序识别为受信任的。

创建 Nutanix 主机连接时，将显示一个“**警告**”页面，显示您正在连接的计算机的证书，并允许您决定是否信任它。

使用 POWERSHELL 创建连接

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*`。
3. 设置以下参数：

```
$ConnectionName = “Name of the connection”

$UserName = “Username of the account on hypervisor”

$ZoneUid =  “UID of the zone where the hosting connection will be created”

$HypervisorAddress = “The IP address of the hypervisor”

$SSLThumbprint =  “The Nutanix PC SSL thumbprint can be set using PowerShell SDK”

$connectionPath = "XDHyp:\Connections\" + $ConnectionName

$SecureUserInput = Read-Host "Enter the password for the user $($UserName)" -AsSecureString

$EncryptedUserInput = $SecureUserInput | ConvertFrom-SecureString

$SecurePass = ConvertTo-SecureString -String $EncryptedUserInput
```

4. 为新的托管连接创建项目。例如：

```
$connection = New-Item -Path @($connectionPath) -ConnectionType "Custom" -HypervisorAddress ` @($HypervisorAddress) -Persist -PluginId "AcropolisHypervisorPCFactory" -Scope @() ` -SecurePassword $SecurePass -SSLThumbprint @($SSLThumbprint) -UserName $UserName -ZoneUid ` $ZoneUid
```

5. 创建代理虚拟机管理程序连接。例如：

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid $connection.HypervisorConnectionUid
```

创建托管单元

当您使用 PowerShell 命令创建托管单元时，请提供以下必需参数：

- `$HostUnitName`：要创建的托管单元的名称
- `ConnectionName`：先前创建的管理程序连接的名称

1. 打开 PowerShell 窗口。

2. 运行 `add-pssnapin citrix*`。
3. 运行 PowerShell 命令以创建托管单元。例如：

```
$hostUnitPath = "XDHyp:\HostingUnits\" + $HostUnitName

New-Item -Path @($hostUnitPath) -RootPath $connectionPath
-HypervisorConnectionName $ConnectionName -CustomProperties ""
-NetworkPath @() -StoragePath @()
```

注意：

创建主机连接时，不需要选择网络或群集。只需要一个托管单元名称。在创建计算机目录时选择网络和群集。

管理主机连接

您可以使用以下方式管理现有主机连接：

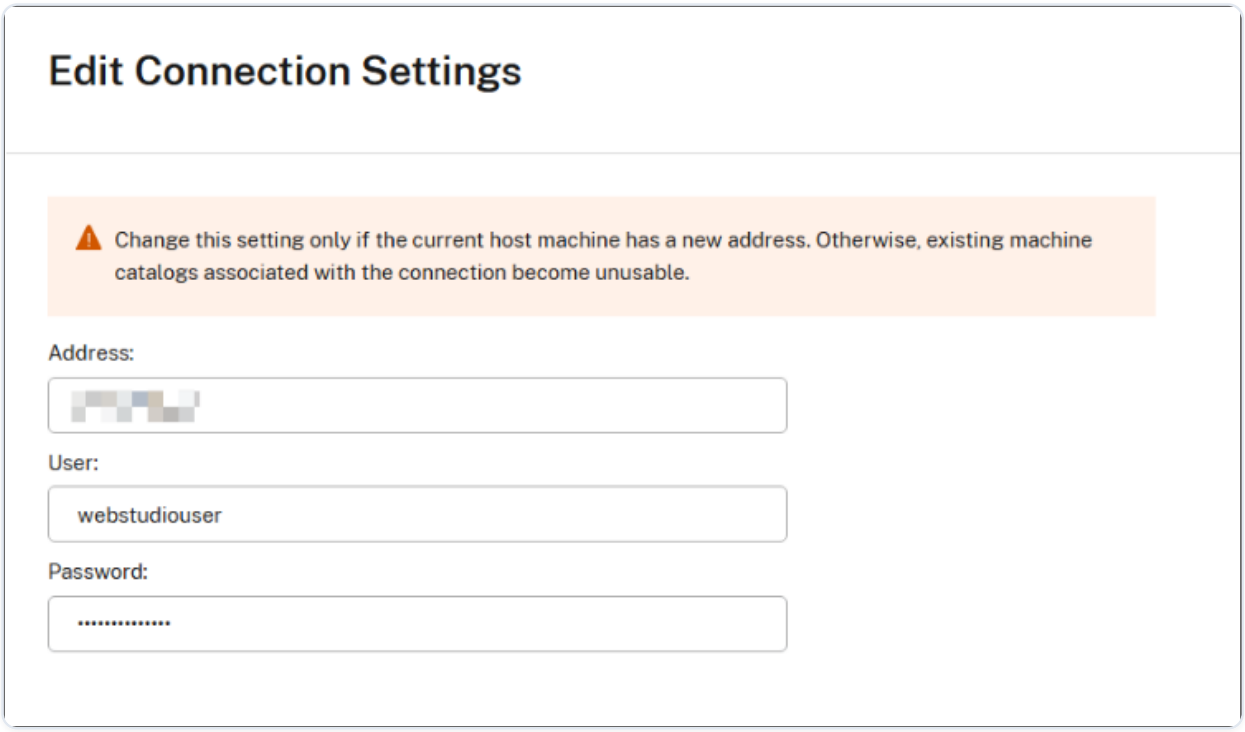
- Web 控制台
- PowerShell

使用 Web Studio 管理主机连接
创建主机连接后，导航到 Web Studio 上的 **Hosting** 节点，右键单击连接以执行以下操作：

- **删除连接**
- **重命名连接**
- **编辑连接**
- **启用维护模式**
- **查看计算机**
- **测试连接**
- **测试 TLS 证书信任**

使用 Web Studio 编辑连接

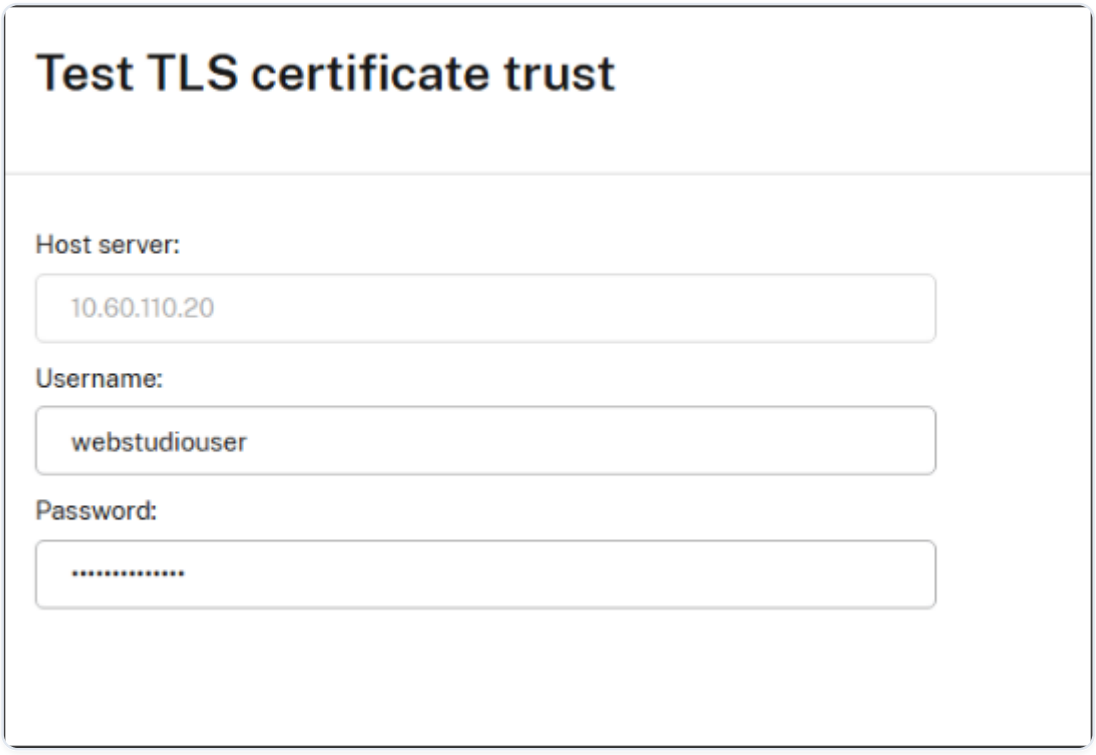
1. 右键单击连接，然后单击 **编辑连接**。
2. 在 **连接属性** 页面上，单击 **编辑设置**。
3. 在 **编辑连接设置** 页面上，您可以更改证书信息，然后单击 **保存**。



4. 在 **警告** 页面上选择 **信任证书** 以信任新的证书指纹。

测试 TLS 证书信任

1. 右键单击连接，然后单击 **测试 TLS 证书信任**。
2. 在 **测试 TLS 证书信任** 页面上，您可以更改证书信息，然后单击 **测试**。



如果测试结果不成功，请使用 Edit a connection using Web Studio 更改连接的证书信息。

使用 PowerShell 管理主机连接

您可以使用 PowerShell 命令来：

- 更改或更新主机连接的用户凭据。例如：

```
$UserName = "Username of the account on hypervisor"

$SecureUserInput = Read-Host "Enter the password for the user $
($UserName)" -AsSecureString

$EncryptedUserInput = $SecureUserInput | ConvertFrom-SecureString

$SecurePass = ConvertTo-SecureString -String $EncryptedUserInput

Set-Item  -LiteralPath @("XDHyp:\Connections\<Host connection name>")
 -SecurePassword $SecurePass -UserName $UserName
```

- 重置 SSLThumbprint。例如：

```
$SSLThumbprint =  "The Nutanix PC SSL thumbprint value"

Set-Item  -LiteralPath @("XDHyp:\Connections\<Host connection name>")
 -SecurePassword $SecurePass -UserName $UserName -SSLThumbprint
$SSLThumbprint
```

所需权限

用于 Nutanix AHV Prism Central 主机连接的管理帐户需要以下权限。
创建主机连接
群集：

- 查看群集

虚拟机电源管理
AHV 虚拟机：

- ACPI 关闭虚拟机
- ACPI 重启虚拟机
- 客户机重启虚拟机
- 客户机关机虚拟机
- 关闭虚拟机电源
- 开启虚拟机电源

- 重置虚拟机
- 查看现有虚拟机

集群:

- 查看集群

子网:

- 查看子网

VM 预配

AHV 虚拟机:

- ACPI 重启虚拟机
- ACPI 关机虚拟机
- 关联虚拟机类别
- 创建新虚拟机
- 创建虚拟机
- 创建虚拟机磁盘
- 创建虚拟机网卡
- 删除现有虚拟机
- 删除虚拟机
- 删除虚拟机磁盘
- 删除虚拟机 GPU
- 删除虚拟机网卡
- 取消关联虚拟机类别
- 弹出虚拟机 CD ROM
- 客户机重启虚拟机
- 客户机关机虚拟机
- 关闭虚拟机电源
- 开启虚拟机电源
- 重置虚拟机
- 虚拟机快照
- 更新虚拟机基本配置

- 更新虚拟机磁盘
- 更新虚拟机磁盘列表
- 更新虚拟机网卡
- 查看现有虚拟机
- 查看虚拟机
- 查看虚拟机光驱
- 查看虚拟机磁盘
- 查看虚拟机 GPU
- 查看虚拟机网卡

AHV 虚拟机恢复点:

- 查看 AHV 虚拟机恢复点

类别:

- 查看类别

集群:

- 查看集群

主机:

- 查看主机

映像:

- 创建映像
- 删除映像
- 更新映像
- 查看映像

恢复点:

- 创建恢复点
- 删除恢复点
- 复制恢复点
- 还原恢复点

- 查看恢复点
- 查看虚拟机恢复点

存储容器:

- 查看存储容器
- 查看存储容器数据存储
- 查看存储容器统计信息

存储策略:

- 查看存储策略

子网:

- 查看子网
- 查看子网虚拟网卡

任务:

- 取消任务
- 查看任务

VM 恢复点:

- 删除 VM 恢复点
- 恢复 VM 恢复点
- 查看 VM 恢复点

VM 模板：

- 查看 VM 模板
- 查看 VM 模板版本
- 部署 VM 模板

卷组：

- 将卷组附加到 AHV VM
- 从 AHV VM 分离卷组
- 查看卷组
- 查看卷组详细信息

VPC：

- 查看 VPC

Nutanix AHV、Nutanix AHV PC 或 Nutanix AHV DRaaS 主机连接

1. 登录到 Citrix Cloud。
2. 单击**管理**。
3. 在左侧窗格中选择 **托管**。
4. 在操作栏中单击 **添加连接和资源**。
5. 在 **连接** 页面上，可以选择以下连接类型：

   - **Nutanix AHV**：指定 Prism Element (PE) 群集地址、凭据以及连接名称。在 **网络** 页面上，选择一个或多个网络并为托管单元命名。

     > **注意：**
     >
     > 如果使用 Nutanix AHV (Prism Element) 作为资源部署计算机，请选择虚拟机磁盘所在的容器。

   - **Nutanix AHV PC**：指定 Prism Central (PC) 地址、凭据以及连接名称。在 **网络** 页面上，从列表中选择网络、群集并为托管单元命名。

     > **注意：**
     >
     > 连接类型 **Nutanix AHV PC** 仅用于创建与 Azure 上的 Nutanix Cloud Cluster (NC2) 的连接。此外，计算机目录只能托管在 Azure 上的 NC2 连接中的单个群集上。此类型的连接需要在 Cloud Connector 上安装 Nutanix 插件

   - **Nutanix AHV DRaaS**：指定您的地址和用户名，然后导入 Nutanix DRaaS 凭据文件 (`.pem`) 中包含的公钥和私钥。（公钥和私钥由 Nutanix DRaaS 管理员在 Nutanix DRaaS 云中生成。）

     - 要导入密钥，请找到您的凭据文件，用记事本（或任何文本编辑器）打开它，然后复制内容。之后，返回到 **连接** 页面，选择 **导入密钥**，粘贴内容，然后选择 **保存**。请勿更改凭据内容或其格式。

下一步

- 如果您处于初始部署过程中，请参阅创建计算机目录
- 有关 Nutanix 的特定信息，请参阅 Create a Nutanix catalog

更多信息

- 创建和管理连接与资源
- Nutanix 虚拟化环境
- Nutanix 云和合作伙伴解决方案

连接到 Nutanix 云和合作伙伴解决方案

(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections.html) 描述了创建连接的向导。以下信息涵盖了 Nutanix 云和合作伙伴解决方案的特定详细信息。

努坦尼克斯 AHV 棱镜中心

Citrix Virtual Apps and Desktops 支持以下云管理程序中的 Nutanix Cloud Clusters (NC2)，用于 Citrix 管理的 Nutanix AHV Prism Central 插件。

- AWS
- 微软 Azure

> **注意：**
>
> - 在 AWS 和 Azure 上创建到 NC2 的连接之前，请在云平台中准备好资源。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-prepare/nutanix-cloud-patrner-solutions.html)。
> - 有关创建托管连接、虚拟机电源管理和目录预配的权限，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections/connection-nutanix.html#required-permissions)。

连接到 AZURE 和 AWS 上的 NC2

连接到 Azure 或 AWS 上的 Nutanix 云集群 (NC2) 需要访问已部署的 Prism Central 实例以及具有 Prism Admin 角色的凭据。

您可以使用以下方式创建主机连接：

- 网络工作室(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections/connection-nutanix.html#create-a-connection-using-web-studio)
- (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections/connection-nutanix.html#create-a-connection-using-powershell)

有关连接的完整信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections/connection-nutanix.html#connection-to-nutanix-ahv-prism-central)

努坦尼克斯 棱镜元素

Citrix Virtual Apps and Desktops 支持以下云管理程序中的 Nutanix Cloud Clusters (NC2)，用于 Nutanix Prism Element 插件。

- AWS

连接到 NUTANIX PRISM

创建 Nutanix 集群后，连接到 Nutanix Prism。 要连接到 Nutanix Prism：

1. 在 10.0.129.0/24 子网中创建一个堡垒虚拟机。
2. RDP 到堡垒虚拟机，访问您在上一节中复制的 **Prism Element** 的 URL。
3. 使用默认凭据登录：`admin:nutanix/4u`。记得更改密码。

在 NUTANIX 集群上创建虚拟机

连接到 **Nutanix Prism** 后，创建 Nutanix 集群上的虚拟机。
如果虚拟机需要 Internet 访问

1. 转到 AWS 控制台。
2. 在与 Nutanix CFS 创建的 VPC 相同的 VPC 中创建一个新子网 10.0.130.0/24。
3. 向此子网的路由表添加路由，以将所有非本地流量定向到上面的 NAT 网关。
4. RDP 到堡垒虚拟机，访问您在上一节中复制的 **Prism Element** 的 URL 并登录。
5. 添加新网络。转到 **设置>网络配置>创建子网**。使用与 AWS 中相同的子网 10.0.130.0/24。
6. 在该新子网中创建所有 VM（AD、CC、VDA 等）。

如果 VM 不需要 Internet 访问

1. RDP 到堡垒 VM，转到您在上一节中复制的 **Prism Element** URL 并登录。
2. 添加新网络。转到 **设置>网络配置>创建子网**。使用子网 10.0.129.0/24。
3. 在该子网中创建所有 VM（AD、CC、VDA 等）。

> **提示：**

> 确保 VM 中的时间和时区信息设置正确。对于 AD 尤其如此。

创建主机连接

1. 在 Web Studio 中，选择左侧窗格中的**托管**。
2. 单击 **添加连接和资源**。
3. 在 **连接** 屏幕上，选择 **创建新连接**，并在 **连接地址** 中输入 `https://xxx.xxx.xxx.xxx:9440`。
4. 按照 UI 完成向导。

> **注意：**
>
> 所有连接器 VM 都必须安装 Nutanix 插件，以便在 Web Studio 中提供 Nutanix 选项，即使这些插件未在 Nutanix 区域中使用。

下一步去哪里

- 如果您处于初始部署过程中，请参阅创建计算机目录
- 有关 Nutanix 的特定信息，请参阅创建 Nutanix 目录

更多信息

- 连接和资源
- Nutanix 虚拟化环境
- Nutanix 云和合作伙伴解决方案

连接到 Oracle C3（预览）

创建和管理连接和资源 一文介绍了通用连接工作流程。以下信息涵盖了 Oracle C3 特有的详细信息。

> **注意：**
>
> 在创建到 Oracle C3 的连接之前，请完成 Oracle C3 环境的设置。请参阅 Oracle C3 虚拟化环境。

创建连接

您可以使用以下方式创建到 Oracle C3 的连接：

- Web 工作室
- PowerShell 命令

使用 WEB STUDIO 创建连接

1. 在**添加连接和资源**中，选择 **Oracle C3** 作为连接类型。
2. 在 **Oracle Compute Cloud@Customer 配置**下，选择**导入配置**，然后粘贴 Oracle C3 配置文件 (`.ini`) 的内容。
3. 在**私钥**下，选择**添加密钥**，然后粘贴凭据文件 (`.pem`) 中的私钥内容。
4. 输入一个易于识别的**连接名称**。
5. 继续向导并验证连接。

> **注意：**
>
> **服务帐户 ID** 是从导入的配置中提取的，无法在 Web Studio 中直接编辑。Oracle C3 端点也从导入配置中的 `region` 值派生，无法在此流程中手动输入。以 Oracle C3 格式输入 `region` 作为 `<service_name>.<domain_name>`（FQDN 样式值）。

> 当您在 Web Studio 中导入配置时，仅导入以下密钥。所有其他密钥都将被忽略：

- `user`
- `fingerprint`
- `tenancy`
- `region`

在以下证书场景中，连接设置可能会停止：

- 证书验证或指纹验证失败：连接创建将被阻止，直到问题解决。

使用 POWERSHELL 命令创建连接

使用 PowerShell 创建连接时，请提供：

- Oracle C3 端点地址，通常为 `https://iaas.<service_name>.<domain_name>`。
- 配置文件的 Oracle C3 用户 OCID (`user`)。

- 凭据文件 (`.pem`) 中的私钥内容，以安全字符串形式传递。
- 包含 `TenancyOcid`、`Fingerprint` 和 `Region` 的 `CustomProperties` XML。
- 用于证书信任验证的 SSL 指纹，如果需要。

示例模式：

```
$CustomProperties = '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">' +



'<Property xsi:type="StringProperty" Name="TenancyOcid" Value="' +
$TenancyOcid + '" />' +



'<Property xsi:type="StringProperty" Name="Fingerprint" Value="' +
$Fingerprint + '" />' +



'<Property xsi:type="StringProperty" Name="Region" Value="' + $Region +
'" />' +



'</CustomProperties>'



$PrivateKey = ConvertTo-SecureString $PrivateKeyContent -AsPlainText
-Force



New-Item -ConnectionType "Custom" `



-HypervisorAddress $Endpoint `
```

```
-Path @("XDHyp:\Connections\$ConnectionName") `

-Persist `

-PluginId "OracleC3PluginFactory" `

-CustomProperties $CustomProperties `

-SecurePassword $PrivateKey `

-UserName $UserOcid `

-SslThumbprint $SslThumbprint
```

注意：

将 `$Region` 设置为 `<service_name>.<domain_name>` 格式的 Oracle C3 区域值。如果您的证书信任策略要求，请使用 `-SslThumbprint`。

证书和指纹验证

要成功连接 Oracle C3，证书验证必须成功，并且在需要时指纹值必须正确。

管理连接

本节内容包括：

- 使用 Web Studio 修复证书问题
- 使用 PowerShell 更新指纹值

修复证书问题

当出现证书问题时，Citrix 会阻止 Oracle C3 连接以保护工作负载操作。在“**主机连接**”列表中，连接旁边会显示一个错误图标。

要修复：

1. 从“**主机连接**”打开连接。
2. 查看**故障排除**详细信息并识别证书问题。
3. 选择**编辑连接 > 编辑设置**。
4. 对于 Oracle C3，如果出现提示，请重新导入配置和私钥。当两者都可用时，保存更改以触发新一轮的证书验证（与连接创建期间相同），并在出现时验证/信任更新的证书指纹。

更新指纹值

创建后，您可以使用 `Set-Item` 更新指纹值。

1. 获取连接详细信息。

```
Get-Item -LiteralPath xdhyp:\connections\<OracleC3ConnectionName>
```

2. 更新指纹值。

```
Set-Item -LiteralPath xdhyp:\connections\<OracleC3ConnectionName> `


-Username <UserName> `


-SslThumbprint <ThumbprintValue>
```

3. 验证更新后的值：

```
Get-Item -LiteralPath xdhyp:\connections\<OracleC3ConnectionName>
```

> **注意：**
>
> 如果提供的指纹不正确或与服务器证书信任不匹配，则更新失败。

下一步操作

- 如果您处于初始部署过程中，请参阅创建计算机目录
- 有关 Oracle C3 的具体信息，请参阅创建 Oracle C3 计算机目录

更多信息

- 创建和管理连接与资源
- Oracle C3 虚拟化环境

连接到 Red Hat OpenShift

(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections.html) 介绍了创建连接的向导。以下信息涵盖了 Red Hat OpenShift 的具体详细信息。

> **注意：**
>
> 在创建与 Red Hat OpenShift 的连接之前，您需要先完成 Red Hat OpenShift 的设置。请参阅 Red Hat OpenShift 虚拟化环境

创建连接

您可以使用以下方式创建到 Red Hat OpenShift 群集的连接：

- Web 工作室
- (#create-a-connection-using-powershell-commands)

使用 WEB STUDIO 创建连接

1. 在 Web Studio 中，打开 **托管 > 添加连接和资源**。
2. 在“**连接**”页面上，按照以下步骤配置连接：
    a. 选择“**创建新连接**”。
    b. 选择 **Red Hat OpenShift** 作为连接类型。
    c. 在“**连接地址**”字段中，输入 OpenShift 服务器的 IP 地址、主机名或 FQDN。
    d. 输入您的服务帐户令牌和易记的连接名称。

e. 在 **Zone name** 字段中选择一个区域。选项是您配置的所有资源位置。

f. 选择**其他工具**以创建虚拟机。

> **注意：**
>
> 选择**其他工具**仅创建托管连接，而不创建托管单元。

3. 单击**下一步**。
4. 如果检测到自签名证书，将显示一个警告页面，其中包含证书指纹。要继续操作：

   a. 将指纹与服务器的指纹进行比较，以验证证书的有效性。

   b. 如果有效，请选择**信任证书**并单击**确定**以完成连接设置。

   该证书被标记为受信任，并且指纹已保存以供将来验证。

5. 在“**范围**”页面上，为此主机选择一个或多个范围。
6. 在“**摘要**”页面上，检查配置，然后单击“**完成**”。

使用 POWERSHELL 命令创建连接

使用 PowerShell 命令创建连接时，请提供以下信息：

- 托管连接名称
- 群集 API 地址
- 用户名
- 密码（服务帐户令牌）
- SSLThumbprint：这是 CA 证书指纹，而不是 API 服务器指纹。如果您尝试创建托管连接时未指定指纹，服务器会提供 CA 证书指纹。
- ZoneUid

1. 打开 PowerShell 窗口。
2. 运行 `add-pssnapin citrix®*`。
3. 运行以下命令以创建托管连接。

   如果您尝试创建托管连接时未指定指纹，则服务器会提供 CA 证书指纹。例如：

```
$newItemParameters = @{

ConnectionType= "Custom"

PluginId= "OpenShiftPluginFactory"

HypervisorAddress = "https://
api.myopenshiftclusteraddress.mydomain.local:6443"

Path= "XDHyp:\Connections\OpenShiftConnectionName"

Persist= $true

UserName= "__ServiceAccount__"

Password= "<service account token>"

ErrorVariable= "connectionError"

 }



& New-Item @newItemParameters




$newItemParameters["SSLThumbprint"] =
$connectionError[0].ErrorData.Thumbprint

$connection = & New-Item @newItemParameters

$brokerConnection = New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $connection.HypervisorConnectionUid
```

创建托管单元

托管单元表示创建 VM 的环境。要创建托管单元，您需要 OpenShift 中的以下输入：

- 命名空间
- 存储类

- 网络附件定义

托管单元是命名空间绑定的。这意味着一个托管单元只能访问一个命名空间并管理该命名空间下的 VM。

您可以使用以下方式创建托管单元：

- Web 工作室
- PowerShell

使用 WEB STUDIO 创建托管单元

1. 导航到 **托管 > 添加连接和资源**。
2. 在 **Connection** 页面上：
   - 要创建新的托管连接以及一个托管单元，请选择**创建新连接**，然后执行以下操作：
     a. 选择 **Red Hat OpenShift** 作为连接类型。
     b. 在“**连接地址**”字段中，输入 OpenShift 服务器的 IP 地址、主机名或 FQDN。
     c. 输入您的服务帐户令牌和易记的连接名称。
     d. 在 **Zone name** 字段中选择一个区域。选项是您配置的所有资源位置。
     e. 选择 **Citrix 预配工具（Machine Creation Services™ 或 Citrix Provisioning）用于创建虚拟机**。
     f. 单击**下一步**。
     g. 在**警告**页面上，验证证书的有效性，并选择**信任证书**。
   - 要从现有主机连接创建托管单元，请选择**使用现有连接**，然后选择相关连接。
3. 在**命名空间选择**页面上，为此连接选择一个命名空间。
4. 在“**存储选择**”页面上，为每种支持的数据类型选择至少一个存储设备，然后才能继续向导中的下一页。有关存储选择的更多信息，请参阅主机存储。
5. 在“**网络**”页面上，输入资源的名称。此名称将显示在 Studio 中，用于标识与连接关联的存储和网络组合。选择虚拟机使用的一个或多个网络。
6. 在“**摘要**”页面上，检查详细信息，然后单击“**完成**”。

使用 POWERSHELL 创建托管单元

使用 PowerShell 命令创建托管单元时，请提供以下信息：

- 托管连接名称

- 托管单元名称
- 目标命名空间名称
- StorageClasses 名称
- NetworkAttachmentDefinition 名称

1. 打开 PowerShell 窗口。
2. 运行 `add-pssnapin citrix*`。
3. 运行 PowerShell 命令以创建托管单元。例如：

```
$HostingConnectionName = "OpenShiftConnectionName"

$HostingUnitName = "HostingUnitName"

$TargetNamespace = "TargetNamespaceName"

$StorageClassToUse = "YourStorageClassesName"

$NetworkAttachmentDefinition = "YourNetworkAttachmentDefinitionName"

New-HypStorage `

-StoragePath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$StorageClassToUse.storage") `

-StorageType "TemporaryStorage"

New-Item `

-CustomProperties "" `

-HypervisorConnectionName $HostingConnectionName `

-NetworkPath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$NetworkAttachmentDefinition.network") `

-Path @("XDHyp:\HostingUnits\$HostingUnitName") -RootPath "XDHyp:
\Connections\$HostingConnectionName\$TargetNamespace.namespace" `

-StoragePath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$StorageClassToUse.storage")
```

后续步骤

- 如果您处于初始部署过程中，请参阅创建计算机目录
- 有关 Red Hat OpenShift 的特定信息，请参阅 创建 Red Hat OpenShift 目录

更多信息

- 连接和资源
- 创建计算机目录

连接到 VMware

创建和管理连接和资源 介绍了创建连接的向导。以下信息涵盖了 VMware 虚拟化环境特有的详细信息。

> **注意：**
>
> 在创建到 VMware 的连接之前，您需要首先完成将 VMware 帐户设置为资源位置。请参阅 VMware 虚拟化环境。

创建连接

在连接创建向导中：

1. 选择 VMware 连接类型。
2. 指定 vCenter SDK 访问点的地址。
3. 指定您之前设置的具有创建 VM 权限的 VMware 用户帐户的凭据。以 domain/username 形式指定用户名。

VMware SSL 指纹

VMware SSL 指纹功能消除了手动创建到 VMware vSphere 管理程序的宿主机连接的需要。在创建连接之前，不再需要手动在站点中的 Delivery Controller 与管理程序证书之间创建信任关系。

VMware SSL 指纹功能将不受信任证书的指纹存储在站点数据库中。此配置可确保即使控制器不信任管理程序，Citrix Virtual Apps and Desktops™ 也能持续将其识别为受信任的。

在 Studio 中创建 vSphere 宿主机连接时，对话框允许您查看要连接的计算机的证书。然后，您可以选择是否信任它。

所需权限

创建一个 VMware 用户帐户和一个或多个 VMware 角色，其中包含本文中列出的一组或所有权限。角色的创建应基于用户权限所需的特定粒度级别，以便随时请求各种 Citrix DaaS™ 操作。要在任何时候授予用户特定权限，请将其与相应的角色关联，至少在数据中心级别，并选中“**传播到子项**”选项。但是，对于 `StorageProfile` 权限和特定的 `Tags` 权限，请在 Root vCenter Server 级别应用权限，而不选中“**传播到子项**”。请参阅每个表中的注释。

下表显示了 Citrix Virtual Apps and Desktops™ 操作与最低所需 VMware 权限之间的映射。

> **注意：**
>
> 权限列表显示名称，特别是 *User Interface*，在某些 vSphere 版本中有所不同。例如，在 vSphere 6.7 中，*User Interface* 权限是 **Change Memory** 和 **Change Settings**，而不是本页所述的所需权限中的 **Settings** 和 **Memory**。

添加连接和资源

SDK	用户界面
系统.匿名、系统.读取和系统.查看	自动添加。可以使用内置的只读角色。

电源管理

SDK	用户界面
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭电源
VirtualMachine.Interact.PowerOn	虚拟机 > 交互 > 开启电源
VirtualMachine.Interact.Reset	虚拟机 > 交互 > 重置
VirtualMachine.Interact.Suspend	虚拟机 > 交互 > 暂停
Datastore.Browse	数据存储 > 浏览数据存储

预配计算机 (MACHINE CREATION SERVICES™)

要使用 MCS 预配计算机，需要以下权限：

SDK	用户界面
Datastore.AllocateSpace	数据存储 > 分配空间
Datastore.Browse	数据存储 > 浏览数据存储
Datastore.FileManagement	数据存储 > 低级别文件操作
Network.Assign	网络 > 分配网络
Resource.AssignVMToPool	资源 > 将虚拟机分配到资源池
VirtualMachine.Config.AddExistingDisk	虚拟机 > 配置 > 添加现有磁盘
VirtualMachine.Config.AddNewDisk	虚拟机 > 配置 > 添加新磁盘
虚拟机.配置.添加或移除设备	虚拟机 > 配置 > 添加或移除设备
VirtualMachine.Config.AdvancedConfig	虚拟机 > 配置 > 高级
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 移除磁盘
VirtualMachine.Config.CPUCount	虚拟机 > 配置 > 更改 CPU 计数
VirtualMachine.Config.Memory	虚拟机 > 配置 > 更改内存
VirtualMachine.Config.Settings	虚拟机 > 配置 > 更改设置
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭电源
VirtualMachine.Interact.PowerOn	虚拟机 > 交互 > 打开电源
VirtualMachine.Interact.Reset	虚拟机 > 交互 > 重置
VirtualMachine.Interact.Suspend	虚拟机 > 交互 > 暂停
VirtualMachine.Inventory.CreateFromExisting	虚拟机 > 清单 > 从现有创建
VirtualMachine.Inventory.Create	虚拟机 > 清单 > 创建新项
VirtualMachine.Inventory.Delete	虚拟机 > 清单 > 移除
VirtualMachine.Provisioning.Clone	虚拟机 > 置备 > 克隆虚拟机

SDK	用户界面
VirtualMachine.State.CreateSnapshot	vSphere 5.0 Update 2、vSphere 5.1 Update 1 和 vSphere 6.x Update 1：虚拟机 > 状态 > 创建快照；vSphere 5.5：虚拟机 > 快照管理 > 创建快照
VirtualMachine.Config.Rename	虚拟机 > 配置 > 重命名

映像更新和回滚

SDK	用户界面
Datastore.AllocateSpace	数据存储 > 分配空间
Datastore.Browse	数据存储 > 浏览数据存储
Datastore.FileManagement	数据存储 > 低级别文件操作
Network.Assign	网络 > 分配网络
Resource.AssignVMToPool	资源 > 将虚拟机分配到资源池
VirtualMachine.Config.AddExistingDisk	虚拟机 > 配置 > 添加现有磁盘
VirtualMachine.Config.AddNewDisk	虚拟机 > 配置 > 添加新磁盘
VirtualMachine.Config.AdvancedConfig	虚拟机 > 配置 > 高级
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 移除磁盘
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭电源
VirtualMachine.Interact.PowerOn	虚拟机 > 交互 > 开机
VirtualMachine.Interact.Reset	虚拟机 > 交互 > 重置
VirtualMachine.Inventory.CreateFromExisting	虚拟机 > 清单 > 从现有创建
VirtualMachine.Inventory.Create	虚拟机 > 清单 > 创建新项
VirtualMachine.Inventory.Delete	虚拟机 > 清单 > 移除
VirtualMachine.Provisioning.Clone	虚拟机 > 置备 > 克隆虚拟机

共享准备好的映像

要跨不同的主机连接共享准备好的映像，目标主机连接需要以下强制性权限：

SDK	用户界面
Datastore.AllocateSpace	数据存储 > 分配空间
Network.Assign	网络 > 分配网络
Resource.AssignVMToPool	资源 > 将虚拟机分配到资源池
VirtualMachine.Config.添加或移除设备	虚拟机 > 配置 > 添加或移除设备
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 移除磁盘
VirtualMachine.Config.Settings	虚拟机 > 配置 > 更改设置
VirtualMachine.Inventory.Register	虚拟机 > 清单 > 注册
VirtualMachine.Inventory.Delete	虚拟机 > 清单 > 移除

删除预配的计算机

SDK	用户界面
Datastore.Browse	数据存储 > 浏览数据存储
Datastore.FileManagement	数据存储 > 低级别文件操作
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 移除磁盘
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭电源
VirtualMachine.Inventory.Delete	虚拟机 > 清单 > 移除

存储配置文件

在 vSAN 或 vVol 数据存储上创建目录期间，要查看、创建或删除存储策略，需要以下权限：

SDK	用户界面
StorageProfile.Update	配置文件驱动的存储 > 配置文件驱动的存储更新。对于 vSphere 8：VM 存储策略 > 更新 VM 存储策略

SDK	用户界面
StorageProfile.View	配置文件驱动的存储 > 配置文件驱动的存储视图。对于 vSphere 8：VM 存储策略 > 查看 VM 存储策略

注意：

在根 vCenter Server 级别应用存储配置文件权限，不勾选 **传播到子对象**。

标签和自定义属性

标签和自定义属性允许您将元数据附加到在 vSphere 清单中创建的 VM，从而更轻松地搜索和筛选这些对象。要创建、编辑、分配和删除标签或类别，需要以下权限：

SDK	用户界面
InventoryService.Tagging.CreateTag	vSphere 标记 > 创建 vSphere 标记
清单服务.标记.创建类别	vSphere 标记 > 创建 vSphere 标记类别
清单服务.标记.编辑标记	vSphere 标记 > 编辑 vSphere 标记
清单服务.标记.编辑类别	vSphere 标记 > 编辑 vSphere 标记类别
清单服务.标记.删除标记	vSphere 标记 > 删除 vSphere 标记
清单服务.标记.删除类别	vSphere 标记 > 删除 vSphere 标记类别
清单服务.标记.附加标记	vSphere 标记 > 分配或取消分配 vSphere 标记
清单服务.标记.对象可附加	vSphere 标记 > 在对象上分配或取消分配 vSphere 标记
全局.管理自定义字段	全局 > 管理自定义属性
Global.SetCustomField	全局 > 设置自定义属性

注意：

- 当 MCS 创建计算机目录时，它会使用特殊名称标签标记目标 VM。这些标签将主映像与 MCS 创建的 VM 区分开来，并防止将 MCS 创建的 VM 用于映像准备。您可以通过 vCenter 中 `XdProvisioned` 属性的值来识别差异。如果 MCS 创建 VM，则该属性设置为 **True**。
- 在根 vCenter Server 级别应用 `InventoryService.Tagging.AttachTag` 权限，不勾选**传播到子对象**。

加密操作

加密操作权限控制谁可以在哪种类型的对象上执行哪种类型的加密操作。vSphere Native Key Provider 使用 `Cryptographer.*` 权限。加密操作需要以下最低权限：

注意：

使用配备 vTPM 的 VM 创建 MCS 计算机目录需要这些权限。

SDK	用户界面
Cryptographer.Access	权限 > 所有权限 > 加密操作 > 直接访问
Cryptographer.AddDisk	权限 > 所有权限 > 加密操作 > 添加磁盘
Cryptographer.Clone	权限 > 所有权限 > 加密操作 > 克隆
Cryptographer.Encrypt	权限 > 所有权限 > 加密操作 > 加密
Cryptographer.EncryptNew	权限 > 所有权限 > 加密操作 > 加密新
Cryptographer.Decrypt	权限 > 所有权限 > 加密操作 > 解密
Cryptographer.Migrate	权限 > 所有权限 > 加密操作 > 迁移
Cryptographer.ReadKeyServersInfo	权限 > 所有权限 > 加密操作 > 读取 KMS 信息

预配计算机 (CITRIX PROVISIONING™)

使用 Citrix Virtual Apps and Desktops 安装向导和导出设备向导通过 Citrix Provisioning 控制台预配 VM 需要克隆和部署模板的这些权限。在创建主机连接时设置权限。您需要预配计算机（Machine Creation Services）中的所有权限以及以下权限。

SDK	用户界面
VirtualMachine.Config.AddRemoveDevice	虚拟机 > 配置 > 添加或移除设备
VirtualMachine.Config.CPUCount	虚拟机 > 配置 > 更改 CPU 计数
VirtualMachine.Config.Memory	虚拟机 > 配置 > 内存
VirtualMachine.Config.Settings	虚拟机 > 配置 > 设置
VirtualMachine.Provisioning.CloneTemplate	虚拟机 > 预配 > 克隆模板
VirtualMachine.Provisioning.DeployTemplate	虚拟机 > 预配 > 部署模板
VApp.Export	vApp > 导出

> **注意：**
>
> `VApp.Export` 是使用计算机配置文件创建 MCS 计算机目录所必需的。

获取并导入证书

为保护 vSphere 通信，Citrix® 建议您使用 HTTPS 而非 HTTP。

HTTPS 需要数字证书。请使用由符合贵组织安全策略的证书颁发机构颁发的数字证书。

如果无法使用由证书颁发机构颁发的数字证书，则可以使用 VMware 安装的自签名证书。仅当贵组织的安全策略允许时才使用此方法。将 VMware vCenter 证书添加到每个 Delivery Controller。

1. 将运行 vCenter Server 的计算机的完全限定域名 (FQDN) 添加到该服务器上的 hosts 文件中，位置为 `%SystemRoot%/WINDOWS/system32/Drivers/etc/`。仅当运行 vCenter Server 的计算机的 FQDN 尚未存在于域名系统中时，才需要执行此步骤。
2. 使用以下三种方法之一获取 vCenter 证书：

   从 vCenter 服务器。

a. 将文件 rui.crt 从 vCenter 服务器复制到 Delivery Controller 上可访问的位置。

b. 在 Controller 上，导航到导出证书的位置并打开 rui.crt 文件。

使用 Web 浏览器下载证书。 如果您使用的是 Internet Explorer，请右键单击 Internet Explorer 并选择**以管理员身份运行**以下载或安装证书。

a. 打开您的 Web 浏览器，并与 vCenter 服务器建立安全的 Web 连接（例如 `<https://server1.domain1.com)>`）。

b. 接受安全警告。

c. 单击显示证书错误的地址栏。

d. 查看证书并单击“详细信息”选项卡。

e. 选择**复制到文件并以 .CER 格式导出**，并在出现提示时提供名称。

f. 保存导出的证书。

g. 导航到导出的证书位置并打开 .CER 文件。

以管理员身份运行 Internet Explorer 直接导入。

- 打开您的 Web 浏览器，并与 vCenter 服务器建立安全的 Web 连接（例如 `<https://server1.domain1.com)>`）。
- 接受安全警告。
- 单击显示证书错误的地址栏。
- 查看证书。

3. 将证书导入到每个 Controller 上的证书存储中。

a. 单击**安装证书**选项，选择**本地计算机**，然后单击**下一步**。

b. 选择**将所有证书放入以下存储**，然后单击**浏览**。选择**受信任的人**，然后单击**确定**。单击**下一步**，然后单击**完成**。

如果在安装后更改 vSphere 服务器的名称，则必须在该服务器上生成新的自签名证书，然后才能导入新证书。

下一步操作

- 如果您处于初始部署过程中，请参阅创建计算机目录
- 有关 VMware 的特定信息，请参阅 创建 VMware 目录

更多信息

- 连接和资源
- 创建计算机目录

连接到 VMware 云和合作伙伴解决方案

在设置 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-prepare/vmware-cloud-partner-solutions.html#azure-vmware-solution-avs-integration)、(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-prepare/vmware-cloud-partner-solutions.html#google-cloud-vmware-engine) 和 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/install-prepare/vmware-cloud-partner-solutions.html#vmware-cloud-on-amazon-web-services-aws) 之后，创建连接。有关创建连接的信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections/connection-vmware-virtualization-environments.html)。

下一步操作

- 如果您处于初始部署过程中，请参阅创建计算机目录
- 有关 VMware 的特定信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-create/create-machine-catalog-vmware.html)

更多信息

- 连接和资源
- 创建计算机目录

用于计算机身份管理的服务账户

服务帐户是存储凭据的容器，配置后可用于在无需用户交互的情况下执行与计算机身份相关的操作。在需要计算机身份管理权限的操作之前创建服务帐户。

您可以将 MCS 计算机目录配置为使用服务帐户来执行以下操作：

- 在 Active Directory 中创建或删除计算机帐户，而无需每次都输入域凭据。
- 管理过时的 Microsoft Entra 加入或 Microsoft Intune 注册设备，而无需通过 Microsoft Entra ID 或 Intune 门户手动删除它们。

支持的服务帐户类型

Citrix® 允许基于身份提供商的类型创建以下服务账户。

身份提供程序类型	描述	凭据
本地 Active Directory 服务帐户	管理计算机目录和计算机帐户，而无需每次都输入域凭据。	本地 Active Directory 用户帐户的用户名和密码。

凭据保护

Citrix 将服务账户凭据存储在客户的站点数据库中。在 Citrix Virtual Apps and Desktops 部署中，站点数据库是每个租户（客户）的数据库，并且只能由为客户运行的服务访问。

还强制执行以下操作以保护存储的凭据：

- 凭据在存储到数据库之前使用 **AES 256** 加密。
- 加密密钥是按站点生成的，并本地存储在 Delivery Controller™ 中，只能由专用于客户的服务访问。
- 数据库连接使用 TLS 1.2 协议加密。

本地 Active Directory 服务帐户

本地 Active Directory 服务帐户是一个容器，用于存储特权域用户帐户的用户名和密码。该用户帐户必须具有足够的权限，才能在 Active Directory 中管理计算机帐户。机器创建服务可以使用此服务帐户执行与计算机帐户相关的操作，而无需每次输入域凭据。

创建本地 Active Directory 服务帐户

使用 Studio 或 PowerShell 创建本地 Active Directory 服务帐户。

先决条件

要创建本地 Active Directory 服务帐户，请务必完成以下任务：

- 在您的 Active Directory 中创建一个域用户帐户，该帐户具有足够的权限，可以在您的 Active Directory 或特定 OU 中创建、更新和删除计算机对象。

使用 WEB STUDIO

1. 在左侧窗格中，选择 **管理员**。
2. 在 **服务帐户** 选项卡中，单击 **创建服务帐户**。
3. 在 **身份类型** 页面上，选择 **本地 Active Directory**。单击 **下一步**。
4. 在 **凭据** 页面上，单击 **输入凭据**，以提供您希望用作服务帐户的特权域用户帐户的用户名和密码。
5. 设置密码过期日期，或将其设置为永不过期。

6. 为此服务帐户选择一个或多个范围。
7. 为服务帐户输入一个友好名称和描述（可选）。
8. 单击 **完成** 以完成创建。

使用 POWERSHELL

您可以使用 PowerShell 命令创建本地 Active Directory 服务。例如：

```
$credential = ConvertTo-SecureString -String $password -AsPlainText -Force

New-AcctServiceAccount -IdentityProviderType ActiveDirectory
-IdentityProviderIdentifier test.local -AccountId test\svcacct_mcs
-AccountSecret $credential -SecretExpiryTime 2030/08/15 -DisplayName
'scvacct_mcs' -Description 'Service account for test.local'
```

注意：

`$password` 是所提供的域用户帐户的匹配密码。

执行计算机身份相关操作

将 Active Directory 或基于 Microsoft Entra 混合的身份池与服务帐户关联后，您可以执行各种计算机身份相关操作，而无需输入域凭据。

- 使用服务帐户创建新的身份帐户

  ```
  New-AcctADAccount -IdentityPoolName MyPool -Count 2 -UseServiceAccount
  ```

- 使用服务帐户修复身份帐户

  ```
  Repair-AcctADAccount -ADAccountName "Domain\account","Domain\account2"
  -UseServiceAccount
  ```

- 使用服务帐户删除身份帐户

  ```
  Remove-AcctADAccount -IdentityPoolName MyPool -RemovalOption Delete
  -ADAccountName "Domain\account","domain\account2" -UserServiceAccount
  ```

下一步

- 要创建本地 Active Directory 加入的目录，请参阅本地 Active Directory 加入的计算机身份的身份池)。
- 要管理服务帐户，请参阅管理服务帐户。

管理服务帐户

管理服务帐户是确保其保持正常状态且凭据为最新状态的关键方面。本文介绍了查看、重命名、编辑、测试和删除服务帐户的步骤。

查看服务帐户详细信息

1. 在左侧窗格中，选择 **管理员**。
2. 选择“**服务帐户**”选项卡。
3. 选择一个服务帐户，并在下方面板中查看其详细信息。在下方面板中查看每个服务帐户的属性以及其关联的计算机目录和故障排除提示。

如果出现以下情况，服务帐户旁边会显示错误或警告图标：

- 服务帐户处于不正常状态。
- 服务帐户的凭据即将到期。

“**故障排除**”选项卡提供诊断和修复问题的信息。

> **注意：**
>
> 修复问题后，执行服务帐户测试以刷新状态。有关详细信息，请参阅测试服务帐户。

重命名服务

1. 在左侧窗格中，选择 **管理员**。
2. 选择“**服务帐户**”选项卡。
3. 选择一个服务帐户，然后单击“**重命名**”。

编辑服务帐户

1. 在左侧窗格中，选择 **管理员**。
2. 选择“**服务帐户**”选项卡。
3. 选择一个服务账户，然后点击**编辑**。

测试服务账户

1. 在左侧窗格中，选择 **管理员**。
2. 选择**服务账户**选项卡。
3. 选择一个服务账户，然后点击**测试服务账户**。

- 对于本地 Active Directory 服务账户，凭据会在测试期间进行验证。
- 对于 Microsoft Entra 服务账户，应用程序 ID 和密钥以及所需的权限会在测试期间进行验证。

根据建议识别并修复问题。**故障排除**选项卡提供诊断和修复问题的信息。修复问题后，测试服务账户。

删除服务账户

在删除服务账户之前，请确保该服务账户未被任何 MCS 计算机目录使用。

1. 在左侧窗格中，选择 **管理员**。
2. 选择**服务账户**选项卡。
3. 选择一个服务账户，然后点击**删除**。

映像管理

简介

MCS 目录创建或更新过程分为两个阶段：

- 主映像创建：将源映像转换为已发布的映像
- 克隆：从已发布的映像创建新的 VM

借助映像管理功能，MCS 将主映像创建阶段与整个预配工作流分开。

您可以从单个源映像准备各种 MCS 映像版本 (准备好的映像)，并在多个不同的 MCS 计算机目录中使用。您还可以在托管单元之间共享准备好的映像版本。此实现显著降低了存储和时间成本，并简化了 VM 部署和映像更新过程。

使用此映像管理功能的好处包括：

- 无需创建目录即可提前生成准备好的映像。
- 在多种场景中重复使用准备好的映像，例如创建和更新目录。
- 显著缩短目录创建或更新时间。
- 在托管单元之间共享准备好的映像版本：

- 对于 Azure 和 VMware，映像版本可以在相同连接类型的主机连接之间共享。
- 对于 Amazon WorkSpaces Core 托管实例，映像版本可以在同一 AWS 区域内或不同区域中，跨绑定到不同托管单元的不同可用区共享。
- 对于 AWS EC2，映像版本可以在同一 AWS 区域内，跨绑定到不同托管单元的不同可用区共享。
- 对于 XenServer，映像版本只能在同一主机连接中的托管单元之间共享。

注意：

- 此功能目前适用于 Amazon WorkSpaces Core 托管实例、Azure 本地、AWS EC2、Azure、Red Hat OpenShift、VMware 虚拟化和 XenServer 环境。
- 您可以不使用准备好的映像来创建 MCS 计算机目录。在这种情况下，您无法获得该功能的优势。但是，对于 Amazon WorkSpaces Core Managed Instances，只能使用准备好的映像版本创建 MCS 目录。您不能直接使用主映像创建目录。

用例

映像管理功能的一些用例如下：

- *版本管理*：映像版本允许您：
  - 管理特定映像的不同迭代或更新。
  - 维护映像的多个版本以用于不同目的。
- *逻辑分组*：您可以创建多个映像定义以：
  - 根据项目、部门或应用程序和桌面类型等各种条件对映像版本进行逻辑分组。
  - 在组织内更高效地管理映像。
- *映像共享*：您可以在相同连接类型的主机连接中的托管单元之间共享准备好的映像版本，以：
  - 确保不同托管单元之间映像的一致性和统一性。

什么是准备好的映像?

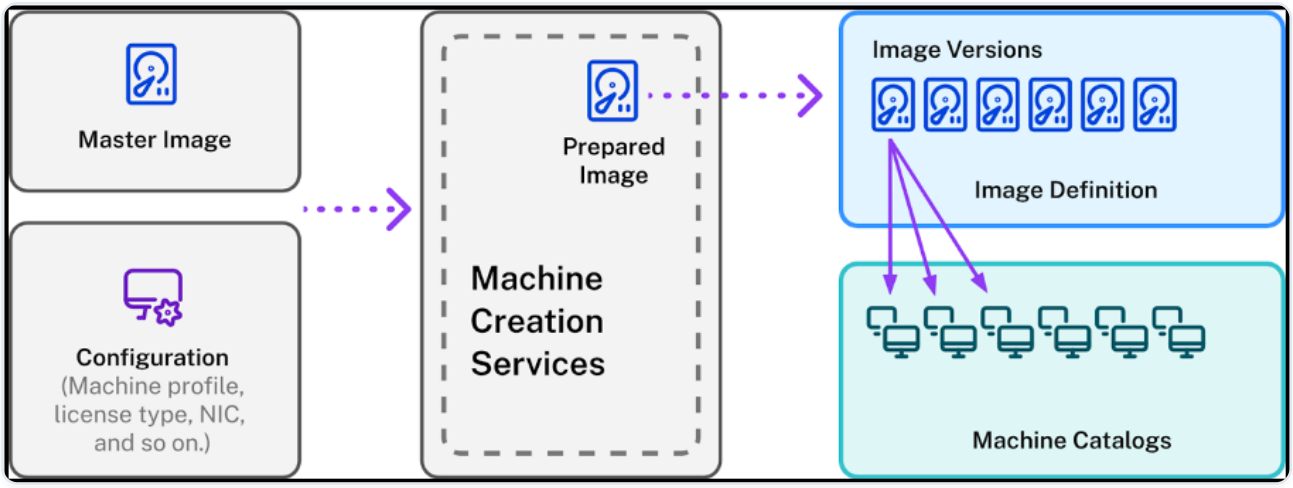
借助映像管理功能，MCS 将主映像阶段从整体目录创建或更新工作流中解耦，并将此过程分解为两个阶段：

1. 从单个源映像创建准备好的映像。

2. 使用准备好的映像创建或更新 MCS 计算机目录。

您可以提前创建准备好的映像。您可以使用单个准备好的映像创建或更新多个 MCS 预配的计算机目录。

了解当您从映像使用 Web Studio 时，准备好的映像如何在多个 MCS 计算机目录中使用的过程：



映像定义：映像定义是映像版本的逻辑分组。映像定义包含以下信息：

- 创建映像的原因
- 映像适用的操作系统
- 有关使用映像的其他信息。

目录不是从映像定义创建的，而是从基于映像定义创建的映像版本创建的。

映像版本：映像版本管理映像定义的版本控制。一个映像定义可以有多个映像版本。使用映像版本作为准备好的映像来创建或更新目录。

- 对于 Azure 和 VMware，映像版本可以在相同连接类型的主机连接之间共享。
- 对于 Amazon WorkSpaces Core 托管实例，映像版本可以在同一 AWS 区域内或不同区域的不同可用区之间共享，并与不同的托管单元关联。
- 对于 AWS EC2，映像版本可以在同一 AWS 区域内跨不同的可用区共享，并绑定到不同的托管单元。
- 对于 XenServer，映像版本只能在同一主机连接中的托管单元之间共享。

或者，如果您想使用 PowerShell 命令创建预配方案以创建或更新目录，则必须根据主映像版本规范创建准备好的映像版本规范，以满足您的环境需求。

- 对于 Azure 和 VMware，映像版本可以在相同连接类型的主机连接之间共享。

- 对于 Amazon WorkSpaces Core 托管实例，映像版本可以在同一 AWS 区域内或不同区域的不同可用区之间共享，并与不同的托管单元关联。
- 对于 AWS EC2，映像版本可以在同一 AWS 区域内跨不同的可用区共享，并绑定到不同的托管单元。
- 对于 XenServer，映像版本只能在同一主机连接中的托管单元之间共享。

要求

- 对于 Windows 主映像，仅支持 VDA 映像版本 2311 或更高版本。必须明确选择并安装 MCS/IO 组件。启用或禁用 MCS I/O 配置必须在计算机目录创建或更新期间确定，因为它默认未启用。

限制

当前，此功能不支持以下各项：

- Azure 中的多个 NIC
- 持久性数据磁盘功能
- 多会话休眠
- 映像类型更改
- 在 Azure 中跨托管单元共享准备好的映像版本时，不允许使用以下共享方法：
  - 直接共享
  - 共享到公共社区库

使用 Web Studio 进行映像生命周期管理

使用 Web Studio 时，映像的生命周期为：

1. 创建准备好的映像：创建映像定义及其初始映像版本。
2. 从初始映像版本创建映像版本。
3. 如果需要，与虚拟化环境中的托管单元共享映像版本。
4. 使用映像版本作为准备好的映像来创建目录。
5. 使用不同的准备好的映像更新计算机目录。
6. 管理映像定义和版本：编辑映像版本的名称和描述，以及映像定义的描述。
7. 删除映像版本。
8. 删除映像定义。

或者，您也可以使用 PowerShell 管理映像。请参阅 使用 PowerShell 管理映像生命周期。

使用 PowerShell 管理映像生命周期

如果要使用 PowerShell 命令创建预配方案，则必须根据环境需要，基于主映像版本规范创建准备好的映像版本规范。

主映像版本规范：主映像版本规范是在映像版本下添加或创建的特定映像。您可以将管理程序中的现有映像添加为主映像版本规范，或者根据环境需要，基于主映像版本规范创建准备好的映像版本规范。准备好的映像版本规范可用于多个预配方案。

您可以根据虚拟化环境，在托管单元之间共享映像版本规范：

- 在 Azure、VMware 和 Amazon WorkSpaces Core 托管实例环境中，您可以在托管单元之间共享映像版本规范，无论它们位于相同连接类型的相同或不同主机连接中。在 Azure 中，通过使用 Azure 计算库 (ACG) 的磁盘共享功能实现共享。
- 对于 AWS EC2，映像版本可以在同一 AWS 区域内跨不同的可用区共享，并绑定到不同的托管单元。
- 在 XenServer 中，您只能在同一主机连接内的托管单元之间共享映像版本规范。

使用 PowerShell 命令时，映像的生命周期为：

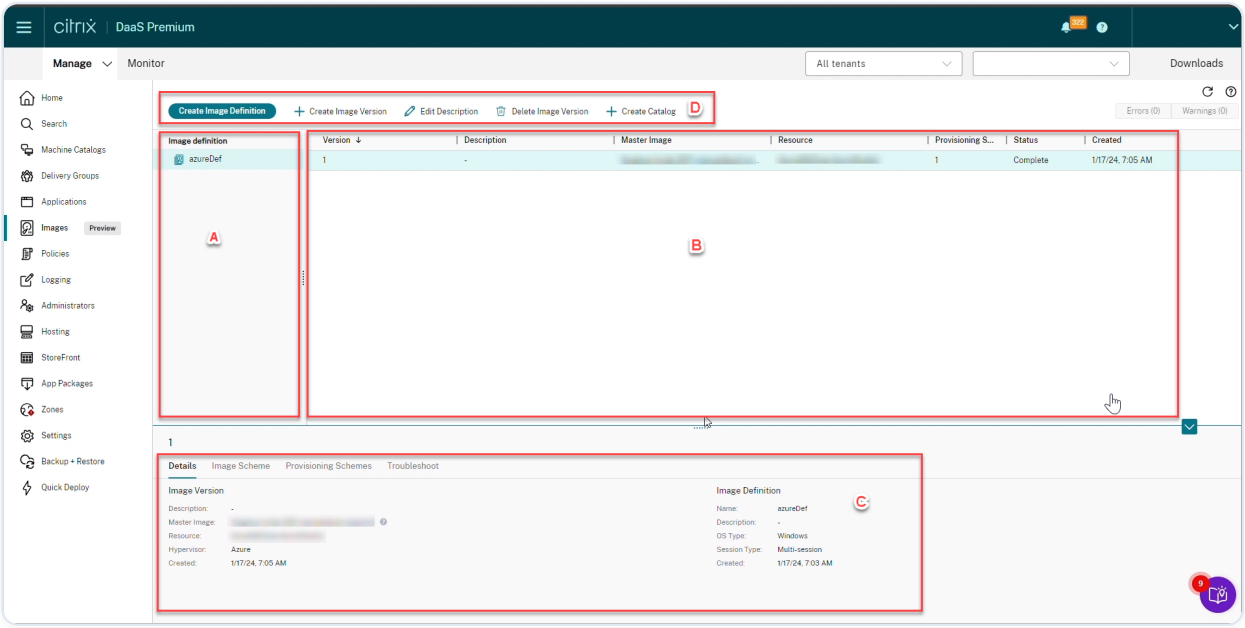
1. 创建映像：
    a. 创建映像定义。
    b. 在指定的托管连接中为映像定义添加新配置。
    c. 创建映像版本。
    d. 添加主映像版本规范。
    e. 创建准备好的映像版本规范。
2. 如果需要，可将映像版本规范与虚拟化环境中的另一个托管单元共享，无论它们是否在同一托管连接中。
3. 使用准备好的映像版本规范创建 MCS 计算机目录：
    a. 创建代理目录。
    b. 创建身份池。
    c. 使用 `New-ProvScheme` 命令创建预配方案，其中包含准备好的映像版本规范 Uid 参数。
    d. 将代理目录与预配方案链接。
4. 在 MCS 计算机目录中创建 VM。
5. 使用 `Set-ProvScheme` 命令更改预配方案的准备好的映像版本规范。

6. 管理映像定义和版本：编辑映像版本和映像定义。
7. 删除 MCS 计算机目录：删除顺序为：计算机目录 > 共享的准备好的映像版本规范（如果共享映像）> 准备好的映像版本规范 > 主映像版本规范 > 映像版本 > 指定托管连接中映像定义的配置 > 映像定义。在删除映像版本规范之前，请确保准备好的映像版本规范未与任何 MCS 计算机目录关联。

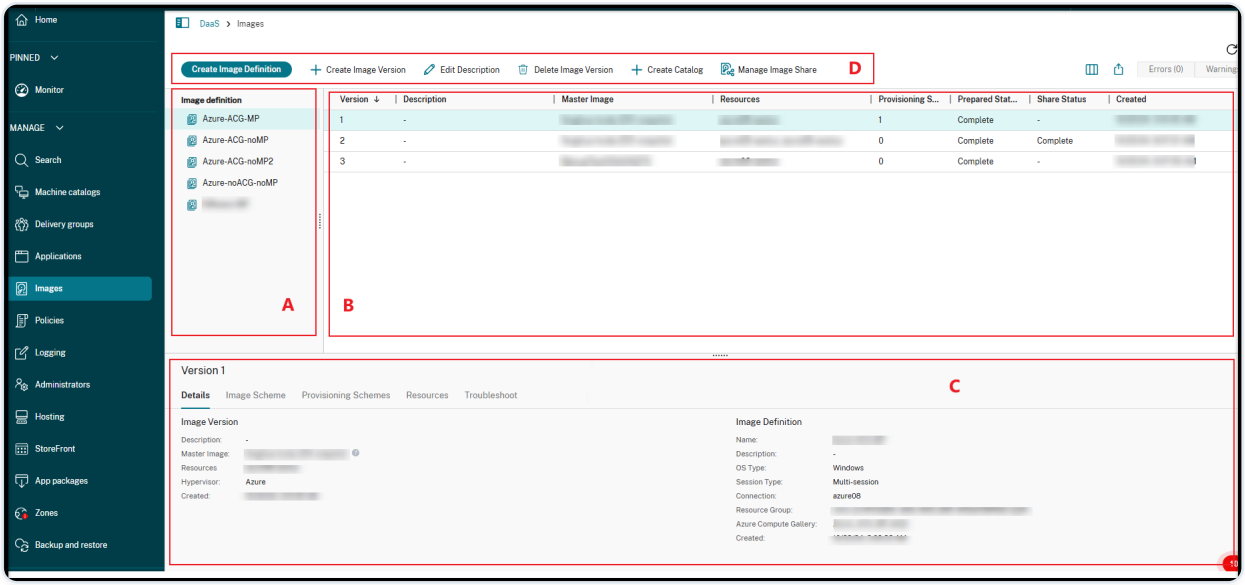
了解“映像”节点

使用“**图像**”节点创建和管理 MCS 准备的图像。其主视图分为四个部分：

- 未跨主机单元共享准备好的图像



- 跨主机单元共享准备好的图像：



标签	部分	描述
A	图像定义	列出以前创建的图像定义。
B	图像版本	显示所选图像定义的图像版本。
C	详细信息	• “**详细信息**”选项卡显示有关所选图像定义或版本的详细信息，例如主映像、资源、虚拟机管理程序、图像定义名称、操作系统类型和会话类型。 • “**图像方案**”选项卡显示有关用于准备图像的模板的信息，例如硬盘、计算机大小、许可证类型、磁盘加密集、计算机配置文件等。 • “**预配方案**”选项卡显示用于创建目录的预配方案名称。 • “**故障排除**”选项卡提供所选映像版本的错误状态。

标签	部分	描述	
		• 在映像共享的情况下：“**资源**”选项卡提供映像版本共享的状态。	
D	操作栏	列出您可以对映像定义和版本执行的操作，例如“**创建映像版本**”、“**编辑描述**”、“**管理映像共享**”（在准备好的映像共享的情况下）、“**删除映像版本**”和“**创建目录**”。	

跨 Azure 订阅或租户共享准备好的映像

若要在 Azure 平台上跨订阅或租户共享准备好的映像，请遵循以下示例：

- **服务主体**：SPN 1
- **订阅**：订阅 1
- **租户**：Tenant 1

您希望与以下对象共享此映像：

- **服务主体**：SPN 2
- **订阅**：订阅 2
- **租户**：Tenant 2（可以与 Tenant 1 相同）

要成功共享和使用映像，您必须在 **Subscription 1** 中（在库、资源组或订阅范围）向 SPN 2 授予以下权限：

- `Microsoft.Resources/subscriptions/read`
- `Microsoft.Compute/galleries/images/read`
- `Microsoft.Compute/galleries/images/versions/read`

> **注意：**

> 对订阅或资源具有任何权限的任何服务主体都会自动继承 `Microsoft.Resources/subscriptions/read` 权限。

或者，将内置角色 **Compute Gallery Image Reader** 分配给 **SPN 2**。

有关分步指导，请参阅此Microsoft 文章。

下一步操作

- 创建准备好的映像计算机目录
  - 为 Amazon WorkSpaces Core 托管实例创建准备好的映像
  - 创建 Amazon WorkSpaces Core 托管实例目录
  - 在 Azure 中创建准备好的映像计算机目录
  - 在 VMware 中创建准备好的映像计算机目录
  - 在 Red Hat OpenShift 中创建准备好的映像计算机目录
  - 在 XenServer 中创建预准备映像计算机目录

创建准备好的映像计算机目录

创建准备好的映像，并使用这些准备好的映像通过以下方式创建 MCS 计算机目录：

- 网络工作室
- PowerShell 命令

目前，您可以在 Amazon WorkSpaces Core Managed Instances、Azure、Red Hat OpenShift、VMware 和 XenServer® 虚拟化环境中创建预准备映像计算机目录。

更多信息

- 映像管理

后续步骤

- 在 Amazon WorkSpaces Core 中创建准备好的映像 和 创建 Amazon WorkSpaces Core 目录
- 在 Azure 中创建准备好的映像计算机目录
- 在 VMware 中创建准备好的映像计算机目录
- 在 Red Hat OpenShift 中创建准备好的映像计算机目录
- 在 XenServer 中创建预准备映像计算机目录

- 管理预准备映像计算机目录

为 Amazon WorkSpaces Core 托管实例创建准备好的映像

创建准备好的映像以创建 MCS 计算机目录。您可以使用以下方式创建准备好的映像：

- Web 工作室
- (#use-powershell)

主要步骤

1. 创建镜像定义和初始镜像版本。
2. 从初始映像版本创建映像版本。

使用 Web Studio

创建镜像定义和初始镜像版本

要创建镜像定义和初始镜像版本，请执行以下操作：

1. 在 Web Studio 中，转至**映像**节点，然后单击**创建映像定义**。在**简介**页面上单击**下一步**。
2. 在**映像定义**页面上，为映像定义指定**操作系统类型**和**会话类型**。
3. 在**映像**页面上，选择**资源**（仅列出适用于所设置连接的资源）、一个用作创建映像版本的模板的主映像，以及一个用于捕获硬件属性的计算机配置文件。选择一个计算机配置文件以从 VM 实例或启动模板版本捕获硬件属性。

   > **注意：**
   >
   > - 在选择映像之前，请验证主映像是否已安装 VDA 2311 或更高版本，并且 VDA 上是否已安装 MCSIO 驱动程序。
   > - 仅支持实例元数据服务 (IMDS) V2，不支持 IMDS V1。有关信息，请参阅 实例元数据服务版本 2 的工作原理。

4. 在**计算机规范**页面上，选择一个计算机大小。默认选择计算机配置文件（在**映像**页面上选择）的计算机大小。
5. 在**网卡**页面上，为准备映像选择或添加网卡。对于每个网卡，选择一个关联的 VPC 子网。
6. 在“**版本描述**”页面上，输入所创建的初始映像版本的描述。
7. 在“**摘要**”页面上，检查映像定义和所创建的初始映像版本的详细信息。输入映像定义的名称和描述。单击“**完成**”。

创建映像版本

映像版本允许管理特定映像的不同迭代或更新。此功能使您能够维护映像的多个版本以用于不同目的。

要从初始映像版本创建映像版本，请执行以下操作：

> **注意：**
>
> 所有映像版本的主机单元必须相同。

1. 转到**映像**节点，选择一个映像版本或映像定义，然后单击**创建映像版本**。
2. 在**映像定义**页面上，您可以更改主机单元，并重新选择该映像版本的主映像和计算机配置文件。
3. 如果您希望映像版本的配置与初始配置的映像版本不同，请在**创建映像版本**对话框的**计算机规格**和**网卡**页面上配置设置。
4. 添加映像版本的描述。单击**完成**。

> **注意：**
>
> 如果映像版本创建因任何原因失败，底部“**故障排除**”选项卡提供“**重试**”选项。

使用 PowerShell

用于创建准备好的映像版本规范的详细 PowerShell 命令如下：

1. 使用 `Test-ProvImageDefinitionNameAvailable command` 检查可用的映像定义名称。例如，

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. 使用 `New-ProvImageDefinition` 命令创建映像定义。例如，

   ```
   New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
   -VdaSessionSupport MultiSession
   ```

3. 使用 `Add-ProvImageDefinitionConnection` 命令在指定的托管连接中为映像定义创建新配置。

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName test-conn
```

4. 使用 `New-ProvImageVersion` 命令创建映像版本。例如，

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

5. 使用 `Add-ProvImageVersionSpec` 命令将主映像版本规范添加到映像版本。例如，

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName wsc -MasterImagePath "XDHyp:
\HostingUnits\wsc\win10-2411-ami (ami-00123456789abcdef).template”"
```

> **注意：**
>
> 您只能为一个主机单元的一个映像版本添加一个主映像版本规范。

6. 使用 `New-ProvImageVersionSpec` 命令从主映像版本规范创建准备好的映像版本规范。`SourceImageVersionSpecUid` 参数派生自 `Add-ProvImageVersionSpec` 命令。例如，

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  00000000-0000-0000-0000-00000000000

-MachineProfile 'XDHyp:\HostingUnits\wsc\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -RunAsynchronously
```

创建映像定义、映像版本和准备好的映像版本规范的完整 PowerShell 命令集示例：

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession
```

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName wsc -CustomProperties $CustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\wsc\win10-2411-ami
(ami-00123456789abcdef).template”



New-ProvImageVersionSpec -MachineProfile 'XDHyp:
\HostingUnits\wsc\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
00000000-0000-0000-0000-00000000000-HostingUnitName wsc

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注意：

- 映像定义中的所有映像版本规范必须属于同一托管单元。
- 一个映像版本只能有一个主映像版本规范和一个准备好的映像版本规范。
- 所有映像版本规范都必须具有计算机配置文件。

跨可用区和区域共享准备好的映像

现在，您可以为 Amazon WorkSpaces Core 托管实例在同一 AWS 区域或不同区域中，跨不同可用区（与不同托管单元关联）共享单个准备好的映像。这使您可以使用一个准备好的映像在各种可用区和区域中创建和更新 MCS 计算机目录。在不同区域的不同可用区之间共享时，准备好的映像版本会从原始区域复制到目标区域。

您可以维护单个准备好的映像，并使用它在与不同托管单元关联的多个可用区和区域中创建和更新计算机目录。这显著减少了映像管理开销，确保了部署之间的一致性，并简化了预配过程。您还可以使用来自不同可用区或区域的准备好的映像无缝更新现有计算机目录。

用例

- **集中式映像管理：** 您在一个可用区（例如，`us-east-1a`）中创建准备好的映像。然后，您可以将此映像共享到同一 `us-east-1` AWS 区域中的其他可用区（例如 `us-east-1b`）或不同 `us-west-1` 区域中的 `us-west-1a`。这允许单个映像服务于多个托管单元，并为您简化维护。
- **高效的目录创建和更新：** 您可以使用在 `AZ 1`（例如，`us-east-1a`）中创建的准备好的映像在 `AZ 1` 中创建新目录。将此映像共享到 `AZ 2`（例如，`us-east-1b`）后，您可以在 `AZ 2` 中使用共享映像在 `AZ 2` 中创建和更新目录。
- **跨托管单元和托管连接部署：**如果您的环境在相同或不同的 AWS 区域和 AWS 账户下有多个托管单元，则可以在这些托管单元之间高效地共享准备好的映像。

限制

- **在同一 AWS 账户内共享：**在当前实施中，您无法跨不同的 AWS 账户共享。

重要注意事项

- **删除顺序：** 要删除原始准备好的映像版本规范，您必须首先删除其所有共享映像版本规范。或者，您必须同时删除原始和共享规范。
- **目录向后兼容性：** 您可以更新在此功能推出之前部署的现有计算机目录。使用在与您最初部署目录的可用区或区域不同的可用区或区域中创建的准备好的映像。
- **完全删除：** 当您删除准备好的映像时，您将无法再在您共享或最初创建它的任何可用区中使用它。此外，在删除所有与该准备好的映像版本关联的目录之前，无法删除准备好的映像版本。

先决条件

在配置或使用此功能之前，请确保满足以下条件：

- 您的环境必须是 Amazon WorkSpaces Core 托管实例环境。
- 您必须在同一个 AWS 账户下配置多个托管单元（每个托管单元可以绑定到不同的可用区）和主机连接（每个主机连接可以绑定到不同的区域）。

使用 WEB STUDIO UI 进行配置

您可以使用 Web Studio UI 跨与不同托管单元关联的可用区共享准备好的映像。

共享准备好的映像

1. 导航到 Web Studio 的**映像**节点，然后选择要与其他可用区共享的准备好的映像版本。
2. 在顶部导航栏中选择“**管理映像共享**”以管理所选映像版本的映像共享。
3. 在**管理映像共享**页面上，选择一个或多个要与之共享映像版本的资源。这些资源可以位于与原始映像版本不同的可用区中。
4. 单击“**保存**”以在其他可用区中的资源中共享映像版本。映像版本将更新，以便在您选择的不同资源之间共享。完成后，使用该映像版本在共享映像版本的可用区中创建目录。

取消共享准备好的映像

1. 在 Web Studio 的**映像**节点上，选择要取消共享的准备好的映像版本。
2. 在顶部导航栏中选择“**管理映像共享**”以管理所选映像版本的映像共享。
3. 清除一个或多个要停止共享映像版本的资源（可用区）的复选框。

> **注意：**
>
> 资源不得再与共享映像版本关联或从中创建任何目录。任何要删除的、从共享映像版本创建的目录都必须先删除。

4. 单击 **保存** 以取消在已清除的可用区之间共享资源。映像版本将更新，使其不再在这些可用区中共享。

使用 POWERSHELL 进行配置

或者，您可以使用 PowerShell 命令在绑定到不同托管单元的可用区之间共享准备好的映像。

共享准备好的映像

1. 确保您拥有要共享的准备好的映像的 `ImageVersionSpecUid`。您可以使用 PowerShell 中的 `Get-ProvImageVersionSpec` 或类似的 `Get-` 命令检索此信息。
2. 确定您希望在其中提供准备好的映像的可用区（可以是相同或不同的区域）的 `HostingUnitName`。这是您为该特定可用区配置的托管单元的名称。
3. **运行 `Add-ProvImageVersionSpecHostingUnit` 命令：** 使用以下 PowerShell 命令。将 `<ImageVersionSpecUid>` 替换为映像的 Uid，将 `<targetHostingUnitName>` 替换为目标可用区中要共享映像版本规范的托管单元的名称：

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
<ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
```

4. 成功执行后，您可以在 Web Studio UI 中看到映像的状态，指示您已将其与指定的托管单元共享。

取消共享准备好的映像

1. 确保您拥有要取消共享的准备好的映像的 `ImageVersionSpecUid`。
2. 确定要从中移除共享映像的可用区的 `HostingUnitName`。
3. **运行 `Remove-ProvImageVersionSpecHostingUnit` 命令：** 使用以下 PowerShell 命令。将 `<ImageVersionSpecUid>` 替换为映像的 Uid，并将 `<targetHostingUnitName>` 替换为目标可用区中您要从中取消共享映像版本规范的托管单元的名称：

```
Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
<ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
```

下一步操作

- 要创建 Amazon WorkSpaces Core 托管实例目录，请参阅创建 Amazon WorkSpaces Core 托管实例目录

更多信息

- 映像管理
- 有关 Amazon WorkSpaces Core GitHub PowerShell 示例，请参阅 citrix-mcs-sdk-samples-Amazon WorkSpaces Core

创建 Amazon WorkSpaces Core 托管实例目录

创建计算机目录 介绍了用于创建计算机目录的向导。以下信息涵盖了 Amazon WorkSpaces Core 托管实例的特定详细信息。

> **注意：**
>
> 目前，支持创建持久和非持久 VM 的目录（`CleanOnBoot` 属性为 `True` 或 `False`）。

先决条件

在创建 Amazon WorkSpaces Core 托管实例目录之前，您需要完成以下创建：

1. 连接到 Amazon WorkSpaces Core 托管实例。请参阅 Connection to Amazon WorkSpaces Core Managed Instances。
2. 准备好的映像。请参阅为 Amazon WorkSpaces Core 托管实例创建准备好的映像。

映像准备期间的网络设置

在映像准备期间，将基于原始 VM 创建一个准备虚拟机 (VM)。此准备 VM 与网络断开连接。为了将网络与准备 VM 断开连接，将创建一个网络安全组以拒绝所有入站和出站流量。此网络安全组将持久存在并被重用。网络安全组的名称为 `Citrix.XenDesktop.IsolationGroup-GUID`，其中 GUID 是随机生成的。

基于计算机配置文件的计算机目录

您可以使用计算机配置文件捕获 EC2 实例 (VM) 或启动模板版本中的硬件属性，并将其应用于预配的计算机。捕获的属性可以包括（例如）租用类型、实例类型、安全组、网络映射、EBS 卷属性、EBS 优化、CPU 选项、休眠功能以及其他受支持的 AWS 配置。

您可以使用 AWS EC2 实例 (VM) 或 AWS 启动模板版本作为计算机配置文件输入。

> **注意：**
>
> - EBS 卷属性仅从计算机配置文件派生。
> - 仅支持实例元数据服务 (IMDS) V2，不支持 IMDS V1。有关信息，请参阅 实例元数据服务版本 2 的工作原理。

AWS 租用

AWS 提供以下租用选项：共享租用（默认类型）和专用租用。共享租用意味着来自不同客户的多个 Amazon WorkSpaces Core 实例可能驻留在同一物理硬件上。专用租用意味着您的 Amazon WorkSpaces Core 实例仅在您部署的其他实例所在的硬件上运行。

> **注意：**
>
> 仅支持专用实例（目前不支持专用主机）。其他客户不使用同一硬件。

租用类型从计算机配置文件中捕获

当您使用 MCS 创建目录以在 AWS 中预配计算机时，租用类型将从计算机配置文件中捕获。

- **共享硬件**：此设置适用于大多数部署。多个客户共享硬件，即使他们之间不进行交互。使用共享硬件是运行 Amazon EC2 实例最经济的选择。
- **专用实例**：此设置更适用于具有特定安全或合规性要求的部署。使用专用实例，您仍然可以享受拥有独立于其他 AWS 客户的主机的好处，但无需支付整个主机的费用。您无需担心主机的容量，但实例的收费费率更高。此外，专用实例对自带许可证 (BYOL) 的支持有限。

灵活计费

Amazon WorkSpaces Core 托管实例支持两种计费模式：

计费模式	描述
按月	固定的月度统一费率计费。适用于持久性桌面和可预测的工作负载。
按小时	按需计费。如果未明确指定计费模式，这是 AWS 的默认配置。

这些选项根据您的工作负载的持久性和使用模式，为管理计算成本提供了灵活性。

此功能需要使用 Amazon WorkSpaces 计费服务。默认情况下，MCS 使用此服务来预配和管理实例，让您能够从更具竞争力的持久性工作负载统一费率定价中受益。

先决条件和注意事项

- AWS 账户配置：您的 AWS 账户必须配置为使用 WorkSpaces 计费服务。虽然 AWS 账户默认已切换，但有些客户可能会要求 AWS 仍使用旧版 EC2 计费服务来使用 WorkSpaces Core 托管实例。

  > **注意：**
  >
  > 如果您的账户使用的是旧版 EC2 计费服务，则**按月**计费选项不可用。

- 主机连接：灵活计费仅适用于 Amazon WorkSpaces Core 主机连接。它不支持标准 AWS EC2 主机连接。
- 竞价型实例：WorkSpaces 计费服务不支持竞价型实例。
- 混合计费：AWS 账户必须对核心托管实例使用 WorkSpaces 计费或 EC2 计费。单个账户中不支持两者混合使用。

- 兼容性：只有特定的实例类型、平台类型（操作系统）和租用类型与某些计费模式兼容。MCS 会执行预检，以确保您的选择（服务产品、计算机配置文件和准备好的映像）与所选的计费模式匹配。

请参阅使用特定计费模式创建计算机目录。

创建目录

创建 Amazon WorkSpaces Core 托管实例目录需要准备好的映像和计算机配置文件。您可以使用 AWS VM 实例或 AWS 启动模板版本作为计算机配置文件输入。

您可以使用以下方式创建目录：

- 网络工作室
- PowerShell

使用 Web Studio 创建目录

从“映像”节点创建计算机目录

使用“**映像**”节点中的“**创建目录**”选项，使用映像版本创建目录。

或者，您可以在“**计算机目录**”节点中创建目录时选择版本，将其链接到目录创建工作流中的准备好的映像选项。请参阅从“计算机目录”节点创建计算机目录。

要从**映像**节点创建 MCS 计算机目录，请执行以下操作：

1. 选择一个映像版本，然后单击**创建目录**。在**简介**页面上单击**下一步**。
2. 在“**计算机管理**”和“**映像**”页面上，设置会根据所选映像版本预先选择。在“映像”页面上，为所选的准备好的映像输入备注。
3. 在以下页面上完成设置。
4. 在**摘要**页面上，检查计算机目录的详细信息。输入计算机目录的名称和描述。单击**完成**。
5. 转到**计算机目录**节点以查看创建的计算机目录。

从计算机目录节点创建计算机目录

要从“计算机目录”节点创建 MCS 计算机目录，请执行以下操作：

1. 在左侧导航窗格中单击**计算机目录**。
2. 单击“**创建计算机目录**”。将显示“**计算机目录设置**”页面。
3. 在“**计算机类型**”页面上，为目录选择计算机类型，例如，“**多会话操作系统**”。
4. 在“**计算机管理**”页面上，选择以下设置：

a. 选择“**已进行电源管理的计算机（例如，虚拟机或刀片式电脑）**”。

b. 选择“**Citrix 预配技术**”。然后，选择“**Citrix Machine Creation Services™**”。

c. 在“**资源**”字段中，选择在创建主机连接时配置的资源（可用区或本地区域），然后单击“**下一步**”。

5. 在“**桌面体验**”页面上，选择用户登录时所需的随机桌面或静态桌面。如果选择了静态桌面，请进一步指定是否要保存用户在本地磁盘上所做的更改（持久性或非持久性）。
6. 在“**映像**”页面上，单击“**选择映像**”以为计算机目录选择准备好的映像。选择您创建的准备好的版本。单击映像版本名称。要查看有关所选映像版本的更多详细信息，请单击带下划线的版本号。单击“**完成**”。

   与准备好的映像关联的计算机配置文件将显示，并且其硬件属性（例如，实例类型、租用类型、网络映射、安全组、卷属性）用于在目录中创建计算机。要将计算机配置文件源更改为其他 VM 或启动模板版本，请单击编辑按钮。
7. 在“**虚拟机**”页面上：

   a. 输入目录的 VM 数量。

   b. 将显示基于计算机配置文件的默认计算机规范。要更改它，请选择编辑图标并选择计算机规范。
8. 在“**网卡**”页面上，为 VM 选择网卡（或 ENI）。
9. 在 **计算机身份** 页面上，为目录中的计算机配置计算机身份类型：

   a. 要配置 **已加入域的计算机（本地 Active Directory 或 Microsoft Entra 混合加入）**，请选择域并为将在此计算机目录中创建的 VM 创建新的 AD 帐户。预配的 VM 将加入所选域。要预配 **未加入域的计算机**，请选择未加入域选项。

   b. 指定将为 VM 创建的新帐户的帐户命名方案。
10. 在“**域凭据**”页面上，单击“**输入凭据**”以提供所选域的凭据。出现提示时，输入管理员级别的用户名和密码。如果您之前已按照我们的产品文档保存了域凭据，也可以使用服务帐户。
11. 依次单击其余页面，直到显示“**摘要**”页面。为计算机目录输入名称，然后选择“**完成**”以创建计算机目录。

在 AWS 本地区域中创建计算机目录的限制

- 某些本地区域仅支持某些硬件配置（例如，珀斯本地区域不支持 GP3 卷，仅支持 GP2）。
- 由于只有 gp2 在所有本地区域中普遍受支持，并非所有区域都支持 gp3，因此 ID 磁盘创建默认使用 gp2 卷类型。
- 您必须选择一个在所需本地区域中支持其硬件规格的计算机配置文件。

- 准备好的映像 AMI 快照和 ID 磁盘快照默认放置在区域中，而不是本地区域（由于 AWS 对本地区域中 EBS 快照支持的可见性限制）。
- 只有支持完整 EC2 和 EBS 服务的本地区域才是受支持的区域。

使用 PowerShell 创建目录

使用准备好的映像版本规范和计算机配置文件创建目录

- 使用 `New-ProvScheme` 命令从准备好的映像版本规范创建 MCS 非持久性计算机目录。例如，

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$true] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

- 使用 `New-ProvScheme` 命令从准备好的映像版本规范创建 MCS 持久性计算机目录。例如，

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$false] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

用于创建目录的 PowerShell 命令完整集示例：

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "wsccatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "domainname"
-IdentityPoolName "wsccatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "aws##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName wsccatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
```

```
-HostingUnitName wsc -IdentityPoolName wsccatalog -CleanOnBoot -Scope @()
-SecurityGroup @() -MachineProfile 'XdHyp:\HostingUnits\cvad-test-
scalestress\us-east-1a.availabilityzone\machine-profile-instance i
(i-0xxxxxxxx).vm' -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName wsccatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

更新计算机配置文件

要更新最初使用计算机配置文件预配的目录上的计算机配置文件，请执行以下操作。在编辑 MCS 计算机目录时，您还可以更改计算机配置文件源的租用类型和休眠功能。

1. 运行 `Set-ProvScheme` 命令。例如，

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

创建具有特定计费模式的计算机目录

目前，您只能在使用 PowerShell 创建计算机目录时指定计费模式。

使用 PowerShell

要通过 PowerShell 指定计费模式，请在 `New-ProvScheme` 命令中使用 `CustomProperties` 参数。

```
$custprop = "BillingMode,Monthly"



New-ProvScheme -ProvisioningSchemeName "MyCatalog" `
```

```
-ImageVersionSpecUid $ImageVersionSpecUid `

-HostingUnitName "wsc-unit" `

-IdentityPoolName "MyIdentityPool" `

-MachineProfile "XdHyp:\HostingUnits\wsc-unit\machine-profile
lt-123.launchtemplate\lt-123 (1).launchtemplateversion" `

-CustomProperties $custprop `

-CleanOnBoot
```

注意：

如果省略 `BillingMode` 属性，则目录默认为 `Hourly`。

更改现有目录的计费模式

您可以将现有目录从 `Monthly` 转换为 `Hourly`，反之亦然。此更改可应用于目录中的新 VM 和现有 VM。

更新的重要注意事项

- 服务窗口：现有 VM 必须经过服务窗口或电源循环才能应用计费更改。
- 验证：MCS 在应用更改之前会验证现有实例类型和平台是否与新的计费模式兼容。

使用 PowerShell 进行更新

- 要更新仅添加到目录中的新 VM 的计费模式，请更新预配方案的计费模式自定义属性：

```
$custprop = "BillingMode,Hourly"



Set-ProvScheme -ProvisioningSchemeName "MyCatalog" -CustomProperties
$custprop
```

- 要更新目录中新 VM 和现有 VM 的计费模式，请创建具有更新的自定义属性的新预配方案版本，并将新版本应用于所有 VM：

```
$custprop = "BillingMode,Hourly"



New-ProvSchemeVersion -ProvisioningSchemeName "MyCatalog"
-CustomProperties $custprop



New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 2 `

-StartsNow -AllVMs `

-MaxDurationInMinutes 100 `

-ProvisioningSchemeName "MyCatalog"
```

监控计费信息

您可以验证目录和单个虚拟机的计费模式。

运行以下 PowerShell 命令以检查您帐户的计费资格：

- 将 `BillingMode` 作为 CustomProperties 的一部分返回

```
Get-ProvScheme –ProvisioningSchemeName “"MyCatalog" "  | Select
 ProvisioningSchemeName,  CustomProperties
```

- 将 `BillingMode` 作为 VMInfo 的一部分返回

```
Get-ProvVMDetails –ProvisioningSchemeName “"MyCatalog" "  | Select-
Object  -ExpandProperty VMInfo
```

故障排除和验证

MCS 包含预检检查以防止不兼容的配置。在目录创建或编辑期间，您可能会遇到以下错误：

- **NoInstanceConfigFoundForBillingMode**：如果所选的服务产品（实例类型）、租期和平台类型不支持所选的计费模式，则会发生此错误。
- **Spot Instance Not Supported**：如果您尝试将 Spot 实例与 WorkSpaces 主机连接一起使用，则验证将失败。

- **EC2 billing restriction**：如果您的 AWS 帐户使用旧版 EC2 计费模型，则尝试设置“每月”计费模式将导致验证错误。

使用 POWERSHELL 创建具有启动模板版本的目录

您可以创建以启动模板版本作为计算机配置文件输入的 MCS 计算机目录。您还可以将计算机配置文件目录的输入从 VM 更新为启动模板版本，以及从启动模板版本更新为 VM。

在 AWS EC2 控制台中，您可以提供启动模板的实例配置信息以及版本号。当您在创建或更新计算机目录时将启动模板版本指定为计算机配置文件输入时，该版本启动模板的属性将复制到预配的 VDA VM。

以下属性可以通过机器配置文件输入或作为 `New-ProvScheme` 或 `Set-ProvScheme` 命令中的参数显式提供。如果它们在 `New-ProvScheme` 或 `Set-ProvScheme` 命令中提供，则它们优先于这些属性的机器配置文件值。

- 服务产品
- 网络

> **注意：**
>
> 如果机器配置文件启动模板中未提供服务产品，或者未在 `New-ProvScheme` 命令中将其作为参数提供，则会收到相应的错误。

要使用启动模板版本作为机器配置文件输入来创建目录，请执行以下操作：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 获取启动模板的启动模板版本列表。例如：

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. 如果尚未创建身份池，请创建身份池。例如：

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `
```

```
-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. 创建预配方案，其中启动模板版本作为机器配置文件输入。例如：

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-ImageVersionSpecUid ‘24dfb047-e867-527g-896c-25664xxxxx1t’ `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. 将预配方案注册为代理目录。例如：

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. 完成目录创建。

更新机器配置文件源

您还可以将机器配置文件目录的输入从 VM 更新为启动模板版本，以及从启动模板版本更新为 VM。例如：

- 要将计算机配置文件目录的输入从 VM 更新为启动模板版本：

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- 要将计算机配置文件目录的输入从启动模板版本更新为 VM：

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

启用 MCSIO 的目录

MCS 存储优化 (MCSIO) 通过将磁盘操作缓存在内存中或小型高速磁盘上，从而提高 VM 的性能。您可以使用 PowerShell 命令创建启用 MCSIO 的非持久性目录。要创建此类目录，您必须在准备 AMI 实例期间安装或升级 VDA 时安装 MCSIO 驱动程序。默认情况下，该驱动程序未安装。

准备好 MCSIO AMI 后（安装 VDA 时，选择在安装中包含 MCSIO 驱动程序的选项），您可以创建启用 MCSIO 的非持久性目录。

> **注意：**
>
> 使用 Studio 仅配置磁盘缓存（不带内存缓存）的 MCSIO 选项已在所有虚拟机管理程序和云服务环境中删除。

创建启用 MCSIO 的目录

添加到 New-ProvScheme PowerShell 命令的四个参数是：

- `UseWriteBackCache`：为给定预配方案启用缓存（回写缓存）

- `WriteBackCacheDiskSize`：指定用于缓存的临时磁盘大小（以 GB 为单位）
- `WriteBackCacheMemorySize`：指定用于缓存的内存量（以 MB 为单位）。这是一个可选参数。

> **注意：**
>
> - `WriteBackCacheDiskSize` 的值必须大于零，因为至少需要 1 GB 的缓存磁盘存储空间。缓存磁盘大小不得大于操作系统磁盘大小。
> - `WriteBackCacheMemorySize` 的值必须为非零且小于计算机目录内存大小。

影响 MCSIO 的自定义属性如下：

- `WBCDiskStorageType`：定义卷类型，用于 Amazon WorkSpaces Core 托管实例中的临时磁盘。此参数采用 `volume-type[:iops][:throughput]` 格式的字符串参数。以下是卷类型：
  - gp2：此卷类型不使用 iops 和吞吐量参数
  - gp3：此卷类型使用 iops 和吞吐量参数
  - io1：此卷类型仅使用 iops 参数
  - io2：此卷类型仅使用 iops 参数

  默认卷类型为 **gp2**。
- `PersistWBC`：控制在 Amazon WorkSpaces Core 托管实例关闭时是保留还是丢弃缓存磁盘。如果设置为 `true`，则保留缓存磁盘。如果设置为 `false`（默认值），则仅在 AMI 实例开机时创建并保留缓存磁盘。
- `PersistOSDisk`：控制在 Amazon WorkSpaces Core 托管实例关闭时是保留还是丢弃操作系统磁盘。如果设置为 `true`，则保留操作系统磁盘。如果设置为 `false`（默认值），则仅在 AMI 实例开机时创建并保留操作系统磁盘。

在 PowerShell 窗口中执行以下步骤以创建启用 MCSIO 的非持久目录：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 创建代理目录和身份池。
4. 创建预配方案。例如：

```
$HostingUnitUid = '0xxxx1d9-bbfc-xxxf-bxxb-exxxxxe008b2'

$MasterImageVM = 'XDHyp:\HostingUnits\ctx-test\aws-apollo-non-
persistent-multi-mcsio-vda-win2022 (ami-0bf1810488acbxxxb).template'

$NetworkMap = @{ 'NetworkPath' = 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\10.0.128.0`/17
(vpc-0fa6e41d72507fxxx).network' }

$SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\private.securitygroup' )

$ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
Instance.serviceoffering'

$CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,false'



$provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
-HostingUnitUid $HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

- MasterImageVM $MasterImageVM `

-NetworkMap $NetworkMap `

-ServiceOffering $ServiceOffering `

-SecurityGroup $SecurityGroup `

-CustomProperties $CustomProperties `

-UseWriteBackCache -WriteBackCacheDiskSize 16 -WriteBackCacheMemorySize
256
```

5. 将 VM 添加到目录。

使用 MCSIO 提高启动性能

如果您启用 MCSIO 并将 `PersistWBC` 和 `PersistOSDisk` 自定义属性设置为 `true`，则可以提高 VM 的启动性能。通过此设置，VM 可以更快地启动，因为它们无需初始化新的缓存磁盘或从其模板重新创建根磁盘。

加密操作系统和身份磁盘

您可以使用 AWS KMS 密钥（客户管理密钥和 AWS 管理密钥）创建 VM 目录，这些密钥可用于加密操作系统磁盘和身份磁盘 (ID)。

- AWS 管理密钥每年自动轮换。
- 客户管理密钥可选择自动轮换，也可以手动管理。

有关 KMS 密钥的更多信息，请参阅以下 AWS 文档：

- AWS KMS 概念
- 自动密钥轮换的工作原理

对于操作系统和身份磁盘的加密，请配置以下选项之一：

- 使用已加密的准备好的映像（例如，从包含使用 KMS 密钥加密的 EBS 根卷的实例或快照创建的 AMI）
- 使用包含加密 EBS 根卷的计算机配置文件源（VM 或启动模板）。

限制

请考虑以下限制：

- MCS 目前仅支持准备好的映像 AMI 上的一个磁盘。
- 您无法直接加密现有的未加密 EBS 卷或快照，也无法修改现有加密卷的 KMS 密钥。为此，您必须：

  a. 创建该卷的新快照。

  b. 从该快照创建新卷。

  c. 加密新卷。

请参阅以下 AWS 文档：

- 加密未加密资源
- EBS 卷自动或默认加密的限制：自动加密现有和新的 Amazon EBS 卷。

创建带磁盘加密的目录

您可以使用以下方法创建带磁盘加密的 MCS 计算机目录：

- 准备好的映像（使用从具有加密磁盘的主映像进行映像管理创建）
- 计算机配置文件

使用计算机配置文件输入时需要考虑的因素包括：

- 计算机配置文件输入的 KMS 密钥优先于准备好的映像的 KMS 密钥。
- 如果未提供计算机配置文件输入，则使用准备好的映像 AMI 的 KMS 密钥来加密目录 VM 的磁盘。
- 如果计算机配置文件中存在块设备映射，则准备好的映像模板 (AMI) 和计算机配置文件中存在的块设备必须匹配。例如，如果 AMI 在 `/dev/sda1` 上定义了一个设备，则计算机配置文件也必须在 `/dev/sda1` 上定义一个设备。
- 如果机器配置文件源中没有密钥，并且准备好的映像未加密，则目录 VM 的磁盘不会加密。
- 当准备好的映像已加密时，机器配置文件源 VM 或启动模板必须具有加密的根卷才能被视为有效输入。

修改现有目录

您可以使用 `Set-ProvScheme` PowerShell 命令修改现有目录，以使其具有：

- 包含新 KMS 密钥的卷的机器配置文件输入。
- 使用映像管理从主映像创建的、具有加密 AMI 的准备好的映像。

重要注意事项：

- 添加到目录中的新 VM 的卷将使用新的 KMS 密钥进行加密。
- 如果存在现有机器配置文件，要更新加密设置，请使用新的机器配置文件运行 `Set-ProvScheme`。
- 您无法将现有目录从加密卷修改为未加密卷。 您无法将映像从加密的准备好的映像 AMI 更新为未加密的准备好的映像 AMI。

为 VM 实例启用 NitroTPM 和 UEFI 安全启动

创建目录时，您现在可以选择已启用 NitroTPM 和/或 UEFI 安全启动的准备好的映像 (AMI)。因此，目录中预配的 VM 也将启用 NitroTPM 和/或 UEFI 安全启动。此实现可确保 VM 的安全性和可信度。有关 NitroTPM 和 UEFI 安全启动的更多信息，请参阅 Amazon 文档。

限制

- 目前，您可以在除中国以外的所有 AWS 区域（包括 AWS GovCloud (US) 区域）中使用 NitroTPM 和安全启动。

- 您无法在现有目录上启用 NitroTPM 和 UEFI 安全启动。如果您需要启用 NitroTPM 和 UEFI 安全启动的目录，请创建一个新目录。

关键步骤

1. 设置您的 AWS 环境。
2. 创建与 AWS 的连接。
3. 创建启用 NitroTPM 和/或 UEFI 安全启动的主映像 (AMI)。
4. 从主映像创建准备好的映像。请参阅为 Amazon WorkSpaces Core 托管实例创建准备好的映像。
5. 通过在 Web Studio 目录创建菜单中选择已启用 NitroTPM 和 UEFI 安全启动的准备好的映像，或者在使用 PowerShell 命令创建预配方案时，创建计算机目录。

添加到所创建目录的 VM 已启用 NitroTPM 和 UEFI 安全启动。

创建支持 NITROTPM 和 UEFI 安全启动的 AMI

1. 您可以从已启用 NitroTPM 和/或 UEFI 安全启动的 VM 创建 AMI。
   a. 使用 AWS Marketplace 映像创建实例。例如，搜索 `TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`。
   b. 下载单会话或多会话 VDA。
   c. 从该 VM 创建 AMI。
2. 使用 register-image 命令：

   ```
   --boot-mode (string)

   --tpm-support (string)
   ```

   有关详细信息，请参阅 register-image。

请参阅以下 AWS 文档：

- 确定 EC2 实例类型支持的启动模式
- 将 NitroTPM 与 Amazon EC2 实例结合使用的要求/.

您可以从 Delivery controller™ 主机打开 PowerShell 窗口，以检查特定项是否：

- 服务产品支持 NitroTPM 或 UEFI 安全启动

```
(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.BootMode

(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
```

- 模板支持 NitroTPM 或 UEFI 安全启动

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.BootMode



(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

更新现有目录的服务产品

您可以使用 `Set-ProvScheme` 更改现有目录的服务产品。此更改适用于新添加的 VM。但是，在以下情况下会出现错误：

AMI 启动模式	AMI 支持 NITRO TPM 吗？	服务产品支持 NITROTPM 和 UEFI 安全启动吗？
UEFI	否	否
传统 BIOS	是	否
UEFI	是	否
UEFI 优先	是	否

复制虚拟机上的标签

您可以将计算机配置文件中指定的 NIC 和磁盘（身份磁盘、回写缓存磁盘和操作系统磁盘）上的标签复制到 MCS 计算机目录中新创建的虚拟机。您可以在任何计算机配置文件源（AWS 虚拟机实例或 AWS 启动模板版本）中指定这些标签。此功能适用于持久和非持久计算机目录和虚拟机。

> **注意：**

- 在 AWS EC2 控制台中，您无法在“**启动模板版本资源标签**”下看到“**标记网络接口**”值。但是，您可以运行 PowerShell 命令 `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` 来查看标签规范。
- 如果计算机配置文件源（虚拟机或启动模板版本）有两个网络接口（eni-1 和 eni-2），并且 eni-1 具有标签 t1，eni-2 具有标签 t2，则虚拟机将获得这两个网络接口的标签。

使用 PowerShell 筛选虚拟机实例

您用作计算机配置文件虚拟机的 AWS 虚拟机实例必须兼容，以便计算机目录能够正确创建和运行。要列出可用作计算机配置文件输入虚拟机的 AWS 虚拟机实例，您可以使用 `Get-HypInventoryItem` 命令。该命令可以对托管单元上可用的虚拟机清单进行分页和筛选。

分页：

Get-HypInventoryItem 支持两种分页模式：

- 分页模式使用 `-MaxRecords` 和 `-Skip` 参数来返回项目集：
  - `-MaxRecords`：默认值为 **1**。这控制要返回的项目数。
  - `-Skip`：默认值为 **0**。这控制从管理程序列表中绝对开头（或绝对结尾）跳过的项目数。
- 滚动模式使用 `-MaxRecords`、`-ForwardDirection` 和 `-ContinuationToken` 参数来允许记录滚动：
  - `-ForwardDirection`：默认值为 **True**。这与 `-MaxRecords` 一起使用，以返回下一组匹配记录或上一组匹配记录。
  - `-ContinuationToken`：返回紧随其后（如果 `ForwardDirection` 为 **false** 则为之前）的项目，但不包括 `ContinuationToken` 中给定的项目。

分页示例：

- 返回名称最低的计算机模板的单个记录。`AdditionalData` 字段包含 `TotalItemsCount` 和 `TotalFilteredItemsCount`：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- 返回名称最低的计算机模板的 10 条记录：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- 返回以最高名称结尾的记录数组：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- 返回从与给定 `ContinuationToken` 关联的计算机模板开始的记录数组：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

筛选：

支持以下用于筛选的其他可选参数。您可以将这些参数与分页选项结合使用。

- `-ContainsName "my_name"`：如果给定字符串与 AMI 名称的一部分匹配，则该 AMI 将包含在 `Get` 结果中。例如：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: 如果 AMI 具有这些标签中的至少一个，则会将其包含在 `Get` 结果中。例如：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **注意：**

> 支持两个标签值。**未标记**标签值匹配其标签列表中没有给定标签的项目。**所有值**标签值匹配具有该标签的项目，无论标签的值如何。否则，仅当项目具有该标签且值等于筛选器中给定的值时，才会发生匹配。

- `-Id "ami-0a2d913927e0352f3"`: 如果 AMI 与给定 ID 匹配，则会将其包含在 `Get` 结果中。例如：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

根据 AdditionalData 参数进行筛选：

`AdditionalData` 筛选器参数根据模板或 VM 的功能、服务产品或 AdditionalData 中的任何属性列出它们。例如：

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

您还可以添加 `-Warn` 参数以指示不兼容的 VM。VM 将包含一个名为 **Warning** 的 `AdditionalData` 字段。例如：

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

下一步操作

- 有关管理 Amazon WorkSpaces Core 目录的信息，请参阅 管理 Amazon WorkSpaces Core 托管实例目录

更多信息

- AWS 虚拟化环境
- 连接到 Amazon WorkSpaces Core 托管实例
- 映像管理
- 为 Amazon WorkSpaces Core 托管实例创建准备好的映像
- 有关 Amazon WorkSpaces Core GitHub PowerShell 示例，请参阅 citrix-mcs-sdk-samples-Amazon WorkSpaces Core。

在 Azure 中创建预准备映像计算机目录

创建准备好的映像，并使用这些准备好的映像通过以下方式创建 MCS 计算机目录：

- Web 工作室
- (#use-powershell)

使用准备好的镜像创建 MCS 计算机目录的关键步骤如下：

1. 创建镜像定义和初始镜像版本。
2. 使用镜像版本作为准备好的镜像来创建目录

使用 Web Studio

创建镜像定义和初始镜像版本

要创建镜像定义和初始镜像版本，请执行以下操作：

1. 在 Web Studio 中，转至**映像**节点，然后单击**创建映像定义**。在**简介**页面上单击**下一步**。
2. 在**映像定义**页面上，为映像定义指定**操作系统类型**和**会话类型**。
3. 选择现有资源组或创建新资源组以保存映像资源。要启用映像共享，请在 Azure 计算库中选择**放置映像版本**，然后选择创建新库或使用现有库来保存其映像版本。
4. 在**映像**页面上，选择**资源**（仅列出适用于所设置连接的资源）和用作创建映像版本模板的主映像。您可以选中**使用计算机配置文件**复选框并选择一个计算机配置文件。

> **注意：**
>
> - 在选择映像之前，请验证主映像是否已安装 VDA 2311 或更高版本，并且 VDA 上是否已安装 MCSIO 驱动程序。
> - 如果要使用机密 VM 类型准备的映像创建 MCS 目录，请使用机密 VM 类型主映像和机密 VM 类型计算机配置文件创建准备的映像。有关准备机密 VM 类型主映像和计算机配置文件的信息，请参阅 Azure 机密 VM。

5. 在**存储和许可证类型**页面上，选择要在映像准备过程中使用的存储和许可证类型。

> **注意：**

> 如果在**映像**页面上选择计算机配置文件，则计算机配置文件的许可证类型会根据配置文件设置预先选择。

6. 在**计算机规范**页面上，选择计算机大小。如果在**映像**页面上选择计算机配置文件，则默认选择计算机配置文件的计算机大小。
7. 在**网卡**页面上，为准备映像选择或添加网卡。对于每个网卡，选择一个关联的虚拟网络。
8. 在**磁盘设置**页面上，选择客户管理的加密密钥 (CMEK)。如果计算机配置文件没有 CMEK 但主映像有，则会预先选择主映像中的 CMEK。
9. 在**版本描述**页面上，输入所创建的初始映像版本的描述。
10. 在**摘要**页面上，检查映像定义和所创建的初始映像版本的详细信息。输入映像定义的名称和描述。单击**完成**。

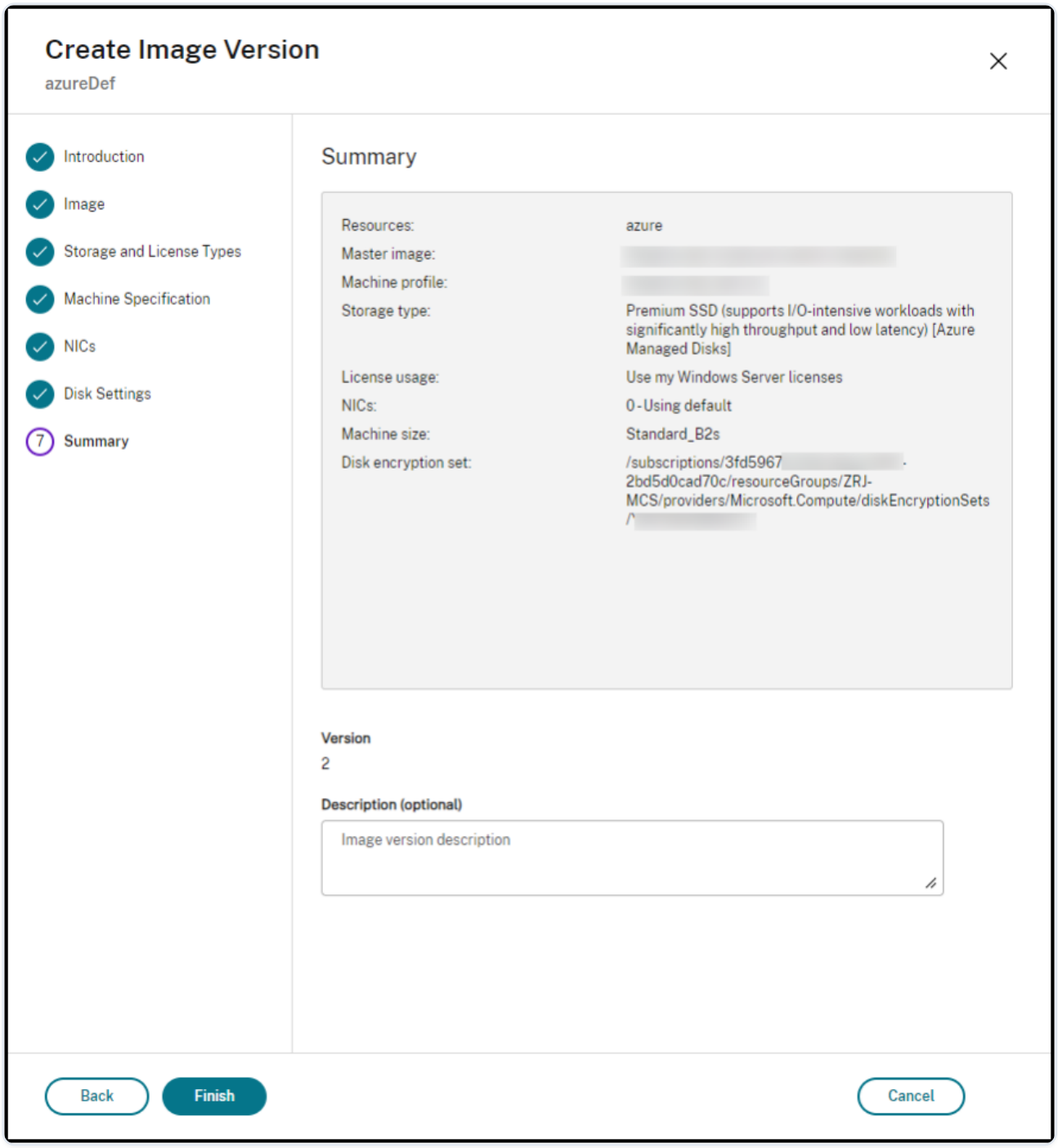
创建映像版本

映像版本允许管理特定映像的不同迭代或更新。此功能使您能够维护映像的多个版本以用于不同目的。

要从初始映像版本创建映像版本，请执行以下操作：

> **注意：**
>
> 所有映像版本的主机单元必须相同。

1. 转到**映像**节点，选择一个映像版本或映像定义，然后单击**创建映像版本**。
2. 在“映像定义”页面上，您可以更改主机单元，并为该映像版本重新选择主映像和计算机配置文件。
3. 如果您希望映像版本的配置与初始配置的映像版本不同，请在“**创建映像版本**”对话框的“**存储和许可证类型**”、“**计算机规范**”、“**NIC**”和“**磁盘设置**”页面上配置设置。
4. 添加映像版本的描述。单击**完成**。



注意：

如果映像版本创建因任何原因失败，底部“**故障排除**”选项卡提供“**重试**”选项。

共享预准备映像

要在 Azure 的不同主机单元之间共享准备好的映像，请按照以下步骤操作：

1. 右键单击映像版本并选择“**管理映像共享**”。Azure 环境中的所有主机单元都会显示。创建映像版本的资源将禁用任何操作。

2. 选择要共享映像的托管单元，然后单击**保存**。**共享状态**列显示“正在进行中”。
3. 单击“**资源**”选项卡以获取有关共享状态的更多详细信息。

> **注意：**
>
> 当映像版本共享状态为进行中时，**删除映像版本**或**管理映像共享**选项将被禁用。

从“映像”节点创建计算机目录

使用“**映像**”节点中的“**创建目录**”选项，使用映像版本创建目录。

或者，您可以在**计算机目录**节点中创建目录时选择版本，链接到目录创建工作流中的准备好的映像选项。请参阅从计算机目录节点创建计算机目录

要从**映像**节点创建 MCS 计算机目录，请执行以下操作：

1. 选择一个映像版本，然后单击**创建目录**。在**简介**页面上单击**下一步**。
2. 在**桌面体验**页面上，选择所需的桌面体验。
3. 从“**映像**”页面到“**磁盘设置**”页面，设置将根据所选映像版本预先选择。
4. 在“**资源组**”页面上，您可以选择创建新的资源组或使用现有资源组来放置此目录的资源。
5. 在以下页面上完成设置。
6. 在**摘要**页面上，检查计算机目录的详细信息。输入计算机目录的名称和描述。单击**完成**。
7. 转到**计算机目录**节点以查看创建的计算机目录。

从计算机目录节点创建计算机目录

要从**计算机目录**节点创建 MCS 计算机目录，请执行以下操作：

1. 在左侧导航窗格中单击**计算机目录**。
2. 单击**创建计算机目录**。此时将显示**计算机目录设置**页面。依次单击**简介**、**计算机类型**和**计算机管理**页面上的**下一步**。
3. 在“**计算机管理**”页面上，选择以下设置：
    a. 选择“**已进行电源管理的计算机（例如，虚拟机或刀片式电脑）**”。
    b. 选择“**Citrix 预配技术**”。然后，选择“**Citrix Machine Creation Services™**”。
    c. 在“**资源**”字段中，列出了属于不同区域的资源。选择任意 Azure 网络资源，然后单击“**下一步**”。
4. 在**映像**页面上：对于主映像类型，请按照以下步骤操作：

a. 选择主映像。
b. 在主映像下，选择一个映像。该边栏列出了与资源属于同一区域的所有映像。
c. 点击 **完成**。
d. 对于预准备映像类型，选择**预准备映像**。
e. 在“**准备好的映像**”下，选择映像定义的映像版本。如有需要，为所选的准备好的映像版本添加备注。
f. 单击映像版本名称。要查看有关所选映像版本的更多详细信息，请单击带下划线的版本号。
g. 如果所选映像版本配置了计算机配置文件，请选择一个计算机配置文件。如果所选映像版本未配置计算机配置文件，则无法选择使用计算机配置文件。

5. 配置以下页面上的设置。
6. 在“**磁盘设置**”页面上，如果所选的准备好的映像使用磁盘加密集，则无法删除加密集，但可以将密钥更改为另一个加密密钥。
7. 在“**资源组**”页面上，您可以选择创建新的资源组或使用现有资源组来放置此目录的资源。
8. 在以下页面上完成设置。
9. 在**摘要**页面上，检查计算机目录的详细信息。输入计算机目录的名称和描述。单击**完成**。

使用 PowerShell

创建准备好的映像

用于创建准备好的映像版本规范的详细 PowerShell 命令如下：

1. 使用 `Test-ProvImageDefinitionNameAvailable command` 检查可用的映像定义名称。例如，

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. 使用 `New-ProvImageDefinition` 命令创建映像定义。例如，

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession
```

3. 使用 `Add-ProvImageDefinitionConnection` 命令在指定的托管连接中为映像定义创建新配置。

   `Add-ProvImageDefinitionConnection` 的 `CustomProperties` 可以包括以下内容。如果不使用这些参数，则使用默认值。

- `ResourceGroups`：包含基础磁盘的资源组。
- `UseSharedImageGallery`：基础磁盘类型的指示器。对于 ACG（映像共享），请使用 `true`；对于快照，请使用 `false`。
- `ImageGallery`：当基础磁盘是 ACG 映像版本时的库名称。

例如，

- 在快照和客户提供的资源组的情况下：

```
$CustomerOwnRsourceGroupProperties = @"

<CustomProperties xmlns="http:// schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="yangj_image" />

</CustomProperties>

"@
```

- 在 ACG 和客户提供的资源组以及映像库的情况下：

```
$CustomerOwnAllProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />

<Property xsi:type="StringProperty" Name="ImageGallery"
Value="gallery" />

</CustomProperties>
```

```
"@
```

- 在 ACG 和客户提供的资源组的情况下：

```
$CustomerOwnResourceGroupProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />

</CustomProperties>

"@
```

- 在 ACG 和 Citrix 管理的资源组以及映像库的情况下：

```
$CustomerOwnResourceGroupNothingProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

</CustomProperties>

"@
```

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 [-CustomProperties $CustomProperties]
```

4. 使用 `New-ProvImageVersion` 命令创建映像版本。例如，

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

5. 使用 `Add-ProvImageVersionSpec` 命令将主映像版本规范添加到映像版本。例如，

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win20
22-snapshot.snapshot"
```

> **注意：**
>
> 您只能为一个主机单元的一个映像版本添加一个主映像版本规范。

6. 使用 `New-ProvImageVersionSpec` 命令从主映像版本规范创建准备好的映像版本规范。

   `New-ProvImageVersionSpec` 的 CustomProperties 可以包括以下内容。如果您不使用这些参数，则使用默认值：

   - `PreparedImageStorageType`：用于准备好的映像的存储类型。默认为 `Standard_LRS`，也可以是 `Premium_LRS` 或 `Standard_ZRS`。`Standard_ZRS` 为映像提供区域冗余。

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb

-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resou
rcegroup\azure-vnet-eastus.virtualprivatecloud\dev.network"}

-ServiceOffering"XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceofferin
g" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"></CustomProperties>"
-RunAsynchronously
```

7. 您还可以使用 `Add-ProvImageVersionSpecHostingUnit` 命令在所有托管连接中与另一个托管单元共享准备好的映像版本规范。

`Add-ProvImageVersionSpecHostingUnit` 的 CustomProperties 可以包括以下内容。如果您不使用这些参数，则使用源准备好的映像规范中的值：

- `PreparedImageStorageType`：用于准备好的映像的存储类型。

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest
```

注意：

一个托管单元和准备类型只能有一个准备好的实例。

创建映像定义、映像版本和准备好的映像版本规范的完整 PowerShell 命令集示例：

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession



$ImageDefinitionCustomProperties = @" <CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance"> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="true" /> <Property
xsi:type="StringProperty" Name="ResourceGroups" Value="rg" /> <Property
xsi:type="StringProperty" Name="ImageGallery" Value="gallery" /> </
CustomProperties> "@



Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 -CustomProperties
$ImageDefinitionCustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"
```

```
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid ` -HostingUnitUid
$hostingunit.HostingUnitUid ` -MasterImagePath "XDHyp:
\HostingUnits\azure28\image.folder\abc.resourcegroup\def-
snapshot.snapshot"



$ImageVersionSpecCustomProperties = @'



<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">



<Property xsi:type="StringProperty" Name="PreparedImageStorageType"
Value="Premium_LRS" />



<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />



</CustomProperties>



'@



New-ProvImageVersionSpec -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network" } -CustomProperties
$ImageVersionSpecCustomProperties -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
-SourceImageVersionSpecUid $SourceImageVersionSpec.ImageVersionSpecUid
```

```
$TargetCustomProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PreparedImageStorageType"
Value="Standard_ZRS" />

</CustomProperties>

'@

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest –TargetCustomProperties $TargetCustomProperties

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注意：

- 映像定义中的所有映像版本规范必须属于同一托管单元。
- 一个映像版本只能有一个主映像版本规范和一个准备好的映像版本规范。

- 所有映像版本规范必须具有计算机配置文件，或者所有映像版本规范都不能具有计算机配置文件。

使用准备好的映像版本规范创建目录

使用 `New-ProvScheme` 命令从准备好的映像版本规范创建 MCS 计算机目录。例如，

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

或者，

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

如果要使用 ACG 映像版本规范，请将 `UseSharedImageGallery` 设置为 `true`。例如，

```
$provSchemeCustomProperties= @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

    <Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" />
```

```
</CustomProperties>

"@

New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -IdentityPoolUid $IdentityPool.IdentityPoolUid `

    -CleanOnBoot -Scope @() -SecurityGroup @() `

    -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
`

    -NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network"} `

    -CustomProperties $provSchemeCustomProperties
```

创建目录的完整 Powershell 命令集示例：

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.local"
-IdentityPoolName "azurecatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "azure##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"
```

```
$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -Scope
@() -SecurityGroup @() -ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2s.serviceoffering"
-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"}
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">    <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="true" /><Property
xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"StandardSSD_LRS`" /></CustomProperties>" -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

跨区域、订阅和租户共享加密的准备映像

Azure Compute Gallery (ACG) 映像可以使用磁盘加密集 (DES) 进行加密。借助 ACG 共享功能，您可以在 Azure 的区域、订阅和租户之间共享加密的准备映像。目标资源需要从准备映像所属的订阅中选择其区域中的 DES。之后，您可以在共享加密准备映像的资源中创建计算机目录。

共享加密准备映像的关键步骤是：

1. 在每个区域中创建磁盘加密集 (DES)：请参阅 Microsoft 文档 使用 Azure 门户为托管磁盘启用客户管理的密钥的服务器端加密。
2. 在 Azure Compute Gallery (ACG) 中为 Azure 主机连接和映像版本创建映像定义，并指定 DES 以加密准备映像：请参阅 创建映像定义和初始映像版本。
3. 跨区域、订阅和租户共享加密的预准备映像：可以使用 Web Studio 或 PowerShell 命令。

您现在可以在共享加密准备映像的资源中创建计算机目录。有关创建目录的更多信息，请参阅 在 Azure 中创建准备映像计算机目录。

> **注意：**
>
> - 如果主区域未加密，则共享区域也不能具有 DES。
> - 如果两个主机单元面向同一区域，则它们具有相同的 DES。

使用 WEB STUDIO 跨区域、订阅和租户共享加密映像

1. 右键单击映像版本，然后选择 **管理映像共享**。将列出具有区域和磁盘加密集的资源。
2. 选择要与映像版本共享的资源。创建映像版本的资源将禁用任何操作。如果未为资源配置 DES，请从下拉菜单中选择一个 DES。

   > **注意：**
   >
   > 同一区域内的资源必须使用相同的加密密钥。

3. 单击 **保存**。
4. 单击“**资源**”选项卡以获取有关共享状态的更多详细信息。

   > **注意：**
   >
   > - 当映像版本共享状态为进行中时，**删除映像版本**或**管理映像共享**选项将被禁用。
   > - 当资源成功共享后，DES 不可编辑。

使用 POWERSHELL 跨区域、订阅和租户共享加密映像

使用命令 `Add-ProvImageVersionSpecHostingUnit` 并添加参数 `CustomProperties`。在 `CustomProperties` 中，为目标资源配置 DES。共享准备好的加密映像时，每个资源都会从准备好的映像所属的订阅中选择其区域中的 DES。例如，

```
$CustomProperties = "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">"

 "<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/xxxxxx-7152-46c4-b061-xxxxxx70c/resourceGroups/
resourcegroup1/providers/Microsoft.Compute/diskEncryptionSets/desid1`" /
>"+

 "</CustomProperties>"

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <Guid>
-HostingUnitUid <Guid> -CustomProperties $CustomProperties
```

更多信息

- 映像管理

下一步操作

- 管理预准备映像计算机目录

在 Azure Local 中创建准备好的映像计算机目录

创建准备好的映像，并使用这些准备好的映像通过以下方式创建 MCS 计算机目录：

- Web 工作室
- (#use-powershell)

使用准备好的镜像创建 MCS 计算机目录的关键步骤如下：

1. 创建镜像定义和初始镜像版本。
2. 使用映像版本作为准备好的映像来创建目录。

使用 Web Studio

创建镜像定义和初始镜像版本

要创建镜像定义和初始镜像版本，请执行以下操作：

1. 在 Web Studio 中，转到**映像**节点，然后单击**创建映像定义**。在**简介**页面上单击**下一步**。
2. 在**映像定义**页面上，为映像定义指定**操作系统类型**和**会话类型**。
3. 选择现有资源组或创建新资源组以保存映像资源。

4. 在**映像**页面上，选择**资源**（仅列出适用于所设置连接的资源）和用作创建映像版本模板的映像。

> **注意：**
>
> - 在选择映像之前，请验证主映像是否已安装 VDA 2311 或更高版本，并且 VDA 上是否已安装 MCSIO 驱动程序。
> - 对于映像选择，您可以选择 Azure Local 库映像或虚拟机。

5. 在**计算机规范**页面上，为准备 VM 选择 CPU 和内存。
6. 在**网卡**页面上，为准备映像选择网卡。对于每个网卡，选择关联的虚拟网络。
7. 在**版本描述**页面上，输入所创建的初始映像版本的描述。
8. 在**摘要**页面上，检查映像定义和所创建的初始映像版本的详细信息。输入映像定义的名称和描述。单击**完成**。

创建映像版本

映像版本允许管理特定映像的不同迭代或更新。此功能使您能够维护映像的多个版本以用于不同目的。

要从初始映像版本创建映像版本，请执行以下操作：

> **注意：**
>
> 所有映像版本的主机单元必须相同。

1. 转到**映像**节点，选择一个映像版本或映像定义，然后单击**创建映像版本**。
2. 在**映像定义**页面上，您可以更改托管单元，并重新选择该映像版本的主映像和计算机配置文件。
3. 如果您希望映像版本的配置与初始配置的映像版本不同，请在**创建映像版本**对话框的**计算机规格**和**网卡**页面上配置设置。
4. 添加映像版本的描述。单击**完成**。

> **注意：**
>
> 如果映像版本创建因任何原因失败，底部“**故障排除**”选项卡提供“**重试**”选项。

从“映像”节点创建计算机目录

使用“**映像**”节点中的“**创建目录**”选项，使用映像版本创建目录。

或者，您可以在“**计算机目录**”节点中创建目录时选择版本，将其链接到目录创建工作流中的准备好的映像选项。请参阅从“计算机目录”节点创建计算机目录。

要从**映像**节点创建 MCS 计算机目录，请执行以下操作：

1. 选择一个映像版本，然后单击**创建目录**。在**简介**页面上单击**下一步**。
2. 在**桌面体验**页面上，选择所需的桌面体验。
3. 从**映像**页面到**网卡**页面，设置是根据所选映像版本预先选择的。
4. 在“**资源组**”页面上，您可以选择创建新的资源组或使用现有资源组来放置此目录的资源。
5. 在以下页面上完成设置。
6. 在**摘要**页面上，检查计算机目录的详细信息。输入计算机目录的名称和描述。单击**完成**。
7. 转到**计算机目录**节点以查看创建的计算机目录。

从计算机目录节点创建计算机目录

要从**计算机目录**节点创建 MCS 计算机目录，请执行以下操作：

1. 在左侧导航窗格中单击**计算机目录**。
2. 单击“**创建计算机目录**”。出现“**计算机目录设置**”页面。依次单击“**下一步**”通过“**简介**”和“**计算机类型**”页面。
3. 在**计算机管理**页面上：
    a. 选择“**已进行电源管理的计算机（例如，虚拟机或刀片式电脑）**”。
    b. 选择“**Citrix 预配技术**”。然后，选择“**Citrix Machine Creation Services™**”。
    c. 在**资源**字段中，列出了属于不同区域的资源。选择任何 Azure 网络资源，然后单击下一步。
4. 在**映像**页面上：
    - 对于主映像类型，请按照以下步骤操作：
        a. 选择主映像。
        b. 在主映像下，选择一个映像。该边栏列出了与资源属于同一区域的所有映像。
        c. 点击 **完成**。
    - 对于准备好的映像类型，请按照以下步骤操作：
        a. 选择**准备好的映像**。

b. 在“**准备好的映像**”下，选择映像定义的映像版本。如有需要，为所选的准备好的映像版本添加备注。

c. 单击映像版本名称。要查看有关所选映像版本的更多详细信息，请单击带下划线的版本号。

5. 配置以下页面上的设置。
6. 在“**资源组**”页面上，您可以选择创建新的资源组或使用现有资源组来放置此目录的资源。
7. 在以下页面上完成设置。
8. 在**摘要**页面上，检查计算机目录的详细信息。输入计算机目录的名称和描述。单击**完成**。

使用 PowerShell

创建准备好的映像

创建 Azure Local 准备好的映像版本规范的详细 PowerShell 命令如下：

1. 使用 `Test-ProvImageDefinitionNameAvailable command` 检查可用的映像定义名称。例如，

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. 使用 `New-ProvImageDefinition` 命令创建映像定义。例如，

```
New-ProvImageDefinition -ImageDefinitionName arc-ACG-image-climber-demo
-OsType Windows -VDASessionSupport SingleSession -Description "arc ACG
image for arc"
```

3. 使用 `Add-ProvImageDefinitionConnection` 命令在指定的托管连接中为映像定义创建新配置。

   `Add-ProvImageDefinitionConnection` 的 `CustomProperties` 可以包括以下内容。如果不使用这些参数，则使用默认值。

   `ResourceGroups`：包含基础磁盘的资源组。

   例如，对于客户提供的资源组：

```
$CustomerOwnRsourceGroupProperties = @"

<CustomProperties xmlns="http:// schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="sz_res_group" />

</CustomProperties>

"@
```

```
Add-ProvImageDefinitionConnection -HypervisorConnectionName Azurelocal
-ImageDefinitionName arc-ACG-image-climber-demo [-CustomProperties
$CustomProperties]
```

4. 使用 `New-ProvImageVersion` 命令创建映像版本。例如，

```
New-ProvImageVersion -ImageDefinitionName arc-ACG-image-climber-demo
```

5. 使用 `Add-ProvImageVersionSpec` 命令将主映像版本规范添加到映像版本。例如，

```
Add-ProvImageVersionSpec -ImageVersionNumber 1 -HostingUnitName
network-2 -MasterImagePath XDHyp:
\HostingUnits\network-2\image.folder\MST-W11WS-2507-11-10-no-
sysprep.galleryimage
```

注意：

您只能为一个主机单元的一个映像版本添加一个主映像版本规范。

6. 使用 `New-ProvImageVersionSpec` 命令从主映像版本规范创建准备好的映像版本规范。例如，

```
New-ProvImageVersionSpec -CustomProperties "<CustomProperties
xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`"
xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"citrix-
xd-39d65e7a-f6c0-4772-9e8d-d6eacb36287f-hilxi`" /><Property
xsi:type=`"StringProperty`" Name=`"OsType`" Value=`"Windows`" /></
CustomProperties>" -NetworkMapping @{"0"="XDHyp:
```

```
\HostingUnits\network-2\network.folder\VM-Network-2.network"}
-SourceImageVersionSpecUid "86c1a467-f900-4434-990a-c4ae39faca10"
```

创建映像定义、映像版本和准备好的映像版本规范的完整 PowerShell 命令集示例：

```
## create image definition

New-ProvImageDefinition -ImageDefinitionName arc-ACG-image-climber-demo
-OsType Windows -VDASessionSupport SingleSession -Description "arc ACG
image for arc"

## create image definition connection

Add-ProvImageDefinitionConnection -CustomProperties "<CustomProperties
xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`"
xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"></
CustomProperties>" -HypervisorConnectionUid "8eac2ad2-
fc81-45d6-9153-9545a779f8d2" -ImageDefinitionUid "39d65e7a-f6c0-4772-9e8d-
d6eacb36287f"

## create new image verison

New-ProvImageVersion -ImageDefinitionName arc-ACG-image-climber-demo

## select azure arc ACG image

Import-Module Citrix.Host.Commands

Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\network-2\image.folder")
| select-object fullpath

## add verison spec through Azure Arc ACG

Add-ProvImageVersionSpec -ImageVersionUid "29da7e07-b7e9-4c8c-
a5f2-4c03dbcba451" -HostingUnitUid "51305f67-34b3-4b22-a5d2-b6d7deaff9ba"
-MasterImagePath XDHyp:\HostingUnits\network-2\image.folder\MST-
W11WS-2507-11-10-no-sysprep.galleryimage

## create new version spec

New-ProvImageVersionSpec -CustomProperties "<CustomProperties
xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`"
xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"><Property
```

```
xsi:type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"citrix-
xd-39d65e7a-f6c0-4772-9e8d-d6eacb36287f-hilxi`" /><Property
xsi:type=`"StringProperty`" Name=`"OsType`" Value=`"Windows`" /></
CustomProperties>" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\network-2\network.folder\VM-Network-2.network"}
-SourceImageVersionSpecUid "86c1a467-f900-4434-990a-c4ae39faca10"
```

注意：

- 映像定义中的所有映像版本规范必须属于同一托管单元。
- 一个映像版本只能有一个主映像版本规范和一个准备好的映像版本规范。

使用准备好的映像版本规范创建目录

使用 `New-ProvScheme` 命令从准备好的映像版本规范创建 MCS 计算机目录。例如，

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

或者，

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

创建目录的完整 PowerShell 命令示例：

```
New-AcctIdentityPool -IdentityPoolName arc-climbers-local -NamingScheme
"arc-c-vm-###" -NamingSchemeType Numeric -Domain "CLIMBERS.LOCAL"

New-ProvScheme -ProvisioningSchemeName arc-ACG-img-climber-3
-HostingUnitName network-2 -IdentityPoolName arc-climbers-local
-ImageVersionSpecUid 0525360d-6cb5-4f08-bb2c-aaf5678a0d54

New-BrokerCatalog -ProvisioningSchemeId 93fbcebd-3a7a-499e-9d8d-
c09e02021c5a -AllocationType Static -Name arc-ACG-img-climber-3
-PersistUserChanges OnLocal -ProvisioningType MCS -SessionSupport
SingleSession
```

更多信息

- 映像管理

下一步操作

- 管理预准备映像计算机目录

在 Nutanix AHV Prism Central 中创建预准备映像计算机目录

创建准备好的映像，并使用这些准备好的映像通过以下方式创建 MCS 计算机目录：

- (#use-powershell)

使用准备好的镜像创建 MCS 计算机目录的关键步骤如下：

1. 创建镜像定义和初始镜像版本。
2. 使用镜像版本作为准备好的镜像来创建目录

使用 PowerShell

Nutanix PC 中映像解耦工作流的 PowerShell 示例。

设置

```
$CustomProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"><StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378"/></CustomProperties>'

$MasterImagePath="XDHyp:\HostingUnits\${HostingUnitName}
\Templates.folder\hai-vda-novtpm01.template\Initial
Version.templateversion"
```

```
$VMNetwork1A="XDHyp:\HostingUnits\${HostingUnitName}\Clusters.folder\mcs-
pvs-ntnx-cluster01.cluster\vmNwCl1-A.network"

$NetworkMapping=@{"0"=$VMNetwork1A}
```

创建映像定义和映像版本

```
$ImageDefinition = New-ProvImageDefinition -ImageDefinitionName
$ImgDefName -OsType Windows -VdaSessionSupport SingleSession

$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefinition.ImageDefinitionName -Description "V1"

Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefinition.ImageDefinitionName -HypervisorConnectionName
$HostingConnection
```

创建映像版本规范

```
$MasterImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName $HostingUnitName
-MasterImagePath $MasterImagePath

$ProvTask = New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $MasterImageVersionSpec.ImageVersionSpecUid -NetworkMapping
$NetworkMapping -MachineProfile $MachineProfile -CustomProperties
$CustomProperties -AdditionalStorageIds
00062c6d-09a3-134b-446d-58a2e17d0f88 -RunAsynchronously

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
$ImgDefName -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"
```

创建预配方案

```
$ProvTask = New-ProvScheme -ProvisioningSchemeName $ProvSchemeName
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName $HostingUnitName -IdentityPoolName $IdentityPoolName
-CleanOnBoot -Scope @() -SecurityGroup @() -NetworkMapping $NetworkMapping
-CustomProperties $CustomProperties -MachineProfile $MachineProfile
-RunAsynchronously
```

将映像版本规范复制到新群集

```
Add-ProvImageVersionSpecInstance -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -StorageID
00062c6d-09a3-134b-446d-58a2e17d0f88
```

在新群集中使用相同的预准备映像创建新的预配方案

```
$CustomProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"><StringProperty Name="ClusterId"
Value="00062c6d-09a3-134b-446d-58a2e17d0f88"/></CustomProperties>'

$ProvTask = New-ProvScheme -ProvisioningSchemeName $ProvSchemeName
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-MachineProfile $MachineProfile -HostingUnitName $HostingUnitName
-IdentityPoolName $IdentityPoolName -CleanOnBoot -Scope @() -SecurityGroup
@() -NetworkMapping $NetworkMapping -CustomProperties $CustomProperties
-RunAsynchronously
```

更多信息

- 映像管理

下一步操作

- 管理使用准备好的映像创建的目录

在 Red Hat OpenShift 中创建预准备映像计算机目录

创建准备好的映像，并使用这些准备好的映像通过以下方式创建 MCS 计算机目录：

- Web 工作室
- (#use-powershell)

使用准备好的镜像创建 MCS 计算机目录的关键步骤如下：

1. 创建镜像定义和初始镜像版本。
2. 使用镜像版本作为准备好的镜像来创建目录

使用 Web Studio

创建镜像定义和初始镜像版本

要创建镜像定义和初始镜像版本，请执行以下操作：

1. 在 Studio 中，转到**映像**节点，然后单击**创建映像定义**。在**简介**页面上单击**下一步**。
2. 在**映像定义**页面上，为映像定义指定**操作系统类型**和**会话类型**。
3. 在**映像**页面上，选择**资源**（仅列出适用于所设置连接的资源）和用作创建映像版本模板的主映像。您可以选中**使用计算机配置文件**复选框并选择一个计算机配置文件。

> **注意：**
>
> 在选择映像之前，请验证主映像是否已安装 VDA 2311 或更高版本，并且 VDA 上是否已安装 MCSIO 驱动程序。

4. 在**计算机规格**页面上，选择计算机大小。如果选择计算机配置文件，则可以看到从计算机配置文件派生的虚拟 CPU 计数，并且该计数不可更改。如果不选择计算机配置文件，则只能看到从主映像派生的内存大小。
5. 在“**网卡**”页面上，为准备映像选择网卡。对于每个网卡，选择一个关联的虚拟网络。默认情况下，选择与托管单元关联的网卡。
6. 在**版本描述**页面上，输入所创建的初始映像版本的描述。
7. 在**摘要**页面上，检查映像定义和所创建的初始映像版本的详细信息。输入映像定义的名称和描述。单击**完成**。

创建映像版本

映像版本允许管理特定映像的不同迭代或更新。此功能使您能够维护映像的多个版本以用于不同目的。

要从初始映像版本创建映像版本，请执行以下操作：

1. 转到**映像**节点，选择一个映像版本或映像定义，然后单击**创建映像版本**。
2. 在“**映像**”页面上，您可以重新选择此映像版本的主映像。
3. 如果您希望映像版本的配置与初始配置的映像版本不同，请在**创建映像版本**对话框的**计算机规格**和**网卡**页面上配置设置。
4. 添加映像版本的描述。单击**完成**。

> **注意：**
>
> 如果映像版本创建因任何原因失败，底部“**故障排除**”选项卡提供“**重试**”选项。

从“映像”节点创建计算机目录

使用“**映像**”节点中的“**创建目录**”选项，使用映像版本创建目录。

或者，您可以在**计算机目录**节点中创建目录时选择版本，链接到目录创建工作流中的准备好的映像选项。请参阅从计算机目录节点创建计算机目录

要从**映像**节点创建 MCS 计算机目录，请执行以下操作：

1. 选择一个映像版本，然后单击**创建目录**。在**简介**页面上单击**下一步**。
2. 在**计算机管理**页面上单击**下一步**。
3. 在**桌面体验**页面上，选择所需的桌面体验。
4. 从**映像**页面到**虚拟机**页面，设置会根据所选映像版本预先选择。
5. 在以下页面上完成设置。
6. 在**摘要**页面上，检查计算机目录的详细信息。输入计算机目录的名称和描述。单击**完成**。
7. 转到**计算机目录**节点以查看创建的计算机目录。

从计算机目录节点创建计算机目录

要从**计算机目录**节点创建 MCS 计算机目录，请执行以下操作：

1. 在左侧导航窗格中单击**计算机目录**。
2. 单击**创建计算机目录**。此时将显示**计算机目录设置**页面。依次单击**简介**、**计算机类型**和**计算机管理**页面上的**下一步**。
3. 在**映像**页面上：
    a. 选择**准备好的映像**。
    b. 在“**准备好的映像**”下，选择映像定义的映像版本。
    c. 单击映像版本名称。要查看有关所选映像版本的更多详细信息，请单击带下划线的版本号。
4. 配置以下页面上的设置。
5. 在**摘要**页面上，检查计算机目录的详细信息。输入计算机目录的名称和描述。单击**完成**。

使用 PowerShell

创建准备好的映像

用于创建准备好的映像版本规范的详细 PowerShell 命令如下：

1. 使用 `Test-ProvImageDefinitionNameAvailable command` 检查可用的映像定义名称。例如，

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. 使用 `New-ProvImageDefinition` 命令创建映像定义。例如，

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport SingleSession
```

3. 使用 `Add-ProvImageDefinitionConnection` 命令在指定的主机连接中为映像定义创建新配置。例如，

```
Add-ProvImageDefinitionConnection -ImageDefinitionUid
$imageDef.ImageDefinitionUid -HypervisorConnectionUid
"00000000-0000-0000-0000-000000000000"
```

4. 使用 `New-ProvImageVersion` 命令创建映像版本。例如，

```
New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. 使用 `Add-ProvImageVersionSpec` 命令将主映像版本规范添加到映像版本。例如，

```
Add-ProvImageVersionSpec -MasterImagePath "XDHyp:
\HostingUnits\YourHostingUnitName\YourMasterImage.vm" -HostingUnitUid
"11111111-1111-1111-1111-111111111111" -ImageVersionUid
$imageVersion.ImageVersionUid
```

> **注意：**
>
> 您只能为一个主机单元的一个映像版本添加一个主映像版本规范。

6. 使用 `New-ProvImageVersionSpec` 命令从主映像版本规范创建准备好的映像版本规范。例如，

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
$masterImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"1" =
"XDHyp:
```

```
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetwo
rkAttachmentDefinition.network" }
```

创建映像定义、映像版本和准备好的映像版本规范的完整 PowerShell 命令集示例：

```
$imageDef = New-ProvImageDefinition -ImageDefinitionName "ImageDefinition"
-OsType "Windows" -VDASessionSupport "MultiSession"




$task = Add-ProvImageDefinitionConnection -ImageDefinitionUid
$imageDef.ImageDefinitionUid -HypervisorConnectionUid
"00000000-0000-0000-0000-000000000000"



$imageVersion = New-ProvImageVersion -ImageDefinitionName
"ImageDefinition"






$masterImageVersionSpec = Add-ProvImageVersionSpec -MasterImagePath
"XDHyp:\HostingUnits\YourHostingUnitName\YourMasterImage.vm"
-HostingUnitUid "11111111-1111-1111-1111-111111111111" -ImageVersionUid
$imageVersion.ImageVersionUid






$newProvImageVersionSpecResult = New-ProvImageVersionSpec
-SourceImageVersionSpecUid $masterImageVersionSpec.ImageVersionSpecUid
-NetworkMapping @{"1" = "XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetworkA
ttachmentDefinition.network" }
```

注意：

- 映像定义中的所有映像版本规范必须属于同一托管单元。
- 一个映像版本只能有一个主映像版本规范和一个准备好的映像版本规范。
- 所有映像版本规范必须具有计算机配置文件，或者所有映像版本规范都不能具有计算机配置文件。

使用准备好的映像版本规范创建目录

使用 `New-ProvScheme` 命令从准备好的映像版本规范创建 MCS 计算机目录。例如，

```
$getProvImageVersionSpecResult = Get-ProvImageVersionSpec
-ImageVersionSpecUid $newProvImageVersionSpecResult.ImageVersionSpecUid



New-ProvScheme -ImageVersionSpecUid
$newProvImageVersionSpecResult.ImageVersionSpecUid -ProvisioningSchemeName
"ProvSchemeImageDecoupling" -HostingUnitName "YourHostingUnitName"
-IdentityPoolName "YourIdentityPoolName" -NetworkMapping @{"1" = "XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetworkA
ttachmentDefinition.network"}
```

更多信息

- 映像管理

下一步操作

- 管理预准备映像计算机目录

在 VMware 中创建预准备映像计算机目录

创建准备好的映像，并使用这些准备好的映像通过以下方式创建 MCS 计算机目录：

- Web 工作室
- (#use-powershell)

使用准备好的镜像创建 MCS 计算机目录的关键步骤如下：

1. 创建镜像定义和初始镜像版本。
2. 使用镜像版本作为准备好的镜像来创建目录

使用 Web Studio

创建镜像定义和初始镜像版本

要创建镜像定义和初始镜像版本，请执行以下操作：

1. 在 Studio 中，转到**映像**节点，然后单击**创建映像定义**。在**简介**页面上单击**下一步**。
2. 在**映像定义**页面上，为映像定义指定**操作系统类型**和**会话类型**。
3. 在**映像**页面上，选择**资源**（仅列出适用于所设置连接的资源）和用作创建映像版本模板的主映像。您可以选中**使用计算机配置文件**复选框并选择一个计算机配置文件。

> **注意：**
>
> 在选择映像之前，请验证主映像是否已安装 VDA 2311 或更高版本，并且 VDA 上是否已安装 MCSIO 驱动程序。

4. 在**计算机规格**页面上，选择计算机大小。如果选择计算机配置文件，则可以看到从计算机配置文件派生的虚拟 CPU 计数，并且该计数不可更改。如果不选择计算机配置文件，则只能看到从主映像派生的内存大小。
5. 在 **NICs** 页面上，选择或添加用于准备映像的 NIC。对于每个 NIC，选择一个关联的虚拟网络。如果您不选择计算机配置文件，则默认选择与主映像关联的 NIC。如果您选择计算机配置文件，则 NIC 将从计算机配置文件派生，并且数量不可更改。
6. 在**版本描述**页面上，输入所创建的初始映像版本的描述。
7. 在**摘要**页面上，检查映像定义和所创建的初始映像版本的详细信息。输入映像定义的名称和描述。单击**完成**。

创建映像版本

映像版本允许管理特定映像的不同迭代或更新。此功能使您能够维护映像的多个版本以用于不同目的。

要从初始映像版本创建映像版本，请执行以下操作：

1. 转到**映像**节点，选择一个映像版本或映像定义，然后单击**创建映像版本**。
2. 在 **Image** 页面上，您可以在同一托管连接中更改托管单元，并重新选择该映像版本的主映像和计算机配置文件。
3. 如果您希望映像版本的配置与初始配置的映像版本不同，请在**创建映像版本**对话框的**计算机规格**和**网卡**页面上配置设置。
4. 添加映像版本的描述。单击**完成**。

注意：

如果映像版本创建因任何原因失败，底部“**故障排除**”选项卡提供“**重试**”选项。

共享预准备映像

先决条件

共享预准备映像使用冷迁移在 vCenter Server 实例之间复制映像。以下先决条件适用于属于不同托管连接的托管单元：

- vCenter Server 之间的冷迁移：冷迁移要求两个环境都支持跨 vCenter 迁移。
  - 两个 vCenter Server 都必须运行 vSphere 7.0 或更高版本（建议使用 vSphere 8.0+）。
  - 不需要增强型链接模式。

  端口要求：确保为迁移打开以下端口：

源	目标	端口	协议	目的
源 vCenter 服务器	目标 vCenter Server	443	TCP	vCenter 之间的 API 通信
源 ESXi 主机	目标 ESXi 主机	902	TCP	NFC（网络文件复制）数据传输
源 ESXi 主机	目标 ESXi 主机	8000	TCP	vMotion 流量

注意：

端口必须双向开放。迁移主要使用 NFC（端口 902）进行数据传输，使用端口 443 进行管理。端口 8000 可能会根据路径使用。源 vCenter 必须在克隆操作期间验证目标的 SSL 证书指纹。

VMkernel 适配器配置：

ESXI 主机	所需服务
源 ESXi 主机	预配或管理
目标 ESXi 主机	与源相同的服务（预配或管理）

双方必须在 VMkernel 适配器上启用相同的流量服务（预配或管理）。不匹配会导致迁移失败。

在 vSphere Client 中，在 **主机 > 配置 > 网络 > VMkernel 适配器** 下进行验证。

已知限制：自定义存储策略在跨 vCenter 复制期间不会保留。将应用目标数据存储的默认存储策略。

- 启用 vTPM 的计算机配置文件：密钥提供程序兼容性。对于启用 vTPM 的配置文件，两个 vCenter Server 都必须访问兼容的密钥提供程序。

要求	详细信息
相同的密钥提供程序访问	目标 vCenter 必须能够访问与源相同的密钥提供程序，或者使用本机密钥提供程序作为桥接。
密钥材料	对于外部 KMS：两个 vCenter 都必须注册到同一个 KMS 群集（或共享密钥材料的 KMS 群集）。
本机密钥提供程序	在两个 vCenter Server 上配置本机密钥提供程序。每个 vCenter 的本机密钥提供程序都是独立的，但 vSphere 接受此组合用于跨 vCenter 操作。如果源和目标不共享外部 KMS，本机密钥提供程序也可以充当桥接。在使用前，必须在两个 vCenter 上备份本机密钥提供程序。

注意：

本机密钥提供程序是最简单的选项。在两台服务器上配置并备份它。如果使用外部 KMS，请确保两个 vCenter 共享相同的群集或密钥材料。在为启用 vTPM 的目录启用映像共享之前，请在 **vSphere Client 中，在 vCenter > 配置 > 安全 > 密钥提供程序** 下验证密钥提供程序配置。

跨不同主机单元共享准备好的映像

要跨不同托管单元共享准备好的映像，请按照以下步骤操作：

1. 右键单击映像版本并选择 **管理映像共享**。您的 VMware 环境中的所有托管单元都会显示。创建映像版本的资源将禁用任何操作。
2. 选择要共享映像的托管单元，然后单击“**保存**”。 “**共享状态**”列显示“**正在进行**”。
3. 单击底部的“**资源**”选项卡，了解有关共享状态的更多详细信息。

> **注意：**
>
> 当映像版本共享状态正在进行时，“**删除映像版本**”或“**管理映像共享**”选项处于禁用状态。 要与不同 VMware 连接中的托管单元共享映像，请确保满足以下要求：
>
> - 两个连接可以相互通信。
> - 虚拟机管理程序版本一致。
> - 在源主机和目标主机的管理 VMkernel 适配器上都启用了预配服务。**主机 > 配置 > 网络 > VMkernel 适配器**是 VMware vSphere Client 中的导航路径。

从“映像”节点创建计算机目录

使用“**映像**”节点中的“**创建目录**”选项，使用映像版本创建目录。

或者，您可以在**计算机目录**节点中创建目录时选择版本，链接到目录创建工作流中的准备好的映像选项。请参阅从计算机目录节点创建计算机目录

要从**映像**节点创建 MCS 计算机目录，请执行以下操作：

1. 选择一个映像版本，然后单击**创建目录**。在**简介**页面上单击**下一步**。
2. 在**桌面体验**页面上，选择所需的桌面体验。
3. 从**映像**页面到**虚拟机**页面，设置会根据所选映像版本预先选择。
4. 在以下页面上完成设置。
5. 在**摘要**页面上，检查计算机目录的详细信息。输入计算机目录的名称和描述。单击**完成**。
6. 转到**计算机目录**节点以查看创建的计算机目录。

从计算机目录节点创建计算机目录

要从**计算机目录**节点创建 MCS 计算机目录，请执行以下操作：

1. 在左侧导航窗格中单击**计算机目录**。
2. 单击**创建计算机目录**。此时将显示**计算机目录设置**页面。依次单击**简介**、**计算机类型**和**计算机管理**页面上的**下一步**。
3. 在**映像**页面上：
   a. 选择**准备好的映像**。
   b. 在“**准备好的映像**”下，选择映像定义的映像版本。
   c. 单击映像版本名称。要查看有关所选映像版本的更多详细信息，请单击带下划线的版本号。
   d. 如果所选映像版本配置了计算机配置文件，请选择一个计算机配置文件。如果所选映像版本未配置计算机配置文件，则无法选择使用计算机配置文件。
4. 配置以下页面上的设置。
5. 在**摘要**页面上，检查计算机目录的详细信息。输入计算机目录的名称和描述。单击**完成**。

使用 PowerShell

创建准备好的映像

用于创建准备好的映像版本规范的详细 PowerShell 命令如下：

1. 使用 `Test-ProvImageDefinitionNameAvailable command` 检查可用的映像定义名称。例如，

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. 使用 `New-ProvImageDefinition` 命令创建映像定义。例如，

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport SingleSession
```

3. 使用 `Add-ProvImageDefinitionConnection` 命令在指定的主机连接中为映像定义创建新配置。例如，

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware
```

4. 使用 `New-ProvImageVersion` 命令创建映像版本。例如，

```
New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. 使用 `Add-ProvImageVersionSpec` 命令将主映像版本规范添加到映像版本。例如，

```
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName vmware
-MasterImagePath $MasterImagePath
```

> **注意：**
>
> 您只能为一个主机单元的一个映像版本添加一个主映像版本规范。

6. 使用 `New-ProvImageVersionSpec` 命令从主映像版本规范创建准备好的映像版本规范。例如，

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping
@{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM Network.network"}
-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

7. 您还可以使用 `Add-ProvImageVersionSpecHostingUnit` 命令在同一托管连接中与另一个托管单元共享准备好的映像版本规范。例如，

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc
```

创建映像定义、映像版本和准备好的映像版本规范的完整 PowerShell 命令集示例：

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport Single
```

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware



$imageVersion = New-ProvImageVersion -ImageDefinitionName image2



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\vmware\shuaiz-win10-
master.vm\shuaiz-win10-master-snap.snapshot"



New-ProvImageVersionSpec -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid `

    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-
VMNetwork.network"} `

    -VMCpuCount 2 -VMMemoryMB 4096




Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc

 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注意：

- 映像定义中的所有映像版本规范必须属于同一托管单元。
- 一个映像版本只能有一个主映像版本规范和一个准备好的映像版本规范。
- 所有映像版本规范必须具有计算机配置文件，或者所有映像版本规范都不能具有计算机配置文件。

使用准备好的映像版本规范创建目录

使用 `New-ProvScheme` 命令从准备好的映像版本规范创建 MCS 计算机目录。例如，

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

或者，

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

在 VMware 中使用准备好的映像版本规范创建目录的示例：

```
New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitName $hostingunit.c-IdentityPoolName
$IdentityPool.IdentityPoolName `

    -CleanOnBoot -Scope @() -SecurityGroup @() -VMCpuCount 2 -VMMemoryMB
```

```
8192 `

    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM
Network.network"}
```

创建目录的完整 Powershell 命令集示例：

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain
"vmware.local" -IdentityPoolName "vmwarecatalog" -IdentityType
"ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "Numeric"
-Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image2 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
-Scope @() -SecurityGroup @() -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

更多信息

- 映像管理

下一步操作

- 管理预准备映像计算机目录

在 XenServer® 中创建准备好的映像计算机目录

创建准备好的映像，并使用这些准备好的映像通过以下方式创建 MCS 计算机目录：

- Web 工作室
- (#use-powershell)

使用准备好的镜像创建 MCS 计算机目录的关键步骤如下：

1. 创建镜像定义和初始镜像版本。
2. 使用镜像版本作为准备好的镜像来创建目录

使用 Web Studio

创建镜像定义和初始镜像版本

要创建镜像定义和初始镜像版本，请执行以下操作：

1. 在 Studio 中，转到**映像**节点，然后单击**创建映像定义**。在**简介**页面上单击**下一步**。
2. 在“**映像定义**”页面上，为映像定义指定“**操作系统类型**”、“**会话类型**”和“**连接**”。
3. 在“**映像**”页面上，选择“**资源**”（仅列出适用于所设置连接的资源）和要用作创建映像版本模板的主映像。

> **注意：**
>
> - 在选择镜像之前，请验证主镜像是否已安装 VDA 2311 或更高版本，并且 VDA 上已安装 MCSIO 驱动程序。

4. 在“**计算机规范**”页面上，您只能看到从主映像派生的内存大小，并且可以根据需要进行更改。
5. 在“**网卡**”页面上，为准备映像选择网卡。对于每个网卡，选择一个关联的虚拟网络。默认情况下，选择与主映像关联的网卡。
6. 在**版本描述**页面上，输入所创建的初始映像版本的描述。
7. 在**摘要**页面上，检查映像定义和所创建的初始映像版本的详细信息。输入映像定义的名称和描述。单击**完成**。

创建映像版本

映像版本允许管理特定映像的不同迭代或更新。此功能使您能够维护映像的多个版本以用于不同目的。

要从初始映像版本创建映像版本，请执行以下操作：

1. 转到**映像**节点，选择一个映像版本或映像定义，然后单击**创建映像版本**。
2. 在“**映像**”页面上，更改托管单元，并根据需要重新选择主映像。
3. 要使用与初始映像版本不同的设置，请在“**创建映像版本**”对话框的“**计算机规范**”和“**网卡**”页面上配置设置。
4. 添加映像版本的描述。单击**完成**。

> **注意：**
>
> 如果映像版本创建因任何原因失败，底部“**故障排除**”选项卡提供“**重试**”选项。

共享准备好的映像

要在 XenServer 的不同主机单元之间共享准备好的映像，请执行以下步骤：

1. 右键单击映像版本，然后选择“**管理映像共享**”。将列出所选连接下的所有主机单元。创建映像版本的资源已禁用任何操作。
2. 选择要共享映像的主机单元，然后单击“**保存**”。“**共享状态**”列显示“**正在进行**”。
3. 单击“**资源**”选项卡以获取有关共享状态的更多详细信息。

> **注意：**
>
> 当映像版本共享状态正在进行时，删除映像版本或管理映像共享的选项将被禁用。

从“映像”节点创建计算机目录

使用“**映像**”节点中的“**创建目录**”选项，使用映像版本创建目录。

或者，您可以在**计算机目录**节点中创建目录时选择版本，链接到目录创建工作流中的准备好的映像选项。请参阅从计算机目录节点创建计算机目录

要从**映像**节点创建 MCS 计算机目录，请执行以下操作：

1. 选择一个映像版本，然后单击**创建目录**。在**简介**页面上单击**下一步**。
2. 在“**计算机管理**”页面上，选择托管单元，然后单击“**下一步**”。
3. 在**桌面体验**页面上，选择所需的桌面体验。
4. 从**映像**页面到**虚拟机**页面，设置会根据所选映像版本预先选择。

5. 在以下页面上完成设置。
6. 在**摘要**页面上，检查计算机目录的详细信息。输入计算机目录的名称和描述。单击**完成**。
7. 转到**计算机目录**节点以查看创建的计算机目录。

从计算机目录节点创建计算机目录

要从**计算机目录**节点创建 MCS 计算机目录，请执行以下操作：

1. 在左侧导航窗格中单击**计算机目录**。
2. 单击**创建计算机目录**。此时将显示**计算机目录设置**页面。依次单击**简介**、**计算机类型**和**计算机管理**页面上的**下一步**。
3. 在**映像**页面上：
   a. 选择**准备好的映像**。
   b. 在“**准备好的映像**”下，选择映像定义的映像版本。
   c. 选择映像版本。要查看有关所选映像版本的更多详细信息，请单击带下划线的版本号。
4. 在以下页面上完成设置。
5. 在**摘要**页面上，检查计算机目录的详细信息。输入计算机目录的名称和描述。单击**完成**。

使用 PowerShell

创建准备好的映像

用于创建准备好的映像版本规范的详细 PowerShell 命令如下：

1. 使用 `Test-ProvImageDefinitionNameAvailable command` 检查可用的映像定义名称。例如，

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName xenimage1
```

2. 使用 `New-ProvImageDefinition` 命令创建映像定义。例如，

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName
xenimage1 -OsType Windows -VdaSessionSupport SingleSession
```

3. 使用 `Add-ProvImageDefinitionConnection` 命令在指定的托管连接中为映像定义创建新配置。

```
Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -HypervisorConnectionName
XenServer1
```

4. 使用 `New-ProvImageVersion` 命令创建映像版本。例如，

```
$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. 使用 `Add-ProvImageVersionSpec` 命令将主映像版本规范添加到映像版本。例如，

```
$MasterImagePath = "XDHyp:\HostingUnits\xenhu \win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName xenhu
-MasterImagePath $MasterImagePath
```

> **注意：**
>
> 您只能为一个主机单元的一个映像版本添加一个主映像版本规范。

6. 使用 `New-ProvImageVersionSpec` 命令从主映像版本规范创建准备好的映像版本规范。例如，

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping
@{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}

-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

7. 您还可以使用 `Add-ProvImageVersionSpecHostingUnit` 命令在同一托管连接中与另一个托管单元共享准备好的映像版本规范。例如，

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName xenhu2
```

创建映像定义、映像版本和准备好的映像版本规范的完整 PowerShell 命令集示例：

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName xenimage1
-OsType Windows -VdaSessionSupport SingleSession




Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -HypervisorConnectionName XenServer1



$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"



$MasterImagePath = "XDHyp:\HostingUnits\xenhu \win10-master.vm\win10-
master-snap.snapshot"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName xenhu -MasterImagePath
$MasterImagePath




New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\xenhu\VM Network.network"}

 -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName xenhu2
```

注意：

- 一个映像版本只能有一个主映像版本规范和一个准备好的映像版本规范。
- 所有映像版本规范必须具有计算机配置文件，或者所有映像版本规范都不能具有计算机配置文件。

使用准备好的映像版本规范创建目录

使用 `New-ProvScheme` 命令从准备好的映像版本规范创建 MCS 计算机目录。例如，

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

或者，

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

使用 XenServer 中的准备好的映像版本规范创建目录的示例：

```
New-ProvScheme -ProvisioningSchemeName assignimage -imageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid 1 `

  -HostingUnitName xenhu -IdentityPoolName poo1 `

  -CleanOnBoot -Scope @() -SecurityGroup @() -VMCpuCount 2 -VMMemoryMB
8192 `

  -NetworkMapping @{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}
```

创建目录的完整 Powershell 命令集示例：

```
$CatalogName = "XenCatalog"

$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" `

  -Name $CatalogName -PersistUserChanges "Discard" -ProvisioningType "MCS"
-Scope @() -SessionSupport "MultiSession"




$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "xen.local"
-IdentityPoolName $CatalogName `

  -IdentityType "ActiveDirectory"  -NamingScheme "xen##" -NamingSchemeType
"Numeric" -Scope @()




$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
xenimage1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"




$Task = New-ProvScheme -ProvisioningSchemeName $CatalogName
```

```
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid `

  -HostingUnitName xenhu -IdentityPoolName $CatalogName -CleanOnBoot
-Scope @() -SecurityGroup @() `

  -NetworkMapping @{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}
-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName $CatalogName




Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

更多信息

- 映像管理

下一步操作

- 管理预准备映像计算机目录

管理准备好的映像计算机目录

您可以使用不同的准备好的映像更新现有 MCS 计算机目录，并使用以下方式管理映像定义和版本：

- Web 工作室
- (#use-powershell)

使用 Web Studio

使用不同的准备好的映像更新计算机目录

要使用不同的准备好的映像更新现有 MCS 计算机目录，请执行以下操作：

1. 在左侧导航窗格中单击**计算机目录**，然后选择要更新的计算机目录。右键单击并选择**更改准备好的映像**。

2. 在**映像**页面上，选择一个准备好的映像。如果需要，为所选的准备好的映像添加备注。

> **注意：**
>
> 适用于 Azure：您还可以选择未启用 ACG 的映像，然后选择**将准备好的映像置于 Azure 计算库中**复选框，将映像置于库中。

3. 要回滚到以前分配的准备好的映像，请单击向导底部的**使用以前的映像分配进行快速回滚**。

   将打开一个新窗口，其中显示所有可用的历史映像分配列表。当您从列表中选择一个映像时，映像页面上准备好的映像树中会自动选择相应的版本。

4. 在“**推出策略**”页面上，选择何时要使用选定的准备好的映像更新此目录。
5. 在**摘要**页面上，检查详细信息。单击**完成**。

您可以查看对目录所做的映像更改历史记录。要查看历史记录，请执行以下操作：

1. 选择一个计算机目录。
2. 在**模板属性**选项卡中的**准备好的映像**字段下，单击**查看映像历史记录**。

管理映像定义和版本

您可以编辑和删除映像定义和版本，以管理各种已创建映像版本和定义的使用。

编辑映像定义

您可以编辑映像定义的名称和描述。

要编辑映像定义，请执行以下操作：

1. 转到“**映像**”节点，选择一个映像定义，然后选择“**编辑映像定义**”。

编辑映像版本

您可以编辑映像版本的描述，以指定该映像版本的用途。

要编辑映像版本，请执行以下操作：

1. 转到“**映像**”节点，选择一个映像版本，然后选择“**编辑描述**”。

删除映像版本

要删除映像版本，请执行以下操作：

1. 转到“**映像**”节点，选择一个映像版本，然后选择“**删除映像版本**”。

> **注意：**
>
> 如果映像版本正在被计算机目录使用，则无法将其删除。

删除映像定义

要删除映像定义，请执行以下操作：

1. 转到**映像**节点，选择一个映像定义，然后选择**删除映像定义**。

> **注意：**
>
> 如果映像定义包含映像版本，则无法删除该映像定义。

使用 PowerShell

使用准备好的映像版本规范更新目录

您可以使用 `Set-ProvSchemeImage` 命令更新目录。例如，

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess][-
ImageAssignmentNote <string>]
```

或者，

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess][-
ImageAssignmentNote <string>]
```

更新目录的完整 Powershell 命令集示例：

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 2 -Filter "PreparationType -eq 'Mcs'"



Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog
```

```
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-RunAsynchronously -ImageAssignmentNote "Update from VST team"
```

获取预配方案的映像更改历史记录

```
Get-ProvSchemeImageVersionSpecHistory -ProvisioningSchemeName azurecatalog
```

删除映像定义、映像版本和准备好的映像版本规范

在删除映像定义、映像版本和准备好的映像版本规范之前，请考虑以下事项：

- 如果映像定义包含任何映像版本，则无法删除该映像定义。
- 如果映像版本包含任何映像版本规范，则无法删除该映像版本。
- 如果主映像版本规范被任何其他准备好的映像版本规范使用，则无法删除该主映像版本规范。
- 如果准备好的映像版本规范被任何 MCS 计算机目录使用，则无法删除该准备好的映像版本规范。
- 如果托管单元被任何其他准备好的映像版本规范使用，则无法删除该托管单元。

详细步骤如下：

1. 删除计算机目录。例如，

   ```
   Remove-ProvScheme -ProvisioningScheneName decouplingCatalog
   ```

2. 删除共享的准备好的映像版本规范。例如，

   ```
   Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>
   -HostingUnitName AzureWest
   ```

3. 删除准备好的映像版本规范。例如，

   ```
   $PreparedImageVersionSpec = Get-ProvImageVersionSpec
   -ImageDefinitionName image1 -ImageVersionNumber 1 -Filter
   "PreparationType -eq 'Mcs'"



   Remove-ProvImageVersionSpec -ImageVersionSpecUid
   $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
   ```

4. 删除主映像版本规范。例如，

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronousl
```

> **注意：**
>
> 主映像版本规范只能在没有关联的准备好的映像版本规范时删除。

5. 删除映像版本。例如，

```
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
1
```

6. 删除指定托管连接中映像定义的配置。例如，

```
Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx
```

7. 删除映像定义。例如，

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

当准备好的映像未在主机单元之间共享时，完整的 PowerShell 命令集示例：

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"
```

```
Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1



Remove-ProvImageDefinition -ImageDefinitionName image1
```

当准备好的映像在主机单元之间共享时，完整的 PowerShell 命令集示例：

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog



Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>

-HostingUnitName AzureWest



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1



Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx



Remove-ProvImageDefinition -ImageDefinitionName image1
```

管理映像定义和映像版本

您可以重命名和编辑映像定义，以及编辑映像版本。

- 使用 `Rename-ProvImageDefinition` 命令重命名映像定义。例如：

  ```
  Rename-ProvImageDefinition -ImageDefinitionUid <Guid>
  -NewImageDefinitionName <string>
  ```

  或者，

  ```
  Rename-ProvImageDefinition -ImageDefinitionName <string>
  -NewImageDefinitionName <string>
  ```

- 使用 `Set-ProvImageDefinition` 命令编辑映像定义。例如：

  ```
  Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
  <string>]
  ```

  或者，

```
Set-ProvImageDefinition -ImageDefinitionName <string> [-Description
<string>]
```

- 使用 `Set-ProvImageVersion` 命令编辑映像版本。例如：

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <string>]
```

或者，

```
Set-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber
<int> [-Description <string>]
```

获取映像定义、映像版本、准备好的映像版本规范和预配方案详细信息

- 使用 `Get-ProvImageDefinition` 命令获取映像定义详细信息。例如：

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount
<int>] [-Skip <int>] [-SortBy <string>] [-Filter <string>]
```

- 使用 `Get-ProvImageVersion` 命令获取映像版本详细信息。例如：
  - 要列出映像定义中的映像版本，

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    或者，

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - 要获取映像版本详细信息，

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    ```

    或者，

```
Get-ProvImageVersion -ImageDefinitionName <string>
-ImageVersionNumber <int>
```

- 使用 `Get-ProvImageVersionSpec` 命令获取准备好的映像版本规范。例如：
  - 要列出映像版本中的所有准备好的映像版本规范，

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid>
```

  - 要列出准备好的映像版本规范中的主映像版本规范，

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "None"'
```

  - 要列出与主映像关联的映像版本中的准备好的映像版本规范，

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
```

  - 要获取映像版本中成功的准备好的映像版本规范，

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and ImageVersionSpecStatus
-eq "Complete"'
```

  - 要获取准备好的映像版本规范详细信息，

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- 使用 `Get-ProvScheme` 命令获取预配方案详细信息。例如：

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <String>]
[-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-
SortBy <String>] [-Filter <String>] [-FilterScope <Guid>]
```

- 使用 `Get-ProvSchemeImageVersionSpecHistory` 命令获取预配方案的准备好的映像版本规范历史记录。例如：

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName
<String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid <Guid>]
[-ImageVersionSpecHistoryUid <Guid>] [-ReturnTotalRecordCount] [-
MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter
<String>] [-FilterScope <Guid>]
```

更多信息

- 映像管理

创建计算机目录

重要提示：

自 Citrix Virtual Apps and Desktops™ 7 2006 起，如果您的当前部署使用了以下任何技术，则只有在移除使用这些技术的生命周期结束 (EOL) 项目后，才能将部署升级到当前版本。

- 个人 vDisk (PvD)
- AppDisks™
- 公有云主机类型：Citrix CloudPlatform、Microsoft Azure Classic

有关详细信息，请参阅移除 PVD、AppDisks 和不受支持的主机。

注意：

从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 唯一的管理控制台。Citrix Studio（基于 MMC）已从安装程序中移除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

如果您的部署要使用公有云主机连接，则需要混合权利许可证才能完成全新安装或升级到当前版本。

当安装程序检测到一个或多个不受支持的技术或没有混合权利许可证的主机连接时，升级会暂停或停止。此时会显示一条解释性消息。安装程序日志中包含详细信息。有关详细信息，请参阅升级和迁移。

简介

物理机或虚拟机集合作为称为“计算机目录”的单个实体进行管理。目录中的所有计算机都具有相同类型的操作系统：多会话操作系统或单会话操作系统，以及 Windows 或 Linux 计算机。

> **注意：**
>
> 有关使用计算机目录预配 macOS 计算机的详细信息，请参阅 macOS VDA 文档中的本文。

创建站点后，Web Studio 会引导您创建第一个计算机目录。创建第一个目录后，Web Studio 会引导您创建第一个交付组。之后，您可以更改已创建的目录，并创建更多目录。

> **提示：**
>
> 升级现有部署会启用 Machine Creation Services (MCS) 存储优化 (MCS I/O) 功能，无需额外配置。Virtual Delivery Agent (VDA) 和 Delivery Controller 升级会处理 MCS I/O 升级。

概述

创建 VM 目录时，您需要指定如何预配这些 VM。您可以使用 Machine Creation Services™ (MCS)。或者，您可以使用自己的工具来提供计算机。

注意事项：

- MCS 支持虚拟机映像中的单个系统磁盘。它会忽略附加到该映像的其余数据磁盘。
- 如果您使用 MCS 预配 VM，则需要提供一个主映像（或映像快照）以在目录中创建相同的 VM。在创建目录之前，您首先使用工具创建和配置主映像。此过程包括在映像上安装 Virtual Delivery Agent (VDA)。然后，您在 Web Studio 中创建计算机目录。您选择该映像（或快照），指定要在目录中创建的 VM 数量，并配置其他信息。
- 如果您的计算机已可用，您仍然需要为这些计算机创建一个或多个计算机目录。
- 如果您直接使用 PowerShell SDK 创建目录，可以指定一个管理程序模板 (**VMTemplates**)，而不是映像或快照。

- 使用模板预配目录被视为一项实验性功能。使用此方法时，虚拟机准备可能会失败。因此，无法使用该模板发布目录。

使用 MCS 或 Citrix Provisioning™ 创建第一个目录时，您将使用创建站点时配置的主机连接。稍后（创建第一个目录和交付组后），您可以更改有关该连接的信息或创建更多连接。

完成目录创建向导后，测试会自动运行以确保其配置正确。测试完成后，您可以查看测试报告。您可以随时从 Web Studio 运行测试。

> **注意：**
>
> MCS 不支持 Windows 10 IoT Core 和 Windows 10 IoT Enterprise。有关详细信息，请参阅 Microsoft 站点。
>
> 有关 Citrix Provisioning 工具的技术详细信息，请参阅Citrix Virtual Apps and Desktops 映像管理。

RDS 许可证检查

Web Studio 目前在创建包含 Windows 多会话操作系统计算机的计算机目录时，不执行对有效 Microsoft RDS 许可证的检查。要查看 Windows **多会话操作系统计算机**的 Microsoft RDS 许可证状态，请转至 Citrix Director。在**计算机详细信息**面板中查看 Microsoft RDS 许可证的状态。此面板位于**计算机详细信息和用户详细信息**页面中。有关详细信息，请参阅Microsoft RDS 许可证运行状况。

VDA 注册

启动代理会话时，VDA 必须向 Delivery Controller™ 注册。未注册的 VDA 可能会导致可用资源利用不足。VDA 未注册的原因有很多，其中许多原因管理员都可以进行故障排除。Web Studio 在目录创建向导中以及将计算机从目录添加到交付组后提供故障排除信息。

使用向导添加现有计算机后，计算机帐户名称列表会指示每台计算机是否适合添加到目录中。将鼠标悬停在每台计算机旁边的图标上，可显示有关该计算机的信息性消息。

如果消息标识了有问题的计算机，请删除该计算机，或添加该计算机。例如，如果消息指示可能无法获取有关计算机的信息，则仍可添加该计算机。

有关详细信息，请参阅：

- CTX136668，用于 VDA 注册故障排除指南
- VDA 版本和功能级别
- VDA 注册方法

MCS 目录创建摘要

以下是您在目录创建向导中提供信息后，默认 MCS 操作的简要概述。

- 如果您选择的是主映像（而不是快照），MCS 会创建一个快照。
- MCS 会创建快照的完整副本，并将该副本放置在主机连接中定义的每个存储位置。
- MCS 将计算机添加到 Active Directory，从而创建唯一的身份。
- MCS 会创建向导中指定的虚拟机数量，并为每个虚拟机定义两个磁盘。除了每个虚拟机的两个磁盘外，主映像也存储在同一存储位置。如果您定义了多个存储位置，则每个位置都会获得以下磁盘类型：
  - 快照的完整副本，它是只读的，并在刚创建的虚拟机之间共享。
  - 一个唯一的 16 MB 身份磁盘，为每个 VM 提供唯一的身份。每个 VM 都会获得一个身份磁盘。
  - 一个唯一的差异磁盘，用于存储对 VM 所做的写入。如果主机存储支持，此磁盘将进行精简预配，并在必要时增加到主映像的最大大小。每个 VM 都会获得一个差异磁盘。差异磁盘保存会话期间所做的更改。对于专用桌面，它是永久性的。对于池化桌面，它会在每次通过交付控制器重新启动后被删除并创建一个新的。
  - 对于 VDA 版本 2511 或更高版本上的 Windows VM，MCS 会为每台计算机分配一个唯一的 `MachineGuid`。此 `MachineGuid` 由 VDA 上安装的某些软件用于许可目的。

或者，在创建用于交付静态桌面的 VM 时，您可以在目录创建向导的**计算机**页面上指定厚（完整副本）VM 克隆。完整克隆不需要在每个数据存储上保留主映像。每个 VM 都有自己的文件。

MCS 存储注意事项

在决定 MCS 的存储解决方案、配置和容量时，有许多因素需要考虑。以下信息提供了存储容量的适当注意事项：

容量注意事项:

- 磁盘

  在大多数 MCS 部署中，Delta 或差异 (Diff) 磁盘为每个 VM 消耗最大的空间。MCS 创建的每个 VM 在创建时至少会获得 2 个磁盘。

  - Disk0 = 差异磁盘：从主基础映像复制时包含操作系统。
  - Disk1 = 身份磁盘：16 MB - 包含每个 VM 的 Active Directory 数据。

  随着产品的演进，您可能需要添加更多磁盘以满足某些用例和功能消耗。例如：

- MCS 存储优化 为每个 VM 创建一个写入缓存式磁盘。在 XenServer、VMware 和 SCVMM 虚拟化环境中，如果您在创建主机连接时将可用操作系统存储列表配置为与可用临时存储列表相同，则 MCS 会将回写缓存 (WBC) 磁盘放置在与操作系统磁盘相同的存储位置。
- MCS 增加了使用 完整克隆 的能力，而不是上一节中描述的 Delta 磁盘方案。

管理程序功能也可能纳入考虑范围。例如：

- XenServer IntelliCache 为每个 XenServer 在本地存储上创建一个读取磁盘。此选项可减少对可能存储在共享存储位置的主映像的 IOPS。

- 管理程序开销

  不同的管理程序使用特定的文件，这些文件会为 VM 带来开销。管理程序还使用存储进行管理和常规日志记录操作。计算要包含以下开销的空间：

  - 日志文件
  - 管理程序特定文件。例如：
    - VMware 会将更多文件添加到 **VM 存储**文件夹。请参阅 VMware 最佳实践。
    - 计算您的虚拟机总大小要求。考虑一个虚拟机，其中包含 20 GB 虚拟磁盘、16 GB 交换文件和 100 MB 日志文件，总共占用 36.1 GB。
  - XenServer 快照；VMware 快照。

- 进程开销

  创建目录、添加计算机和更新目录具有独特的存储影响。例如：

  - 初始目录创建 需要将基本磁盘的副本复制到每个存储位置。
  - 向目录添加计算机 不需要将基本磁盘复制到每个存储位置。目录创建因所选功能而异。
  - 更新目录 以在每个存储位置创建额外的基本磁盘。目录更新还会经历一个临时存储峰值，在此期间，目录中的每个 VM 在一定时间内都有 2 个差异磁盘。

更多注意事项：

- **RAM 大小调整：** 影响某些管理程序文件和磁盘的大小，包括 I/O 优化磁盘、写入缓存和快照文件。
- **精简/厚置备：** 由于精简置备功能，NFS 存储是首选。

机器创建服务 (MCS) 存储优化

Machine Creation Services (MCS) 存储优化功能也称为 MCS I/O。此功能仅适用于 Azure、GCP、XenServer、VMware、AWS 和 SCVMM。

- 写入缓存容器是*基于文件*的，与 Citrix Provisioning 中的功能相同。例如，Citrix Provisioning 写入缓存文件名是 `D:\vdiskdif.vhdx`，MCS I/O 写入缓存文件名是 `D:\mcsdif.vhdx`。
- 通过支持写入到写入缓存磁盘的 Windows 崩溃转储文件来改进诊断。
- MCS I/O 保留了*RAM 中缓存并溢出到硬盘*的技术，以提供最优的多层写入缓存解决方案。此功能允许管理员在每个层（RAM 和磁盘）的成本与性能之间进行平衡，以满足所需的工作负载预期。

将写入缓存方法从*基于磁盘*更新为*基于文件*需要进行以下更改：

1. MCS I/O 不再支持仅限 RAM 的缓存。在 Web Studio 中创建计算机目录时指定磁盘大小。
2. 虚拟机写入缓存磁盘在首次启动虚拟机时自动创建和格式化。虚拟机启动后，写入缓存文件 `mcsdif.vhdx` 将写入到格式化的卷 `MCSWCDisk` 中。
3. 页面文件将重定向到此格式化的卷 `MCSWCDisk`。因此，此磁盘大小会考虑总磁盘空间量。它包括磁盘大小与生成的工作负载之间的差值以及页面文件大小。这通常与虚拟机 RAM 大小相关。

启用 MCS 存储优化更新

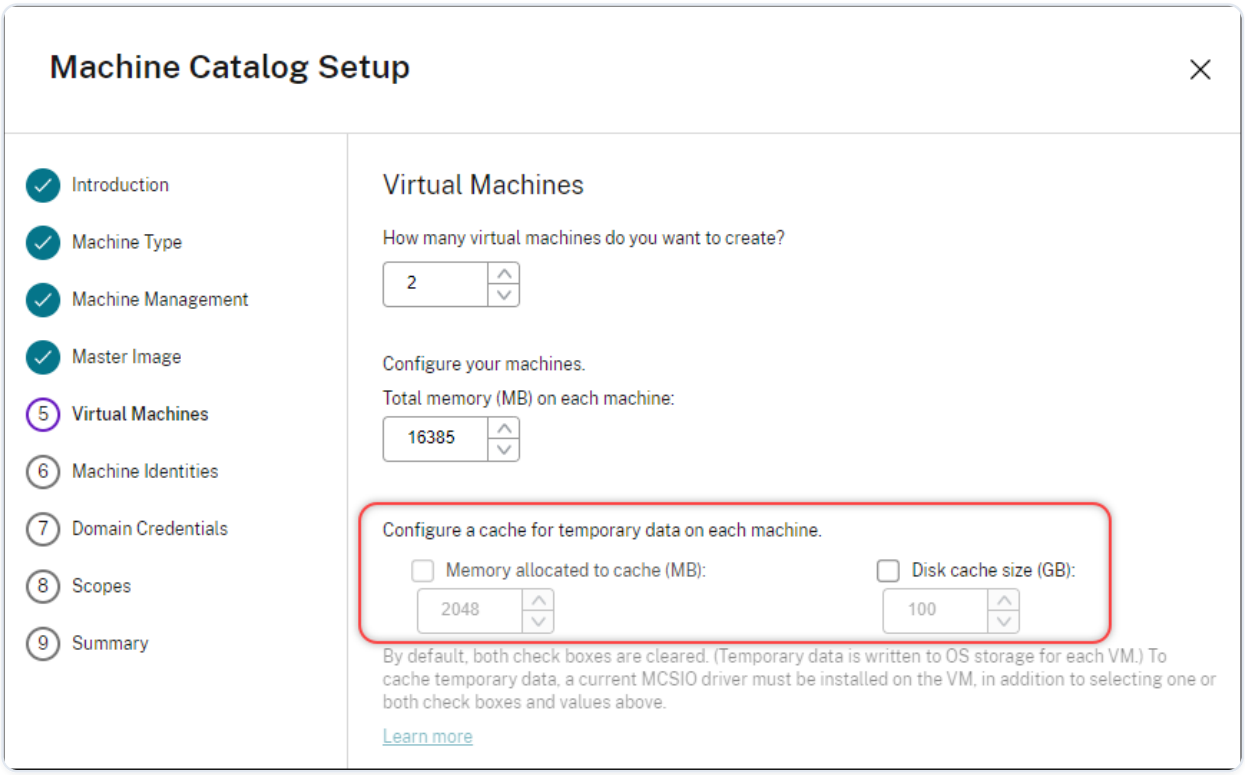
要启用 MCS I/O 存储优化功能，请将 Delivery Controller 和 VDA 升级到最新版本的 Citrix Virtual Apps and Desktops。

> **注意：**

> 如果您升级已启用 MCS I/O 的现有部署，则无需进行额外配置。VDA 和 Delivery Controller 升级会处理 MCS I/O 升级。

> 启用 MCS 存储优化更新时，请考虑以下事项：

- 创建计算机目录时，管理员可以配置 RAM 和磁盘大小。



- 将现有计算机目录更新到包含配置为版本 1903 的 VDA 的新 VM 快照会导致以下行为：新快照继续使用现有目录的 MCS I/O RAM 和磁盘大小设置。现有原始磁盘将被格式化。

重要提示：

MCS 存储优化在 Citrix Virtual Apps and Desktops 版本 1903 中发生了变化。此版本支持基于文件的写入缓存技术，提供更好的性能和稳定性。与以前的 Citrix Virtual Apps and Desktops 版本相比，MCS I/O 提供的新功能可能需要更高的写入缓存存储要求。Citrix 建议您重新评估磁盘大小，以确保它有足够的磁盘空间用于分配的工作流和额外的页面文件大小。页面文件大小通常与系统 RAM 的量有关。如果现有目录磁盘大小不足，请创建计算机目录并分配更大的写入缓存磁盘。

为 MCS I/O 回写缓存磁盘分配特定驱动器号

您可以为 MCS I/O 回写缓存磁盘分配特定驱动器号。此实现有助于避免您使用的任何应用程序的驱动器号与 MCS I/O 回写缓存磁盘的驱动器号之间发生冲突。要为 MCS I/O 回写缓存磁盘分配驱动器号，可以使用 PowerShell 命令。支持的管理程序包括 Azure、GCP、VMware、SCVMM 和 XenServer。

注意：

> 此功能需要 VDA 2305 或更高版本。

限制

- 仅适用于 Windows 操作系统
- 回写缓存磁盘的适用驱动器号：`E` 到 `Z`
- 当 Azure 临时磁盘用作回写缓存磁盘时，不适用
- 仅在创建新计算机目录时适用

为回写缓存磁盘分配驱动器号

要为回写缓存磁盘分配驱动器号，请执行以下操作：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*`。
3. 如果尚未创建身份池，请创建一个。
4. 使用 `New-ProvScheme` 命令和属性 `WriteBackCacheDriveLetter` 创建预配方案。例如：

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
```

```
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. 完成目录创建。有关详细信息，请参阅 `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`。

准备主映像

有关创建连接主机的详细信息，请参阅 连接和资源。

主映像包含操作系统、非虚拟化应用程序、VDA 和其他软件。

须知：

- 主映像也可能被称为克隆映像、黄金映像、基础 VM 或基础映像。主机供应商使用不同的术语。
- 确保主机具有足够的处理器、内存和存储以容纳所创建的计算机数量。
- 配置桌面和应用程序所需的正确硬盘空间量。此值以后无法更改，也无法在计算机目录中更改。
- 远程电脑访问计算机目录不使用主映像。

在主映像上安装并配置以下软件：

- 适用于您的管理程序的集成工具（例如 Citrix VM Tools、Hyper-V Integration Services 或 VMware tools）。如果省略此步骤，应用程序和桌面可能无法正常运行。
- VDA。Citrix 建议安装最新版本以访问最新功能。如果未在主映像上安装 VDA，则会导致目录创建失败。
- 根据需要安装第三方工具，例如防病毒软件或电子软件分发代理。使用适合用户和计算机类型（例如更新功能）的设置来配置服务。
- 您未虚拟化的第三方应用程序。Citrix 建议虚拟化应用程序。虚拟化通过消除在添加或重新配置应用程序后更新主映像的需要来降低成本。此外，安装的应用程序越少，主映像硬盘的大小就越小，从而节省了存储成本。
- 如果您计划发布 App-V 应用程序，请安装具有推荐设置的 App-V 客户端。App-V 客户端可从 Microsoft 获取。
- 使用 MCS 时，如果您本地化 Microsoft Windows，请安装区域设置和语言包。在预配期间，创建快照时，预配的 VM 将使用已安装的区域设置和语言包。

> **重要提示：**
>
> 如果您正在使用 MCS，请勿在主映像上运行 Sysprep。

> 准备主映像：

1. 使用管理程序的管理工具创建主映像，然后安装操作系统以及所有 Service Pack 和更新。指定 vCPU 数量。如果使用 PowerShell 创建计算机目录，您还可以指定 vCPU 值。使用 Web Studio 创建目录时，无法指定 vCPU 数量。配置桌面和应用程序所需的硬盘空间量。该值以后或在目录中无法更改。

2. 确保硬盘连接到设备位置 0。大多数标准主映像模板默认配置此位置，但某些自定义模板可能不会。
3. 在主映像上安装并配置上面列出的软件。
4. 如果您不使用 MCS，请将主映像加入到应用程序和桌面所属的域中。确保主映像在创建计算机的主机上可用。如果您正在使用 MCS，则无需将主映像加入域。预配的计算机将加入到目录创建向导中指定的域。
5. Citrix 建议您创建并命名主映像的快照。如果在创建目录时指定主映像而不是快照，Web Studio 会创建一个快照。您无法为其命名。

批量许可激活

MCS 支持批量许可激活，以自动化和管理 Windows 操作系统和 Microsoft Office 的激活。MCS 支持的批量许可激活的三种模式是：

- 密钥管理服务 (KMS)
- 基于 Active Directory 的激活 (ADBA)
- 多次激活密钥 (MAK)

创建计算机目录后，您可以更改激活设置。

密钥管理服务 (KMS)

KMS 是一种轻量级服务，不需要专用系统，可以轻松地与提供其他服务的系统共同托管。所有 Citrix 支持的 Windows 版本都支持此功能。在映像准备期间，MCS 会执行 Microsoft Windows 和 Microsoft Office KMS 重新武装。您可以通过运行命令 `Set-Provserviceconfigurationdata` 跳过重新武装。有关 KMS 激活的更多信息，请参阅 使用密钥管理服务激活。

> **注意：**
>
> 运行命令 `Set-Provserviceconfigurationdata` 后创建的所有计算机目录都具有与该命令中提供的相同设置。

基于 Active Directory 的激活 (ADBA)

ADBA 使您能够通过计算机的域连接来激活它们。计算机在加入域时会立即激活。只要这些计算机保持加入域并与其保持联系，它们就会保持激活状态。所有 Citrix 支持的 Windows 版本都支持此功能。有关基于 Active Directory 的激活的更多信息，请参阅使用 基于 Active Directory 的激活 进行激活。

多次激活密钥 (MAK)

MAK 是一种借助 Microsoft 服务器激活批量许可证并验证 Windows 系统的方法。您必须从 Microsoft 购买 MAK 密钥，该密钥分配有固定数量的激活次数。每次激活 Windows 系统时，激活次数都会减少。激活系统有两种方式：

- 在线激活：如果您要激活的 Windows 系统具有 Internet 访问权限，则系统会在安装产品密钥时自动激活 Windows。此过程会将相应 MAK 的激活次数减少 1。
- 离线激活：如果 Windows 系统无法连接到 Internet 进行在线激活，MCS 会从 Microsoft 服务器获取确认 ID 和安装 ID，以激活 Windows 系统。这种激活方式对于非持久性计算机目录很有用。

> **注意：**
>
> - MCS 不支持使用 MAK 激活 Microsoft Office。
> - 所需的最低 VDA 版本为 2303。

主要要求

- Delivery Controller 必须具有 Internet 访问权限。
- 如果要更新的新映像具有与原始映像不同的 MAK 密钥，请创建新目录。
- 在主映像上安装 MAK 密钥。有关在 Windows 系统上安装 MAK 密钥的步骤，请参阅 部署 MAK 激活。
- 如果您不使用映像准备：

  a. 在 `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation` 下添加注册表 DWORD 值 `Manual`。

  b. 将值设置为 `1`。

激活计数

要查看 MAK 密钥剩余的激活次数，或检查 VM 是否正在消耗两次或更多次激活，请使用批量激活管理工具 (VAMT)。请参阅 安装 VAMT。

使用 MAK 激活 WINDOWS 系统

要使用 MAK 激活 Windows 系统：

1. 在主映像上安装产品密钥。此步骤会消耗一个激活计数。

2. 创建 MCS 计算机目录。
3. 如果您不使用映像准备：

   a. 在 `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation` 下添加注册表 DWORD 值 `Manual`。

   b. 将值设置为 `1`。

   此方法会禁用联机激活选项。
4. 将 VM 添加到计算机目录。
5. 启动虚拟机。
6. 根据是联机激活还是脱机激活，Windows 系统会被激活。

   - 如果是联机激活，则在安装产品密钥后，Windows 系统会被激活。
   - 如果是脱机激活，MCS 会与预配的虚拟机通信以获取 Windows 系统的激活状态。然后，MCS 会从 Microsoft 服务器检索确认 ID 和安装 ID。这些 ID 用于激活 Windows 系统。

故障排除

如果预配的虚拟机未通过已安装的 MAK 密钥激活，请在 PowerShell 窗口中运行 `Get-ProvVM` 或 `Get-ProvScheme` 命令。

- `Get-ProvScheme` 命令：请参阅与最新主映像中的 MCS 计算机目录关联的参数 `WindowsActivationType`。
- `Get-ProvVM` 命令。请参阅参数 `WindowsActivationType`、`WindowsActivationStatus`、`WindowsActivationStatusErrorCode` 和 `WindowsActivationStatusError`。

您可以检查错误并验证解决问题的步骤。

使用 Web Studio 创建计算机目录

创建目录之前：

- 查看本节以了解您所做的选择以及您提供的信息。
- 确保您已创建到管理程序的连接、云服务以及托管您计算机的其他资源。
- 如果您已创建用于预配计算机的主映像，请确保您已在该映像上安装 VDA。

要启动目录创建向导：

1. 如果这是要创建的第一个目录，系统会引导您进行正确的选择（例如“设置计算机并创建计算机目录以运行应用程序和桌面”）。目录创建向导随即打开。

2. 如果您已创建目录并想创建另一个，请按照以下步骤操作：

   a. 登录 Web Studio，在左侧窗格中选择**计算机目录**，然后在操作栏中选择**创建计算机目录**。

   b. 要使用文件夹组织目录，请在默认的**计算机目录**文件夹下创建文件夹。有关详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-manage.html#create-a-catalog-folder)。

   c. 选择要创建目录的文件夹，然后单击**创建计算机目录**。目录创建向导随即打开。

该向导将引导您完成以下各项。您看到的向导页面因您所做的选择而异。

操作系统

每个目录只包含一种类型的计算机。请选择一种。

- **多会话操作系统：** 多会话操作系统目录提供托管共享桌面。计算机可以运行受支持的 Windows 或 Linux 操作系统版本，但目录不能同时包含这两种操作系统。（有关该操作系统的详细信息，请参阅 Linux VDA 文档。）
- **单会话操作系统：** 单会话操作系统目录提供 VDI 桌面，您可以将其分配给不同的用户。
- **远程电脑访问：** 远程电脑访问目录为用户提供对其物理办公桌面计算机的远程访问。远程电脑访问不需要 VPN 来提供安全性。

计算机管理

创建远程电脑访问目录时，此页面不会出现。

计算机管理页面指示计算机的管理方式以及用于部署计算机的工具。

选择目录中的计算机是否通过 Web Studio 进行电源管理。

- 计算机通过 Web Studio 进行电源管理，例如，VM 或刀片式 PC。此选项仅在您已配置到主机的连接时可用。
- 计算机不通过 Web Studio 进行电源管理，例如，物理计算机。

如果您指出计算机通过 Web Studio 进行电源管理，请选择用于创建 VM 的工具。

- 思杰预配技术
  - **Citrix Machine Creation Services (MCS)** 使用 MCS 预配和映像创建 VM 目录。MCS 将从主映像克隆的映像复制到这些 VM。
  - **Citrix Provisioning Services (PVS)** 使用 MCS 预配和 PVS 映像创建 VM 目录。这些 VM 用作 PVS 目标设备，PVS 服务器可以将单个共享磁盘映像流式传输到它们。

> **注意：**
>
> - 此选项仅适用于在 Citrix Cloud™ 中注册的 PVS 站点，并且目前仅限于 Azure 资源。
> - 在创建 Citrix Provisioning 目录时，在“**目标设备**”页面上，您可能会看到，在用于选择要预配的计算机的场和站点的下拉菜单中，列出了不再存在的场和站点。作为一种解决方法，您可以运行 PowerShell 命令 `Unregister-HypPvsSite` 从数据库中删除这些场和站点。有关 PowerShell 命令的信息，请参阅 Unregister-HypPvsSite。

- **其他服务或技术** 一种用于管理数据中心中现有计算机的工具。Citrix 建议您使用 Microsoft System Center Configuration Manager 或其他第三方应用程序来确保目录中的计算机保持一致。

桌面类型（桌面体验）

> **注意：**
>
> **桌面体验**页面上的选项因您在**计算机类型**页面上选择的计算机类型而异。

- 对于**多会话操作系统**计算机，用户每次登录时都会分配一个随机桌面。选择以下选项之一：
  - **是，将更改保存到托管虚拟桌面的计算机的本地磁盘。**（持久）
  - **否，在用户注销时放弃所有更改并清除虚拟桌面。**（非持久）

  > **注意：**
  >
  > 对于持久多会话计算机，用户对桌面所做的更改将被保存，并可供所有授权用户访问。

- 对于**单会话操作系统**计算机，您将在“**桌面体验**”页面上获得以下选项：
  - **我希望用户每次登录时都连接到新的（随机）桌面。**
  - **我希望用户每次登录时都连接到相同的（静态）桌面。**

    对于静态桌面，您可以进一步决定用户所做的更改在注销后是保存还是丢弃。

如果您选择“**将更改保存到托管虚拟桌面的计算机的本地磁盘：持久**”，则在“**虚拟机**”页面中，虚拟机复制模式提供快速复制或完全复制选项。

如果您选择“**在用户注销时放弃所有更改并清除虚拟桌面：非持久**”，则无法在“**虚拟机**”页面中配置虚拟机复制模式。

映像和计算机配置文件

此页面仅在使用 MCS 创建 VM 时显示。

1. 为计算机目录选择映像类型，然后选择映像。提供了两种映像类型：

   - **主映像。** 尚未经过映像准备过程的映像。映像准备过程在目录创建开始时自动启动。

     > **注意：**
     >
     > - 使用 MCS 时，请勿在主映像上运行 Sysprep。
     > - 如果指定主映像而不是快照，Web Studio 会创建一个快照，但您无法为其命名。

   - **准备好的映像。** 已完成映像准备过程并可直接用于 VM 创建的映像。在目录创建期间选择准备好的映像而不是主映像，可确保更快、更可靠地创建计算机目录，并简化映像生命周期管理。如果需要，为选定的准备好的映像添加备注。

     > **注意：**
     >
     > - 使用准备好的映像创建的 VM 不支持休眠。
     > - 目前，仅在 Azure 和 VMware 环境中支持使用准备好的映像创建目录。

   有关如何创建准备好的映像的详细信息，请参阅 映像管理（预览版）。

   选择映像时，如果需要，可以为选定的映像添加备注。

   要启用最新产品功能，请确保主映像已安装最新 VDA 版本。请勿更改默认的最低 VDA 选择。但是，如果必须使用早期 VDA 版本，请参阅 VDA 版本和功能级别。

   如果您选择的快照或 VM 与您之前在向导中选择的计算机管理技术不兼容，则会显示错误消息。

2. 要使用现有 VM 作为计算机配置文件，请选择**使用计算机配置文件**，然后选择该 VM。

> **注意：**
>
> 目前，使用计算机配置文件仅限于 Azure、AWS、GCP 和 VMware VM。
>
> 对于 VMware 部署，在使用计算机配置文件创建计算机目录时，必须指定要保留虚拟机的文件夹。

要提供虚拟机文件夹位置，请在目录创建向导中，转到**虚拟机**页面，然后转到**选择一个文件夹来放置计算机**部分并选择虚拟机文件夹位置。如果未指定，系统会将所选计算机配置文件的文件夹视为默认位置。

3. 对于 AWS 部署，您可以选择启动模板作为计算机配置文件。
4. 选择目录的最低功能级别。要启用最新产品功能的使用，请确保主映像已安装最新版本的 VDA。

计算机

创建远程电脑访问目录时，此页面不会出现。

此页面的标题取决于您在**计算机管理**页面上选择的内容：**计算机**、**虚拟机**或**虚拟机和用户**。

使用 MCS 时：

- 指定要创建的虚拟机数量。如果不想创建任何虚拟机，请输入 **0**（零）。稍后，您可以通过执行“**添加计算机**”为现有空目录创建虚拟机。
- 选择每个 VM 的内存量（以 MB 为单位）。
- 每个创建的虚拟机都带有一个硬盘。其大小在主映像中设置。您无法在目录中更改硬盘大小。
- 如果您的部署包含多个区域，您可以为目录选择一个区域。
- 如果您正在创建静态桌面虚拟机，请选择虚拟机复制模式。请参阅虚拟机复制模式。
- 如果您正在创建不使用 vDisk 的随机桌面虚拟机，您可以配置一个缓存，用于存储每台计算机上的临时数据。请参阅配置临时数据缓存。

使用其他工具时：

添加（或导入列表）Active Directory 计算机帐户名称。添加/导入虚拟机后，您可以更改其 Active Directory 帐户名称。如果您在“**桌面体验**”页面上指定了静态计算机，则可以选择为添加的每个虚拟机指定 Active Directory 用户名。

添加或导入名称后，您可以使用“**删除**”按钮从列表中删除名称，同时您仍在此页面上。

使用其他工具时（但不是 MCS）：

每个添加（或导入）的计算机的图标和工具提示有助于识别可能不符合添加到目录条件或无法向 Delivery Controller 注册的计算机。有关详细信息，请参阅VDA 版本和功能级别。

在创建虚拟机时添加 SID

您现在可以添加参数 `ADAccountSid` 以在创建新虚拟机时唯一标识这些计算机。

为此：

1. 创建具有受支持身份类型的目录。
2. 使用 `NewProvVM` 将计算机添加到目录中。例如：

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID ")  -
RunAsynchronously
```

但是，您无法预配具有以下特征的计算机：

- 不在目录身份池中的 AD 帐户
- 处于不可用状态的 AD 帐户

虚拟机复制模式

您在“**计算机**”页面上指定的复制模式决定 MCS 是从主映像创建精简（快速复制）克隆还是完整（完全复制）克隆。（默认 = 精简克隆）

- 使用快速复制克隆可实现更高效的存储利用和更快的计算机创建。
- 使用完整复制克隆可获得更好的数据恢复和迁移支持，并且在计算机创建后可能降低 IOPS。

> **注意：**
>
> 完整复制克隆方法仅适用于在多会话或单会话操作系统上预配持久性 VM。

VDA 版本和功能级别

目录的功能级别控制目录中计算机可用的产品功能。使用新产品版本中引入的功能需要新的 VDA。但是，该目录中具有早期 VDA 版本的计算机无法注册。

“**计算机**”（或“**设备**”）页面底部附近的一个菜单允许您选择最低 VDA 级别。这设置了目录的最低功能级别。默认情况下，为本地部署选择了最新的功能级别。如果您遵循 Citrix 的建议，始终将 VDA

和核心组件安装并升级到最新版本，则无需更改此选择。但是，如果您必须继续使用旧版 VDA，请选择正确的值。

Citrix Virtual Apps and Desktops 版本可能不包含新的 VDA 版本，或者新的 VDA 不影响功能级别。在这种情况下，功能级别可能指示的 VDA 版本早于已安装或已升级的组件。每个版本的新增功能文章都会指出默认功能级别的任何更改。

所选功能级别会影响其上方的计算机列表。在列表中，每个条目旁边的工具提示指示计算机的 VDA 是否与该功能级别的目录兼容。

如果每台计算机上的 VDA 未达到或超过所选的最低功能级别，则页面上会显示消息。您可以继续向导。这些计算机以后可能无法向控制器注册。或者，您可以：

- 从列表中删除包含旧版 VDA 的计算机，升级其 VDA，然后将其重新添加到目录中。
- 选择较低的功能级别，这会阻止访问最新的产品功能。

如果计算机因类型错误而未添加到目录中，也会显示一条消息。示例包括尝试将服务器添加到单会话操作系统目录，或将最初为随机分配创建的单会话操作系统计算机添加到静态计算机目录。

> **重要提示：**
>
> 在版本 1811 中，添加了一个额外功能级别：**1811（或更高版本）**。该级别旨在用于未来的 Citrix Virtual Apps and Desktops 功能。**7.9（或更高版本）** 选项仍为默认值。该默认值现在对所有部署都有效。
>
> 如果选择 **1811（或更高版本）**，则该目录中任何较早的 VDA 版本都无法向控制器注册。但是，如果目录中仅包含版本 1811 或更高支持版本的 VDA，则它们都符合注册条件。这包括包含为更高版本的 Citrix Virtual Apps and Desktops 版本（包括版本 1903 和当前版本之前的其他 19XX 版本）配置的 VDA 的目录。

配置临时数据缓存

使用 MCS 管理目录中的随机非持久性计算机时，可以为计算机启用回写缓存以提高 I/O 性能。

回写缓存称为 MCSIO。有关详细信息，请参阅此博客文章。

先决条件

要启用回写缓存，目录必须满足以下要求：

- 使用指定临时数据存储的连接。有关详细信息，请参阅连接和资源。

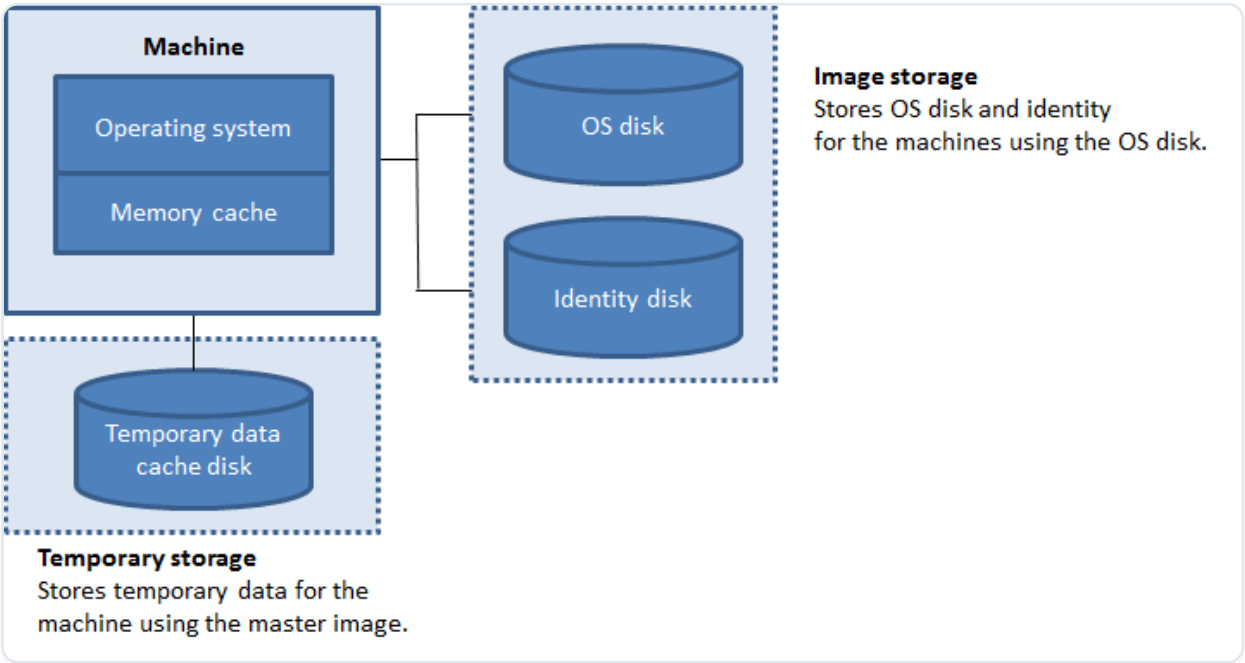
- VDA 必须至少为版本 7.9 并安装了当前的 MCSIO 驱动程序。

> **注意：**
>
> 安装此驱动程序是安装或升级 VDA 时的可选操作。默认情况下，不安装该驱动程序。

- 要为磁盘缓存启用驱动器号分配，VM 必须满足以下附加要求：
  - 操作系统：Windows
  - VDA 版本：2305 或更高版本

注意事项

- 回写缓存分为*内存*缓存和*磁盘*缓存。默认情况下，它们的默认值因连接类型而异。通常，默认值足以满足大多数情况；但是，请考虑以下所需的空间：
  - Windows 自身创建的临时数据文件，包括 Windows 页面文件。
  - 用户配置文件数据。
  - 同步到用户会话的 ShareFile 数据。
  - 会话用户或用户可能在会话中安装的任何应用程序可能创建或复制的数据。



- 已移除配置仅包含磁盘缓存而无内存缓存的回写缓存的选项。要为临时数据启用缓存，建议选择**磁盘缓存大小 (GB)** 和**分配给缓存的内存 (MB)**，并为内存缓存指定大于 0 的大小。临时数据最初写入内存缓存。当内存缓存达到其配置限制时，最旧的数据将移动到临时数据缓存磁盘。

- 内存缓存是每台计算机总内存的一部分。因此，如果启用**内存缓存大小 (MB)（推荐）**复选框，请考虑增加每台计算机的总内存量。
- 如果保持**内存缓存大小 (MB)（推荐）**复选框处于未选中状态，则临时数据将直接写入磁盘缓存，仅使用最少量的内存。
- 更改 **磁盘缓存大小 (GB)** 的默认值可能会影响性能。大小必须与用户要求和计算机上的负载相匹配。

> **重要提示：**
>
> 如果磁盘缓存空间不足，用户的会话将变得不可用。

- 如果清除“**磁盘缓存大小**”复选框，则不会创建缓存磁盘。在这种情况下，请指定一个足够大的“**分配给缓存的内存**”值，以容纳所有临时数据。这仅在有大量 RAM 可分配给每个 VM 时才可行。
- 如果您取消选中这两个复选框，临时数据不会被缓存。它会被写入差分磁盘（位于操作系统存储中）针对每个虚拟机。（这是 7.9 之前版本中的预配操作。）
- 如果您打算使用此目录创建 AppDisks，请勿启用缓存。
- 创建计算机目录后，无法更改其中的缓存值。

安全

安全性页面仅在您未在 AWS 虚拟化环境中分配计算机配置文件的情况下创建计算机目录时显示。使用**安全性**页面配置 VM 的安全组。这在编辑和克隆现有计算机目录时也适用。

如果您创建基于计算机配置文件的计算机目录，则安全组配置将从计算机配置文件继承，并且**安全性**页面不会显示。

网卡 (NIC)

创建远程电脑访问目录时，此页面不会出现。

如果您计划使用多个 NIC，请将虚拟网络与每张网卡关联。例如，您可以将一张网卡分配给访问特定的安全网络，将另一张网卡分配给访问更常用的网络。您也可以在此页面上添加或删除 NIC。

计算机帐户

此页面仅在创建远程电脑访问目录时出现。

在“**计算机帐户**”页面上，指定要添加的 Active Directory 计算机帐户或组织单位 (OU)，这些帐户或组织单位对应于用户或用户组。请勿在 OU 名称中使用正斜杠 (/)。

添加 OU 时，如果域未显示在列表中，您可以执行以下操作：

- 使用精确匹配搜索它。
- 浏览所有域以查找它。

您可以选择之前配置的电源管理连接，或者选择不使用电源管理。如果您想使用电源管理，但尚未配置合适的连接，您可以稍后创建该连接，然后编辑计算机目录以更新电源管理设置。

计算机身份

此页面仅在使用 MCS 创建虚拟机时出现。

目录中的每台计算机都必须具有唯一的身份。此页面允许您配置目录中计算机的身份。计算机在预配后会加入到该身份。创建目录后，无法更改身份类型。

配置此页面上的设置的通用工作流程如下：

1. 从列表中选择一个身份。
2. 指示是创建帐户还是使用现有帐户，以及这些帐户的位置（域）。

您可以选择以下选项之一：

- **本地 Active Directory**。由组织拥有并使用属于该组织的 Active Directory 帐户登录的计算机。它们存在于本地。
- **已混合加入 Microsoft Entra**。由组织拥有并使用属于该组织的 Active Directory 域服务帐户登录的计算机。它们存在于云中和本地。有关要求、限制和注意事项的信息，请参阅已混合加入 Microsoft Entra。

  > **注意：**
  >
  > - 在使用 Microsoft Entra 混合加入之前，请确保您的 Azure 环境满足先决条件。请参阅配置 Microsoft Entra 混合加入。
  > - 此选项要求主映像满足操作系统先决条件。有关详细信息，请参阅已混合加入 Microsoft Entra 的设备。

- **未加入域**。未加入任何域的计算机。有关要求和限制的信息，请参阅未加入域。

> **重要提示：**

- 如果选择 **本地 Active Directory** 或 **Microsoft Entra 混合加入** 作为身份类型，则目录中的每台计算机都必须具有相应的 Active Directory 计算机帐户。
- **未加入域**身份类型要求 VDA 版本为 2311 或更高版本作为目录的最低功能级别。要使其可用，请更新最低功能级别。

在配置计算机身份之前，请确保您拥有在计算机所在的 OU 中创建计算机帐户的权限。目录中的每台计算机都必须具有唯一的名称。然后选择如何配置计算机身份：

- 如果创建新的计算机帐户，请指定 OU 和计算机命名方案。有关详细信息，请参阅 计算机帐户命名方案。创建目录时，会自动创建一个身份池，用于保存为此目录定义的所有计算机身份。
- 如果使用现有计算机帐户，请选择环境中的现有身份池。

注意：

确保 OU 名称不使用正斜杠 (`/`)。

在创建目录并在**计算机身份**页面上选择**使用现有身份池**时，服务帐户行为取决于身份池配置：

- 如果所选身份池未配置服务帐户，则在**域凭据**页面上选择存储的服务帐户将不起作用。**添加计算机**操作可能会失败，并显示服务帐户找不到的错误。为避免此情况，请在**域凭据**页面上手动输入域凭据。
- 如果所选身份池已配置服务帐户，则**域凭据**页面上选择的任何服务帐户都将被忽略。**添加计算机**操作始终使用与身份池关联的服务帐户。

如果您使用现有帐户，请浏览到这些帐户或单击“**导入**”并指定一个包含帐户名称的 .csv 文件。导入的文件内容必须使用以下格式：

- ADcomputeraccountname.domain

确保您要添加的所有计算机都有足够的帐户。Web Studio 界面管理这些帐户。因此，要么允许该界面重置所有帐户的密码，要么指定帐户密码，该密码必须对所有帐户都相同。

对于包含物理机或现有计算机的目录，请选择或导入现有帐户，并将每台计算机分配给 Active Directory 计算机帐户和用户帐户。

计算机帐户命名方案

目录中的每台计算机都必须具有唯一的名称。创建目录时，必须指定计算机帐户命名方案。使用通配符（井号）作为名称中出现的连续数字或字母的占位符。

指定命名方案时，请注意以下规则：

- 命名方案必须包含至少一个通配符。您必须将所有通配符放在一起。
- 整个名称（包括通配符）必须包含至少 2 个字符，但不能超过 15 个字符。它必须包含至少一个非数字字符和一个 #（通配符）字符。
- 名称不能包含空格或以下任何字符：`,~!@'$%\^&.(){}{\/*?"<>|=+[];:_".`。
- 名称不能以连字符 (-) 结尾。

此外，在指定命名方案时，请为增长留出足够的空间。请考虑以下示例：如果您使用方案“veryverylong#”创建 1,000 个计算机帐户，则创建的最后一个帐户名称 (veryverylong1000) 包含 16 个字符。因此，该命名方案会导致一个或多个计算机名称超出 15 个字符的最大限制。

您可以指示序列值是数字 (0-9) 还是字母 (A-Z)：

- **0-9**。如果选中，指定的通配符将解析为连续数字。

  > **注意：**
  >
  > 如果只有一个通配符 (#)，则帐户名称以 1 开头。如果有两个，则帐户名称以 01 开头。如果有三个，则帐户名称以 001 开头，依此类推。

- **A-Z**。如果选中，指定的通配符将解析为连续字母。

例如，命名方案 PC-Sales-##（选择 **0-9**）将生成名为 PC-Sales-01、PC-Sales-02、PC-Sales-03 等的帐户。

您可以选择指定帐户名称的开头。

- 如果选择 **0-9**，帐户将按顺序命名，从指定的数字开始。输入一个或多个数字，具体取决于您在前面字段中使用的通配符数量。例如，如果使用两个通配符，请输入两个或更多数字。
- 如果选择 **A-Z**，帐户将按顺序命名，从指定的字母开始。输入一个或多个字母，具体取决于您在前面字段中使用的通配符数量。例如，如果使用两个通配符，请输入两个或更多字母。

域凭据

输入具有执行帐户操作权限的管理员凭据。详细步骤如下：

1. 单击 **输入凭据**。此时将显示“Windows 安全”页面。
2. 在 **用户名** 字段中，输入管理员的 SamName、用户名或用户 SID：
   - 如果输入 SamName，则“**域**”字段会自动填充。
   - 如果输入用户名或 SID，可以通过在“**域**”字段中输入域名或 SID 来将用户搜索限制到特定域。
3. 单击“**检查名称**”以检查用户名是否有效或唯一。
4. 在“**密码**”字段中，输入管理员的域密码。
5. 点击 **完成**。

> **注意：**
>
> 如果在“**计算机身份**”中选择的身份类型是“**Microsoft Entra 混合联接**”，则输入的凭据必须已获得 `Write userCertificate` 权限。

摘要、名称和描述

在 **摘要** 页面上，查看您指定的设置。输入目录的名称和描述。此信息将显示在 Web Studio 中。

完成后，单击 **完成** 以开始创建目录。 完成后，选择 **完成** 以开始创建目录。

在**计算机目录**中，新目录将显示一个内联进度条。

要查看创建进度的详细信息：

1. 将鼠标悬停在计算机目录上。
2. 在出现的工具提示中，单击**查看详细信息**。

   将显示一个分步进度图，您可以在其中看到以下内容：

   - 步骤历史记录
   - 当前步骤的进度和运行时间
   - 剩余步骤

MCS 时间同步

时间同步由主映像和加入目录的计算机身份类型决定。根据主映像和目录，您将获得以下时间同步方法：

主映像	目录	结果时间同步方法
NDJ	AD 或 Microsoft Entra 混合	默认情况下，NT5DS。您可以使用主映像中的注册表设置禁用 MCS 更改时间同步设置。
NDJ	NDJ 或 微软 Entra ID	与原始时间同步设置相同
AD 或 Microsoft Entra 混合	AD 或 Microsoft Entra 混合	与原始时间同步设置相同
微软 Entra ID	微软 Entra ID	与原始时间同步设置相同

注意：

原始时间同步由以下注册表设置控制，无法更改：

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

值: MaxAllowedPhaseOffset, MaxNegPhaseCorrection, and MaxPosPhaseCorrection

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

值: Type

要禁用 MCS 更改时间同步设置，请在主映像中设置以下注册表设置的值：

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- 名称: TimeSyncMethodKeep
- 类型: DWORD
- 0 (或者，未配置值 TimeSyncMethodKeep)：不保留原始时间同步设置。
- 1: 保留原始时间同步设置和默认参数值。

有关设置自定义属性的重要注意事项

在 GCP 和 Azure 环境中，必须在 `New-ProvScheme` 和 `Set-ProvScheme` 处正确设置自定义属性。如果指定了不存在的自定义属性，则会收到以下错误消息，并且命令无法运行。

- 在 Azure 中: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`.
- 在 GCP 中: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`.

故障排除

> **重要提示：**

> 使用 Web Studio 创建计算机目录后，您将无法再使用 `Get-ProvTask` PowerShell 命令检索与计算机目录创建相关的任务。此限制是由于 Web Studio 在创建计算机目录后会删除这些任务，无论目录是否成功创建。

> Citrix 建议收集日志以帮助支持团队提供解决方案。使用 Citrix Provisioning 时，请按照以下过程生成日志文件：

1. 在主映像上，创建以下注册表项，其值为 1（作为 DWORD (32 位) 值）：`HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. 关闭主映像并创建快照。
3. 在 Delivery Controller 上，运行以下 PowerShell 命令：`Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
4. 基于该快照创建目录。
5. 当准备 VM 在管理程序上创建时，登录并从 `C:\` 的根目录中提取以下文件：Image-prep.log 和 PvsVmAgentLog.txt。
6. 关闭计算机，此时它会报告故障。
7. 运行以下 PowerShell 命令以重新启用映像准备计算机的自动关机：`Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`。

为 MCS I/O 回写缓存磁盘分配特定驱动器号

您可以为 MCS I/O 回写缓存磁盘分配特定的驱动器号。此实施有助于避免您使用的任何应用程序的驱动器号与 MCS I/O 回写缓存磁盘的驱动器号之间发生冲突。为此，您可以使用 PowerShell 命令。支持的管理程序包括 Azure、GCP、VMware、SCVMM 和 XenServer。

> **注意：**
>
> 此功能需要 VDA 2305 或更高版本。

限制

- 仅适用于 Windows 操作系统
- 回写缓存磁盘的适用驱动器号：`E` 到 `Z`
- 当 Azure 临时磁盘用作回写缓存磁盘时，不适用
- 仅在创建新计算机目录时适用

为回写缓存磁盘分配驱动器号

为回写缓存磁盘分配驱动器号：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*`。
3. 如果尚未创建身份池，请创建一个。有关信息，请参阅创建目录。
4. 使用 `New-ProvScheme` 命令和属性 `WriteBackCacheDriveLetter` 创建预配方案。例如：

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
```

```
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
```

```
</CustomProperties>'
```

5. 完成目录创建。

在创建 MCS 计算机目录之前验证配置

您可以使用 `New-ProvScheme` 命令中的参数 `-validate` 在创建 MCS 计算机目录之前验证配置设置。在使用该参数运行此 PowerShell 命令后，如果使用了不正确的参数或参数与其他参数冲突，您将收到相应的错误消息。然后，您可以使用错误消息来解决问题，并使用 PowerShell 成功创建 MCS 计算机目录。目前，此功能适用于 AWS、Azure、GCP 和 VMware 虚拟化环境。

注意：

在验证时，您不得创建实际的 MCS 计算机目录。您必须使用命令结果来修复错误，然后创建成功的目录。因此，在运行 `New-ProvScheme` 命令时，请使用虚假的身份池名称。

要验证配置，请执行以下步骤：

1. 从 Delivery Controller 主机打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行 `New-ProvScheme` 命令并使用参数 `-validate`。为使命令正常工作，请提供一个虚假的身份池名称。例如，

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg"
-IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
MasterImageVM "XDHyp:
\HostingUnits\vSanRg\Windows19MasterImage.vm\Citrix_XD_NonMachineProfil
eWin19Machines.snapshot" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vSanRg\\VM Network.network"} -ProvisioningSchemeName
"MachineProfileW10Machines"  -Scope @()

-VMCpuCount 2  -VM

MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-Win11-
tpm-BL-TEMPLATE.template" -TenancyType Shared  -FunctionalLevel "L7_20"
-Validate
```

```
$result.TerminatingError | Format-List -Property *
```

错误消息：

```
ErrorData    : {[[ValidationFailureCount, xxx], [InvalidMemoryValue,
The memory size provided 6143 must be a multiple of 4 MB and must be
greater than or equal to 4 MB.], [InconsistentGuestOsSetting, The
GuestOs setting - windows9_64Guest of the selected machine profile does
not match with the setting - windows2019srv_64Guest of master image.
Please select a machine profile that matches the GuestOs setting of the
master image.], [InconsistentVtpmSetting, The vTPM setting of the
selected machine profile does not match with the selected master image.
Please select a machine profile that matches the vTPM setting of the
master image.], [InconsistentFirmwareSetting, The firmware setting -
efi of the selected machine profile does not match with the setting -
bios of master image. Please select a machine profile that matches the
firmware setting of the master image ErrorId      : ValidationFailure

ErrorMessage : ValidationFailure

Operation    : ValidatingInputs
```

4. 验证配置设置后，您可以使用真实的身份池名称和正确的参数创建 MCS 计算机目录。

将 VM 加入 Azure Arc

Azure Arc 使组织能够管理托管在任何位置的资源（例如 VM），就像它们在 Azure 中运行一样。借助 Azure Arc，您可以使用 Azure Monitor 等 Azure 服务，对资源进行全面的可见性和主动管理。

要将 VM 加入 Azure Arc，请使用 `New-ProvScheme` 命令创建 MCS 计算机目录。您还可以使用 `Set-ProvScheme` 命令更新现有目录。只有添加到目录中的新 VM 才会加入 Azure Arc。

目前，此功能适用于所有 Citrix 本地虚拟机管理程序 VMware、Nutanix 和 SCVMM。

先决条件

在 MCS 目录上启用 Azure Arc 加入之前，请考虑以下事项：

- 具有以下内容的 Azure 资源组：
  - `Allows` 帐户，用于读取、创建和删除 Arc 服务器。
  - `Allows` 帐户，用于管理 VM 扩展、许可证和专用链接范围。

- 在资源组范围内分配给服务主体的 `Azure Connected Machine Resource Administrator` 角色。

请参阅 使用 Azure 门户分配 Azure 角色。

- 具有以下内容的主映像
  - VDA：晚于 2311，不包括 2411。

    > **注意：**
    >
    > CVAD 2411 不支持 Azure Arc 载入。

  - 已安装 AzureConnectedMachineAgent 代理。您可以从 Microsoft 文档的 Windows 或 Linux 部分下载 MSI。

将 VM 加入 Azure Arc 的步骤

1. 设置具有 `AzureArcResourceManagement` 功能的服务帐户。

   服务帐户通过存储凭据来访问 Microsoft Entra ID 等身份提供程序，用于身份验证或授权。每个服务帐户都绑定到一个身份提供程序。

   要创建新的服务帐户以使用 `AzureArcResourceManagement capability` 访问 AzureAD，请运行：

   ```
   New-AcctServiceAccount -IdentityProviderType “AzureAD”
   -IdentityProviderIdentifier “tenant-id” -AccountId “application-id”
   -AccountSecret “application-secret” -Capabilities
   “AzureArcResourceManagement”
   ```

   `application-id` 必须是已分配 Azure Connected Machine Resource Administrator 角色的同一服务主体。

2. 将服务帐户分配给身份池。例如：

   ```
   Set-AcctIdentityPool -IdentityPoolUid “idn-pool-uid” -ServiceAccountUid
   “service-account-uid”
   ```

3. 使用以下 Arc 参数创建或更新 MCS 目录：

- `EnableAzureArcOnboarding`：指示是否需要在目录上启用 Arc Onboarding。
- `AzureArcSubscriptionId`：指示创建 Arc 连接的 VM 的 Azure 订阅。
- `AzureArcRegion`：指示创建 Arc 连接的 VM 的 Azure 区域。
- `AzureArcResourceGroup`：指示创建 Arc 连接的 VM 的 Azure 资源组。有关 Azure Arc 资源组的信息，请参阅 。

示例：为新目录启用 Azure Arc Onboarding：

```
`New-ProvScheme -ProvisioningSchemeName "demo" -MasterImageVM "XDHyp:
\HostingUnits\hosting-unit\masterVMName.vm\masterSnapshotName.snapshot"
-HostingUnitName “hosting-unit” -IdentityPoolName “identity-pool”`



-EnableAzureArcOnboarding -AzureArcSubscriptionId “azure-sub”
-AzureArcResourceGroup “azure-resourcegroup” - AzureArcRegion “azure-
region”
```

示例：为现有目录启用 Azure Arc Onboarding：

```
Set-ProvScheme -ProvisioningSchemeName "demo" -EnableAzureArcOnboarding
$true -AzureArcSubscriptionId “azure-sub” -AzureArcResourceGroup
“azure-resourcegroup” - AzureArcRegion “azure-region”
```

示例：为现有目录禁用 Azure Arc Onboarding：

```
Set-ProvScheme -ProvisioningSchemeName "demo" -EnableAzureArcOnboarding
$false:
```

4. 将新计算机添加到目录以载入 Arc。
5. 启动 VM 后，您必须在 Azure 门户的 **AzureArcResourceGroup** 下看到该 VM 作为连接的计算机。

注意事项

- Arc 载入目前仅支持新虚拟机。因此，如果您使用 `Set-ProvScheme` 更新现有目录，则只有新添加的虚拟机在首次开机时才会被载入到 Arc。
- Arc 自定义属性仍支持现有目录以实现向后兼容性。但是，如果您运行 `New-ProvScheme` 并带有 Arc 自定义属性（例如 `EnableAzureArcOnboarding`），则目录创建失败。

- 如果您将 `EnableAzureArcOnboarding` 配置为 `true`，则必须添加 `New-ProvScheme` 和 `Set-ProvScheme` 中的所有参数。

故障排除

使用 `New-ProvScheme` 创建 SCVMM 目录时，您可能会遇到以下错误：

```
Master Image/Machine Profile's VM's device id is different than the
NetworkMapping's device id '0'. Please provide a device id that matches
the master image/machine profile.
```

在这种情况下，请确保在 `New-ProvScheme` 的 `NetworkMapping` 参数中明确指定 `DeviceId`。例如：

```
New-ProvScheme -ProvisioningSchemeType "MCS" -InitialBatchSizeHint 1
-HostingUnitName $HostingUnitName `

            -IdentityPoolName $CatalogName -MasterImageVM $MasterImage
-ProvisioningSchemeName $CatalogName `

            -VMCpuCount 2 -VMMemoryMB 4096  -EnableAzureArcOnboarding `

            -AzureArcSubscriptionId $AzureArcSubscription -AzureArcRegion
$AzureArcRegion `

            -AzureArcResourceGroup $AzureArcResourceGroup

            -NetworkMapping @{"FDDxxxxxx-xxxx-4xxx-9EBC-3xxxxxxxx"="XDHyp:
\HostingUnits\<hosting unit name>\abc.network"}
```

适用于受支持的本地管理程序的额外存储的映像复制

此功能可实现映像版本规范实例在本地管理程序支持的多个存储位置之间的高效复制和管理。

用例

- 您可以将映像版本复制到新的或已替换的存储位置，从而允许在映像准备过程期间或之后在其他位置预配虚拟机。
- 创建新映像版本并指定其他存储位置时，准备好的映像版本规范会自动复制到这些指定的存储位置。
- 如果需要将现有映像版本与已替换或新添加的存储位置一起使用，您可以添加一个映像版本实例以复制到新的存储位置。

- 当向现有映像版本添加托管单元以及额外存储时，准备好的映像版本规范实例将复制到目标托管单元中指定的额外存储。

PowerShell 命令

- 添加一个新的映像实例，该实例将准备好的映像版本规范复制到指定的存储位置。

```
Add-ProvImageVersionSpecInstance -ImageVersionSpecUid <
ImageVersionSpecUid > -StorageIds "<StorageId1,StorageId2>"
-RunAsynchronously
```

- 删除现有映像版本规范实例副本，且该副本未被任何现有虚拟机使用。

```
Remove-ProvImageVersionSpecInstance -ImageVersionSpecUid <
ImageVersionSpecUid >  -ImageInstanceUid < ImageInstanceUid >
-RunAsynchronously
```

- 获取映像版本规范实例列表。

```
Get-ProvImageVersionSpecInstance -ImageVersionSpecUid  <
ImageVersionSpecUid >
```

下一步

有关创建特定云服务目录的信息，请参阅：

- 创建 AWS 目录
- 创建 XenServer 目录
- 创建 Google Cloud Platform 目录
- 创建 Microsoft Azure 目录
- 创建微软系统中心虚拟机管理器目录
- 创建 Nutanix 目录
- 创建 VMware 目录

如果这是创建的第一个目录，Web Studio 会引导您创建交付组。

要查看整个配置过程，请参阅安装和配置。

您可以使用 Web Studio 和 PowerShell 创建 Citrix Provisioning 目录。 此实现为您提供以下优势：

- 一个统一控制台，用于管理 MCS 和 Citrix Provisioning 目录。
- Citrix Provisioning 目录的新功能，例如身份管理解决方案、按需预配等。

目前，此功能仅适用于 Azure 和 VMware 工作负载。但是，在 VMware 环境中，您目前只能使用 PowerShell 命令创建目录。有关详细信息，请参阅在 Citrix Studio 中创建 Citrix Provisioning 目录。

更多信息

- 创建和管理连接及资源
- 管理计算机目录

创建 Amulet Hotkey CoreStation 计算机目录

创建计算机目录 描述了通用的计算机目录工作流程。以下信息涵盖了 Amulet Hotkey CoreStation 的具体细节。

> **注意：**
>
> 在创建 Amulet Hotkey CoreStation 目录之前，请完成 连接到 Amulet Hotkey CoreStation。

> 您可以使用以下方式创建 Amulet Hotkey CoreStation 计算机目录：

- 网络工作室
- (#using-powershell-commands)

使用 Web Studio

在“计算机目录设置”向导中：

1. 在“**操作系统**”页面上，选择“**多会话操作系统**”或“**单会话操作系统**”。
2. 在“**计算机管理**”页面上，选择“**已进行电源管理的计算机和另一项服务或技术**”。
3. 在“**虚拟机**”页面上，添加计算机及其 Active Directory 计算机帐户。您可以执行以下任一操作：
    - 单击“**添加计算机**”以手动添加计算机。“**选择 VM 窗口**”随即出现。展开您之前创建的 Amulet Hotkey CoreStation 机箱连接，然后选择要添加的节点。然后添加关联的计算机帐户名称。
    - 单击 **添加 CSV 文件** 以批量添加计算机。有关使用 CSV 文件添加计算机的信息，请参阅 使用 CSV 文件批量将计算机添加到目录。

“**范围**”和“**摘要**”页面不包含 Amulet Hotkey CoreStation 特定的信息。

使用 POWERSHELL 命令

运行 `New-BrokerCatalog` 和 `New-BrokerMachine` PowerShell 命令以创建代理目录并将计算机导入代理目录。

例如：

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

下一步操作

- 如果这是创建的第一个目录，Web Studio 将引导您创建交付组
- 要查看整个配置过程，请参阅安装和配置
- 有关电源管理，请参阅电源管理 Amulet Hotkey CoreStation VM

更多信息

- 创建和管理连接与资源
- 连接到 Amulet Hotkey CoreStation
- 创建计算机目录

创建 AWS EC2 目录

(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-create.html) 介绍了创建计算机目录的向导。以下信息涵盖了 AWS EC2 虚拟化环境特有的详细信息。

> **注意：**
>
> 在创建 AWS 目录之前，您需要完成与 AWS 的连接创建。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections/connection-aws.html)。

映像准备期间的网络设置

在映像准备期间，将基于原始 VM 创建一个准备虚拟机 (VM)。此准备 VM 与网络断开连接。为了断开准备 VM 的网络连接，将创建一个网络安全组以拒绝所有入站和出站流量。此网络安全组将持久存在并被重复使用。该网络安全组的名称为 `Citrix.XenDesktop.IsolationGroup-GUID`，其中 GUID 是随机生成的。

AWS 租用

AWS 提供以下租用选项：

- 共享租用（默认类型）和专用租用。共享租用意味着来自不同客户的多个 Amazon EC2 实例可能驻留在同一物理硬件上。
- 专用租用意味着您的 EC2 实例仅在您部署的其他实例所在的硬件上运行。其他客户不使用同一块硬件。

预配到 AWS 主机的要求

- 导入的 BYOL（自带许可证）映像 (AMI)。对于专用主机，请使用和管理您现有的许可证。
- 具有足够利用率的专用主机分配，以满足预配请求。
- 启用 **自动放置**。

配置 AWS 租用的选项

- **使用共享硬件**。此设置适用于大多数部署。多个客户共享硬件，即使他们之间不进行交互。使用共享硬件是运行 Amazon EC2 实例最经济实惠的选项。
- **使用专用主机**。Amazon EC2 专用主机是具有完全专用 EC2 实例容量的物理服务器，允许您使用现有的按插槽或按 VM 计费的软件许可证。专用主机具有基于实例类型的预设利用率。例如，分配的单个 C4 Large 实例类型的专用主机仅限于运行 16 个实例。有关详细信息，请参阅 AWS 网站。

  此设置适用于具有许可限制或安全要求且需要使用专用主机的部署。使用专用主机，您拥有整个物理主机并按小时计费。拥有该主机可让您启动该主机允许的任意数量的 EC2 实例，而无需额外费用。
- **使用专用实例**。此设置更适用于具有特定安全或合规性要求的部署。使用专用实例，您仍然可以享受拥有独立于其他 AWS 客户的主机的好处，但您无需支付整个主机的费用。您无需担心主机的容量，但实例的收费费率更高。

> **注意：**
>
> 如果没有正在进行的目录创建或映像更新任务，您可以删除任何可用的准备身份磁盘。

> 要使用 Studio 配置 AWS 租用，请参阅 使用 Web Studio 创建目录；要使用 PowerShell 配置，请参阅 使用 PowerShell 配置 AWS 专用主机租用。

标记 AWS 操作资源

Amazon Machine Image (AMI) 表示一种虚拟设备类型，用于在 Amazon 云环境（通常称为 EC2）中创建虚拟机。您可以使用 AMI 部署使用 EC2 环境的服务。当您创建目录以使用 MCS for AWS 预配计算机时，您选择 **AMI** 作为该目录的黄金映像。

> **重要提示：**
>
> 要使用操作资源标记，必须同时使用计算机配置文件和启动模板创建目录。

> 要创建 AWS 目录，您必须首先为您希望作为黄金映像的实例创建 AMI。MCS 从该实例读取标签并将其合并到启动模板中。然后，启动模板标签将应用于在您的 AWS 环境中创建的所有 Citrix® 资源，包括：

- 虚拟机
- VM 磁盘
- VM 网络接口
- S3 存储桶
- S3 对象
- 启动模板
- AMI

您可以在创建目录时使用 Studio 和 PowerShell 标记操作资源。对于 Studio，请参阅 使用 Web Studio 创建目录（**映像**页面）。对于 PowerShell，请参阅 使用 PowerShell 标记操作资源。

创建目录

您可以使用以下方式创建目录：

- Web 控制台
- PowerShell

使用 Web Studio 创建目录

1. 在左侧导航窗格中单击**计算机目录**。

2. 单击“**创建计算机目录**”。将显示“**计算机目录设置**”页面。
3. 在 **Machine Type** 页面上，为目录选择一种计算机类型，例如，多会话操作系统。
4. 在“**计算机管理**”页面上，选择以下设置：
    a. 选择电源管理的计算机（例如，虚拟机或刀片式 PC）。
    b. 选择“**Citrix 预配技术**”。然后，选择“**Citrix Machine Creation Services™**”。
    c. 在**资源**字段中，选择您在创建主机连接时配置的资源（可用区或本地区域），然后单击**下一步**。
5. 在“**桌面体验**”页面上，选择用户登录时所需的随机桌面或静态桌面。
6. 在**映像**页面上：
    a. 选择要用作目录中所有计算机主映像的计算机模板。
    b. 如果您希望目录中的 VM 继承计算机配置文件中的配置，请选择一个计算机配置文件。默认情况下，选中“**使用计算机配置文件**”复选框。要将计算机配置文件源更改为其他 VM 或启动模板版本，请单击编辑按钮。
    c. 选中“**将计算机标签应用于操作资源**”复选框，以将计算机标签应用于操作资源。此选项控制是否将计算机标签应用于在您的 AWS 环境中创建的每个有助于预配计算机的项目。操作资源是目录创建的副产品。它们包括临时资源和持久资源，例如准备 VM 实例和 AMI。

> **注意：**
>
> 仅当您在不分配计算机配置文件的情况下创建计算机目录时，才会显示“**安全**”页面。

7. 在“**虚拟机**”页面上：
    a. 输入目录的 VM 数量。
    b. 将显示基于计算机配置文件的默认计算机规范。要更改它，请选择编辑图标并选择计算机规范。
    c. 配置 AWS 租用模式。请参阅配置 AWS 租用模式的选项。
    d. 当主计算机大小达到最大容量时，您还可以配置辅助虚拟机。单击**辅助大小**（可选）。在**辅助计算机大小**窗口中，列出的虚拟机同时具有 Spot 和常规虚拟机类型。您最多可以选择 10 个辅助计算机大小。选择 10 个虚拟机后，列表中其他虚拟机将禁用进一步选择。单击**下一步**。在**辅助计算机大小**面板中，您可以选择多个计算机大小并拖放以更改优先级顺序。单击**完成**。所选计算机大小将显示在“辅助大小”（可选）中。单击编辑图标以根据需要进行编辑。

8. 仅当您在不分配计算机配置文件的情况下创建计算机目录时，才会显示**安全**页面。使用**安全**页面配置 VM 的安全组。这在编辑和克隆现有计算机目录时也适用。

   如果您创建基于计算机配置文件的计算机目录，则安全组配置将从计算机配置文件继承，并且**安全性**页面不会显示。

9. 在**网卡**页面上，为虚拟机选择网卡（或 ENI）。
10. 在**磁盘设置**页面上，选择是否启用回写缓存。
11. 在**计算机身份**页面上，通过选择域并为将在此计算机目录中创建的虚拟机创建新的 AD 帐户，为目录中的计算机配置本地 Active Directory 或 Microsoft Entra 混合加入。预配的虚拟机将加入所选域。指定将为虚拟机创建的新 AD 帐户的帐户命名方案。单击“下一步”。
12. 在**域凭据**页面上，单击**输入凭据**以提供所选域的凭据。出现提示时输入管理员级别的用户名和密码。如果您之前已按照我们的产品文档保存了域凭据，则还可以使用服务帐户。
13. 依次单击其余页面，直到显示“**摘要**”页面。为计算机目录输入名称，然后选择“**完成**”以创建计算机目录。

在 AWS 本地区域中创建计算机目录的限制

- 某些本地区域仅支持某些硬件配置（例如，珀斯本地区域不支持 GP3 卷，仅支持 GP2）。
- 由于只有 gp2 在所有本地区域中普遍受支持，并非所有区域都支持 gp3，因此 ID 磁盘创建默认使用 gp2 卷类型。
- 您必须选择一个在所需本地区域中支持其硬件规格的计算机配置文件。
- 准备好的映像 AMI 快照和 ID 磁盘快照默认放置在区域中，而不是本地区域（由于 AWS 对本地区域中 EBS 快照支持的可见性限制）。
- 只有支持完整 EC2 和 EBS 服务的本地区域才是受支持的区域。

使用 PowerShell 创建目录

使用 POWERSHELL 配置 AWS 专用主机租用

或者，您可以通过 PowerShell 预配 AWS 专用主机。使用 `New-ProvScheme` cmdlet，并将参数 `TenancyType` 设置为 `Host`。

使用 POWERSHELL 标记操作资源

要使用 PowerShell 标记资源，请执行以下操作：

1. 从 DDC 主机打开 PowerShell 窗口。
2. 运行命令 `asnp citrix` 以加载 Citrix 特定的 PowerShell 模块。

要标记预配 VM 的资源，请使用自定义属性 `AwsOperationalResourcesTagging`。示例：

```
New-ProvScheme -ProvisioningSchemeName test

-CustomProperties “AwsOperationalResourcesTagging,true”

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"

... <Other <standard provscheme parameters>
```

支持 MCSIO 的目录

MCS 存储优化 (MCSIO) 通过在内存或小型高速磁盘中缓存磁盘操作来提高 VM 的性能。您可以使用 PowerShell 命令创建支持 MCSIO 的非持久性目录。要创建此类目录，您必须在准备 AMI 实例期间安装或升级 VDA 时安装 MCSIO 驱动程序。默认情况下，该驱动程序未安装。

准备好 MCSIO AMI 后（在安装 VDA 时，选择在安装中包含 MCSIO 驱动程序的选项），您可以创建支持 MCSIO 的非持久性目录。

注意：

使用 Studio 仅配置磁盘缓存（不带内存缓存）的 MCSIO 选项已从所有虚拟机管理程序和云服务环境中删除。

创建支持 MCSIO 的目录

添加到 New-ProvScheme PowerShell 命令的四个参数是：

- `UseWriteBackCache`: 启用给定预配方案的缓存（回写缓存）
- `WriteBackCacheDiskSize`: 指定用于缓存的临时磁盘大小（以 GB 为单位）
- `WriteBackCacheMemorySize`: 指定用于缓存的内存量（以 MB 为单位）。这是一个可选参数。

注意：

- `WriteBackCacheDiskSize` 的值必须大于零，因为至少需要 1 GB 的缓存磁盘存储。缓存磁盘大小不得大于操作系统磁盘大小。
- `WriteBackCacheMemorySize` 的值必须是非零且小于计算机目录内存大小。

> 影响 MCSIO 的自定义属性包括：

- `WBCDiskStorageType`: 定义卷类型，该类型用于 AWS 中的临时磁盘。此参数采用 `volume-type[:iops][:throughput]` 格式的字符串参数。以下是卷类型：
  - gp2: 请勿将 iops 和吞吐量参数用于此卷类型
  - gp3: 将 iops 和吞吐量参数用于此卷类型
  - io1: 仅将 iops 参数用于此卷类型
  - io2: 仅将 iops 参数用于此卷类型

  默认卷类型为 **gp2**。
- `PersistWBC`: 控制在 AWS 实例关闭时是保留还是丢弃缓存磁盘。如果设置为 `true`，则保留缓存磁盘。如果设置为 `false`（默认值），则仅在 AMI 实例开机时创建并保留缓存磁盘。
- `PersistOSDisk`: 控制在 AWS 实例关闭时是保留还是丢弃操作系统磁盘。如果设置为 `true`，则保留操作系统磁盘。如果设置为 `false`（默认值），则仅在 AMI 实例开机时创建并保留操作系统磁盘。

在 PowerShell 窗口中执行以下步骤以创建启用 MCSIO 的非持久目录：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 创建代理目录和身份池。
4. 创建预配方案。例如：

```
$HostingUnitUid = '0xxxx1d9-bbfc-xxxf-bxxb-exxxxxe008b2'

$MasterImageVM = 'XDHyp:\HostingUnits\ctx-test\aws-apollo-non-
persistent-multi-mcsio-vda-win2022 (ami-0bf1810488acbxxxb).template'

$NetworkMap = @{ 'NetworkPath' = 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\10.0.128.0`/17
(vpc-0fa6e41d72507fxxx).network' }

$SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\private.securitygroup' )

$ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
Instance.serviceoffering'
```

```
$CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,false'




$provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
-HostingUnitUid $HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

- MasterImageVM $MasterImageVM `

-NetworkMap $NetworkMap `

-ServiceOffering $ServiceOffering `

-SecurityGroup $SecurityGroup `

-CustomProperties $CustomProperties `

-UseWriteBackCache -WriteBackCacheDiskSize 16 -WriteBackCacheMemorySize
256
```

5. 将 VM 添加到目录。

使用 MCSIO 提高启动性能

如果启用 MCSIO 并将 `PersistWBC` 和 `PersistOSDisk` 自定义属性设置为 `tru`e，则可以提高 VM 的启动性能。通过此设置，VM 可以更快地启动，因为它们无需初始化新的缓存磁盘或从其模板重新创建根磁盘。

使用 PowerShell 创建基于计算机配置文件的计算机目录

您可以使用计算机配置文件从 EC2 实例 (VM) 或启动模板版本捕获硬件属性，并将其应用于预配的计算机。捕获的属性可以包括例如 EBS 卷属性、实例类型、EBS 优化、CPU 选项、租用类型、休眠功能、安全组以及其他受支持的 AWS 配置。

您可以使用 AWS EC2 实例 (VM) 或 AWS 启动模板版本作为计算机配置文件输入。

> **注意：**

> EBS 卷属性仅从计算机配置文件派生。

重要注意事项

创建 MCS 计算机目录时的重要注意事项：

- 如果您在 `New-ProvScheme` 和 `Set-ProvScheme` 命令中添加机器硬件属性参数，则参数中提供的值将覆盖机器配置文件中的值。
- 如果您将 `AwsCaptureInstanceProperties` 设置为 `true` 并且未设置 `MachineProfile` 属性，则仅捕获 IAM 角色和标签。
- 您不能同时设置 `AwsCaptureInstanceProperties` 和 `MachineProfile`。

> **注意：**
>
> `AwsCaptureInstanceProperties` 已弃用。

- 如果未提供机器配置文件，则必须明确提供以下属性的值：
  - 安全组
  - ENI 或虚拟网络
- 仅当您启用 `AwsCaptureInstanceProperties` 或指定机器配置文件时，才能启用 `AwsOperationalResourcesTagging`。

创建 MCS 机器目录后需要考虑的重要事项是：

- 您无法将目录从基于机器配置文件的目录更改为非基于机器配置文件的目录。

在机器配置文件输入中配置安全组

您可以创建一个 MCS 机器目录，其中预配的 VM 会根据每个 ENI（网络接口）分配安全组。为此，请使用具有不同安全组映射到不同 ENI 的机器配置文件输入（EC2 实例或启动模板）。例如，如果机器配置文件输入具有 ENI A 和 SG 1 以及 ENI B 和 SG 2，则预配的 VM 也必须具有 ENI A 和 SG 1 以及 ENI B 和 SG 2。

检索网络接口详细信息

运行以下命令以获取网络接口数据记录列表，包括接口 SubnetId、分配的安全组和分配的网络。

```
(Get-HypInventoryItem -LiteralPath 'XdHyp:\HostingUnits\cvad-test' –
ResourceType vm). AdditionalData
```

> **注意：**
>
> MCS 目前不允许每个网络接口有多个网络。

使用计算机配置文件创建计算机目录

要使用计算机配置文件创建计算机目录，请执行以下操作：

1. 打开一个 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 如果尚未创建，请创建身份池。例如，

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain abcdf -NamingSchemeType Numeric
```

4. 运行 New-ProvScheme 命令。例如：

```
New-ProvScheme -ProvisioningSchemeName demet-test-1

-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1

-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4

-CleanOnBoot

-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-demet-
ami.0 (ami-0ca813xxxxxx061ef).template'

-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).vm'
```

5. 完成目录创建。

更新计算机配置文件

要更新最初使用计算机配置文件预配的目录上的计算机配置文件，请执行以下操作。您还可以在编辑 MCS 计算机目录时更改计算机配置文件源的租用类型和休眠功能。

1. 运行 `Set-ProvScheme` 命令。例如，

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

使用 POWERSHELL 创建具有启动模板版本的目录

您可以创建以启动模板版本作为计算机配置文件输入的 MCS 计算机目录。您还可以将计算机配置文件目录的输入从 VM 更新为启动模板版本，以及从启动模板版本更新为 VM。

在 AWS EC2 控制台上，您可以提供启动模板的实例配置信息以及版本号。当您在创建或更新计算机目录时将启动模板版本指定为计算机配置文件输入时，该启动模板版本的属性将复制到预配的 VDA VM。

以下属性可以使用计算机配置文件输入提供，也可以在 `New-ProvScheme` 或 `Set-ProvScheme` 命令中显式作为参数提供。如果在 `New-ProvScheme` 或 `Set-ProvScheme` 命令中提供了这些属性，则它们将优先于这些属性的计算机配置文件值。

- 服务产品
- 网络
- 租用类型

注意：

如果计算机配置文件启动模板中未提供服务产品，或者未在 `New-ProvScheme` 命令中将其作为参数提供，则会收到相应的错误。

要使用启动模板版本作为计算机配置文件输入来创建目录，请执行以下操作：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 获取启动模板的启动模板版本列表。例如：

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. 如果尚未创建身份池，请创建一个。例如：

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. 使用启动模板版本作为计算机配置文件输入创建预配方案。例如：

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. 将预配方案注册为代理目录。例如：

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
```

```
-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. 完成目录创建。

更新计算机配置文件源

您还可以将计算机配置文件目录的输入从 VM 更新为启动模板版本，以及从启动模板版本更新为 VM。例如：

- 要将计算机配置文件目录的输入从 VM 更新为启动模板版本：

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- 要将计算机配置文件目录的输入从启动模板版本更新为 VM：

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

加密操作系统、ID 和 WBC 磁盘

您可以使用 AWS KMS 密钥（客户管理密钥和 AWS 管理密钥）创建持久和非持久的 VM 目录，这些密钥可用于加密操作系统磁盘、身份磁盘 (ID) 和回写缓存磁盘 (WBC)。

- AWS 管理密钥每年自动轮换。
- 客户管理密钥的自动轮换是可选的，可以手动管理。

有关 KMS 密钥的更多信息，请参阅以下 AWS 文档：

- AWS KMS 概念
- 自动密钥轮换的工作原理

要加密操作系统、ID 和 WBC 磁盘，请配置以下其中一项：

- 使用已加密的主映像（例如，从包含使用 KMS 密钥加密的 EBS 根卷的实例或快照创建的 AMI）
- 使用包含加密 EBS 根卷的计算机配置文件源（VM 或启动模板）。

限制

请考虑以下限制：

- MCS 目前仅支持主映像 AMI 上的一个磁盘。
- 您无法直接加密现有的未加密 EBS 卷或快照，也无法修改现有加密卷的 KMS 密钥。为此，您必须：

  a. 创建该卷的新快照。

  b. 从该快照创建新卷

  c. 加密新卷。

请参阅以下 AWS 文档：

- 加密未加密资源
- EBS 卷自动或默认加密的限制：自动加密现有和新的 Amazon EBS 卷。

创建具有磁盘加密的目录

您可以使用以下方法创建具有磁盘加密的 MCS 计算机目录：

- 主映像
- 计算机配置文件

使用计算机配置文件输入时的注意事项包括：

- 计算机配置文件输入的 KMS 密钥优先于主映像的 KMS 密钥。
- 如果未提供计算机配置文件输入，则使用主映像 AMI 的 KMS 密钥来加密目录 VM 的磁盘。
- 如果计算机配置文件存在块设备映射，则主映像模板 (AMI) 和计算机配置文件中存在的块设备必须匹配。例如，如果 AMI 在 `/dev/sda1` 上定义了设备，则计算机配置文件也必须在 `/dev/sda1` 上定义设备。
- 如果计算机配置文件源中没有密钥且主映像未加密，则目录 VM 的磁盘不会加密。
- 当主映像加密时，计算机配置文件源 VM 或启动模板必须具有加密的根卷才能被视为有效输入。

修改现有目录

您可以使用 `Set-ProvScheme` PowerShell 命令修改现有目录，以使其具有：

- 具有包含新 KMS 密钥的卷的计算机配置文件输入。
- 使用新 KMS 密钥加密的主映像模板 AMI。

重要注意事项：

- 添加到目录的新 VM 的卷使用新的 KMS 密钥进行加密。
- 要在存在现有计算机配置文件时更新加密设置，请使用新的计算机配置文件运行 `Set-ProvScheme`。
- 您无法将现有目录从加密卷修改为未加密卷。 您无法从加密的主 AMI 更新映像到未加密的主 AMI。

为 VM 实例启用 NitroTPM 和 UEFI 安全启动

创建目录时，您现在可以选择启用 NitroTPM 和/或 UEFI 安全启动的主映像 (AMI)。因此，目录中预配的 VM 也将启用 NitroTPM 和/或 UEFI 安全启动。此实现可确保 VM 的安全性和可信度。有关 NitroTPM 和 UEFI 安全启动的更多信息，请参阅 Amazon 文档。

限制

- 目前，您可以在除中国以外的所有 AWS 区域（包括 AWS GovCloud (US) 区域）中使用 NitroTPM 和安全启动。
- 您无法在现有目录上启用 NitroTPM 和 UEFI 安全启动。如果您想要一个启用了 NitroTPM 和 UEFI 安全启动的目录，请创建一个新目录。

主要步骤

1. 设置您的 AWS 环境。
2. 创建到 AWS 的连接。
3. 创建启用了 NitroTPM 和/或 UEFI 安全启动的主映像 (AMI)。
4. 在 Web Studio 目录创建菜单中或使用 PowerShell 命令创建预配方案时，通过选择启用了 NitroTPM 和 UEFI 安全启动的主映像来创建计算机目录。

添加到所创建目录的 VM 已启用 NitoTPM 和 UEFI 安全启动。

创建支持 NITROTPM 和 UEFI 安全启动的 AMI

1. 您可以从已启用 NitroTPM 和/或 UEFI 安全启动的 VM 创建 AMI。
    a. 使用 AWS Marketplace 映像创建实例。例如，搜索 `TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`。

b. 下载单会话或多会话 VDA。

c. 从该 VM 创建 AMI。

2. 使用 register-image 命令：

```
--boot-mode (string)

--tpm-support (string)
```

有关详细信息，请参阅 register-image。

请参阅以下 AWS 文档：

- 确定 EC2 实例类型支持的启动模式
- 将 NitroTPM 与 Amazon EC2 实例结合使用的要求/.

您可以从 Delivery controller™ 主机打开 PowerShell 窗口，以检查特定项是否：

- 服务产品支持 NitroTPM 或 UEFI 安全启动

```
(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.BootMode

(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
```

- 模板支持 NitroTPM 或 UEFI 安全启动

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.BootMode



(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

更新现有目录的服务产品

您可以使用 `Set-ProvScheme` 更改现有目录的服务产品。此更改适用于新添加的 VM。但是，在以下情况下会收到错误：

AMI 启动模式	AMI 支持 NITRO TPM 吗？	服务产品支持 NITROTPM 和 UEFI 安全启动吗？
UEFI	否	否
传统 BIOS	是	否
UEFI	是	否
UEFI 首选	是	否

复制虚拟机上的标签

您可以将计算机配置文件中指定的 NIC 和磁盘（身份磁盘、回写缓存磁盘和操作系统磁盘）上的标签复制到 MCS 计算机目录中新创建的虚拟机。您可以在任何计算机配置文件源（AWS VM 实例或 AWS 启动模板版本）中指定这些标签。此功能适用于持久性和非持久性计算机目录和虚拟机。

注意：

- 在 AWS EC2 控制台中，您无法在 **Launch Template Version Resource Tags** 下看到 **Tag Network Interfaces** 值。但是，您可以运行 PowerShell 命令 `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` 来查看标签规范。
- 如果计算机配置文件源（VM 或启动模板版本）有两个网络接口（eni-1 和 eni-2），并且 eni-1 具有标签 t1，eni-2 具有标签 t2，则 VM 会获取这两个网络接口的标签。

使用 PowerShell 筛选 VM 实例

您用作计算机配置文件 VM 的 AWS VM 实例必须兼容，以便计算机目录能够正确创建和运行。要列出可用作计算机配置文件输入 VM 的 AWS VM 实例，您可以使用 `Get-HypInventoryItem` 命令。该命令可以对托管单元上可用的 VM 清单进行分页和筛选。

分页：

Get-HypInventoryItem 支持两种分页模式：

- 分页模式使用 `-MaxRecords` 和 `-Skip` 参数返回项目集：
  - `-MaxRecords`：默认值为 **1**。这控制要返回的项目数。
  - `-Skip`：默认值为 **0**。这控制从管理程序中列表的绝对开头（或绝对结尾）跳过的项目数。

- 滚动模式使用 `-MaxRecords`、`-ForwardDirection` 和 `-ContinuationToken` 参数以允许记录滚动：
  - `-ForwardDirection`：默认值为 **True**。这与 `-MaxRecords` 一起使用，以返回下一组匹配记录或上一组匹配记录。
  - `-ContinuationToken`：返回紧随其后（如果 `ForwardDirection` 为 **false**，则返回紧随其前）但不包括 `ContinuationToken` 中给定项的项。

分页示例：

- 返回名称最低的计算机模板的单个记录。`AdditionalData` 字段具有 `TotalItemsCount` 和 `TotalFilteredItemsCount`：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- 返回名称最低的计算机模板的 10 条记录：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- 返回以最高名称结尾的记录数组：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- 返回从与给定 `ContinuationToken` 关联的计算机模板开始的记录数组：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

筛选：

支持以下附加可选参数进行筛选。您可以将这些参数与分页选项结合使用。

- `-ContainsName "my_name"`：如果给定字符串与 AMI 名称的一部分匹配，则该 AMI 将包含在 `Get` 结果中。例如：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`：如果 AMI 具有这些标记中的至少一个，则它将包含在 `Get` 结果中。例如：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **注意：**
>
> 支持两个标记值。**未标记**标记值匹配其标记列表中没有给定标记的项。**所有值**标记值匹配具有该标记的项，无论标记的值如何。否则，仅当项具有该标记且值等于筛选器中给定的值时，才会发生匹配。

- `-Id "ami-0a2d913927e0352f3"`：如果 AMI 与给定 ID 匹配，则它将包含在 `Get` 结果中。例如：

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxxx
```

根据 AdditionalData 参数进行筛选：

`AdditionalData` 筛选器参数根据模板或 VM 的功能、服务产品或 AdditionalData 中的任何属性列出模板或 VM。例如：

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

您还可以添加 `-Warn` 参数来指示不兼容的 VM。VM 包含一个名为 **Warning** 的 `AdditionalData` 字段。例如：

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

VM 的备份 SKU 列表

公共云有时可能会出现特定 EC2 实例类型（“主 SKU”）容量不足的情况。如果主 VM 配置不可用，则 VM 无法启动，从而导致时间损失和业务中断。为了解决此类情况，请提供一个备份 EC2 实例类型（“备份 SKU”）列表，以便 MCS 在出现容量相关问题时可以回退到这些类型。

在创建或更新 MCS 计算机目录时，使用自定义属性 `BackupVmConfiguration` 提供备份 EC2 实例类型列表（“备份 SKU 列表”）。

如果主 EC2 实例失败，MCS 会尝试按照您指定的顺序回退到备份 EC2 实例类型。如果 MCS 无法回退到任何提供的备份 EC2 实例类型，则会显示错误消息。然后，您可以尝试再次启动主 EC2 实例。如果此操作失败，MCS 会重试备份 EC2 实例类型。

备份 SKU 列表可以包含按需实例。

此功能适用于持久性和非持久性 MCS 计算机目录。

重要注意事项

- 您可以在备份 SKU 列表中提供多个备份 EC2 实例类型。
- 备份 SKU 列表必须是唯一的。
- 备份 EC2 实例不能与主 EC2 实例相同。
- 备份 EC2 实例必须是有效的 AWS 实例类型。
- 请勿指定重复的服务产品。例如：`BackupVmConfiguration,t2.small|t3.small|t2.small` 无效。
- 列表中指定的服务产品必须与计算机目录配置兼容。例如，如果目录使用 UEFI 且备份列表中指定的服务产品不支持 UEFI，则目录创建或更新会在预检期间失败。
- 您可以使用 `Set-ProvScheme` PowerShell 命令修改现有目录的备份 SKU 列表。您可以使用 `Set-ProvVM` 和 `Set-ProvVMUpdateTimeWindow` PowerShell 命令修改现有 VM。

配置备份 EC2 实例

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 创建 Broker 目录。
4. 创建身份池。

5. 使用自定义属性 `BackupVmConfiguration` 添加备份 EC2 实例列表并创建预配方案。例如：

```
$serviceOffering = "XDHyp:\HostingUnits\$hostingUnitName\T3 Medium
Instance.serviceoffering"

$customProperties =
"AwsCaptureInstanceProperties,false;AwsOperationalResourcesTagging,fals
e;BackupVmConfiguration,t2.small|t2.large|t3.small|t3.large;"

$createdProvScheme = New-ProvScheme -ProvisioningSchemeName
$provisioningSchemeName -HostingUnitName $hostingUnitName
-IdentityPoolName $provisioningSchemeName -NetworkMapping
$networkMapping -SecurityGroup $securityGroupPath -ServiceOffering
$serviceOffering -MasterImageVM $masterImageVm -CustomProperties
$customProperties
```

6. 使用预配方案的唯一 ID 更新 BrokerCatalog。
7. 创建虚拟机并将其添加到目录。

使用 AWS Spot 实例创建目录

与按需实例相比，Spot 实例可节省高达 90% 的成本。如果容量不可用，Amazon EC2 可能会中断 Spot 实例，因此它们仅适用于非关键应用程序和桌面。

有关 Spot 实例的信息，请参阅 AWS 文档 Spot 实例。

此外，您可以将 Spot 实例用作主 EC2 实例类型和备份 EC2 实例。您可以使用 PowerShell 提供备份 EC2 实例类型列表（可以是按需实例和 Spot 实例的“备份 SKU”），以便 MCS 在出现容量相关问题时可以回退到这些实例。

重要注意事项

- 您只能使用计算机配置文件工作流创建 Spot 实例目录。
- 仅支持持久性 Spot 实例请求类型。不支持一次性 Spot 实例请求。
- 仅支持 **Stop** 和 **Hibernate** 中断行为。
- 您可以将现有目录的配置从按需实例更改为 Spot 实例，反之亦然。但是，将 EC2 实例从按需更改为 Spot 实例很复杂。请参阅 AWS 文档 将 EC2 实例从按需定价切换到 Spot 定价。
- 删除已预配的 Spot 实例时，请取消现有的 Spot 实例请求。否则，AWS 将创建一个新的 Spot 实例。

使用 AWS SPOT 实例创建目录的步骤

1. 使用 Spot 实例创建计算机配置文件源。有关创建 Spot 实例的步骤，请参阅 创建 Spot 实例请求 。
2. 使用包含 `New-ProvScheme` PowerShell 命令的计算机配置文件创建计算机目录。您可以使用 `Set-ProvScheme` 命令更新目录。

将 SPOT 实例用作备份 SKU

您可以将 Spot 实例用作主 EC2 实例类型和备份 EC2 实例。您可以使用 PowerShell 提供备份 EC2 实例类型列表（可以是按需实例和 Spot 实例的“备份 SKU”），以便 MCS 在出现容量相关问题时回退到这些实例。

> **注意：**
>
> 您可以在备份 SKU 列表中指定重复的 Spot 实例。示例：`BackupVmConfiguration,t2.small:Spot|t2.small|t3.small` 有效。

所需权限

如果您将 Spot 实例用作主 EC2 实例或备份 EC2 实例，则需要以下权限：

- `ec2:DescribeSpotInstanceRequests`
- `ec2:CancelSpotInstanceRequests`

配置备份 SPOT 实例

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 创建 Broker 目录。
4. 创建身份池。
5. 使用自定义属性 `BackupVmConfiguration` 添加备份 EC2 实例列表并创建预配方案。例如：

```
$serviceOffering \= "XDHyp:\\HostingUnits\\$hostingUnitName\\T3 Medium
Instance.serviceoffering"

$customProperties \=
"AwsCaptureInstanceProperties,false;AwsOperationalResourcesTagging,fals
e;BackupVmConfiguration,t2.small|t2.large|t3.small:Spot|t3.large:Spot"
```

```
$createdProvScheme \= New-ProvScheme \-ProvisioningSchemeName
$provisioningSchemeName \-HostingUnitName $hostingUnitName \-
IdentityPoolName $provisioningSchemeName \-NetworkMapping
$networkMapping \-SecurityGroup $securityGroupPath \-ServiceOffering
$serviceOffering \-MasterImageVM $masterImageVm \-CustomProperties
$customProperties
```

6. 使用预配方案的唯一 ID 更新 BrokerCatalog。
7. 创建虚拟机并将其添加到目录。

下一步

- 如果这是创建的第一个目录，系统将引导您创建交付组。
- 要查看整个配置过程，请参阅 安装和配置。
- 要管理目录，请参阅管理计算机目录和管理 AWS EC2 目录。

更多信息

- 创建和管理连接和资源
- 连接到 AWS EC2
- 创建计算机目录

创建 Azure Local 目录

创建计算机目录 介绍了创建计算机目录的向导。以下信息涵盖了 Azure Local 环境特有的详细信息。

> **注意：**
>
> 在创建 Azure Local 计算机目录之前，您需要完成与 Azure Local 的连接。请参阅连接到 Azure Local。

要求

- VDA 版本：2507 及更高版本
- 不支持 Windows 10/11 多会话工作负载

创建主映像

创建计算机目录需要主映像。

MCS 使用 Azure Local VM 映像作为主映像。在使用 MCS 在 Azure Local 群集中预配工作负载之前，您需要准备一个已安装 VDA 的 Azure Local VM 映像。

1. 使用 Azure 门户创建 Azure Local VM。
2. 连接到创建的 Azure Local VM 以安装 VDA 和所需的软件。
3. 使用 Windows 任务计划程序创建一个计划任务，以便在虚拟机启动时在系统上下文中运行以下脚本。

```
$tagFileName = 'E6DA6616-8EC4-48E0-BE93-58CE6ACE3CFB.tag'


$foundDrive = $null


foreach ($drive in Get-PSDrive -PSProvider FileSystem) {


$tagPath = Join-Path $drive.Root $tagFileName


if (Test-Path $tagPath) {


    $foundDrive = $drive.Root


    break


}


}
```

```
if ([string]::IsNullOrEmpty($foundDrive)) { exit 0 }

$installScript = Join-Path $foundDrive 'install.ps1'

if (Test-Path $installScript) {

powershell.exe -NoProfile -ExecutionPolicy Bypass -File $installScript

} else { exit 1 }

sc.exe stop mocguestagent 2>$null

sc.exe delete mocguestagent 2>$null

Remove-Item 'HKLM:
\SYSTEM\CurrentControlSet\Services\EventLog\Application\mocguestagent'
-Recurse -Force -ErrorAction SilentlyContinue

$setupComplete = 'C:\Windows\Setup\Scripts\SetupComplete.cmd'
```

```
if (Test-Path $setupComplete) { & $setupComplete }
```

4. 停止 Azure Local 虚拟机。
5. 请参阅从现有 Azure Local VM 创建 VM 映像，以从准备好的 Azure Local VM 创建 Azure Local VM 映像。

注意：

当您使用已安装并载入 Azure Connected Machine 代理版本 1.61 或更高版本的 Azure Local VM 准备主映像时，由于删除代理配置文件时访问被拒绝，MCS 中的目录创建在映像准备过程中失败。作为一种解决方法，在创建主映像时执行以下操作：导航到 `C:\ProgramData\AzureConnectedMachineAgent\Config\agentconfig.json`，右键单击该文件，选择**属性**，然后清除**只读**属性复选框。

创建目录

您可以创建 Azure Local 目录，以在 Azure Local 环境中创建、交付和电源管理计算机。

注意：

- 目录名称的长度不得超过 49 个字符。
- 避免在目录名称或计算机命名方案中使用 Microsoft Azure 保留字。有关详细信息，请参阅 Microsoft 文档。

您可以使用以下方式创建目录：

- Web 工作室
- (#create-a-catalog-using-powershell)

使用 WEB STUDIO 创建目录

您可以在 Azure Local 环境中创建 MCS 计算机目录。

在“计算机目录设置”向导中：

1. 在“**操作系统**”页面上，选择“**多会话操作系统**”或“**单会话操作系统**”。
2. 在**计算机管理**页面上：

a. 选择**已进行电源管理的计算机（例如，虚拟机或刀片式 PC）**。
b. 选择使用 **Citrix 预配技术**部署计算机。
c. 在 Citrix Machine Creation Services (MCS) 下选择 Azure Local 托管单元。

3. 在**桌面体验**页面上，根据您在“计算机类型”页面上选择的计算机类型选择选项。
4. 在**映像**页面上：

a. 选择主映像。目前，Azure Local 不支持准备好的映像。
b. 您可以向所选映像添加备注。

> **注意：**
>
> - 选择主映像后，操作系统类型将自动填充。
> - 不支持计算机配置文件。

5. 在**网卡**页面上，选择一个或多个网卡，并将虚拟网络与每个网卡关联。
6. 在“**虚拟机**”页面上：

a. 指定要创建的虚拟机数量。如果您不想创建任何虚拟机，请输入 0。稍后，您可以通过添加计算机为空目录创建 VM。
b. 选择每个 VM 的内存量（以 MB 为单位）和虚拟 CPU 数量。
c. 为计算机配置回写缓存以提高 I/O 性能。

7. 按照屏幕上的说明完成剩余步骤，这些步骤不包含 Azure Local 特有的信息。

您还可以使用 Web Studio 创建 Azure Local 目录，以交付和管理 Azure Local 集群中现有计算机的强大功能。

在“计算机目录设置”向导中：

1. 在“**操作系统**”页面上，选择“**多会话操作系统**”或“**单会话操作系统**”。
2. 在“**计算机管理**”页面上，选择“**已进行电源管理的计算机**”，然后选择“**其他服务或技术**”作为部署计算机的方式。
3. 在**虚拟机**页面上，添加计算机及其 Active Directory 计算机帐户。您可以：

- 手动添加计算机：单击**添加计算机**以手动添加计算机。此时将显示**选择 VM**窗口。展开您之前创建的 Azure Local 连接，然后选择要添加的 VM。然后添加关联的计算机帐户名称。

- 使用 CSV 文件添加计算机：单击**从 CSV 文件导入以批量添加计算机**。有关使用 CSV 文件添加计算机的信息，请参阅使用 CSV 文件批量将计算机添加到目录。

4. 按照屏幕上的说明完成剩余步骤，这些步骤不包含 Azure Local 特有的信息。

使用 POWERSHELL 创建目录

您可以使用 PowerShell 命令在 Azure Local 环境中创建 MCS 计算机目录。

脚本头

请确保提供脚本头中定义的正确参数值。

```
$catalogName = "" # Name of the catalog you want to create



$masterImageResourceGroupName = "" # Name of resource group that the
master Azure Local VM image resides in



$catalogResourceGroup = "" # Name of resource group that the created VMs
reside in



$masterImage = "" # Name of the master Azure Local VM image you want to
use



$vNet = "" # Name of the logical network that the created VMs should be
attached to



$masterImagePath = "XDHyp:\HostingUnits\$hostingUnitName\image.folder\
$masterImageResourceGroupName.resourcegroup\$masterImage"



$networkMapping = @{"0"="XDHyp:\HostingUnits\$hostingUnitName\
\network.folder\$vNet.network"}
```

```
$customPropertiesXml = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"$catalogResourceGroup`" /><Property
xsi:type=`"StringProperty`" Name=`"OsType`" Value=`"Windows`" /></
CustomProperties>"
```

创建包含 1 个 VM 的 MCS 目录

运行 asnp citrix*

创建计算机目录

```
New-BrokerCatalog -AllocationType "Random" -IsRemotePC $false
-MinimumFunctionalLevel "L7_34" -Name $catalogName -PersistUserChanges
"Discard" -ProvisioningType "MCS" -SessionSupport "SingleSession"
```

创建身份池

```
New-AcctIdentityPool -AllowUnicode $true -Domain "test.local"
-IdentityPoolName $catalogName -IdentityType "ActiveDirectory"
-NamingScheme "demoVM#" -NamingSchemeType "Numeric" -OU
"CN=Computers,DC=test,DC=local"
```

创建预配方案

```
New-ProvScheme -CleanOnBoot $true -CustomProperties $customPropertiesXml
-HostingUnitName $hostingUnitName -IdentityPoolName $catalogName
-MasterImageVM $masterImagePath -NetworkMapping $networkMapping
-ProvisioningSchemeName $catalogName -ProvisioningSchemeType "MCS"
-VMCpuCount 4 -VMMemoryMB 8192
```

将目录链接到预配方案

```
$schemeUid =(Get-ProvScheme -ProvisioningSchemeName
$catalogName).ProvisioningSchemeUid.Guid



Set-BrokerCatalog -Name $catalogName -ProvisioningSchemeId $schemeUid
```

创建 AD 帐户

```
New-AcctADAccount -Count 1 -IdentityPoolName $catalogName
```

预配 VM

```
New-ProvVM -ADAccountName "domain\demoVM1" -ProvisioningSchemeName
$catalogName
```

将计算机添加到代理目录

```
New-BrokerMachine -CatalogName $catalogName -MachineName 'domain\demoVM1'
```

下一步操作

- 如果这是创建的第一个目录，Web Studio 会引导您创建交付组
- 有关电源管理 Azure 本地 VM 的信息，请参阅电源管理 Azure 本地 VM。

更多信息

- 创建和管理连接与资源
- 连接到 Azure Local
- 创建计算机目录

创建 XenServer® 目录

创建计算机目录 介绍了创建计算机目录的向导。以下信息涵盖了 XenServer 虚拟化环境特有的详细信息。

> **注意：**
>
> 在创建 XenServer 目录之前，您需要完成与 XenServer 的连接创建。请参阅连接到 XenServer。

使用 XenServer 连接创建计算机目录

支持 GPU 的计算机需要专用的主映像。这些 VM 需要支持 GPU 的显卡驱动程序。配置支持 GPU 的计算机，以允许 VM 运行使用 GPU 进行操作的软件。

1. 在 XenCenter® 中，创建具有标准 VGA、网络和 vCPU 的 VM。
2. 更新 VM 配置以启用 GPU 使用（直通或 vGPU）。
3. 安装受支持的操作系统并启用 RDP。

4. 安装 Citrix VM Tools 和 NVIDIA 驱动程序。
5. 清除虚拟网络计算 (VNC) 管理控制台以优化性能，然后重新启动 VM。
6. 系统会提示您使用 RDP。使用 RDP 安装 VDA，然后重新启动 VM。
7. （可选）为 VM 创建快照，作为其他 GPU 主映像的基线模板。
8. 使用 RDP 安装在 XenCenter 中配置并使用 GPU 功能的客户特定应用程序。

限制

- 如果 Citrix Virtual Apps and Desktops 部署（其 VM 托管在 Citrix Hypervisor 8.2 累积更新 1 上）在单个 MCS 目录中使用多个 GFS2 SR，则目录中的 VM 在部署期间无法访问 VDI。系统会报告“VDI is currently in use”错误。
- Citrix Hypervisor 8.2 累积更新 1 不支持带 GFS2 SR 的 MCS 完全克隆 VM。

有关详细信息，请参阅 Constraints。

这些限制不适用于 XenServer 8 及更高版本。

使用机器配置文件创建计算机目录

使用 MCS 创建目录以预配计算机时，可以使用计算机配置文件从虚拟机捕获硬件属性，并将其应用于目录中新预配的 VM。如果未使用 `MachineProfile` 参数，则硬件属性将从主映像 VM 或快照中捕获。

> **注意：**
>
> 目前，您只能使用 VM 作为计算机配置文件输入。
>
> 启用 MCSIO 后，您可以在创建 MCS 目录后更新内存和磁盘缓存大小。您可以显式配置以下参数以覆盖计算机配置文件输入中的参数值：

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

要使用计算机配置文件创建目录：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*`。

3. 创建身份池。身份池是用于存储要创建的 VM 的 Active Directory (AD) 帐户的容器。例如：

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
"ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
"Numeric" -Scope @() -ZoneUid "xxxxxxxx"
```

4. 在 Active Directory 中创建所需的 AD 计算机帐户。

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -Force

New-AcctIdentity -IdentityPoolName "ExampleIdentityPool" -Count 10
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. 运行 `New-ProvScheme` 命令以创建目录。例如：

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()

-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm"
```

6. 将预配方案注册为代理目录。例如：

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
```

```
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. 将 VM 添加到目录。

要使用新的计算机配置文件更新目录：

1. 运行 `Set-ProvScheme` 命令。例如：

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

   有关 Set-ProvScheme 命令的详细信息，请参阅 Set-ProvScheme。

注意：

- 在此情况下，`Set-ProvScheme` 命令不会更改目录中现有 VM 的计算机配置文件。只有添加到目录中的新创建 VM 才具有新的计算机配置文件。
- 您无法将基于计算机配置文件的计算机目录转换为非基于计算机配置文件的计算机目录。

下一步操作

- 如果这是创建的第一个目录，Web Studio 会引导您创建交付组
- 要查看整个配置过程，请参阅安装和配置
- 要管理目录，请参阅 Manage machine catalogs 和 Manage a XenServer catalog

更多信息

- 创建和管理连接与资源
- 连接到 XenServer
- 创建计算机目录

创建 Google Cloud Platform 目录

创建计算机目录 介绍了用于创建计算机目录的向导。以下信息涵盖了 Google 云环境特有的详细信息。

> **注意：**
>
> 在创建 Google Cloud Platform (GCP) 目录之前，您需要完成与 GCP 的连接创建。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections/connection-gcp.html)。

准备主 VM 实例和永久性磁盘

> **提示：**
>
> 永久性磁盘是 Google Cloud 中虚拟磁盘的术语。

> 要准备主 VM 实例，请创建并配置一个 VM 实例，其属性应与您计划的计算机目录中克隆的 VDA 实例所需的配置相匹配。此配置不仅适用于实例大小和类型，还包括元数据、标签、GPU 分配、网络标签和服务帐户属性等实例属性。

作为主映像创建过程的一部分，MCS 使用您的主 VM 实例来创建 Google Cloud *实例模板*。然后，该实例模板用于创建构成计算机目录的克隆 VDA 实例。克隆实例继承了创建实例模板所用的主 VM 实例的属性（VPC、子网和永久性磁盘属性除外）。

根据您的具体要求配置主 VM 实例的属性后，启动该实例，然后为该实例准备永久性磁盘。

我们建议您手动创建磁盘快照或磁盘映像。这样做可以让您使用有意义的命名约定来跟踪版本，为您提供更多选项来管理主映像的早期版本，并节省计算机目录创建时间。如果您不创建自己的快照，MCS 会为您创建一个临时快照（该快照在预配过程结束时删除）。手动创建操作系统磁盘或映像的多区域快照还可以让您在不同的 GCP 区域中使用相同的主映像来创建计算机目录。

创建计算机目录

您可以通过两种方式创建计算机目录：

- 使用 Web Studio 创建计算机目录
- 使用 PowerShell 创建计算机目录

使用 WEB STUDIO 创建计算机目录

> **注意：**

> 在创建计算机目录之前，请先创建您的资源。配置计算机目录时，请使用 Google Cloud 建立的命名约定。有关详细信息，请参阅 存储桶和对象命名准则。

> 请遵循 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-create.html) 中的指导。以下描述是 Google Cloud 目录特有的。

1. 登录 Web Studio 并在左侧窗格中选择 **计算机目录**。
2. 在操作栏中选择 **Create Machine Catalog**。
3. 在 **操作系统** 页面上，选择 **多会话操作系统**，然后选择 **下一步**。
   - Citrix Virtual Apps and Desktops™ 也支持单会话操作系统。
4. 在**计算机管理**页面上，选择**已进行电源管理的计算机**和 **Citrix Machine Creation Services™** 选项，然后选择**下一步**。如果有多个资源，请从菜单中选择一个。
5. 在**映像**页面上，根据需要完成这些步骤，然后单击**下一步**。
   a. 选择主映像。您可以选择以下映像类型：
      - 虚拟机（其区域与所选托管单元相同）。
      - 快照（支持多区域快照）。
      - 操作系统映像（支持多区域公共和非公共映像）。 如果您想使用独占租户功能，请务必选择节点组属性配置正确的映像。请参阅 (#enable-zone-selection)。
   b. 要从计算机配置文件继承计算机属性，请选择 **使用计算机配置文件**，然后从 **虚拟机** 选项卡或 **实例模板** 选项卡中选择一个配置文件。

      > **注意：**
      >
      > - 目前，此目录中的 VM 继承所选计算机配置文件中的存储、计算机类型和磁盘加密设置。
      > - 如果选择实例模板作为计算机配置文件，则默认情况下会选择所有区域。您可以根据需要选择区域。

   c. 选择目录的最低功能级别。
6. 在 **存储类型** 页面上，选择用于包含此计算机目录操作系统的存储类型。以下每个存储选项都具有独特的定价和性能特征。（身份磁盘始终使用区域标准永久性磁盘创建。）

- 标准永久性磁盘
- 均衡永久性磁盘
- SSD 永久性磁盘

有关 Google Cloud 存储选项的详细信息，请参阅 `<https://cloud.google.com/compute/docs/disks/>`。

7. 在 **虚拟机** 页面上，指定要创建的 VM 数量，查看 VM 的详细规范，然后选择 **下一步**。如果将单租户节点组用于计算机目录，请务必**仅**选择预留单租户节点可用的区域。请参阅启用区域选择。
8. 在**磁盘设置**页面上，您可以配置以下设置：

   - 选择是否启用回写式缓存。启用回写式缓存后，您可以执行以下操作：
     - 配置用于缓存临时数据的磁盘和 RAM 大小。有关详细信息，请参阅配置临时数据缓存。
     - 选择回写式缓存磁盘的存储类型。以下存储选项可用于回写式缓存磁盘：
       - 标准永久性磁盘
       - 均衡永久性磁盘
       - SSD 永久性磁盘

       有关 Google Cloud 存储选项的详细信息，请参阅存储选项。
     - 选择回写缓存磁盘的类型。
       - **使用非持久性回写缓存磁盘**。如果选择此选项，回写缓存磁盘不会为预配的 VM 持久保留。磁盘在电源循环期间会被删除，并且重定向到磁盘的任何数据都将丢失。
       - **使用持久性回写缓存磁盘**。如果选择此选项，回写缓存磁盘会为预配的 VM 持久保留。启用此选项会增加您的存储成本。
   - 启用 MCS 存储优化 (MCS I/O) 后，您可以执行以下任一操作：
     - 选择是否在电源循环期间保留 VDA 的系统磁盘。有关详细信息，请参阅启用 MCS 存储优化更新。
     - 更新内存和磁盘缓存大小。
   - 选择是否使用您自己的密钥来保护磁盘内容。要使用此功能，您必须首先创建自己的客户管理加密密钥 (CMEK)。有关详细信息，请参阅使用客户管理加密密钥 (CMEK)。

     > **注意：**

> 它仅在 Studio 界面中可用。

> 创建密钥后，您可以从列表中选择其中一个密钥。创建目录后，您无法更改密钥。Google Cloud 不支持轮换现有永久性磁盘或映像上的密钥。因此，预配目录后，该目录将绑定到特定版本的密钥。如果该密钥被禁用或销毁，则使用该密钥加密的实例和磁盘将变得无法使用，直到该密钥重新启用或恢复。

9. 在 **计算机帐户** 页面上，选择一个 Active Directory 帐户，然后选择 **下一步**。
   - 如果选择**创建新的 Active Directory 帐户**，请选择一个域，然后输入表示在 Active Directory 中创建的预配 VM 计算机帐户的命名方案的字符序列。帐户命名方案可以包含 1-64 个字符，不能包含空格、非 ASCII 字符或特殊字符。
   - 如果选择**使用现有 Active Directory 帐户**，请选择**浏览**以导航到所选计算机的现有 Active Directory 计算机帐户。
10. 在 **域凭据** 页面上，选择 **输入凭据**，键入用户名和密码，选择 **保存**，然后选择 **下一步**。
    - 您键入的凭据必须具有执行 Active Directory 帐户操作的权限。
11. 在**摘要**页面上，确认信息，为目录指定名称，然后选择**完成**。

> **注意：**
>
> 从版本 2402 开始，GCP 目录名称必须符合以下规则：
>
> - 以小写字母开头。
> - 仅包含小写字母 (a-z)、数字和连字符。
> - 以小写字母或数字结尾。 当您尝试重命名不符合这些规则的现有 GCP 目录时，将显示错误消息，指导您根据更新的规则重命名它们。

计算机目录创建可能需要很长时间才能完成。要验证计算机是否已在目标节点组上创建，请转到 Google Cloud 控制台。

导入手动创建的 Google Cloud 机器

*您可以创建到 Google Cloud 的连接，然后创建包含 Google Cloud 计算机的目录。*然后，您可以通过 Citrix Virtual Apps and Desktops™ 手动重启 Google Cloud 计算机。借助此功能，您可以：

- 将手动创建的 Google Cloud 多会话操作系统计算机导入到 Citrix Virtual Apps and Desktops 计算机目录中。
- 从 Citrix Virtual Apps and Desktops 目录中删除手动创建的 Google Cloud 多会话操作系统计算机。
- 使用现有的 Citrix Virtual Apps and Desktops 电源管理功能来电源管理 Google Cloud Windows 多会话操作系统计算机。例如，为这些计算机设置重启计划。

此功能不需要更改现有的 Citrix Virtual Apps and Desktops 预配工作流，也不需要删除任何现有功能。我们建议您使用 MCS 在 Web Studio 中预配计算机，而不是导入手动创建的 Google Cloud 计算机。

共享虚拟私有云

共享虚拟私有云 (VPC) 包含一个主机项目（从中提供共享子网）以及一个或多个使用该资源的服务项目。共享 VPC 是大型安装的理想选择，因为它们提供对共享企业 Google 云资源的集中控制、使用和管理。有关详细信息，请参阅 Google 文档站点。

借助此功能，Machine Creation Services (MCS) 支持预配和管理部署到共享 VPC 的计算机目录。此支持在功能上等同于当前在本地 VPC 中提供的支持，但在两个方面有所不同：

1. 您必须向用于创建主机连接的服务帐户授予额外权限。此过程允许 MCS 访问和使用共享 VPC 资源。
2. 您必须创建两条防火墙规则，一条用于入站，一条用于出站。这些防火墙规则在映像主控过程中使用。

所需的新权限

创建主机连接时需要具有特定权限的 Google Cloud 服务帐户。必须将这些额外权限授予用于创建基于共享 VPC 的主机连接的任何服务帐户。

> **提示：**
>
> 这些附加权限对于 Citrix Virtual Apps and Desktops 来说并非新功能。它们用于促进本地 VPC 的实施。通过共享 VPC，这些附加权限允许访问其他共享 VPC 资源。
>
> 最多需要向与主机连接关联的服务帐户授予四个额外权限，以支持共享 VPC：

1. **compute.firewalls.list** - 此权限是强制性的。它允许 MCS 检索共享 VPC 上存在的防火墙规则列表。

2. **compute.networks.list** - 此权限是强制性的。它允许 MCS 识别服务帐户可用的共享 VPC 网络。
3. **compute.subnetworks.list** – 此权限是可选的，具体取决于您如何使用 VPC。它允许 MCS 识别可见共享 VPC 中的子网。在使用本地 VPC 时已需要此权限，但它也必须分配给共享 VPC 主机项目。
4. **compute.subnetworks.use** - 此权限是可选的，具体取决于您如何使用 VPC。在预配的计算机目录中使用子网资源时，此权限是必需的。在使用本地 VPC 时已需要此权限，但它也必须分配给共享 VPC 主机项目。

使用这些权限时，请考虑根据用于创建计算机目录的权限类型，有不同的方法：

- 项目级权限：
  - 允许访问主机项目中的所有共享 VPC。
  - 要求将权限 #3 和 #4 分配给服务帐户。
- 子网级权限：
  - 允许访问共享 VPC 中的特定子网。
  - 权限 #3 和 #4 是子网级别分配固有的，因此无需直接分配给服务帐户。

选择符合您的组织需求和安全标准的方法。

> **提示：**
>
> 有关项目级和子网级权限之间差异的更多信息，请参阅 Google Cloud 文档。

防火墙规则

在准备计算机目录期间，会准备一个计算机映像，用作目录的主映像系统磁盘。在此过程中，磁盘会临时附加到虚拟机。此虚拟机必须在隔离环境中运行，以防止所有入站和出站网络流量。这通过一对拒绝所有流量的防火墙规则实现；一个用于入站流量，一个用于出站流量。使用 Google Cloud 本地 VPC 时，MCS 会在本地网络中创建此防火墙，并将其应用于用于主映像创建的计算机。主映像创建完成后，防火墙规则将从映像中删除。

我们建议将使用共享 VPC 所需的新权限数量保持在最低限度。共享 VPC 是更高级别的企业资源，通常具有更严格的安全协议。因此，请在主机项目中的共享 VPC 资源上创建一对防火墙规则，一个用于入站，一个用于出站。为它们分配最高优先级。使用以下值将新的目标标记应用于每个规则：

`citrix-provisioning-quarantine-firewall`

当 MCS 创建或更新计算机目录时，它会搜索包含此目标标记的防火墙规则。然后，它会检查规则的正确性，并将其应用于用于为目录准备主映像的计算机。如果未找到防火墙规则，或者找到了规则但规则或其优先级不正确，则会出现类似以下内容的消息：

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."
```

配置共享 VPC

在 Web Studio 中将共享 VPC 添加为主机连接之前，请完成以下步骤以添加您打算预配到的项目中的服务帐户：

1. 创建 IAM 角色。
2. 将用于创建 CVAD 主机连接的服务帐户添加到共享 VPC 主机项目 IAM 角色。
3. 将您打算预配到的项目中的 Cloud Build 服务帐户添加到共享 VPC 主机项目 IAM 角色。
4. 创建防火墙规则。

创建 IAM 角色
确定角色的访问级别 — *项目级访问*或使用*子网级访问*的更受限模型。

IAM 角色的项目级别访问。对于项目级别的 IAM 角色，请包含以下权限：

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

要创建项目级别的 IAM 角色：

1. 在 Google Cloud 控制台中，导航到 **IAM 和管理 > 角色**。
2. 在 **角色** 页面上，选择 **创建角色**。
3. 在 **创建角色** 页面上，指定角色名称。选择 **添加权限**。
    a. 在“**添加权限**”页面上，单独向角色添加权限。要添加权限，请在“**筛选表**”字段中键入权限名称。选择权限，然后选择“**添加**”。
    b. 选择 **创建**。

子网级别 IAM 角色。此角色在选择“**创建角色**”后省略了权限 `compute.subnetworks.list` 和 `compute.subnetworks.use` 的添加。对于此 IAM 访问级别，必须将权限 `compute.firewalls.list` 和 `compute.networks.list` 应用于新角色。

要创建子网级别的 IAM 角色：

1. 在 Google Cloud 控制台中，导航到 **VPC 网络** > **共享 VPC**。“**共享 VPC**”页面随即显示，其中显示了宿主项目包含的共享 VPC 网络的子网。
2. 在 **共享 VPC** 页面上，选择您要访问的子网。
3. 在右上角，选择 **添加成员** 以添加服务帐户。
4. 在 **添加成员** 页面上，完成以下步骤：
    a. 在 **新成员** 字段中，键入您的服务帐户名称，然后从菜单中选择您的服务帐户。
    b. 选择 **选择角色** 字段，然后选择 **计算网络用户**。
    c. 选择 **保存**。
5. 在 Google Cloud 控制台中，导航到 **IAM 和管理** > **角色**。
6. 在 **角色** 页面上，选择 **创建角色**。
7. 在 **创建角色** 页面上，指定角色名称。选择 **添加权限**。
    a. 在 **添加权限** 页面上，单独为角色添加权限。要添加权限，请在 **筛选表** 字段中键入权限名称。选择该权限，然后选择 **添加**。
    b. 选择 **创建**。

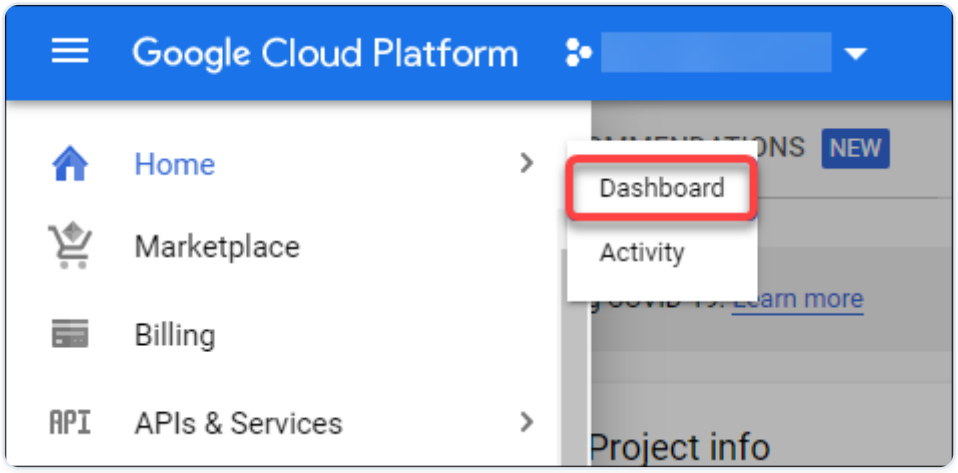
将服务帐户添加到主机项目 IAM 角色
创建 IAM 角色后，执行以下步骤为主机项目添加服务帐户：

1. 在 Google Cloud 控制台中，导航到主机项目，然后导航到 **IAM 和管理 > IAM**。
2. 在 **IAM** 页面上，选择 **添加** 以添加服务帐户。
3. 在“**添加成员**”页面上：
    a. 在 **新成员** 字段中，键入您的服务帐户名称，然后从菜单中选择您的服务帐户。
    b. 选择一个角色字段，键入您创建的 IAM 角色，然后从菜单中选择该角色。
    c. 选择 **保存**。

服务帐户现已为主机项目配置。
将云构建服务帐户添加到共享 VPC

每个 Google Cloud 订阅都有一个服务帐户，其名称是项目 ID 号，后跟 `cloudbuild.gserviceaccount`。例如：`705794712345@cloudbuild.gserviceaccount`。

您可以通过在 Google Cloud 控制台中选择 **Home** 和 **Dashboard** 来确定您项目的项目 ID 号：



在屏幕的 **Project Info** 区域下方找到 **Project Number**。

执行以下步骤将 Cloud Build 服务帐户添加到共享 VPC：

1. 在 Google Cloud 控制台中，导航到主机项目，然后导航到“**IAM 和管理**”>“**IAM**”。
2. 在“**权限**”页面上，选择“**添加**”以添加帐户。
3. 在 **添加成员** 页面上，完成以下步骤：
   a. 在“**新成员**”字段中，键入 Cloud Build 服务帐户的名称，然后从菜单中选择您的服务帐户。
   b. 选择“**选择角色**”字段，键入 `Computer Network User`，然后从菜单中选择该角色。
   c. 选择 **保存**。

创建防火墙规则

作为主映像创建过程的一部分，MCS 会复制选定的计算机映像，并使用它来准备目录的主映像系统磁盘。在主映像创建过程中，MCS 会将磁盘附加到临时虚拟机，然后该虚拟机运行准备脚本。此虚拟机必须在禁止所有入站和出站网络流量的隔离环境中运行。为了创建隔离环境，MCS 需要两条*拒绝所有*防火墙规则（一条入站规则和一条出站规则）。因此，请在*主机项目*中创建两条防火墙规则，如下所示：

1. 在 Google Cloud 控制台中，导航到主机项目，然后转到 **VPC network > Firewall**。
2. 在 **Firewall** 页面上，选择 **CREATE FIREWALL RULE**。
3. 在 **Create a firewall rule** 页面上，完成以下操作：
   - **名称**。键入规则的名称。
   - **网络**。选择入站防火墙规则适用的共享 VPC 网络。

- **优先级**。值越小，规则的优先级越高。我们建议使用较小的值（例如，10）。
- **流量方向**。选择 **Ingress**。
- **匹配操作**。选择 **Deny**。
- **目标**。使用默认值 **Specified target tags**。
- **目标标记**。键入 `citrix-provisioning-quarantine-firewall`。
- **源筛选器**。使用默认值 **IP ranges**。
- **源 IP 范围**。键入与所有流量匹配的范围。键入 `0.0.0.0/0`。
- **协议和端口**。选择**拒绝所有**。

4. 选择**创建**以创建规则。
5. 重复步骤 1–4 以创建另一条规则。对于 **Direction of traffic**，选择 **Egress**。

添加连接
添加与 Google 云环境的连接。请参阅 添加连接。

启用区域选择

Citrix Virtual Apps and Desktops 支持区域选择。通过区域选择，您可以指定要创建 VM 的区域。通过区域选择，管理员可以将独占租户节点放置在他们选择的区域中。要配置独占租用，您必须在 Google Cloud 上完成以下操作：

- 预留 Google Cloud 单租户节点
- 创建 VDA 主映像

预留 GOOGLE CLOUD 独占租户节点

要预留单租户节点，请参阅 Google Cloud 文档。

> **重要提示：**

> 节点模板用于指示在节点组中预留的系统的性能特征。这些特征包括 vGPU 的数量、分配给节点的内存量以及在节点上创建的计算机所使用的计算机类型。有关详细信息，请参阅 Google Cloud 文档。

创建 VDA 主映像

要在单租户节点上成功部署计算机，您需要在创建主 VM 映像时采取额外的步骤。Google Cloud 上的计算机实例具有一个名为 *节点亲和性标签* 的属性。用作部署到单租户节点的目录的主映像的实例需要一个与 **目标节点组** 名称匹配的 *节点亲和性标签*。为此，请记住以下几点：

- 对于新实例，在创建实例时，在 Google Cloud 控制台中设置标签。有关详细信息，请参阅 预配单租户 VM。
- 对于现有实例，使用 **gcloud** 命令行设置标签。有关详细信息，请参阅 配置节点亲和性标签。

> **注意：**
>
> 如果您打算将单租户与共享 VPC 结合使用，请参阅 共享虚拟私有云。

创建计算机目录
设置节点亲和性标签后，配置计算机目录。

客户管理的加密密钥 (CMEK)

您可以将客户管理的加密密钥 (CMEK) 用于 MCS 目录。使用此功能时，您需要将 Google Cloud Key Management Service `CryptoKey Encrypter/Decrypter` 角色分配给 Compute Engine 服务代理。Citrix Virtual Apps and Desktops 帐户必须在存储密钥的项目中具有正确的权限。有关详细信息，请参阅 通过使用 Cloud KMS 密钥帮助保护资源。

您的 Compute Engine 服务代理采用以下形式：`service-<Project _Number>@compute-system.iam.gserviceaccount.com`。此形式不同于默认的 Compute Engine 服务帐户。

> **注意：**
>
> 此 Compute Engine 服务帐户可能不会显示在 Google Console **IAM 权限**显示中。在这种情况下，请使用 `gcloud` 命令，如通过使用 Cloud KMS 密钥帮助保护资源 中所述。

向 CITRIX VIRTUAL APPS AND DESKTOPS 帐户分配权限

Google Cloud KMS 权限可以通过多种方式配置。您可以提供*项目级* KMS 权限或*资源级* KMS 权限。有关详细信息，请参阅权限和角色。
项目级权限
一种选择是为 Citrix Virtual Apps and Desktops 帐户提供项目级权限以浏览 Cloud KMS 资源。为此，请创建一个自定义角色，并添加以下权限：

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`

- `cloudkms.cryptokeys.get`

将此自定义角色分配给您的 Citrix Virtual Apps and Desktops。这允许您在清单中浏览相关项目中的区域密钥。

资源级权限

对于另一个选项，即资源级权限，在 Google Cloud 控制台中，浏览到您用于 MCS 预配的 `cryptoKey`。将 Citrix Virtual Apps and Desktops 帐户添加到您用于目录预配的密钥环或密钥中。

> **提示：**
>
> 使用此选项，您无法在清单中浏览项目的区域密钥，因为 Citrix Virtual Apps and Desktops 帐户对 Cloud KMS 资源没有项目级列表权限。但是，您仍然可以通过在 `ProvScheme` 自定义属性中指定正确的 `cryptoKeyId` 来使用 CMEK 预配目录，如下所述。

使用自定义属性通过 CMEK 进行预配

通过 PowerShell 创建预配方案 时，请在 `ProvScheme CustomProperties` 中指定 `CryptoKeyId` 属性。例如：

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

`cryptoKeyId` 必须按以下格式指定：

`projectId:location:keyRingName:cryptoKeyName`

例如，如果您想在区域 `us-east1` 的密钥环 `my-example-key-ring` 中使用密钥 `my-example-key`，并且项目 ID 为 `my-example-project-1`，则您的 `ProvScheme` 自定义设置将类似于：

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />
```

```
</CustomProperties>'
```

与此预配方案相关的所有 MCS 预配磁盘和映像都使用此客户管理的加密密钥。

提示：

如果您使用全局密钥，客户属性位置必须显示 `global`，而不是 **region** 名称（在上面的示例中为 **us-east1**）。例如：`<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`。

轮换客户管理的密钥

Google Cloud 不支持轮换现有持久性磁盘或映像上的密钥。一旦预配了计算机，它就与创建时使用的密钥版本绑定。但是，可以创建新版本的密钥，并且该新密钥将用于新预配的计算机或在目录使用新主映像更新时创建的资源。

关于密钥环的重要注意事项

密钥环无法重命名或删除。此外，配置它们时可能会产生不可预见的费用。删除或移除密钥环时，Google Cloud 会显示错误消息：

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
nor key rings are billed for, just the active key versions within the
keys.
```

提示：

有关详细信息，请参阅从控制台编辑或删除密钥环。

统一存储桶级访问兼容性

Citrix Virtual Apps and Desktops 与 Google Cloud 上的统一存储桶级访问控制策略兼容。此功能增强了 IAM 策略的使用，该策略向服务帐户授予权限以允许操作资源，包括存储桶。通过统一存储桶级访问控制，Citrix Virtual Apps and Desktops 允许您使用访问控制列表 (ACL) 来控制对存储桶或其中存储的对象的访问。有关 Google Cloud 统一存储桶级访问的概述信息，请参阅 统一存储桶级访问。有关配置信息，请参阅 要求统一存储桶级访问。

使用 PowerShell 创建计算机目录

本节详细介绍了如何使用 PowerShell 创建目录：

- 创建具有持久性回写缓存磁盘的目录
- 使用 MCSIO 提高启动性能
- 使用计算机配置文件创建计算机目录
- 创建以计算机配置文件作为实例模板的计算机目录
- 使用 PowerShell 创建包含受保护 VM 的目录
- 在单租户节点上创建 Windows 11 VM

创建具有持久性回写缓存磁盘的目录

要配置具有持久回写缓存磁盘的目录，请使用 PowerShell 参数 `New-ProvScheme` `CustomProperties`。

> **提示：**
>
> 此处仅将 PowerShell 参数用于基于云的托管连接。如果您想为本地解决方案（例如 XenServer®）使用持久回写缓存磁盘预配计算机，则不需要 PowerShell，因为磁盘会自动持久化。
>
> 此参数支持一个额外的属性 `PersistWBC`，用于确定回写缓存磁盘如何为 MCS 预配的计算机持久化。`PersistWBC` 属性仅在指定 `UseWriteBackCache` 参数且设置 `WriteBackCacheDiskSize` 参数以指示已创建磁盘时使用。
>
> **注意：**

此行为适用于 Azure 和 GCP，其中默认的 MCSIO 回写缓存磁盘在电源循环时会被删除并重新创建。您可以选择持久保存磁盘，以避免删除和重新创建 MCSIO 回写缓存磁盘。

当 Citrix Virtual Apps and Desktops 管理员从管理界面关闭计算机时，将 `PersistWBC` 属性设置为 `true` 不会删除回写缓存磁盘。

当 Citrix Virtual Apps and Desktops 管理员从管理界面关闭计算机时，将 `PersistWBC` 属性设置为 `false` 会删除回写缓存磁盘。

注意：

如果省略 `PersistWBC` 属性，则该属性默认为 `false`，并且当计算机从管理界面关闭时，回写缓存将被删除。

例如，使用 CustomProperties 参数将 `PersistWBC` 设置为 `true`：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

注意：

`PersistWBC` 属性只能使用 `New-ProvScheme` PowerShell cmdlet 进行设置。在创建后尝试更改预配方案的 `CustomProperties` 对计算机目录以及计算机关闭时回写缓存磁盘的持久性没有影响。

例如，将 `New-ProvScheme` 设置为使用回写缓存，同时将 `PersistWBC` 属性设置为 `true`：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

使用 MCSIO 提高启动性能

启用 MCSIO 后，可以提高 Azure 和 GCP 托管磁盘的启动性能。使用 PowerShell `PersistOSDisk` 自定义属性在 `New-ProvScheme` 命令中配置此功能。与 `New-ProvScheme` 相关的选项包括：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

要启用此功能，请将 `PersistOSDisk` 自定义属性设置为 `true`。例如：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
```
```

```
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

使用机器配置文件创建计算机目录

使用 Machine Creation Services (MCS) 创建目录以预配计算机时，可以使用计算机配置文件从虚拟机捕获硬件属性，并将其应用于目录中新预配的 VM。如果未使用 `MachineProfile` 参数，则硬件属性将从主映像 VM 或快照中捕获。 您明确定义的某些属性（例如 `StorageType`、`CatalogZones` 和 `CryptoKeyIs`）将从计算机配置文件中忽略。

- 要使用计算机配置文件创建目录，请使用 `New-ProvScheme` 命令。例如，`New-ProvScheme –MachineProfile "path to VM"`。如果您未指定 `MachineProfile` 参数，则硬件属性将从主映像 VM 中捕获。
- 要使用新的计算机配置文件更新目录，请使用 `Set-ProvScheme` 命令。例如，`Set-ProvScheme –MachineProfile "path to new VM"`。此命令不会更改目录中现有 VM 的计算机配置文件。只有添加到目录中的新创建的 VM 才具有新的计算机配置文件。
- 您也可以更新主映像，但是，当您更新主映像时，硬件属性不会更新。如果要更新硬件属性，必须使用 `Set-ProvScheme` 命令更新计算机配置文件。这些更改仅适用于目录中的新计算机。要更新现有计算机的硬件属性，可以使用 `Set-ProvVMUpdateTimeWindow` 命令以及 `-StartsNow` 和 `-DurationInMinutes -1` 参数。

> **注意：**
>
> - `StartsNow` 表示计划的开始时间是当前时间。

- 带有负数（例如，–1）的 `DurationInMinutes` 表示计划时间窗口没有上限。

使用实例模板作为计算机配置文件创建计算机目录

您可以选择 GCP 实例模板作为计算机配置文件的输入。实例模板是 GCP 中的轻量级资源，因此非常经济高效。

使用实例模板作为计算机配置文件创建新的计算机目录

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 使用以下命令在 GCP 项目中查找实例模板：

```
cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
```

4. 使用 NewProvScheme 命令创建以实例模板作为计算机配置文件的新的计算机目录：

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -HostingUnitName
<HostingUnitName> -IdentityPoolName <identity pool name> -MasterImageVM

XDHyp:\HostingUnits\<HostingUnitName> \Base.vm\Base.snapshot
-MachineProfile XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\mytemplate.tem
plate
```

   有关 New-ProvScheme 命令的更多信息，请参阅 https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/。

5. 使用 PowerShell 命令完成计算机目录的创建。有关如何使用远程 PowerShell SDK 创建目录的信息，请参阅 https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/。

将现有计算机目录的计算机配置文件更改为实例模板

将现有计算机目录的计算机配置文件更改为实例模板的详细步骤如下：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行以下命令：

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -MachineProfile
XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\<TemplateName>
.template
```

有关 Set-ProvScheme 命令的信息，请参阅 https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/。

使用 PowerShell 创建包含受保护 VM 的目录

您可以创建具有受保护虚拟机属性的 MCS 计算机目录。受保护虚拟机通过一组安全控制进行强化，这些控制使用高级平台安全功能（如安全启动、虚拟可信平台模块、UEFI 固件和完整性监控）提供可验证的 Compute Engine 实例完整性。

MCS 支持使用计算机配置文件工作流创建目录。如果使用计算机配置文件工作流，则必须启用 VM 实例的受保护虚拟机属性。然后，您可以将此 VM 实例用作计算机配置文件输入。

使用计算机配置文件工作流创建包含受保护 VM 的 MCS 计算机目录。

1. 在 Google Cloud 控制台中启用 VM 实例的受保护 VM 选项。请参阅“快速入门：启用受保护 VM 选项”。
2. 使用 VM 实例通过计算机配置文件工作流创建 MCS 计算机目录。
   a. 打开 PowerShell 窗口。
   b. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
   c. 如果尚未创建身份池，请创建一个。
   d. 运行 `New-ProvScheme` 命令。例如：

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>

-HostingUnitName gcp-hostint-unit

-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm

-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
machine.vm
```

3. 完成计算机目录的创建。

使用新的计算机配置文件更新计算机目录：

1. 运行 `Set-ProvScheme` 命令。例如：

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>

-MasterImageVM XDHyp:\HostingUnits\<hostin-unit>\catalog-vda.vm

-MachineProfile "DHyp:\HostingUnits\<hostin-unit>\catalog-machine.vm
```

要将 `Set-ProvScheme` 中所做的更改应用于现有 VM，请运行 `Set-ProvVMUpdateTimeWindow` 命令。

1. 运行 `Set-ProvVMUpdateTimeWindow` 命令。例如：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. 重新启动 VM。

在单租户节点上创建 Windows 11 VM

您可以在 GCP 中创建 Windows 11 VM。但是，如果您在主映像上安装 Windows 11，则必须在主映像创建过程中启用 vTPM。此外，您还必须在计算机配置文件源（VM 或实例模板）上启用 vTPM。

在单租户节点上创建 Windows 11 VM 的关键步骤如下：

1. 设置 Google Cloud 虚拟化环境。有关信息，请参阅 Google Cloud 环境。
2. 安装 VDA。请参阅 安装 VDA。
3. 创建与 Google Cloud 环境的连接。有关信息，请参阅 连接到 Google Cloud 环境。
4. 创建 Windows 11 自带许可证 (BYOL) 主映像并将映像导入 Google Cloud。请参阅 创建 Windows 11 BYOL 主映像。
5. 创建计算机配置文件源：在单租户节点上预配 VM 并启用源计算机配置文件的 vTPM。请参阅 在单租户节点上预配 VM。
6. 使用已启用 vTPM 的 Windows 11 计算机配置文件源创建 MCS 计算机目录。计算机配置文件源必须具有与单租户节点中描述的相同的实例类型。请参阅 使用 Windows 11 计算机配置文件源创建 MCS 计算机目录。

创建 WINDOWS 11 BYOL 主映像

有两种选项可以创建 Windows 11 BYOL 主映像并将其导入 Google Cloud：

- 使用 Google Cloud Cloud Build 工具

- 在任何其他虚拟机管理程序上创建主映像

使用 Google Cloud Cloud Build 工具

1. 将 Windows 11 ISO、GCP SDK、.NET framework 和 PowerShell 安装程序文件上传到 GCP 存储桶。
2. 在云构建 `.yaml` 文件中提供文件位置作为参数。
3. 从命令行运行以下 Cloud Build 以构建最终的 Windows 11 映像。GCP 使用 GCP 中的 Daisy 工作流在所选项目中引导并创建主映像，然后将主映像导入 GCP。

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

注意：

将所有大写字母文本替换为实际的资源详细信息。

有关完整信息，请参阅创建自定义 Windows BYOL 映像。
在任何其他虚拟机管理程序上创建主映像

1. 使用任何其他虚拟机管理程序创建 Windows 11 主映像。
2. 将主映像以 OVF 格式导出到本地计算机。
3. 使用本地 gcloud CLI 将 OVF 文件上传到 GCP 存储桶。

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
```

4. 从命令行运行以下 Cloud Build 以构建最终的 Windows 11 映像。GCP 使用 GCP 中的 Daisy 工作流在所选项目中引导并创建主映像，然后将主映像导入 GCP。

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

注意：

> 将所有大写字母文本替换为实际的资源详细信息。

在单租户节点上预配 VM

使用单租户节点可使您的 VM 与其他项目中的 VM 物理隔离，或将您的 VM 分组到同一主机硬件上。有关单租户节点的信息，请参阅 GCP 文档 单租户概述。

有关在单租户节点上预配 VM（计算机配置文件源）的信息，请参阅 GCP 文档 在单租户节点上预配 VM。

> **注意：**
>
> - 选择与节点组相同的实例类型和区域。
> - 在“受保护的 VM”部分中启用 vTPM。有关详细信息，请参阅 快速入门：启用受保护的 VM 选项。
> - 禁用源 VM 上的 Bitlocker。

使用 WINDOWS 11 计算机配置文件源创建 MCS 计算机目录

您可以使用 Web Studio 或 PowerShell 命令创建 MCS 计算机目录以创建 Windows 11 VM。

> **注意：**
>
> - 对于主映像，选择 Windows 11 快照或 VM。
> - 对于计算机配置文件源，选择 Windows 11 VM 作为计算机配置文件。计算机配置文件源必须具有与单租户节点中描述的相同的实例类型。

> 有关使用 Web Studio 的信息，请参阅使用 Web Studio 创建计算机目录。

有关 PowerShell 命令的信息，请参阅使用计算机配置文件创建计算机目录

创建目录并启动虚拟机后，您可以在 Google Cloud 控制台上看到在独占租户节点上运行的 Windows 11 虚拟机。

具有继承标签的虚拟机和磁盘

MCS 计算机目录虚拟机和磁盘（身份磁盘、回写缓存磁盘和操作系统磁盘）可以继承计算机配置文件源（GCP 虚拟机实例或实例模板）的标签。您可以使用这些标签来区分不同团队拥有的实例（例如，team:research 和 team:analytics），并进一步将其用于成本核算或预算。有关标签的更多信息，请参阅 GCP 文档 使用标签组织资源。

您可以使用计算机配置文件源创建新目录、更新现有目录以及更新现有虚拟机以继承标签。

此功能适用于持久性和非持久性 MCS 计算机目录。

您可以执行以下操作：

- 创建具有继承标签的目录
- 更新具有继承标签的现有目录
- 更新具有继承标签的现有虚拟机
- 检索虚拟机和启动磁盘标签的信息
- 删除虚拟机

创建具有继承标签的目录

要创建 MCS 计算机目录，其中虚拟机和磁盘从计算机配置文件源继承标签，请执行以下操作：

1. 创建带有标签的计算机配置文件源（虚拟机实例或实例模板）。有关创建带有标签的虚拟机的信息，请参阅 GCP 文档 使用标签创建资源。实例模板是从虚拟机创建的，并采用虚拟机中定义的标签。
2. 使用 Web Studio 或 PowerShell 命令创建 MCS 目录。
3. 如果使用 Web Studio，请在**映像**页面上选择**使用计算机配置文件**，然后选择 VM 或模板。
4. 如果使用 PowerShell 命令，请执行以下操作：

    a. 打开 PowerShell 窗口。

    b. 运行 asnp citrix*。

    c. 创建身份池。身份池是用于存储要创建的 VM 的 Active Directory (AD) 帐户的容器。

    d. 在 Active Directory 中创建所需的 AD 计算机帐户。

    e. 运行 `New-ProvScheme` 命令以创建目录。例如：

    New-ProvScheme，其中模板作为计算机配置文件输入（持久目录）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

New-ProvScheme，其中实例模板作为计算机配置文件输入（非持久目录）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `

-CleanOnBoot
```

New-ProvScheme，其中 VM 实例作为计算机配置文件输入（持久目录）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

```
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

New-ProvScheme，其中 VM 实例作为计算机配置文件输入（非持久目录）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-CleanOnBoot
```

f. 将预配方案注册为代理目录。

g. 将 VM 添加到目录。

使用继承的标签更新现有目录

要更新现有目录以使其具有新的计算机配置文件，请运行 Set-ProvScheme 命令。运行该命令后，添加到目录中的所有新 VM 都将具有新计算机配置文件源的标签。非持久目录将在下次开机时更新。

例如：

将实例模板作为计算机配置文件输入的 Set-ProvScheme：

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

将 VM 实例作为计算机配置文件输入的 Set-ProvScheme：

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

使用继承的标签更新现有 VM

要使用更新的计算机配置文件源更新现有 VM，请运行以下命令：

1. `Set-ProvScheme`
2. `Set-ProvVMUpdateTimeWindow`。例如：

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

3. 重新启动 VM。

检索 VM 和启动磁盘标签的信息

创建 VM 后，您可以使用带 `AdditionalData` 参数的 `Get-Item` 命令获取 VM 和启动磁盘标签的信息。

要检索 VM 标签的信息，请运行以下命令：

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-
name\vm_name.vm).AdditionalData.Tags
```

要检索启动磁盘标签的信息，请运行以下命令：

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm\bootdisk-
name.attacheddisk).AdditionalData.Tags
```

注意：

为了保持各个虚拟机管理程序之间的一致性，我们使用术语“标签”来显示 GCP 标签。

删除 VM

您可以选择从目录中移除 VM，但不会从 GCP 中删除 VM。在这种情况下，仅从 VM 中移除 Citrix 标签。所有其他添加的标签都不会从 VM 中删除。您可以使用 Web Studio 或 PowerShell 命令移除 VM。

使用 Web Studio

1. 选择虚拟机并右键单击。
2. 单击 **删除**。
3. 选择 **从目录中删除虚拟机，但不要删除虚拟机**。

使用 PowerShell 命令

运行 `Remove-ProvVM` 并使用 `ForgetVM` 参数。有关详细信息，请参阅 SDK 文档 Remove-ProvVM。

Google Cloud 应用商店

您可以浏览并选择 Citrix 在 **Google Cloud Marketplace** 上提供的映像来创建计算机目录。目前，MCS 仅支持此功能的计算机配置文件工作流。

要通过 Google Cloud Marketplace 搜索 Citrix VDA VM 产品，请转至 https://console.cloud.google.com/marketplace。

您可以使用 **Google Cloud Marketplace** 上的自定义映像或 Citrix ready® 映像来更新计算机目录的映像。

> **注意：**
>
> 如果计算机配置文件不包含存储类型信息，则该值将从自定义属性中派生。
>
> 支持的 Google Cloud Marketplace 映像包括：

- Windows 2019 单会话
- Windows 2019 多会话
- 乌班图

使用 Citrix 准备好的映像作为创建计算机目录的源的示例：

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \

-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \

-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
win2019-single-vda-v20220819.publicimage \

-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

后续步骤

- 如果这是创建的第一个目录，Web Studio 会引导您创建交付组
- 要查看整个配置过程，请参阅安装和配置
- 要管理目录，请参阅管理计算机目录和管理 Google Cloud Platform 目录

更多信息

- 创建和管理连接与资源
- 连接到 Google 云环境
- 创建计算机目录

创建 HPE Moonshot 计算机目录

创建计算机目录 介绍了用于创建计算机目录的向导。以下信息涵盖了 HPE Moonshot 环境特有的详细信息。

注意：

- 创建与 HPE Moonshot 的连接
- 确保有一个或多个 HPE Moonshot 节点可用，并在这些节点上安装 VDA。
- 有关创建初始 HPE Moonshot 盒式映像的信息，请参阅 OS Deployment on Moonshot User Guide。

您可以使用以下方式创建 HPE Moonshot 计算机目录：

- 网络工作室
- PowerShell 命令

使用 Web Studio 创建计算机目录

在“**计算机目录设置**”向导中：

1. 在“**操作系统**”页面上，选择“**多会话操作系统**”或“**单会话操作系统**”。
2. 在**计算机管理**页面上，选择**已进行电源管理的计算机**和**其他服务或技术**。
3. 在“**虚拟机**”页面上，添加计算机及其 Active Directory 计算机帐户。您可以执行以下任一操作：
   - 单击**添加计算机**以手动添加计算机。此时将显示**选择 VM**窗口。展开您之前创建的 HPE Moonshot 机箱连接，然后选择要添加的节点（VM）。然后添加关联的计算机帐户名称。
   - 单击 **添加 CSV 文件** 以批量添加计算机。有关使用 CSV 文件添加计算机的信息，请参阅 使用 CSV 文件批量将计算机添加到目录。

作用域和**摘要**页面不包含 HPE Moonshot 特定的信息。

使用 PowerShell 命令创建计算机目录

运行 `New-BrokerCatalog` 和 `New-BrokerMachine` PowerShell 命令以创建代理目录并将计算机导入到代理目录。

例如：

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

下一步操作

- 如果这是创建的第一个目录，Web Studio 将引导您创建交付组
- 要查看整个配置过程，请参阅安装和配置
- 要管理目录，请参阅管理计算机目录 和管理 HPE Moonshot 目录

更多信息

- 创建和管理连接与资源

- 连接到 HPE Moonshot
- 创建计算机目录

创建 Microsoft Azure 目录

创建计算机目录 介绍了创建计算机目录的向导。以下信息涵盖了 Microsoft Azure Resource Manager 云环境特有的详细信息。

> **注意：**
>
> 在创建 Microsoft Azure 目录之前，您需要完成与 Microsoft Azure 的连接创建。请参阅连接到 Microsoft Azure。

创建计算机目录

您可以通过两种方式创建计算机目录：

- 在 Web Studio 中使用 Azure Resource Manager 映像创建计算机目录
- 使用 PowerShell 创建计算机目录

在 WEB STUDIO 中使用 AZURE RESOURCE MANAGER 映像创建计算机目录

映像可以是磁盘、快照，也可以是 Azure 计算库中映像定义的映像版本，用于在计算机目录中创建 VM。在创建计算机目录之前，请在 Azure Resource Manager 中创建映像。有关映像的常规信息，请参阅创建计算机目录。

> **注意：**
>
> 已弃用支持使用与主机连接中配置的区域不同的区域中的主映像。请使用 Azure 计算库将主映像复制到所需区域。

> 创建 MCS 计算机目录时，将基于原始 VM 创建一个临时 VM，以执行准备任务，例如启用 DHCP 和许可证重新武装。此临时 VM 称为准备 VM。此准备 VM 的名称遵循 **Preparati-84x9n** 格式，其中最后五个字符是随机生成的，以避免重复。此准备 VM 的命名约定是固定的，无法自定义。准备任务完成后，准备 VM 将被销毁。

要断开准备 VM 的网络连接，将创建一个网络安全组以拒绝所有入站和出站流量。网络安全组每个目录自动创建一次。网络安全组的名称为 `Citrix-Deny-All-a3pgu-GUID`，其中 GUID 是随机生成的。例如，`Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`。

在计算机目录创建向导中：

- “**计算机类型**”和“**计算机管理**”页面不包含 Azure 特定的信息。请遵循 创建计算机目录 一文中的指导。
- 在**映像**页面上，选择要用作在此目录中创建计算机的模板的映像。

  如果选择**主映像**作为要使用的映像类型，请单击**选择映像**并按照以下步骤选择主映像（如果需要）：

  a. （仅适用于在租户内或跨租户配置了共享映像的连接）选择映像所在的订阅。

  b. 选择资源组。

  c. 导航到 Azure VHD、Azure 计算库或 Azure 映像版本。如果需要，为所选映像添加备注。

  选择映像时，请考虑以下事项：

  - 验证映像上是否安装了 Citrix VDA。
  - 如果选择附加到 VM 的 VHD，则必须在继续下一步之前关闭 VM。

> **注意：**
>
> - 与在目录中创建计算机的连接（主机）对应的订阅用绿点表示。其他订阅是与该订阅共享 Azure 计算库的订阅。在这些订阅中，仅显示共享库。有关如何配置共享订阅的信息，请参阅在租户内（跨订阅）共享映像 和跨租户共享映像。
> - 当您选择启用了受信任启动的映像或快照时，必须使用将受信任启动作为**安全类型**的计算机配置文件。然后，您可以通过在计算机配置文件中指定 SecureBoot 和 vTPM 的值来启用或禁用它们。共享映像库不支持受信任启动。有关 Azure 受信任启动的信息，请参阅 `<https://docs.microsoft.com/zh-cn/azure/virtual-machines/trusted-launch>`。
> - 您可以使用 Windows 上的临时 OS 磁盘和受信任启动来创建预配方案。当您选择具有受信任启动的映像时，必须选择启用了 vTPM 的受信任启动计算机配置文件。要使用临时 OS 磁盘创建计算机目录，请参阅如何使用临时 OS 磁盘创建计算机。
> - 当映像复制正在进行时，您可以继续选择该映像作为主映像并完成设置。但是，在复制映像时，目录创建可能需要更长时间才能完成。MCS 要求复制在目录创建后一小时内完成。如果复制超时，目录创建将失败。您可以在 Azure 中验证复制状态。如果复制仍处于挂起状态或复制完成后，请重试。

- 在 Azure 中为计算机目录选择主映像时，MCS 会根据您选择的主映像和计算机配置文件识别操作系统类型。如果 MCS 无法识别，请选择与主映像匹配的操作系统类型。
- 您可以使用 Gen2 映像预配 Gen2 VM 目录，以提高启动时间性能。但是，不支持使用 Gen1 映像创建 Gen2 计算机目录。同样，也不支持使用 Gen2 映像创建 Gen1 计算机目录。此外，任何没有代次信息的旧映像都是 Gen1 映像。

如果选择**准备好的映像**作为要使用的映像类型，请单击**选择映像**并根据需要选择准备好的映像。

为确保成功创建 VM，请验证映像是否已安装 Citrix VDA 2311 或更高版本，并且 VDA 上存在 MCSIO。

选择映像后，**使用计算机配置文件（Microsoft Entra ID 必需）复选框会自动选中。单击选择计算机配置文件**以从资源组列表中浏览到 VM 或 ARM 模板规范。目录中的 VM 可以从选定的计算机配置文件继承配置。

验证 ARM 模板规范，以确保其可用作计算机配置文件来创建计算机目录。有两种方法可以验证 ARM 模板规范：

- 从资源组列表中选择 ARM 模板规范后，单击**下一步**。如果 ARM 模板规范存在错误，则会显示错误消息。
- 运行以下 PowerShell 命令之一：
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

VM 可以从计算机配置文件继承的配置示例包括：

- 加速网络
- 启动诊断
- 主机磁盘缓存（与操作系统和 MCSIO 磁盘相关）
- 计算机大小（除非另有说明）
- 放置在 VM 上的标签

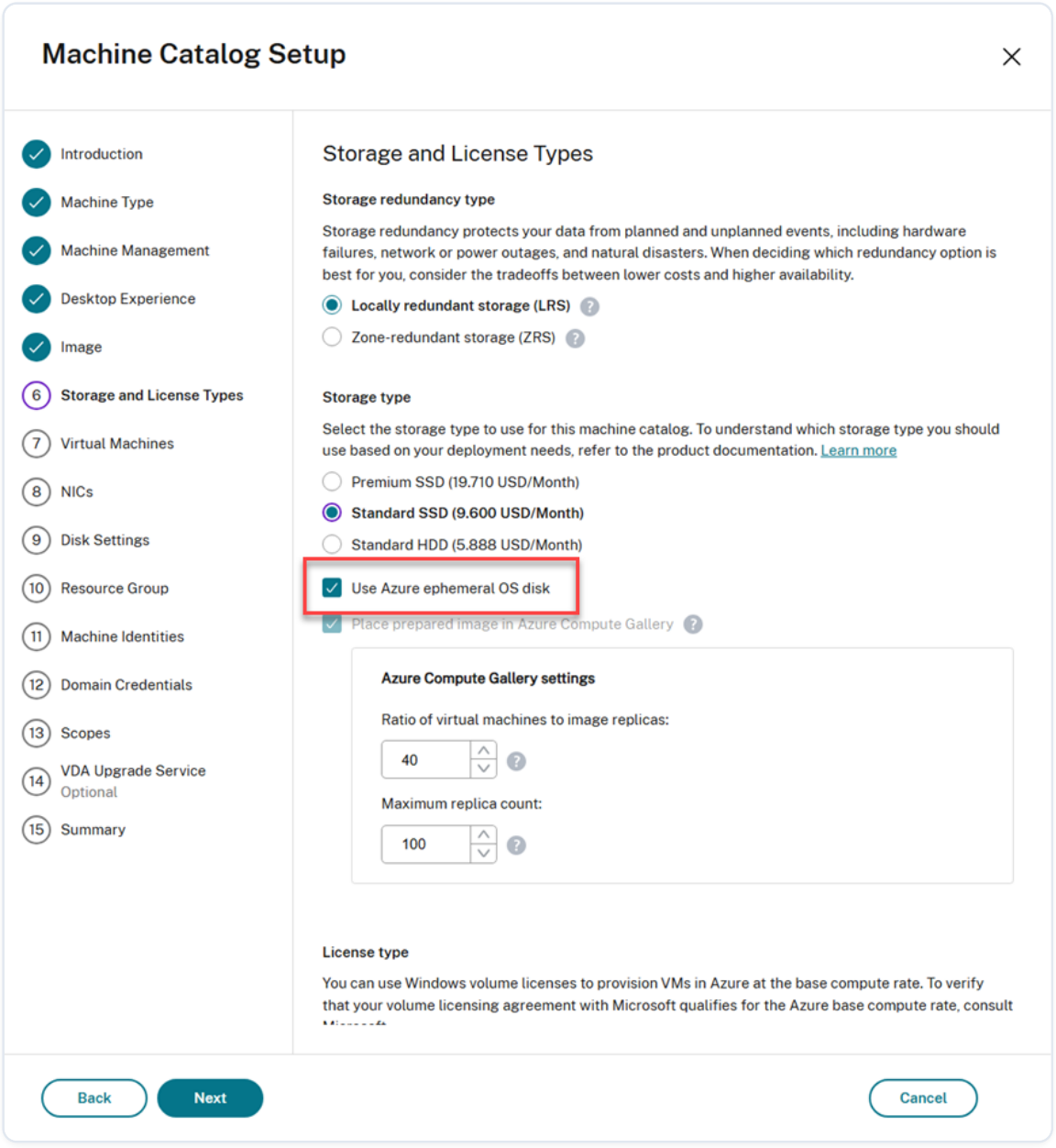
创建目录后，您可以查看映像从计算机配置文件继承的配置。在**计算机目录**节点上，选择目录以在下部窗格中查看其详细信息。然后，单击**模板属性**选项卡以查看计算机配置文件属性。**标签**部分最多显示三个标签。要查看放置在 VM 上的所有标签，请单击**查看全部**。

如果您希望 MCS 在 Azure 专用主机上预配 VM，请启用**使用专用主机组**复选框，然后从列表中选择一个主机组。主机组是表示专用主机集合的资源。专用主机是一种服务，提供托管一个或多个 VM 的物理服务器。您的服务器专用于您的 Azure 订阅，不与其他订阅者共享。当您使用专用主机时，Azure 可确保您的 VM 是在该主机上运行的唯一计算机。此功能适用于必须满足法规或内部安全要求的场景。要了解有关主机组及其使用注意事项的更多信息，请参阅 Azure 专用主机。

> **重要提示：**
>
> - 仅显示启用了 Azure 自动放置功能的主机组。
> - 使用主机组会更改向导后面提供的**虚拟机**页面。该页面上仅显示所选主机组包含的计算机大小。此外，可用区会自动选择，不可供选择。

- **存储和许可证类型**页面仅在使用 Azure Resource Manager 映像时显示。
  - 选择**存储冗余类型**：
    - 本地冗余存储 (LRS)：LRS 允许您从所有可用的存储类型中进行选择。使用 LRS 时，Azure 会将虚拟机 (VM) 专门部署在指定的可用区内。
    - 区域冗余存储 (ZRS)：ZRS 允许在 VM 放置方面具有更大的灵活性，因为 Azure 可以在任何可用区域中启动 VM。这是优于本地冗余存储 (LRS) 的一个关键优势，即使磁盘的原始区域变得不可访问，也能确保 VM 的可用性。但是，ZRS 仅与高级 SSD 和标准 SSD 存储类型兼容。
  - 选择用于计算机目录的**存储类型**：存储类型决定了向导的**虚拟机**页面上提供的计算机大小。
    - **高级 SSD**。提供高性能、低延迟的磁盘存储选项，适用于具有 I/O 密集型工作负载的 VM。
    - **标准 SSD**。提供经济高效的存储选项，适用于需要在较低 IOPS 级别下保持一致性能的工作负载。
    - **标准 HDD**。提供可靠、低成本的磁盘存储选项，适用于运行对延迟不敏感的工作负载的 VM。
  - 选择**使用 Azure 临时 OS 磁盘**。Azure 临时 OS 磁盘提供了一种经济高效的存储选项，它重用 VM 的本地磁盘来托管操作系统磁盘。或者，您可以使用 PowerShell 创建使用临时 OS 磁盘的计算机。有关详细信息，请参阅 Azure 临时磁盘。使用临时 OS 磁盘时请考虑以下事项：

- Azure 临时 OS 磁盘和 MCS I/O 不能同时启用。
- 要更新使用临时 OS 磁盘的计算机，您必须选择一个大小不超过 VM 缓存磁盘或临时磁盘大小的映像。
- 您不能使用向导后面提供的**在电源循环期间保留 VM 和系统磁盘**选项。



注意：

- 无论您选择哪种存储类型，身份磁盘始终使用标准 SSD 创建。
- 如果选择 **ZRS** 作为**存储冗余**，则只能选择 **高级 SSD** 和**标准 SSD**。

有关 Azure 存储类型和存储复制的详细信息，请参阅以下内容：

- `<https://docs.microsoft.com/zh-cn/azure/storage/common/storage-introduction/>`
- `<https://docs.microsoft.com/zh-cn/azure/virtual-machines/premium-storage-performance/>`
- `<https://docs.microsoft.com/zh-cn/azure/storage/common/storage-redundancy/>`

选择是使用现有 Windows 许可证还是 Linux 许可证。

- Windows 许可证：将 Windows 许可证与 Windows 映像（Azure 平台支持映像或自定义映像）结合使用，可让您以更低的成本在 Azure 中运行 Windows VM。许可证有两种类型：
  - **Windows Server 许可证**。允许您使用 Windows Server 或 Azure Windows Server 许可证，从而可以使用 Azure 混合权益。有关详细信息，请参阅 `<https://azure.microsoft.com/zh-cn/pricing/hybrid-benefit/>`。Azure 混合权益将 Azure 中运行 VM 的成本降低到基本计算费率，免除了 Azure 库中额外 Windows Server 许可证的费用。
  - **Windows 客户端许可证**。允许您将 Windows 10 和 Windows 11 许可证带到 Azure，从而无需额外许可证即可在 Azure 中运行 Windows 10 和 Windows 11 VM。有关详细信息，请参阅 客户端访问许可证和管理许可证。

您可以通过运行以下 PowerShell 命令来验证预配的 VM 是否正在使用许可权益：`Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`。

- 对于 Windows Server 许可证类型，请验证许可证类型是否为 **Windows_Server**。更多说明可在 `<https://docs.microsoft.com/zh-cn/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>` 处找到。
- 对于 Windows Client 许可证类型，请验证许可证类型是否为 **Windows_Client**。更多说明可在 `<https://docs.microsoft.com/zh-cn/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>` 处找到。

或者，您可以使用 `Get-Provscheme` PowerShell SDK 进行验证。例如：`Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`。有关此 cmdlet 的更多信息，请参阅 `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>`。

- Linux 许可证：使用自带订阅 (BYOS) Linux 许可证，您无需支付软件费用。BYOS 费用仅包含计算硬件费用。许可证有两种类型：

- **RHEL_BYOS**：要成功使用 RHEL_BYOS 类型，请在您的 Azure 订阅上启用 Red Hat Cloud Access。
- **SLES_BYOS**：SLES 的 BYOS 版本包含 SUSE 的支持。

您可以在 `New-ProvScheme` 和 `Set-ProvScheme` 处将 LicenseType 值设置为 Linux 选项。

在 `New-ProvScheme` 处将 LicenseType 设置为 RHEL_BYOS 的示例：

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog"
-RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="RHEL_BYOS" /></CustomProperties>'
```

在 `Set-ProvScheme` 处将 LicenseType 设置为 SLES_BYOS 的示例：

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
CustomProperties>'
```

注意：

如果 `LicenseType` 值为空，则默认值为 Azure Windows Server 许可证或 Azure Linux 许可证，具体取决于 OsType 值。

> 将 LicenseType 设置为空的示例：

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /></
CustomProperties>'
```

请参阅以下文档以了解许可证类型及其优势：

- `<https://docs.microsoft.com/zh-cn/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>`
- `<https://docs.microsoft.com/zh-cn/azure/virtual-machines/linux/azure-hybrid-benefit-linux>`

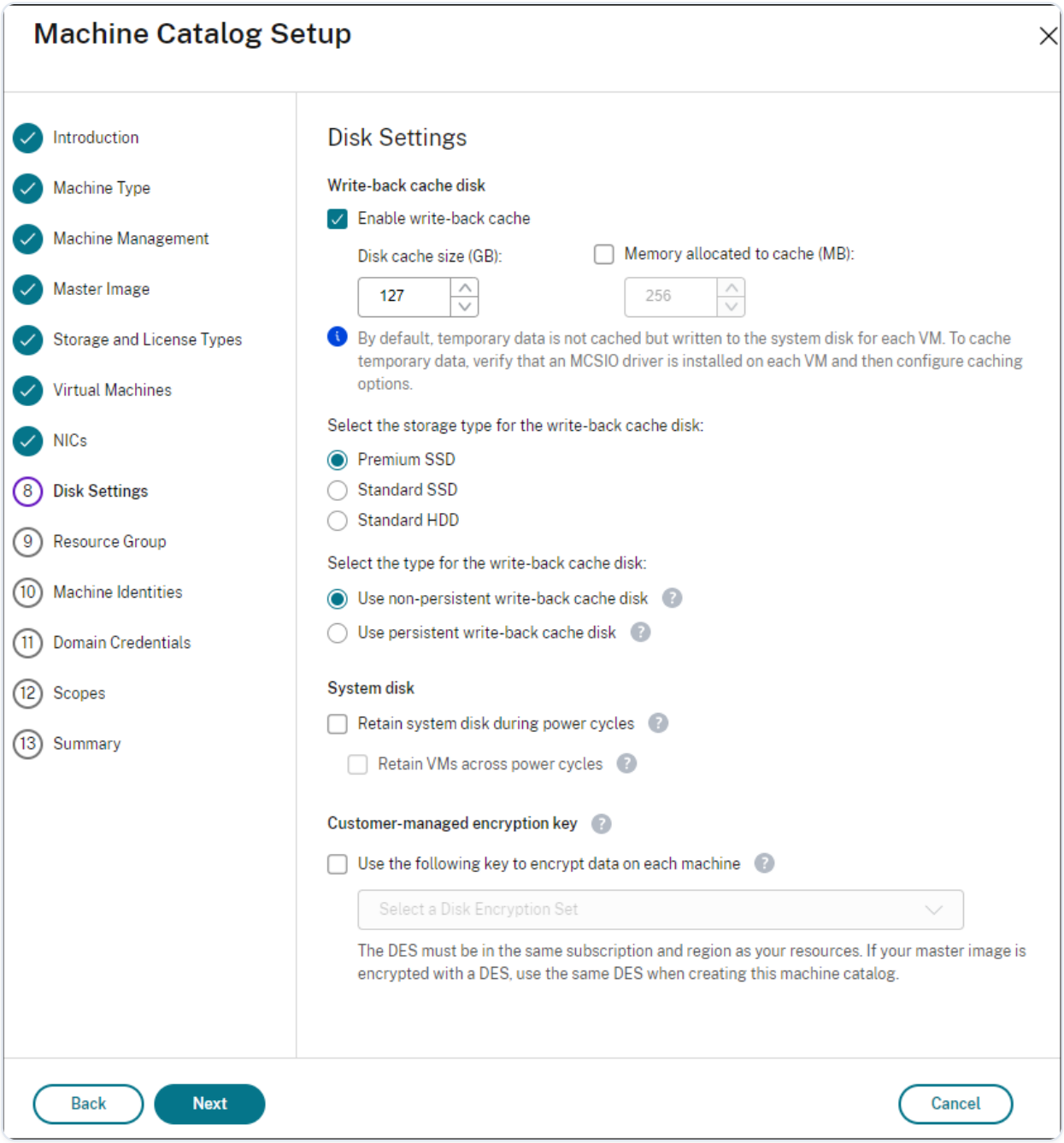
Azure 计算库（以前称为 Azure 共享映像库）是用于管理和共享映像的存储库。它允许您在整个组织中提供映像。我们建议您在创建大型非持久性计算机目录时将映像存储在 SIG 中，因为这样做可以更快地重置 VDA OS 磁盘。选择**将准备好的映像放入 Azure 计算库**后，将显示**Azure 计算库设置**部分，允许您指定更多 Azure 计算库设置：

- **虚拟机与映像副本的比率**。允许您指定 Azure 要保留的虚拟机与映像副本的比率。默认情况下，Azure 为每 40 台非持久性计算机保留一个映像副本。对于持久性计算机，该数字默认为 1,000。
- **最大副本数**。允许您指定 Azure 要保留的映像副本的最大数量。默认值为 100。

> **注意：**
>
> 在 ACG 中创建一个库来存储映像。此库仅供 MCS 用于 VM 创建，不会显示在**选择映像**页面上。

- 在**虚拟机**页面上，指示要创建的 VM 数量和计算机大小。创建目录后，可以通过编辑目录来更改计算机大小。

- **NICs** 页面不包含 Azure 特定的信息。请遵循 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-create.html#nic) 文章中的指导。
- 在**磁盘设置**页面上，选择是否启用回写缓存。启用 MCS 存储优化功能后，您可以在创建目录时配置以下设置。这些设置适用于 Azure 和 GCP 环境。



启用回写缓存后，您可以执行以下操作：

- 配置用于缓存临时数据的磁盘和 RAM 大小。有关详细信息，请参阅配置临时数据缓存。
- 选择回写式缓存磁盘的存储类型。以下存储选项可用于回写式缓存磁盘：
  - 高级 SSD
  - 标准 SSD

- 标准 HDD

> **注意：**
>
> 如果在**存储和许可证类型**页面上选择 **ZRS** 作为**存储冗余**，则回写缓存磁盘存储冗余默认设置为 ZRS

- 选择是否希望回写缓存磁盘对预配的 VM 保持持久。选择**启用回写缓存**以使选项可用。默认情况下，选择**使用非持久性回写缓存磁盘**。
- 选择回写缓存磁盘的类型。
  - **使用非持久性回写缓存磁盘**。如果选择此选项，回写缓存磁盘将在电源循环期间删除。重定向到它的任何数据都将丢失。如果 VM 的临时磁盘有足够的空间，它将用于托管回写缓存磁盘以降低成本。目录创建后，您可以检查预配的计算机是否使用临时磁盘。为此，请单击目录并验证“**模板属性**”选项卡上的信息。如果使用临时磁盘，您将看到“**非持久性回写缓存磁盘**”，其值为“**是（使用 VM 的临时磁盘）**”。否则，您将看到“**非持久性回写缓存磁盘**”，其值为“**否（不使用 VM 的临时磁盘）**”。
  - **使用持久性回写缓存磁盘**。如果选择此选项，回写缓存磁盘将为预配的 VM 保留。启用此选项会增加存储成本。

> **注意：**
>
> 如果满足以下所有条件，目录将自动使用 Azure 临时磁盘作为 WBC 磁盘：
>
> - MCSIO 已启用。
> - WBC 磁盘是非持久性的。
> - VM 大小包含一个足以容纳 WBC 磁盘的临时磁盘。
> - 未为 WBC 磁盘指定驱动器号。 此功能适用于目录创建和编辑，有助于降低存储成本。

- 选择是否在电源循环期间保留 VDA 的 VM 和系统磁盘。

在电源循环期间保留 VM 和系统磁盘。在您选择**启用回写缓存**时可用。默认情况下，VM 和系统磁盘在关机时删除，并在启动时重新创建。如果要减少 VM 重启时间，请选择此选项。请记住，启用此选项还会增加存储成本。

- 选择是否启用**存储成本节省**。如果启用，则在 VM 关闭时将存储磁盘降级为标准 HDD，从而节省存储成本。VM 在重启时会切换回其原始设置。此选项适用于存储磁盘和回写缓存磁盘。或者，您也可以使用 PowerShell。请参阅在 VM 关闭时将存储类型更改为较低层。

> **注意：**
>
> Microsoft 对 VM 关闭期间更改存储类型施加了限制。Microsoft 将来也可能会阻止存储类型更改。有关更多信息，请参阅这篇Microsoft 文章。

- 选择是否加密此目录中计算机上的数据以及要使用的加密密钥。使用客户管理的密钥 (CMK) 进行服务器端加密，可让您在托管磁盘级别管理加密并保护目录中计算机上的数据。默认设置继承自计算机配置文件或主映像，其中配置文件具有优先权：
  - 如果您使用的是带有 *CMK* 的*计算机配置文件*，则会自动选择“**使用以下密钥加密每台计算机上的数据**”选项，并默认为*计算机配置文件*中的密钥。
  - 如果您使用的是带有平台管理密钥 (PMK) 的*计算机配置文件*，并且*主映像*已进行 *CMK* 加密，则会自动选择“**使用以下密钥加密每台计算机上的数据**”选项，并默认为主映像中的密钥。
  - 如果您*未*使用*计算机配置文件*，并且*主映像*已进行 *CMK* 加密，则会自动选择“**使用以下密钥加密每台计算机上的数据**”选项，并默认为*主映像*中的密钥。

  有关详细信息，请参阅Azure 服务器端加密。

- 在“**资源组**”页面上，选择是创建资源组还是使用现有组。
  - 如果您选择创建资源组，请选择“**下一步**”。
  - 如果您选择使用现有资源组，请从**可用预配资源组**列表中选择组。**请记住**：选择足够的组以容纳您在目录中创建的计算机。如果选择的组太少，将显示一条消息。如果您计划稍后向目录中添加更多 VM，则可能需要选择多于最低要求的组。目录创建后，无法向目录中添加更多资源组。

  有关详细信息，请参阅Azure 资源组。

- 在“**计算机身份**”页面上，选择身份类型并配置此目录中计算机的身份。如果将 VM 选为 **Microsoft Entra joined**，则可以将其添加到 Microsoft Entra 安全组。详细步骤如下：

a. 在**身份类型**字段中，选择 **Microsoft Entra joined**。将显示 **Microsoft Entra 安全组（可选）**选项。

b. 单击“**Microsoft Entra 安全组: 创建新组**”。

c. 输入组名称，然后单击**创建**。

d. 按照屏幕上的说明登录到 Azure。 如果组名在 Azure 中不存在，则会显示一个绿色图标。否则，将显示一条错误消息，要求您输入新名称。

e. 输入用于虚拟机的计算机帐户命名方案。

目录创建后，Citrix Virtual Apps and Desktops 会代表您访问 Azure，并为该组创建安全组和动态成员资格规则。根据该规则，具有此目录中指定的命名方案的 VM 将自动添加到安全组中。

将具有不同命名方案的 VM 添加到此目录需要您登录到 Azure。然后，Citrix Virtual Apps and Desktops™ 可以访问 Azure 并根据新的命名方案创建动态成员资格规则。

删除此目录时，从 Azure 删除安全组也需要登录到 Azure。

- **域凭据**和**摘要**页面不包含 Azure 特定的信息。请遵循创建计算机目录文章中的指导。

> **提示：**
>
> 在**摘要**页面上，您可以根据 Azure 的公开标价查看此计算机目录中虚拟机的每月估算成本。如果托管目录的连接在 Azure 中具有 `Microsoft.Consumption/pricesheets/read` 权限，则估算将使用您组织的合同定价进行计算。
>
> 选择成本估算以查看详细信息。为了获得更准确的估算，请根据您的使用情况调整设置，例如每日开机时间、每周工作天数和节省选项。

完成向导。

Azure 临时磁盘符合回写缓存磁盘条件的条件

仅当满足以下所有条件时，才能将 Azure 临时磁盘用作回写缓存磁盘：

- 回写缓存磁盘必须是非持久性的，因为 Azure 临时磁盘不适用于持久数据。
- 所选的 Azure VM 大小必须包含临时磁盘。
- 不需要启用临时 OS 磁盘。
- 接受将回写缓存文件放置在 Azure 临时磁盘上。

- Azure 临时磁盘大小必须大于（回写缓存磁盘大小 + 分页文件保留空间 + 1 GB 缓冲区空间）的总大小。

非持久性回写缓存磁盘方案

下表描述了在创建计算机目录时，临时磁盘用于回写缓存的三种不同场景。

场景	结果
所有使用临时磁盘作为回写缓存的条件均已满足。	WBC 文件 `mcsdif.vhdx` 放置在临时磁盘上。
临时磁盘没有足够的空间用于回写缓存。	已创建 VHD 磁盘 `MCSWCDisk`，并且 WBC 文件 `mcsdif.vhdx` 已放置在此磁盘上。
临时磁盘有足够的空间用于回写缓存，但 `UseTempDiskForWBC` 设置为 **false**。	已创建 VHD 磁盘 `MCSWCDisk`，并且 WBC 文件 `mcsdif.vhdx` 已放置在此磁盘上。

创建 Azure 模板规范

您可以在 Azure 门户中创建 Azure 模板规范，并在 Web Studio 和 PowerShell 命令中使用它来创建或更新 MCS 计算机目录。

为现有 VM 创建 Azure 模板规范：

1. 转到 Azure 门户。选择一个资源组，然后选择 VM 和网络接口。从顶部的 **...** 菜单中，单击 **导出模板**。
2. 如果要为目录预配创建模板规范，请清除 **包含参数** 复选框。在 JSON 文件中验证 `parameters` 和 `variables` 部分是否为：

   ```
   "parameters": {},

   "variables": {}
   ```

3. 单击 **下载** 将模板保存为 JSON 文件。
4. 在 Azure 门户上，选择 **模板规范** 并单击 **导入模板**。
5. 浏览并导入保存在计算机上的计算机配置文件（JSON 格式）。
6. 提供 **名称**、**订阅**、**资源组**、**位置** 和 **版本**。单击 **下一步: 编辑模板**。
7. 执行 **审查+创建** 并创建模板规范。

8. 在 **Template Specs**（模板规范）页面上，验证您刚刚创建的模板规范。单击该模板规范。在左侧面板中，单击 **Versions**（版本）。
9. 您可以单击 **Create new version**（创建新版本）来创建新版本。指定新的版本号，更改为当前模板规范，然后单击 **Review + Create**（审核 + 创建）以创建模板规范的新版本。

您可以使用以下 PowerShell 命令获取有关模板规范和模板版本的信息：

- 要获取有关模板规范的信息，请运行：

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec
```

- 要获取有关模板规范版本的信息，请运行：

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec\bgg1.0.templatespecversion
```

在创建或更新目录时使用模板规范

您可以使用模板规范作为计算机配置文件输入来创建或更新 MCS 计算机目录。为此，您可以使用 Web Studio 或 PowerShell 命令。

- 对于 Web Studio，请参阅 在 Web Studio 中使用 Azure Resource Manager 映像创建计算机目录
- 对于 PowerShell，请参阅 使用 PowerShell 在创建或更新目录时使用模板规范

Azure 服务器端加密

Citrix Virtual Apps and Desktops 通过 Azure Key Vault 支持 Azure 托管磁盘的客户管理加密密钥。通过此支持，您可以使用自己的加密密钥加密计算机目录的托管磁盘，从而管理您的组织和合规性要求。有关详细信息，请参阅 Azure 磁盘存储的服务器端加密。

将此功能用于托管磁盘时：

- 要更改磁盘加密所用的密钥，请在 `DiskEncryptionSet` 中更改当前密钥。与该 `DiskEncryptionSet` 关联的所有资源都将更改为使用新密钥进行加密。
- 当您禁用或删除密钥时，使用该密钥的任何虚拟机（VM）的磁盘都会自动关闭。关闭后，除非重新启用密钥或分配新密钥，否则虚拟机将无法使用。任何使用该密钥的目录都无法开机，并且您无法向其中添加虚拟机。

使用客户管理加密密钥时的重要注意事项

使用此功能时，请考虑以下事项：

- 与客户管理密钥相关的所有资源（Azure Key Vault、磁盘加密集、VM、磁盘和快照）必须位于同一订阅和区域中。
- 使用客户管理密钥加密的磁盘、快照和映像无法移动到其他资源组和订阅。
- 有关每个区域的磁盘加密集限制，请参阅 Microsoft 网站。

> **注意：**
>
> 有关配置 Azure 服务器端加密的信息，请参阅快速入门：使用 Azure 门户创建 Key Vault。

Azure 客户管理的加密密钥

创建计算机目录时，可以选择是否加密目录中预配的计算机上的数据。使用客户管理的加密密钥进行服务器端加密，可让您在托管磁盘级别管理加密并保护目录中计算机上的数据。磁盘加密集 (DES) 表示客户管理的密钥。要使用此功能，您必须首先在 Azure 中创建 DES。DES 采用以下格式：

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

从列表中选择一个 DES。您选择的 DES 必须与您的资源位于相同的订阅和区域中。

请参阅 使用客户管理密钥创建计算机目录。

Azure 主机磁盘加密

您可以创建具有主机加密功能的 MCS 计算机目录。目前，MCS 仅支持此功能的计算机配置文件工作流。您可以使用 VM 或模板规范作为计算机配置文件的输入。

此加密方法不通过 Azure 存储加密数据。托管 VM 的服务器会加密数据，然后加密的数据流经 Azure 存储服务器。因此，此加密方法可实现端到端数据加密。

限制：

主机上的 Azure 磁盘加密为：

- 并非所有 Azure 计算机大小都支持
- 与 Azure 磁盘加密不兼容

要创建具有主机加密功能的计算机目录：

1. 检查订阅是否启用了主机加密功能。为此，请参阅 `<https://learn.microsoft.com/zh-cn/rest/api/resources/features/get?tabs=HTTP/>`。如果未启用，则必须为订阅启用该功能。有关为订阅启用该功能的信息，请参阅 `<https://learn.microsoft.com/zh-cn/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>`。
2. 检查特定的 Azure VM 大小是否支持主机加密。为此，请在 PowerShell 窗口中运行以下命令之一：

   ```
   PS XDHyp:\Connections\<your connection>\east
   us.region\serviceoffering.folder>
   ```

   ```
   PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
   ```

3. 在 Azure 门户中创建虚拟机或模板规范，作为计算机配置文件的输入，并启用主机加密。
   - 如果要创建 VM，请选择支持主机加密的 VM 大小。创建 VM 后，VM 属性 **主机加密** 将启用。
   - 如果要使用模板规范，请在 `securityProfile` 中将参数 `Encryption at Host` 分配为 **true**。
4. 通过选择 VM 或模板规范，使用计算机配置文件工作流创建 MCS 计算机目录。
   - 操作系统磁盘/数据磁盘：通过客户管理的密钥和平台管理的密钥进行加密
   - 临时操作系统磁盘：仅通过平台管理的密钥进行加密
   - 缓存磁盘：通过客户管理的密钥和平台管理的密钥进行加密

   您可以使用 Web Studio 或运行 PowerShell 命令来创建计算机目录。

从计算机配置文件中检索主机加密信息

当您使用 `AdditionalData` 参数运行 PowerShell 命令时，可以从计算机配置文件中检索主机加密信息。如果 `EncryptionAtHost` 参数为 **True**，则表示已为计算机配置文件启用主机加密。

例如：当计算机配置文件输入是 VM 时，运行以下命令：

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.v
m).AdditionalData
```

例如：当计算机配置文件输入是模板规范时，运行以下命令：

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_t
emplatespec.templatespec\EncryptionAtHost.templatespecversion).AdditionalD
ata
```

托管磁盘上的双重加密

您可以创建具有双重加密的计算机目录。使用此功能创建的任何目录都将所有磁盘通过平台和客户管理的密钥进行服务器端加密。您拥有并维护 Azure Key Vault、加密密钥和磁盘加密集 (DES)。

双重加密是平台端加密（默认）和客户管理的加密 (CMEK)。因此，如果您是高度安全敏感的客户，担心与任何加密算法、实施或受损密钥相关的风险，则可以选择此双重加密。持久性操作系统和数据磁盘、快照和映像都通过双重加密进行静态加密。

注意：

- 您可以使用 Web Studio 和 PowerShell 命令创建和更新具有双重加密的计算机目录。有关 PowerShell 命令，请参阅 创建具有双重加密的计算机目录。
- 您可以使用非计算机配置文件工作流或基于计算机配置文件的工作流来创建或更新具有双重加密的计算机目录。
- 如果您使用非计算机配置文件工作流创建计算机目录，则可以重复使用存储的 `DiskEncryptionSetId`。
- 如果您使用计算机配置文件，则可以使用 VM 或模板规范作为计算机配置文件输入。

限制：

- Ultra 磁盘或高级 SSD v2 磁盘不支持双重加密。
- 非托管磁盘不支持双重加密。
- 如果您禁用与目录关联的 DiskEncryptionSet 密钥，则该目录的虚拟机将被禁用。
- 与客户管理的密钥（Azure Key Vault、磁盘加密集、VM、磁盘和快照）相关的所有资源必须位于同一订阅和区域中。
- 每个订阅每个区域最多只能创建 50 个磁盘加密集。

Azure 资源组

Azure 预配资源组提供了一种预配向用户提供应用程序和桌面的 VM 的方法。您可以创建资源组或使用现有资源组在 MCS 计算机目录中预配 VM。您可以在多个计算机目录中使用相同的资源组。有关 Azure 资源组的信息，请参阅 Microsoft 文档。

AZURE 资源组使用情况

每个 Azure 资源组的虚拟机、托管磁盘、快照和映像的数量没有限制。（每个 Azure 资源组 240 个 VM 和 800 个托管磁盘的限制已取消。）

- 使用完全范围的服务主体创建计算机目录时，MCS 只创建一个 Azure 资源组并将其用于该目录。
- 使用窄范围的服务主体创建计算机目录时，必须为该目录提供一个空的、预先创建的 Azure 资源组。

Azure 临时磁盘

Azure 临时磁盘 允许您重新利用缓存磁盘、临时磁盘或 NVMe 磁盘来存储已启用 Azure 的虚拟机的操作系统磁盘。此功能对于需要比标准 HDD 磁盘性能更高的 SSD 磁盘的 Azure 环境非常有用。有关使用 Azure 临时磁盘创建目录的信息，请参阅 使用 Azure 临时磁盘创建目录。

> **注意：**
>
> 持久性目录不支持临时操作系统磁盘。
>
> 临时操作系统磁盘要求您的预配方案使用托管磁盘和共享映像库。

存储临时操作系统临时磁盘

您可以选择将临时操作系统磁盘存储在虚拟机临时磁盘、资源磁盘或 NVMe 磁盘上。此功能使您能够将临时操作系统磁盘与没有缓存或缓存不足的虚拟机配合使用。此类虚拟机具有临时磁盘、资源磁盘或 NVMe 磁盘来存储临时操作系统磁盘，例如 `Ddv4`。

请考虑以下事项：

- 临时磁盘存储在虚拟机缓存磁盘、虚拟机临时（资源）磁盘或 NVMe 磁盘中。缓存磁盘优先于临时磁盘，除非缓存磁盘不足以容纳操作系统磁盘的内容。
- 对于更新，如果新映像大于缓存磁盘但小于临时磁盘，则会导致用 VM 的临时磁盘替换临时 OS 磁盘。

AZURE 临时磁盘和 MACHINE CREATION SERVICES (MCS) 存储优化 (MCS I/O)

Azure 临时 OS 磁盘和 MCS I/O 不能同时启用。

重要注意事项如下：

- 不能同时启用临时 OS 磁盘和 MCS I/O 来创建计算机目录。
- 如果您在 `New-ProvScheme` 或 `Set-ProvScheme` 中将 PowerShell 参数 (`UseWriteBackCache` 和 `UseEphemeralOsDisk`) 设置为 **true**，则它们将失败并显示相应的错误消息。
- 对于已启用这两种功能而创建的现有计算机目录，您仍然可以：
  - 更新计算机目录。
  - 添加或删除 VM。
  - 删除计算机目录。

Azure 计算库

使用 Azure 计算库（以前称为 Azure 共享映像库）作为 Azure 中 MCS 预配计算机的已发布映像存储库。您可以在库中存储已发布的映像，以加快操作系统磁盘的创建和填充，从而缩短非持久性虚拟机的启动和应用程序启动时间。共享映像库包含以下三个元素：

- *库*：映像存储在此处。MCS 为每个计算机目录创建一个库。
- *库映像定义*：此定义包含有关已发布映像的信息（操作系统类型和状态、Azure 区域）。MCS 为为目录创建的每个映像创建一个映像定义。
- *库映像版本*：共享映像库中的每个映像可以有多个版本，每个版本可以在不同区域有多个副本。每个副本都是已发布映像的完整副本。

> **注意：**
>
> 共享映像库功能仅与托管磁盘兼容。它不适用于旧版计算机目录。
>
> 有关详细信息，请参阅 Azure 计算库概述。

有关使用 PowerShell 通过 Azure 计算库映像创建或更新计算机目录的信息，请参阅 使用 Azure 计算库映像创建或更新计算机目录。

Azure 机密 VM

Azure 机密计算 VM 确保您的虚拟桌面在内存中加密并在使用中受到保护。

您可以使用 MCS 创建包含 Azure 机密 VM 的目录。您必须使用计算机配置文件工作流来创建此类目录。您可以将 VM 和 ARM 模板规范都用作计算机配置文件输入。

您还可以使用机密 VM 类型 Azure 主映像和机密 VM 类型 Azure 计算机配置文件来创建准备好的映像，然后使用此准备好的映像来创建 MCS 目录。

机密 VM 的重要注意事项

支持的 VM 大小以及使用机密 VM 创建计算机目录的重要注意事项如下：

- 要查看机密 VM 支持的 VM 大小，请参阅 大小。
- 使用机密 VM 创建计算机目录。
    - 您可以使用 Web Studio 和 PowerShell 命令创建包含 Azure 机密 VM 的计算机目录。
    - 您必须使用基于计算机配置文件的 workflow 来创建包含 Azure 机密 VM 的计算机目录。您可以将 VM 或模板规范用作计算机配置文件输入。
    - 主映像和计算机配置文件输入必须都启用相同的机密安全类型。不同的 Azure 资源使用不同的标签来指示机密 VM 类型。

      对于 Azure 快照、托管磁盘或虚拟机，安全类型为：

        - ConfidentialVM_DiskEncryptedWithCustomerKey。
        - ConfidentialVM_DiskEncryptedWithPlatformKey。
        - ConfidentialVM_VMGuestStateOnlyEncryptedWithPlatformKey

      对于 Azure ARM 模板规范版本，安全类型为：

        - VMGuestStateOnly: 仅加密 VM 访客状态的机密 VM
        - DiskWithVMGuestState: 机密虚拟机，其操作系统磁盘和虚拟机访客状态均使用平台管理的密钥或客户管理的密钥加密。普通和临时操作系统磁盘都可以加密。
    - 您可以使用 AdditionalData 参数获取各种资源类型（例如托管磁盘、快照、Azure 计算库映像、虚拟机和 ARM 模板规范）的机密虚拟机信息。例如：

      ```
      PS C:\Users\username> (get-item XDHyp:
      \HostingUnits\mynetwork\image.folder\username-dev-testing-
      rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
      ```

      附加数据字段包括：
    - DiskSecurityType

- ConfidentialVMDiskEncryptionSetId
- DiskSecurityProfiles

  要获取机器大小的机密计算属性，请运行以下命令：`(Get-Item -path "XDHyp:\Connections\my-connection-name\EastUS.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  附加数据字段为 `ConfidentialComputingType`。
- 您不能将主映像或机器配置文件从机密安全类型更改为非机密安全类型，也不能从非机密安全类型更改为机密安全类型。
- 对于任何不正确的配置，您都会收到相应的错误消息。

准备主映像和机器配置文件

在创建一组机密虚拟机之前，请按照以下步骤为其准备主映像和机器配置文件：

1. 在 Azure 门户中，创建具有特定设置的机密虚拟机，例如：
   - **安全类型**：机密虚拟机
   - **机密操作系统磁盘加密**：已启用。
   - **密钥管理**：使用平台管理密钥的机密磁盘加密 有关创建机密 VM 的更多信息，请参阅这篇 Microsoft 文章。
2. 在创建的 VM 上准备主映像。在创建的 VM 上安装必要的应用程序和 VDA。

   > **注意：**
   >
   > 不支持使用 VHD 创建机密 VM。相反，请为此目的使用 Azure 计算库、托管磁盘或快照。
3. 使用以下任一方式创建计算机配置文件：
   - 如果在步骤 1 中创建的现有 VM 具有所需的计算机属性，则使用该 VM。
   - 如果选择 ARM 模板规范作为计算机配置文件，请根据需要创建模板规范。具体来说，配置满足机密 VM 要求的参数，例如 *SecurityEncryptionType* 和 *diskEncryptionSet*（用于客户管理的密钥）。有关详细信息，请参阅(#create-an-azure-template-spec)。

     > **注意：**

- 确保主映像和计算机配置文件具有相同的安全密钥类型。
- 要创建需要使用客户管理密钥进行机密 OS 磁盘加密的机密 VM，请确保主映像和计算机配置文件中的磁盘加密集 ID 相同。

如果要使用机密 VM 类型准备的映像创建 MCS 目录，则使用机密 VM 类型主映像和机密 VM 类型计算机配置文件创建准备的映像。有关创建准备的映像的信息，请参阅(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/create-prepared-image-machine-catalogs-azure.html#create-an-image-definition-and-initial-image-version)。

使用 WEB STUDIO 或 POWERSHELL 命令创建机密 VM

要创建一组机密 VM，请使用主映像和从所需机密 VM 派生的计算机配置文件创建计算机目录。

要使用 Web Studio 创建目录，请按照 创建计算机目录 中所述的步骤操作。请记住以下注意事项：

- 在**映像**页面上，选择您为创建机密 VM 准备的主映像和计算机配置文件。计算机配置文件选择是强制性的，并且只有与所选主映像具有相同安全加密类型的配置文件才可供选择。
- 在**虚拟机**页面上，只有支持机密 VM 的计算机大小可供选择。
- 在**磁盘设置**页面上，您无法指定磁盘加密集，因为它继承自选定的计算机配置文件。

启动完整性监视

如果您的 VM 启用了安全启动和虚拟可信平台模块 (vTPM)，并且安装了 `GuestAttestation` 扩展，则 Microsoft Defender for Cloud 可以远程验证您的 VM 是否以正常方式启动。此监视称为**启动完整性监视**。有关启动完整性监视的更多信息，请参阅 启动完整性监视概述。

您可以使用计算机配置文件（VM 或模板规范）为 MCS 计算机目录 VM（持久性 VM 和非持久性 VM）启用启动完整性监视。启动完整性监视仅支持受信任启动和机密 VM。

您可以使用 `Set-ProvScheme` 更新现有目录以使用启动完整性，从而指向已启用启动完整性的计算机配置文件。然后，添加到目录的新 VM 将启用完整性监视。

您还可以使用 `Set-ProvVmUpdateTimeWindow`、`Set-ProvVm` 或 `Maintenance Cycles` 更新目录中的现有 VM。您可以将以下 VM 转换为：

- 没有完整性监视的 VM 变为具有完整性监视的 VM
- 具有完整性监视的 VM 变为没有完整性监视的 VM

创建启用完整性监视的计算机目录

所需权限：

确保您具有以下权限：

- `Microsoft.Compute/virtualMachines/extensions/read`
- `Microsoft.Compute/virtualMachines/extensions/write`

执行以下操作以创建启用完整性监视的 MCS 计算机目录：

1. 创建已安装 `GuestAttestation` 扩展的计算机配置文件（VM 或模板规范）。（链接到以下内容）
2. 使用 Web Studio 或 PowerShell 命令，通过计算机配置文件输入创建 MCS 计算机目录。

> **注意：**
>
> 您可以使用带 `AdditionalData` 参数的 `Get-Item` PowerShell 命令检查 VM 或模板规范的 `GuestAttestationExtensionEnabled` 状态。

3. 将 VM 添加到目录。

创建已安装 GuestAttestation 扩展的计算机配置文件
创建 VM 或模板规范作为机器配置文件输入，并启用完整性监视，这意味着已安装 GuestAttestation 扩展。

要创建已启用完整性监视的 VM，请执行以下操作：

1. 登录 Azure 门户。
2. 如果要创建新 VM：
   a. 将“**安全类型**”选择为“**受信任的启动虚拟机**”或“**机密虚拟机**”。
   b. 单击“**配置安全功能**”并选中“**完整性监视**”复选框。

> **注意：**
>
> 对于完整性监视，必须启用安全启动和 vTPM。

3. 在“**概述**”页面上，转到“**安全类型**”部分，验证“**安全类型**”是否为“**受信任的启动**”或“**机密虚拟机**”，并且已启用“**完整性监视**”。
4. 导航到“**扩展 + 应用程序**”页面以验证是否已安装 `GuestAttestation`。

要启用现有 VM 的完整性监视，请参阅启用完整性监视 - Azure 门户。

要创建已安装 `GuestAttestation` 扩展的模板规范：

- 您可以使用模板规范安装 GuestAttestation。请参阅 启用完整性监视 - 模板规范。

> **注意：**
>
> 在此模板规范中，在“**设置**”下，您可以配置用于证明的终结点。如果您不进行配置，则 Azure 会决定要配置哪些终结点。

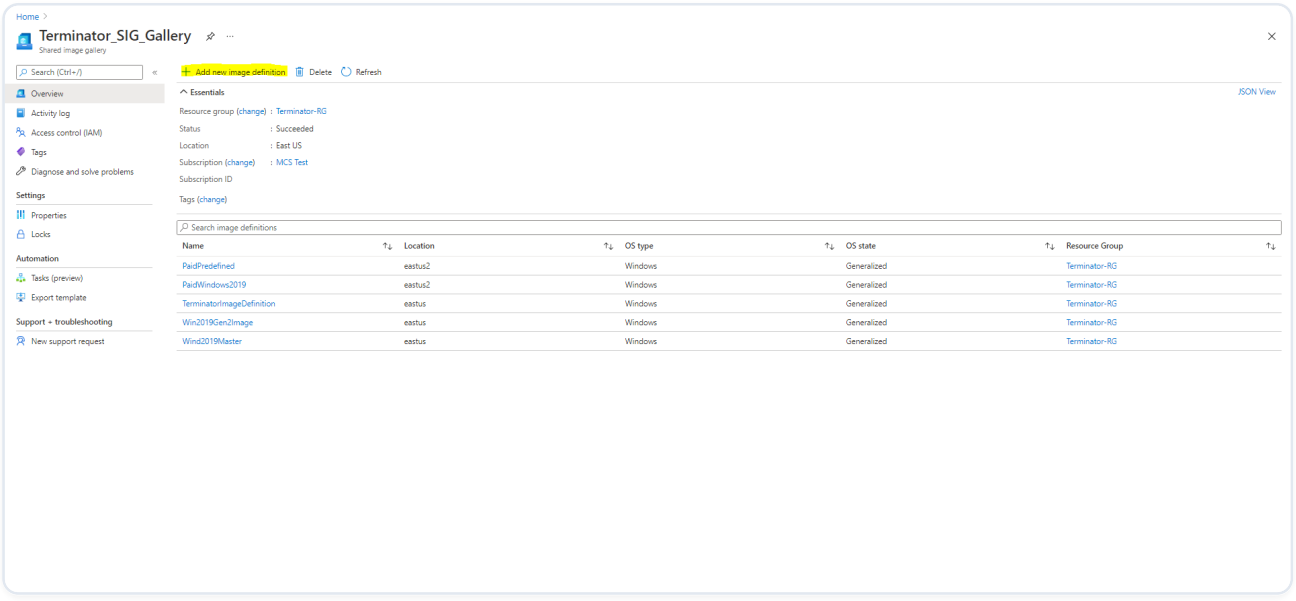
Azure 应用商店

Citrix Virtual Apps and Desktops 支持在 Azure 上使用包含计划信息的主映像来创建计算机目录。有关详细信息，请参阅 Microsoft Azure Marketplace。

> **提示：**
>
> Azure Marketplace 上的一些映像（例如标准 Windows Server 映像）不附加计划信息。Citrix Virtual Apps and Desktops 功能适用于付费映像。

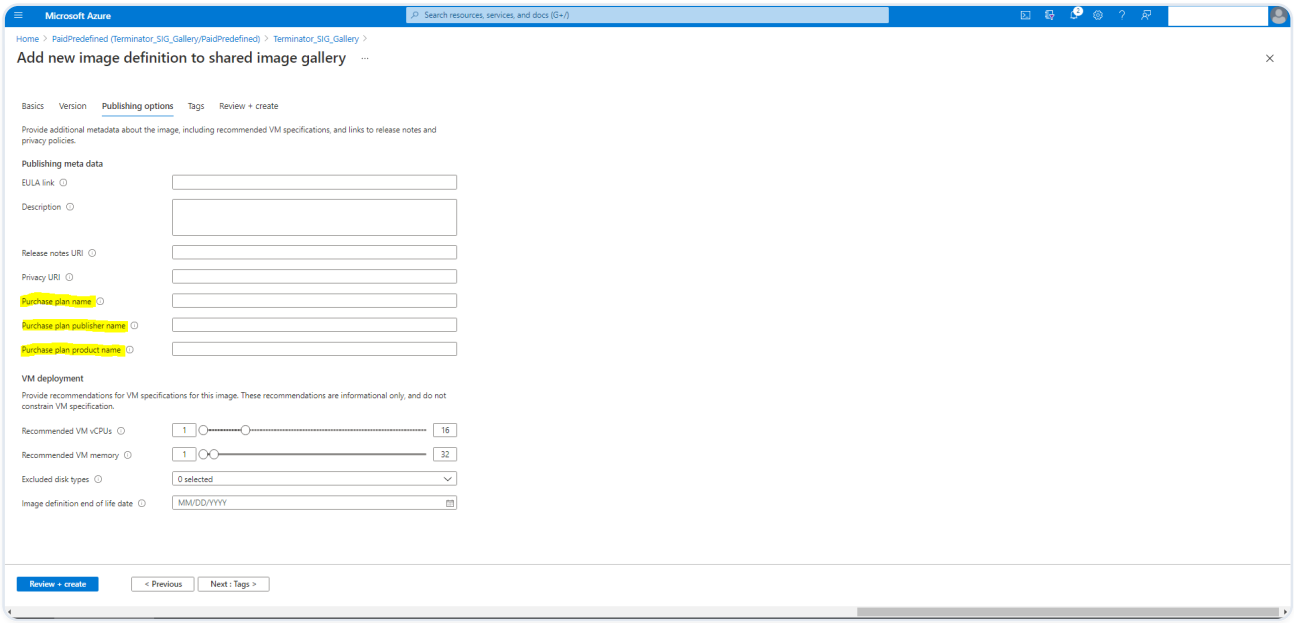
确保在共享映像库中创建的映像包含 AZURE 计划信息

使用本节中的过程在 Web Studio 中查看共享映像库映像。这些映像可以选择用作主映像。要将映像放入共享映像库，请在库中创建映像定义。

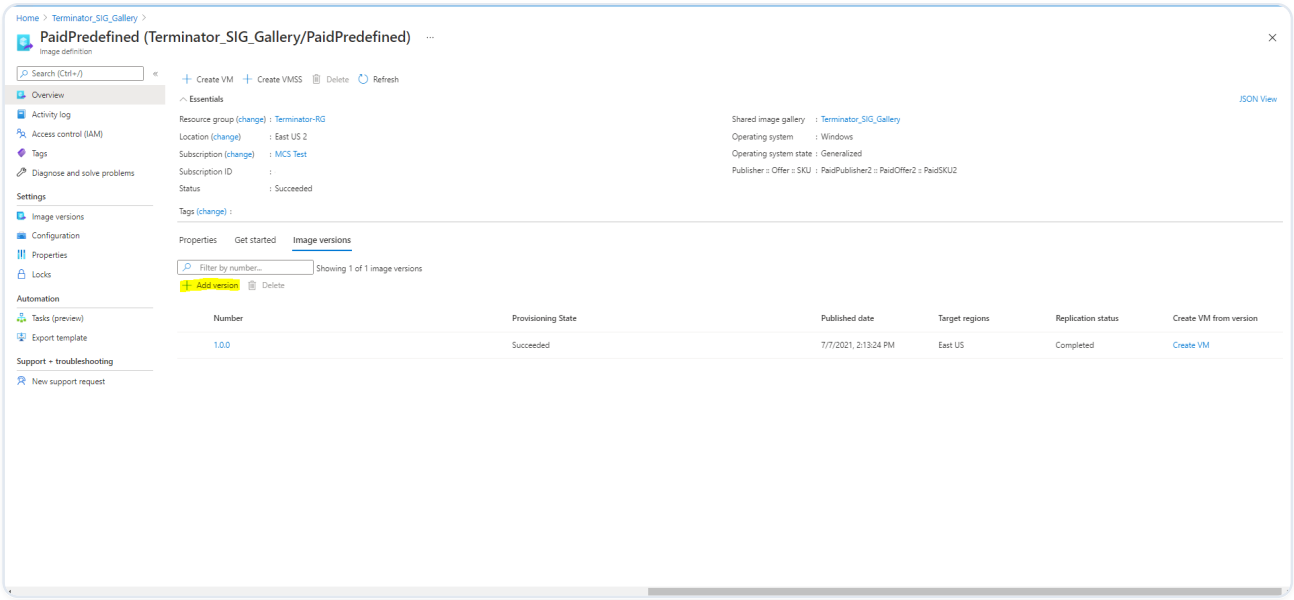


在**发布选项**页面中，验证购买计划信息。

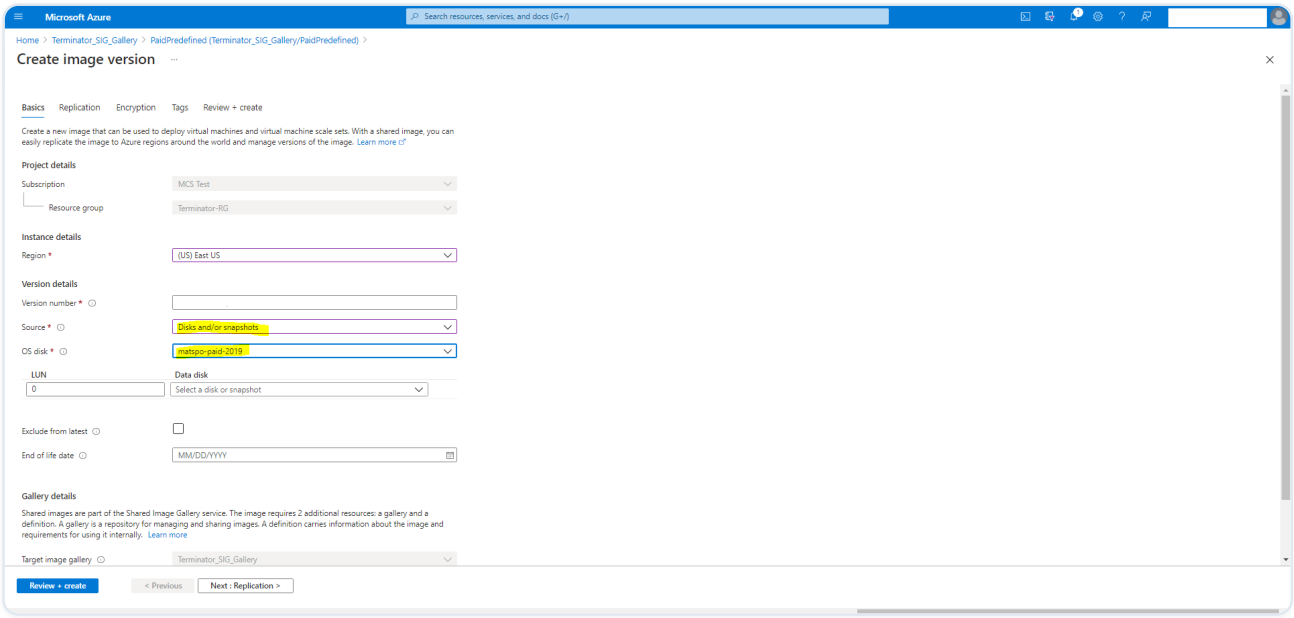
购买计划信息字段最初为空。使用用于镜像的购买计划信息填充这些字段。未能填充购买计划信息可能导致计算机目录创建过程失败。



验证购买计划信息后，在定义中创建镜像版本。此版本用作主镜像。单击**添加版本**：



在**版本详细信息**部分中，选择镜像快照或托管磁盘作为源：



创建按需容量预留 VM 目录

按需容量预留使您能够在 Azure 区域或可用性区域中预留计算容量，预留时间不限。有关 Azure 按需容量预留的更多信息，请参阅 Microsoft 文档 按需容量预留。

您可以使用计算机配置文件（VM 或模板规范）创建具有按需容量预留的 Azure VM 的 MCS 计算机目录。您还可以更新现有计算机目录和现有 VM，以添加或删除按需容量预留。

此功能适用于持久性和非持久性计算机目录。

限制

此功能不适用于：

- Spot 虚拟机
- 主机组
- 已启用休眠的 VM

有关限制的更多信息，请参阅 Microsoft 文档 限制和约束。

创建按需容量预留 VM 目录的步骤

1. 创建计算机配置文件源（VM 或 ARM 模板规范）。有关创建 VM 或 ARM 模板规范的信息，请参阅 将 VM 关联到容量预留组。
2. 运行以下 PowerShell 命令以检查计算机配置文件是否已启用按需容量预留。如果计算机配置文件已启用按需容量预留，则会获得 `capacityReservationGroup id`。

   例如，

   如果计算机配置文件源是 VM，请运行以下命令：

```
(Get-Item "XDHyp:\HostingUnits\azure-res-
conn2\machineprofile.folder\fifthcolumn.resourcegroup\demand-
capacity.vm").AdditionalData
```

如果计算机配置文件源是模板规范，请运行以下命令：

```
(Get-Item "XDHyp:\HostingUnits\azure-res-
conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
templatespec.templatespec\14.0.0-capacity-
reservation.templatespecversion").AdditionalData
```

3. 使用 Web Studio 或 PowerShell 命令，使用计算机配置文件创建计算机目录。

您可以使用 `Set-ProvScheme` 命令更新目录。您还可以使用 PowerShell 命令 `Set-ProvVmUpdateTimeWindow` 更新现有 VM。计算机配置文件将在下次开机时更新。

嵌套虚拟化

如果将主虚拟机配置为启用了嵌套虚拟化，则使用该主虚拟机创建的 MCS 计算机目录中的所有虚拟机都将启用嵌套虚拟化。此功能适用于持久性虚拟机和非持久性虚拟机。您可以通过映像更新来更新现有 MCS 计算机目录和现有虚拟机以启用嵌套虚拟化。

目前，只有 Dv3 和 Ev3 VM 大小支持嵌套虚拟化。

有关嵌套虚拟化的信息，请参阅 Microsoft 博客 Azure 中的嵌套虚拟化。

仅限 NVMe 的 SKU

通常，旧一代的通用、内存优化和计算优化 VM（D/Ev5 或 Fv2 及更早版本）支持 SCSI。新一代（Da/Ea/Fav6 及更新版本）通常仅支持 NVMe 存储接口。MCS 支持 NVMe 存储控制器类型，以支持 Azure 上的新 VM SKU。

有关 NVMe 的信息，请参阅 Microsoft 文档 NVMe 常见问题解答。

您可以使用以下服务产品创建 MCS 目录：

- 同时支持 SCSI 和 NVMe，请参阅 使用同时支持 SCSI 和 NVMe 的服务产品创建目录
- 仅支持 NVMe，请参阅 使用仅支持 NVMe 的服务产品创建目录

限制

- 所有支持 NVMe 的服务产品都不支持同时进行受信任启动。
- Gen 1 VM 不支持 NVMe。

- 某些操作系统映像可能不支持 NVMe。在这种情况下，Azure UI 上的 NVMe 选项将显示为灰色。

使用同时支持 SCSI 和 NVME 的服务产品创建目录

1. 创建用作主映像的 VM。

   a. 使用支持 NVMe 的市场映像。支持 NVMe 的 Azure Marketplace 映像列表可在 远程 NVMe 支持的操作系统映像 中找到。

   b. 拍摄 VM 操作系统磁盘的快照，以在 `New-ProvScheme` 命令的 `MasterImageVM` 参数中使用，或直接使用托管磁盘。

   检查您的主映像是否支持 NVMe，可使用以下方法之一：

   - 检查 `Get-Item` 的 `AdditionalData` 字段中的 `SupportedDiskControllerTypes` 。例如：

     ```
     (get-item XDHyp:
     \HostingUnits\mynetwork\image.folder\abc.resourcegroup\deg-
     snapshot).AdditionalData
     ```

     `SupportedDiskControllerTypes` 必须是 `SCSI, NVMe` 。

   - 使用 Azure CLI 和 PowerShell

2. 使用同时支持 NVMe 和 SCSI 的服务产品。
3. 使用已启用 NVMe 的 VM 或模板规范作为计算机配置文件。选择任何将 `DiskControllerType` 设置为 NVMe 的 VM。直接将该 VM 用作计算机配置文件，或导出模板并将模板规范用作计算机配置文件。

使用仅支持 NVME 的服务产品创建目录

1. 创建用作主映像的 VM。使用支持 NVMe 的市场映像。支持 NVMe 的 Azure Marketplace 映像列表可在 适用于远程 NVMe 的支持的操作系统映像 中找到。
2. 使用仅支持 NVMe 的服务产品。

> **注意：**
>
> 由于服务产品支持 NVMe，因此您不需要将 `DiskControllerType` 设置为 `NVMe` 的计算机配置文件即可在目录上启用 NVMe。但是，如果您使用计算机配置文件，则 `DiskControllerType` 必须设置为 `NVMe` ，或者必须为空或未指定。

修改现有持久性 VM

VM 创建后，无法更改其 NVMe 配置。更改持久性 VM 的 NVMe 配置的方法是重新部署 VM。执行此操作的逻辑是：

1. 保存 VM 的当前状态。
2. 启动现有 VM 后，检测 VM 是否需要重新部署。
    a. 如果配置更改是从 NVMe 到 NVMe 或从 SCSI 到 SCSI，则无需重新部署 VM。
    b. 如果配置更改是从 SCSI 到 NVMe，反之亦然，则重新部署并重新创建 VM。

使用 PowerShell 创建计算机目录

本节详细介绍了如何使用 PowerShell 创建目录：

- 创建具有非持久性回写缓存磁盘的目录
- 创建具有持久性回写缓存磁盘的目录
- 使用 MCSIO 提高启动性能
- 使用 PowerShell 创建或更新目录时使用模板规范
- 具有受信任启动的计算机目录
- 使用计算机配置文件属性值
- 使用客户管理的加密密钥创建计算机目录(#create-a-machine-catalog-with-customer-managed-encryption-key)
- 创建具有双重加密的计算机目录
- 创建具有 Azure 临时磁盘的目录
- Azure 专用主机
- 使用 Azure 计算库映像创建或更新计算机目录
- 配置共享映像库
- 将计算机预配到指定的可用性区域
- 存储类型
- 使用 Azure Spot VM 创建目录(#create-a-catalog-using-azure-spot-vms)
- 配置备份虚拟机大小
- 复制所有资源上的标签
- 预配安装了 Azure Monitor 代理的目录虚拟机

创建具有非持久性回写缓存磁盘的目录

要配置具有非持久性回写缓存磁盘的目录，请使用 PowerShell 参数 `New-ProvScheme CustomProperties`。自定义属性 `UseTempDiskForWBC` 指示您是否接受使用 Azure 临时存储来存储回写缓存文件。如果希望将临时磁盘用作回写缓存磁盘，则在运行 `New-ProvScheme` 时必须将其配置为 true。如果未指定此属性，则参数默认为 **False**。

例如，使用 `CustomProperties` 参数将 `UseTempDiskForWBC` 设置为 **true**：

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/
> `

</CustomProperties>'
```

注意：

将计算机目录提交为使用 Azure 本地临时存储作为回写缓存文件后，以后无法更改为使用 VHD。

创建具有持久性回写缓存磁盘的目录

要配置具有持久回写缓存磁盘的目录，请使用 PowerShell 参数 `New-ProvScheme` `CustomProperties`。此参数支持一个额外的属性 `PersistWBC`，用于确定 MCS 预配的计算机的回写缓存磁盘如何持久化。`PersistWBC` 属性仅在指定 `UseWriteBackCache` 参数且设置 `WriteBackCacheDiskSize` 参数以指示已创建磁盘时使用。

在支持 `PersistWBC` 之前，`CustomProperties` 参数中找到的属性示例包括：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

使用这些属性时，请注意，如果 `CustomProperties` 参数中省略了这些属性，它们将包含默认值。`PersistWBC` 属性有两个可能的值：**true** 或 **false**。

当 Citrix Virtual Apps and Desktops 管理员使用 Web Studio 关闭计算机时，将 `PersistWBC` 属性设置为 **true** 不会删除回写缓存磁盘。

当 Citrix Virtual Apps and Desktops 管理员使用 Web Studio 关闭计算机时，将 `PersistWBC` 属性设置为 **false** 会删除回写缓存磁盘。

> **注意：**
>
> 如果省略 `PersistWBC` 属性，则该属性默认为 **false**，并且在使用 Web Studio 关闭计算机时会删除回写缓存。
>
> 例如，使用 `CustomProperties` 参数将 `PersistWBC` 设置为 true：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

重要提示：

`PersistWBC` 属性只能使用 `New-ProvScheme` PowerShell cmdlet 进行设置。在创建后尝试更改预配方案的 `CustomProperties` 对计算机目录以及计算机关闭时回写缓存磁盘的持久性没有影响。

例如，设置 `New-ProvScheme` 以使用回写缓存，同时将 `PersistWBC` 属性设置为 true：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"
```

```
-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

使用 MCSIO 提高启动性能

启用 MCSIO 后，可以提高 Azure 和 GCP 托管磁盘的启动性能。在 `New-ProvScheme` 命令中使用 PowerShell `PersistOSDisk` 自定义属性来配置此功能。与 `New-ProvScheme` 相关的选项包括：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

要启用此功能，请将 `PersistOSDisk` 自定义属性设置为 `true`。例如：
```

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

使用 PowerShell 通过模板规范创建或更新目录

您可以使用模板规范作为计算机配置文件输入来创建或更新 MCS 计算机目录。为此，您可以使用 Web Studio 或 PowerShell 命令。

对于 Web Studio，请参阅 使用 Web Studio 中的 Azure Resource Manager 映像创建计算机目录

使用 PowerShell 命令：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*`。
3. 创建或更新目录。
   - 要创建目录：
     a. 使用 `New-ProvScheme` 命令，并将模板规范作为计算机配置文件输入。例如：

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
image.folder/fgthj.resourcegroup/nab-ws-
vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>

[-LoggingId <Guid>]

[-BearerToken <String>][-AdminAddress <String>]

[<CommonParameters>]
```

     b. 完成目录创建。
   - 要更新目录，请使用 `Set-ProvScheme` 命令，并将模板规范作为计算机配置文件输入。例如：

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
Us.region/vm.folder/MasterDisk.vm'

MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'
```

```
[-ProvisioningSchemeName] <String>

[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]

[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <String>]
[<CommonParameters>]
```

具有可信启动的计算机目录

要成功创建具有可信启动的计算机目录，请使用：

- 启用了可信启动的主映像。您必须使用计算机配置文件，但计算机配置文件不必启用可信启动。如果您使用启用了可信启动的主映像和未启用可信启动的计算机配置文件，则会收到警告消息，因为主映像和计算机配置文件之间的可信启动配置不匹配。
- 支持受信任启动的 VM 大小
- 支持可信启动的 Windows VM 版本。目前，Windows 10、Windows 11、Windows Server 2016、2019 和 2022 支持可信启动。

要查看 Citrix Virtual Apps and Desktops 提供的清单项，并确定 VM 大小是否支持受信任启动，请运行以下命令：

1. 打开 PowerShell 窗口。
2. 运行 **asnp citrix*** 以加载 Citrix 特定的 PowerShell 模块。
3. 运行以下命令：

```
$s = (ls XDHyp:\HostingUnits\<name of hosting
unit>\serviceoffering.folder\"<VM size>.serviceoffering)
```

4. 运行 `$s | select -ExpandProperty Additionaldata`
5. 检查 `SupportsTrustedLaunch` 属性的值。
   - 如果 `SupportsTrustedLaunch` 为 **True**，则 VM 大小支持受信任启动。
   - 如果 `SupportsTrustedLaunch` 为 **False**，则 VM 大小不支持受信任启动。

根据 Azure 的 PowerShell，您可以使用以下命令确定支持受信任启动的 VM 大小：

```
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and
($_.Name -eq "<VM size>") })[0].Capabilities
```

以下示例描述了运行 Azure PowerShell 命令后 VM 大小是否支持受信任启动。

- *示例 1*：如果 Azure VM 仅支持第 1 代，则该 VM 不支持受信任启动。因此，运行 Azure PowerShell 命令后，不会显示 `TrustedLaunchDisabled` 功能。
- *示例 2*：如果 Azure VM 仅支持第 2 代，并且 `TrustedLaunchDisabled` 功能为 **True**，则第 2 代 VM 大小不支持受信任启动。
- *示例 3*：如果 Azure VM 仅支持第 2 代，并且运行 PowerShell 命令后未显示 `TrustedLaunchDisabled` 功能，则第 2 代 VM 大小支持受信任启动。

有关 Azure 虚拟机受信任启动的更多信息，请参阅 Microsoft 文档 Azure 虚拟机受信任启动。

使用受信任启动创建计算机目录

1. 创建启用受信任启动的主映像。请参阅 Microsoft 文档 受信任启动 VM 映像。
2. 创建安全类型为 **受信任启动虚拟机** 的 VM 或模板规范。有关创建 VM 或模板规范的更多信息，请参阅 Microsoft 文档部署受信任启动 VM。
3. 使用 Web Studio 或 PowerShell 命令创建计算机目录。
   - 如果要使用 Web Studio，请参阅 使用 Web Studio 中的 Azure Resource Manager 映像创建计算机目录。
   - 如果要使用 PowerShell 命令，请使用 `New-ProvScheme` 命令，并将 VM 或模板规范作为计算机配置文件输入。有关创建目录的完整命令列表，请参阅 创建目录。

     `New-ProvScheme` 将 VM 作为计算机配置文件输入的示例：

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name"
     -IdentityPoolName "name" -InitialBatchSizeHint 1

     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
     fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

     -MachineProfile "XDHyp:
     \HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<mac
     hine profile vm.vm>"

     -ProvisioningSchemeName <String>

     -HostingUnitName <String>

     -IdentityPoolName <String>
     ```

```
[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

`New-ProvScheme` 将模板规范作为计算机配置文件输入的示例：

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name"
-IdentityPoolName "name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

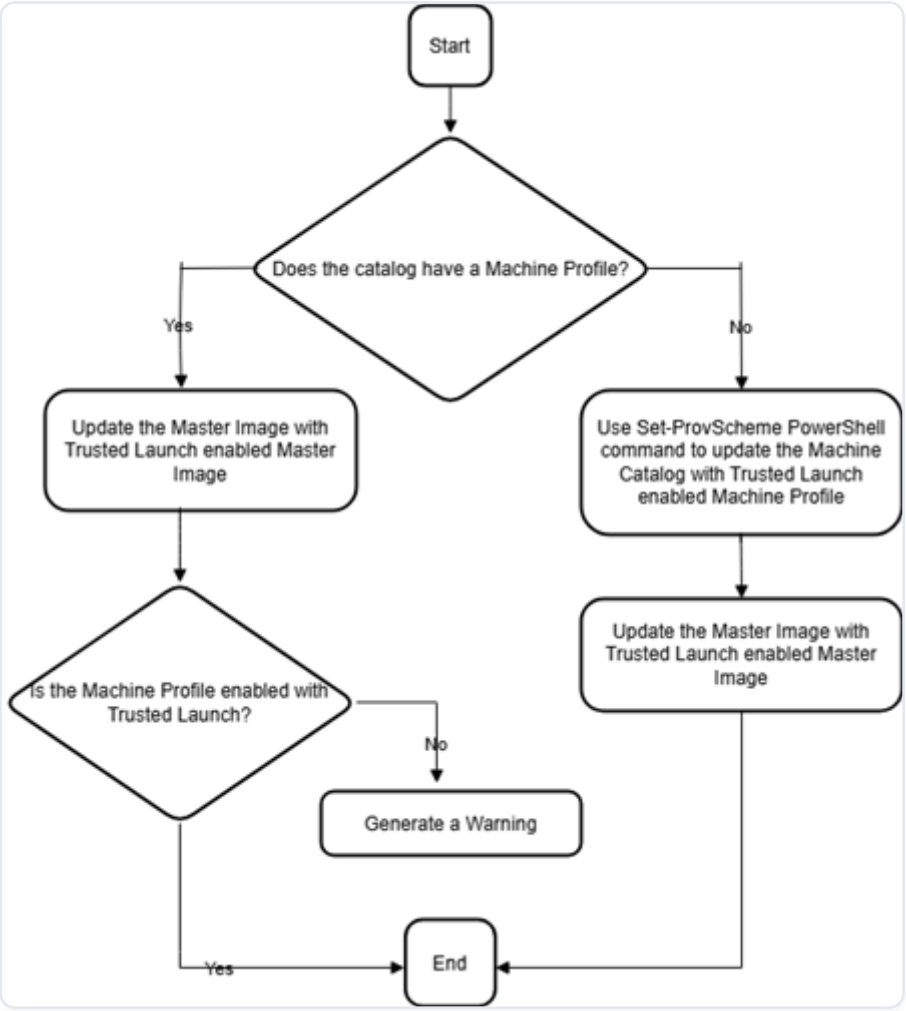
[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

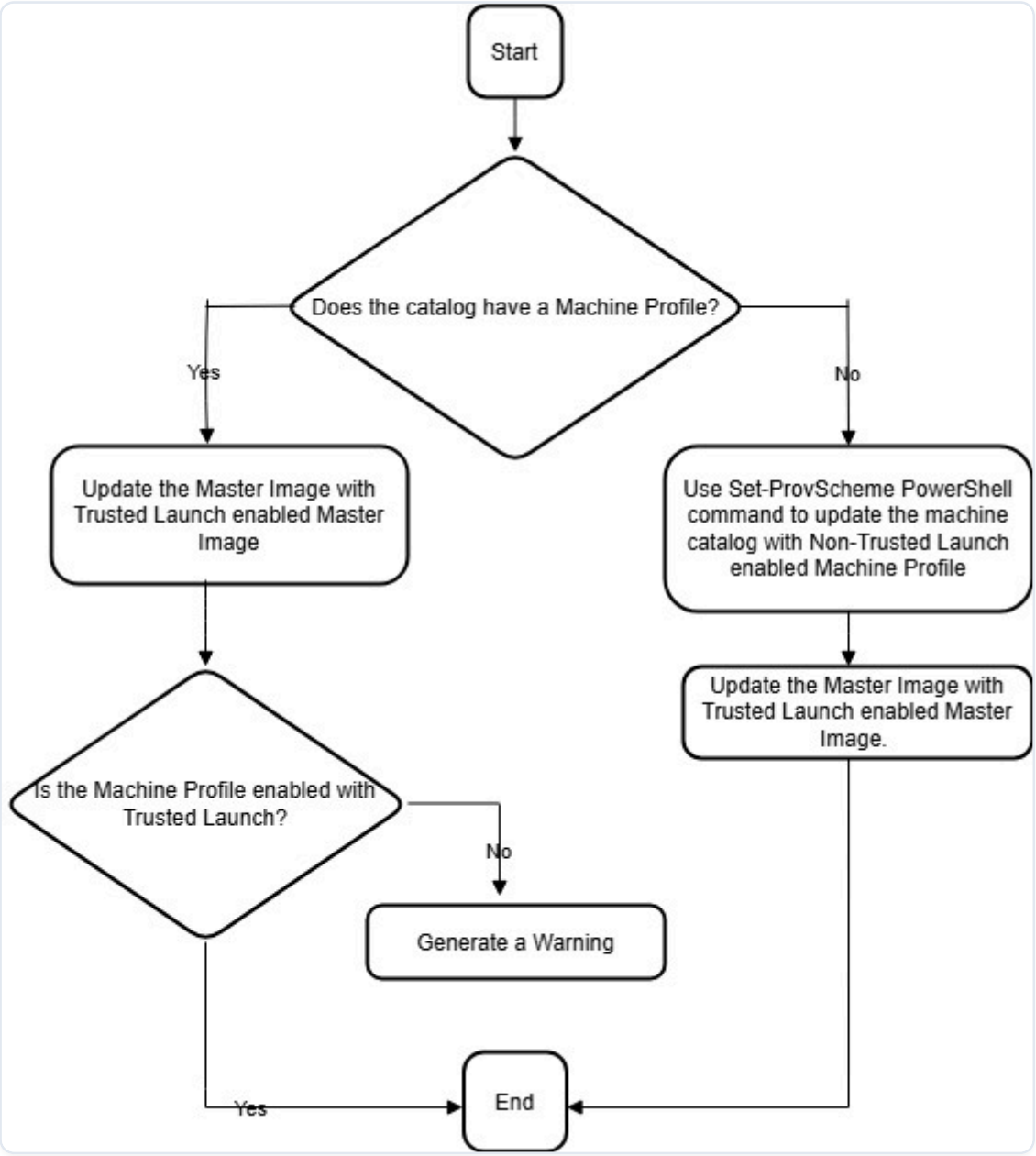
使用受信任启动更新计算机目录

您可以更新持久性和非持久性计算机目录：

对于持久性计算机目录：



对于非持久性计算机目录：



使用受信任启动创建计算机目录时出错

在使用受信任启动创建计算机目录时，在以下场景中会收到相应的错误：

场景	错误
如果在创建非托管目录时选择计算机配置文件	`MachineProfileNotSupportedForUnmanagedCatalog`
如果您在创建托管目录时未选择计算机配置文件，且该目录的主映像源的安全类型为受信任启动	`MachineProfileNotFoundForTrustedLaunchMasterImage`
如果您选择的计算机配置文件的安全类型与主映像的安全类型不同	`SecurityTypeConflictBetweenMasterImageAndMachineProfile`

场景	错误
如果您选择的 VM 大小不支持可信启动，但在创建目录时使用支持可信启动的主映像	`MachineSizeNotSupportTrustedLaunch`

使用计算机配置文件属性值

计算机目录使用自定义属性中定义的以下属性：

- 可用区
- 专用主机组 ID
- 磁盘加密集 ID
- 操作系统类型
- 许可证类型
- 存储类型

如果未明确定义这些自定义属性，则属性值将从 ARM 模板规范或 VM（以用作计算机配置文件者为准）中设置。此外，如果 `ServiceOffering` 未指定，则它将从计算机配置文件中设置。

> **注意：**
>
> 如果计算机配置文件中缺少某些属性且未在自定义属性中定义，则在适用的情况下将采用属性的默认值。

> 以下部分描述了 `New-ProvScheme` 和 `Set-ProvScheme` 中的一些场景，其中 `CustomProperties` 定义了所有属性或值是从 MachineProfile 派生的。

- New-ProvScheme 场景
  - MachineProfile 具有所有属性，且未定义 CustomProperties。示例：

    `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

    以下值被设置为目录的自定义属性：

    ```
    Get-ProvScheme | select CustomProperties

    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    ```

```
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- MachineProfile 具有某些属性，且未定义 CustomProperties。示例：MachineProfile 仅包含 LicenseType 和 OsType。

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

  以下值被设置为目录的自定义属性：

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>
```

```
</CustomProperties>
```

- MachineProfile 和 CustomProperties 都定义了所有属性。示例：

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

  自定义属性优先。以下值被设置为目录的自定义属性：

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones"
Value="<CustomPropertiesA-value>"/>

</CustomProperties>
```

- MachineProfile 中定义了一些属性，CustomProperties 中也定义了一些属性。示例：
  - CustomProperties 定义 LicenseType 和 StorageAccountType
  - MachineProfile 定义 LicenseType、OsType 和 Zones

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

以下值被设置为目录的自定义属性：

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- 某些属性在 MachineProfile 中定义，某些属性在 CustomProperties 中定义。此外，ServiceOffering 未定义。示例：
  - CustomProperties 定义 StorageType
  - MachineProfile 定义 LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mp
.vm"

-ServiceOffering "XDHyp:
\HostingUnits\azureunit\serviceoffering.folder\<explicit-machine-
size>.serviceoffering"
```

以下值被设置为目录的自定义属性：

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<explicit-machine-size>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="value-
from-machineprofile"/>

</CustomProperties>
```

- 如果 OsType 既不在 CustomProperties 中也不在 MachineProfile 中，则：
  - 该值从主映像中读取。
  - 如果主映像是未托管磁盘，则 OsType 设置为 Windows。示例：

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -MasterImageVM "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.manageddisk"`

主映像中的值将写入自定义属性，在本例中为 Linux。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>
```

```
</CustomProperties>
```

- Set-ProvScheme 方案
  - 一个现有目录，包含：
    - `StorageAccountType` 和 OsType 的自定义属性
    - 定义区域的 MachineProfile `mpA.vm`
  - 更新：
    - 定义 StorageAccountType 的 MachineProfile mpB.vm
    - 一组新的自定义属性 $CustomPropertiesB，定义了 LicenseType 和 OsType

    `Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm" -CustomProperties $CustomPropertiesB`

    以下值被设置为目录的自定义属性：

    ```
    Get-ProvScheme | select CustomProperties

    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">

    <Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<mpB-value>"/>

    <Property xsi:type="StringProperty" Name="OSType"
    Value="<CustomPropertiesB-value>"/>

    <Property xsi:type="StringProperty" Name="LicenseType"
    Value="<CustomPropertiesB-value>"/>

        </CustomProperties>
    ```

  - 一个现有目录，包含：
    - S`torageAccountType` 和 OsType 的 CustomProperties
    - 定义 StorageAccountType 和 LicenseType 的 MachineProfile `mpA.vm`

- 更新：
  - 一组新的自定义属性 $CustomPropertiesB，定义了 StorageAccountType 和 OsType。

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

以下值被设置为目录的自定义属性：

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp-A-
value>"/>

</CustomProperties>
```

- 一个现有目录，包含：
  - `StorageAccountType` 和 OsType 的自定义属性
  - 定义了区域的计算机配置文件 `mpA.vm`
- 更新：
  - 一个定义了 StorageAccountType 和 LicenseType 的计算机配置文件 mpB.vm
  - `ServiceOffering` 未指定

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

以下值被设置为目录的自定义属性：

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<value-from-machineprofile>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<prior-
CustomProperties-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpB-
value>"/>

</CustomProperties>
```

创建或更新每台 VM 具有多个 NIC 的目录

MCS 支持每台 VM 具有多个 NIC。您可以将 VM 上的多个 NIC 关联到多个子网，但是，这些子网必须位于同一虚拟网络 (VNet) 中。您可以使用 PowerShell 命令来：

- 在虚拟机上创建具有多个 NIC 的目录(#create-a-catalog-with-multiple-nics-on-a-vm)
- 更新现有目录配置以使虚拟机具有多个 NIC，从而使新创建的虚拟机具有多个 NIC(#update-a-catalog-to-have-multiple-nics-on-a-vm)
- 更新现有虚拟机以使其具有多个 NIC(#update-an-existing-vm-to-have-multiple-nics-on-a-vm)

您可以创建或更新非计算机配置文件型计算机目录和计算机配置文件型计算机目录，以使虚拟机具有多个 NIC。目前，对于基于计算机配置文件的计算机目录，您只能拥有与计算机配置文件源中指定的 NIC 数量相同的 NIC。

加速网络等属性源自计算机配置文件源。

> **注意：**

> 虚拟机大小必须支持相同数量的 NIC 和相应的加速网络，否则会出错。

> 您可以检索与所选虚拟机大小关联的最大 NIC 数量。当您使用 `AdditionalData` 参数运行 PowerShell `get-item` 命令时，名为 `MaxNetworkInterfaces` 的 PowerShell 属性会显示最大 NIC 计数。

检索最大 NIC 计数

要检索最大 NIC 计数：

1. 从 Delivery Controller™ 主机打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行 `Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"` 以列出所有可用的虚拟机大小。
4. 运行 `get-item -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering").AdditionalData`
5. 检查 `MaxNetworkInterfaces` 以了解最大 NIC 计数。

在虚拟机上创建具有多个网卡的目录

要在虚拟机上创建具有多个网卡的目录，请执行以下操作：

1. 从 Delivery Controller 主机打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 专用 PowerShell 模块。
3. 如果尚未创建身份池，请创建一个。
4. 创建预配方案：
   - 如果正在创建非计算机配置文件型计算机目录，请运行带 `NetworkMappings` 参数的 `New-ProvScheme` 命令。可以将多个子网添加到参数 `NetworkMappings`。例如：

     ```
     New-Provscheme -NetworkMappings
     @{"0"="subnetpath1";"1"="subnetpath1"}
     ```

   - 如果正在创建计算机配置文件型计算机目录：
     a. 在 Azure 中创建具有多个网卡的虚拟机。有关信息，请参阅创建和管理具有多个网卡的 Windows 虚拟机。您还可以创建新的虚拟机，然后在 Azure 门户的“网络”页面中附加网络接口。
     b. 运行 `New-ProvScheme` 命令，并将虚拟机作为计算机配置文件输入。

> **注意：**
>
> 创建计算机配置文件型计算机目录时，`NetworkMappings` 的计数必须与计算机配置文件的 `NetworkInterfaceCount` 相同。`NetworkInterfaceCount` 可以从 `Get-item -Path "machine profile path"` 的 `AdditionalData` 中检索。

5. 完成目录创建。

更新目录以使虚拟机具有多个网卡

要更新目录以使虚拟机具有多个网卡，请执行以下操作：

1. 从 Delivery Controller 主机打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 专用的 PowerShell 模块。
3. 更新预配方案：
   - 如果要创建非计算机配置文件型计算机目录，请运行带 `NetworkMappings` 参数的 `Set-ProvScheme` 命令。您可以向参数 `NetworkMappings` 添加多个子网。例如：

     ```
     Set-Provscheme -NetworkMappings
     @{"0"="subnetpath1";"1"="subnetpath1"}
     ```

   - 如果要创建基于计算机配置文件的计算机目录：
     a. 在 Azure 中创建具有多个 NIC 的 VM。有关信息，请参阅创建和管理具有多个 NIC 的 Windows 虚拟机。
     b. 运行 `Set-ProvScheme` 命令，并将 VM 作为计算机配置文件输入。

更新现有 VM 以在 VM 上具有多个 NIC

您还可以使用 `Set-ProvVMUpdateTimeWindow` 更新现有 VM，并在更新时间窗口内对现有 VM 执行电源循环。

预配安装了 Azure Monitor Agent 的目录 VM

Azure 监视是一项服务，可用于收集、分析和处理来自您的 Azure 和本地环境的遥测数据。

Azure Monitor Agent (AMA) 从虚拟机等计算资源收集监视数据，并将数据传送到 Azure Monitor。它目前支持收集事件日志、Syslog 和性能指标，并将其发送到 Azure Monitor Metrics 和 Azure Monitor Logs 数据源。

要通过唯一标识监视数据中的 VM 来启用监视，您可以预配安装了 AMA 作为扩展的 MCS 计算机目录的 VM。

要求

- 权限：确保您拥有 所需 Azure 权限 中指定的最低 Azure 权限以及使用 Azure Monitor 的以下权限：
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- 数据收集规则：在 Azure 门户中设置数据收集规则。有关设置 DCR 的信息，请参阅 创建数据收集规则。DCR 是特定于平台的（Windows 或 Linux）。请确保根据所需平台创建 DCR。 AMA 使用数据收集规则 (DCR) 来管理资源（例如 VM）与数据源（例如 Azure Monitor Metrics 和 Azure Monitor Logs）之间的映射。
- 默认工作区：在 Azure 门户中创建工作区。有关创建工作区的信息，请参阅 创建 Log Analytics 工作区。当您收集日志和数据时，信息将存储在工作区中。工作区具有唯一的工作区 ID 和资源 ID。工作区名称对于给定的资源组必须是唯一的。创建工作区后，配置数据源和解决方案以将其数据存储在工作区中。
- 已将监视器扩展列入白名单：扩展 `AzureMonitorWindowsAgent` 和 `AzureMonitorLinuxAgent` 是 Citrix 定义的白名单扩展。要查看白名单扩展列表，请使用 PoSH 命令 `Get-ProvMetadataConfiguration`。
- 主映像：Microsoft 建议在从现有计算机创建新计算机之前从现有计算机中删除扩展。如果未删除扩展，可能会导致残留文件和意外行为。有关详细信息，请参阅 如果从现有 VM 重新创建 VM 。

要预配启用 AMA 的目录 VM：

1. 设置计算机配置文件模板。
   - 如果要使用 VM 作为计算机配置文件模板：
     a. 在 Azure 门户上创建 VM。
     b. 启动 VM。
     c. 在**资源**下将 VM 添加到数据收集规则。这会在模板 VM 上调用代理安装。

注意：

如果必须创建 Linux 目录，请设置 Linux 计算机。

- 如果要使用模板规范作为计算机配置文件模板：

  a. 设置模板规范。

  b. 将以下扩展和数据收集规则关联添加到生成的模板规范：

```
{
"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {
    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
}
},
```

```
 {

    "type": "Microsoft.Insights/dataCollectionRuleAssociations",

    "apiVersion": "2021-11-01",

    "name": "<associatio-name>",

    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",

    "dependsOn": [

     "Microsoft.Compute/virtualMachines/<vm-name>",

    "Microsoft.Compute/virtualMachines/<vm-name>/extensions/
AzureMonitorWindowsAgent"

    ],

    "properties": {

       "description": "Association of data collection rule.
Deleting this association will break the data collection for this
Arc server.",

     "dataCollectionRuleId": "/subscriptions/<azure-
subscription>/resourcegroups/<azure-resource-group>/providers/
microsoft.insights/datacollectionrules/<azure-data-collection-
rule>"

     }

    }
```

2. 创建或更新现有 MCS 计算机目录。

   - 要创建新的 MCS 目录，请执行以下操作：

     a. 在 Web Studio 中选择该 VM 或模板规范作为计算机配置文件。

     b. 继续执行后续步骤以创建目录。

   - 要更新现有 MCS 目录，请使用以下 PoSH 命令：

- 要让新 VM 获取更新的计算机配置文件模板，请运行以下命令：

```
Set-ProvScheme -ProvisioningSchemeName "name"

-MachineProfile "XDHyp:
\HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
machine-profile.vm"
```

- 要使用更新的计算机配置文件模板更新现有 VM：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

3. 启动目录 VM。
4. 转到 Azure 门户，检查监视器扩展是否已安装在 VM 上，以及 VM 是否显示在 DCR 的资源下。几分钟后，监视数据将显示在 Azure Monitor 上。

故障排除

有关 Azure Monitor Agent 故障排除指南的信息，请参阅以下内容：

- https://learn.microsoft.com/zh-cn/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/zh-cn/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

使用客户管理的加密密钥创建计算机目录

使用客户管理的加密密钥创建计算机目录的详细步骤如下：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 输入 `cd xdhyp:/`。
4. 输入 `cd .\HostingUnits\(your hosting unit)`。
5. 输入 `cd diskencryptionset.folder`。
6. 输入 `dir` 以获取磁盘加密集列表。
7. 复制磁盘加密集的 ID。
8. 创建一个自定义属性字符串以包含磁盘加密集的 ID。例如：

```
$customProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
Value=`"False`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/
abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>

</CustomProperties>
```

9. 如果尚未创建身份池，请创建一个。例如：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain def.local -NamingSchemeType Numeric
```

10. 运行 New-ProvScheme 命令：例如：

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\azure-
res2\image.folder\def.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-res2\
\virtualprivatecloud.folder\def.resourcegroup\def-
vnet.virtualprivatecloud\subnet1.network"}

-ProvisioningSchemeName "name"
```

```
-ServiceOffering "XDHyp:\HostingUnits\azure-
res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<machin
e profile vm.vm>"

-CustomProperties $customProperties
```

11. 完成创建计算机目录。

创建具有双重加密的计算机目录

您可以使用 Web Studio 和 PowerShell 命令创建和更新具有双重加密的计算机目录。

创建具有双重加密的计算机目录的详细步骤如下：

1. 使用平台管理的密钥和客户管理的密钥创建 Azure Key Vault 和 DES。有关如何创建 Azure Key Vault 和 DES 的信息，请参阅使用 Azure 门户为托管磁盘启用静态双重加密。
2. 要浏览托管连接中可用的 DiskEncryptionSets：
   a. 打开 **PowerShell** 窗口。
   b. 运行以下 PowerShell 命令：
      i. `asnp citrix*`
      ii. `cd xdhyp:`
      iii. `cd HostingUnits`
      iv. `cd YourHostingUnitName`（例如 azure-east）
      v. `cd diskencryptionset.folder`
      vi. `dir`

   您可以使用 `DiskEncryptionSet` 的 ID 来使用自定义属性创建或更新目录。
3. 如果要使用计算机配置文件工作流，请创建 VM 或模板规范作为计算机配置文件输入。
   - 如果要使用 VM 作为计算机配置文件输入：
     a. 在 Azure 门户中创建 VM。
     b. 导航到 **磁盘>密钥管理** 以使用任何 `DiskEncryptionSetID` 直接加密 VM。
   - 如果要使用模板规范作为计算机配置文件输入：

a. 在模板中，在 `properties>storageProfile>osDisk>managedDisk` 下，添加 `diskEncryptionSet` 参数并添加双重加密 DES 的 ID。

4. 创建计算机目录。

- 如果使用 Web Studio，除了 创建计算机目录 中的步骤外，请执行以下操作之一。
  - 如果您不使用基于计算机配置文件的流程，请在**磁盘设置**页面上，选择**使用以下密钥加密每台计算机上的数据**。然后，从下拉菜单中选择您的双重加密 DES。继续创建目录。
  - 如果使用计算机配置文件流程，请在**映像**页面上，选择一个主映像和一个计算机配置文件。确保计算机配置文件在其属性中具有磁盘加密集 ID。

  目录中创建的所有计算机都将通过您选择的 DES 关联的密钥进行双重加密。
- 如果使用 PowerShell 命令，请执行以下操作之一：
  - 如果不使用基于计算机配置文件的流程，请在 `New-ProvScheme` 命令中添加自定义属性 `DiskEncryptionSetId`。例如：

```
New-ProvScheme -CleanOnBoot -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />

</CustomProperties>'

-HostingUnitName "Redacted"

-IdentityPoolName "Redacted"

-InitialBatchSizeHint 1

-MasterImageVM "Redacted"
```

```
-NetworkMapping @{"0"="Redacted"}

-ProvisioningSchemeName "Redacted"

-ServiceOffering "Redacted"
```

- 如果使用基于计算机配置文件的流程，请在 `New-ProvScheme` 命令中使用计算机配置文件输入。例如：

```
New-ProvScheme -CleanOnBoot

-HostingUnitName azure-east

-IdentityPoolName aio-ip

-InitialBatchSizeHint 1

-MasterImageVM XDHyp:\HostingUnits\azure-
east\image.folder\abc.resourcegroup\fgb-vda-snapshot.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-
east\virtualprivatecloud.folder\apa-
resourceGroup.resourcegroup\apa-resourceGroup-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName aio-test

-MachineProfile XDHyp:\HostingUnits\azure-
east\machineprofile.folder\abc.resourcegroup\abx-
mp.templatespec\1.0.0.templatespecversion
```

5. 使用远程 PowerShell SDK 完成目录创建。有关如何使用远程 PowerShell SDK 创建目录的信息，请参阅 https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/。目录中创建的所有计算机都将通过您选择的 DES 关联的密钥进行双重加密。

将未加密的目录转换为使用双重加密

您可以更新计算机目录的加密类型（使用自定义属性或计算机配置文件）。

- 如果不使用基于计算机配置文件的流程，请在 `Set-ProvScheme` 命令中添加自定义属性 DiskEncryptionSetId。例如：

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/12345678-xxxx-1234-1234-123456789012/resourceGroups/
Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/
SampleEncryptionSet" />

</CustomProperties>'
```

- 如果使用基于计算机配置文件的流程，请在 `Set-ProvScheme` 命令中使用计算机配置文件输入。例如：

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
XDHyp:\HostingUnits\azure-
east\machineprofile.folder\aelx.resourcegroup\elx-
mp.templatespec\1.0.0.templatespecversion
```

成功后，您在目录中添加的所有新 VM 都将由您选择的 DES 关联的密钥进行双重加密。

验证目录是否已双重加密

- 在 Web Studio 中：
  a. 导航到 **计算机目录**。
  b. 选择要验证的目录。单击屏幕底部附近的**模板属性**选项卡。
  c. 在 **Azure 详细信息** 下，验证 **磁盘加密集** 中的磁盘加密集 ID。如果目录的 DES ID 为空，则该目录未加密。
  d. 在 Azure 门户中，验证与 DES ID 关联的 DES 的加密类型是平台管理的和客户管理的密钥。
- 使用 PowerShell 命令：
  a. 打开 **PowerShell** 窗口。
  b. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
  c. 使用 `Get-ProvScheme` 获取计算机目录的信息。例如：

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

d. 检索计算机目录的 DES ID 自定义属性。例如：

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-1234-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />
```

e. 在 Azure 门户中，验证与 DES ID 关联的 DES 的加密类型是平台管理的和客户管理的密钥。

使用 Azure 临时磁盘创建目录

要使用临时磁盘，在运行 `New-ProvScheme` 时，必须将自定义属性 `UseEphemeralOsDisk` 设置为 **true**。

> **注意：**
>
> 如果自定义属性 `UseEphemeralOsDisk` 设置为 **false** 或未指定值，则所有预配的 VDA 将继续使用预配的操作系统磁盘。

以下是用于预配方案的自定义属性示例集：

```
"CustomProperties": [

            {

                "Name": "UseManagedDisks",

                "Value": "true"

            },

            {

                "Name": "StorageType",

                "Value": "Standard_LRS"
```

```
        },
        {
            "Name": "UseSharedImageGallery",
            "Value": "true"
        },
        {
            "Name": "SharedImageGalleryReplicaRatio",
            "Value": "40"
        },
        {
            "Name": "SharedImageGalleryReplicaMaximum",
            "Value": "10"
        },
        {
            "Name": "LicenseType",
            "Value": "Windows_Server"
        },
        {
            "Name": "UseEphemeralOsDisk",
            "Value": "true"
        }
```

```
        ],
```

为目录配置临时磁盘

要为目录配置 Azure 临时 OS 磁盘，请在 `Set-ProvScheme` 中使用 `UseEphemeralOsDisk` 参数。将 `UseEphemeralOsDisk` 参数的值设置为 **true**。

> **注意：**
>
> 要使用此功能，您还必须启用参数 `UseManagedDisks` 和 `UseSharedImageGallery`。
>
> 例如：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

配置临时磁盘使用的存储类型

默认情况下，`Standard_LRS` 是临时 OS 磁盘功能使用的存储类型。您可以通过指定 `StorageType` 自定义属性，将存储类型设置为使用 SSD，以提高读取操作的磁盘 IOPS。当前支持的值为 `Standard_LRS`、`StandardSSD_LRS` 和 `Premium_LRS`。

`StorageType` 也可以通过 `Set-ProvScheme` 和 `Set-ProvVMUpdateTimeWindow` 在现有临时计算机上进行更新。

针对临时磁盘的重要注意事项

要使用 `New-ProvScheme` 预配临时操作系统磁盘，请考虑以下限制：

- 用于目录的 VM 大小必须支持临时操作系统磁盘。

- 与 VM 大小关联的缓存或临时磁盘的大小必须大于或等于操作系统磁盘的大小。
- 临时磁盘大小必须大于缓存磁盘大小。

在以下情况下，也请考虑这些问题：

- 创建预配方案时。
- 修改预配方案时。
- 更新映像时。

Azure 专用主机

您可以使用 MCS 在 Azure 专用主机上预配 VM。在 Azure 专用主机上预配 VM 之前：

- 创建主机组。
- 在该主机组中创建主机。
- 确保有足够的主机容量用于创建目录和虚拟机。

您可以通过以下 PowerShell 脚本创建具有主机租用定义的计算机目录：

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

使用 MCS 在 Azure 专用主机上预配虚拟机时，请考虑：

- *专用主机*是目录属性，目录创建后无法更改。Azure 目前不支持专用租用。
- 使用 `HostGroupId` 参数时，需要一个在托管单元区域中预配置的 Azure 主机组。
- Azure 自动放置是必需的。此功能会发出请求以载入与主机组关联的订阅。有关详细信息，请参阅 Azure 专用主机上的 VM 规模集 - 公共预览版。如果未启用自动放置，MCS 将在目录创建期间引发错误。

使用 Azure 计算库映像创建或更新计算机目录

选择用于创建计算机目录的映像时，您可以选择在 Azure 计算库中创建的映像。

要使这些映像显示，您必须：

1. 配置 Citrix 虚拟应用和桌面 站点。
2. 连接到 Azure 资源管理器。
3. 在 Azure 门户中，创建一个资源组。有关详细信息，请参阅使用门户创建 Azure 计算库。
4. 在资源组中，创建 Azure 计算库。
5. 在 Azure 计算库中，创建映像定义。
6. 在映像定义中，创建映像版本。

使用以下 PowerShell 命令创建或更新使用 Azure 计算库中映像的计算机目录：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 选择一个资源组，然后列出该资源组的所有库。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group")
```

4. 选择一个图库，然后列出该图库的所有映像定义。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery")
```

5. 选择一个映像定义，然后列出该映像定义的所有映像版本。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery\sigtestimage.imagedefinitio
n")
```

6. 使用以下元素创建和更新 MCS 目录：
   - 资源组
   - 图库
   - 图库映像定义

- 图库映像版本

有关如何使用远程 PowerShell SDK 创建目录的信息，请参阅 https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/。

配置共享映像库

使用 `New-ProvScheme` 命令创建支持共享映像库的预配方案。使用 `Set-ProvScheme` 命令为预配方案启用或禁用此功能，并更改副本比率和副本最大值。

预配方案中添加了三个自定义属性以支持共享映像库功能：

`UseSharedImageGallery`

- 定义是否使用共享映像库存储已发布的映像。如果设置为 **True**，则映像存储为共享映像库映像，否则映像存储为快照。
- 有效值为 **True** 和 **False**。
- 如果未定义该属性，则默认值为 **False**。

`SharedImageGalleryReplicaRatio`

- 定义机器与图库映像版本副本的比率。
- 有效值为大于 0 的整数。
- 如果未定义该属性，则使用默认值。持久性操作系统磁盘的默认值为 1000，非持久性操作系统磁盘的默认值为 40。

`SharedImageGalleryReplicaMaximum`

- 定义每个图库映像版本的最大副本数。
- 如果未定义该属性，则默认值为 100。
- 如果未定义该属性，则默认值为 100。

> **提示：**
>
> 当使用共享映像库存储 MCS 预配目录的已发布映像时，MCS 会根据目录中的计算机数量、副本比率和最大副本数来设置库映像版本副本计数。副本计数是通过将目录中的计算机数量除以副本比率（向上舍入到最接近的整数值），然后将该值限制为最大副本计数来计算的。例如，如果副本比率为 20，最大值为 5，则 0-20 台计算机创建一个副本，21-40 台计算机创建 2 个副本，41-60 台计算机创建 3 个副本，61-80 台计算机创建 4 个副本，81 台以上计算机创建 5 个副本。

用例：更新共享映像库副本比率和最大副本数

现有计算机目录使用共享映像库。使用 `Set-ProvScheme` 命令更新目录中所有现有计算机和任何未来计算机的自定义属性：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

用例：将快照目录转换为共享映像库目录

对于此用例：

1. 运行 `Set-ProvScheme`，并将 `UseSharedImageGallery` 标志设置为 **True**。可以选择包含 `SharedImageGalleryReplicaRatio` 和 `SharedImageGalleryReplicaMaximum` 属性。
2. 更新目录。
3. 对计算机进行电源循环以强制更新。

例如：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

提示：

参数 `SharedImageGalleryReplicaRatio` 和 `SharedImageGalleryReplicaMaximum` 不是必需的。`Set-ProvScheme` 命令完成后，共享映像库映像尚未创建。一旦目录配置为使用库，下一次目录更新操作会将已发布的映像存储在库中。目录更新命令会创建库、库映像和映像版本。对计算机进行电源循环会更新它们，此时（如果适用）副本计数会更新。从那时起，所有现有的非持久性计算机都将使用共享映像库映像进行重置，所有新预配的计算机都将使用该映像创建。旧快照会在几小时内自动清理。

用例：将共享映像库目录转换为快照目录

对于此用例：

1. 运行 `Set-ProvScheme`，并将 `UseSharedImageGallery` 标志设置为 **False** 或未定义。
2. 更新目录。
3. 对计算机进行电源循环以强制更新。

例如：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

提示：

与从快照更新到共享映像库目录不同，每台计算机的自定义数据尚未更新以反映新的自定义属性。运行以下命令查看原始共享映像库自定义属性：`Get-ProvVm -ProvisioningSchemeName catalog-name`。`Set-ProvScheme` 命令完成后，映像快照尚未创建。一旦目录配置为不使用库，下一次目录更新操作会将已发布的映像存储为快照。从那时起，所有现有的非持久性计算机都将使用快照进行重置，所有新预配的计算机都将从快照创建。对计算机进行电源循环会更新它们，此时自定义计算机数据会更新以反映 `UseSharedImageGallery` 设置为 **False**。旧的共享映像库资产（库、映像和版本）会在几小时内自动清理。

将计算机预配到指定的可用性区域

您可以在 Azure 环境中将计算机预配到特定的可用性区域。您可以使用 PowerShell 实现此目的。

> **注意：**
>
> - 如果未指定区域，MCS 会让 Azure 将计算机放置在该区域内。如果指定了多个区域，MCS 会将计算机随机分布在这些区域中。
> - 如果您在“**存储和许可证类型**”页面上选择 ZRS 作为存储冗余，则会收到一条警告，建议您清除区域选择并让 Azure 管理 VM 可用性区域。仅当您选择具有可用性区域的计算机配置文件或主机组时，才会收到此警告。

通过 POWERSHELL 配置可用性区域

使用 PowerShell，您可以通过 `Get-Item` 查看产品库存项。例如，要查看 *美国东部区域* `Standard_B1ls` 服务产品：

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

要查看区域，请使用该项的 `AdditionalData` 参数：

```
$serviceOffering.AdditionalData
```

如果未指定可用性区域，则计算机的预配方式不会改变。

要通过 PowerShell 配置可用性区域，请使用 `New-ProvScheme` 操作中可用的 **区域** 自定义属性。**区域** 属性定义了用于预配计算机的可用性区域列表。这些区域可以包括一个或多个可用性区域。例如，`<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>` 用于区域 1 和 3。

使用 `Set-ProvScheme` 命令更新预配方案的区域。

如果提供了无效区域，则预配方案不会更新，并且会显示一条错误消息，提供有关如何修复无效命令的说明。

> **提示：**
>
> 如果您指定了无效的自定义属性，则预配方案不会更新，并显示相关错误消息。

存储类型

为使用 MCS 的 Azure 环境中的虚拟机选择不同的存储类型。对于目标 VM，MCS 支持：

- 操作系统磁盘：高级 SSD、SSD 或 HDD
- 回写缓存盘：高级 SSD、SSD 或 HDD

使用这些存储类型时，请考虑以下事项：

- 确保您的 VM 支持所选的存储类型。
- 如果您的配置使用 Azure 临时磁盘，则不会获得回写缓存磁盘设置选项。

> **提示：**
>
> `StorageType` 配置用于操作系统类型和存储帐户。`WBCDiskStorageType` 配置用于回写缓存存储类型。对于普通目录，`StorageType` 是必需的。如果未配置 `WBCDiskStorageType`，则 `StorageType` 将用作 `WBCDiskStorageType` 的默认值。

> 如果未配置 WBCDiskStorageType，则 StorageType 将用作 WBCDiskStorageType 的默认值

配置存储类型

要为 VM 配置存储类型，请在 `New-ProvScheme` 中使用 `StorageType` 参数。将 `StorageType` 参数的值设置为受支持的存储类型之一。

以下是预配方案中 `CustomProperties` 参数的示例集：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />
```

```
</CustomProperties>'
```

启用区域冗余存储

您可以在目录创建期间选择区域冗余存储。它将您的 Azure 托管磁盘同步复制到多个可用区，从而允许您通过利用其他区域中的冗余来从一个区域的故障中恢复。

您可以在存储类型自定义属性中指定 **Premium_ZRS** 和 **StandardSSD_ZRS**。ZRS 存储可以使用现有自定义属性或通过 **MachineProfile** 模板进行设置。ZRS 存储还支持带 `-StartsNow` 和 `-DurationInMinutes -1` 参数的 `Set-ProvVMUpdateTimeWindow` 命令，并且您可以将现有计算机从 LRS 存储更改为 ZRS 存储。

限制：

- 仅支持托管磁盘
- 仅支持高级和标准固态硬盘 (SSD)
- 不支持 `StorageTypeAtShutdown`
- 仅在某些区域可用。
- 大规模创建 ZRS 磁盘时，Azure 的性能会下降。因此，首次开机时，请分批启动计算机（每次少于 300 台）。

将区域冗余存储设置为磁盘存储类型
您可以在初始目录创建期间选择区域冗余存储，也可以在现有目录中更新存储类型。
使用 PowerShell 命令选择区域冗余存储
在 Azure 中使用 `New-ProvScheme` PowerShell 命令创建新目录时，请在 `StorageAccountType` 中使用 `Standard_ZRS` 作为值。 例如：

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_ZRS" />
```

设置此值时，动态 API 会对其进行验证，以确定其是否可以正确使用。如果 ZRS 的使用对您的目录无效，则可能会出现以下异常：

- **StorageTypeAtShutdownNotSupportedForZrsDisks**：StorageTypeAtShutdown 自定义属性不能与 ZRS 存储一起使用。
- **StorageAccountTypeNotSupportedInRegion**：如果您尝试在不支持 ZRS 的 Azure 区域中使用 ZRS 存储，则会发生此异常
- **ZrsRequiresManagedDisks**：区域冗余存储只能与托管磁盘一起使用。

您可以使用以下自定义属性设置磁盘存储类型：

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **注意：**
>
> 在目录创建期间，如果未设置自定义属性，将使用计算机配置文件的操作系统磁盘 `StorageType`。

从计算机配置文件捕获虚拟机和网卡上的诊断设置

您可以在创建计算机目录、更新现有计算机目录以及更新现有虚拟机时，从计算机配置文件捕获虚拟机和网卡上的诊断设置。

您可以创建虚拟机或模板规范作为计算机配置文件源。

关键步骤

1. 在 Azure 中设置所需的 ID。您必须在模板规范中提供这些 ID。
    - 存储帐户
    - 日志分析工作区
    - 采用标准层定价的事件中心命名空间
2. 创建计算机配置文件源。
3. 创建新的计算机目录、更新现有目录或更新现有虚拟机。

在 AZURE 中设置所需的 ID

在 Azure 中设置以下其中一项：

- 存储帐户
- 日志分析工作区
- 具有标准层定价的事件中心命名空间

设置存储帐户

在 Azure 中创建标准存储帐户。在模板规范中，将存储帐户的完整 resourceId 指定为 `storageAccountId`。

一旦虚拟机设置为将数据记录到存储帐户，数据可以在 `insights-metrics-pt1m` 容器下找到。

设置日志分析工作区

创建日志分析工作区。在模板规范中，将日志分析工作区的完整 resourceId 指定为 workspaceId。

一旦虚拟机设置为将数据记录到工作区，就可以在 Azure 的“日志”下查询数据。您可以在 Azure 的“日志”下运行以下命令，以显示资源记录的所有指标的计数：

```
AzureMetrics | summarize Count=count() by ResourceId
```

设置事件中心

执行以下操作以在 Azure 门户中设置事件中心：

1. 创建具有标准层定价的事件中心命名空间。
2. 在命名空间下创建事件中心。
3. 导航到事件中心下的 **捕获**。打开开关以使用 Avro 输出类型进行捕获。
4. 在现有存储帐户中创建新容器以捕获日志。
5. 在模板规范中，按以下格式指定 `eventHubAuthorizationRuleId`：`/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. 指定事件中心的名称。

将 VM 设置为向事件中心记录数据后，数据将捕获到配置的存储容器中。

创建计算机配置文件源

您可以将 VM 或模板规范创建为计算机配置文件源。

创建基于 VM 的计算机配置文件（带诊断设置）

如果要创建 VM 作为计算机配置文件，请首先在模板 VM 本身设置诊断设置。您可以参考 Microsoft 文档 Azure Monitor 中的诊断设置 中提供的详细说明。

您可以运行以下命令来验证现在是否已将诊断设置与 VM 或 NIC 相关联：

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

创建基于模板规范的计算机配置文件（带诊断设置）

如果要使用已启用诊断设置的 VM 并将其导出到 ARM 模板规范中，则这些设置不会自动包含在模板中。您必须在 ARM 模板中手动添加或修改诊断设置。

但是，如果您希望将 VM 作为计算机配置文件，MCS 会确保准确捕获关键诊断设置并将其应用于 MCS 目录中的资源。

1. 创建定义 VM 和 NIC 的标准模板规范。
2. 根据规范添加其他资源以部署诊断设置：Microsoft.Insights diagnosticSettings。对于范围，通过名称和部分 ID 引用模板中的 VM 或 NIC。例如，要在模板规范中创建附加到名为 test-VM 的 VM 的诊断设置，请将范围指定为：

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

3. 使用模板规范作为计算机配置文件源。

创建或更新包含诊断设置的目录

创建计算机配置文件源后，您现在可以使用 `New-ProvScheme` 命令创建计算机目录，使用 `Set-ProvScheme` 命令更新现有计算机目录，并使用 `Request-ProvVMUpdate` 命令更新现有 VM。

页面文件位置确定

页面文件位置根据以下情况确定：

> **注意：**
>
> 默认页面文件位置是操作系统磁盘。

场景	位置
页面文件设置在自定义属性中指定	如自定义属性中指定
临时 OS 磁盘或休眠已启用	操作系统磁盘
虚拟机具有临时磁盘	临时磁盘
MCS I/O 已启用	WBC 磁盘

页文件设置方案

下表描述了在映像准备和预配方案更新期间页文件设置的一些可能方案：

期间	方案	结果
映像准备	您将源映像页文件设置在临时磁盘上，而您在预配方案中指定的虚拟机大小没有临时磁盘	页文件放置在操作系统上
映像准备	您在操作系统磁盘上设置源映像页面文件，而您在预配方案中指定的 VM 大小具有临时磁盘	页面文件放置在临时磁盘上
映像准备	您在临时磁盘上设置源映像页面文件，并在预配方案中启用临时操作系统磁盘	页面文件放置在操作系统磁盘上
预配方案更新	当 VDA 版本早于 2311 时，您尝试更新预配方案	修改页面文件设置并发出警告
预配方案更新	当 VDA 版本为 2311 或更高版本时，您尝试更新预配方案	根据 页面文件位置确定 确定页面文件位置

指定页面文件设置

使用 PowerShell 命令，您可以指定页面文件设置，包括位置和大小。这将覆盖 MCS 根据 页面文件位置确定 确定的页面文件设置。您可以通过在创建计算机目录期间运行以下 `New-ProvScheme` 命令来完成此操作。

重要注意事项

在继续创建目录之前，请考虑以下事项：

- 您必须在 `New-ProvScheme` 命令中提供所有自定义属性（'PageFileDiskDriveLetterOverride'、'InitialPageFileSizeInMB' 和 'MaxPageFileSizeInMB'），或者不提供任何属性。
- Citrix Studio 不支持此功能。
- 初始页面文件大小必须介于 16 MB 和 16777216 MB 之间。
- 最大页面文件大小必须大于或等于初始页面文件大小，且小于 16777216 MB。
- 您可以同时将初始页面文件大小和最大页面文件大小设置为零。

> **注意：**

您可以修改现有目录中新添加的 VM 的页面文件设置，而无需更新主映像。要修改页面文件设置，您需要 VDA 2311 或更高版本。您可以使用 PowerShell 命令修改页面文件设置。有关更多信息，请参阅修改页面文件设置。

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "zijinnet" `

-IdentityPoolName "PageFileSettingExample" `

-ProvisioningSchemeName "PageFileSettingExample" `

-InitialBatchSizeHint 1 `

-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-zijincloud-
resources.resourcegroup\CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3ef
eea88f.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\zijinnet\
\virtualprivatecloud.folder\\East US.region\\virtualprivatecloud.folder\
\neal-zijincloud-resources.resourcegroup\\neal-zijincloud-resources-
vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\zijinnet\\serviceoffering.folder\
\Standard_B2ms.serviceoffering" `

-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="d"/> `

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048"/> `

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196"/> `
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

</CustomProperties>'
```

修改页面文件设置

您可以修改现有目录中新添加的 VM 的页面文件设置，而无需更新主映像。目前，此功能仅适用于 Azure 环境。

要修改页面文件设置，您需要 VDA 2311 或更高版本。您可以使用 PowerShell 命令修改页面文件设置。

以下是您可以在 Azure 环境中修改的各种页面文件设置：

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`
- `MaxPageFileSizeInMB`

修改现有目录的页面文件设置

要修改现有计算机目录的页面文件设置，请运行 `Set-ProvScheme` 命令。在这种情况下，更新仅应用于添加到目录的新 VM。例如：

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="StandardSSD_LRS" />

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="D" />

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
```

```
Value="2048" />

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property  xsi:type="StringProperty" Name="Zones" Value="1" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
test-group1" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

注意：

如果启用回写缓存并尝试使用 PowerShell 命令将 `PageFileDiskDriveLetterOverride` 设置为 `C:`，则 MCS IO 驱动程序会自动将页面文件重定向到正确的磁盘驱动器，而不是 `C:`。

使用 Azure Spot VM 创建目录

Azure Spot VM 允许您利用 Azure 未使用的计算容量，从而显著节省成本。但是，分配 Azure Spot VM 的能力取决于当前的容量和定价。因此，Azure 可能会根据 逐出策略 逐出正在运行的 VM、无法创建 VM 或无法启动 VM。因此，Azure Spot VM 适用于某些非关键应用程序和桌面。有关详细信息，请参阅 使用 Azure Spot 虚拟机。

限制

- 并非所有 VM 大小都支持 Azure Spot VM。有关详细信息，请参阅限制。

  您可以运行以下 PowerShell 命令来检查 VM 大小是否支持 Spot VM。如果 VM 大小支持 Spot VM，则 `SupportsSpotVM` 为 **True**。

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-
  conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering").
  AdditionalData
  ```

- 目前，Azure Spot VM 不支持休眠。

要求

为 Azure Spot VM 目录创建计算机配置文件源（VM 或模板规范）时，您必须选择 Azure Spot 实例（如果使用 VM）或将 `priority` 设置为 `Spot`（如果使用模板规范）。

使用 AZURE SPOT VM 创建目录的步骤

1. 创建计算机配置文件源（VM 或启动模板）。

   - 有关使用 Azure 门户创建 VM 的信息，请参阅 使用 Azure 门户部署 Azure 现成虚拟机。
   - 要创建模板规范，请在模板规范的 **resources > type: Microsoft.Compute/virtualMachines > properties** 下添加以下属性。例如：

     ```
     "priority": "Spot",

     "evictionPolicy": "Deallocate",

     "billingProfile": {

     "maxPrice": 0.01

     }
     ```

注意：

- 逐出策略可以是 **Deallocate** 或 **Delete**。
- 对于非持久性 VM，MCS 始终将逐出策略设置为 **Delete**。如果 VM 被逐出，它将与任何非持久性磁盘（例如，OS 磁盘）一起被删除。任何持久性磁盘（例如，身份磁盘）都不会被删除。但是，如果目录类型是持久性的，或者 `PersistOsDisk` 自定义属性设置为 True，则 OS 磁盘是持久性的。同样，如果 `PersistWbc` 自定义属性设置为 **True**，则 WBC 磁盘是持久性的。
- 对于持久性 VM，MCS 始终将逐出策略设置为 Deallocate。如果 VM 被逐出，它将被解除分配。磁盘不会发生任何更改。
- 最高价格是您每小时愿意支付的价格。如果您使用的是 **仅容量**，则此值为 **-1**。最高价格只能为 null、-1 或大于零的十进制数。有关详细信息，请参阅 定价。

2. 您可以运行以下 PowerShell 命令来检查计算机配置文件是否启用了 Azure Spot VM。如果 `SpotEnabled` 参数为 **True** 且 `SpotEvictionPolicy` 设置为 **Deallocate** 或 **Delete**，则表示计算机配置文件已启用 Azure Spot VM。例如，

   - 如果计算机配置文件源是 VM，请运行以下命令：

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-delete.vm"). AdditionalData
     ```

   - 如果计算机配置文件源是模板规范，请运行以下命令：

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-templatespec.templatespec\14.0.0-spot-delete.templatespecversion").AdditionalData
     ```

3. 使用具有 `New-ProvScheme` PowerShell 命令的计算机配置文件创建计算机目录。

您可以使用 `Set-ProvScheme` 命令更新目录。您还可以使用 PowerShell 命令 `Set-ProvVmUpdateTimeWindow` 更新现有 VM。计算机配置文件将在下次开机时更新。

正在运行的 AZURE SPOT VM 上的逐出

如果计算容量不可用或每小时价格高于配置的最大价格，Azure 会逐出正在运行的 Spot VM。默认情况下，您不会收到逐出通知。VM 会简单地冻结，然后被逐出。Microsoft 建议使用计划事件来监视逐出。请参阅 持续监视逐出。您还可以从 VM 内部运行脚本，以便在逐出前收到通知。例如，Microsoft 有一个用 Python 编写的轮询脚本 ScheduledEvents.cs。

故障排除

- 您可以使用 `Get-ProvVM` 命令在预配的 VM 的 customMachineData 中查看 Spot VM 属性。如果优先级字段设置为 **Spot**，则表示正在使用 Spot。
- 您可以在 Azure 门户中检查 VM 是否正在使用 Spot：

  a. 在 Azure 门户中查找 VM。

  b. 转到“**概述**”页面。

  c. 滚动到底部并找到“**Azure Spot**”部分。

  - 如果未使用 Spot，则此字段为空。
  - 如果正在使用 Spot，则会设置“**Azure Spot**”和“**Azure Spot 逐出策略**”字段。

1. 您可以在“配置”页面上查看 VM 的计费配置文件或每小时最高价格。

配置备份 VM 大小

公共云可能会出现特定 VM 大小容量不足的情况。当 Azure 容量不足时，MCS 会回退到预配置的备份 VM 大小列表。此精选列表由客户根据其工作负载要求量身定制，可增加在 VM 之前处于休眠状态时，其中一个大小在开机或恢复时具有足够容量的可能性。

启动电源操作时，MCS 会实施自动回退序列以确保高可用性。工作流程如下：

1. 启动：用户或管理员通过 Web Studio 发出 **PowerOn** 或 **Resume** 命令。
2. 异常监控：MCS 尝试使用主配置启动 VM。它监控特定的 Azure 容量异常，例如“配额超出”、“分配失败”或“区域分配失败”以及“SKU 不可用”（可以概括地说，我们监控 Azure 的任何容量或分配故障）。
3. 顺序回退：如果发生上述错误之一，MCS 会自动按顺序遍历 BackupVmConfiguration 列表，直到 VM 成功启动。如果 BackupVmConfiguration 中的所有大小都失败，则电源操作将被标记为失败。
4. 更新与重新创建逻辑：
    - 直接更新：在大多数情况下，MCS 会对备份 SKU 执行简单的 VM 大小更新，然后启动 VM。
    - 删除并重新创建：为了保持环境完整性，某些转换需要删除现有 VM 并在其位置创建新 VM。这发生在以下情况：
        - 在 Spot 和常规 VM 类型之间切换。
        - 在支持资源磁盘（临时存储）的 VM 大小和不支持资源磁盘的 VM 大小之间切换。
5. 数据持久性与恢复：在“删除并重新创建”操作期间，如果所有备份大小也因 Azure 容量严重短缺而失败，VM 可能会暂时从 Azure 门户中消失。但是，不会发生数据丢失。在下一次 PowerOn 尝试时，MCS 将使用原始设置重新创建 VM，并重新附加现有的操作系统、身份和数据磁盘。
6. Spot VM 计费和 MaxPrice 行为 如果您的主要配置使用具有 Spot 优先级和特定计费配置文件 (MaxPrice) 的计算机配置文件 (VM 模板)，则在回退期间适用以下逻辑：
    - 主大小：使用您的计算机配置文件中定义的 MaxPrice。逐出基于价格或容量。
    - 备份 Spot 大小：BackupVmConfiguration 属性当前不支持为每个 SKU 提供唯一的 `MaxPrice` 输入，MCS 按如下方式处理转换：
    - MaxPrice 重置：MCS 将 MaxPrice 设置为 -1。
    - 逐出策略转变：这会将 Azure 逐出行为从基于价格更改为基于容量。

- 定价：您将按当前 Spot 价格计费，最高不超过该备份 SKU 的标准即用即付 (PAYG) 费率。这可确保仅当 Azure 确实耗尽物理容量时才逐出 VM，而不是因为价格波动。

7. 备份状态的持久性：启动后，VM 在会话期间保持备份大小，直到处理关机或休眠请求。
8. 恢复主大小：在下次开机或恢复时，MCS 始终尝试将 VM “归位”到其主要服务产品（如目录或计算机配置文件中所定义）。如果主大小仍然不可用，则回退序列会重复。

休眠的挑战

Azure 不允许更改处于休眠状态的 VM 的大小，如 一般限制 中所述。VM 必须处于“已停止”状态。因此，在更改大小之前，MCS 会发出解除分配请求以清除休眠状态，这会导致 VM 的休眠状态丢失。然后，MCS 循环遍历备份大小，更新 VM 大小，并将其开机。

备份 VM 大小不支持的方案

不支持以下配置：

- 对于持久性 VM，不支持以下方案：
  - VM 使用 DiskControllerType SCSI，但备份 VM 大小仅支持 DiskControllerType NVMe。
  - VM 使用 DiskControllerType NVMe，但备份 VM 大小仅支持 DiskControllerType SCSI。
- 对于启用了 MCSIO 的非持久性 VM，如果回写缓存磁盘使用资源磁盘临时存储，则不支持切换到没有临时存储的大小。

配置备份 VM 大小的先决条件

如果以下任何条件未满足，则会抛出错误。

- 仅当计算机配置文件在计算机目录上使用时才支持。
- 类型是可选的，可以是 Spot 或 Regular。如果未指定，则默认为 Regular。
- ServiceOffering 的每个组合都必须是唯一的，以避免重复配置。
- 区域配额必须有足够的内核用于 ServiceOffering。
- 网络接口数量不得超过 ServiceOffering 允许的最大值。
- 此 BackupVmConfiguration 列表中的 ServiceOfferings 必须与当前的自定义属性、主映像的功能和 MachineProfile 兼容。一些失败场景包括：
  - Azure 专用主机：如果使用专用主机，主机组中的主机必须支持 ServiceOffering。
  - 临时操作系统磁盘：如果自定义属性中启用了临时操作系统磁盘，ServiceOffering 必须支持临时操作系统磁盘。
  - 高级存储：如果自定义属性中指定了高级存储，ServiceOffering 必须支持高级存储。
  - 加速网络：如果 MachineProfile 中启用了加速网络，ServiceOffering 必须支持加速网络。

- 主机磁盘加密：如果 MachineProfile 中启用了主机加密，ServiceOffering 必须支持主机加密。
- 临时存储：如果正在使用 MCSIO 并且回写缓存位于临时磁盘上，则不允许使用没有临时存储的 VM 大小。
- HyperVGeneration：ServiceOffering 必须与 MasterImageVM 中指定的 VM 代次（1 或 2）兼容。
- 可信启动：如果 MachineProfile 中启用了可信启动，ServiceOffering 必须支持可信启动。
- 机密虚拟机：如果在 MachineProfile 中启用，ServiceOffering 必须支持机密虚拟机。

创建具有备份虚拟机大小的目录

> **注意：**
>
> 为解决 Studio UI 冻结问题，请在运行 PowerShell 命令时将所有单引号替换为 `"`。

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 创建代理目录。此目录将填充即将创建的计算机。
4. 创建身份池。这将成为为即将创建的计算机创建的 AD 帐户的容器。
5. 使用计算机配置文件创建预配方案。请参阅 如何配置备份配置。
6. 使用预配方案的唯一 ID 更新 `BrokerCatalog`。
7. 创建虚拟机并将其添加到目录。

更新现有目录

您可以使用 `Set-ProvScheme` 命令更新预配方案。请参阅 如何配置备份配置。

更新现有虚拟机

您可以使用 `Set-ProvVMUpdateTimeWindow` PowerShell 命令更新目录中的现有虚拟机。此命令会在给定时间窗口内的下次开机时更新从与目录关联的预配方案创建的虚拟机。例如：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartTimeInUTC "3/12/2022 3am" -DurationInMinutes 60`
```

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

您可以使用 `Set-ProvVM` 命令为选定数量的现有 MCS VM 配置备份 VM 大小列表。但是，要应用更新，请使用 `Set-ProvVMUpdateTimeWindow` 为 VM 设置更新时间窗口，并在该窗口内启动 VM。例如，

1. 运行 `Set-ProvVM` 命令，为选定的现有 MCS VM 配置备份 VM 大小列表。例如：

```
Set-ProvVM -ProvisioningSchemeName "name" -VMName "Vm-001"

-CustomProperties

"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`"/>

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
Name=`"BackupVmConfiguration`" Value=`"[{&quot;ServiceOffering&quot;:
&quot;Standard_D2as_v4&quot;, &quot;Type&quot;: &quot;Spot&quot;},
{&quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;,
&quot;Type&quot;: &quot;Regular&quot;}, {&quot;ServiceOffering&quot;:
&quot;Standard_D2s_v3&quot;, &quot;Type&quot;: &quot;Spot&quot;}]`"/>
</CustomProperties>"
```

2. 运行 `Set-ProvVMUpdateTimeWindow` 命令以应用更新。例如：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

复制所有资源上的标签

您可以将计算机配置文件中指定的标签复制到新 VM 或计算机目录中现有 VM 的所有资源，例如多个 NIC 和磁盘（操作系统磁盘、身份磁盘和回写缓存磁盘）。计算机配置文件源可以是 VM 或 ARM 模板规范。

注意：

您必须在标签上添加策略（请参阅分配标签合规性策略定义）或在计算机配置文件源中添加标签，以保留资源上的标签。

先决条件

创建计算机配置文件源（VM 或 ARM 模板规范），以便在该 VM 的 VM、磁盘和 NIC 上具有标签。

- 如果您希望将 VM 作为计算机配置文件输入，请在 Azure 门户中将标签应用于 VM 和所有资源。请参阅使用 Azure 门户应用标签。
- 如果您希望将 ARM 模板规范作为计算机配置文件输入，请在每个资源下添加以下标签块。

```
 "tags": {

"TagC": "Value3"

},
```

注意：

模板规范中最多可以有一个磁盘，并且至少有一个 NIC。

将标签复制到新计算机目录中 VM 的资源

1. 创建以 VM 或 ARM 模板规范作为计算机配置文件输入的非持久性或持久性目录。
2. 将 VM 添加到目录并将其开机。您必须看到机器配置文件中指定的标签已复制到该 VM 的相应资源。

注意：

> 如果机器配置文件中提供的 NIC 数量与您希望 VM 使用的 NIC 数量不匹配，则会收到错误。

修改现有 VM 资源上的标签

1. 创建一个包含所有资源上标签的机器配置文件。
2. 使用更新的机器配置文件更新现有机器目录。例如：

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName>
-MachineProfile <PathToYourMachineProfile>
```

3. 关闭要应用更新的 VM。
4. 请求 VM 的计划更新。例如：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <YourCatalogName>  -
VMName machine1 -StartsNow -DurationInMinutes -1
```

5. 打开 VM。
6. 您必须看到机器配置文件中指定的标签已复制到相应的资源。

> **注意：**
>
> 如果机器配置文件中提供的 NIC 数量与 `Set-ProvScheme` 中提供的 NIC 数量不匹配，则会收到错误。

创建预格式化的 WBC 磁盘目录

您可以创建预格式化的 WBC 磁盘目录，以提高预配计算机的启动性能。要实现此功能，请创建启用 WBC 的 Azure 目录，并包含一个额外的自定义属性 `PreformatWriteBackCache` 作为 `True`。

您可以使用 `Set-ProvScheme` 命令更新现有目录，以更新 WBC 磁盘大小。

此功能与映像管理工作流兼容，在该工作流中，MCS 将主映像阶段与整个预配工作流分离。有关映像管理的信息，请参阅映像管理。

创建启用了 WBC 且 `PreformatWriteBackCache` 为 `True` 的 Azure 目录的示例：

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>

'@



New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `

-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

更新现有目录的 WBC 磁盘缓存大小的示例：

```
Set-ProvScheme -ProvisioningSchemeName provisioningschemename
-WriteBackCacheDiskSize 127
```

对于 MCS 预配的 Citrix Provisioning™ 目录，在关机时删除 WBC 磁盘

在 Azure 中创建 MCS 预配的 Citrix Provisioning 目录时，可以将 WBC 磁盘预配为非持久性（`PersistWBC` 为 False）。此配置有助于在关闭 Azure 中 MCS 预配的 Citrix Provisioning 目录的 VM 后删除回写缓存 (WBC) 磁盘。

条件：

您必须将自定义属性 `PreformatWriteBackCache` 设置为 `True` 才能使此功能正常工作。

创建 Azure 目录的示例，其中 `PersistWBC` 为 `False` 且 `PreformatWriteBackCache` 为 `True`：

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>

'@



New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `

-NetworkMapping $networkMapping `
```

```
-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

您还可以使用 `Set-ProvScheme` 命令更新现有目录，以更新 `PersistWBC` 自定义属性。

预配数据磁盘

您可以为 Azure 中 MCS 计算机目录的 MCS 创建的持久性或非持久性 VM 创建并分配持久性数据磁盘。

数据磁盘必须从托管磁盘作为映像源进行预配。

数据磁盘属性

如果未在自定义属性中指定数据磁盘的属性，则数据磁盘将从自定义属性或操作系统磁盘模板派生属性。

- 从自定义属性派生的属性
  - `DiskEncryptionSetId`
  - `Zones`
  - `StorageType`
- 如果未在自定义属性中指定，则从操作系统磁盘模板派生的属性
  - `DiskEncryptionSetId`
  - `Zones`
  - `StorageType`

注意：

- 如果未在自定义属性或操作系统磁盘模板中指定区域冗余存储 (ZRS)，则数据磁盘将放置在与操作系统磁盘和身份磁盘相同的区域中。
- 标签仅从操作系统磁盘模板派生。

限制

当前不支持以下操作：

- 预配多个数据磁盘。
- 预配非持久性数据磁盘。
- 使用模板创建数据磁盘。
- 修改现有目录和虚拟机以使用数据磁盘。
- 重置数据磁盘。
- 数据磁盘的映像更新。
- 使用托管磁盘以外的源。
- 将数据磁盘存储在 Azure 计算库 (ACG) 中。
- 将 `StorageTypeAtShutdown` 用于数据磁盘

创建带数据磁盘的目录

在 `New-ProvScheme` PowerShell 命令中包含以下参数，以预配带数据磁盘的 MCS 计算机目录。

- `DataDisk`：有效 ManagedDisk 类型清单项的路径。
- `DataDiskPersistence`：指示 `DataDisk` 是持久的还是非持久的。但是，目前仅支持持久性数据磁盘。

例如：

```
New-ProvScheme  -CleanOnBoot -HostingUnitName "<HostingUnitName >"
-IdentityPoolName "<IdentityPoolName >" -InitialBatchSizeHint 1
-MasterImageVM disk.manageddisk -NetworkMapping <NetworkMapping >
-ProvisioningSchemeName "<ProvisioningSchemeName >" -DataDisk "XDHyp:
\HostingUnits\Azure-Resources-1\image.folder\<resourcegroupname>\xxxx-
datadisk.manageddisk"  -DataDiskPersistence "Persistent"  -Scope @()
-VMCpuCount 4  -VMMemoryMB 6144  -TenancyType Shared  -FunctionalLevel
"L7_20"
```

确定数据磁盘是否正在使用

执行以下操作以验证数据磁盘是否已分配给虚拟机：

- 运行 `Get-ProvVm` 并检查虚拟机的 `CustomVmData`。如果虚拟机正在使用数据磁盘，则会有一个角色为 `DiskRole.DataDisk` 的磁盘记录。
- 检查 Azure 门户中虚拟机下是否存在数据磁盘。

删除数据磁盘

如果删除目录，则数据磁盘将被删除，除非使用 `forgetVM` 或 `purgeDBOnly` 选项。如果删除 VM，则数据磁盘将被删除，除非使用 `forgetVM` 或 `purgeDBOnly` 选项。

从非托管磁盘迁移到托管磁盘

在 September 30, 2025，Azure 将正式停用非托管磁盘（即 VHD）。任何使用非托管磁盘的现有 VM 都将在截止日期后停止并解除分配。

但是，您可以将 MCS 预配的 VM 从非托管磁盘迁移到托管磁盘，这有助于避免因 Azure 的非托管磁盘停用计划而导致的服务中断。

连接到 VM 的所有非托管磁盘都将转换。这包括身份磁盘、操作系统磁盘和 WBC 磁盘（如果使用）。

有关 Azure 非托管磁盘停用计划的更多信息，请参阅 在 September 30, 2025 之前迁移 Azure 非托管磁盘。

用例

此功能适用于持久性和非持久性 MCS 预配的目录。

它还支持按需和非按需（旧版）VM 的迁移：

- 按需 VM：将现有磁盘从非托管磁盘转换为托管磁盘，以与 Azure 的更新支持保持一致。
- 非按需（旧版）VM：旧版或非按需 VM 仅支持非托管磁盘。使用此功能将旧版 VM 转换为按需 VM，同时迁移到托管磁盘。

有关按需预配的更多信息，请参阅 Azure 按需预配。

限制

- 一旦计算机目录或 VM 转换为托管磁盘，就无法再转换回非托管磁盘
- 对于非按需（旧版）VM，迁移过程包括将其转换为按需预配。您不能只转换磁盘并继续使用非按需 VM。

重要注意事项

- 转换不会自动发生。它作为开机操作的一部分进行。
- 如果为 VM 请求了多个更新，则磁盘转换优先。其他更新将推迟到后续开机时进行。
- VM 成功转换并开机后，将清理 VM 的 VHD 以节省成本。存储帐户本身不会被清理。
    - 存储帐户中可能仍然存在基本磁盘。您可以运行目录更新，然后会创建一个新的快照（或 ACG）基本磁盘。
    - 目录中的所有 VM 转换完毕并创建新的基本磁盘后，即可删除空存储帐户。

所需权限

您需要在 Azure 服务主体上拥有以下权限，才能允许从非托管磁盘转换为托管磁盘：

```
Microsoft.Compute/virtualMachines/convertToManagedDisks/write
```

配置步骤

对于按需目录：

1. 运行 `Set-ProvScheme`（或针对持久性 VM 运行 `Set-ProvVM`）以将 `UseManagedDisks` 更新为 `True`。例如：

   ```
   Set-ProvScheme -ProvisioningSchemeName "<provscheme-name>"
   -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
   2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
   instance`"><Property xsi:type=`"StringProperty`"
   Name=`"UseManagedDisks`" Value=`"true`" /></CustomProperties>"
   ```

   ```
   Set-ProvVM -ProvisioningSchemeName "<provscheme-name>" -VMName "<vm-
   name>" -CustomProperties "<CustomProperties xmlns=`"http://
   schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
   www.w3.org/2001/XMLSchema-instance`"><Property
   xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /
   ></CustomProperties>"
   ```

2. 运行 `Set-ProvVMUpdateTimeWindo`w` 以应用更新。在此示例中，更新将在 VM 下次开机时应用。

   ```
   Set-ProvVmUpdateTimeWindow -ProvisioningSchemeName "<provscheme-name>"
   -VMName "<vm-name>"
   ```

3. 启动 VM。

对于非按需（旧版）目录：

1. 运行 `Set-ProvScheme`（或针对持久性 VM 运行 `Set-ProvVM`）以将 `Set DeploymentSchema` 配置为 `1.1`。例如：

   ```
   Set-ProvScheme -ProvisioningSchemeName "<provscheme-name>"
   -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
   2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
   ```

```
instance`"><Property xsi:type=`"StringProperty`"
Name=`"DeploymentSchema`" Value=`"1.1`" /></CustomProperties>"
```

```
Set-ProvVM -ProvisioningSchemeName "<provscheme-name>" -VMName "<vm-
name>" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"DeploymentSchema`" Value=`"1.1`" /
></CustomProperties>
```

2. 运行 `Set-ProvVMUpdateTimeWindow` 以应用更新。在此示例中，更新将在 VM 下次开机时应用。

```
Set-ProvVmUpdateTimeWindow -ProvisioningSchemeName "<provscheme-name>"
-VMName "<vm-name>"
```

3. 启动 VM。

故障排除

如果 VM 未能从非托管磁盘转换为托管磁盘：

- 验证 `UseManagedDisks` 或 `DeploymentSchema` 自定义属性是否已正确设置：
  - 如果使用 `Set-ProvScheme`，请通过运行 `Get-ProvScheme` 验证 ProvScheme 自定义属性。有关详细信息，请参阅 Get-ProvScheme。
  - 如果使用 `Set-ProvVM`，请通过运行 `Get-ProvVMConfiguration` 验证 VM 是否具有包含更新的自定义属性的新配置。有关详细信息，请参阅 Set-ProvVM。
- 验证您的 Azure 服务主体中是否存在以下权限：
  - `Microsoft.Compute/virtualMachines/convertToManagedDisks/write`
- 运行 `Get-ProvOperationEvent` 以查看预配方案的任何警告。有关详细信息，请参阅 Get-ProvOperationEvent。例如：

```
Get-ProvOperationEvent -LinkedObjectType ProvisioningScheme
-LinkedObjectUid <your-provscheme-id>
```

下一步

- 如果这是创建的第一个目录，Web Studio 将引导您创建交付组

- 要查看整个配置过程，请参阅安装和配置
- 要管理目录，请参阅管理计算机目录 和管理 Microsoft Azure 目录

更多信息

- 创建和管理连接与资源
- 连接到 Microsoft Azure 资源管理器
- 创建计算机目录

创建微软系统中心虚拟机管理器目录

(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-create.html) 介绍了用于创建计算机目录的向导。以下信息涵盖了 Microsoft System Center Virtual Machine Manager (VMM) 虚拟化环境的特定详细信息。

> **注意：**
>
> 在创建 VMM 目录之前，您需要完成与 VMM 的连接创建。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections/connection-mscvmm.html)。

创建主 VM

1. 在主 VM 上安装 VDA，然后选择优化桌面以提高性能的选项。
2. 为主 VM 创建快照以用作备份。
3. 创建虚拟桌面。

SMB 3 文件共享上的 MCS

对于使用 MCS 在 SMB 3 文件共享上创建的用于 VM 存储的计算机目录，请确保凭据满足以下要求。这些要求可确保来自 Controller 的 Hypervisor 通信库 (HCL) 的调用成功连接到 SMB 存储：

- VMM 用户凭据必须包含对 SMB 存储的完全读写访问权限。
- VM 生命周期事件期间的存储虚拟磁盘操作通过 Hyper-V 服务器使用 VMM 用户凭据执行。

使用 SMB 存储时，请从 Controller 到各个 Hyper-V 计算机启用身份验证凭据安全支持提供程序 (CredSSP)。对于 VMM 2012 SP1 和 Windows Server 2012 上的 Hyper-V，请使用此过程。有关详细信息，请参阅 CTX137465。

HCL 使用 `CredSSP` 打开与 Hyper-V 计算机的连接。此功能将 Kerberos 加密的用户凭据传递给 Hyper-V 计算机。远程 Hyper-V 计算机上的会话中的 **PowerShell** 命令使用提供的凭据运行。在这种情况下，使用 VMM 用户的凭据，以便与存储的通信命令正常工作。

以下任务使用源自 HCL 的 PowerShell 脚本，然后将这些脚本发送到 Hyper-V 计算机以对 SMB 3.0 存储执行操作。

- **整合主映像**：主映像创建 MCS 预配方案（计算机目录）。它克隆并平展主 VM，以便从创建的新磁盘创建 VM（并删除对原始主 VM 的依赖）。

  root\\virtualization\\v2 命名空间上的 ConvertVirtualHardDisk

  示例：

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

- **创建差异磁盘**：从通过整合主映像生成的主映像创建差异磁盘。然后将差异磁盘附加到新的 VM。

  root\\virtualization\\v2 命名空间上的 CreateVirtualHardDisk

  示例：

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

- **上传身份磁盘**：HCL 无法直接将身份磁盘上传到 SMB 存储。因此，Hyper-V 计算机必须将身份磁盘上传并复制到存储。由于 Hyper-V 计算机无法从 Controller 读取磁盘，因此 HCL 必须首先通过 Hyper-V 计算机复制身份磁盘，如下所示。

  a. HCL 通过管理员共享将身份上载到 Hyper-V 计算机。

  b. Hyper-V 计算机通过在 PowerShell 远程会话中运行的 PowerShell 脚本将磁盘复制到 SMB 存储。在 Hyper-V 计算机上创建一个文件夹，并且该文件夹的权限仅锁定给 VMM 用户（通过远程 PowerShell 连接）。

c. HCL 从管理员共享中删除文件。

d. 当 HCL 完成将身份磁盘上传到 Hyper-V 计算机后，远程 PowerShell 会话会将身份磁盘复制到 SMB 存储。然后将其从 Hyper-V 计算机中删除。

如果身份磁盘文件夹被删除，则会重新创建该文件夹，以便可以重复使用。

- **下载身份磁盘**：与上传一样，身份磁盘通过 Hyper-V 计算机传递到 HCL。如果不存在，以下过程将在 Hyper-V 服务器上创建一个仅具有 VMM 用户权限的文件夹。

  a. Hyper-V 计算机通过 PowerShell 脚本将磁盘从 SMB 存储复制到本地 Hyper-V 存储。此脚本在 PowerShell V3 远程会话中运行。

  b. HCL 将磁盘从 Hyper-V 计算机的管理员共享读取到内存中。

  c. HCL 从管理员共享中删除文件。

使用计算机配置文件创建目录

您可以使用计算机配置文件在 System Center Virtual Machine Manager (SCVMM) 环境中创建和更新 MCS 计算机目录。您可以启用 vTPM。您还可以将计算机配置文件 VM 的自定义标记添加到预配的 VM。

重要注意事项

- 主映像只能是快照，不能是 VM。
- 您只能使用 VM 作为计算机配置文件源。
- 您可以从 Hyper-V 控制台配置 VTPM，而不是从 SCVMM 控制台。
- 如果主映像已启用 vTPM，则必须在计算机配置文件源上启用 vTPM。
- vTPM 仅在第 2 代计算机上受支持。
- 如果单独提供，以下参数将覆盖计算机配置文件中捕获的值：
  - VMCpuCount
  - VMMemoryMB
  - 磁盘存储
- 自定义标签仅从计算机配置文件继承，而不从主映像继承。`CitrixProvisioningSchemeId` 标签默认添加到 VM。如果您不想包含 `CitrixProvisioningSchemeId` 标签，则在创建托管单元时添加 `-NoVmTagging` 参数。示例：

```
New-Item -HypervisorConnectionName  $ConnectionName `

    -NetworkPath @($NetworkPath) `
```

```
    -Path @($HostingUnitPath) `

    -PersonalvDiskStoragePath @() `

    -RootPath $RootPath `

    -StoragePath @($StoragePath) `

    -NoVmTagging

    ```
```

- 您可以使用 `Set-ProvScheme` 命令更新现有目录。
- 启用 MCSIO 后，您可以在创建 MCS 目录后更新内存和磁盘缓存大小。

使用机器配置文件创建计算机目录

1. 创建一个虚拟机作为机器配置文件源。有关详细信息，请参阅在 VMM 结构中预配虚拟机。选定后，无法更改**代**。您可以在 SCVMM 中执行以下操作：
    - 要启用 vTPM：
        a. 创建虚拟机后，登录到 Hyper-V 主机并在**Hyper-V 管理器**下找到您的虚拟机。
        b. 右键单击虚拟机，然后转到**设置**。
        c. 在**安全性**下，选中**启用受信任的平台模块**复选框。
2. 打开 **PowerShell** 窗口。
3. 运行 `asnp citrix®*` 以加载 Citrix 特定的 PowerShell 模块。
4. 创建一个 Broker 目录。此目录将填充即将创建的计算机。
5. 创建一个身份池。这将成为为即将创建的计算机创建的 AD 帐户的容器。
6. 使用机器配置文件创建预配方案。例如：

```
New-ProvScheme -HostingUnitName "<hostingunit name>"

-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<path
to the checkpoint/snapshot>"
```
```

```
-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<path
to the machine profile VM>"
```

7. 使用预配方案的唯一 ID 更新 Broker 目录。
8. 创建虚拟机并将其添加到目录。

更新现有目录

您可以使用 Set-ProvScheme 命令更新现有目录。例如：

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
"XDHyp:\<path to the machine profile VM>"
```

删除虚拟机

您可以选择从目录中移除虚拟机，但不会从 SCVMM 中删除该虚拟机。在这种情况下，`CitrixProvisioningSchemeId` 标记仅从虚拟机中移除。自定义标记不会从虚拟机中删除。您可以使用 Web Studio 或 PowerShell 命令移除虚拟机。

使用 Web Studio 移除虚拟机

1. 选择虚拟机并右键单击。
2. 单击 **删除**。
3. 选择 **从目录中删除虚拟机，但不要删除虚拟机**。

使用 PowerShell 命令

`Remove-ProvVM` 带有 `ForgetVM` 参数。有关详细信息，请参阅：

- 删除标记
- 删除没有管理程序访问权限的计算机

下一步操作

- 如果这是创建的第一个目录，Web Studio 会引导您创建交付组
- 要查看整个配置过程，请参阅安装和配置
- 要管理目录，请参阅管理计算机目录和管理 Microsoft System Center Virtual Machine Manager 目录

更多信息

- 创建和管理连接与资源
- 连接到 微软系统中心虚拟机管理器

- 创建计算机目录

创建 Nutanix 目录

(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-create.html) 介绍了创建计算机目录的向导。以下信息涵盖了 Nutanix 虚拟化环境特有的详细信息。

> **注意：**
>
> 在创建 Nutanix 目录之前，您需要完成与 Nutanix 的连接创建。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections/connection-nutanix.html)。

使用 Nutanix 计算机模板版本创建计算机目录

使用 Citrix 管理的 Nutanix AHV Prism Central 主机连接创建 MCS 预配的计算机目录时，基础映像是根据 Nutanix VM 模板版本创建的。一个主要优点是 Nutanix Prism Central 允许 VM 模板在多个群集之间使用。因此，Citrix 管理员可以将单个 Nutanix VM 模板版本用作多个 MCS 计算机目录的主 VM，即使这些目录位于不同的 Nutanix 群集上。

您还可以选择模板版本作为计算机配置文件的源。主映像的模板版本默认为新目录的计算机配置文件。但是，您可以更改计算机配置文件的模板版本。以下硬件属性是从计算机配置文件中捕获的：CPU、内存、每插槽核心数、GPU 和类别。您甚至可以选择指定 CPU、内存、每插槽核心数属性来覆盖所选计算机配置文件的设置。

> **注意：**
>
> 类别是键值对，用于对虚拟机、群集和映像等实体进行分组和管理，以应用策略和自动化。

> 在创建目录之前，请创建主 VM，并将其转换为 Nutanix Prism Central 中的 VM 模板版本。有关步骤，请参阅 Nutanix 文档。

您可以使用以下方式创建目录：

- Web Studio。您还可以使用现有虚拟机创建目录。请参阅使用现有计算机创建计算机目录（电源管理）
- (#create-a-machine-catalog-using-powershell-commands)

限制

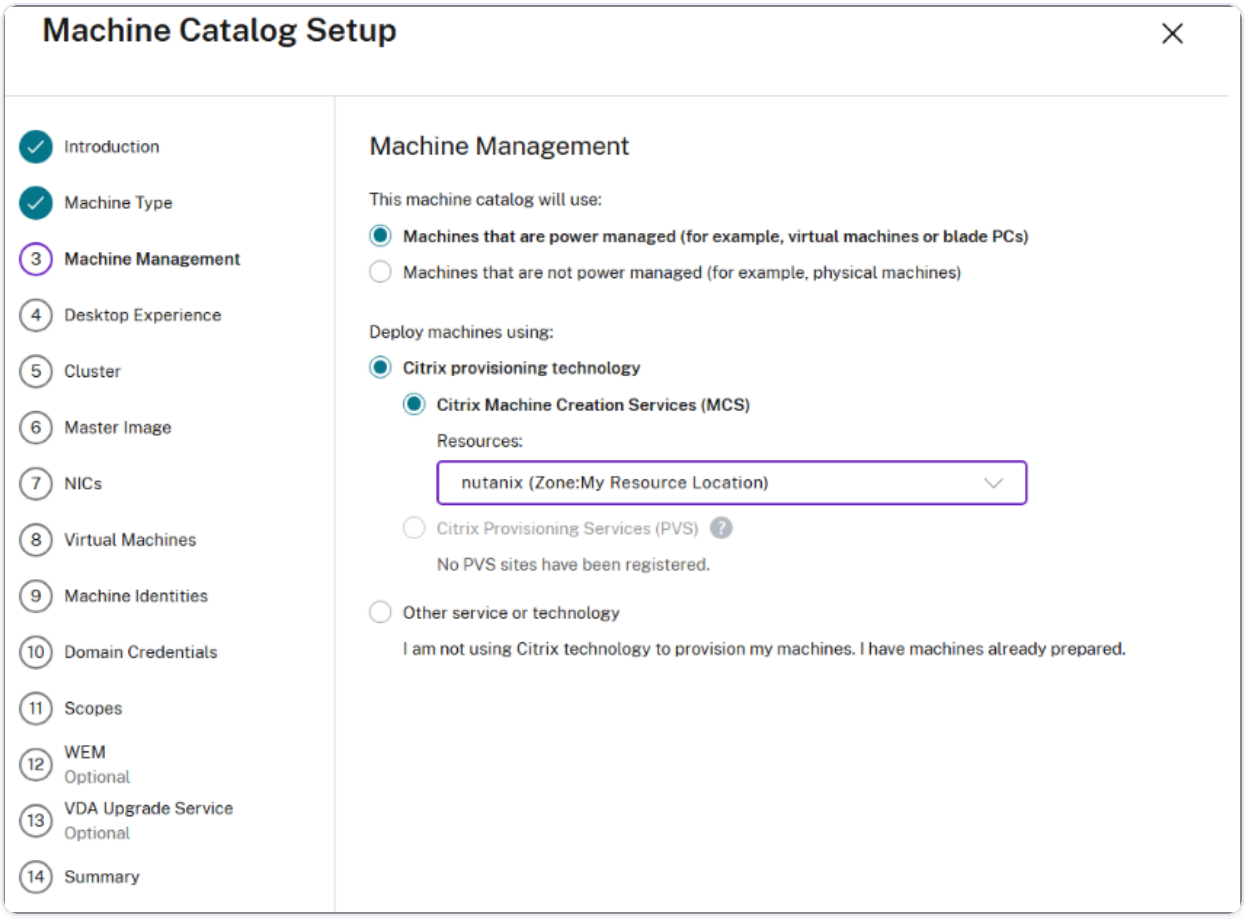
- 不支持将多个 NIC 连接到同一子网。

- 由于 Nutanix 的限制，每个 MCS 预配的计算机目录只能分配到覆盖网络、VLAN 基本子网和 VLAN 子网中单一类型的网络中的 NIC。
- 在某些情况下，更新非持久性计算机目录的 MCS 主映像可能会导致潜在问题。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/security-policies/secure-boot.html#secure-boot-and-vtpm-in-nutanix-prism-central)。
- 当选择 Nutanix VM 模板作为主映像时，模板名称或模板版本名称不得包含 # 或 & 等字符。

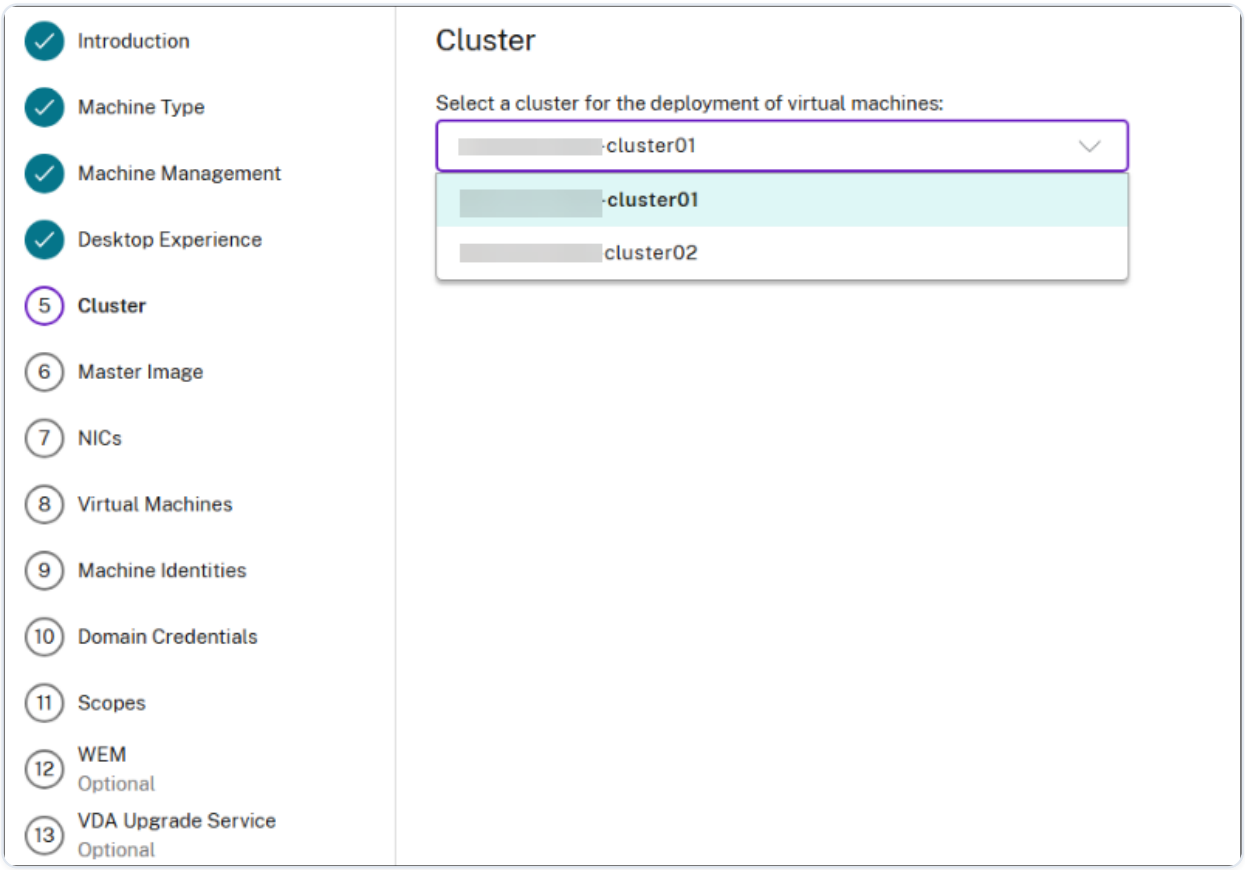
使用 WEB STUDIO 创建计算机目录

在“计算机目录设置”向导中：

1. 在“**计算机类型**”页面上，选择“**多会话操作系统**”、“**单会话操作系统**”或“**远程电脑访问**”。
2. 在“**计算机管理**”页面上，选择“**已进行电源管理的计算机**”和 **Citrix Machine Creation Services™** 作为部署方法。选择“**资源**”。

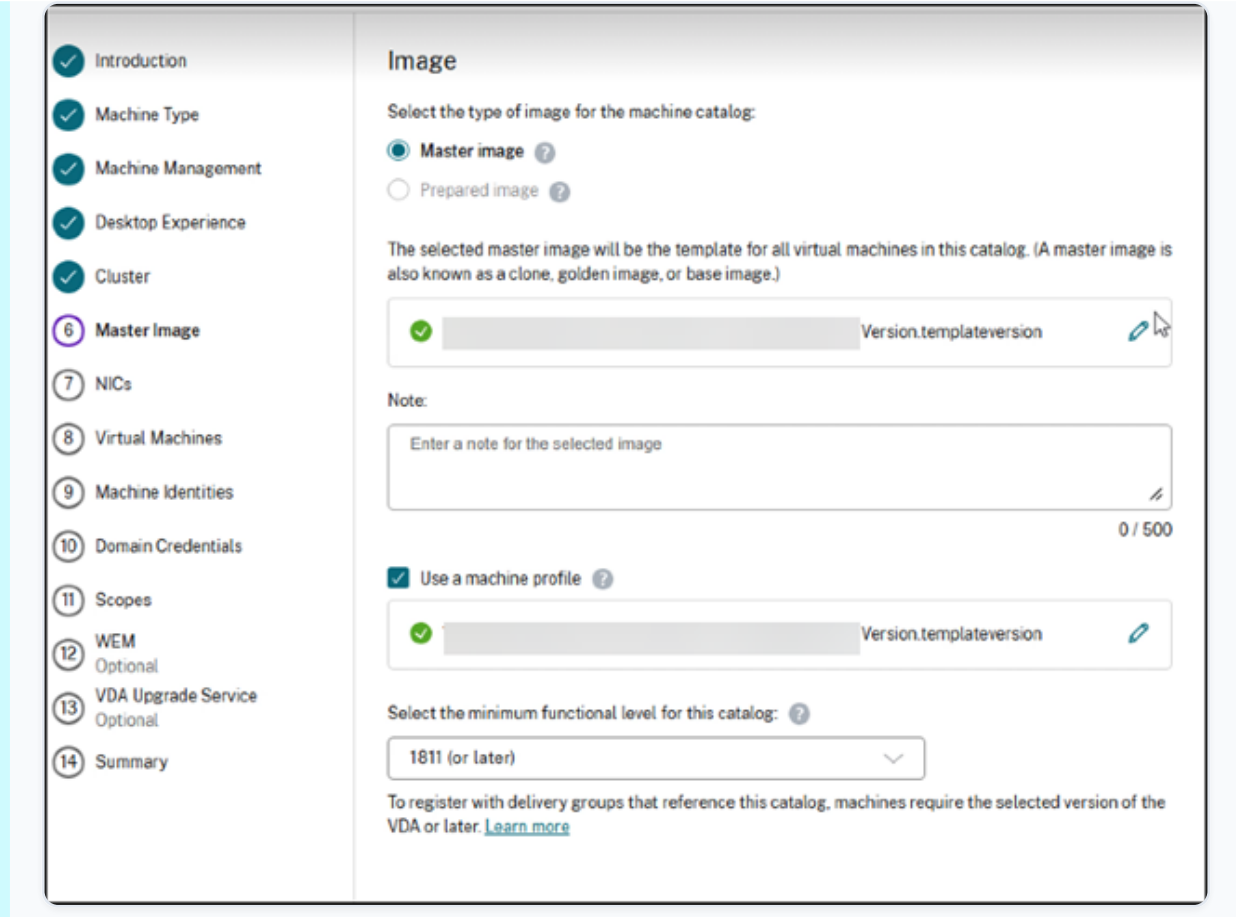


3. 在“**桌面体验**”页面上，选择两个选项之一。
4. 在“**群集**”页面上，选择一个群集用于部署 VM。



5. 在“**主映像**”页面上，单击“**主映像**”并选择一个主映像（模板版本）。您可以按名称筛选计算机模板。主映像的模板版本默认为新目录的计算机配置文件。但是，您可以更改计算机配置文件的模板版本。

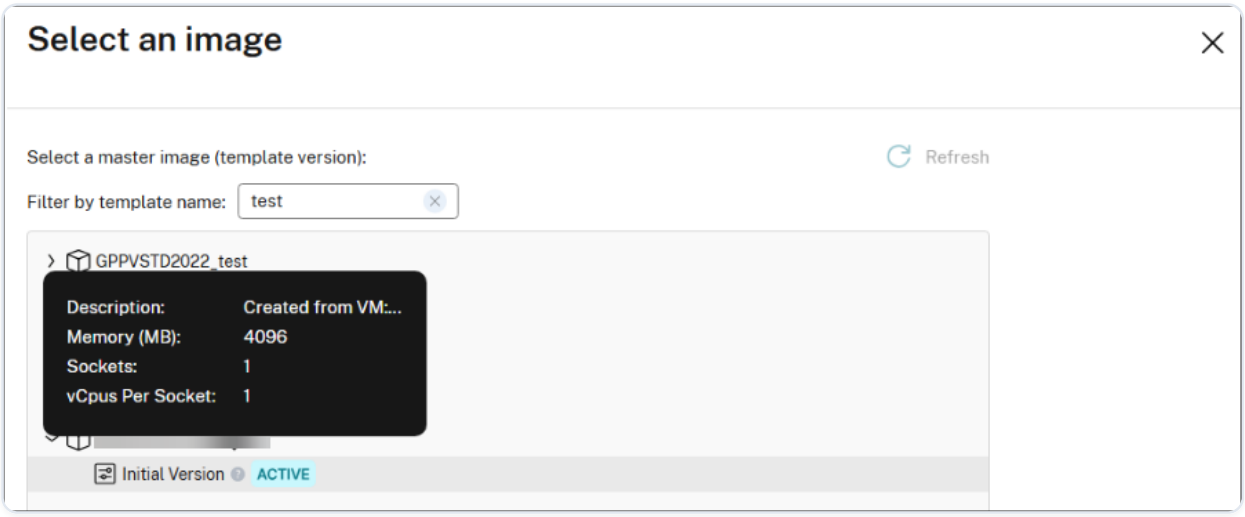
> **注意：**
>
> 您可以将单个 Nutanix VM 模板版本用作多个 MCS 计算机目录的主 VM，即使这些目录位于不同的 Nutanix 群集上。



按名称筛选计算机模板：

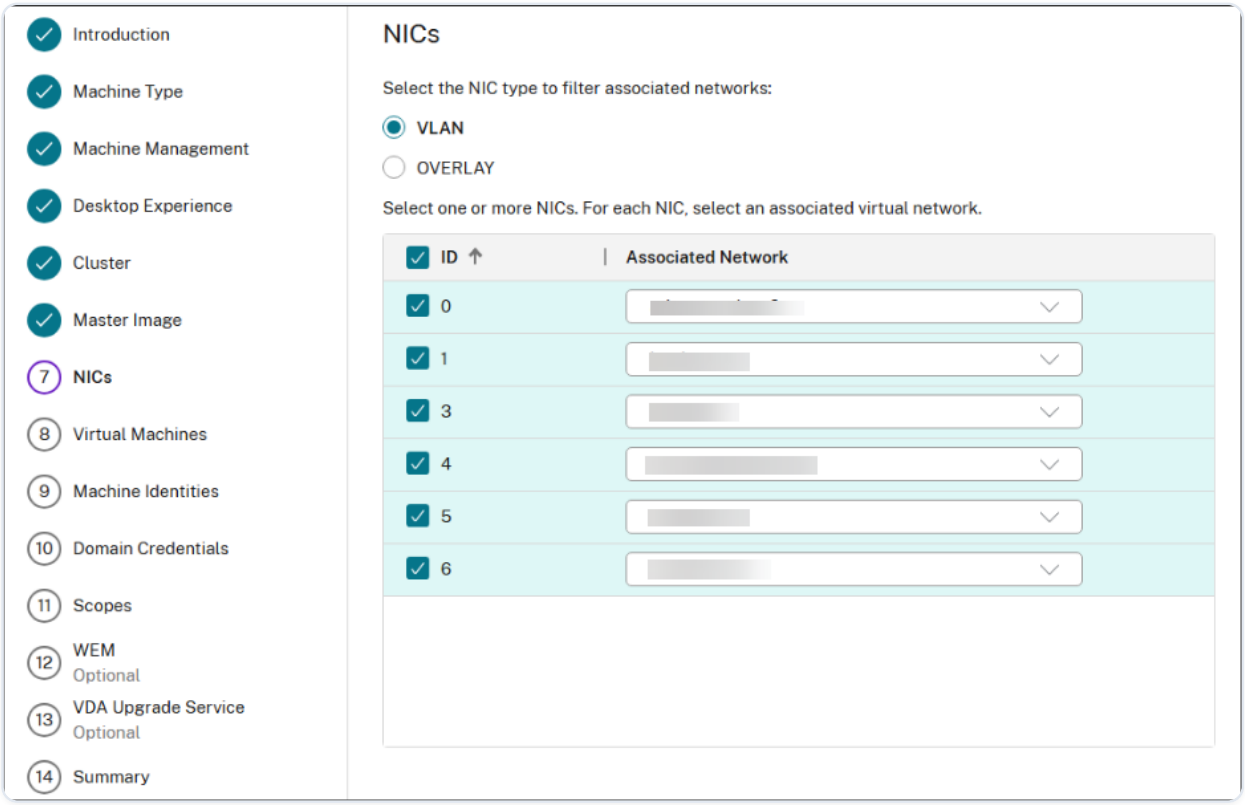


请参阅模板说明：



6. 在“**NICs**”页面上：

   - 选择 NIC 类型以筛选关联的网络。
   - 选择主映像包含的一个或多个 NIC，然后为每个 NIC 选择一个关联的虚拟网络。



7. 在“**Virtual Machines**”页面上，指示要创建的虚拟机数量，并为每台计算机的总内存 (MB)、虚拟 CPU 和每个 CPU 的核心数配置计算机。这些值将自动从计算机配置文件中填充。
8. 在**摘要**页面上，检查计算机目录的详细信息。输入计算机目录的名称和描述。单击**完成**。

导出计算机配置文件

您可以将计算机目录使用的计算机配置文件导出到 JSON 文件。

1. 选择计算机目录并导航到“**Templates Properties**”选项卡。

2. 在“**Machine Profile**”详细信息下，单击“**Last version**”旁边的“**Export**”。

使用 POWERSHELL 命令创建计算机目录

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*`。
3. 如果尚未创建身份池，请创建一个。例如：

```
New-AcctIdentityPool    -Domain "<string>" -IdentityPoolName "<string>"
-IdentityType "ActiveDirectory"  -NamingScheme "DemoVM-##"
-NamingSchemeType "Numeric" -ZoneUid "GUID" -Scope @()
```

4. 创建预配方案。

   例如：不带计算机配置文件

```
New-ProvScheme -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"ClusterId`"
Value=`"00062c63-1fb0-58c9-4fc8-5c2573352378`" /><Property
xsi:type=`"StringProperty`" Name=`"CPUCores`" Value=`"1`" /></
CustomProperties>" -HostingUnitName "<Hosting unit name>"
-IdentityPoolName "<string>" -InitialBatchSizeHint 1  -MasterImageVM
"XDHyp:\HostingUnits\<Hosting Unit Name>\Templates.folder\<template
name>.template\<template version name>.templateversion" -NetworkMapping
@{"5"="XDHyp:\HostingUnits\<Hosting unit name>\Clusters.folder\<Cluster
Name>.cluster\<Network name>.network"} -ProvisioningSchemeName
"<Catalog name>" -ProvisioningSchemeType "MCS" -RunAsynchronously
-Scope @() -VMCpuCount 2 -VMMemoryMB 10240
```

   例如：带计算机配置文件

   使用计算机配置文件从模板版本捕获硬件属性，并将其应用于预配的虚拟机。如果未指定计算机配置文件，硬件属性将从主映像模板版本中捕获。

> **注意：**

- 即使使用计算机配置文件，操作系统磁盘、vTPM 和安全启动属性也始终从主映像中捕获。
- 由于不从计算机配置文件读取操作系统磁盘，因此您可以创建无盘 VM 并将其转换为可用于计算机配置文件的模板版本。
- 由于存储了计算机配置文件模板版本的完整 JSON 规范，因此即使您从 Prism Central 中删除了模板版本，也可以创建 VM。

从计算机配置文件捕获的属性包括：

属性	API 中的属性名称 (GETTEMPLATEVERSIONBYID)	备注/参考资料
CPU	numSockets	
RAM	memorySizeBytes	
核心	numCoresPerSocket	
类别	类别	类别管理
GPU	GPU	GPU 摘要视图
每核心线程数	numThreadsPerCore	aCLI-VM
NUMA 节点	numNumaNodes	
启用 VCPU 硬绑定	isVcpuHardPinningEnabled	
启用 CPU 直通	isCpuPassthroughEnabled	
启用内存超额分配	isMemoryOvercommitEnabled	通过 Prism Central (AHV) 创建虚拟机
启用 GPU 控制台访问	isGpuConsoleEnabled	
启用 CPU 热插拔	isCpuHotplugEnabled	

属性	API 中的属性名称 (GETTEMPLATEVERSIONBYID)	备注/参考资料
启用 SCSI 控制器	isScsiControllerEnabled	
时区	hardwareClockTimezone	通过 Prism Central (AHV) 创建虚拟机
启用 AHV 品牌	isBrandingEnabled	
启用 VGA 控制台	isVgaConsoleEnabled	
虚拟机	isAgentVm	通过 Prism Central (AHV) 创建虚拟机

注意：

使用相同的主映像模板版本，您可以创建具有各种计算机配置文件的不同目录，每个配置文件都具有上述一组不同的属性。例如，您可以分配可链接到 Nutanix 策略的不同类别，调整 CPU/内存，修改内存超额使用设置，或者添加和删除多个 GPU。

命令行参数，例如 `VMCpuCount`、`VMMemoryMB` 和 `CPUCores`（在 `CustomProperties` 中），可以提供，并且其值优先于计算机配置文件模板版本中的相应参数值。如果未提供，则从给定的计算机配置文件中读取这些参数。

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378" />

    <StringProperty Name="CPUCores" Value="2" />

</CustomProperties>
```

```
"@



New-ProvScheme -HostingUnitName "<Hosting unit name>" `

           -IdentityPoolName "<string>" `

           -InitialBatchSizeHint 1 `

           -MasterImageVM "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<template name>.template\<template version
name>.templateversion" `

           -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<template name for machine
profile>.template\<template version name>.templateversion" `

           -NetworkMapping @{"0"="XDHyp:\HostingUnits\<Hosting unit
name>\Clusters.folder\<Cluster Name>.cluster\<Network name>.network"} `

           -ProvisioningSchemeName "<Catalog name>" `

           -ProvisioningSchemeType "MCS" `

           -CustomProperties $customProperties `

           -RunAsynchronously `

           -VMCpuCount 2 `

           -Scope @()
```

5. 将预配方案注册为代理目录。例如：

```
New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False  -
MinimumFunctionalLevel "L7_20" -Name "<Catalog Name>"
-PersistUserChanges "Discard" -ProvisioningType "MCS"    -
SessionSupport "MultiSession" -ZoneUid "GUID"  -ProvisioningSchemeId
fe7df345-244e-4xxxx-xxxxxxxxx `  -Scope @()
```

使用现有计算机创建计算机目录（电源管理）

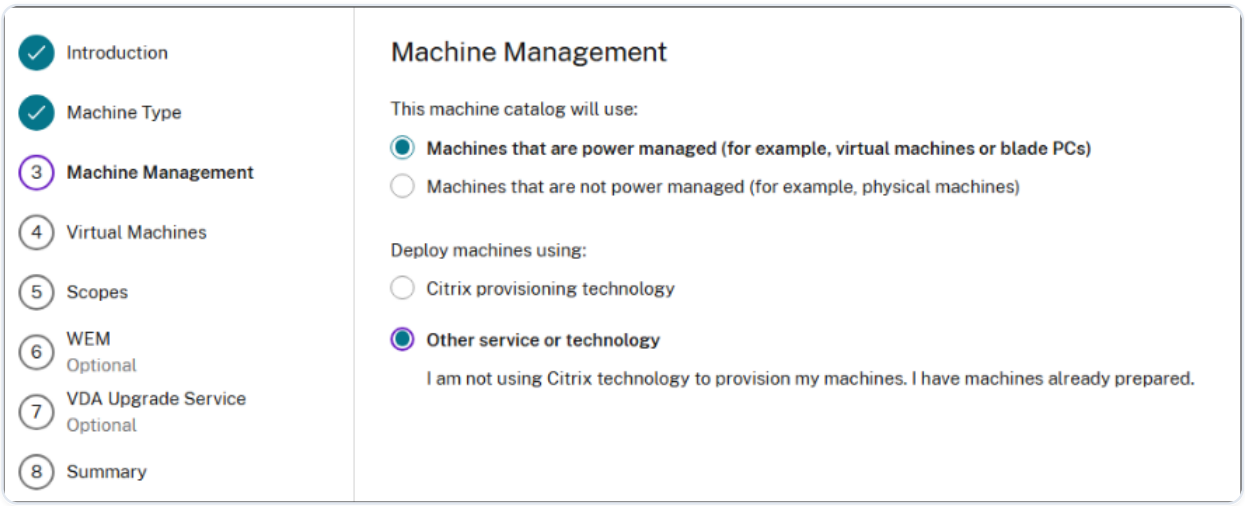
您可以使用以下方式创建包含现有计算机（电源管理）的计算机目录：

- Web 工作室
- PowerShell

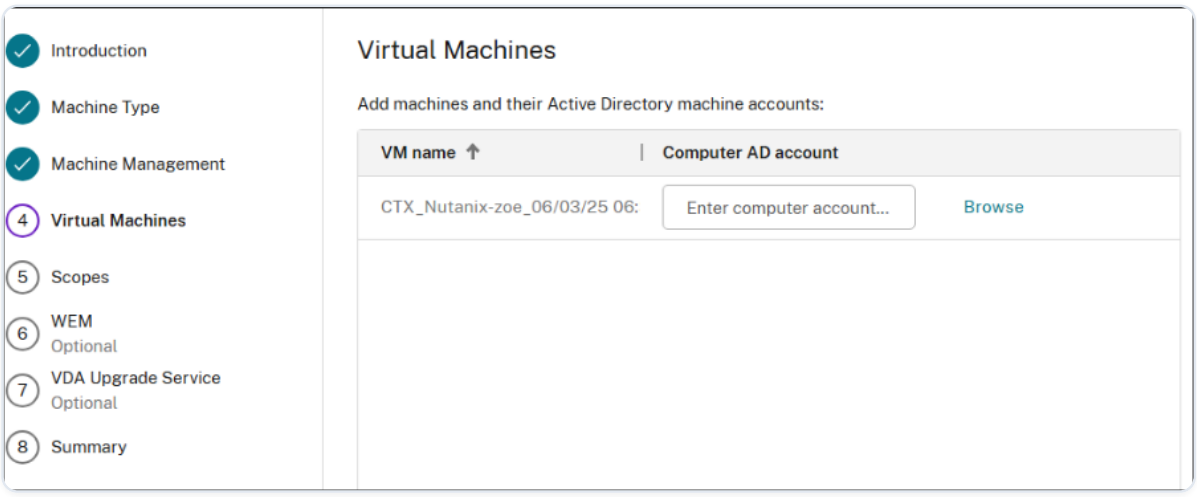
使用 WEB STUDIO 创建包含现有计算机（电源管理）的计算机目录

在“计算机目录设置”向导中：

1. 在“**操作系统**”页面上，选择“**多会话操作系统**”或“**单会话操作系统**”。
2. 在**计算机管理**页面上，选择**电源管理的计算机**和**其他服务或技术**。



3. 在**虚拟机**页面上，添加计算机及其 Active Directory 计算机帐户。您可以执行以下操作之一：
   - 单击“**从 CSV 文件导入**”以批量添加计算机。
   - 单击**添加计算机**以手动添加计算机。此时将显示**选择 VM**窗口。展开您之前创建的 Nutanix AHV Prism Central 连接，然后选择要添加的 VM。然后添加关联的计算机帐户名称。



4. **作用域**和**摘要**页面不包含特定于 Nutanix AHV Prism Central 的信息。

使用 POWERSHELL 创建包含现有计算机（电源管理）的计算机目录

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*`。
3. 创建目录以拥有分配给用户的电源管理型 VM。例如：

```
New-BrokerCatalog -AllocationType "Permanent"  -IsRemotePC $False
-MachinesArePhysical $False  -Name "<Catalog Name>" -PersistUserChanges
"OnLocal" -ProvisioningType "Manual" -Scope @() -SessionSupport
"SingleSession" -ZoneUid "fb202053-8c35-4db2-a299-a8d9538ec6be"
```

4. 将 VM 添加到目录。例如：

```
New-BrokerMachine  -CatalogUid 6 -HostedMachineId "d859caf3-4bf0-447b-
b012-8af0594c7d88" -HypervisorConnectionUid 1 -IsReserved $False  -
MachineName "S-1-5-21-1334627847-1250330507-3910179295-100245"
```

使用 Nutanix 快照创建计算机目录

本部分介绍如何使用 Nutanix Acropolis (Prism Element) 主机连接创建 MCS 预配的计算机目录。在创建目录之前，请在 Nutanix 中创建主映像和快照。有关详细信息，请参阅 Nutanix 文档。

在“计算机目录设置”向导中：

- **Container**（容器）或 **Cluster and Container**（群集和容器）页面是 Nutanix 独有的。
  - 如果使用 Nutanix AHV XI 作为资源部署计算机，请在 **Container**（容器）页面上选择一个容器，用于放置 VM 的身份磁盘。
  - 如果使用 Nutanix AHV PC 作为资源部署计算机，您会看到 **Cluster and Container**（群集和容器）页面。选择用于部署 VM 的群集，然后选择一个容器。
- 在 **Image**（映像）页面上，选择映像快照。如果需要，请使用 Acropolis 控制台重命名快照。如果重命名快照，请重新启动目录创建向导以查看刷新后的列表。
- 在 **Virtual Machines**（虚拟机）页面上，指示虚拟 CPU 的数量和每个 vCPU 的核心数。
- 在 **NICs**（网卡）页面上，选择网卡类型以筛选关联的网络。此选项仅适用于 Nutanix AHV PC 连接。
- **Machine Identities**（计算机身份）、**Domain Credentials**（域凭据）、**Scopes**（范围）和 **Summary**（摘要）页面不包含 Nutanix 特定的信息。

限制

使用 Nutanix 主机连接（特别是 Nutanix AHV 插件 2.7.1 和 Nutanix AHV 插件 2.5.1）创建 MCS 目录时，预配的虚拟机的硬盘大小在 Web Studio 上显示不正确。

- Nutanix AHV 插件 2.7.1：显示的大小 (1 GB) 小于实际存储大小。
- Nutanix AHV 插件 2.5.1：显示的大小 (32 GB) 小于实际存储大小。

但是，如果主映像 VM 是 VM 中的快照，则此功能按设计运行。

下一步操作

- 如果这是创建的第一个目录，Web Studio 会引导您创建交付组
- 要查看整个配置过程，请参阅安装和配置
- 要管理目录，请参阅管理计算机目录和管理 Nutanix 目录

更多信息

- 创建和管理连接和资源
- 连接到 Nutanix
- 连接到 Nutanix 云和合作伙伴解决方案
- 创建计算机目录

创建 Oracle C3 计算机目录（预览）

创建计算机目录 描述了通用的计算机目录工作流程。以下信息涵盖了 Oracle C3 特定的详细信息。

> **注意：**

> 在创建 Oracle C3 目录之前，请完成以下先决条件：

> - 连接到 Oracle C3。
> - 确保有一台或多台 Oracle C3 计算机可用于载入。
> - 为这些计算机做好所需的 VDA 准备工作。

> 您可以使用以下方式创建 Oracle C3 计算机目录：

- Web 工作室

- PowerShell 命令

使用 Web Studio 创建计算机目录

在“计算机目录设置”向导中：

1. 在**操作系统**页面上，选择**多会话操作系统**或**单会话操作系统**。
2. 在**计算机管理**页面上，选择**已进行电源管理的计算机**和**其他服务或技术**。
3. 在**虚拟机**页面上，通过执行以下操作之一来添加计算机和关联的计算机帐户：
    - 选择**添加计算机**以从 Oracle C3 连接手动添加 Oracle C3 计算机。
    - 选择**添加 CSV 文件**以批量添加 Oracle C3 计算机和计算机帐户映射。

作用域和**摘要**页面不包含 Oracle C3 特定的信息。

使用 PowerShell 命令创建计算机目录

使用 `New-BrokerCatalog` 和 `New-BrokerMachine` 创建目录并导入现有 Oracle C3 计算机。

示例模式：

```
New-BrokerCatalog -AllocationType "Random" -ProvisioningType "Manual" `

-SessionSupport "MultiSession" -Name "OracleC3-Catalog" `

-PersistUserChanges "OnLocal"

New-BrokerMachine -CatalogUid <CatalogUid> `

-HostedMachineId <OracleC3MachineId> `

-HypervisorConnectionUid <OracleC3ConnectionUid> `
```

```
-MachineName <Domain\MachineAccount>
```

下一步操作

- 如果这是创建的第一个目录，Web Studio 会引导您创建交付组
- 要查看整个配置过程，请参阅安装和配置
- 有关电源管理，请参阅电源管理 Oracle C3 VM

更多信息

- 创建和管理连接与资源
- 连接到 Oracle C3
- 创建计算机目录

创建 Red Hat OpenShift 目录

创建计算机目录 介绍了创建计算机目录的向导。以下信息涵盖了 Red Hat OpenShift 虚拟化环境特有的详细信息。

> **注意：**
>
> 在创建 Red Hat OpenShift 目录之前，请完成与 Red Hat OpenShift 的连接和托管单元的创建。请参阅连接到 Red Hat OpenShift。

创建主映像 VM

创建计算机目录需要主映像 VM。

1. 使用您的登录 ID 访问 OpenShift 控制台。
2. 导航到 **Virtualization > VirtualMachines** 以查看 VM 列表，包括主映像 VM。
3. 创建主映像。创建主映像时，请确保主映像 VM 只有一个存储设备。

> **注意：**
>
> - 确保根据客户对群集环境的要求，将可路由的 NAD 添加到主映像 VM。

- 当主映像加入域时，在用于目录创建后，它可能会失去域信任。由于 OpenShift 环境的限制，此问题会影响 Citrix Virtual Apps and Desktops™ 2503。解决方法是不在主映像中加入域。Citrix 正在与 Red Hat 合作以增强网络隔离功能。
- 在 Red Hat OpenShift 虚拟化环境中创建 MCS 计算机目录时，不能使用具有不同操作系统类型的主映像和计算机配置文件。这是因为 Red Hat OpenShift 管理每种操作系统类型的方式。因此，不支持将 Windows VM 用作主映像，而将非 Windows（例如 Linux）VM 用作计算机配置文件，反之亦然。
- 目前，使用 `InstanceType` 创建的 VM 不支持作为主映像。

创建目录

您可以创建 OpenShift 目录，以便在您的 OpenShift 环境中创建、交付和电源管理计算机。

- 使用 Web Studio 创建目录
- 使用 PowerShell 命令创建目录(#create-a-catalog-using-powershell-commands)

使用 WEB STUDIO 创建目录

您可以使用 Web Studio 在 Red Hat OpenShift 环境中创建带或不带计算机配置文件的 MCS 计算机目录。VM 用作计算机配置文件输入。

在“计算机目录设置”向导中：

1. 在“**操作系统**”页面上，选择“**多会话操作系统**”或“**单会话操作系统**”。
2. 在“计算机管理”页面上：
   - 选择“**已进行电源管理的计算机（例如，虚拟机或刀片式电脑）**”。
   - 选择使用 **Citrix 预配技术 Citrix Machine Creation Services™ (MCS)** 部署计算机。
   - 在 Citrix Machine Creation Services (MCS) 下选择 Openshift 托管单元
3. 在“**桌面体验**”页面上，根据您在“**计算机类型**”页面上选择的计算机类型选择选项。
4. 在**映像**页面上：
   a. 选择主映像。目前，Openshift 不支持准备好的映像。
   b. 您可以为所选映像添加备注。
   c. 您可以选中“使用计算机配置文件”复选框并选择一个计算机配置文件。
   d. 要启用最新产品功能，请确保主映像已安装最新 VDA 版本。请勿更改默认的最低 VDA 选择。但是，如果必须使用较早的 VDA 版本，请参阅 VDA 版本和功能级别。

5. 在**网卡**页面上，选择一个或多个网卡，并将虚拟网络与每个网卡关联。
6. 在“**虚拟机**”页面上：
    a. 指定要创建的虚拟机数量。如果您不想创建任何虚拟机，请输入 0（零）。稍后，您可以通过添加计算机来为现有空目录创建虚拟机。
    b. 选择每个 VM 的内存量（以 MB 为单位）。
    c. 如果您正在创建随机非持久性目录，可以为计算机启用回写式缓存以提高 I/O 性能。请参阅配置临时数据缓存。
7. 按照屏幕上的说明完成剩余步骤，这些步骤不包含 OpenShift 特定的信息。

您还可以使用 Studio 创建 OpenShift 目录，以在您的 OpenShift 环境中交付和管理现有计算机的电源。请执行以下操作：

在“计算机目录设置”向导中：

1. 在**操作系统**页面上，选择**多会话操作系统或单会话操作系统**。
2. 在“**计算机管理**”页面上，选择“**已进行电源管理的计算机和另一项服务或技术**”。
3. 在**虚拟机**页面上，添加计算机及其 Active Directory 计算机帐户。您可以：
    - *手动添加计算机*：单击**添加计算机**以手动添加计算机。将显示**选择虚拟机**窗口。展开您之前创建的 OpenShift 连接，然后选择要添加的节点（虚拟机）。然后添加关联的计算机帐户名称。
    - *使用 CSV 文件添加计算机*：单击**添加 CSV 文件**以批量添加计算机。有关使用 CSV 文件添加计算机的信息，请参阅使用 CSV 文件批量将计算机添加到目录。
4. 按照屏幕上的说明完成剩余步骤，这些步骤不包含 OpenShift 特定的信息。

使用 POWERSHELL 命令创建目录

您可以使用 PowerShell 命令在 Red Hat OpenShift 环境中创建 MCS 计算机目录。您可以创建使用或不使用计算机配置文件的计算机目录。VM 用作计算机配置文件输入。

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*`。
3. 运行 PowerShell 命令以
    a. 创建身份池
    b. 创建 AD 帐户
    c. 创建带或不带计算机配置文件的持久性 VM 的 MCS 计算机目录。

d. 将 VM 添加到目录

e. 创建代理目录

f. 将代理计算机添加到新 VM

以下是示例脚本：

创建身份池

```
New-AcctIdentityPool `

    -IdentityPoolName "IdentityPoolName" `

    -ZoneUid "00000000-0000-0000-0000-000000000000" `

    -NamingScheme "vm###" `

    -NamingSchemeType "Numeric" `

    -AllowUnicode `

    -Domain "MyDomain.local" `

    -AdminAddress "MyDDC.MyDomain.Local"
```

创建 AD 帐户

```
New-AcctADAccount `

    -IdentityPoolUid "11111111-1111-1111-1111-111111111111" `

    -ADUserName "MyDomain\MyUserName" `

    -ADPassword SecurePassword `

    -Count 1 `

    -AdminAddress "MyDDC.MyDomain.Local"
```

创建具有持久性计算机的预配方案（不带计算机配置文件）

```
New-ProvScheme `

    -ProvisioningSchemeName "ProvisioningSchemeName" `
```

```
    -HostingUnitName "HostingUnitName" `

    -IdentityPoolName "IdentityPoolName" `

    -ProvisioningSchemeType "MCS" `

    -MasterImageVM "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MasterImageVM.vm"
`

    -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MyNetwork.network"
 } `

    -VMCpuCount 1 `

    -VMMemoryMB 4096 `

    -InitialBatchSizeHint 1 `

    -AdminAddress "MyDDC.MyDomain.Local"
```

创建具有持久性计算机的预配方案（带计算机配置文件）

```
New-ProvScheme `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -HostingUnitName "HostingUnitName" `

    -IdentityPoolName "IdentityPoolName" `

    -ProvisioningSchemeType "MCS" `

    -MasterImageVM "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MasterImageVM.vm"
`

    -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MyNetwork.network"
 } `

    -VMCpuCount 1 `
```

```
    -VMMemoryMB 4096 `

    -InitialBatchSizeHint 1 `

    -AdminAddress "MyDDC.MyDomain.Local" `

    -MachineProfile "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MachineProfileVM.v
m"
```

创建新的 ProvVM

```
New-ProvVM `

    ProvisioningSchemeName "ProvisioningSchemeName" `

    ADAccountName "MyDomain\vm001" `

    AdminAddress "MyDDC.MyDomain.Local"



Lock-ProvVM `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -Tag "Brokered" `

    -VMID "TargetNamespace:vm001"
```

创建新的代理目录

```
New-BrokerCatalog `

    -Name "ProvisioningSchemeName" `

    -ProvisioningType "MCS" `

    -SessionSupport "MultiSession" `

    -AllocationType "Random" `
```

```
    -PersistUserChanges "OnLocal" `

    -ZoneUid "00000000-0000-0000-0000-000000000000" `

    -AdminAddress "MyDDC.MyDomain.Local"
```

设置代理目录元数据

```
Set-BrokerCatalogMetadata `

    -CatalogId "1" `

    -Name "Citrix_DesktopStudio_IdentityPoolUid" `

    -Value "11111111-1111-1111-1111-111111111111"



Set-BrokerCatalog `

    -Name "ProvisioningSchemeName " `

    -ProvisioningSchemeId "22222222-2222-2222-2222-222222222222"
```

为新的 ProvVM 创建代理计算机

```
New-BrokerMachine `

    -CatalogUid "33333333-3333-3333-3333-333333333333" `

    -AdminAddress "MyDDC.MyDomain.Local" `

    -MachineName "S-0-0-00-0000000000-0000000000-000000000-000000"
```

vCPU 计算和 CPU 拓扑约束

更新 OpenShift 虚拟机 CPU 配置时，插件会根据请求的 vCPU 计数以及计算机配置文件中现有的 CPU 拓扑（核心数和线程数）计算套接字数量。

使用的公式为：

```
sockets = requestedVCpuCount / (cores × threads)
```

要求

- 计算机配置文件的核心数和线程数都必须大于零。
- 请求的 vCPU 计数必须是核心数 × 线程数的精确倍数。如果不能被整除，则更新将被拒绝。
- 仅调整套接字值；计算机配置文件中的核心数和线程数保持不变。

示例

计算机配置文件	请求的 VCPU	计算的套接字	有效？
核心=2, 线程=2	8	8 / (2×2) = 2	是
核心=2, 线程=2	6	6 / (2×2) = 1.5	否
核心=4, 线程=1	12	12 / (4×1) = 3	是

已知限制

如果机器配置文件定义的CPU拓扑中，核心数 × 线程数大于1，则仅支持该乘积的精确倍数的vCPU数量。

确保在创建或更新预配方案时，请求的vCPU数量与机器配置文件的拓扑保持一致。

下一步操作

- 如果这是创建的第一个目录，Web Studio 会引导您创建交付组
- 要查看整个配置过程，请参阅安装和配置
- 有关电源管理，请参阅电源管理 Red Hat OpenShift VM

更多信息

- 创建和管理连接与资源
- 连接到 Red Hat OpenShift
- 创建计算机目录

创建 VMware 目录

创建计算机目录 介绍了创建计算机目录的向导。以下信息涵盖了 VMware 虚拟化环境特有的详细信息。

> **注意：**

在创建 VMware 目录之前，您需要完成与 VMware 的连接创建。请参阅连接到 VMware。

创建主 VM

使用主 VM 在计算机目录中提供用户桌面和应用程序。在您的虚拟机管理程序上：

1. 在主 VM 上安装 VDA，选择优化桌面的选项，这可以提高性能。
2. 为主 VM 创建快照以用作备份。

注意：

您可以使用 MCS 在 vSAN 8.0 环境中预配 VM。

使用机器配置文件创建计算机目录

您可以使用计算机配置文件创建 MCS 计算机目录。计算机配置文件输入的源是 VMware 模板。计算机配置文件从 VMware 模板捕获硬件属性，并将其应用于目录中新预配的 VM。

注意：

- 主映像输入（快照）和计算机配置文件输入 (VMware 模板) 必须都启用 vTPM 或都禁用 vTPM。此规则适用于 `New-ProvScheme` 和 `Set-ProvScheme`。
- 如果主映像启用了 vTPM，则 VMware 模板只能来自与主映像相同的 VM 源。
- 加密存储策略仅支持完整克隆。
- 基于计算机配置文件的目录利用提供的 VMware 模板收集存储控制器信息，并依赖于附加的虚拟磁盘。该模板必须包含一个虚拟磁盘，该虚拟磁盘是检索用于配置虚拟机虚拟磁盘的存储控制器信息所必需的。

计算机配置文件中的 VMware 模板必须在目录生命周期内存在，才能允许向目录预配 VM。如果没有 VMware 模板，则无法预配新的 VM。当 VMware 模板被删除时，您必须使用 `Set-ProvScheme` 命令提供一个新模板。

- MCS 捕获 VMware 模板的属性。您可以使用 Get-Provscheme 命令创建引用 VMware 模板存储属性的新 VMware 模板。
- 或者，如果计算机目录和预配的 VM 存在，则 MCS 预配的计算机也可以用于创建新的 VMware 模板。

- 当启用 MCSIO 时，您可以在创建 MCS 目录后更新内存和磁盘缓存大小。

根据不同的操作系统，您可以创建具有不同配置的计算机目录：

- 如果主映像上安装了 Windows 11，则要求为主映像启用 vTPM。因此，作为计算机配置文件来源的 VMware 模板必须附加 vTPM。
- 如果主映像上安装了 Windows 10 且未附加 vTPM，则可以使用非 vTPM VMware 模板作为计算机配置文件的来源来创建计算机目录。

还有另一种配置，您可以使用完整复制磁盘模式创建计算机目录，并应用带有加密存储策略的计算机配置文件模板。

要使用 PowerShell 命令并以计算机配置文件作为输入来创建计算机目录：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix®*`。
3. 运行以下命令：

    - 要创建计算机目录，其中 vTPM 附加的 VMware 模板作为计算机配置文件输入的来源，并且主映像安装了 Windows 11：

    ```
    $identityPool = New-AcctIdentityPool  -IdentityPoolName "<string>"

    -NamingScheme "<string>-###"

    -NamingSchemeType Numeric

    -Domain "<domain name"

    -ZoneUid "<Uid>"  -Scope @()
    ```

    ```
    $provScheme =New-ProvScheme  -CleanOnBoot

    -HostingUnitName "vSanRg"

    -IdentityPoolName "<string>"

    -InitialBatchSizeHint 1

    -MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
    name>.snapshot"
    ```

```
-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<network name>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4

-VMMemoryMB 6144

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template" -TenancyType Shared

-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<catalog name>"

-ProvisioningType 'MCS'

-Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 要创建计算机目录，其中非 vTPM VMware 模板作为计算机配置文件的来源，并且主映像安装了 Windows 10：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###" -NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-CleanOnBoot -HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False
```

```
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 要使用完整复制磁盘模式创建计算机目录，并应用带有加密存储策略的计算机配置文件模板：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"
```

```
-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "XDHyp:
\HostingUnits\<hosting unit name>\<template name>.template"

-TenancyType Shared

-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"  -IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<string>" -ProvisioningType 'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

要更新计算机配置文件，请使用 Set-ProvScheme 命令。例如：

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
-MachineProfile 'XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template'
```

检查多个网卡

当使用计算机配置文件以及 `New-ProvScheme` 和 `Set-ProvScheme` 命令中的 `NetworkMapping` 参数时，在多个网卡的预检期间会收到各种错误消息。

多个网卡的预检清单如下：

- 仅使用并验证计算机配置文件模板中的网卡数量。这些网卡指向的网络不会被使用或根据托管单元网络进行验证。

- 如果计算机配置文件模板中的网卡数量大于托管单元中的网络数量，则会收到错误消息。
- 如果机器配置文件模板中的 NIC 计数为零，您会收到错误消息。 当机器配置文件模板中的 NIC 计数为一时，则：
  - 如果在 `New-ProvScheme` 或 `Set-ProvScheme` 命令中未指定网络映射，并且托管单元网络为一个，则使用托管单元网络。
  - 如果指定了网络映射，则在有效的情况下使用指定的网络映射。
- 当机器配置文件模板中的 NIC 计数大于 1，或者托管单元网络计数大于 1 时，则：
  - 命令中需要有效的网络映射，并且应为每个 NIC 提供映射（即，NetworkMapping 计数应与机器配置文件 NIC 计数相同）。
  - 在托管单元中，多个 NIC 不能映射到同一网络。
  - `NetworkMapping` 计数和机器配置文件 NIC 计数必须小于或等于托管单元网络计数。
  - 必须为从 0 到 n-1 的每个 ID 提供 `NetworkMapping`，其中 n 是机器配置文件模板中网络适配器的数量。

在 MCS 创建的 VM 上预配数据盘

数据盘允许存储持久性数据，例如事件日志、安全跟踪和应用程序数据。您可以为 VMware 中 MCS 计算机目录的 MCS 创建的持久性或非持久性 VM 创建并分配持久性或非持久性数据盘。

从主映像预配数据盘。准备好的主映像数据盘存储在 `<Prov Scheme Name>-dataDisk-<datastoreId>` 文件夹中。

您可以创建基于机器配置文件和非基于机器配置文件的 MCS 目录。对于基于机器配置文件的 MCS 目录，您可以使用相同的主映像 VM 作为机器配置文件的数据盘源。

预配的 VM 的数据盘从主映像派生存储策略和大小等属性。对于基于机器配置文件的目录，它可以选择使用 VM 模板的数据盘来派生属性。如果 VM 模板没有数据盘，则使用存储的默认策略。

预配的 VM 的数据盘与操作系统和身份盘在同一目录中创建。

支持的数据盘方案

以下是支持的操作系统磁盘和数据磁盘方案：

- 持久性操作系统磁盘与持久性数据磁盘
- 非持久性操作系统磁盘与持久性数据磁盘
- 非持久性操作系统磁盘与非持久性数据磁盘

> **注意：**
>
> 持久性计算机目录不能具有非持久性数据磁盘。

限制

目前不支持以下操作：

- 预配多个数据磁盘。
- 重置数据磁盘。
- 将具有数据磁盘的 MCS 目录更新为不带数据磁盘的 MCS 目录。同样，将不带数据磁盘的 MCS 目录更新为具有数据磁盘的 MCS 目录。

主要步骤

1. 在 VMware 中创建带数据磁盘的主映像 VM。对于基于计算机配置文件的 MCS 目录，您可以将相同的主映像 VM 用作计算机配置文件的数据磁盘源。
2. 使用 `New-ProvScheme` PowerShell 命令创建具有数据磁盘预配 VM 的 MCS 计算机目录。请参阅创建具有数据磁盘预配 VM 的目录。
3. 使用 `New-ProvVM` PowerShell 命令将 VM 添加到目录。
4. 登录到 VM 以查看数据磁盘是否已正确格式化。如果主映像 VM 中引用的数据磁盘上有内容，则该内容也位于数据磁盘上。

在 VMWARE 中创建带数据磁盘的主映像 VM

1. 创建具有两个硬盘的 VM。一个是操作系统磁盘，另一个是数据磁盘。请按照此指南将新硬盘（数据磁盘）添加到现有 VM。
2. 登录到 VM 以初始化磁盘、设置所需的驱动器号并添加内容。

创建具有数据磁盘预配 VM 的目录

在 `New-ProvScheme` PowerShell 命令中包含以下参数，以预配带数据盘的 MCS 计算机目录。

- `DataDisk`：指定数据盘的路径。
- `DataDiskPersistence`：指示数据盘是持久的还是非持久的。

  如果 `CleanOnBoot` 为 false，则数据盘不能是非持久的。计算机目录配置完成后，无法更改 `DataDiskPersistence` 的值。

创建目录后，使用 `New-ProvVM` 命令添加 VM。

映像更新

运行 `Publish-ProvMasterVMImage` 命令以更新操作系统和数据盘的源。运行 `Publish-ProvMasterVMImage` 命令后：

- 新 VM 将使用更新的操作系统和数据盘创建。
- 现有 VM 的非持久性磁盘将在下次电源循环时更新。
- 现有 VM 的持久性磁盘不会在下次电源循环时更新。

删除数据盘

如果删除目录，则数据盘将被删除，除非使用 `forgetVM` 或 `purgeDBOnly` 选项。如果删除 VM，则数据盘将被删除，除非使用 `forgetVM` 或 `purgeDBOnly` 选项。这些条件仅适用于持久性 MCS 计算机目录。

故障排除

如果目录创建失败，请参阅 CTX294978。

下一步操作

- 如果这是创建的第一个目录，Web Studio 会引导您创建交付组
- 要查看整个配置过程，请参阅安装和配置
- 要管理目录，请参阅 管理计算机目录 和 管理 VMware 目录

更多信息

- 创建和管理连接与资源
- 连接到 VMware
- 创建计算机目录

不同计算机身份加入类型的身份池

使用 MCS，您可以将计算机预配为本地 AD 加入、Microsoft Entra 混合加入或未加入域。

有关如何在 Web Studio 中配置计算机身份的信息，请参阅创建计算机目录。

有关如何创建不同计算机身份加入类型的身份池的具体信息，请参阅以下内容：

- 本地 Active Directory 加入的计算机身份的身份池
- Microsoft Entra 混合加入的计算机身份的身份池
- 未加入域的计算机身份的身份池

本地 Active Directory 加入的计算机身份的身份池

本文介绍了如何创建本地 Active Directory 加入的计算机身份的身份池。

使用 Web Studio

以下信息是对 创建计算机目录 中指南的补充。

1. 在“**计算机身份**”页面上：
   a. 选择身份类型为**本地 Active Directory**。
   b. 选择一个 Active Directory 帐户选项：
      - **创建新的 Active Directory 帐户**：
        ◦ 如果您选择**创建新的 Active Directory 帐户**并且不使用现有身份池，请为这些帐户选择一个域并指定帐户命名方案。

        要快速查找特定域，请在**位置（域）下拉列表顶部的搜索框中键入域名，然后单击 Enter。Web Studio 在检索匹配域时会显示进度指示器。如果您键入的域在域排除列表中，Web Studio 会通知您该域已被排除，并提供指向设置 > 站点设置 > 将域添加到排除列表**的链接，您可以在其中查看或删除该域。

        > **注意：**
        >
        > 为了加快在具有许多林或部分可达信任的环境中查找域的速度，请将不可达或不需要的域添加到排除列表中。有关详细信息，请参阅配置域排除列表。

        ◦ 如果您选择**创建新的 Active Directory 帐户**并使用现有身份池创建新帐户，则从列表中选择一个身份池。
      - **使用现有 Active Directory 帐户**：您可以浏览或从 CSV 文件导入，并重置密码或为所有帐户指定相同的密码。
   c. 单击“**下一步**”。
2. 在**域凭据**页面上，选择一个服务帐户或手动输入凭据。有关服务帐户的信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/on-premises-ad-service-accounts.html)。

修改服务帐户关联

要更改关联的服务帐户或向现有 MCS 计算机目录添加关联，请使用**编辑计算机目录**页面。

- 要添加服务帐户，请在**服务帐户**页面上单击**选择服务帐户**。

- 要更改服务帐户关联，请在**服务帐户**页面上单击编辑图标。

使用 PowerShell

您可以通过将本地服务帐户与身份池关联，将本地服务帐户与 MCS 创建的计算机目录关联。您可以创建身份池或更新现有身份池以将其与服务帐户关联。

例如：要创建新的身份池并将其与服务帐户关联，请运行以下命令：

```
New-AcctIdentityPool -IdentityType ActiveDirectory -IdentityPoolName
MyPool -NamingScheme Acc#### -Domain MyDomain.com -NamingSchemeType
Numeric -OU "CN=MyOU,DC=MyDomain,DC=com" -ServiceAccountUid
$serviceAccountUid
```

例如：要更新现有身份池以将其与服务帐户关联，请运行以下命令：

```
$identityPoolUid = (Get-ProvScheme -ProvisioningSchemeName
"MyProvScheme").IdentityPoolUid

Set-AcctIdentityPool -IdentityPoolUid $identityPoolUid -ServiceAccountUid
$serviceAccountUid
```

注意：

`$serviceAccountUid` 必须是本地 Active Directory 服务帐户的有效 UID。

Microsoft Entra 混合加入的计算机身份的身份池

本文介绍如何创建以下身份池：

- Microsoft Entra 混合加入目录
- 已注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录

有关要求、限制和注意事项的信息，请参阅 Microsoft Entra 混合加入。

创建 Microsoft Entra 混合加入目录

使用 WEB STUDIO

以下信息是对 创建计算机目录 中指南的补充。

在目录创建向导的“**计算机身份**”页面上：

- 选择“**Microsoft Entra 混合加入**”。创建的计算机由组织拥有，并使用属于该组织的 Active Directory 帐户登录。
- 要将创建的计算机注册到 Microsoft Intune（包括 Configuration Manager）进行设备管理，请选择“**使用 Configuration Manager 将计算机注册到 Microsoft Intune**”。为避免在目录创建过程中出现错误，请确保主映像满足以下要求：
  - 已安装 VDA 2405 或更高版本。
  - 已安装 **Configuration Manager 客户端**，且站点代码未分配。有关详细信息，请参阅这篇 Microsoft 文章。

> **注意：**
>
> 如果选择“**Microsoft Entra 混合加入**”作为身份类型，则目录中的每台计算机都必须具有相应的 AD 计算机帐户。

- 单击“**添加扩展属性**”以将唯一的自定义数据直接存储在您的 Entra ID 设备对象上。在“**添加扩展属性**”页面上，添加“**扩展属性**”和“**值**”。

> **注意：**
>
> - 您最多可以添加 15 个扩展属性。
> - 名称和值必须唯一且不能为空。

添加或修改扩展属性

要更改或向现有 MCS 计算机目录添加其他扩展属性，或向没有服务帐户的 MCS 目录添加扩展属性，请使用**编辑计算机目录**向导。

- 要更改或添加其他扩展属性，请导航到**Microsoft Entra 设备扩展属性**页面。单击铅笔图标，然后添加或更新扩展属性。
- 要向没有 Microsoft Entra 服务帐户的 MCS 目录添加扩展属性：
  a. 导航到**服务帐户**页面。为 Microsoft Intra ID 选择一个 Microsoft Entra 服务帐户。
  b. 转到 Microsoft Entra 设备扩展属性页面，单击**添加扩展属性**。

使用 POWERSHELL

以下是与 Web Studio 中的操作等效的 PowerShell 步骤。有关如何使用远程 PowerShell SDK 创建目录的信息，请参阅 `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`。

本地 AD 加入的目录与 Microsoft Entra 混合加入的目录之间的区别在于身份池和计算机帐户的创建。

要为 Microsoft Entra 混合加入目录创建身份池以及帐户：

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"

New-AcctIdentity -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
-ADUserName "corp\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -All
-ADUserName "corp\admin1" -ADPassword $password
```

注意：

`$password` 是具有写入权限的 AD 用户帐户的匹配密码。

用于创建 Microsoft Entra 混合加入的目录的所有其他命令与传统本地 AD 加入的目录相同。

要创建具有指定扩展属性的新身份池并将其与服务帐户关联，请运行以下命令：

```
New-AcctIdentityPool -IdentityPoolName HybridAzureAD -NamingScheme ACC####
-NamingSchemeType Numeric -Domain "abc.local" -IdentityType HybridAzureAD
-ServiceAccountUid $serviceAccountUid -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

当虚拟机首次开机并加入 Microsoft Entra ID 后，它会将其 Entra ID deviceId 报告给 MCS。

例如：要检查 `EntraIDDeviceID`，请运行 `Get-AcctADAccount` 或 `Get-AcctIdentity`。

```
Get-AcctADAccount -IdentityPoolName MyPool
```

重启后，对于持久和非持久虚拟机，`EntraIDDeviceID` 保持不变。

注意：

当您从目录中删除虚拟机但未从 Azure 中删除时，MCS 会自动删除关联的设备 ID 和扩展属性。

要编辑现有目录的扩展属性，请运行以下命令：

注意：

- 将现有目录 VM 升级到 VDA 2511 或更高版本后，需要重新启动。此重新启动允许 VM 将其 Entra ID deviceId 报告给 MCS，从而使 MCS 能够配置 VM 的扩展属性。
- 现有目录应具有具有“Device.ReadWrite.All”权限的 AzureAD 类型服务帐户。

要添加一些新属性：

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

要删除一些现有属性

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{}
```

或

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{extensionAttribute1 = ""; extensionAttribute2 = ""}
```

`Set-AcctIdentityPool` 还会更新已加入 Entra ID 并在其身份中拥有 `EntraIDDeviceID` 值的 VM 的 Entra ID 设备的扩展属性。

查看 MICROSOFT ENTRA 混合加入过程的状态

在 Web Studio 中，当交付组中的 Microsoft Entra 混合加入计算机处于开机状态时，可以查看 Microsoft Entra 混合加入过程的状态。要查看状态，请使用 搜索 识别这些计算机，然后对于每台计算机，检查下部窗格中“**详细信息**”选项卡上的“**计算机身份**”。以下信息可能会显示在“**计算机身份**”中：

- Microsoft Entra 混合加入
- 尚未加入 Microsoft Entra ID

> **注意：**
>
> - 计算机初次开机时，您可能会遇到 Microsoft Entra 混合加入延迟。这是由默认的计算机身份同步间隔（Microsoft Entra Connect 的 30 分钟）引起的。计算机仅在通过 Microsoft Entra Connect 将计算机身份同步到 Microsoft Entra ID 后才处于 Microsoft Entra 混合加入状态。
> - 如果计算机未能处于 Microsoft Entra 混合加入状态，它们不会向 Delivery Controller 注册。它们的注册状态显示为“**初始化**”。

> 此外，您还可以使用 Web Studio 了解计算机不可用的原因。为此，请在“**搜索**”节点上单击一台计算机，检查下部窗格中“**详细信息**”选项卡上的“**注册**”，然后阅读工具提示以获取更多信息。

故障排除

如果计算机未能进行 Microsoft Entra 混合加入，请执行以下操作：

- 检查计算机帐户是否已通过 Microsoft Microsoft Entra ID 门户同步到 Microsoft Entra ID。如果已同步，则会显示“**尚未加入 Microsoft Entra ID**”，表示注册状态待定。

  要将计算机帐户同步到 Microsoft Entra ID，请确保：

  - 计算机帐户位于配置为与 Microsoft Entra ID 同步的 OU 中。即使计算机帐户位于配置为同步的 OU 中，没有 **userCertificate** 属性的计算机帐户也不会同步到 Microsoft Entra ID。
  - **userCertificate** 属性在计算机帐户中填充。使用 Active Directory Explorer 查看该属性。

  - 计算机帐户创建后，Microsoft Entra Connect 必须至少同步过一次。如果没有，请在 Microsoft Entra Connect 计算机的 PowerShell 控制台中手动运行 `Start-ADSyncSyncCycle -PolicyType Delta` 命令以触发立即同步。

- 通过查询 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix** 下的 **DeviceKeyPairRestored** 值，检查 Citrix 托管的 Microsoft Entra 混合加入设备密钥对是否已正确推送到计算机。

  验证该值是否为 1。如果不是，可能的原因是：

  - 与预配方案关联的身份池的 `IdentityType` 未设置为 `HybridAzureAD`。您可以通过运行 `Get-AcctIdentityPool` 来验证这一点。
  - 计算机未通过计算机目录的相同预配方案进行预配。
  - 计算机未加入本地域。加入本地域是 Microsoft Entra 混合加入的先决条件。

- 通过在 MCS 预配的计算机上运行 `dsregcmd /status /debug` 命令来检查诊断消息。

  - 如果 Microsoft Entra 混合加入成功，则命令行输出中的 **AzureAdJoined** 和 **DomainJoined** 均为 **YES**。
  - 如果不是，请参阅 Microsoft 文档以排查问题：`<https://docs.microsoft.com/zh-cn/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>`。
  - 如果您收到错误消息 **Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**，请运行以下 PowerShell 命令来修复用户证书：

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
    UserCertificate
    ```

    有关用户证书问题的更多信息，请参阅 CTX566696。

创建已注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录

您可以为已注册到 Microsoft Intune 的 Microsoft Entra 混合加入目录创建启用共同管理的目录，用于持久性单会话和多会话 VM。您可以使用 Studio 和 PowerShell 创建启用共同管理的目录。

使用 WEB STUDIO

以下信息是对 创建计算机目录 中指南的补充。

在“**计算机目录设置**”向导中：

- 在“**计算机身份**”页面上，选择“**Microsoft Entra 混合加入**”，然后选择“**使用 Configuration Manager 将计算机注册到 Microsoft Intune**”。通过此操作，Configuration Manager 和 Microsoft Intune（即共同管理）将管理 VM。

使用 POWERSHELL

以下是与 Studio 中的步骤等效的 PowerShell 步骤。

要使用 Remote PowerShell SDK 通过 Configuration Manager 将计算机注册到 Microsoft Intune，请在 `New-AcctIdentityPool` 中使用 `DeviceManagementType` 参数。此功能要求目录已加入 Microsoft Entra 混合，并且 Microsoft Entra ID 拥有正确的 Microsoft Intune 许可证。

Microsoft Entra 混合加入目录与启用共同管理的目录之间的区别在于身份池的创建。例如：

```
New-AcctIdentityPool -AllowUnicode -DeviceManagementType "IntuneWithSCCM"
IdentityType="HybridAzureAD" -IdentityPoolName "CoManagedCatalog"
-NamingScheme "CoManaged-VM-##" -NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
```

故障排除

如果计算机未能注册到 Microsoft Intune 或未能达到共同管理状态，请执行以下操作：

- 检查 Intune 许可证

  检查您的 Microsoft Entra 租户是否已分配适当的 Intune 许可证。有关 Microsoft Intune 的许可证要求，请参阅 Microsoft Intune 许可。

- 检查 Microsoft Entra 混合加入状态

  检查 MCS 预配的计算机是否已加入 Microsoft Entra 混合。如果未加入 Microsoft Entra 混合，则这些计算机不符合共同管理的条件。请参阅 故障排除 以排查 Microsoft Entra 混合加入问题。

- 检查共同管理资格

  - 检查 MCS 预配的计算机是否已正确分配到预期的 Configuration Manager 站点。要获取分配的站点，请在受影响的计算机上运行以下 PowerShell 命令。

    ```
    (New-Object -ComObject "Microsoft.SMS.Client").GetAssignedSite()
    ```

  - 如果未向 VM 分配站点，请使用以下命令检查 Configuration Manager 站点是否可以自动发现。

```
(New-Object -ComObject "Microsoft.SMS.Client").AutoDiscoverSite()
```

- 如果无法发现站点代码，请确保在 Configuration Manager 环境中正确配置了边界和边界组。有关详细信息，请参阅 注意事项。
- 检查 `C:\Windows\CCM\Logs\ClientLocation.log` 以了解任何 Configuration Manager 客户端站点分配问题。
- 检查计算机的共同管理状态。在受影响的计算机上打开**Configuration Manager 控制面板**，然后转到**常规**选项卡。共同管理属性的值必须为**已启用**。如果不是，请检查 `C:\Windows\CCM\Logs\CoManagementHandler.log` 下的日志。

- 检查 Intune 注册

  即使满足所有先决条件，计算机也可能无法注册到 Microsoft Intune。请检查 **应用程序和服务日志 > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider** 下的 Windows 事件日志，以查找 Intune 注册问题。

未加入域的计算机身份的身份池

本文介绍如何使用 Citrix Virtual Apps and Desktops 创建未加入域的目录的身份池。

有关要求、限制和注意事项的信息，请参阅 未加入域。

在创建计算机目录之前，您需要满足以下条件：

1. 新的资源位置
   - 导航到 Citrix Cloud™ 管理员 UI > 左上角汉堡菜单 > **资源位置**。
   - 单击 **+ 资源位置**。
   - 输入新资源位置的名称，然后单击 **保存**。
2. 创建托管连接。有关详细信息，请参阅 创建和管理连接 部分。

使用 Citrix Virtual Apps and Desktops™，您可以创建基于工作组或未加入域的计算机的目录。创建未加入域的计算机取决于帐户身份池的创建方式。帐户身份池是 MCS 在目录预配期间用于创建和跟踪计算机名称的机制。

使用 Web Studio

以下信息是对 创建计算机目录 中指南的补充。

在目录创建向导中：

- 在“**计算机身份**”页面上，选择“**未加入域**”。创建的计算机未加入任何域。

> **注意：**
>
> **未加入域**身份类型要求 VDA 版本为 2311 或更高版本，作为目录的最低功能级别。要使其可用，请在必要时更新最低功能级别。

使用 PowerShell

您可以使用 Remote PowerShell SDK 为未加入域的目录创建身份池。

使用 PowerShell 参数 **WorkgroupMachine** 和 **IdentityType** 为未加入域的目录创建身份池。这些参数无需指定所有 AD 特定参数，包括域管理员凭据：

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup"
-WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme
"NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"
```

用于创建未加入域的目录的所有其他命令与用于传统本地 Active Directory 加入的目录的命令相同。

管理计算机目录

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中移除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

简介

您可以从计算机目录中添加或移除计算机、重命名、更改描述或管理目录的 Active Directory 计算机帐户。

维护目录还包括确保每台计算机都具有最新的操作系统更新。包括防病毒更新、操作系统升级或配置更改。

- 包含使用 Machine Creation Services™ (MCS) 创建的池化随机计算机的目录通过更新目录中使用的主映像，然后更新计算机来维护计算机。此方法使您能够高效地更新大量用户计算机。
- 对于包含静态、永久分配的计算机的目录以及远程 PC 访问计算机目录，您可以在 Web Studio 之外管理用户计算机的更新。可以使用第三方软件分发工具单独或集体执行此任务。

有关创建和管理到主机管理程序的连接的信息，请参阅连接和资源。

> **注意：**
>
> MCS 不支持 Windows 10 IoT Core 和 Windows 10 IoT Enterprise。有关详细信息，请参阅 Microsoft 站点。

关于持久性实例

更新使用持久或专用实例创建的 MCS 目录时，为该目录创建的任何新计算机都将使用更新后的映像。现有实例将继续使用原始实例。更新映像的过程与任何其他类型的目录相同。请考虑以下事项：

- 对于持久性磁盘目录，现有计算机不会更新到新映像，但添加到目录中的任何新计算机都使用新映像。
- 对于非持久性磁盘目录，计算机映像将在下次计算机重置时更新。
- 对于持久性计算机目录，更新映像也会更新使用该映像的目录实例。
- 对于非持久性目录，如果您希望不同计算机使用不同的映像，则这些映像必须位于单独的目录中。

管理计算机目录

您可以通过两种方式管理计算机目录：

- 使用 Web Studio
- 使用 PowerShell

使用 Web Studio

本节详细介绍了如何使用 Web Studio 管理目录：

- 管理计算机目录
  - 简介
  - 关于持久实例

- 管理计算机目录
- 使用 Web Studio
- 查看目录详细信息
  - 向目录添加计算机
  - 从目录中删除计算机
- 编辑目录
- 重命名目录
- 将目录移动到其他区域(#move-a-catalog-to-a-different-zone)
- 删除目录
- (#将 Azure 中的旧版 MCS 目录转换为基于计算机配置文件的目录)
- 管理目录中的 Active Directory 计算机帐户
- 更新目录(#update-a-catalog)
  - 更新或创建主映像(#update-or-create-a-master-image)
  - 更改主映像(#change-the-master-image)
  - 回滚主映像(#roll-back-the-master-image)
- 更改功能级别或撤消更改
- 克隆目录
- 使用文件夹组织目录
  - 创建目录文件夹(#create-a-catalog-folder)
  - 移动目录(#move-a-catalog)
  - 管理目录文件夹(#manage-catalog-folders)
- 升级 VDA
- 重试目录创建
- 使用令牌注册非 MCS 预配的 VDA(#enroll-non-mcs-provisioned-vdas-using-tokens)
- 使用 PowerShell(#use-powershell)
- 检索与目录相关的警告和错误
- 向映像添加描述
- 重置操作系统磁盘

- 更改现有预配方案的网络设置(#change-the-network-setting-for-an-existing-provisioning-scheme)
- 管理计算机目录的版本
- 将非计算机配置文件型计算机目录转换为计算机配置文件型计算机目录
- 修复活动计算机帐户的身份信息
  - 条件(#conditions)
  - 重置身份磁盘(#reset-identity-disk)
- 更改现有计算机目录上的缓存配置(#change-cache-configuration-on-an-existing-machine-catalog)
  - 要求
  - 更改缓存配置
- 通过本地文件共享访问支持 VDA 更新
  - PowerShell 命令
  - 先决条件
  - 如何设置文件共享权限
  - 从本地文件共享更新 VDA
- 故障排除
- 后续步骤

查看目录详细信息

1. 使用搜索功能查找特定的计算机目录。有关说明，请参阅 搜索实例。
2. 根据需要从搜索结果中选择一个目录。
3. 有关目录列的说明，请参阅下表。
4. 有关目录列的说明，请参阅下表。

列	描述
计算机目录	目录的名称和分配类型。分配类型包括
	• 随机：目录中的计算机随机分配给用户。
	• 永久：目录中的计算机永久分配给用户。

列	描述
计算机类型	目录中计算机支持的会话类型。可能的值包括
	• 操作系统类型：多会话操作系统（虚拟）；用户数据：丢弃。
	• 操作系统类型：多会话操作系统（虚拟）；用户数据：在本地磁盘上
	• 操作系统类型：单会话操作系统（远程电脑访问）
	• 操作系统类型：单会话操作系统（虚拟）；用户数据：丢弃
	• 操作系统类型：单会话操作系统（虚拟）；用户数据：在本地磁盘上
计算机数量	目录中的计算机数量和预配方法。可能的预配方法包括：Machine Creation Services (MCS 计算机)、手动和 Citrix Provisioning™ Services。
已分配数量	目录中分配给交付组的计算机数量。
文件夹	目录在**计算机目录**树中的位置。它显示目录所在的文件夹名称（包括尾随的反斜杠），如果目录位于根级别，则显示 `-`。
VDA 升级	VDA 升级状态。可能的值包括：未配置、已计划、可用和最新。
映像状态	目录映像更新的状态。仅适用于非持久性计算机目录。可能的值包括：完全更新、部分更新、待定更新、正在准备

5. 单击底部详细信息窗格中的选项卡，以获取有关所选目录的更多信息。

选项卡	描述
详细信息	总结了关键的计算机目录设置，例如计算机类型、预配方法、服务帐户、操作系统和 VDA 版本，使您能够快速查看和管理资源。
模板属性	仅适用于 MCS 预配的目录。
	显示所选目录的详细预配信息，包括
	• 计算机模板属性
	• 管理程序特定详细信息
	• 计算机配置文件属性
计算机	显示所选目录中计算机名称的分页列表。
交付组	适用于远程电脑目录。
	显示与所选目录关联的交付组。它显示交付组名称和目录关联。
标签	在多租户环境中不可用。
	显示分配给所选计算机目录的标签名称和标签说明。
工作区环境管理	仅当 WEM 服务已预配且可访问时可见。
	显示工作区环境管理系统优化设置。
成本洞察	仅适用于 Azure MCS 目录，此项显示
	• 过去 30 天内产生的总成本。
	• 当前 30 天总成本与前一个 30 天期间的比较。
	访问此选项卡需要 Citrix **成本管理 > 管理 > 读取成本** 权限（云管理员的默认权限），并且需要 `Microsoft.CostManagement/query/read` Azure 权限才能查看成本详细信息。

选项卡	描述
故障排除	显示目录错误或警告以及建议的操作。

将计算机添加到目录

开始之前：

- 确保虚拟化主机具有足够的处理器、内存和存储来容纳其他计算机。
- 确保您有足够的未使用的 Active Directory 计算机帐户。如果您使用现有帐户，则可以添加的计算机数量受可用帐户数量的限制。
- 如果您使用 Web Studio 为其他计算机创建 Active Directory 计算机帐户，则必须具有相应的域管理员权限。

要将计算机添加到目录：

1. 在 Studio 中，选择左侧窗格中的**计算机目录**。
2. 选择一个计算机目录，然后在操作栏中选择**添加计算机**。
3. 在**虚拟机**页面上，选择要添加的虚拟机数量。
4. 在**计算机身份**页面上，按如下方式配置设置：
   - 从列表中选择一个身份。
   - 如果适用，指示是创建帐户还是使用现有帐户，以及这些帐户的位置（域）。

     如果现有 Active Directory 帐户不足以满足您要添加的 VM 数量，请选择创建帐户的域和位置。

     如果您使用现有 Active Directory 帐户，请浏览到这些帐户，或者选择**导入**并指定一个包含帐户名称的 `.csv` 文件。确保有足够的帐户用于您要添加的所有计算机。Studio 管理这些帐户。允许该界面重置所有帐户的密码，或者指定帐户密码（所有帐户的密码必须相同）。
   - 如果此身份池被其他目录使用，则无法使用 Studio 将其更改为其他池。请改用 **Set-ProvScheme** PowerShell cmdlet。
   - 指定帐户命名方案，使用井号标记指示序列号或字母出现的位置。例如，命名方案 PC-Sales-##（选择 0-9）将生成名为 PC-Sales-01、PC-Sales-02、PC-Sales-03 等的计算机帐户。
   - （可选）您可以指定帐户名称的开头。

     指定帐户名称的开头时，请注意以下情况：如果起始数字或字母已被使用，则创建的第一个帐户将使用其后最近的未使用数字或字母命名。

5. 在**域凭据**页面上，选择**输入凭据**并输入具有足够权限以创建计算机帐户的用户凭据。

计算机以后台进程的形式创建，并且在创建大量计算机时可能需要很长时间。即使关闭 Studio，计算机创建也会继续。

从目录中删除计算机

从计算机目录中删除计算机后，用户将无法再访问它，因此在删除计算机之前，请确保：

- 用户数据已备份或不再需要。
- 所有用户均已注销。启用维护模式可阻止新连接连接到计算机。
- 计算机已关机。

要从目录中删除计算机，请执行以下操作：

1. 登录到 Web Studio。
2. 在左侧窗格中选择**计算机目录**。
3. 选择一个目录，然后在操作栏中选择 **查看计算机**。
4. 选择一台或多台计算机，然后在操作栏中选择 **删除**。

选择是否删除正在移除的计算机。如果您选择删除计算机，请指明这些计算机的 Active Directory 帐户是保留、禁用还是删除。

编辑目录

1. 在**描述**页面上，更改目录描述。
2. 在左侧窗格中选择**计算机目录**。
3. 选择一个目录，然后在操作栏中选择 **编辑计算机目录**。
4. 在 **范围** 页面上，更改范围。
5. 在 **NIC** 页面上，执行以下操作：

   - 要更改 NIC 的子网映射，请从 **关联的网络** 字段中选择一个网络。
   - 要添加子网映射，请选择 **添加 NIC**，从 **关联的网络** 字段中选择一个网络，然后单击 **保存**。

   只有与目录关联的主机中存在的子网才会显示在 **关联的网络** 字段中。

   您只能将 NIC 添加到没有计算机配置文件的 Azure 计算机目录。

> **注意：**

- 对于 AWS 计算机目录，您不能将同一个子网映射到多个 NIC。
- 对于具有计算机配置文件的计算机目录，目录上的 NIC 数量必须等于计算机配置文件上的 NIC 数量。
- IBM Cloud 管理程序不支持此功能。
- 此功能仅在 Nutanix 虚拟机管理程序的情况下支持 Nutanix Prism Element。

6. 您可能会看到其他页面，具体取决于目录类型。

   对于使用 Azure Resource Manager 映像创建的目录，将显示以下页面。请记住，您所做的更改仅适用于以后添加到目录的计算机。现有计算机保持不变。

   - 在**虚拟机**页面上，更改要创建计算机的计算机大小和可用区。

     注意：

     - 仅显示目录支持的计算机大小。
     - 如有必要，选择**仅显示其他计算机目录中使用的计算机大小**以筛选计算机大小列表。
     - 对于 Azure 目录，如果“**存储和许可证类型**”页面上的“**存储冗余**”为“**ZRS**”，则会收到一条警告，建议清除区域选择并让 Azure 管理 VM 可用性区域。

   - 在**计算机配置文件**页面上，选择是使用还是更改计算机配置文件。

     注意：

     对于 Azure 目录，当您修改包含可用区并选择 ZRS 作为存储冗余的计算机配置文件时，会收到警告，建议您清除区域选择。

   - （仅当目录配置了专用组主机时可见）在“**专用主机组**”页面上，选择是否更改主机组。
   - 在**存储和许可证类型**页面上，选择是否更改存储冗余类型（适用于 Azure 目录）、存储类型、许可证类型和 Azure 计算机库设置（仅当使用**将准备好的映像放置在 Azure 库中**时可用）。

> **注意：**
>
> 如果新选择的设置不支持当前计算机大小，则会出现一个警告对话框，通知您更改设置会重置计算机大小设置。如果您选择继续，则“**虚拟机**”菜单旁边会出现一个红点，提示您选择新的计算机大小。

- 在“**许可证类型**”页面上，选择是否更改 Windows 许可证或 Linux 许可证设置。

对于远程电脑访问目录，将显示以下页面：

- 在**电源管理**页面上，更改电源管理设置并选择电源管理连接。
- 在**组织单位**页面上，添加或删除 Active Directory OU。

7. 单击**应用**以应用所做的更改，然后单击**保存**以退出。

重命名目录

1. 登录到 Web Studio。
2. 在左侧窗格中选择**计算机目录**。
3. 选择一个目录，然后在操作栏中选择**重命名计算机目录**。
4. 输入新名称。

将目录移动到其他区域

如果您的部署具有多个区域，则可以将目录从一个区域移动到另一个区域。

将目录移动到包含该目录中 VM 的管理程序以外的其他区域会影响性能。

1. 登录到 Web Studio。
2. 在左侧窗格中选择**计算机目录**。
3. 选择一个目录，然后在操作栏中选择“**移动**”。
4. 选择要将目录移动到的区域。

删除目录

删除目录之前，请确保：

- 所有用户均已注销，并且您未运行任何断开连接的会话。
- 目录中的所有计算机均已启用维护模式，以便无法建立新连接。
- 目录中的所有计算机均已关机。

- 目录未关联交付组。换句话说，交付组不包含来自该目录的计算机。

要删除目录，请执行以下操作：

1. 登录到 Web Studio。
2. 在左侧窗格中选择**计算机目录**。
3. 选择一个目录，然后在操作栏中选择**删除计算机目录**。
4. 指示目录中的计算机是否被删除。如果您选择删除计算机，指示这些计算机的 Active Directory 计算机帐户是保留、禁用还是删除。

将 Azure 中的旧版 MCS 目录转换为基于计算机配置文件的目录

要将非基于计算机配置文件的计算机目录转换为基于计算机配置文件的计算机目录，请完成以下步骤：

1. 在**计算机目录**页面上，右键单击要转换的**计算机目录**名称，然后选择**编辑计算机目录**。
2. 在**编辑计算机目录 > 计算机配置文件**页面上，选中**使用计算机配置文件（Microsoft Entra ID 必需）**复选框。
3. 单击**选择计算机配置文件**。
4. 在**选择计算机配置文件**页面上，选择要用作计算机配置文件的虚拟机或启动模板。
5. 如果某些当前设置与新的计算机配置文件设置不同，请为要使用的设置选择所需选项，然后单击**继续**。
6. 单击**应用**。

> **注意：**
>
> 目前，此功能仅支持 Azure、AWS 和 VMware。

管理目录中的 Active Directory 计算机帐户

要管理计算机目录中的 Active Directory 帐户，您可以：

- 通过从单会话操作系统和多会话操作系统目录中删除 Active Directory 计算机帐户来释放未使用的计算机帐户。然后，这些帐户可用于其他计算机。
- 添加帐户，以便在向目录添加更多计算机时，计算机帐户已就位。请勿在 OU 名称中使用正斜杠 (/)。

要管理 Active Directory 帐户：

1. 登录到 Web Studio。
2. 在左侧窗格中选择**计算机目录**。
3. 选择一个目录，然后在操作栏中选择**管理 AD 帐户**。
4. 选择是添加还是删除计算机帐户。如果添加帐户，请指定如何处理帐户密码：要么全部重置，要么输入一个适用于所有帐户的密码。

   如果您不知道当前帐户密码，可以重置密码；您必须具有执行密码重置的权限。输入密码时，导入帐户时会更改其密码。删除帐户时，选择 Active Directory 中的帐户是保留、禁用还是删除。

指示在从目录中删除计算机或删除目录时，Active Directory 帐户是保留、禁用还是删除。

更新目录

建议您在更新目录中的计算机之前保存主映像的副本或快照。数据库会保留每个计算机目录所使用的主映像的历史记录。回滚或还原目录中的计算机以使用主映像的先前版本。如果用户遇到您部署到其桌面的更新问题，请执行此任务。这可最大程度地减少用户停机时间。请勿删除、移动或重命名主映像。您无法将目录还原为使用它们。

计算机更新后，会自动重新启动。

更新或创建主映像

在更新计算机目录之前，请更新现有主映像或在主机管理程序上创建一个主映像。

1. 在您的管理程序上，拍摄当前 VM 的快照并为该快照指定一个有意义的名称。如果需要，此快照可用于还原（回滚）目录中的计算机。
2. 如有必要，启动主映像，然后登录。
3. 安装更新或对主映像进行任何必要的更改。
4. 关闭 VM。
5. 拍摄虚拟机的快照。为其指定一个有意义的名称，以便在 Web Studio 中更新目录时能够识别。尽管 Web Studio 可以创建快照，但 Citrix 建议您使用管理程序管理控制台创建快照。然后在 Web Studio 中选择该快照。此过程使您能够提供有意义的名称和描述，而不是自动生成的名称。对于 GPU 主映像，您只能通过 XenServer® 控制台更改主映像。

更改主映像

要准备并将更新推出到目录中的所有计算机，请执行以下操作：

1. 登录到 Web Studio。
2. 在左侧窗格中选择**计算机目录**。
3. 选择一个目录，然后在操作栏中选择**更改主映像**。

4. 在**映像**页面上，选择要部署的主机和映像。

> **提示：**
>
> 对于 MCS 创建的目录，您可以通过为映像添加备注来对其进行批注。备注最多可包含 500 个字符。每次更改主映像时，无论您是否添加备注，都会创建一个与备注相关的条目。如果您在未添加备注的情况下更新目录，则该条目显示为 null (-)。要查看映像的备注历史记录，请选择目录，单击下部窗格中的**模板属性**，然后单击**查看备注历史记录**。

5. 在**推出策略**页面上，选择何时使用新的主映像更新计算机目录中的计算机：在下次关机时或立即更新。

> **注意：**
>
> **部署策略**页面不适用于持久性 VM，因为部署仅适用于非持久性 VM。

6. 验证**摘要**页面上的信息，然后单击**完成**。每台计算机更新后会自动重新启动。

要跟踪更新进度，请在**计算机目录**中找到该目录，以查看内联进度条和分步进度图。

当直接使用 PowerShell SDK 而不是 Web Studio 更新目录时，请指定一个管理程序模板 (**VMTemplates**)。将其用作映像或映像快照的替代方案。

要将新的主映像推出到基于 Azure 的计算机目录，请执行以下操作：

1. 在 Web Studio 中，选择左侧窗格中的**计算机目录**。
2. 选择一个 Azure 目录，然后在操作栏中选择“**更改主映像**”。
3. 在“**更改主映像**”页面上，在“主映像”下选择一个映像。该边栏列出了与资源属于同一区域的所有映像。

推出策略：

在下次关机时更新映像将立即影响任何当前未使用的计算机，即没有活动用户会话的计算机。正在使用的系统将在当前活动会话结束时收到更新。请考虑以下事项：

- 在适用的计算机上完成更新之前，无法启动新会话。
- 对于单会话操作系统计算机，当计算机未使用或用户未登录时，计算机将立即更新。

- 对于具有子计算机的多会话操作系统，不会自动重新启动。要应用更新的主映像，请使用 Studio、PowerShell 或 Workspace 重新启动计算机。从计算机或管理程序重新启动不会应用更新。

> **提示：**
>
> 通过使用主机连接的高级设置来限制正在重新启动的计算机数量。使用这些设置可以修改给定目录所采取的操作；高级设置因虚拟机管理程序而异。

回滚主映像

推出更新或新的主映像后，您可以将其回滚。如果新更新的计算机出现问题，此过程可能是必需的。回滚时，目录中的计算机将回滚到上次正常工作的映像。任何需要较新映像的新功能将不再可用。与推出一样，回滚计算机也包括重新启动。

1. 登录到 Web Studio。
2. 在左侧窗格中选择**计算机目录**。
3. 选择目录，然后在操作栏中选择**回滚主映像**。
4. 指定何时将较早的主映像应用于计算机，如上一节中关于推出操作的描述。

回滚仅应用于需要还原的计算机。未通过新的或更新的主映像进行更新的计算机不会收到通知消息，也不会被强制注销。

要跟踪回滚进度，请在**计算机目录**中找到该目录，以查看内联进度条和分步进度图。

更改功能级别或撤消更改

在将计算机上的 VDA 升级到较新版本后，更改计算机目录的功能级别。Citrix 建议将所有 VDA 升级到最新版本，以启用对所有最新功能的访问。

更改计算机目录的功能级别之前：

- 启动已升级的计算机，使其向控制器注册。此过程允许 Web Studio 确定目录中的计算机需要升级。

要更改目录的功能级别：

1. 登录 Web Studio。
2. 在左侧窗格中选择**计算机目录**。
3. 选择目录。下部窗格中的**详细信息**选项卡显示版本信息。

4. 选择 **更改功能级别**。如果 Web Studio 检测到目录需要升级，它会显示一条消息。按照提示操作。如果一台或多台计算机无法升级，将显示一条消息解释原因。为确保所有计算机正常运行，Citrix 建议您在单击 **更改** 继续之前解决计算机问题。

目录更改完成后，您可以通过选择目录，然后在操作栏中选择 **撤消功能级别更改** 来将计算机还原到其以前的 VDA 版本。

克隆目录

克隆目录之前，请注意以下事项：

- 您无法更改与操作系统和计算机管理相关的设置。克隆的目录会从原始目录继承这些设置。

> **注意：**
>
> 如果您选择要克隆的 Azure 目录并选择主映像，则边栏选项卡会列出与资源属于同一区域的所有映像。

- 克隆目录可能需要一些时间才能完成。如有必要，请选择**隐藏进度**以在后台运行克隆。
- 克隆的目录继承了原始目录的名称，并带有一个后缀 `Copy`。您可以更改名称。请参阅 重命名目录。
- 克隆完成后，请务必将克隆的目录分配给交付组。

1. 登录 Web Studio，然后在左侧窗格中选择 **计算机目录**。
2. 选择一个目录，然后在操作栏中选择 **克隆**。
3. 在 **克隆选定的计算机目录** 窗口中，查看克隆目录的设置并根据需要配置设置。选择 **下一步** 以继续到下一页。
4. 在 **摘要** 页面上，查看设置摘要并选择 **完成** 以开始克隆。
5. 如有必要，选择 **隐藏进度** 以在后台运行克隆。

使用文件夹组织目录

您可以创建文件夹来组织目录，以便于访问。例如，您可以按映像类型或组织结构来组织目录。

> **提示：**
>
> 您可以通过单击操作栏右上角的 **文件夹** 图标，为“计算机目录”节点设置首选默认视图（文件夹视图或列表视图）。

创建目录文件夹

在开始之前，请先规划如何组织目录。请考虑以下事项：

- 您可以将文件夹嵌套最多五层（不包括默认根文件夹）。
- 目录文件夹可以包含目录和子文件夹。
- Web Studio 中的所有节点（例如 **计算机目录**、**交付组**、**应用程序** 和 **应用程序组**）在后端共享相同的文件夹树。为避免在重命名或移动文件夹时出现名称冲突，请为不同节点中的一级文件夹使用唯一的名称。

  如果您使用 `New-BrokerAdminFolder` SDK cmdlet 创建文件夹并希望它显示在**计算机目录**节点下，则必须使用 `Set-BrokerAdminFolderMetadata` cmdlet 添加 `ContainsMachineCatalogs` 元数据。

  示例：

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsMachineCatalogs -Value true
  ```

要创建目录文件夹，请按照以下步骤操作：

1. 在左侧窗格中选择**计算机目录**。
2. 在文件夹层次结构中，选择一个文件夹，然后在**操作**栏中选择**创建文件夹**。
3. 输入新文件夹的名称，然后单击**完成**。

> **提示：**
>
> 如果您在意外位置创建了文件夹，可以将其拖动到正确位置。

移动目录

您可以在文件夹之间移动目录。详细步骤如下：

1. 在左侧窗格中选择**计算机目录**。
2. 按文件夹查看目录。您还可以打开文件夹层次结构上方的 **查看所有** 以一次性查看所有目录。
3. 右键单击目录，然后选择 **移动计算机目录**。
4. 选择要将目录移动到的文件夹，然后单击 **完成**。

> **提示：**
>
> 您可以将目录拖动到文件夹中。

管理目录文件夹

您可以删除、重命名和移动目录文件夹。

仅当文件夹及其子文件夹不包含目录时，才能删除该文件夹。

要管理文件夹，请按照以下步骤操作：

1. 在左侧窗格中选择**计算机目录**。
2. 在文件夹层次结构中，选择一个文件夹，然后根据需要选择 **操作** 栏中的操作：
   - 要重命名文件夹，请选择 **重命名文件夹**。
   - 要删除文件夹，请选择 **删除文件夹**。
   - 要移动文件夹，请选择 **移动文件夹**。
3. 按照屏幕上的说明完成剩余步骤。

升级 VDA

您可以使用 Studio 界面轻松升级 VDA。有关详细信息和分步指导，请参阅 Citrix VDA 升级服务 文档。

重试目录创建

> **注意：**
>
> 此功能仅适用于 MCS 目录。

> 失败的目录会标有错误图标。要查看详细信息，请转到每个目录的**故障排除**选项卡。在重试创建目录之前，请注意以下事项：

- 首先检查故障排除信息并解决问题。该信息描述了发现的问题并提供了解决这些问题的建议。
- 您无法更改与 操作系统 和 计算机管理 相关的设置。目录会从原始目录继承这些设置。
- 创建可能需要一些时间才能完成。如有必要，请选择**隐藏进度**以在后台运行创建。

要重试创建目录，请执行以下操作：

1. 在 Web Studio 中，选择左侧窗格中的 **计算机目录**。
2. 选择目录，然后转到其**故障排除**选项卡。
3. 单击重试超链接以重试创建目录。
4. 在出现的向导中，根据需要更改设置。如果无需进行更改，可以直接转到**摘要**页面。
5. 完成后，选择**完成**以开始创建。

使用令牌注册非 MCS 预配的 VDA

您现在可以为非 MCS 预配的 VDA 生成和管理注册令牌。此实现允许通过 WebSocket 进行 VDA 注册，而无需使用 MCS 预配 VDA。此功能还支持 Linux Virtual Delivery Agent、适用于 macOS 的 Citrix Virtual Delivery Agent 以及与 Citrix Virtual Apps and Desktops™ 配合使用的非域加入 VDA。

开始之前

1. 配置您的站点。有关详细信息，请参阅 创建站点。
2. 在 Delivery Controller 上安装 TLS 证书。有关详细信息，请参阅 在控制器上安装 TLS 服务器证书。
3. 在 VDA 上安装根 CA 和中间 CA 以信任 Delivery Controller。
4. 在 Delivery Controller 上启用 WebSocket 连接。在站点中的每个 Delivery Controller 上运行以下命令：

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy"
-Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
```

> **注意：**
>
> 确保在启用 WebSocket 后重新启动 Delivery Controller。

生成注册令牌

在决定为非 Citrix 预配的计算机启用基于令牌的注册后，您必须首先按计算机目录生成令牌，然后与 VDA 安装管理员共享这些令牌。

注册令牌具有以下特点：

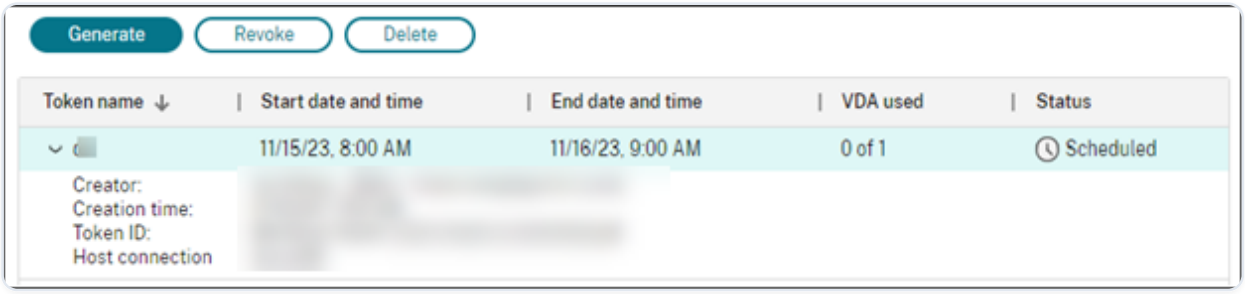
- 注册范围：1–5000 台 VDA 计算机

- 有效期：最长 14 天

要使用 Web Studio 为目录生成令牌，请执行以下步骤：

1. 在 **Web Studio > 计算机目录**中，找到一个非 MCS 预配的目录，该目录在“**计算机计数**”列中显示“**预配方法: 手动**”。
2. 右键单击该目录，然后选择“**管理注册令牌**”。
3. 在出现的“**生成注册令牌**”页面上，提供以下令牌信息：
   - 键入令牌的名称。
   - 输入其有效期。有效期不得超过 14 天。令牌仅在指定期间内有效。
   - （可选）选择一个主机连接，用于对使用该令牌注册的 VDA 进行电源管理。选项包括此目录区域下的所有主机连接。
   - 输入令牌使用限制（介于 1–5000 之间）。
4. 单击“**生成**”。
5. 在出现的“**令牌已成功生成**”窗口中，复制令牌并将其保存在安全位置，或者单击“**下载**”将其下载到“**下载**”文件夹。

   令牌记录将显示在令牌列表中。



6. 将令牌共享给 VDA 安装管理员。

   有关如何在计算机上安装 VDA 和令牌的详细信息，请参阅 安装 VDA。

管理令牌

您可以通过两种方式撤销令牌并使其无法用于 VDA 注册：

- 撤销：撤销令牌，但将其保留在列表中以用于日志记录。
- 删除：撤销令牌并将其从列表中删除。

> **注意：**

> 过期令牌会在 14 天内自动删除。

使用 WebSocket VDA 注册工具将计算机注册到目录

WebSocket VDA 注册工具方便了 VDA 计算机的基于令牌的注册。此工具通过使用注册令牌将 VDA 添加到计算机目录来帮助您将连接转换为 WebSocket 连接。

> **注意：**
>
> 此工具旨在注册尚未注册到任何计算机目录的 VDA 计算机。

> 按照说明运行注册工具：

1. 登录到 VDA。
2. 在 `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool` 中找到工具 `EnrollMachine.exe`。
3. 使用适当的输入参数运行该工具。例如， `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

下表描述了注册工具的输入参数：

参数名称	必需	描述	示例
`-websocket_token_stdin`	是	读取注册令牌。	`.\EnrollMachine.exe -websocket_token_stdin`
`-websocket_token_string`		直接从命令行参数读取注册令牌。	`.\EnrollMachine.exe -websocket_token_string:<token>`
`-websocket_token_file:[token-file-path]`		从提供的路径读取注册令牌。	`.\EnrollMachine.exe -websocket_token_`

参数名称	必需	描述	示例
			`file:C:\token\test2.txt`
`log:[log-file-path]`	否	显示注册工具日志。	`.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]`
`-help`	否	显示简要帮助文本。	`.\EnrollMachine.exe -help`

成功注册后，您将在工具和日志中收到成功消息。请务必登录 Web Studio 以验证 VDA 计算机是否已添加到目录中，并且计算机的状态是否已注册。

故障排除

默认情况下，您可以在以下位置找到注册工具的日志：

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

如果您为日志指定了不同的路径，可以使用 `log:[log-file-path]` 来检索日志。

下表列出了注册工具返回的代码：

代码	字符串	描述
0	成功	VDA 已成功添加到计算机目录。
-1	无效参数	注册令牌中的输入参数无效。
-2	未找到代理代理	未找到代理代理服务。
-3	令牌无效	输入的令牌无效。
-4	令牌缺少所需声明	令牌缺少所需的声明，例如 CustomerId 或注册 URI。

代码	字符串	描述
-5	内部错误	发生了一般性错误。
-6	超时	任务已超时。
-7	无法确定计算机AD加入状态	返回计算机AD加入状态的服务失败。
-8	AD计算机无法找到Sid	返回AD计算机Sid的服务失败。
-9	注册请求失败	请求因HTTP错误而失败。
-10	注册响应缺少必填字段	注册工具响应缺少参数 `VirtualSiteId`。
-11	权限不足	您没有运行此任务所需的权限。
-12	无法确定计算机Aad加入状态	检查计算机AD加入状态的服务抛出错误。
-13	Aad计算机未能找到设备ID	系统添加的附加参数 `AAD device id` 为空。
-14	Aad设备ID无效	由系统添加的附加参数 `AAD device id` 不是有效的GUID。
-15	无有效MAC地址	MAC 地址无效。
-16	FailedToGetComputerHostNameForVdaInstanceName	未能获取计算机主机名以设置附加参数 `VdaInstanceName`。
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	未能打开 VDA 注册表项以写入交付控制器列表。
-18	失败的令牌已达到最大计数	失败的令牌已达到最大计数。

使用 PowerShell

本节详细介绍了如何使用 PowerShell 管理目录：

- 检索与目录相关的警告和错误
- 向映像添加描述
- 重置操作系统磁盘
- 更改现有预配方案的网络设置
- 管理计算机目录的版本
- 将非计算机配置文件型计算机目录转换为计算机配置文件型计算机目录
- 修复活动计算机帐户的身份信息
- 更改现有计算机目录上的缓存配置
- 通过本地文件共享访问支持 VDA 更新

检索与目录关联的警告和错误

您可以获取历史错误和警告，以了解 MCS 计算机目录的问题并修复这些问题。

使用 PowerShell 命令，您可以执行以下操作：

- 获取错误或警告列表
- 将警告状态从**新建**更改为**已确认**
- 删除错误或警告

要运行 PowerShell 命令，请执行以下操作：

1. 打开一个 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。

要获取错误和警告列表：

运行 `Get-ProvOperationEvent` 命令。

- 无参数：获取所有错误和警告
- 使用 `LinkedObjectType` 和 `LinkedObjectUid` 参数：获取与特定预配方案关联的所有错误和警告
- 使用 `EventId` 参数：获取与此事件 ID 匹配的特定错误或警告
- 使用 `Filter` 参数：通过自定义筛选器获取错误或警告

要将错误或警告的状态从 **New** 更改为 **Acknowledged**：

运行 `Confirm-ProvOperationEvent` 命令。

- 使用 `EventId` 参数：设置与此事件 ID 匹配的特定错误或警告的状态。您可以从 `Get-ProvOperationEvent` 命令的输出中获取特定错误或警告的 `EventId`
- 使用 `LinkedObjectType` 和 `LinkedObjectUid` 参数：设置与特定预配方案关联的所有错误和警告的状态
- 使用 `All` 参数：将所有错误和警告的状态设置为 **Acknowledged**

要删除错误或警告：

运行 `Remove-ProvOperationEvent` 命令。

- 使用 `EventId` 参数：删除与此事件 ID 匹配的特定错误或警告。您可以从 `Get-ProvOperationEvent` 命令的输出中获取特定错误或警告的 `EventId`。
- 使用 `LinkedObjectType` 和 `LinkedObjectUid` 参数：删除与特定预配方案关联的所有错误和警告。
- 使用 `All` 参数：删除所有错误和警告。

有关详细信息，请参阅 Citrix PowerShell SDK。

删除无管理程序访问权限的计算机

删除 VM 或预配方案时，MCS 需要从 VM（有时也从基础磁盘）中删除标签，以便删除选项中包含的资源不再被 MCS 跟踪或识别。但是，其中一些资源只能通过管理程序访问。即使没有管理程序访问权限，也可以使用 `Remove-ProvVM` PowerShell 中的 `PurgeDBOnly` 选项从数据库中删除 VM 资源对象，例如 VM、基础磁盘、ACG 中的映像等。

此选项适用于：

- 所有受支持的管理程序
- 持久性和非持久性 VM

限制

不能同时使用 -PurgeDBOnly 和 -ForgetVM 命令。

使用 PurgeDBOnly 命令

运行 PowerShell 命令 `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM` 时，删除操作在以下情况下可能会失败：

- 主机连接处于维护模式
- 凭据无效
- 身份验证失败

- 未经授权的操作
- 管理程序无法访问

> **注意：**
>
> Remove-provVM -ForgetVM 仅针对持久性 VM。如果列表中的某个 VM 为非持久性，则操作将失败。

> 当操作因管理程序无法访问而失败时，将显示以下提示：

`Try to use -PurgeDBOnly option to clean DDC database.`.

使用 `Remove-ProvVM` PowerShell 命令中的 `-PurgeDBOnly` 选项从 MCS 数据库中删除 VM 引用。例如，

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -PurgeDBOnly
```

为映像添加描述

您可以添加有关计算机目录映像更新相关更改的信息性描述。使用此功能可在创建目录时或更新目录的现有主映像时添加描述。您还可以显示目录中每个主映像的信息。使用以下命令添加或查看映像描述：

- 要在使用主映像创建计算机目录时添加备注，请在 `NewProvScheme` 命令中使用 `MasterImageNote` 参数。例如：

  ```
  C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -HostingUnitName
  <name> -IdentityPoolName <name> -MasterImageVM

  XDHyp:\HostingUnits\<hosting unit name>\<vm name>.vm\Base.snapshot
  -MasterImageNote "Note"
  ```

- 要更新与计算机目录关联的主映像，请在 `Publish-ProvMasterVMImage` 命令中使用 `MasterImageNote` 参数。例如：

  ```
  C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name>
  -MasterImageVM XDHyp:\HostingUnits\<hosting unit name>\<vm
  name>.vm\base.snapshot -MasterImageNote "Note"
  ```

- 要显示每个映像的信息，请使用 Get-ProvSchemeMasterVMImageHistory 命令。例如：

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
MyScheme -Showall
```

要跟踪回滚进度，请在**计算机目录**中找到该目录，以查看内联进度条和分步进度图。

在某些情况下无法回滚，包括以下情况。（**回滚主映像**选项不可见）。

- 您没有回滚权限。
- 目录不是使用 MCS 创建的。
- 目录是使用操作系统磁盘映像创建的。
- 用于创建目录的快照已损坏。
- 用户对目录中计算机的更改不会持久保存。
- 目录中的计算机正在运行。

重置操作系统磁盘

使用 PowerShell 命令 `Reset-ProvVMDisk` 重置 MCS 创建的计算机目录中持久性 VM 的操作系统磁盘。目前，此功能适用于 AWS、Azure、XenServer、Google Cloud、SCVMM 和 VMware 虚拟化环境。

要成功运行 PowerShell 命令，请确保：

- 目标 VM 位于持久性 MCS 目录中。
- MCS 计算机目录运行正常。
- 这意味着预配方案和主机存在，并且预配方案具有正确的条目。
- 管理程序未处于维护模式。
- 目标 VM 已关机并处于维护模式。

执行以下步骤重置操作系统磁盘：

1. 打开 PowerShell 窗口。
2. 运行 **asnp citrix*** 以加载 Citrix 特定的 PowerShell 模块。
3. 通过以下任一方式运行 PowerShell 命令 `Reset-ProvVMDisk`：
    - 将 VM 列表指定为逗号分隔列表，并对每个 VM 执行重置：

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc","def")
-OS
```

- 将 VM 列表指定为 `Get-ProvVM` 命令的输出，并对每个 VM 执行重置：

```
(Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc"
-OS
```

- 按名称指定单个 VM：

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
```

- 为 `Get-ProvVM` 命令返回的每个 VM 创建单独的重置任务。这种方式效率较低，因为每个任务都会执行相同的冗余检查，例如虚拟机监控程序功能检查、每个 VM 的连接检查。

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
-ProvisioningSchemeName "xxx" -OS
```

4. 将出现一个确认提示，其中列出了要重置的 VM 以及一条警告消息，指出这是一个不可恢复的操作。如果您不提供答案并按 **Enter**，则不会执行任何进一步的操作。

> **注意：**
>
> 在重置过程完成之前，请勿将 VM 退出维护模式或将其开机。
>
> 您可以运行 PowerShell 命令 `-WhatIf` 来打印它将执行的操作，然后退出而不执行该操作。

您还可以使用以下方法之一绕过确认提示：

- 提供 `-Force` 参数：

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Force
```

- 提供 `-Confirm:$false` 参数：

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Confirm:$false
```

- 在运行 `Reset-ProvVMDisk` 之前，将 `$ConfirmPreference` 更改为 **None**：

```
PS C:\Windows\system32> $ConfirmPreference='None'

PS C:\Windows\system32> $ConfirmPreference

None

PS C:\Windows\system32> Reset-ProvVMDisk -ProvisioningSchemeName
"xxx" -VMName "abc" -OS
```

5. 运行 `Get-ProvTask` 以获取 `Reset-ProvVMDisk` 命令返回的任务状态。

更改现有预配方案的网络设置

您可以更改现有预配方案的网络设置，以便在新子网上创建新的 VM。在 `Set-ProvScheme` 命令中使用 `-NetworkMapping` 参数更改网络设置。

> **注意：**
>
> 此功能在 Citrix Virtual Apps and Desktops 2203 LTSR CU3 及更高版本中受支持。

要更改现有预配方案的网络设置，请执行以下操作：

1. 在 PowerShell 窗口中，运行命令 `asnp citrix*` 以加载 PowerShell 模块。
2. 运行 `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` 以获取要更改的网络路径。
3. 为新的网络设置分配一个变量。例如：

```
$NewNetworkMap = @{"0"= "XDHYP:\HostingUnits\MyNetworks\Network
0.network"}
```

4. 运行 `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap`。

5. 运行 `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` 以验证现有预配方案的新网络设置。

管理计算机目录的版本

当 MCS 计算机目录使用 `Set-ProvScheme` 命令更新时，当前配置将保存为一个版本。然后，您可以使用 PowerShell 命令管理计算机目录的各个版本。您可以：

- 查看计算机目录的版本列表
- 使用任何以前的版本更新计算机目录
- 如果某个版本未被该计算机目录的 VM 使用，则手动删除该版本
- 更改计算机目录保留的最大版本数（默认为 99）

一个版本包括计算机目录的以下信息：

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

运行以下命令（作为示例提供）以管理计算机目录的各个版本。

- 要查看计算机目录各个版本的配置详细信息：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- 要查看特定版本的计算机目录的配置详细信息：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version 2
```

- 要查看与计算机目录关联的版本总数：

```
(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count
```

- 要使用任何以前的版本更新计算机目录：

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- 如果某个版本未被该计算机目录的任何 VM 使用，则手动删除该版本：

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version
3
```

- 设置计算机目录保留的最大版本数（默认为 99）。此设置适用于所有目录。例如，在这种情况下，所有 MCS 预配的目录将最多保留 15 个版本。

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -Value
15
```

如果版本数达到最大版本数，并且计算机目录中的任何 VM 正在使用旧版本，则无法创建新版本。在这种情况下，请执行以下操作之一：

- 增加计算机目录要保留的最大版本数限制。
- 更新使用旧版本的一些 VM，以便这些旧版本不再被任何 VM 引用，并且可以删除。

将非计算机配置文件型计算机目录转换为计算机配置文件型计算机目录

您可以使用 VM、模板规范（对于 Azure）、启动模板（对于 AWS）或 VMware 模板（对于 VMware）作为计算机配置文件输入，将非计算机配置文件型计算机目录转换为计算机配置文件型计算机目录。添加到目录的新 VM 将从计算机配置文件中获取属性值，除非被显式自定义属性覆盖。

> **注意：**
>
> 现有的计算机配置文件型计算机目录无法更改为非计算机配置文件型计算机目录。

为此：

1. 创建包含 VM 且不带计算机配置文件的永久或非永久计算机目录。
2. 打开 **PowerShell** 窗口。
3. 运行 `Set-ProvScheme` 命令，将计算机配置文件中的属性值应用于添加到计算机目录的新 VM。例如：
   - 对于 Azure：

```
Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile XDHyp:
\HostingUnits\<HostingUnitName>\machineprofile.folder\<ResourceGroup
Name>\<TemplateSpecName>\<VersionName>
```

- 对于 AWS：

```
Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile "XDHyp:
\HostingUnits\<hosting-unit>\<launch-
template>.launchtemplate\<launch-template-
version>.launchtemplateversion"
```

- 对于 VMware：

```
Set-ProvScheme -ProvisioningSchemeName "my-prov-scheme"
-MachineProfile "XDHyp:\HostingUnits\my-hosting-unit\my-
template.template"
```

> **注意：**
>
> 将 `FolderID` 设置为自定义属性，以避免从 VMware 模板派生 `FolderID`。

修复活动计算机帐户的身份信息

您可以重置存在身份相关问题的活动计算机帐户的身份信息。您可以选择仅重置计算机密码和信任密钥，或重置身份磁盘的所有配置。此实现适用于持久和非持久 MCS 计算机目录。

> **注意：**
>
> 目前，此功能支持 AWS、GCP、Azure、SCVMM、XenServer 和 VMware 虚拟化环境。

条件

为成功重置身份磁盘，请确保以下事项：

- 关闭 VM 并将其设置为维护模式
- 不要在 PowerShell 命令中包含参数 -OS

重置身份磁盘

要重置身份磁盘：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 重置身份信息。

   - 要仅重置计算机密码和信任密钥，请运行以下命令：

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1
     -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
     -Target IdentityInfo
     ```

     命令中使用的参数说明如下：

     - IdentityAccountName：必须修复的身份帐户的名称。
     - PrivilegedUserName：对身份提供程序（AD 或 AzureAD）具有写入权限的用户帐户。
     - PrivilegedUserPassword：PrivilegedUserName 的密码。
     - Target：修复操作的目标。它可以是 IdentityInfo，用于修复帐户密码/信任密钥；也可以是 UserCertificate，用于修复 Microsoft Entra 混合加入计算机身份的用户证书属性。

   - 要重置身份磁盘的所有配置，请按以下顺序运行以下命令：

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1
     -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
     -Target IdentityInfo
     ```

     ```
     Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>  -
     Identity
     ```

   - 要完全重新创建身份磁盘：

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name>
     -Identity -Recreate
     ```

     注意：

> 如果计算机是使用 VDA 2511 或更高版本的 Windows 计算机，则无论 `-Recreate` 设置如何，它都将继续使用与以前相同的 `MachineGuid`。

4. 键入 **y** 以确认操作。您还可以使用 `-Force` 参数跳过确认提示。例如：

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name>
-Identity -Force
```

5. 运行 `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` 以检查更新的身份磁盘设置。身份磁盘的属性（例如，`IdentityDiskId`）必须已更新。`StorageId` 和 `IdentityDiskIndex` 不得更改。

更改现有计算机目录上的缓存配置

创建启用了 MCSIO 的非持久目录后，可以使用 Set-ProvScheme 命令修改以下参数：

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

此功能目前适用于：

- GCP 和 Microsoft Azure 环境，以及
- 启用了 MCSIO 的非持久性目录

要求

修改缓存配置的要求如下：

- 更新到最新版本的 VDA（2308 或更高版本）。
- 为现有计算机目录启用参数 `UseWriteBackCache`。使用 `New-ProvScheme` 创建一个启用了 `UseWriteBackCache` 的计算机目录。例如：

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -HostingUnitUid
$HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

-MasterImageVM $MasterImage `

-ServiceOffering $ServiceOffering `
```

```
-NetworkMap $NetworkMap `

-SecurityGroup $SecurityGroup `

-UseWriteBackCache -WriteBackCacheDiskSize 8
```

更改缓存配置

运行 Set-ProvScheme 命令。例如：

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
-WriteBackCacheDisk32 -WriteBackCacheMemorySize 128
```

注意：

- `WriteBackCacheDiskSize` 的值必须大于零，因为至少需要 1 GB 的缓存磁盘存储空间。
- `WriteBackCacheMemorySize` 的值必须小于计算机目录内存大小。
- 这些更改仅影响更改后添加到目录的新 VM。现有 VM 不受这些更改的影响。

通过本地文件共享访问支持 VDA 更新

通过 PowerShell cmdlet 指定 VDA 安装程序位置，这减少了您提供网络规则以允许每个 VDA 从 Citrix Managed Azure CDN 获取新 VDA 安装程序的工作量。

PowerShell cmdlet 命令

New-VusCatalogSchedule 和 **New-VusMachineUpgrade** cmdlet 中新增了两个可选参数，允许您使用本地文件共享中的安装程序

- **VdaWorkstationPackageUri** - 指定工作站操作系统 VDA 安装程序的 UNC 路径
- **VdaServerPackageUri** - 指定服务器操作系统 VDA 安装程序的 UNC 路径

先决条件

- 随 VDA 2311 提供的 VUS 代理安装程序
- VDA 升级代理到版本 7.40.0.35 或更高版本（使用 VDA 安装程序版本 2311 或更高版本）

- Virtual Apps and Desktops Remote PowerShell SDK 版本 7.40 或更高版本（于 Jan 10, 2024 或之后发布）

如何设置文件共享权限

包含 VDA 安装程序包的网络共享必须对作为本地系统 (NT AUTHORITY\SYSTEM 主体) 运行的 VDA 升级代理服务具有读取访问权限。

- **已加入域的文件共享权限**

  当 VDA 计算机已加入域时，**本地系统**帐户（VUA 以本地系统身份运行）在访问网络共享时使用计算机凭据。

  最小权限可以通过授予域计算机**读取**访问权限来设置。

  a. 选择您网络上要与之共享文件的人员。

  b. 单击**高级共享设置**并打开**文件和打印机共享**。

- **未加入域的文件共享权限**

  当 VDA 计算机未加入域时，则 **本地系统** 帐户（VUA 以本地系统身份运行）在访问网络共享时使用 **匿名登录**。

  a. 选择一个共享文件夹。

  b. 禁用密码保护。

     a. 转到文件夹**属性**。

     b. 选择**网络和共享中心**。

     c. 关闭**密码保护共享**。

  c. 单击**高级共享**以授予共享权限。

     a. 选择**权限**。

     b. 授予 **匿名登录** **读取** 共享权限。

  d. 选择**安全选项卡**以授予文件夹权限

     a. 单击**编辑**以向共享文件夹添加权限

     b. 选择共享文件夹，授予文件夹权限给 **ANONYMOUS LOGON**。

  e. 单击 **高级** 以启用 **文件和打印机共享**。

  f. 将共享文件夹名称添加到 **网络访问安全策略**。

> **注意：**
>
> 重新启动计算机以使更改立即生效。

从本地文件共享更新 VDA

1. 下载 VDA 安装程序并将其放置在共享文件中。

   > **注意：**
   >
   > 借助 Virtual Upgrade Service，您可以选择当前版本轨道或 LTSR 轨道。
   >
   > **例如：** 如果计算机目录设置为当前版本 2311，并且 VDA 版本为 2305，则必须将 VDA 升级到版本 2311。

   a. 导航到我们的网站上的 **下载** 页面。
   b. 选择 **Citrix Virtual Apps and Desktops** 作为产品。
   c. 选择 **Citrix Virtual Apps and Desktops 7 2311, 所有版本**。
   d. 从可展开的 **产品 ISO 中包含但单独打包的组件** 中选择 VDA 安装程序。

2. 根据目录类型选择相关的 VDA 安装程序。

   - 如果目录类型为 **多会话**，请下载 **多会话操作系统 VDA 安装程序**
   - 如果目录类型为 **单会话**，请下载 **单会话操作系统 VDA 安装程序**
   - 如果目录类型为**远程电脑访问**，请下载**单会话操作系统核心服务 VDA 安装程序**

> **注意：**
>
> 文件共享安装程序的版本必须**完全**匹配 VUS 发布到云端的最新安装程序版本。

虚拟机的存储迁移

您可以在 VMware 和 XenServer 环境中将现有虚拟机的磁盘存储从旧存储移动到新存储。在迁移过程中，MCS 会保留虚拟机功能，例如电源管理、重置操作系统磁盘等。您还可以使用新的磁盘存储将新虚拟机添加到计算机目录。为此，请使用 PowerShell 命令 `Move-ProvVMDisk`。

您可以迁移完整克隆的持久性虚拟机和非持久性虚拟机。

- 对于持久性完整克隆虚拟机：操作系统磁盘、身份磁盘和非 MCS 预配磁盘。
- 对于非持久性虚拟机：操作系统磁盘、身份磁盘和回写缓存 (WBC) 磁盘。

新存储必须满足以下条件：

- 它必须与旧存储位于同一群集中。
- 运行 VM 的主机必须能够访问旧数据存储和新数据存储。

迁移磁盘存储

要迁移磁盘存储，请执行以下操作：

1. 将目标存储添加到现有托管单元。您可以运行 PowerShell 命令 `Add-Hyphostingunitstorage` 来添加目标存储：

   如果您不想将新 VM 添加到旧存储，请将旧存储更改为**已取代**。您可以使用 Studio 或 PowerShell 命令执行此操作。对于 Studio，请参阅编辑存储。或者，运行 `Set-Hyphostingunitstorage` 并将 `Superseded` 设置为 `true` 以禁用在旧存储中创建新 VM。

   > **注意：**
   >
   > 对于非持久性 VM：
   >
   > - 如果使用 WBC，请在托管单元中配置 WBC 目标存储。
   > - 如果配置了操作系统目标存储，则 WBC（如果使用）必须与操作系统目标存储兼容。
   > - 如果未配置操作系统目标存储，则 WBC（如果使用）必须与当前操作系统存储兼容。

2. 关闭 VM 并打开**维护模式**。
3. 获取有关预配方案、托管单元、操作系统磁盘存储和 WBC 磁盘存储的信息。

   - 运行 `ProvResourceInStorage` 以获取操作系统存储信息。例如：

     ```
     $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
     xxxxx

     $result
     ```

```
$result.ProvResourceInStorage | Format-List -Property *
```

- 运行 `TemporaryStorageInfo` 以获取 WBC 存储信息。例如：

```
$result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
xxxxx

$result

$result.TemporaryStorageInfo | Format-List -Property *
```

4. 使用 `Move-ProvVMDisk` PowerShell 命令将操作系统磁盘、身份磁盘和 WBC 磁盘（适用于非持久性 VM）迁移到目标存储。

注意：

- 始终在 DiskType 和 `DestinationStorageId` 参数中提供操作系统磁盘和身份磁盘。
- 操作系统磁盘和身份磁盘的 `DestinationStorageId` 必须相同。

示例：

持久性 VM：

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myFullCloneProvScheme" -VMName "machine01"
-DiskType OS,Identity -DestinationStorageId datastore1,datastore1
```

重要提示：

对于持久性 VM，所有磁盘都将移动。您无法选择要移动哪些磁盘。

非持久性 VM：

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myCleanOnBootProvScheme" -VMName "machine01"
-DiskType OS,Identity,WBC -DestinationStorageId None,None,datastore1
```

重要提示：

- 如果您不想迁移特定磁盘，请将 `DestinationStorageId` 参数的值设置为 `None`。
- 如果 VM 具有 WBC 磁盘，请在 `DiskType` 参数中添加 WBC 磁盘，并在 `DestinationStorageId` 参数中添加所需信息。

将现有 MCS 预配的目录迁移到准备好的映像计算机目录

您可以使用 PowerShell 命令 `Set-ProvSchemeImage` 将现有 MCS 预配的计算机目录转换为准备好的映像计算机目录。但是，迁移后无法恢复到旧版目录。目前，此功能适用于 Azure 和 VMware 虚拟化环境。

限制

请考虑以下限制：

- 如果 MCS 目录使用持久数据磁盘，则无法将该目录迁移以使用准备好的映像。
- 如果 MCS 目录使用非托管磁盘，则无法将该目录迁移以使用准备好的映像。

迁移到准备好的映像计算机目录

要迁移，请执行以下操作：

1. 使用 Studio 或 PowerShell 命令创建映像定义和映像版本。请参阅以下内容中创建映像定义和映像版本的步骤：
   - 阿祖尔：
     - Web 工作室
     - PowerShell
   - 威睿：
     - Web 工作室
     - PowerShell

2. 运行 `Get-ProvScheme` 命令以获取预配方案 UID。例如：

```
Get-ProvScheme -ProvisioningSchemeName <name> | select
ProvisioningSchemeName, ProvisioningSchemeUid
```

3. 运行 `Get-ProvImageVersionSpec` 命令以获取映像定义名称、映像版本规范 UID。例如：

```
Get-ProvImageVersionSpec -ImageDifinitionName <name> -Filter
{IsPrepared -eq $true} | select ImageDefinitionName ImageVersionSpecUId
```

4. 运行 `Set-ProvSchemeImage` 命令以将现有 MCS 预配的计算机目录迁移到准备好的映像计算机目录中。例如：

```
Set-ProvSchemeImage -ProvisioningSchemeName [ProvisioningSchemeName]
-ImageVersionSpecUid [ImageVersionSpecUid]
```

5. 运行 `Get-ProvScheme` 命令以检查目录是否已迁移。例如：

```
Get-ProvScheme -ProvisioningSchemeName <name> | select
ProvisioningSchemeName, ProvisioningSchemeUid, ImageVersionSpecUid
```

故障排除

- 对于状态为“电源状态未知”的计算机，请参阅 CTX131267 获取指导。
- 要修复持续显示未知电源状态的 VM，请参阅 如何修复持续显示未知电源状态的 VM。

下一步

有关管理特定云服务目录的信息，请参阅：

- 管理 AWS 目录
- 管理 XenServer 目录
- 管理 Google Cloud Platform 目录
- 管理 Microsoft Azure 目录
- 管理 Microsoft System Center 虚拟机管理器目录
- 管理 VMware 目录

管理 AWS EC2 目录

管理计算机目录 介绍了用于管理计算机目录的向导。以下信息涵盖了 AWS EC2 云环境特有的详细信息。

> **注意：**
>
> 在管理 AWS 目录之前，您需要完成 AWS 目录的创建。请参阅 创建 AWS EC2 目录。

删除标签

创建目录或 VM 时，MCS 创建的标签会在以下资源上创建：

- 虚拟机
- 根磁盘卷
- 身份磁盘卷
- NIC
- 根磁盘映像 (AMI)
- 启动模板
- AMI 或根磁盘的快照

您可以从 Citrix® 数据库中删除 VM 和计算机目录，并删除 MCS 创建的标签。您可以使用：

- 使用 `Remove-ProvVM` 和 `ForgetVM` 参数从单个 VM 或计算机目录中的 VM 列表中删除 VM 和 MCS 创建的标签。
- 使用 `ForgetVM` 参数 `Remove-ProvScheme` 从 Citrix 数据库中移除计算机目录，并从计算机目录中移除资源。

此功能仅适用于持久性 VM。

为此：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 在移除 VM 之前解锁 VM。例如：

```
Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
```

4. 运行以下命令之一，从资源中删除 VM、计算机目录和 MCS 创建的标签。

   - 运行 `Remove-ProvVM` 和 `ForgetVM` 以从 Citrix 数据库中删除 VM 并从 VM 中删除标签。例如：

     ```
     Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
     -ForgetVM
     ```

   - 运行 `Remove-ProvScheme` 以从 Citrix 数据库中移除计算机目录，并从计算机目录中移除资源。例如：

     ```
     Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
     ```

5. 验证 VM 是否已从 Delivery Controller™ 中删除，但未从虚拟机管理程序中删除。

   a. 运行 `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`。此操作不应返回任何内容。

   b. 转到 AWS EC2 控制台。您应该会看到 VM，但标签现已删除。以下资源的标签已删除：

      - 虚拟机
      - 根磁盘卷
      - 身份磁盘卷
      - NIC

6. 如果删除计算机目录，请验证该目录是否已从 Delivery Controller 中删除。

   a. 运行 `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`。这必须返回一个错误。

   b. 在 AWS EC2 控制台中验证是否已删除以下资源。

      - 根磁盘映像 (AMI)
      - 启动模板
      - AMI 或根磁盘的快照

识别 MCS 创建的资源

以下是 MCS 添加到资源的标签。表中的标签表示为“key”:“value”。

资源名称	标签
ID 磁盘	"名称": "VMName_IdentityDisk"
	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
映像	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
NIC	“描述”: “XD NIC”
	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
操作系统磁盘	"名称": "VMName_rootDisk"
	"Xd配置": "XdProvisioned=True"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] “Citrix 资源”: “ ”
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
准备虚拟机	"Name": "准备 - 目录名称 - xxxxxxxxxx"
	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] “Citrix 资源”: “ ”

资源名称	标签
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
已发布的快照	"Xd配置": "Xd已预配=true"
	如果不是 Volume Worker AMI 的快照，则为 "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
模板	[when AwsCaptureInstanceProperties = true] "Xd配置": "XdProvisioned=true"
	[when AwsCaptureInstanceProperties = true] "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
目录中的 VM	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:id":"lt-xxxx"
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:version": "n"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""

资源名称	标签
卷工作器 AMI	"Xd配置": "Xd已预配=true"
卷工作器引导程序	"名称": "XenDesktop® 临时"
	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixVolumeWorkerBootstrapper": ""
卷工作器实例	“名称”: “Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx”
	"Xd配置": "Xd已预配=true"

更多信息

- 创建和管理连接与资源
- 连接到 AWS EC2
- 创建计算机目录
- 创建 AWS EC2 目录
- 管理计算机目录

管理 Amazon WorkSpaces Core 托管实例目录

管理计算机目录 介绍了用于管理计算机目录的向导。以下信息涵盖了 Amazon WorkSpaces Core 托管实例的特定详细信息。

> **注意：**
>
> 在管理 Amazon WorkSpaces Core 托管实例目录之前，您需要完成 Amazon WorkSpaces Core 托管实例目录的创建。请参阅 创建 Amazon WorkSpaces Core 托管实例目录。

删除标签

当您创建目录或虚拟机时，会在以下资源上创建标签：

- 虚拟机
- 根磁盘卷
- 身份磁盘卷
- 弹性网络接口 (ENI)
- 根磁盘映像 (AMI)
- 启动模板
- AMI 或根磁盘的快照

您可以从 Citrix® 数据库中删除虚拟机和计算机目录，并删除 Citrix 创建的标签。您可以使用：

- `Remove-ProvVM` 带有 `ForgetVM` 参数，以从单个虚拟机或计算机目录中的虚拟机列表中删除虚拟机和 Citrix 创建的标签。

  > **注意：**
  >
  > 使用 `ForgetVM` 参数，VM 将从 Citrix 的预配方案数据库中移除，但 VM 仍保留在虚拟机管理程序中。

- 使用 `ForgetVM` 参数 `Remove-ProvScheme` 从 Citrix 数据库中移除计算机目录，并从计算机目录中移除资源。

为此，请执行以下操作：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 在移除 VM 之前解锁 VM。例如：

   ```
   Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   ```

4. 运行以下命令之一，从资源中移除 VM、计算机目录和 Citrix 创建的标签。

   - 运行 `Remove-ProvVM` 并使用 `ForgetVM` 从 Citrix 数据库中移除 VM，并从 VM 中移除 Citrix 创建的标签。例如：

     ```
     Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
     -ForgetVM
     ```

- 运行 `Remove-ProvScheme` 以从 Citrix 数据库中移除计算机目录，并从计算机目录中移除资源。例如：

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
```

5. 验证 VM 是否已从 Delivery Controller™ 中移除，但未从虚拟机管理程序中移除。

   a. 运行 `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`。此操作不应返回任何内容。

   b. 转到 AWS EC2 控制台。您应该会看到 VM，但 Citrix 创建的标签现已移除。以下资源中的 Citrix 创建的标签已移除：

      - 虚拟机
      - 根磁盘卷
      - 身份磁盘卷
      - ENI

6. 如果删除计算机目录，请验证该目录是否已从 Delivery Controller 中删除。

   a. 运行 `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`。这必须返回一个错误。

   b. 在 AWS EC2 控制台中验证是否已删除以下资源。

      - 根磁盘映像 (AMI)
      - 启动模板
      - AMI 或根磁盘的快照

识别 MCS 创建的资源

以下是 MCS 添加到 AWS 平台资源的标签。表中的标签表示为“key”:“value”。

资源名称	标签
ID 磁盘	"名称": "VMName_IdentityDisk"
	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

资源名称	标签
映像	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ENI	"描述": "XD 网卡"
	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
操作系统磁盘	"名称": "VMName_rootDisk"
	"Xd配置": "XdProvisioned=True"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
准备虚拟机	"Name": "准备 - 目录名称 - xxxxxxxxxx"
	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
已发布的快照	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
模板	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
目录中的 VM	"Xd配置": "Xd已预配=true"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

更多信息

- AWS 虚拟化环境
- 连接到 Amazon WorkSpaces Core 托管实例
- 映像管理
- 为 Amazon WorkSpaces Core 托管实例创建准备好的映像
- 创建 Amazon WorkSpaces Core 托管实例目录
- 管理准备好的映像计算机目录

管理 XenServer® 目录

管理计算机目录 介绍了用于管理计算机目录的向导。以下信息涵盖了 XenServer 虚拟化环境特有的详细信息。

> **注意：**
>
> 在管理 XenServer 目录之前，您需要完成 XenServer 目录的创建。请参阅创建 XenServer 目录。

识别 MCS 创建的资源

以下是 MCS 添加到资源的标签。表中的标签表示为“key”:“value”。

资源名称	标签
发布的基盘及其在每个网络或本地存储上的副本	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ID 磁盘	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
操作系统磁盘	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
准备虚拟机	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
目录中的 VM	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

资源名称	标签
WBC 磁盘	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

更多信息

- 创建和管理连接与资源
- 连接到 XenServer
- 创建计算机目录
- 创建 XenServer 目录
- 管理计算机目录

管理 Google Cloud Platform 目录

管理计算机目录 介绍了用于管理计算机目录的向导。以下信息涵盖了 Google 云环境特有的详细信息。

> **注意：**
>
> 在管理 Google Cloud Platform 目录之前，您需要完成 Google Cloud Platform 目录的创建。请参阅创建 Google Cloud Platform 目录。

管理计算机目录

要将计算机添加到目录、更新计算机以及回滚更新，请参阅 Manage machine catalogs。

电源管理

Citrix DaaS™ 允许您对 Google Cloud 计算机进行电源管理。使用左窗格中的**搜索**节点查找要进行电源管理的计算机。以下电源操作可用：

- 删除
- 启动
- 重新启动
- 强制重新启动
- 关机
- 强制关机

- 添加到交付组
- 管理标签
- 启用维护模式

您还可以使用 Autoscale 对 Google Cloud 计算机进行电源管理。为此，请将 Google Cloud 计算机添加到交付组，然后为该交付组启用 Autoscale。有关 Autoscale 的详细信息，请参阅 Autoscale。

使用 POWERSHELL 更新预配的计算机

`Set-ProvScheme` 命令会更改预配方案。但是，它不影响现有计算机。使用 PowerShell 命令 `Set-ProvVMUpdateTimeWindow`，您现在可以将当前预配方案应用于现有持久或非持久计算机或计算机集。目前，在 GCP 中，此功能支持的属性更新是计算机配置文件。

您可以更新：

- 单个 VM
- 特定 VM 列表或与预配方案 ID 关联的所有现有 VM
- 与预配方案名称关联的特定 VM 列表或所有现有 VM

要更新现有 VM：

1. 检查现有计算机的配置。例如，

   ```
   Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
   ```

2. 更新预配方案。例如，

   ```
   `Set-ProvScheme –ProvisioningSchemeName "my-catalog" –MachineProfile
   "XDHyp:\HostingUnits\<hosting-unit>\machineprofileinstance.vm"
   ```

3. 检查 VM 的当前属性是否与当前预配方案匹配，以及 VM 上是否有任何待处理的更新操作。例如，

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
   ```

   您还可以查找具有特定版本的计算机。例如，

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

4. 更新现有计算机。

   - 要更新所有现有计算机：

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - 要更新特定计算机列表：

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
     ```

   - 要根据 `Get-ProvVM` 的输出更新计算机：

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
     ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
     -DurationInMinutes -1
     ```

5. 查找已计划更新的计算机。例如，

   ```
   Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
   ProvisioningSchemeUpdateAfter
   ```

6. 重新启动计算机。下次开机时，属性更改将应用于现有计算机。您可以使用以下命令检查更新状态：

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
   ```

更改现有目录的磁盘相关自定义属性

您可以更改现有目录和目录中现有 VM 的以下磁盘相关自定义属性：

- `PersistOSDisk`
- `PersistWBC`

- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

> **注意：**
>
> - `StorageType` 属性用于操作系统磁盘
> - `PersistOsDisk` 属性只能为启用了回写缓存的非持久性目录设置

> 此实现可帮助您在创建目录后为不同的磁盘选择不同的存储类型，从而平衡与不同存储类型相关的定价。

为此，请使用 PowerShell 命令 `Set-ProvScheme` 和 `Set-ProvVMUpdateTimeWindow`：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix®*`。
3. 运行 `Get-ProvVM -VMName <VM name>` 以获取自定义属性。
4. 更改自定义属性字符串：
   a. 将自定义属性复制到记事本并更改自定义属性。
   b. 在 **PowerShell** 窗口中，从记事本粘贴修改后的自定义属性，并将变量分配给修改后的自定义属性。例如：

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com/2014/xd/
machinecreation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CatalogZones" Value="" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" /
>

<Property xsi:type="StringProperty" Name="PersistOSDisk"
Value="true" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="pd-standard" />
```

```
<Property xsi:type="StringProperty" Name="StorageType" Value="pd-
standard" />

</CustomProperties>'
```

5. 更新现有目录。例如：

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName>
-CustomProperties $cp
```

6. 更新现有 VM。例如：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. 重新启动 VM。下次开机时，自定义属性更改将应用于现有 VM。

防止意外删除计算机

Citrix DaaS 允许您保护 Google Cloud 上的 MCS 资源，以防止意外删除。通过将 `deletionProtection` 标志设置为 TRUE 来配置预配的 VM。

默认情况下，通过 MCS 或 Google Cloud 插件预配的 VM 会在启用 InstanceProtection 的情况下创建。此实现适用于持久和非持久目录。当实例从模板重新创建时，非持久目录会更新。对于现有持久计算机，您可以在 Google Cloud 控制台中设置该标志。有关设置标志的详细信息，请参阅 Google 文档站点。添加到持久目录的新计算机是在启用 `deletionProtection` 的情况下创建的。

如果您尝试删除已设置 `deletionProtection` 标志的 VM 实例，则请求将失败。但是，如果您被授予权限 `compute.instances.setDeletionProtection` 或分配了 IAM **Compute Admin** 角色，则可以重置该标志以允许删除资源。

识别 MCS 创建的资源

以下是 MCS 添加到资源的标签。表中的标签表示为“key”:“value”。

资源名称	标签
ID 磁盘	"CitrixResource": "内部"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

资源名称	标签
映像	"CitrixResource": "内部"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
操作系统磁盘	"CitrixResource": "内部"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
准备虚拟机	"CitrixResource": "内部"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
已发布的快照	"CitrixResource": "内部"
存储桶	"Citrix 资源": "内部"
模板	"CitrixResource": "内部"
	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
目录中的 VM	"CitrixResource": "内部"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx". 该插件还会为 MCS 预配的 VM 添加此标签："citrix-provisioning-scheme-id": "provSchemeId"。您可以使用此标签在 GCP 控制台中按目录进行筛选。
WBC 磁盘	"CitrixResource": "内部"
	CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

注意：

> 如果添加了 **CitrixResource** 标签以将其标识为由 MCS 创建的资源，则 VM 在 Citrix 清单中不可见。您可以删除或重命名该标签以使其可见。

更多信息

- 创建和管理连接与资源
- 连接到 Google Cloud 环境
- 创建计算机目录
- 创建 Google Cloud Platform 目录
- 管理计算机目录

管理 HPE Moonshot 目录

(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-manage.html) 介绍了管理计算机目录的向导。以下信息涵盖了 HPE Moonshot 目录的特定详细信息。

> **注意：**

> 在管理 HPE Moonshot 目录之前，您需要完成 HPE Moonshot 目录的创建。

电源管理

Citrix Virtual Apps and Desktops™ 允许您对 HPE Moonshot 计算机进行电源管理。使用导航窗格中的**搜索**节点找到要进行电源管理的计算机。以下电源操作可用：

- 启动
- 关机
- 强制关机
- 重新启动
- 重置

> **注意：**

> 不支持**挂起**和**恢复**电源操作。

更多信息

- 创建和管理连接和资源 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/connections.html)
- 连接到 HPE Moonshot
- 创建计算机目录
- 创建 HPE Moonshot 计算机目录
- 管理计算机目录

管理 Microsoft Azure 目录

管理计算机目录 介绍了用于管理计算机目录的向导。以下信息涵盖了 Microsoft Azure Resource Manager 云环境特有的详细信息。

> **注意：**
>
> 在管理 Microsoft Azure 目录之前，您需要完成创建 Microsoft Azure 目录。请参阅创建 Microsoft Azure 目录。

VM 关闭时将存储类型更改为较低层

通过在关闭 VM 时将托管磁盘的存储类型切换到较低层，可以节省存储成本。为此，请使用 `StorageTypeAtShutdown` 自定义属性。

关闭 VM 时，磁盘的存储类型会更改为较低层（如 `StorageTypeAtShutdown` 自定义属性中指定）。启动 VM 后，存储类型会恢复为原始类型（如 `StorageType` 自定义属性或 `WBCDiskStorageType` 自定义属性中指定）。

> **重要提示：**
>
> 磁盘在 VM 至少启动一次后才存在。因此，首次启动 VM 时无法更改存储类型。

要求

- 适用于托管磁盘。这意味着您将自定义属性 `UseManagedDisks` 设置为 true。
- 适用于具有持久性 OS 磁盘的持久性和非持久性目录。这意味着您将自定义属性 `persistOsDisk` 设置为 true。

- 适用于具有持久性 WBC 磁盘的非持久性目录。这意味着您将自定义属性 `persistWBC` 设置为 true。

限制

- 根据 Microsoft 的规定，您每天只能更改磁盘类型两次。请参阅 Microsoft 文档。根据 Citrix 的规定，只要对 VM 执行启动或解除分配操作，就会发生 `StorageType` 更新。因此，将每台 VM 的电源操作次数限制为每天两次。例如，早上执行一次电源操作以启动 VM，晚上执行一次电源操作以解除分配 VM。

将存储类型更改为较低层

在继续这些步骤之前，请参阅要求和限制。

1. 添加自定义属性 `StorageTypeAtShutdown`，将值设置为 Standard_LRS (HDD)，并使用 `New-ProvScheme` 创建目录。有关使用 PowerShell 创建目录的信息，请参阅 `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`。

   > **注意：**
   >
   > 如果 `StorageTypeAtShutdown` 的值不是空值或 Standard_LRS (HDD)，则操作失败。
   >
   > 创建持久目录时设置自定义属性的示例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
```

```
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

创建非持久目录时设置自定义属性的示例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

> **注意：**
>
> 当您使用计算机配置文件时，自定义属性优先于 `MachineProfile` 中定义的属性。

2. 关闭 VM 并在 Azure 门户中检查 VM 的存储类型。磁盘的存储类型将更改为较低层级，如 `StorageTypeAtShutdown` 自定义属性中指定。
3. 开启 VM。磁盘的存储类型将切换回以下位置提及的存储类型：
   - 操作系统磁盘的 `StorageType` 自定义属性
   - 仅当您在 `CustomProperties` 中指定时，WBC 磁盘的 `WBCDiskStorageType` 自定义属性。否则，它将切换回 `StorageType` 中提及的存储类型。

将 `STORAGETYPEATSHUTDOWN` 应用于现有目录

在继续这些步骤之前，请参阅要求和限制。

使用 `Set-ProvScheme` 将 VM 添加到现有目录。此功能适用于运行 `Set-ProvScheme` 后添加的新 VM。现有计算机不受影响。

将VM添加到现有目录时设置自定义属性的示例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
```

```
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'



$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName



Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName
-CustomProperties $customProperties
```

在关机时将现有VM的存储类型更改为较低层

在继续这些步骤之前，请参阅要求和限制。

您可以通过在 VM 关闭时将现有 VM 的存储类型更改为较低层级来节省存储成本。为此，请使用 `StorageTypeAtShutdown` 自定义属性。

要在VM关机时将目录中现有计算机的存储类型更改为较低层，请执行以下操作：

1. 打开PowerShell窗口。
2. 运行 `asnp citrix®*` 以加载Citrix特定的PowerShell模块。
3. 运行 `Get-Provscheme -ProvisioningSchemeName $CatalogName`。
4. 更改自定义属性字符串。

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

5. 更新现有目录的预配方案。此更新适用于运行`Set-ProvScheme`后添加的新VM。

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -CustomProperties
$customProperties
```

6. 更新现有VM以启用`StorageTypeAtShutdown`。

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName
-StartsNow -DurationInMinutes -1
```

7. 下次启动计算机时，计算机的`StorageTypeAtShutdown`属性将更新。存储类型将在下次关机时更改。
8. 运行以下命令以查看目录中每个 VM 的`StorageTypeAtShutdown`值：

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach { $vmName =
$_.VMName; $storageTypeAtShutdown = ($_.CustomVmData | ConvertFrom-
Json).StorageTypeAtShutdown.DiskStorageAccountType; return New-Object
psobject -Property @{ "VMName" = $vmName; "StorageTypeAtShutdown" =
$storageTypeAtShutdown } }
```

将预配的计算机更新到当前预配方案状态

`Set-ProvScheme`命令会更改预配方案。但是，它不影响现有计算机。使用 PowerShell 命令`Set-ProvVMUpdateTimeWindow`，您可以将当前预配方案应用于现有持久或非持久计算机或一组计算机。您还可以为现有 MCS 预配计算机的配置更新安排时间段。在计划的时间段内进行的任何开机或重新启动都会将计划的预配方案更新应用于计算机。目前，在 Azure 中，您可以更新`ServiceOffering`、`MachineProfile`以及以下自定义属性：

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

- `Zones`

> **注意：**
>
> - 您只能更新 `StorageType`、`WBCDiskStorageType` 和 `IdentityDiskStorageType` 自定义属性，用于 Azure 环境中使用托管磁盘的目录。
> - 如果您运行 `Set-ProvVMUpdateTimeWindow` 两次，则最新命令生效。
> - 如果使用 `Set-ProvVMUpdateTimeWindow` 更新了 VM，并且 Zones 自定义属性提供的当前可用区列表已更改为不包含 VM 当前正在使用的区域，则 VM 的持久性磁盘将被复制到新区域，并删除原始磁盘。例如，在区域 3 中预配的 VM，如果 Zones 自定义属性设置为“1,2”并进行更新，则会将 VM 及其磁盘移动到区域 1 或区域 2，具体取决于这两个区域中哪个区域的计算机较少，以便在区域 1 和区域 2 之间平衡计算机。
> - 如果区域自定义属性被完全清除（设置为空值），则会移除 VM 的区域亲和性，从而允许 Azure 根据容量将 VM 放置在任何可用性区域中。在这种情况下，VM 的持久磁盘将保留在其原始区域中，并且不会移动。

> 您可以更新：

- 单个 VM
- 特定 VM 列表或与预配方案 ID 关联的所有现有 VM
- 特定 VM 列表或与预配方案名称（计算机目录名称）关联的所有现有 VM

对预配方案进行以下更改后，Azure 中持久性目录的 VM 实例将重新创建：

- 更改 `MachineProfile`
- 删除 `LicenseType`
- 删除 `DedicatedHostGroupId`

> **注意：**
>
> 现有计算机的操作系统磁盘及其所有数据保持不变，并且新的 VM 将附加到该磁盘。

> 更新现有 VM 之前：

1. 检查现有计算机的配置。例如，

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. 更新预配方案。例如，

   - 以 VM 作为计算机配置文件输入：

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -MachineProfile
     "XDHyp:\HostingUnits\<hosting-unit>\machineprofile.folder\<resource-
     group>.resourcegroup\<virtual-machine>.vm"
     ```

   - 以模板规范作为计算机配置文件输入：

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog"

     -MachineProfile "XDHyp:\HostingUnits\<hosting-
     unit>\machineprofile.folder\<resource-
     group>.resourcegroup\<template-spec>.templatespec\<template-spec-
     version>.templatespecversion"

     -ServiceOffering "XDHyp:\HostingUnits\<hosting-
     unit>\serviceoffering.folder\<service-offering>.serviceoffering"
     ```

   - 仅使用服务产品：

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
     "XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
     offering>.serviceoffering"
     ```

3. 检查 VM 的当前属性是否与当前预配方案匹配，以及 VM 上是否有任何待处理的更新操作。例如，

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
   ```

   您还可以查找具有特定版本的计算机。例如，

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

要请求现有计算机的更新并在下次重新启动时应用：

1. 运行以下命令以更新现有计算机，并在下次重新启动时应用更新。

   - 要更新所有现有计算机。例如，

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - 要更新特定计算机列表。例如，

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
     ```

   - 要根据 Get-ProvVM 的输出更新计算机。例如，

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
     ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
     -DurationInMinutes -1
     ```

   注意：

   - `StartsNow` 表示计划的开始时间是当前时间。
   - 带有负数（例如，–1）的 `DurationInMinutes` 表示计划时间窗口没有上限。

2. 查找已计划更新的计算机。例如，

   ```
   Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
   ProvisioningSchemeUpdateAfter
   ```

3. 重新启动计算机。下次开机时，属性更改将应用于现有计算机。您可以使用以下命令检查更新状态。例如，

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

要将 VM 计划为在下次在计划的时间窗口内启动时更新到最新的预配设置：

1. 运行以下命令：
   - 将开始时间设置为当前时间以安排更新

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -VMName vm1 -StartsNow -DurationInMinutes 120
     ```

   - 在周末安排更新

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
     -VMName “vm1” -StartTimeInUTC “10/15/2022 9:00am” -DurationInMinutes
     (New –TimeSpan –Days 2).TotalMinutes
     ```

   注意：

   - `VMName` 是可选的。如果未指定，则为整个目录计划更新。
   - 使用 `StartsNow` 而不是 `StartTimeInUTC` 来指示计划开始时间是当前时间。
   - `DurationInMinutes` 是可选的。默认值为 120 分钟。负数（例如 –1）表示计划时间窗口没有上限。

2. 检查更新状态。

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
   ```

3. 启动虚拟机。如果您在计划的时间段之后启动计算机，则不会应用配置更新。如果您在计划的时间段内启动计算机，
   - 如果计算机已关机，并且
     - 如果您未开机，则不应用配置更新

    - 如果您开机，则应用配置更新
- 如果计算机已开机，并且
    - 如果您不重新启动计算机，则不会应用配置更新。
    - 如果您重新启动计算机，则会应用配置更新。

要取消配置更新：

您还可以取消单个虚拟机、多个虚拟机或整个目录的配置更新。要取消配置更新：

1. 运行 `Clear-ProvVMUpdateTimeWindow`。例如：
    - 要取消为单个虚拟机计划的配置更新：

      ```
      Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
      -VMName “vm1”
      ```

    - 要取消为多个虚拟机计划的配置更新：

      ```
      Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
      -VMName "vm1","vm2"
      ```

      注意：

      虚拟机必须来自同一目录。

更新单个 VM 的属性

您可以使用 PowerShell 命令 `Set-ProvVM` 更新持久性 MCS 计算机目录中单个 VM 的属性。但是，更新不会立即应用。您必须使用 PowerShell 命令 `Set-ProvVMUpdateTimeWindow` 设置时间窗口才能应用更新。

此实现有助于您高效地管理单个 VM，而无需更新整个计算机目录。目前，此功能仅适用于 Azure 环境。

目前，您可以更新的属性包括：

- `CustomProperties`
- `ServiceOffering`

- `MachineProfile`

使用此功能，您可以：

- 更新 VM 的属性
- 在更新计算机目录后保留在 VM 上更新的属性
- 还原应用于 VM 的配置更新

更新 VM 属性之前：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 检查现有计算机目录的配置。例如：

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

4. 检查要应用更新的 VM 的配置。例如：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

更新 VM 的属性

执行以下操作以更新 VM 上的属性：

1. 关闭要应用更新的 VM。
2. 更新 VM 的属性。例如，如果要更新 VM 的存储类型 (`StorageType`) 自定义属性，请运行以下命令：

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

您可以同时更新计算机目录中两个 VM 的属性。例如：

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2
-CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

注意：

更新不会立即应用。

3. 获取指定要更新的属性列表和配置版本。例如：

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -VMName
machine1
```

检查 `Version` 的属性值以及要更新的属性（在本例中为 `StorageType`）。

4. 检查配置版本。例如：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

检查 `ProvVMConfigurationVersion` 的属性值。更新尚未应用。VM 仍处于旧配置中。

5. 请求计划更新。例如：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog
-StartsNow -DurationInMinutes -1
```

有关计划更新的详细信息，请参阅 将预配的计算机更新到当前预配方案状态。

注意：

任何待处理的预配方案更新也将应用。

6. 重新启动 VM。例如：

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. 检查配置版本。例如：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

检查 `ProvVMConfigurationVersion` 的属性值。更新现已应用。VM 现在具有新配置。

8. 要对 VM 应用进一步的配置更新，请关闭 VM，然后重复这些步骤。

在更新计算机目录后保留在 VM 上更新的属性

执行以下操作以保留在 VM 上更新的属性：

1. 关闭要应用更新的 VM。
2. 更新计算机目录。例如，如果要更改 VM 大小 (`ServiceOffering`) 和存储类型 (`StorageType`)，请运行以下命令：

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -ServiceOffering
Standard_E4_v3 -CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

3. 获取计算机目录的配置详细信息。例如：

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

`ProvisioningSchemeVersion` 现在增加了一。VM 大小和存储类型也已更新。

4. 更新 VM 的属性。例如，为 VM 提供计算机配置文件。

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-group>.resourcegroup\<template-
spec>.templatespec\<template-spec-version>.templatespecversion"
```

> **注意：**
>
> 计算机配置文件输入具有一个标签和指定的不同 VM 大小 (`ServiceOffering`)。

5. 获取将 VM 上的配置更新与计算机目录更新合并后 VM 将具有的属性列表。例如：

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

注意：

对 VM 的任何更新都将覆盖对计算机目录所做的更新。

6. 请求 VM 的计划更新。例如：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

7. 重新启动 VM。例如：

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

虚拟机保留其从机器配置文件派生的更新后的虚拟机大小。机器配置文件中指定的标签值也应用于虚拟机。但是，存储类型是从最新的预配方案中派生的。

8. 获取虚拟机的配置版本。例如：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvisioningSchemeVersion` 和 `ProvVMConfigurationVersion` 现在显示最新版本。

回滚应用于虚拟机的配置更新

1. 将更新应用于虚拟机后，关闭虚拟机。
2. 运行以下命令以删除应用于虚拟机的更新。例如：

```
Set-ProvVM -RevertToProvSchemeConfiguration -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

3. 请求 VM 的计划更新。例如：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

4. 重新启动 VM。例如：

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. 检查虚拟机的配置版本。例如：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` 值现在是计算机目录的配置版本。

更改磁盘加密

您可以在 Azure 虚拟化环境中更改磁盘加密并执行以下操作：

- 使用 `New-ProvScheme` 命令创建磁盘加密集 (DES) 与主映像 DES 不同的 MCS 计算机目录。例如：

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/testrsg/
providers/Microsoft.Compute/diskEncryptionSets/test-diskEncryptionSet"/
>

</CustomProperties>

"@

New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName $provisioningSchemeName `

-HostingUnitName $hostingUnitName `

-IdentityPoolName $identityPoolName `

-InitialBatchSizeHint $numberOfVms `

-masterImagePath $masterImagePath `
```

```
-NetworkMapping $networkMapping `

-CustomProperties $customProperties
```

- 使用 `Set-ProvScheme` 和 `Set-ProvVMUpdateTimeWindow` 命令将现有 MCS 计算机目录和现有 VM 的磁盘加密类型从一个 DES 密钥更改为另一个 DES 密钥。重启 VM 后，您可以看到更新的 DES 密钥。例如：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- 使用 `Set-ProvScheme` 和 `Set-ProvVMUpdateTimeWindow` 命令更新以前未启用 CMEK 的 MCS 计算机目录和 VM，以使其具有客户管理的加密密钥 (CMEK) 加密 (DES)、主机上的磁盘加密或双重加密。有关不同加密类型的信息，请参阅 Azure 服务器端加密、Azure 主机上的磁盘加密 和 托管磁盘上的双重加密。
- 使用 `Set-ProvScheme` 和 `Set-ProvVMUpdateTimeWindow` 命令将以前已加密的现有 MCS 计算机目录和 VM 更新为非加密。例如：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'
```

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- 通过专用终结点启用磁盘加密（使用启用了 `ProxyHypervisorTrafficThroughConnector` 的 MCS 计算机目录）。有关如何通过专用终结点启用磁盘加密的信息，请参阅通过专用终结点启用磁盘加密。

启用带专用终结点的磁盘加密

根据 Azure 的限制，目前，您无法为专用终结点使用客户管理的密钥进行服务器端加密。但是，您可以更新现有 MCS 计算机目录和带有专用终结点的 VM，以使用 DES 密钥进行加密。

更新带有专用终结点的现有计算机目录

更新带有专用终结点的现有计算机目录的详细步骤如下：

1. 通过 `ProxyHypervisorTrafficThroughConnector` 创建不带磁盘加密的目录。
2. 运行 `Set-ProvScheme` 以使用 `DiskEncryptionSetId` 更新目录。

注意：

`DiskEcryptionSetId` 可以通过 `CustomProperties` 或 `MachineProfile` 进行配置。当它在 `CustomProperties` 和 `MachineProfile` 中都定义时，将应用在 `CustomProperties` 中定义的属性。

使用 `CustomProperties` 时的示例：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1"/>

</CustomProperties>'
```

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

使用 MachineProfile 时的示例：使用已启用磁盘加密的 VM 或具有磁盘加密设置的模板规范：

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -MachineProfile
"XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

或者，您可以使用 Web Studio 更新计算机配置文件。

3. 运行 `Set-ProvVMUpdateTimeWindow` 以更新现有目录 VM。例如：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

4. 重启 VM 后，您可以在 Azure 门户中 VM 的磁盘上看到更新的磁盘加密。
5. 在添加新的目录 VM 之前，运行 `Set-ProvScheme` 以取消设置磁盘加密。

> **注意：**
>
> 此步骤是必需的，因为您正在更新专用终结点目录。如果您不执行此步骤，则在尝试向目录添加新 VM 时将收到错误。
>
> 例如：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'
```

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

6. 向目录添加新 VM。

更新单个目录 VM

更新单个目录 VM 的详细步骤如下：

1. 通过 `ProxyHypervisorTrafficThroughConnector` 创建不带磁盘加密的目录。
2. 运行 `Set-ProvVM` 以使用 `DiskEncryptionSetId` 更新目录 VM。

> **注意：**
>
> 可以通过 `CustomProperties` 或 `MachineProfile` 配置 `DiskEcryptionSetId`。
>
> 使用 `CustomProperties` 时的示例：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-CustomProperties $customProperties
```

使用 MachineProfile 时的示例：

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

3. 运行 `Set-ProvVMUpdateTimeWindow` 以更新现有目录 VM。例如：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01 -StartsNow -DurationInMinutes -1
```

4. 重启 VM 后，您可以在 Azure 门户中看到 VM 磁盘上更新的磁盘加密。
5. 将新 VM 添加到目录。

将临时磁盘用作现有目录的 WBC 磁盘

您可以将 Azure 临时磁盘用作现有 MCS 计算机目录的回写缓存 (WBC) 磁盘。使用 `Set-ProvScheme` PowerShell 命令更新现有目录和 VM。

先决条件

现有目录必须满足以下条件：

> **注意：**
>
> 如果现有目录不满足以下要求，则 WBC 磁盘不会放置在临时磁盘内。

- MCSIO 已启用：自定义属性 `WriteBackCacheMemorySize`、`WriteBackCacheDiskSize` 和 `UseWriteBackCache` 已启用。
- 未启用临时 OS 磁盘。
- WBC 是非持久性的：`PersistWBC` 为 `false`。
- `UseTempDiskForWBC` 为 null 或 false。
- 临时磁盘大小必须大于（回写缓存磁盘大小 + 分页文件保留空间 + 1 GB 缓冲区空间）的总大小。

> **重要：**
>
> 不允许将服务产品从包含临时磁盘的更改为不包含临时磁盘的，反之亦然。

更新现有目录

要更新现有目录，请运行以下命令：

1. 在现有目录上运行 `Set-ProvScheme` 以将 `UseTempDiskForWBC` 更新为 `true`。例如：

```
Set-ProvScheme -ProvisioningSchemeName name -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Standard_LRS`"/><Property
xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"ManagedDisksPreview`"
Value=`"False`"/><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"False`"/><Property
xsi:type=`"StringProperty`" Name=`"UseTempDiskForWBC`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"False`"/></CustomProperties>"
```

2. 将新计算机添加到目录并开机。新 VM 在临时磁盘内具有 WBC 磁盘。

检索 Azure VM、快照、操作系统磁盘和库映像定义的信息

您可以显示 Azure VM 的信息，包括操作系统磁盘和类型、快照和库映像定义。分配计算机目录时，此信息会显示在主映像上的资源中。使用此功能可以查看和选择 Linux 或 Windows 映像。PowerShell 属性 `TemplateIsWindowsTemplate` 已添加到 `AdditionDatafield` 参数。此字段包含 Azure 特定的信息：VM 类型、操作系统磁盘、库映像信息和操作系统类型信息。将 `TemplateIsWindowsTemplate` 设置为 **True** 表示操作系统类型为 Windows；将 `TemplateIsWindowsTemplate` 设置为 **False** 表示操作系统类型为 Linux。

提示：

`TemplateIsWindowsTemplate` PowerShell 属性显示的信息源自 Azure API。有时，此字段可能为空。例如，数据磁盘的快照不包含 `TemplateIsWindowsTemplate` 字段，因为无法从快照中检索操作系统类型。

例如，使用 PowerShell 将 Azure VM `AdditionData` 参数设置为 **True** 以表示 Windows 操作系统类型：

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value
```

```
ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192

ServiceOfferingCores 2

TemplateIsWindowsTemplate True

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

克隆 MCS 目录

将现有的持久性和非持久性 MCS 目录拆分为多个目录。通过创建原始预配方案的克隆，您可以将不同的目录级策略和配置应用于特定的 VM 子集。当组织内不同的职能角色（例如财务或高管）与标准用户相比需要不同的资源配置（例如备份限制）时，此功能特别有用。

用法示例

管理员管理着一个大型 VM 目录。高管团队需要的备份数量高于标准策略允许的范围。管理员使用 `Copy-ProvScheme` 命令将现有目录预配方案克隆到新目录中。这允许管理员将专用备份策略应用于新的高管目录，同时为组织的其他部分保留原始设置。

适用性

- Azure 环境
- 持久性和非持久性 MCS 目录
- MCS 预配的 Citrix Provisioning 目录

限制

- **预配方案：** 仅复制预配方案的最新版本。
- **备份计划**：备份计划不会复制到新目录；新目录必须配置自己的备份计划。
- **身份池**：与身份相关的对象不会被克隆，而是使用相同的 `ADAccountIdentityPool` 保持共享。
- **交付组**：在克隆过程中，交付组操作和用户分配不会更改或关联。

重要注意事项

- **资源组 (目标位置)**:
  - 如果您未提供 `TargetLocation` (Azure 资源组):
    - 对于 Citrix 托管资源组，将创建一个新的 Citrix 托管资源组。
    - 对于 BYO（自带）资源组，新的预配方案资源将在同一资源组中创建。
  - 如果您提供 `TargetLocation`:
    - 资源将在提供的资源组中创建。
    - 指定的资源组必须已在 Azure 中存在。
- **基本磁盘快照**：始终会创建基本磁盘快照的副本，无论资源组配置如何。

先决条件

- 必须存在一个现有预配方案（源目录）。
- 如果指定目标位置，则目标 Azure 资源组必须存在。

使用 POWERSHELL 进行配置

1. 打开 PowerShell 窗口。
2. 使用所需参数运行 `Copy-ProvScheme` 命令：`SourceProvisioningSchemeName`（或 `SourceProvisioningSchemeUid`）和 `TargetProvisioningSchemeName`。

   示例 1：按名称复制预配方案。

   此示例将名为“Backup”的方案复制到名为“TestCopy”的新方案。

   ```
   Copy-ProvScheme -SourceProvisioningSchemeName Backup
   -TargetProvisioningSchemeName TestCopy
   ```

   示例 2：按 Uid 将预配方案复制到特定资源组

   此示例使用其 Uid 复制方案，并指定名为“TestRg”的目标资源组。

   ```
   Copy-ProvScheme -SourceProvisioningSchemeUid 771e205d-1ee5-4ad2-b044-
   ecf3d7f24ec7 -TargetProvisioningSchemeName TestCopy -TargetLocation
   TestRg
   ```

识别 MCS 创建的资源

以下是 MCS 添加到资源的标签。表中的标签表示为“key”:“value”。

资源名称	标签
ID 磁盘	"思杰预配方案 ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
映像	"思杰预配方案 ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
NIC	"思杰预配方案 ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
操作系统磁盘	"思杰预配方案 ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
准备虚拟机	"思杰预配方案 ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
已发布的快照	"思杰预配方案 ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
资源组	"CitrixResource" : "内部"
	CitrixSchemaVersion: 2.0
	"思杰预配方案 ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
存储帐户	"思杰预配方案 ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

资源名称	标签
	"CitrixResource" : "内部"
目录中的 VM	"思杰预配方案 ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
WBC 磁盘	"思杰预配方案 ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"

注意：

如果添加了 **CitrixResource** 标签以将其标识为由 MCS 创建的资源，则 VM 在 Citrix 清单中不可见。您可以删除或重命名该标签以使其可见。

删除标签

创建目录或 VM 时，会在以下资源上创建标签：

- 资源组
- 虚拟机
- 操作系统磁盘
- 标识磁盘
- 网络接口
- 存储帐户

您可以从 Citrix 数据库中删除 VM 和计算机目录，并删除标签。您可以使用：

- 使用 `ForgetVM` 参数的 `Remove-ProvVM` 可从单个 VM 或计算机目录中的 VM 列表中删除 VM 和标记。
- 使用 `ForgetVM` 参数的 `Remove-ProvScheme` 可从 Citrix 数据库中删除计算机目录，并从整个计算机目录中删除标记。

此功能仅适用于持久性 VM。

为此：

1. 打开 **PowerShell** 窗口。
2. 运行 **asnp citrix*** 以加载 Citrix 特定的 PowerShell 模块。
3. 运行 `Remove-ProvVM` 以从 Citrix 数据库中删除 VM 并从 VM 中删除标记。 例如：

```
Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -VMName “vmname” -ForgetVM
```

4. 运行 `Remove-ProvScheme` 以从 Citrix 数据库中删除计算机目录并从计算机目录中删除标记。 例如：

```
Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName” -ForgetVM
```

> **注意：**
>
> 在 `Remove-ProvScheme` 中使用 `ForgetVM` 参数后，如果预配方案存在于自带资源组 (BYORG) 或 Citrix 托管资源组中，MCS 将删除所有快照，包括基本磁盘快照。

更多信息

- 创建和管理连接与资源
- 连接到 Microsoft Azure
- 创建计算机目录
- 创建 Microsoft Azure 目录
- 管理计算机目录

管理 Microsoft System Center 虚拟机管理器目录

管理计算机目录 介绍了用于管理计算机目录的向导。以下信息涵盖了 Microsoft System Center Virtual Machine Manager (VMM) 虚拟化环境特有的详细信息。

> **注意：**

> 在管理 VMM 目录之前，您需要完成 VMM 目录的创建。请参阅创建 Microsoft System Center Virtual Machine Manager 目录。

识别 MCS 创建的资源

以下是 MCS 添加到资源的标签。表中的标签表示为“key”:“value”。

资源名称	标签
准备虚拟机	此标签的字符串表示形式为: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	自定义属性条目：“XdConfig:””XdProvisioned=True”
目录中的 VM	此标签的字符串表示形式为: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	自定义属性条目：“XdConfig:””XdProvisioned=True”

更多信息

- 创建和管理连接与资源
- 连接到 微软系统中心虚拟机管理器
- 创建计算机目录
- 创建微软系统中心虚拟机管理器目录
- 管理计算机目录

管理 Nutanix 目录

(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-manage.html)介绍了用于管理计算机目录的向导。以下信息涵盖了 Nutanix AHV Prism Central 环境的特定详细信息。

> **注意：**

在 Nutanix AHV Prism Central 上管理计算机目录之前，您需要完成在 Nutanix AHV Prism Central 上创建计算机目录。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-create/create-machine-catalog-nutanix.html)。

您可以使用以下方式在 Nutanix AHV Prism Central 上管理计算机目录：

- Web 工作室
- (#use-powershell)

使用 Web Studio

以下是使用 Web Studio 在 Nutanix AHV Prism Central 上管理计算机目录的选项：

选项	描述
添加计算机	创建虚拟机并将其添加到计算机目录。
删除计算机目录	删除计算机目录。您可以选择同时删除虚拟机，或保留持久性虚拟机不变。
更改主映像	更改用作目录中所有 VM 模板的主映像。
添加或更改计算机配置文件	更改计算机配置文件的模板版本，或将计算机配置文件添加到现有目录。
管理配置集	将目录绑定到 Workspace Environment Management™ 配置集，或切换到其他配置。
编辑计算机目录	修改目录的配置，例如网卡和虚拟机。
查看计算机	跳转到“**搜索**”节点以查看属于该目录的所有 VM。
重命名计算机目录	更改目录名称。
升级 VDA	按目录升级 VDA。此功能仅适用于静态持久性计算机。
更改功能级别	选择目录的最低功能级别。设置功能级别可使所有功能可用。
测试计算机目录	测试目录是否存在错误或警告。

选项	描述
管理标签	创建、编辑和删除标签。选择要应用于目录的标签。
移动计算机目录	将目录移动到另一个文件夹。

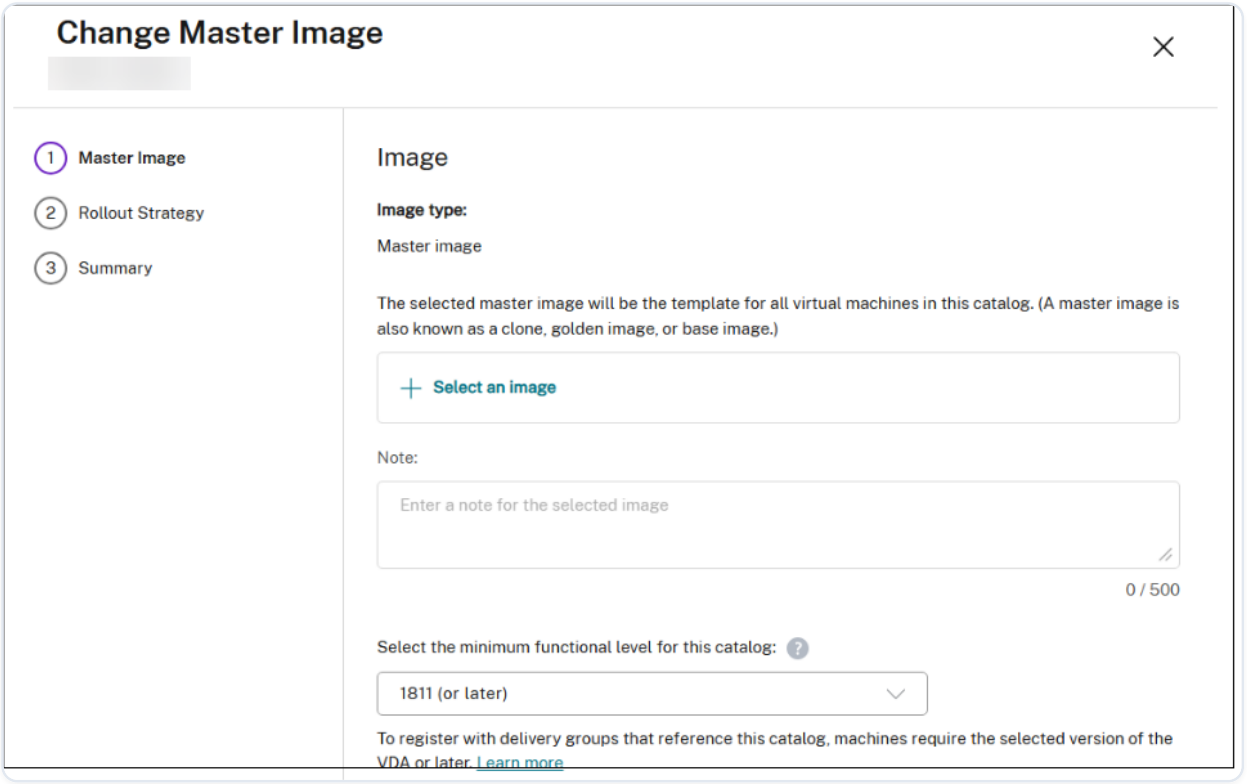
注意：

目前，**克隆**选项不可用。

更改主映像

要更改目录的主映像，请执行以下步骤：

1. 在**计算机目录**页面上，右键单击要更新的计算机目录，然后选择**更改主映像**。
2. 在**更改主映像**页面上，单击**选择映像**。



3. 在**选择映像**页面上，展开模板并选择要用作主映像的模板版本。您可以按名称筛选计算机模板。
4. 在**推出策略**页面上，选择您希望何时应用更新。

注意：

> 对于使用 Nutanix AHV Prism Central 主机连接插件的 MCS 预配的非持久性目录，更新主映像以在 Legacy 和 UEFI 之间切换引导配置会阻止现有 VM 在下次启动时启动。 更新主映像时，仅更新操作系统磁盘。硬件属性保持不变。要更新硬件属性，请参阅 添加或更改计算机配置文件、更改 NIC 和 更改 VM 配置。

添加或更改计算机配置文件

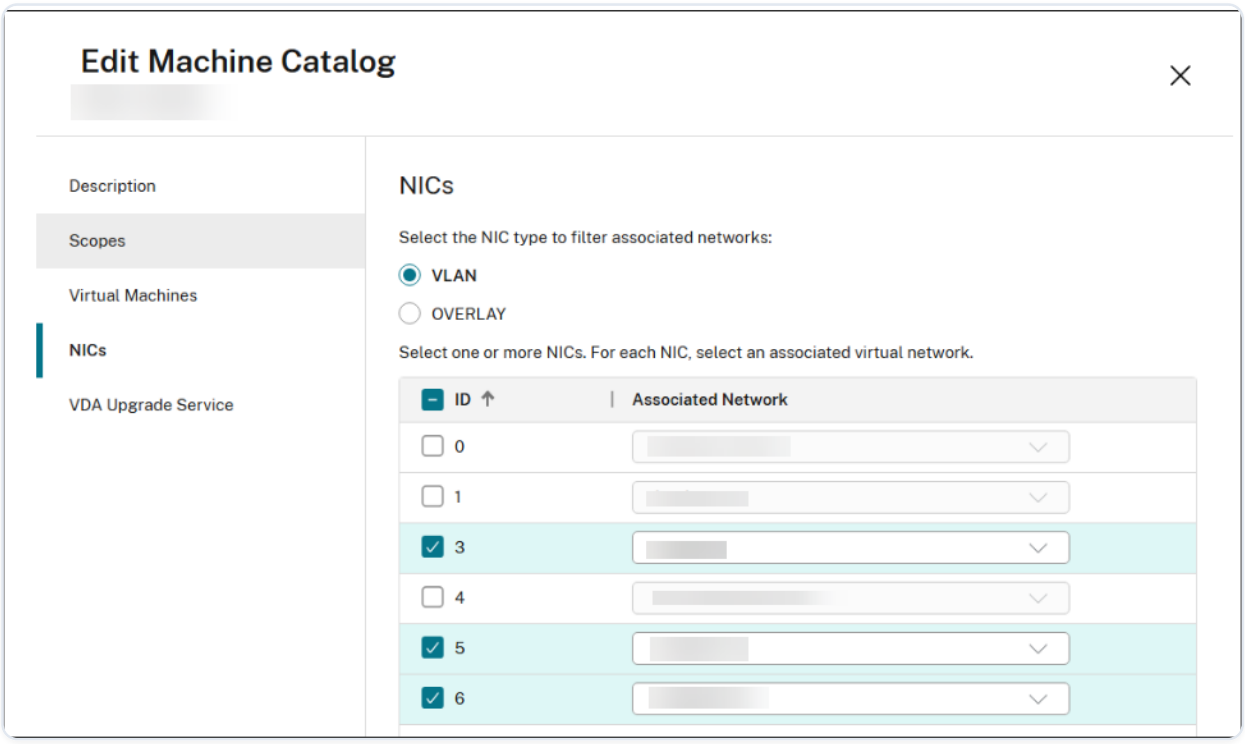
要为目录添加或更改计算机配置文件，请按照以下步骤操作：

1. 在**计算机目录**页面上，右键单击要修改的计算机目录，然后选择**编辑计算机目录**。
2. 在**计算机配置文件**页面上，
   - 如果计算机目录已具有计算机配置文件，请单击铅笔图标以选择其他计算机配置文件模板版本。您可以按模板名称进行筛选。确认计算机配置文件设置。
   - 如果计算机目录没有计算机配置文件，请选择“使用计算机配置文件”并选择一个计算机配置文件。确认计算机配置文件设置。
3. **虚拟机**页面必须反映根据所选计算机配置文件模板版本更新的配置。

更改网卡

要更改目录的网卡，请按照以下步骤操作：

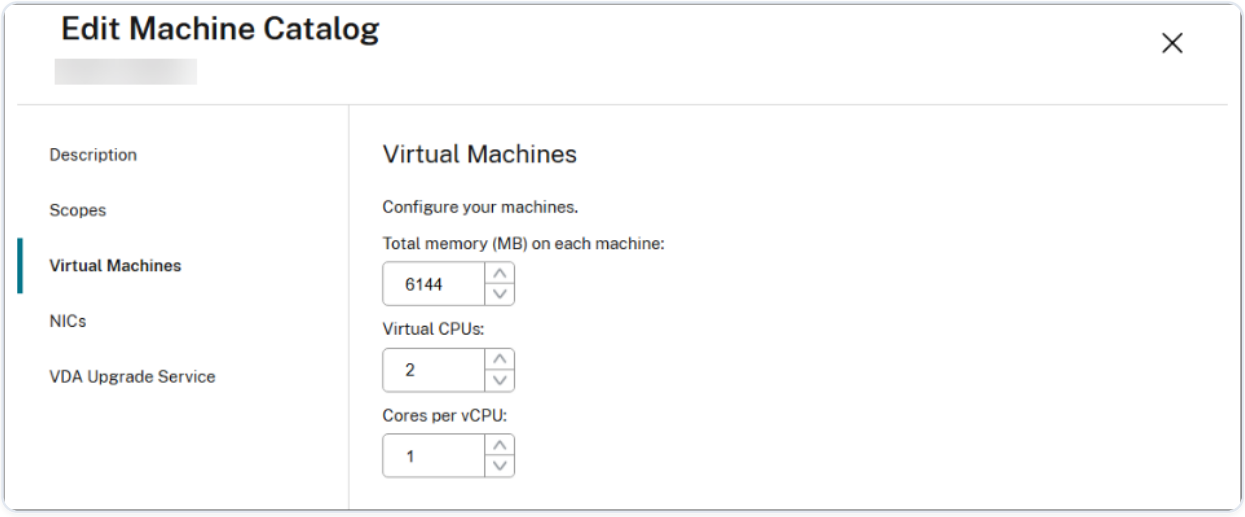
1. 在**计算机目录**页面上，右键单击要修改的计算机目录，然后选择**编辑计算机目录**。
2. 在“**NICs**”页面上：
   a. 选择 NIC 类型
   b. 选中或清除复选框以选择 NIC，并为每个 NIC 选择关联的虚拟网络。



更改 VM 配置

要更改 VM 的配置，包括内存、CPU 计数和每个 vCPU 的核心数，请执行以下步骤：

1. 在**计算机目录**页面上，右键单击要修改的计算机目录，然后选择**编辑计算机目录**。
2. 在**虚拟机**页面上，使用向上或向下箭头，或直接输入值来调整 VM 的内存、CPU 计数和每个 vCPU 的核心数。



使用 PowerShell

更改主映像

所需的参数为：

- `ProvisioningSchemeName`：要编辑的预配方案的名称。

- `MasterImage`：新主映像的字面路径。

运行以下命令。例如：

```
Set-ProvSchemeMetadata  -Name "ImageManagementPrep_DoImagePreparation"
-ProvisioningSchemeName "<ProvisioningSchemeName>" -Value "True"



Publish-ProvMasterVMImage  -MasterImageVM "<Literal path to the new master
image- template version> -ProvisioningSchemeName
"<ProvisioningSchemeName>" -RunAsynchronously
```

注意：

更新主映像时，仅更新操作系统磁盘。硬件属性保持不变。要更新硬件属性，请参阅添加或更改计算机配置文件、更改 NIC 和更改 NIC 和 VM 配置。

添加或更改计算机配置文件

使用 `Set-ProvScheme` 命令：

- 使用新的计算机配置文件更新目录，或
- 更新现有目录（没有计算机配置文件），使其开始使用计算机配置文件作为硬件规范的来源。

注意：

这不会更新目录中现有 VM 的硬件规范。只有添加到目录中的新 VM 才具有给定计算机配置文件中的硬件规范。

要更改计算机配置文件或将现有目录转换为开始使用计算机配置文件：

```
Set-ProvScheme -ProvisioningSchemeName <ProvScheme Name> `

               -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion"
```

计算机配置文件必须至少有一个 NIC，并且计算机配置文件中的 NIC 数量必须与 NetworkMapping 中的子网映射匹配

模板版本的 NIC 总数可以从其清单项的 `AdditionalData` 中使用以下方法获取：

```
$tv = Get-Item -Path "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion"

$tv.AdditionalData.TotalNics
```

要更改具有覆盖硬件规范的计算机配置文件：

可以使用特定的命令行参数配置某些设置。这些命令行参数，例如 `VMCpuCount` 和 `VMMemoryMB`，以及 `CPUCores` 在 `CustomProperties` 中，优先于计算机配置文件模板版本中的值。

```
$customProperties = @"

    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378" />

        <StringProperty Name="CPUCores" Value="2" />

    </CustomProperties>

"@



Set-ProvScheme -ProvisioningSchemeName <ProvScheme Name> `

               -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion" `

               -CustomProperties $customProperties `

               -VMCpuCount 4 `
```

```
                -VMMemoryMB 4096
```

更改 NIC 和 VM 配置

所需的参数为：

- `ProvisioningSchemeName`：要编辑的预配方案的名称。
- `NetworkMapping`：更新的网络映射。

运行以下命令。例如：

```
Set-ProvScheme  -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`"
Name=`"ClusterId`" Value=`"000xxxx-1fb0-xxxxx-4fc8-5c257335xxxx`" /
><Property xsi:type=`"StringProperty`" Name=`"CPUCores`" Value=`"1`" /></
CustomProperties>"  -NetworkMapping @{"6"="XDHyp:\HostingUnits\<Hosting
Unit Name>\Clusters.folder\<Cluster Name>\<Network name>.network"}
-ProvisioningSchemeName "<ProvisioningSchemeName>" -VMCpuCount 4
```

重置持久性 VM 的操作系统磁盘

重置持久性 VM（尤其是那些启用了 vTPM 的 VM）中的操作系统磁盘可能会破坏依赖 vTPM 密钥和 BitLocker 的应用程序，从而可能阻止启动。因此，此功能允许：

- 重置持久性 VM 的操作系统磁盘并保留 VM 硬件配置。
- 管理启用了 vTPM 的 VM，以避免在磁盘交换期间破坏 vTPM 依赖关系。

您可以使用 `Reset-ProvVMDisk` PowerShell 命令重置持久性 VM 的操作系统磁盘。

- 对于启用了 vTPM 的 VM：使用原始硬件信息从恢复点创建新的 VM，从而保留 vTPM 密钥。
- 对于非 vTPM VM：替换操作系统磁盘。

有关示例，请参阅重置操作系统磁盘。

将计算机目录迁移到 Citrix 管理的 Nutanix AHV Prism Central 主机连接

将您的 Citrix 计算机目录及其关联的 VM 从现有的 Nutanix AHV（适用于 Prism Element）和 Nutanix AHV PC（适用于 Azure 上的 NC2）主机连接迁移到 Citrix 管理的 Nutanix AHV Prism Central 主机连接。对于迁移，请使用 PowerShell 命令，这些命令还包括在出现问题时的快速回滚选项，以及迁移后清理源资源的命令。

优势

- **最小化中断**：您可以顺利过渡到 Nutanix AHV Prism Central 插件。这对外现有部署影响最小。
- **无缝升级路径**：它为您升级基础架构和利用新的管理界面提供了一条清晰且受支持的路径。
- **数据完整性和安全性**：回滚选项可确保您在出现不可预见的问题时将环境恢复到其原始状态。这降低了风险。
- **资源效率**：成功迁移后，您可以清理源资源。这优化了存储和管理开销。
- **灵活性**：它支持由 MCS 和第三方技术预配的目录的迁移。这提供了更广泛的适用性。

适用性

此功能适用于 Nutanix AHV（用于 Prism Element）和 Nutanix AHV PC（用于 Azure 上的 NC2）主机连接下的计算机目录：

- 由 MCS 管理的计算机目录，包括持久类型和非持久类型。
- 仅限电源管理的计算机目录，其中包含由第三方技术预配的 VM。

系统要求

- **Nutanix AHV Prism Element (PE) AOS 版本**：您需要最低 6.8 版本。
- **Nutanix Prism Central (PC) 版本**：您需要最低 2024.3 版本。

> **注意：**
>
> 由于 Nutanix 的已知问题，Nutanix Prism Central 7.3 需要 AOS 7.3。

限制

- **PVS 目录不受支持**：此功能**不**支持使用 **Citrix Provisioning Services** (PVS) Xendesktop 安装向导创建的计算机目录。
- **回滚限制**：
  - 仅当您在初始迁移后**未**修改目录时，才允许回滚已迁移的目录。
  - 当您执行“**清理源资源**”操作时，它会清除迁移状态。这会阻止任何后续回滚。
- **不支持重新迁移**：已迁移的计算机目录不支持重新迁移。
- **多主机连接虚拟机**：不支持迁移包含从多个主机连接导入的虚拟机的仅电源管理的计算机目录。

重要注意事项

- **Nutanix 群集管理**：托管 Nutanix AHV 群集必须注册到 Nutanix Prism Central。

- **主映像模板创建**：对于 MCS 计算机目录，迁移命令提供了一个选项，可用于从计算机目录主映像的原始快照在 Prism Central 上生成虚拟机模板版本。此虚拟机模板版本以后可用作 Prism Central 主机连接下计算机目录的 MCS 主映像。默认情况下，此选项未启用。
- **回滚先决条件**：

  为了能够成功回滚，原始源环境（包括主机连接、基本磁盘）必须保持不变。在确认迁移成功之前，您还必须避免对已迁移的计算机目录进行任何配置更改以及添加/删除虚拟机。 确认后，您可以执行最终的“清理源资源”操作，但请注意，这是一个不可逆的步骤，将使回滚无法进行。

迁移和回滚所需的权限

要迁移目录或回滚，您需要以下权限：

Prism Element 管理员：

- 创建虚拟机

Prism Central 管理员：

- 创建 VM 模板
- 删除 VM 模板
- 删除 VM 恢复点
- 删除虚拟机

有关 Citrix 管理的 Nutanix AHV Prism Central 主机连接所需特定权限的完整列表，请参阅所需权限。

如何迁移

您可以通过专用的 PowerShell cmdlet 管理此功能。一般工作流程涉及三个主要操作：迁移、回滚和清理源资源。

迁移计算机目录

- 此操作将计算机目录及其关联的 VM 从源 Nutanix AHV 或 Nutanix AHV PC 主机连接移动到目标 Citrix 管理的 Nutanix AHV Prism Central 主机连接。
- 对于 MCS 预配的目录，此过程会在目标连接中创建新的基础磁盘。
- 您可以选择从原始主映像快照在目标连接中创建等效的主 VM（VM 模板版本）。

1. **创建新的 Nutanix AHV Prism Central 主机连接**：在迁移之前，将托管 Nutanix AHV 群集注册到 Nutanix Prism Central，并建立指向目标 Nutanix Prism Central 实例的新 Nutanix AHV Prism Central 主机连接。此连接将作为您迁移的目录的目标。有关详细信息，请参阅Nutanix AHV Prism Central 主机连接。

2. **迁移现有计算机目录**：对于现有计算机目录，请使用 `Switch-ProvCatalog` PowerShell cmdlet 启动到 Citrix 管理的 Nutanix AHV Prism Central 主机连接的迁移。

```
c:\PS>Switch-ProvCatalog -BrokerCatalogUid <Catalog_UID>
-DestinationHypervisorConnectionName "DestinationConnection"
-DestinationHostingUnitName "DestinationUnit"
-CreateMasterImageAtDestination
```

   - 将 `<Catalog_UID>` 替换为您要迁移的计算机目录的唯一标识符。使用以下 PowerShell cmdlet 按目录名称 `Get-BrokerCatalog -Name <Catalog Name>` 查找 `BrokerCatalogUid`。
   - `DestinationConnection` 是在步骤 1 中创建的新 **Nutanix AHV Prism Central 主机连接** 的名称。
   - `DestinationUnit` 是您在 `DestinationConnection` 中为托管单元指定的名称，计算机目录将驻留在该托管单元中。
   - `-CreateMasterImageAtDestination` 参数是可选的。它会在目标 Prism Central 上创建主映像 VM 模板版本。

3. **验证迁移完成情况**：执行迁移 cmdlet 后，监视 PowerShell 窗口中的任务状态，确保其成功完成。迁移完成后，目录将移动到在步骤 1 中创建的目标主机连接。您必须看到任务类型为 SwitchProvCatalog 的已完成状态。以下是验证迁移完成情况的建议步骤：

   - 检查 Studio 中目录的状态。
   - 验证目录中的 VM 现在是否与新的目标管理程序连接相关联。
   - 验证目录中的 VM 是否显示正确的电源状态。
   - 通过添加或删除计算机或执行电源操作来测试已迁移计算机目录的功能，确保目录正常运行。

回滚已迁移的目录

此操作会将计算机目录及其 VM 恢复到其原始源主机连接。它会删除您在迁移过程中创建的任何资源。

> **重要提示：**
>
> 仅当您在迁移后未修改目录且未运行“**清理源资源**”操作时，才执行回滚。原始源连接保持不变，并且仍包含其基本磁盘。

```
c:\PS>Switch-ProvCatalog -BrokerCatalogUid <Catalog_UID> -Rollback
```

清理源资源

成功迁移后，此操作会从原始管理程序连接中删除源资源，例如基本磁盘。

> **重要提示：**
>
> 执行此命令时，它会清除迁移状态。这使得后续回滚变得不可能。

```
c:\PS>Switch-ProvCatalog -BrokerCatalogUid <Catalog_UID>
-CleanupSourceResources
```

在继续操作之前，您会收到一个确认提示，因为此操作不可逆。请确认提示以完成清理。

更多信息

- 创建和管理连接与资源
- 连接到 Nutanix
- 连接到 Nutanix 云和合作伙伴解决方案
- 创建计算机目录
- 创建 Nutanix 目录
- 管理计算机目录

管理 VMware 目录

管理计算机目录 描述了管理计算机目录的向导。以下信息涵盖了 VMware 虚拟化环境特有的详细信息。

> **注意：**
>
> 在管理 VMware 目录之前，您需要完成创建 VMware 目录。请参阅 创建 VMware 目录。

更新计算机目录的文件夹 ID

您可以通过在 `Set-ProvScheme` 命令的自定义属性中指定 `FolderId` 来更新 MCS 计算机目录的文件夹 ID。更新文件夹 ID 后创建的 VM 将在此新文件夹 ID 下创建。如果在 `CustomProperties` 中未指定此属性，则 VM 将在主映像所在的文件夹下创建。

执行以下步骤以更新计算机目录的文件夹 ID。

1. 打开 Web 浏览器并输入 **vSphere Web Client** 的 URL。
2. 输入凭据并单击 **Login**。
3. 在 **vSphere Web Client** 中创建 VM 放置文件夹。
4. 打开 PowerShell 窗口。
5. 运行 **asnp citrix®*** 以加载 Citrix 特定的 PowerShell 模块。
6. 在 `Set-ProvScheme` 的 `CustomProperties` 中指定 `FolderID`。在此示例中，文件夹 ID 值为 `group-v2406`。

```
Set-ProvScheme -ProvisioningSchemeUid
"50bb319c-2e83-4a37-9ea1-94f630687372" -CustomProperties
"<CustomProperties xmlns=""http://schemas.citrix.com/2014/xd/
machinecreation"" xmlns:xsi=""http://www.w3.org/2001/XMLSchema-
instance""><Property xsi:type=""StringProperty"" Name=""FolderId""
Value=""group-v2406"" /></CustomProperties>"
```

7. 使用 Studio 将 VM 添加到计算机目录。
8. 在 vSphere Web Client 上检查新 VM。新 VM 在新文件夹下创建。

在 VSPHERE 中查找文件夹 ID

在任何 ESXi 或 vCenter 服务器系统上访问托管对象浏览器 (MOB)，以查找 VM 的文件夹 ID。

MOB 是一种基于 Web 的服务器应用程序，内置于所有 ESX/ESXi 和 vCenter 服务器系统中。此 vSphere 实用程序允许您查看有关 VM、数据存储和资源池等对象的详细信息。

1. 打开 Web 浏览器并输入 `http://x.x.x.x/mob`，其中 x.x.x.x 是 vCenter Server 或 ESX/ESXi 主机的 IP 地址。例如，`<https://10.60.4.70/mob>`。
2. 在 MOB 的“**主页**”上，单击属性 **content** 的值。
3. 单击 **rootFolder** 的值。
4. 单击 **childEntity** 的值。
5. 单击 **vmFolder** 的值。

6. 您可以在 **childEntity** 的值中找到文件夹 ID。

识别 MCS 创建的资源

以下是 MCS 添加到资源的标签。表中的标签表示为“key”:“value”。

资源名称	标签
准备虚拟机	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"Xd配置:Xd已置备=真"
目录中的 VM	"思杰预配方案标识符": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"Xd配置:Xd已置备=真"

更多信息

- 创建和管理连接与资源
- 连接到 VMware
- 创建计算机目录
- 创建 VMware 目录
- 管理计算机目录

电源管理

借助 Citrix Virtual Apps and Desktops™，您可以在各种受支持的虚拟机管理程序和云服务中对 MCS 预配的 VM 进行电源管理。电源管理操作为您提供：

- 最佳用户体验
- 成本管理和节电

可用的电源操作包括：

- 启动
- 关机
- 重新启动
- 挂起
- 恢复

- 强制重新启动
- 强制关机

注意：

- 对于非持久性 VM，电源循环（关机/启动和重新启动）会导致操作系统磁盘重置。
- 电源操作功能和行为因虚拟机管理程序或云服务而异。

本文介绍了与某些受支持的虚拟机管理程序相关的关键电源管理功能。

- 管理 AWS VM 的电源
- 管理 Azure VM 的电源

管理 Amulet Hotkey CoreStation 虚拟机电源

Citrix Virtual Apps and Desktops™ 允许您对 Amulet Hotkey CoreStation 虚拟机进行电源管理。使用导航窗格中的**搜索**节点查找要管理电源的计算机。

提供以下电源操作：

- 启动
- 关机
- 强制关机
- 强制重新启动
- 重新启动

注意：

- 重置、挂起和恢复电源操作不受支持。
- 关机/重新启动：请求节点关闭操作系统并断电。这相当于短按物理桌面计算机的电源按钮。如果存在活动用户或正在运行的程序中断关机，或者需要安装操作系统更新，则工作站可能不会响应关机请求。

电源管理 AWS 虚拟机

有关所需权限的信息，请参阅所需的 AWS 权限。

实例休眠

休眠过程会存储实例的内存中状态，以及其私有 IP 地址和弹性 IP 地址，使其能够从上次中断的地方继续运行。

当实例被指示休眠时，它会将内存中状态写入根 EBS 卷中的文件，然后自行关闭。Amazon EBS 卷是一种持久的块级存储设备，您可以将其连接到实例。将卷连接到实例后，您可以像使用物理硬盘一样使用它。加密实例的根 EBS 卷。加密可确保敏感数据从内存复制到 EBS 卷时得到适当保护。有关 EBS 加密的信息，请参阅 Amazon EBS 加密。

以下是支持的实例休眠的限制：

- 仅支持高达 150 GB 的实例内存 (RAM)
- 不支持 UEFI 启动模式
- 仅支持通用型 SSD 和预置 IOPS SSD 作为 EBS 卷类型。

创建支持休眠的虚拟机

要创建支持休眠的虚拟机，请执行以下操作：

1. 创建主机连接。请参阅 连接到 AWS。
2. 启动一个实例，该实例的 EBS 根已加密且已启用 **Stop-Hibernate** 属性。有关如何启动实例、加密根 EBS 卷以及启用休眠的详细信息，请参阅 `<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/>`。使用此实例作为主映像来创建 AMI。
3. 准备主映像：
   a. 在主映像上安装 VDA。Citrix 建议安装最新版本以访问最新功能。如果未在主映像上安装 VDA，则会导致目录创建失败。有关如何安装 VDA 的详细信息，请参阅 安装 VDA。
   b. 将主映像加入到应用程序和桌面所属的域中。确保主映像在创建计算机的主机上可用。
4. 从该实例创建 AMI。有关从实例创建 AMI 的信息，请参阅 从 Amazon EC2 实例创建 AMI。
5. 使用 `New-ProvScheme` 命令创建计算机目录。将 `AwsCaptureInstanceProperties` 自定义属性设置为 **True**。有关在 Web Studio 中启用 AWS 实例属性的信息，请参阅**在 Web Studio 中应用 AWS 实例属性和标记操作资源**。

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot

-CustomProperties "AwsCaptureInstanceProperties,true;"
```

```
-HostingUnitName "xxx" -IdentityPoolName $catalog_name
-InitialBatchSizeHint 1

-MasterImageVM "xyz.template" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\MyConn\\us-east-2a.availabilityzone\10.0.0.0``/24
(vpc-0f1771e45671aedcd).network"}

-ProvisioningSchemeName $catalog_name

-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -ServiceOffering
"xxx"
```

有关使用 PowerShell 命令创建计算机目录的信息，请参阅 `<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>`。

在以下情况下，将创建可休眠的 VM：

- 您选择的 AMI 是从启用了 **Stop-Hibernate** 属性的主映像创建的。
- 主 VM 已加入域并安装了 VDA。
- 您选择正确的 VM 大小（服务产品），该大小可以处理休眠。

New-ProvScheme 命令在以下情况下会显示相应的错误消息：

- 主 VM 已启用休眠，但服务产品无法处理休眠。
- 如果主 VM 未加入域且未安装 VDA。

服务产品和 AMI 的休眠状态

要获取服务产品和 AMI（模板）的休眠状态，请运行以下命令：

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

更新现有支持休眠的预配方案的服务产品

1. 运行 `Set-ProvScheme` 命令。例如，

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering
<String>
```

如果服务产品不兼容，系统会显示异常消息。

创建支持休眠的计算机目录

创建计算机目录时，您可以使用支持休眠的计算机配置文件。

1. 在目录创建向导中，请按照说明操作，直到选择计算机配置文件。
2. 在**计算机模板**页面上，单击**选择计算机配置文件**并选择一个计算机配置文件。
3. 在“**虚拟机**”页面上，单击“**编辑**”图标并选择一个虚拟机。

> **注意：**
>
> 如果计算机配置文件启用了休眠，系统将仅显示可休眠的虚拟机。

4. 按照屏幕上的说明完成所有设置。“**摘要**”页面显示目录的休眠状态。

> **注意：**
>
> 在编辑计算机目录时，当您将计算机配置文件更改为启用休眠的配置文件时，系统会要求您相应地重新配置虚拟机。

更新支持休眠的计算机目录

如果您尝试使用不支持休眠的计算机目录更新现有计算机目录，则更新将失败并显示相应的错误消息。

休眠虚拟机的电源管理

您可以对休眠的虚拟机执行以下电源管理操作：

1. 从运行状态挂起 VM。
2. 从挂起状态恢复虚拟机。
3. 从挂起状态重新启动虚拟机。

Azure 本地 VM 的电源管理

Citrix Virtual Apps and Desktops™ 允许您对 Azure 本地 VM 进行电源管理。使用导航窗格中的**搜索**节点查找要进行电源管理的计算机。

提供以下电源操作：

- 启动
- 关机
- 强制关机
- 重新启动

> **注意：**
>
> 重置、挂起和恢复电源操作不受支持。

管理 Azure VM 的电源

有关所需权限的信息，请参阅所需的 Azure 权限。

Azure 按需预配

借助 Azure 按需预配，VM 仅在 Citrix Virtual Apps and Desktops™ 在预配完成后启动开机操作时创建。

当您使用 MCS 在 Azure Resource Manager 中创建计算机目录时，Azure 按需预配功能具有以下特点：

- 降低存储成本
- 加快目录创建速度

创建 MCS 目录时，Azure 门户会在资源组中显示网络安全组、网络接口、基础映像和身份磁盘。

Azure 门户不会显示 VM，直到 Citrix Virtual Apps and Desktops™ 为其启动开机操作。有两种类型的计算机，其区别如下：

- 对于池化计算机，操作系统磁盘和回写缓存仅在 VM 存在时才存在。当您在控制台中关闭池化计算机时，VM 在 Azure 门户中不可见。如果您定期关闭计算机（例如，在工作时间之外），则可以显著节省存储成本。

- 对于专用计算机，操作系统磁盘在 VM 首次开机时创建。Azure 门户中的 VM 会一直保留在存储中，直到计算机身份被删除。当您在控制台中关闭专用计算机时，VM 在 Azure 门户中仍然可见。

注意：

对按需预配功能之前创建的 Azure 目录（“旧版”目录）的支持已弃用。因此，请重新创建 Azure 旧版目录 VM。然后，这些目录将按需预配，从而节省存储成本。

在电源循环时保留已预配的虚拟机

选择在电源循环时是否保留已预配的虚拟机。使用 PowerShell 参数 `New-ProvScheme CustomProperties`。此参数支持一个额外的属性 `PersistVm`，用于确定已预配的虚拟机在电源循环时是否持久存在。将 `PersistVm` 属性设置为 **true** 以在关机时保留虚拟机，或将该属性设置为 **false** 以确保虚拟机在关机时不被保留。

注意：

`PersistVm` 属性仅适用于启用了 `CleanOnBoot` 和 `UseWriteBackCache` 属性的预配方案。如果未为非持久性虚拟机指定 `PersistVm` 属性，则它们在关机时会从 Azure 环境中删除。

在以下示例中，`New-ProvScheme CustomProperties` 参数将 `PersistVm` 属性设置为 **true**：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />
```

```
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>
```

在以下示例中，`New-ProvScheme CustomProperties` 参数通过将 `PersistVM` 设置为 **true** 来保留回写缓存：

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"
```

```
 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache

 -WriteBackCacheDiskSize 127

 -WriteBackCacheMemorySize 256
```

提示：

`PersistVm` 属性决定是否保留已预配的虚拟机。`PersistOsdisk` 属性决定是否持久化操作系统磁盘。要保留已预配的虚拟机，请首先保留操作系统磁盘。请勿在未首先删除虚拟机的情况下删除操作系统磁盘。您可以使用 `PersistOsdisk` 属性，而无需指定 `PersistVm` 参数。

自定义存储类型更改失败时的开机行为

开机时，托管磁盘的存储类型可能由于 Azure 上的故障而无法更改为所需类型。在这种情况下，VM 将保持关闭状态，并向您发送故障消息。但是，您可以选择即使存储无法恢复到其配置类型也开机 VM，或者选择保持 VM 关闭。

- 如果您将自定义属性 `FailSafeStorageType` 配置为 **true**（默认设置），或者未在 `New-ProvScheme` 或 `Set-ProvScheme` 命令中指定它：
  - 开机时，VM 以不正确的存储类型开机。
  - 关机时，虚拟机以不正确的存储类型保持关机状态。
- 如果您在 `New-ProvScheme` 或 `Set-ProvScheme` 命令中将自定义属性 `FailSafeStorageType` 配置为 **false**：
  - 开机时，VM 保持关闭状态，并使用不正确的存储类型。
  - 关机时，虚拟机以不正确的存储类型保持关机状态。

要创建计算机目录：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix®*` 以加载 Citrix 特定的 PowerShell 模块。
3. 如果尚未创建，请创建身份池。

4. 在 `New-ProvScheme` 中添加自定义属性。例如：

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\Azure-
Resources-1\image.folder\abc.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\Azure-
Resources-1\ght.folder\abc.resourcegroup\abc-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\Azure-
Resources-1\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"true`" />

</CustomProperties>"
```

5. 创建计算机目录。有关如何使用远程 PowerShell SDK 创建目录的信息，请参阅 `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`。

更新现有计算机目录以包含 `FailSafeStorageType` 自定义属性。此更新不影响现有 VM。

1. 在 `Set-ProvScheme` 命令中更新自定义属性。例如：

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "

<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"false`" />

</CustomProperties>"
```

要将 Set-ProvScheme 中所做的更改应用于现有 VM，请运行带有 `-StartsNow` 和 `-DurationInMinutes -1` 参数的 `Set-ProvVMUpdateTimeWindow` 命令。

1. 运行 `Set-ProvVMUpdateTimeWindow` 命令，并使用 `-StartsNow` 和 `-DurationInMinutes -1` 参数。例如：

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

2. 重新启动 VM。

创建支持休眠的 VM

在 Azure 环境中，您可以创建支持休眠的 MCS 计算机目录。使用此功能，您可以暂停 VM，然后在用户再次登录时重新连接到 VM 的先前状态。

休眠功能适用于以下情况：

- 单会话操作系统
- 持久和非持久 VM
- 静态和随机（池化）VDI 桌面

无论 VDI 桌面是静态还是随机的，在休眠 VM 后，您都可以恢复到同一会话。

在本节中，请参阅以下内容：

- 先决条件
- 限制
- 创建和管理支持休眠的计算机目录
- 为现有支持休眠的 VM 创建计算机目录
- 检查休眠属性
- VM 的电源管理（手动和自动）

使用休眠的先决条件

要使用休眠，请确保完成以下任务：

- 在 Windows 和 Linux 的主映像上安装 Azure VM 代理。Windows 映像的页面文件可以位于临时磁盘上。在计算机目录上启用休眠时，MCS 会将页面文件位置设置为基础磁盘中的 C: 驱动器。
- MCS 会自动为生成的资源设置休眠属性。您无需配置主资源的属性来支持休眠。
- 在您的订阅中使用支持休眠的 VM 大小。
- 创建支持休眠的计算机配置文件（VM 或模板规范），以便 VM 继承休眠功能。要创建 VM，请参阅休眠入门。

> **注意：**
>
> 根据 Microsoft 的说法，您可以从 OS 磁盘部署启用休眠的 VM。此功能目前支持某些区域，并将很快适用于所有区域。有关详细信息，请参阅从 OS 磁盘部署启用休眠的 VM。
>
> 要创建模板规范，请执行以下操作：

a. 打开 Azure 门户。选择要在模板中使用的 VM 的配置。在左侧窗格中选择**导出模板**。

b. 清除**包括参数**复选框。复制上下文并将其保存为 JSON 文件，例如 `VMExportTemplate.json`。

c. 确保模板上的参数 `hibernationEnabled` 为 `true`。如果参数不是 `true`，请检查您使用的 VM 配置。您可以在模板文件中指定支持的 VM 大小。但是，您也可以在创建目录时指定计算机大小。

d. 将网络接口资源的模板添加到 JSON 文件 `VMExportTemplate.json`。这样，您就拥有了一个包含两个资源的 ARM 模板文件。

e. 选择 **Azure 门户 > 模板规范 > 导入模板 > 选择本地模板文件**以将此模板文件作为 ARM 模板规范导入。

f. 创建 ARM 模板规范后，您可以将其用作计算机配置文件。

> **注意：**
>
> 同步到 Citrix Studio 可能需要几分钟时间。

有关详细信息，请参阅 Microsoft 文档使用休眠的先决条件。

限制

- 仅支持单会话操作系统计算机目录（持久和非持久）。
- 临时 OS 磁盘和 MCS I/O 功能不支持 Azure 休眠。
- 休眠可能会在 Windows 自动更新期间失败。

有关详细信息，请参阅 Microsoft 文档。

创建和管理支持休眠的计算机目录

要创建支持休眠的 VM，可以使用以下方法创建和管理支持休眠的计算机目录：

- Web 工作室，或
- PowerShell 命令

使用 Web Studio 创建目录

1. 选择**创建计算机目录**。目录创建向导随即打开。
2. 在**计算机类型**页面上，为此目录选择**单会话操作系统**计算机类型。
3. 在**计算机管理**页面上，按如下所示选择设置：
   a. 选择“**已进行电源管理的计算机（例如，虚拟机或刀片式电脑）**”。
   b. 选择 **Citrix 机器创建服务™ (MCS)**。
4. 在“**桌面体验**”页面上，根据需要选择随机或静态桌面体验。
5. 在“**映像**”页面上，选择主映像。选中“**使用计算机配置文件**”复选框，然后选择支持休眠的计算机配置文件。单击工具提示以了解计算机配置文件是否支持休眠。

> **注意：**
>
> 如果您选择 Azure 托管的主映像，则该边栏将列出与资源属于同一区域的所有映像。

6. 在“**存储和许可证类型**”页面上，选择要用于此目录的存储和许可证。
7. 在“**虚拟机**”页面上，选择 VM 数量、VM 大小和可用区。

> **注意：**
>
> 仅显示支持休眠的计算机大小供您选择。

8. 在“**NIC**”页面上，添加要供 VM 使用的 NIC。
9. 在“**磁盘设置**”页面上，选择回写缓存磁盘的存储类型和大小。
10. 在“**资源组**”页面上，选择要预配 VM 的资源组。
11. 在“**计算机身份**”页面上，选择“**创建新的 Active Directory 帐户**”。然后，指定帐户命名方案。
12. 在“**域凭据**”页面上，单击“**输入凭据**”。输入您的域凭据以在目标 Active Directory 域中执行帐户创建。
13. 在“**摘要**”页面上，输入计算机目录的名称，然后单击“**完成**”。

MCS 计算机目录创建完成后，在目录列表中找到该目录，然后单击“**模板属性**”选项卡。参数“**休眠**”的值必须为“**支持**”。

如果要编辑计算机目录，请考虑以下限制：

- 如果当前计算机目录支持休眠，则不能：
  - 将 VM 大小更改为不支持休眠的大小。
  - 将计算机配置文件更改为不支持休眠的配置文件。
- 如果当前计算机目录不支持休眠，则不能：
  - 目前，使用 Web Studio 将计算机配置文件更改为支持休眠的配置文件。

创建用于管理现有支持休眠的 VM 的计算机目录
如果您已有支持休眠的 VM 并希望暂停和恢复它们，请创建一个计算机目录以导入这些 VM 进行电源管理。

> **注意：**
>
> 您可以创建包含支持休眠和不支持休眠的 VM 的计算机目录。但是，如果您需要与休眠相关的功能，则必须仅使用支持休眠的 VM 创建计算机目录。

> 要使用 Web Studio 为现有支持休眠的 VM 创建目录，请按照屏幕上的说明完成步骤，并注意以下关键设置：

1. 在“**计算机管理**”页面上，选择“**已进行电源管理的计算机**”，然后选择“**其他服务或技术**”作为部署计算机的方式。
2. 在“**虚拟机**”页面上，仅添加或导入支持休眠的 VM。

使用 PowerShell 命令创建计算机目录
满足所有使用休眠的要求 后，您可以使用 `New-ProvScheme` 命令创建支持休眠的计算机目录。有关如何使用远程 PowerShell SDK 创建目录的信息，请参阅 New-ProvScheme。

创建目录时，您可以使用以下 PowerShell 命令检查 VM 大小和计算机配置文件是否支持休眠：

- 对于 VM 大小，运行以下命令并检查属性 `supportsHibernation` 是否为 **True**。例如，

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder") |
select Name, AdditionalData | ConvertTo-Json
```

- 对于计算机配置文件，运行以下命令并检查属性 `supportsHibernation` 是否为 **True**。例如，

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork>
\machineprofile.folder\abc.resourcegroup")|select Name, AdditionalData|
ConvertTo-Json
```

如果要编辑计算机目录，请考虑以下限制：

- 如果当前计算机目录支持休眠，您不能：
  - 将 VM 大小更改为不支持休眠的大小
  - 将计算机配置文件更改为不支持休眠的配置文件
- 如果当前计算机目录不支持休眠，您不能：
  - 目前，使用 Web Studio 将计算机配置文件更改为支持休眠的配置文件。

有关如何使用远程 PowerShell SDK 修改目录的 VM 大小和计算机配置文件，请参阅 `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>`。

检查休眠属性

您可以使用 PowerShell 命令检查计算机目录、VM 和代理计算机的休眠属性：

- 要检查预配方案的休眠属性，请运行以下 PowerShell 命令。`HibernationEnabled` 参数必须为 `True`。

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).VMMetadata
-join "" |  ConvertFrom-Json | Select HibernationEnabled
```

- 要检查预配 VM 的休眠属性，请运行以下 PowerShell 命令。`SupportsHibernation` 参数必须为 `True`。

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json |
Select SupportsHibernation
```

- 要检查代理计算机的休眠容量，请运行以下 PowerShell 命令。**挂起**和**恢复**电源操作表示休眠功能。

```
(Get-BrokerMachine -MachineName
<YourMachineName>).SupportedPowerActions
```

支持休眠的 VM 的电源管理

您可以对支持休眠的 VM 执行以下电源管理操作：

- 从运行状态**挂起** VM
- 从挂起状态**恢复** VM
- 从挂起状态**强制关闭** VM
- 从挂起状态**强制重启** VM

有关详细信息，请参阅以下内容：

- 挂起
- 恢复

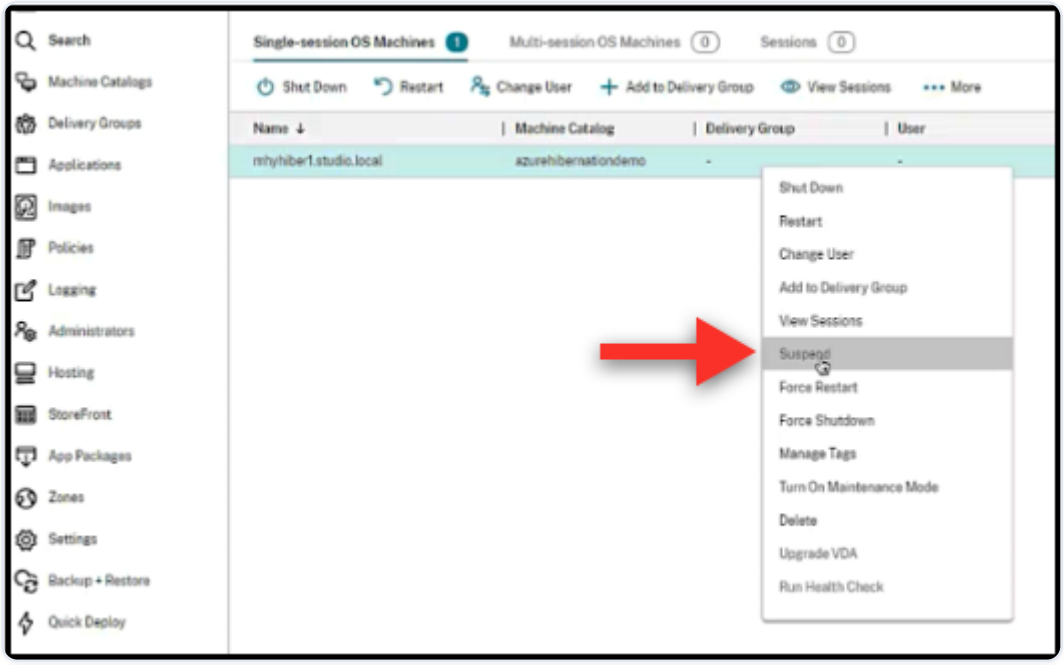
挂起

您可以通过以下方式之一挂起 VM：

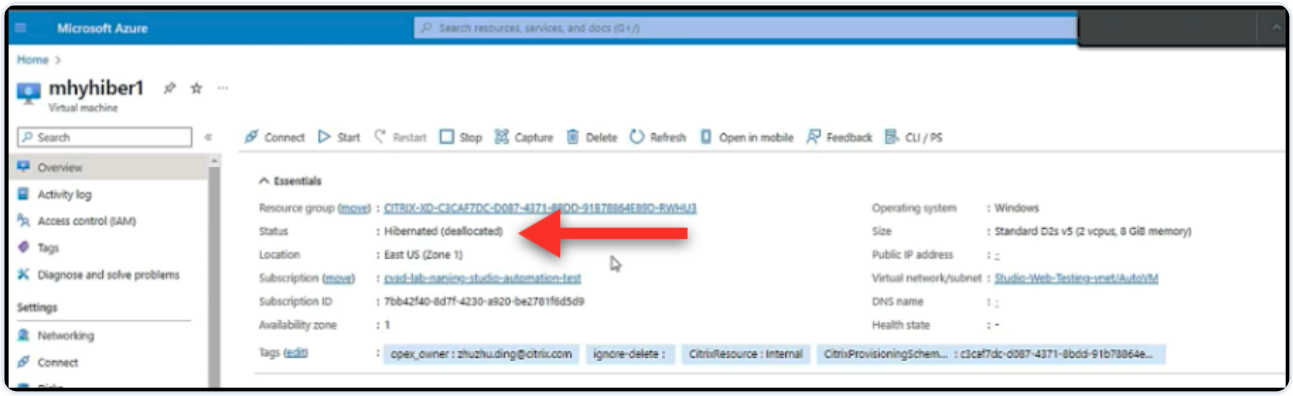
- **手动**使用 Web Studio
- 使用超时策略**自动**：有关详细信息，请参阅其他设置。

要手动挂起 VM：

1. 右键单击 VM，然后选择“**挂起**”。单击“**是**”以确认操作。“**电源状态**”从“**正在挂起**”变为“**已挂起**”。



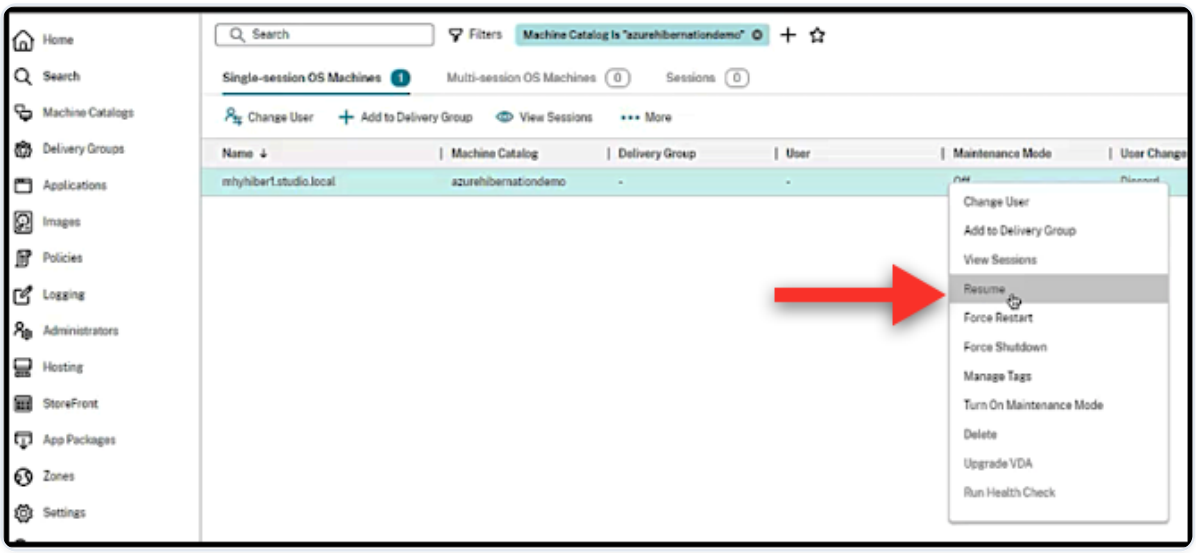
您可以在 Azure 门户中检查 VM 的状态。



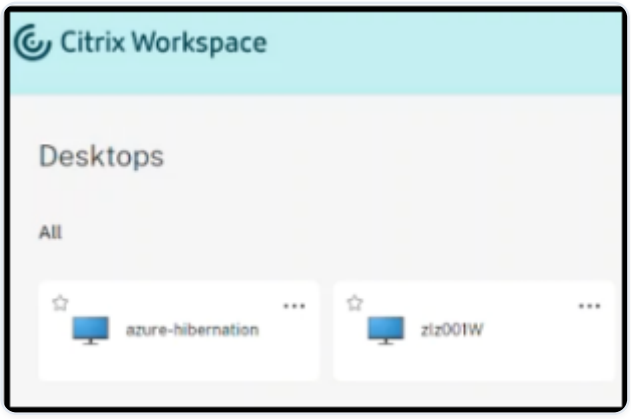
恢复

要恢复已休眠的 VM，请使用以下方法之一：

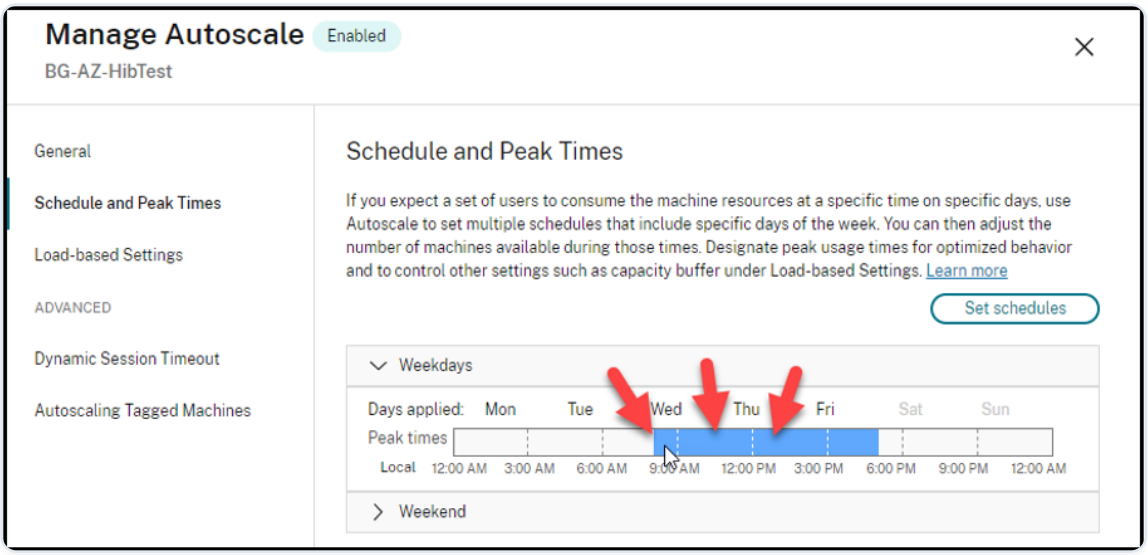
- **手动**：
  - 管理员可以使用 Web Studio 恢复 VM。



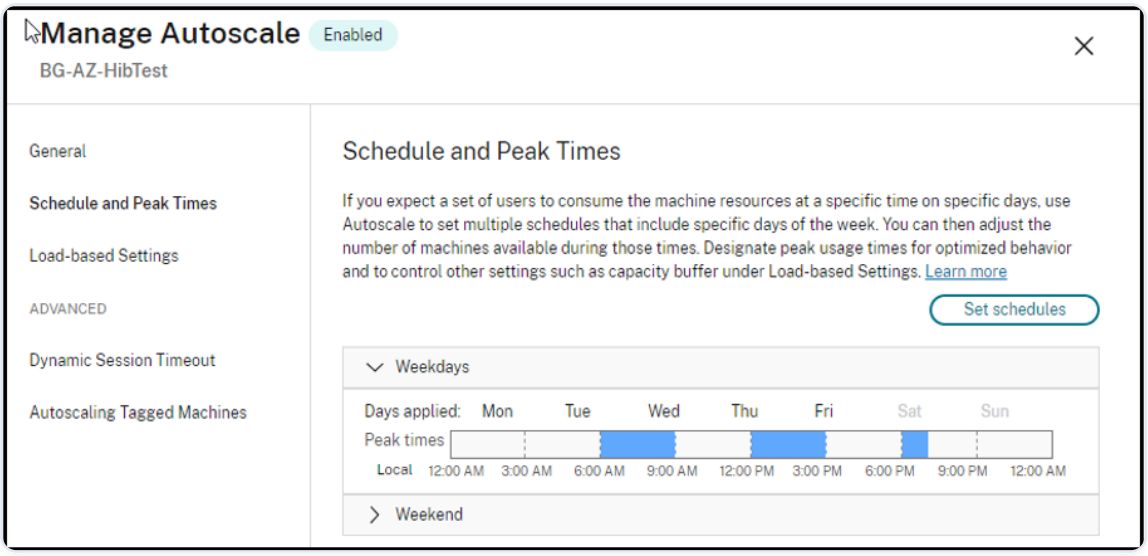
- 最终用户在单击桌面图标后，可以使用 Citrix Workspace™ 菜单启动 VM。



- **自动**：
  - 如果正确配置了高峰时段，Autoscale™ 可以自动开启已休眠的计算机。您可以通过单击时间表以 30 分钟为间隔设置高峰时段。每个蓝色框表示一个标记为高峰时段的时间段。高峰时段可以包含连续和非连续的时间段。
    - 连续时间段

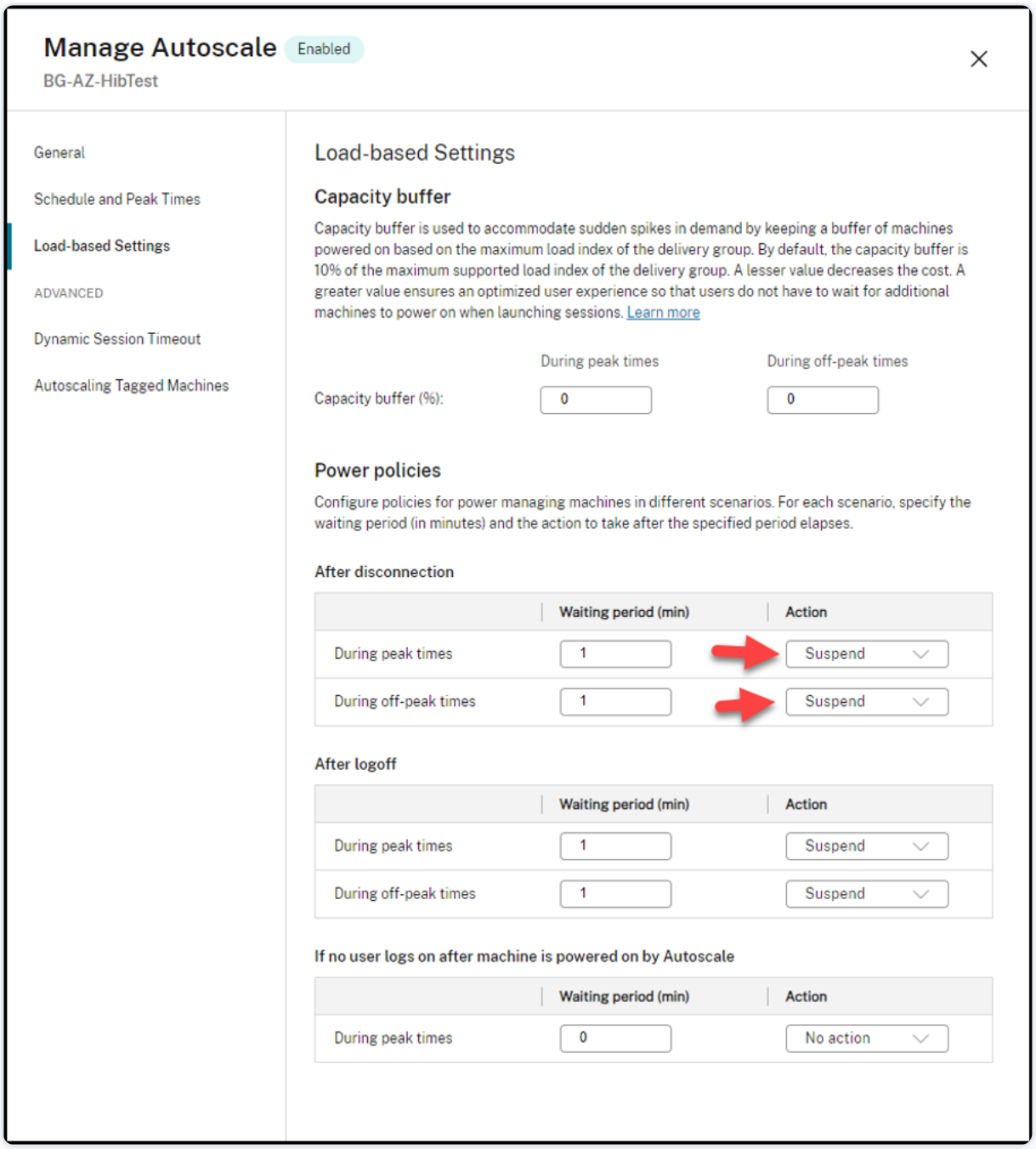


- 非连续时段



注意：

在 **管理自动缩放 > 基于负载的设置** 中，如果将 **操作** 配置为 **挂起**，请确保该交付组中的所有 VM 都具有休眠功能。否则，无法休眠的 VM 将继续运行。



获取休眠失败的警告消息

如果 MCS 预配的现有支持休眠的 VM 休眠失败，您可以使用 PowerShell 命令 `Get-ProvOperationEvent` 获取警告消息。有关 PowerShell 命令的信息，请参阅 SDK 文档 Get-ProvOperationEvent。

为此，请执行以下操作：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行 `Get-ProvOperationEvent` 以在休眠失败时获取警告消息。

```
Get-ProvOperationEvent -filter { OperationName -eq "Suspend" }
```

输出：

```
EventAdditionalData : Error code = OperationNotAllowed and Error
message = The Hibernate-Deallocate Operation cannot be performed on a
VM that has extension 'AzureHibernateExtension' in failed state. For
more information, see https://aka.ms/hibernate-resume/errors. Error
details from the extension : Enabling

                  hibernate failed. Response from the powercfg command.
Exit Code: 1. Error message:

                  Hibernation failed with the following error: The
request is not supported.



                  The following items are preventing hibernation on
this system.

                    The current Device Guard configuration has disabled
hibernation.

                    An internal system component has disabled
hibernation.

                            Hypervisor

                  Status: 409

                  ErrorCode: OperationNotAllowed



                  Content:

                  {

                    "error": {

                      "code": "OperationNotAllowed",
```

```
                    "message": "The Hibernate-Deallocate Operation
cannot be performed on a VM that has extension
'AzureHibernateExtension' in failed state. For more information, see
https://aka.ms/hibernate-resume/errors. Error details from the
extension : Enabling hibernate failed. Response from the

                powercfg command. Exit Code: 1. Error message:
\nHibernation failed with the following error: The request is not
supported.\r\r\n\r\nThe following items are preventing hibernation on
this system.\r\n\tThe current Device Guard configuration has disabled
hibernation.\r\n\tAn internal system

                component has disabled hibernation.
\r\n\t\tHypervisor"

                  }

                }

EventCategory       : Warning

EventDateTime       : 1/11/2024 4:18:31 AM

EventId             : 0

EventMessage        : Failed to suspend machine my-resource-group/my-
vm.

EventSeverity       : Important

EventSource         : AzureRmPlugin

EventState          : New

LinkedObjectType    : ProvisioningScheme

LinkedObjectUid     : 589cb600-6e65-479f-9d47-9715c4732366

OperationName       : Suspend

OperationTargetName : my-resource-group/my-vm

OperationTargetType : VirtualMachine
```

```
OperationType       : PowerManagement

Recommendation      :
```

排查休眠问题

如果您尝试同时启用休眠和受信任启动 VM 功能，但来宾操作系统配置不正确，则会收到以下错误消息。

错误代码	错误消息
OperationNotAllowed	无法对扩展“AzureHibernateExtension”处于失败状态的 VM 执行休眠-解除分配操作。有关详细信息，请参阅 `<https://aka.ms/hibernate-resume/errors/>`。扩展的错误详细信息：启用休眠失败。来自 powercfg 命令的响应。退出代码：1。错误消息：休眠失败，出现以下错误：不支持该请求。以下项阻止此系统休眠。**当前的 Device Guard 配置已禁用休眠。内部系统组件已禁用休眠**。

要解决此问题，请确保在客户机 VM 中启用了虚拟化。例如，确认在 Windows 环境中启用了 Hyper-V。根据 Microsoft Windows 限制，仅当在 VM 上启用受信任启动时，嵌套虚拟化才支持休眠。

有关警告消息的详细信息，请参阅 Microsoft 文档 排查 VM 休眠问题。

注意：

与恢复 VM 失败相关的错误消息将在未来版本中提供。

更多信息

有关 Citrix Azure 休眠的详细信息，请参阅 Citrix Tech Zone 文章。

电源管理 Oracle C3 VM（预览版）

Citrix Virtual Apps and Desktops™ 允许您对 Oracle C3 VM 进行电源管理。使用导航窗格中的“**搜索**”节点来查找要进行电源管理的计算机。

提供以下电源操作：

- 启动
- 关机
- 强制关机
- 重新启动
- 重置

> **注意：**
>
> 不支持挂起和恢复电源操作。

Red Hat OpenShift 虚拟机的电源管理

Citrix Virtual Apps and Desktops™ 允许您对 Red Hat OpenShift 虚拟机进行电源管理。使用导航窗格中的“搜索”节点来查找您要进行电源管理的计算机。

提供以下电源操作：

- 启动
- 关机
- 强制关机
- 重新启动

> **注意：**
>
> 重置、挂起和恢复电源操作不受支持。

电源管理 Nutanix AHV 虚拟机

借助 Citrix DaaS™，您可以对 Nutanix AHV 虚拟机进行电源管理。使用导航窗格中的“**搜索**”节点查找要进行电源管理的计算机。

您可以使用以下电源操作：

- 启动
- 关机
- 强制关机

- 强制重新启动
- 重新启动

> **注意：**
>
> - 重置、挂起和恢复电源操作不受支持。
> - 关机或重新启动：如果活动用户或正在运行的程序中断关机，或者操作系统需要更新，则虚拟机可能不会响应关机请求。为确保在 Windows 虚拟机上正确执行客户机关机和重新启动，请在 VDA 上应用建议的电源操作设置，例如屏幕保护程序和显示电源设置。有关详细信息，请参阅 Nutanix KB。

安全策略

本文介绍了各种受支持的云服务上的安全功能。安全功能包括：

- 安全组
- 安全启动
- 加密功能

安全组

安全组是一组安全规则，用于筛选虚拟网络中资源之间的网络流量。安全规则允许或拒绝到多种类型资源的入站网络流量或来自多种类型资源的出站网络流量。每条规则都指定以下属性：

- 名称：网络安全组中的唯一名称
- 优先级：规则按优先级顺序处理，数字越小优先级越高，因此数字较小的规则会在数字较大的规则之前处理
- 源或目标：任意、单个 IP 地址、无类别域间路由 (CIDR) 块（例如 10.0.0.0/24）、服务标签或应用程序安全组
- 协议：您为每个安全组添加规则所依据的协议
- 方向：规则是应用于入站流量还是出站流量
- 端口范围：您可以指定单个端口或端口范围
- 操作：允许或拒绝

有关支持的管理程序的更多信息，请参阅以下内容：

- AWS 中的安全组
- Microsoft Azure 中的安全组
- Google Cloud Platform 中的安全组

AWS 中的安全组

安全组充当虚拟防火墙，用于控制 VPC 中实例的流量。您可以向安全组添加规则，以允许公有子网中的实例与私有子网中的实例进行通信。您还可以将这些安全组与 VPC 中的每个实例相关联。入站规则控制到实例的传入流量，出站规则控制来自实例的传出流量。

有关映像准备期间网络设置的更多信息，请参阅映像准备期间的网络设置。

启动实例时，可以指定一个或多个安全组。要配置安全组，请参阅 配置安全组。

Microsoft Azure 中的安全组

Citrix Virtual Apps and Desktops 支持 Azure 中的网络安全组。网络安全组应与子网关联。有关详细信息，请参阅 网络安全组。

有关在映像准备期间创建的网络安全组的详细信息，请参阅 使用 Azure Resource Manager 映像创建计算机目录。

Google Cloud Platform 中的安全组

在准备计算机目录期间，会准备一个计算机映像，用作目录的主映像系统磁盘。在此过程中，磁盘会临时附加到虚拟机。此虚拟机必须在隔离环境中运行，以防止所有入站和出站网络流量。这是通过一对拒绝所有防火墙规则实现的。有关详细信息，请参阅 防火墙规则。

安全启动和 vTPM

安全启动是统一可扩展固件接口 (UEFI) 的一项功能，负责启动系统。它确保在启动过程中只加载受信任的软件。

可信平台模块 (TPM) 是一种硬件芯片，可为加密密钥和其他敏感数据提供安全存储。虚拟可信平台模块 (vTPM) 执行与 TPM 相同的功能，但它在软件中执行加密协处理器功能。尽管 TPM 可以增强安全性，但它不是安全启动的要求。

有关支持的管理程序的更多信息，请参阅以下内容：

- AWS 中的安全启动和 NitroTPM
- Google Cloud Platform 中的安全启动和 vTPM
- Microsoft Azure 中的安全启动和 vTPM
- Nutanix Prism Central 中的安全启动和 vTPM

- VMware 中的 vTPM
- XenServer® 的安全启动和 vTPM

AWS 中的安全启动和 NitroTPM

在 AWS 环境中，您可以选择启用 NitroTPM 和/或 UEFI 安全启动的主映像 (AMI)。因此，目录中预配的 VM 也启用了 NitroTPM 和/或 UEFI 安全启动。此实施可确保 VM 的安全性和可信度。有关 NitroTPM 和 UEFI 安全启动的更多信息，请参阅 Amazon 文档。有关创建启用 NitroTPM 和 UEFI 安全启动的目录的信息，请参阅 为 VM 实例启用 NitroTPM 和 UEFI 安全启动。

Google Cloud Platform 中的安全启动和 vTPM

您可以在 Google Cloud Platform (GCP) 上预配受保护的虚拟机。受保护的 VM 的可验证完整性通过使用以下功能实现：

- 安全启动
- 启用 vTPM 的度量启动
- 完整性监控

有关使用 PowerShell 创建包含受保护 VM 的目录的详细信息，请参阅使用 PowerShell 创建包含受保护 VM 的目录。

> **注意：**
>
> 如果在主映像上安装 Windows 11，则必须在主映像创建过程中启用 vTPM。此外，如果使用计算机配置文件创建目录，则必须在计算机配置文件源（VM 或实例模板）上启用 vTPM。有关在独占租户节点上创建 Windows 11 VM 的信息，请参阅在独占租户节点上创建 Windows 11 VM。

Microsoft Azure 中的安全启动和 vTPM

在 Azure 环境中，您可以创建启用可信启动的计算机目录。Azure 提供可信启动作为一种无缝方式来提高第 2 代 VM 的安全性。可信启动可防止高级和持久性攻击技术。要启用可信启动，请使用基于计算机配置文件的目录配置。可信启动的核心是 VM 的安全启动。可信启动还使用 vTPM 执行云的远程证明。这用于平台健康检查和做出基于信任的决策。您可以单独启用安全启动和 vTPM。 有关创建具有可信启动的计算机目录的更多信息，请参阅 具有可信启动的计算机目录。

Nutanix Prism Central 中的安全启动和 vTPM

MCS 支持使用 Nutanix Prism Central 创建包含 vTPM、UEFI 和安全启动的计算机目录。您可以选择启用 vTPM 和 UEFI 安全启动的主映像（模板）。

在 Nutanix Prism Central 中，UEFI 安全启动不需要 vTPM。但是，要将 vTPM 链接到 VM，VM 必须通过 UEFI 启动，无论是否启用安全启动。

此外，可以从 Nutanix Prism Central 导入启用 vTPM、UEFI 和安全启动的 VM，并由 Citrix Virtual Apps and Desktops 进行电源管理。

Nutanix 提供对 vTPM 和 UEFI 安全启动的支持。请参阅：

- AHV 上的 vTPM（虚拟可信平台模块）支持。
- VM 的安全启动支持
- 使用虚拟可信平台模块保护 AHV VM

VMware 中的 vTPM

MCS 支持创建包含 vTPM 的计算机目录。如果主映像上安装了 Windows 11，则要求为主映像启用 vTPM。如果使用基于计算机配置文件的配置并启用了 vTPM，则目录中的 VM 将从 VM 模板继承相同的 vTPM 内容。如果未使用计算机配置文件且主映像启用了 vTPM，则目录中的 VM 将具有空白 vTPM。有关更多信息，请参阅 使用计算机配置文件创建计算机目录。

XenServer® 的安全启动和 vTPM

XenServer 在其某些受支持的 VM 操作系统上提供 UEFI 安全启动。安全启动可防止未签名、签名不正确或已修改的二进制文件在启动期间运行。在强制执行安全启动的 UEFI 启用 VM 上，所有驱动程序都必须经过签名。有关详细信息，请参阅来宾 UEFI 和安全启动。

在 XenServer 8 中，UEFI 安全启动不需要 vTPM。但是，要将 vTPM 链接到 VM，该 VM 必须通过 UEFI 启动，无论是否启用安全启动。Windows 11 VM 需要链接的 vTPM，并且在从提供的模板创建 Windows 11 VM 时会自动创建。对于其他操作系统，vTPM 是可选的。有关详细信息，请参阅 vTPM。

加密功能

加密功能可保护虚拟机内容，使其免受共享虚拟机主机上恶意来宾的攻击以及管理主机上所有虚拟机的管理程序控制软件发起的攻击。

有关支持的云服务的更多信息，请参阅以下内容：

- AWS 中的加密功能
- Google Cloud Platform 中的加密功能
- Microsoft Azure 中的加密功能

AWS 中的加密功能

本节介绍 AWS 虚拟化环境中的加密功能。

自动加密

您可以为账户中创建的新 Amazon EBS 卷和快照副本启用自动加密。有关详细信息，请参阅自动加密。

Google Cloud Platform 中的加密功能

本节介绍 Google Cloud Platform (GCP) 虚拟化环境中的加密功能。

如果您需要对密钥操作进行比 Google 管理的加密密钥所允许的更多控制，则可以使用客户管理的加密密钥。使用客户管理的加密密钥时，对象在存储到存储桶中时会由 Cloud Storage 使用该密钥进行加密，并在对象提供给请求者时由 Cloud Storage 自动解密。有关详细信息，请参阅客户管理的加密密钥。

您可以将客户管理的加密密钥 (CMEK) 用于 MCS 目录。有关详细信息，请参阅使用客户管理的加密密钥 (CMEK)。

Microsoft Azure 中的加密功能

本节介绍 Azure 虚拟化环境中的加密功能。

AZURE 服务器端加密

大多数 Azure 托管磁盘都使用 Azure 存储加密进行加密，该加密使用服务器端加密 (SSE) 来保护您的数据并帮助您履行安全和合规性承诺。Citrix Virtual Apps and Desktops 通过 Azure Key Vault 支持 Azure 托管磁盘的客户管理的加密密钥。有关详细信息，请参阅Azure 服务器端加密。

AZURE 主机端磁盘加密

您可以创建具有主机端加密功能的 MCS 计算机目录。

此加密方法不通过 Azure 存储加密数据。托管 VM 的服务器加密数据，然后加密的数据流经 Azure 存储服务器。因此，这种加密方法对数据进行端到端加密。

有关创建具有主机端加密功能的 MCS 计算机目录的详细信息，请参阅 Azure 主机端磁盘加密。

AZURE 双重加密

双重加密是平台端加密（默认）和客户管理加密 (CMEK)。因此，如果您是高度安全敏感的客户，担心与任何加密算法、实施或受损密钥相关的风险，则可以选择此双重加密。持久 OS 和数据磁盘、快照和映像都使用双重加密进行静态加密。有关详细信息，请参阅 托管磁盘上的双重加密。

AZURE 机密 VM

Azure 机密计算 VM 可确保您的虚拟桌面在内存中加密并在使用中受到保护。

您可以使用 MCS 创建包含 Azure 机密 VM 的目录。您必须使用计算机配置文件工作流来创建此类目录。您可以将 VM 和 ARM 模板规范都用作计算机配置文件输入。

有关详细信息，请参阅 Azure 机密 VM。

服务窗口

服务窗口功能提供了一种调度和自动化 MCS 预配 VM 操作的功能。此功能目前支持各种操作，例如重置操作系统磁盘和硬件配置更改。您可以安排这些操作，稍后返回验证完成情况，而无需手动执行更新。

您可以为特定的 VM 列表或整个计算机目录安排操作。每个操作都在指定的时间运行。可以为同一 VM 安排多个操作。但是，您不能为单个 VM 安排多个硬件更新。

您还可以：

- 添加服务窗口的描述。
- 提供详细消息，以便在操作运行时显示给任何已登录的用户。
- 指定任务元数据在完成后应保留多少天。
- 配置在强制执行操作之前，为已登录用户保存工作而授予的缓冲分钟数。

优点

改进的用户体验和连续性

- **优雅的会话处理**：您可以定义专业的通知，以便在 VM 关闭电源之前保存工作，而不是突然断开连接。
- **计划停机时间**：您可以将繁重的更新任务移至非高峰时段（例如，凌晨 2:00），而无需您在该时间手动登录。
- **经济高效的硬件更新**：使用服务窗口更新硬件可为大型实施节省大量成本。此功能会自动分析 VM 是否需要重新启动才能应用设置。因此，通过避免不必要的重新启动，服务窗口可最大程度地降低这些费用。

高级硬件灵活性

- **更新硬件配置**：使用服务窗口安排硬件更新。系统智能地管理更新流程，检查是否需要重新启动并处理会话注销，确保您的目录能够满足新的资源需求，而无需手动监督。
- **灵活的 SKU 重新配置**：轻松更新 SKU，这以前需要手动重新创建目录。
- **现有 VM 的休眠支持**：克服了“临时磁盘”的限制。服务窗口允许 MCSIO 驱动程序将页面文件重新定位到 C: 驱动器，并为已部署的 VM 启用休眠属性。

重要注意事项

- **用户通知**：已登录用户会收到有关服务窗口操作的初始警报，确保他们有足够的时间保存工作。通知期结束后，计算机将自动关机以执行操作。

服务窗口操作

服务窗口目前支持操作系统磁盘重置、修复现有 MCS 预配目录的 Active Directory 帐户、为现有 MCS 预配目录启用 Entra 混合加入以及硬件配置更改。这些操作可以使用 Web Studio 或 PowerShell 执行。

Web Studio：目前仅支持 Azure 环境。有关指导，请参阅特定的管理程序文章。

PowerShell 命令：本文概述了通用命令，而详细的、特定于管理程序的脚本可在我们的 GitHub 页面 `<https://github.com/citrix/citrix-mcs-sdk-samples/>` 上找到。

重置操作系统磁盘

操作系统磁盘重置可以使用 PowerShell 命令 `New-ProvMaintenanceCycle` 完成。该命令为整个目录或特定 VM 创建新的服务窗口。周期从您在 `ScheduledStartTimeInUTC` 中指定的时间开始。您还需要提供 `MaxDurationInMinutes`，它表示服务窗口可以运行的最长时间。

示例：重置特定 VM 的操作系统磁盘

```
New-ProvMaintenanceCycle -Operation ResetOSDisk
-MaintenanceCycleDescription "Resetting Boot Disk" -StartsNow
-MaxDurationInMinutes 100 -ProvisioningSchemeName CVC -PurgeDBAfterInDays
1 -SessionWarningTimeInMinutes 15 -SessionWarningLogOffTitle "Scheduled
Maintenance" -SessionWarningLogOffMessage "There is a scheduled
maintenance coming up and involves turning off the machine, please save
your work and log out, Thank You" -VMName VDA02,VDA03
```

示例：重置整个目录的操作系统磁盘

```
New-ProvMaintenanceCycle -Operation ResetOSDisk
-MaintenanceCycleDescription "Resetting Boot Disk" -StartsNow
-MaxDurationInMinutes 100 -ProvisioningSchemeName CVC -PurgeDBAfterInDays
1 -SessionWarningTimeInMinutes 15 -SessionWarningLogOffTitle "Scheduled
Maintenance" -SessionWarningLogOffMessage "There is a scheduled
maintenance coming up and involves turning off the machine, please save
your work and log out, Thank You" -AllVMs
```

更新硬件设置

使用服务窗口安排硬件更新，从而完全控制更改何时生效。您可以选择仅针对新创建的 VM、整个目录（新 VM 和现有 VM）或根据需要针对特定 VM。

- 要更新新 VM 或整个目录的硬件设置，请选择一个预配方案版本并运行 PowerShell 命令 `New-ProvSchemeHardwareUpdate`。您可以将先前创建的预配方案版本应用于 VM。您还可以在具有临时磁盘的 VM 上启用休眠。
- 要更新特定 VM 的硬件设置，请选择一个 VM 配置版本并运行 PowerShell 命令 `New-ProvVmHardwareUpdate`。

重要注意事项

- 在安排硬件更新后添加到目录的新计算机将继续使用旧规范创建，直到应用新规范的指定 UTC 时间。
- 在创建服务窗口期间，单个验证失败会阻止创建周期并返回错误消息。
- 要启用休眠，请考虑以下事项：
  - VDA 版本必须高于 2503。
  - 必须安装机器创建服务 I/O (MCSIO)。
  - 计算机配置文件必须支持休眠。
  - VM SKU 和操作系统必须支持休眠。
  - 如果启用了 VBS，则还必须启用 Hyper-V。嵌套虚拟化要求 VM 上启用受信任启动。
  - 可用操作系统磁盘大小必须大于 VM 的内存大小。

在整个计算机目录或新 VM 上安排硬件更新

1. 运行 `New-ProvSchemeVersion` 以创建具有更新硬件设置的新预配方案版本。有关详细信息，请参阅 SDK 文档。
2. 运行 PowerShell 命令 `New-ProvSchemeHardwareUpdate` 以安排服务窗口进行硬件更新，如预配方案版本中指定的那样。

示例：计算机目录中的 `AllVMs`（新的和现有的）被考虑进行更新：

```
New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 4
-MaintenanceCycleDescription "Updating RAM and CPU Count to 8GB and 4"
-StartsNow -MaxDurationInMinutes 100 -ProvisioningSchemeName CVC
-PurgeDBAfterInDays 1 -SessionWarningTimeInMinutes 15
-SessionWarningLogOffTitle "Scheduled Maintenance"
-SessionWarningLogOffMessage "There is a scheduled maintenance coming up
```

```
and involves turning off the machine, please save your work and log out,
Thank You" -AllVMs
```

示例：计算机目录中的 `NewVMsOnly`（新的和现有的）被考虑进行更新：

```
New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 4
-MaintenanceCycleDescription "Updating RAM and CPU Count to 8GB and 4"
-StartsNow -MaxDurationInMinutes 100 -ProvisioningSchemeName CVC
-PurgeDBAfterInDays 1 -SessionWarningTimeInMinutes 15
-SessionWarningLogOffTitle "Scheduled Maintenance"
-SessionWarningLogOffMessage "There is a scheduled maintenance coming up
and involves turning off the machine, please save your work and log out,
Thank You" -NewVMsOnly
```

运行 `Get-ProvSchemeHardwareUpdate` 以检索与硬件方案更新关联的服务窗口对象。示例：

```
Get-ProvSchemeHardwareUpdate -MaintenanceCycleId xxxx-xxxx-yyyy-zzzz
```

在特定 VM 上安排硬件更新

1. 运行 `New-ProvVmConfiguration` 以创建新的预配 VM 配置。有关详细信息，请参阅 SDK 文档。
2. 运行 PowerShell 命令 `New-ProvVmHardwareUpdate` 以根据 VM 配置版本中的指定计划硬件更新的服务窗口。

注意：

对于每个 VM，任何个性化设置（VM 配置版本）始终优先于预配方案版本中定义的规范。如果 VM 上未对特定设置进行个性化设置，则其值将从关联的预配方案版本继承。

示例：

```
New-ProvVmHardwareUpdate -ProvVmConfigurationVersion 4 -StartsNow
-MaxDurationInMinutes 100 -ProvisioningSchemeName CVC -VMName AbcTest01
```

运行 `Get-ProvVmHardwareUpdate` 以检索与硬件 VM 更新关联的服务窗口对象。示例：

```
Get-ProvVmHardwareUpdate -MaintenanceCycleId xxxx-xxxx-yyyy-zzzz
```

您还可以使用 `Remove-ProvVmConfiguration` 命令删除用于创建预配 VM 版本的个性化设置。示例：

```
Remove-ProvVmConfiguration -Version 2 -VMName AbcTest01
```

修复现有目录的 AD 帐户

您可以使用服务窗口修复现有本地 AD 域加入和 Microsoft Entra 混合加入的 MCS 计算机目录的 Active Directory (AD) 计算机帐户。当 VM 失去域信任时，此功能非常有用。此功能适用于持久和非持久 MCS 计算机目录。

要修复现有 MCS 计算机目录的 AD 帐户，可以使用 PowerShell 命令完成以下步骤：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 通过以下任一方式运行 `New-ProvIdentityUpdate` 命令：
   - 按名称修复特定 VM 的 AD 帐户：

     ```
     New-ProvIdentityUpdate -MaintenanceCycleDescription 'repair AD
     account' -Operation RepairADAccount -MaxDurationInMinutes 60
     -ProvisioningSchemeName <catalog-name> -VMName @("vm-1", "vm-2")
     -StartsNow
     ```

   - 要将操作安排在将来某个时间而不是立即开始：

     ```
     New-ProvIdentityUpdate -MaintenanceCycleDescription 'repair AD
     account' -Operation RepairADAccount -MaxDurationInMinutes 60
     -ProvisioningSchemeName <catalog-name> -AllVMs
     -ScheduledStartTimeInUTC "2026-04-01T02:00:00Z"
     ```

4. 运行 `Get-ProvMaintenanceCycle` 以检查维护周期的状态。

有关详细信息，请参阅 Citrix PowerShell SDK

注意：

- 此功能仅适用于本地 Active Directory 域加入和 Microsoft Entra 混合加入的 MCS 计算机目录。它不支持 Entra ID 域加入和非域加入的计算机。
- 预配方案的身份池必须具有本地 Active Directory 服务帐户，该帐户具有足够的权限来重置域中计算机帐户的密码。

为现有 MCS 预配的目录启用 Entra 混合加入

您现在可以使用服务窗口将现有已加入本地 Active Directory 的 MCS 计算机目录转换为 Microsoft Entra 混合加入目录。此功能适用于持久性和非持久性 MCS 计算机目录。

要为现有 MCS 计算机目录启用 Entra 混合加入，可以使用 PowerShell 命令完成以下步骤：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 通过以下任一方式运行 `New-ProvIdentityUpdate` 命令：

   - 立即为目录中的所有 VM 启用 Entra 混合加入：

     ```
     New-ProvIdentityUpdate -MaintenanceCycleDescription 'enable Entra
     hybrid join' -Operation MigrateActiveDirectoryToEntraHybridJoin
     -MaxDurationInMinutes 60 -ProvisioningSchemeName <catalog-name>
     -AllVMs -StartsNow
     ```

   - 按名称为特定 VM 启用 Entra 混合加入：

     ```
     New-ProvIdentityUpdate -MaintenanceCycleDescription 'enable Entra
     hybrid join' -Operation MigrateActiveDirectoryToEntraHybridJoin
     -MaxDurationInMinutes 60 -ProvisioningSchemeName <catalog-name>
     -VMName @("vm-1", "vm-2") -StartsNow
     ```

   - 启用 Entra 混合加入并为新 VM 指定目标 OU：

     ```
     New-ProvIdentityUpdate -MaintenanceCycleDescription 'enable Entra
     hybrid join' -Operation MigrateActiveDirectoryToEntraHybridJoin
     -MaxDurationInMinutes 60 -ProvisioningSchemeName <catalog-name>
     -AllVMs -StartsNow -OU "OU=SyncedDevices,DC=example,DC=com"
     ```

   - 安排操作在将来某个时间执行，而不是立即开始：

```
New-ProvIdentityUpdate -MaintenanceCycleDescription 'enable Entra
hybrid join' -Operation MigrateActiveDirectoryToEntraHybridJoin
-MaxDurationInMinutes 60 -ProvisioningSchemeName <catalog-name>
-AllVMs -ScheduledStartTimeInUTC "2026-04-01T02:00:00Z"
```

4. 运行 `Get-ProvMaintenanceCycle` 以检查维护周期的状态。

有关详细信息，请参阅 (https://developer-docs.citrix.com/zh-cn/citrix-virtual-apps-desktops-sdk/2607 LTSR/)

注意：

- 为确保目录正常工作，必须将目录中所有现有虚拟机转换为 Microsoft Entra 混合加入。
- 此功能不支持共享身份池的 MCS 预配目录。
- 现有预配方案的基础映像必须安装 VDA 版本 2212 或更高版本，请参阅 Microsoft Entra 混合加入的要求。
- 预配方案的身份池必须具有本地 Active Directory 服务帐户，该帐户具有在域中设置 userCertificate 属性的权限。
- 确保包含计算机帐户的 OU 配置为通过 Microsoft Entra Connect 同步到 Entra ID。您有两个选项：
  - 配置 Azure AD Connect 以将设备从原始 OU 同步到 Entra ID。
  - 手动将现有计算机帐户移动到已配置 Azure AD Connect 同步的 OU 中。

与服务窗口相关的其他 PowerShell 命令

- `Get-ProvMaintenanceCycle`：检索所有服务窗口的信息。示例：

```
Get-ProvMaintenanceCycle -MaintenanceCycleId
10073b8e-7e94-4527-8580-0e448eae0ad1
```

- `Get-ProvMaintenanceCycleVM`：检索单个 VM 的每个服务窗口操作的信息及其状态。示例：

```
Get-ProvMaintenanceCycleVM -MaintenanceOperation HardwareUpdate
-VirtualMachineSid 42263076-44ae-1ff9-f58b-62d57ddf8db5
```

各种服务窗口状态为：

- 正在运行
- 失败
- 已完成
- 正在取消
- 已取消
- 未处理
- 待处理
- 未完成
- 已修复
- 正在恢复

- `Remove-ProvMaintenanceCycle`: 当服务窗口未激活时，移除服务窗口。示例：

```
Remove-ProvMaintenanceCycle -MaintenanceCycleId
867af1ba-5b72-402e-9dc3-033298248f8e
```

- `Cancel-ProvMaintenanceCycle`: 如果操作尚未由 MCS 在 VM 上启动，则此 PowerShell 命令会取消该操作。MCS 不会取消当前正在 VM 上运行的操作。示例：

```
Cancel-ProvMaintenanceCycle -MaintenanceCycleId
867af1ba-5b72-402e-9dc3-033298248f8e
```

- `Restart-ProvMaintenanceCycle`: 如果服务窗口因外部原因（例如虚拟机管理程序关闭或时间不足）而失败或未完成，此命令有助于重新启动周期并处理任何失败或未处理的作业。示例：

```
Restart-ProvMaintenanceCycle -MaintenanceCycleId
4f363b78-458a-403a-82e5-7fcc6caa498b -ScheduledStartTimeInUTC "June
19th 2024, 6AM" -MaxAllocatedDurationInMinutes 400
```

- `Update-ProvMaintenanceCycle`: 如果服务窗口已计划但尚未启动，此命令会更改某些参数。

示例：更新最大持续时间：

```
Update-ProvMaintenanceCycle -MaintenanceCycleId
4f363b78-458a-403a-82e5-7fcc6caa498b -MaxDurationInMinutes 100
```

示例：更新预配方案的 VM：

```
Update-ProvMaintenanceCycle -MaintenanceCycleId
4f363b78-458a-403a-82e5-7fcc6caa498b -ProvisioningSchemeUid
867af1ba-5b72-402e-9dc3-033298248f8e -VMName ncn01,ncn02
```

下一步操作

有关使用 Web Studio 在 Azure 中管理服务窗口操作的信息，请参阅 Azure 中的服务窗口操作。

Azure 中的服务窗口操作

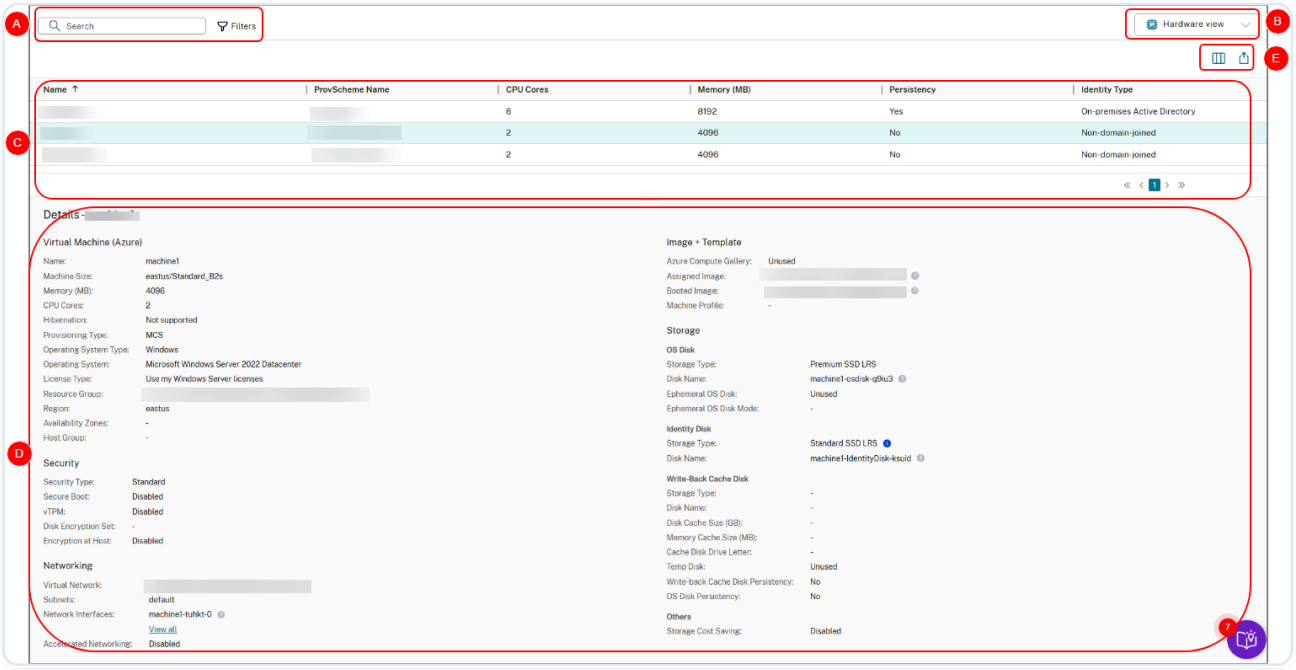
本文介绍如何在 Azure 环境中使用 Web Studio 执行服务窗口操作。

服务窗口目前支持操作系统磁盘重置和硬件配置更改。

使用“**搜索**”和“**计算机目录**”节点中的“**硬件视图**”来更新硬件设置和重置操作系统磁盘。

搜索节点中的硬件视图

“**搜索**”节点中的硬件视图显示 MCS 预配的 VM 及其关键属性，包括计算机安全设置、网络详细信息、映像和计算机配置文件详细信息。



标注	区域	描述
A	搜索栏	提供快速搜索和基于筛选器的搜索，允许您定义复杂的搜索条件。有关详细信息，请参阅 搜索计算机。**提示：** 使用筛选器可根据特定属性快速缩小计算机范围。例如，使用“**身份类型 = Microsoft Entra 已加入**”可查看所有 Microsoft Entra 已加入的计算机。
B	切换到默认视图	从硬件视图切换到默认视图。
C	主视图	显示您的 MCS 预配计算机及其关键属性。您可以通过选择“**要显示的列**”图标来自定义视图。有关可用列的更多信息，请参阅计算机列。
D	详细信息窗格	显示所选计算机的详细信息。
E	列表级操作	显示可对整个显示列表执行的操作: • **导出**图标：将主视图中显示的计算机列表导出到 CSV 文件。 • **要显示的列**图标：自定义列表的主视图。

参考：计算机列

此表列出了硬件视图中的所有列及其说明。

列	描述
名称	计算机的 DNS 主机名。
预配方案名称	用于预配计算机的预配方案的名称。
CPU 核心数	分配给计算机的 CPU 核心数。
内存 (MB)	分配给计算机的内存量 (MB)。
持久性	指示计算机的磁盘和数据是否在重新启动后仍然保留。
身份类型	计算机的身份类型。
待处理的映像更新	指示计算机的 VM 映像是否已过时，以及是否应在计算机下次重新启动时更新为新映像。
上次启动时间 (UTC)	计算机上次启动的日期和时间 (UTC)。
使用 WBC	指示计算机是否配置了 WBC（也称为 MCSIO）。
WBC 磁盘大小 (GB)	计算机的 MCSIO 磁盘缓存大小。
WBC 内存大小 (MB)	计算机的 MCSIO 内存缓存大小。
身份提供程序	计算机的身份提供程序。
激活类型	仅适用于 Windows VDA。计算机的 Windows 许可证激活类型。值包括：不支持的 VDA、密钥管理服务、多重激活密钥和无效。

更新 VM 的硬件设置

此功能提供了一种集中式方法，可使用服务窗口管理和应用对 VM 硬件设置（例如存储、许可证和 NIC）的更改。

限制

- 目前仅支持 Azure MCS 持久性 VM。

- 不支持快速部署目录 VM。
- 所有 VM 都必须属于同一目录。
- 为避免潜在问题，如果执行以下操作，请将 VDA 升级到版本 2503 或更高版本：
  - 为使用临时磁盘的现有 VM 启用休眠。
  - 更改带临时磁盘的 Azure SKU 和不带临时磁盘的 Azure SKU 之间的 VM 大小。

更新单个 VM 的硬件设置

1. 导航到“**搜索**”节点。切换到“**硬件视图**”。右键单击要更新的 VM，然后选择“**更新硬件**”。
2. 在“**更新硬件**”页面上，单击“**创建版本**”。仅配置要更改的设置。没有默认设置。
3. 导航到“**摘要**”页面，然后单击“**完成**”。
4. 选择“**计划**”或“**仅保存版本**”以确认何时将更改应用于所选 VM。
   - 如果选择“**计划**”，您将被重定向到“**应用于 VM**”页面。配置计划时间和信息，然后单击“**保存**”。将创建一个带有计划的新硬件版本。VM 将在计划完成后更新。
   - 如果选择“**仅保存版本**”，系统将创建一个新的硬件版本，而不会立即将更改应用于所选 VM。

> **注意：**
>
> 新创建的硬件版本继承了上一版本的更改。
>
> 即使您保存硬件更改而未安排应用时间，您仍然可以将其应用于 VM。

1. 导航到“**搜索**”节点。切换到“**硬件视图**”。右键单击 VM，然后选择“**更新硬件**”。
2. 在“**更新硬件**”页面上，选择一个版本。单击“**应用于 VM**”以创建计划。VM 将在计划完成后更新。

更新多个 VM 的硬件设置

1. 导航到“**搜索**”节点。切换到“**硬件视图**”。选择多个 VM，右键单击，然后选择“**更新硬件**”。
2. 在“**创建硬件版本**”向导中，没有默认设置。仅配置您要更改的设置。
3. 在“**计划**”页面上配置计划。
4. 导航到“**摘要**”页面。完成创建工作流程。
5. 创建后，您可以右键单击每个 VM 并选择“**更新硬件**”以查看版本详细信息。

管理单个 VM 的硬件版本

您可以删除硬件版本、取消计划并清除单个 VM 的自定义设置。

- **删除硬件版本**：在“**更新硬件**”页面上，选择一个或多个版本，然后单击“**删除**”以删除版本。
- **取消计划**：在“**更新硬件**”页面上，如果要取消尚未开始的计划，请在“**计划**”状态列中单击“**取消**”以取消它。
- **清除自定义设置**：在“**更新硬件**”页面上，如果要创建或应用一个删除所有自定义硬件设置的版本，请单击“**清除自定义设置**”。要创建版本并安排其应用，请选择“**计划**”。要创建版本而不应用它，请选择“**仅保存版本**”。

重置操作系统磁盘

此功能提供了一种使用服务窗口重置一个或多个 VM 的操作系统磁盘的方法。

限制

- 目前，仅支持 Azure MCS 持久性 VM。
- 不支持快速部署目录 VM。
- 所有 VM 必须属于同一目录。

重置单个或多个 VM 的操作系统磁盘

1. 导航到“**搜索**”节点。切换到“**硬件视图**”。右键单击要重置操作系统磁盘的一个或多个 VM，然后选择“**重置操作系统磁盘**”（如果可用）。
2. 选择立即重置或稍后安排。

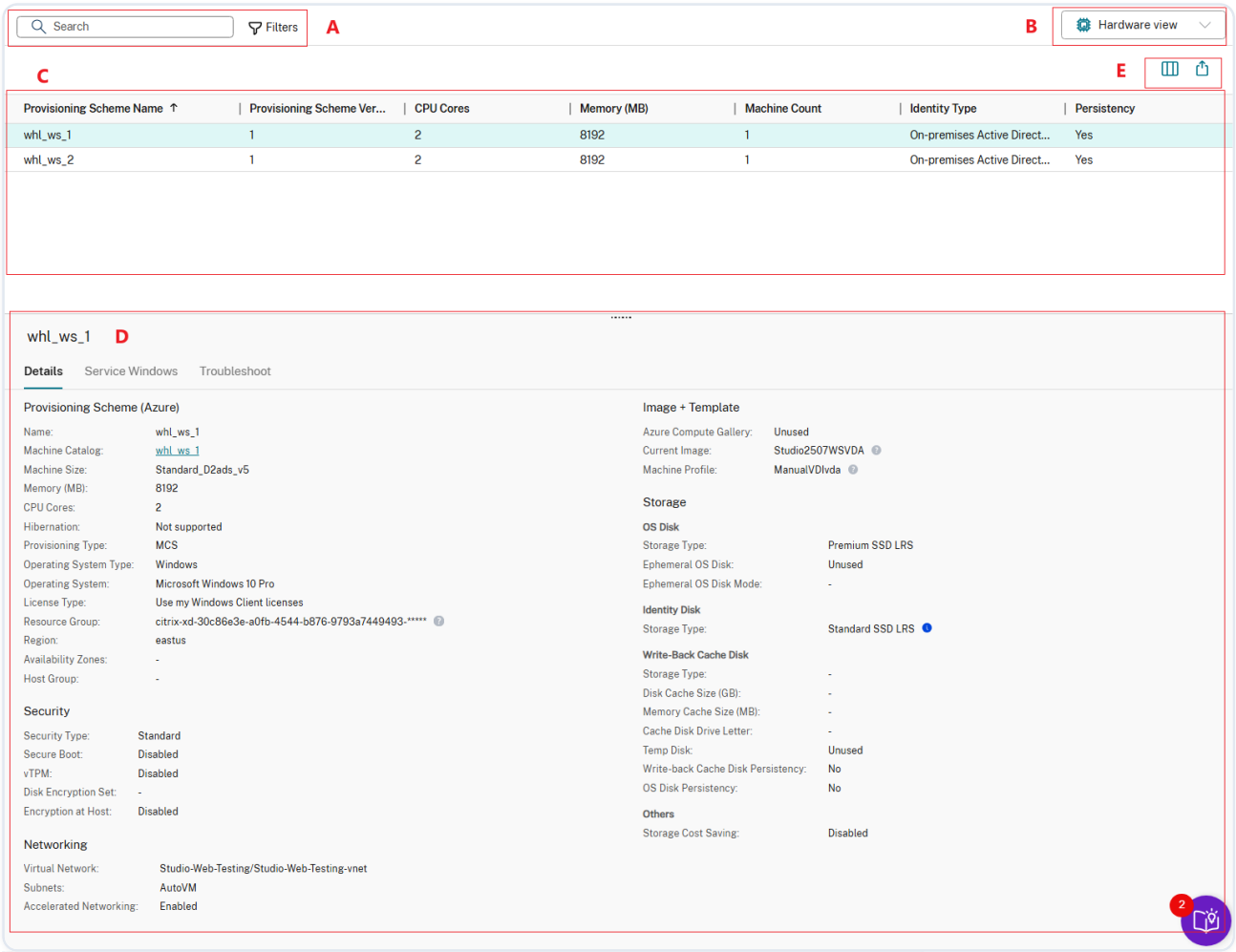
监视 VM 的任务状态

要检查重置操作系统磁盘是否成功应用：

1. 选择 VM。
2. 导航到“**详细信息 > 服务窗口**”选项卡，然后查看“**状态**”列。
3. 单击“任务 ID”以访问“**任务中心**”。此中心提供详细的任务进度和结果。请参阅在任务中心监视和管理任务。

计算机目录节点中的硬件视图

“**计算机目录**”节点中的“**硬件视图**”显示您的预配方案及其关键属性，包括安全设置、网络详细信息、映像和计算机配置文件详细信息。



标注	区域	描述
A	搜索栏	提供快速搜索和基于筛选器的搜索，允许您定义复杂的搜索条件。
B	硬件视图下拉菜单	选择以从“**硬件视图**”切换到“**默认视图**”。
C	主视图	显示您的预配方案及其关键属性。您可以通过选择“要显示的列”图标来自定义视图。有关可用列的更多信息，请参阅预配方案列。

标注	区域	描述
D	详细信息窗格	显示所选预配方案的详细信息。
E	列表级操作	显示可对整个显示列表执行的操作： • **导出**图标：将主视图中显示的目录列表导出到 CSV 文件。 • **要显示的列**图标：自定义列表的主视图。

参考：PROVSCHEME 列

此表列出了“**硬件视图**”中的所有列及其说明。

列	描述
ProvScheme 名称	预配方案的名称。
ProvScheme 版本	预配方案的版本号
CPU 核心数	分配给预配方案的 CPU 核心数。
内存 (MB)	分配给预配方案的内存量（以 MB 为单位）。
计算机计数	预配方案预配的计算机数量。
持久性	指示预配方案的磁盘和数据是否在重新启动后仍然保留。
身份类型	预配方案的身份类型。
使用 WBC	指示预配方案是否配置了 WBC（也称为 MCSIO）。
WBC 磁盘大小 (GB)	预配方案的 MCSIO 磁盘缓存大小。

列	描述
WBC 内存大小 (MB)	预配方案的 MCSIO 内存缓存大小。
激活类型	仅适用于 Windows VDA。预配方案的 Windows 许可证激活类型。值包括：不支持的 VDA、密钥管理服务、多重激活密钥和无效。

更新计算机目录的硬件设置

此功能提供了一种集中式方法，可使用服务窗口管理和应用对计算机目录 VM 硬件设置（例如计算机配置文件、存储、许可证和 NIC）的更改。更改适用于现有 VM 和新 VM。

您可以执行以下操作：

- 更新计算机目录的硬件设置
- 管理硬件版本
- 监视计算机目录的任务状态

限制

- 目前，仅支持 Azure MCS 计算机目录。
- 不支持快速部署目录。
- 为避免潜在问题，如果执行以下操作，请将 VDA 升级到版本 2503 或更高版本：
  - 为使用临时磁盘的现有 VM 启用休眠。
  - 在带临时磁盘的 Azure SKU 和不带临时磁盘的 Azure SKU 之间更改 VM 大小。

更新计算机目录硬件设置的步骤

1. 转到 **Machine Catalog** 节点，切换到 **Hardware** 视图，右键单击要更新的计算机目录，然后选择 **Update Hardware**。
2. 在“**更新硬件**”页面上，单击“**创建版本**”。仅配置要更改的设置。没有默认设置。
3. 导航到“**摘要**”页面，然后单击“**完成**”。
4. 选择“**计划**”或“**仅保存版本**”以确认何时将更改应用于选定的计算机目录。
   - 如果选择“**计划**”，您将被重定向到“**应用于计算机目录**”页面。配置计划时间和信息，然后单击“**保存**”。将创建一个带有计划的新硬件版本。计算机目录将在计划完成后更新。
   - 如果选择“**仅保存版本**”，系统将创建一个新的硬件版本，而不会立即将更改应用于选定的计算机目录。

> **注意：**
>
> 新创建的硬件版本继承了以前版本的更改。

> 即使您保存硬件更改而未安排应用时间，您仍然可以将其应用于计算机目录。

1. 右键单击计算机目录，然后选择“**更新硬件**”。
2. 在“**更新硬件**”页面上，选择一个版本。单击“**应用于计算机目录**”以创建计划。计算机目录将在计划完成后更新。

管理计算机目录的硬件版本

您可以删除硬件版本并取消计算机目录的计划。

- **删除硬件版本**：在“**更新硬件**”页面上，选择一个或多个版本，然后单击“**删除**”以删除版本。
- **取消计划**：在“**更新硬件**”页面上，如果您想取消尚未开始的计划，请在“**计划**”状态列中单击“**取消**”以取消它。

监视计算机目录的任务状态

要检查硬件更新是否成功应用：

1. 选择计算机目录。
2. 导航到**详细信息 > 服务窗口**选项卡，并查看**状态**列。
3. 单击任务 ID 以访问**任务中心**。此中心提供详细的任务进度和结果。请参阅在任务中心监视和管理任务

负载均衡计算机

负载均衡有助于组织在利用云所提供的一切优势的同时，实现所需的成本平衡。负载均衡在交付组级别进行配置。

> **注意：**
>
> 负载均衡仅适用于多会话操作系统计算机。

> 负载均衡有两种选项：

- 水平负载均衡

- 垂直负载均衡

默认情况下，水平负载均衡处于启用状态。

水平负载均衡： 在水平负载均衡模型中，传入的用户会话被分配给可用负载最低的计算机。考虑以下示例，在一个部署中，假设我们有两个 VDA。一个具有活动用户会话（用户 1），第二个用户（用户 2）正在等待会话。水平负载均衡算法将用户 2 分配给 VDA 2，因为其负载指数更有利。因此，水平算法将会在所有可用 VDA 之间分配会话，这可能会阻碍计算机在负载降低时关闭。

垂直负载均衡： 在垂直负载均衡模型中，会话被分配给负载指数最高的 VDA。这有助于将传入的用户会话整合到已被其他用户使用的 VDA 上，并有助于减少必须开机并保持就绪以供用户会话使用的 VDA 数量。让我们考虑与水平负载均衡中提到的相同部署。用户 1 被分配到 VDA 1，并且垂直负载均衡算法应用于用户 2 会话。用户 2 被分配到 VDA 1，因为 VDA 1 上的负载指数更高。因此，所有传入会话都将分配给负载最高的 VDA，直到达到高负载指数水印。只有在那之后，其他 VDA 才开始接收会话。

站点级别的负载均衡设置

您可以为所有交付组配置负载均衡（站点范围设置）。

要从 Studio 配置此功能，请在左侧窗格中选择**设置**。在**计算机上的负载均衡会话**下选择一个选项。

或者，您可以使用 PowerShell 在站点范围内启用或禁用垂直负载均衡。在 `Set-BrokerSite` cmdlet 中使用 `UseVerticalScalingForRdsLaunches` 设置。使用 `Get-BrokerSite` 显示 `UseVerticalScalingForRdsLaunches` 设置的值。有关详细信息，请参阅 cmdlet 帮助。

> **提示：**
>
> 要指定计算机可以托管的最大会话数，请使用 最大会话数 策略设置。

交付组级别的负载均衡设置

您可以在交付组级别配置负载平衡，并覆盖从站点级别继承的负载平衡设置。

您可以在创建交付组或编辑现有交付组时配置此项。请参阅步骤 2. 负载平衡。

负载管理

负载管理衡量服务器负载并确定在当前环境条件下选择哪个服务器。此选择基于：

- **服务器维护模式状态**：仅当维护模式关闭时，多会话操作系统计算机才会被考虑用于负载平衡。

- **服务器负载指数**：确定提供多会话操作系统计算机的服务器接收连接的可能性。该指数是负载评估器（会话数以及 CPU、磁盘和内存使用情况等性能指标的设置）的组合。负载评估器在负载管理策略设置中指定。默认情况下，负载指数在其计算中仅使用会话数，而不使用 CPU、磁盘或内存，除非在负载管理策略设置中对其进行配置。有关策略设置的信息，请参阅负载管理策略设置。

  服务器负载指数为 10000 表示服务器已满载。如果没有其他可用服务器，用户在启动会话时可能会收到一条消息，指出桌面或应用程序当前不可用。 您可以在 Director (Monitor)、Studio 搜索和 SDK 中监视负载指数。

  在控制台显示中，要显示“**服务器负载指数**”列（默认情况下处于隐藏状态），请选择一台计算机，右键单击列标题，然后选择“**选择列**”。在“**计算机类别**”中，选择“**负载指数**”。

  在 SDK 中，使用 `Get-BrokerMachine` cmdlet。有关详细信息，请参阅 CTX202150。

- **并发登录容忍策略设置**：登录到服务器的最大并发请求数。（此设置等同于 XenApp 6.x 版本中的负载限制。）

  当所有服务器都达到或高于并发登录容忍设置时，下一个登录请求将分配给待处理登录数最少的服务器。如果有多个服务器满足这些条件，则选择负载指数最低的服务器。请参阅并发登录容忍。

  > **提示：**
  >
  > 要强制执行登录容忍设置并导致超出指定数量的并发登录失败，您可以运行 `Set-BrokerServiceConfigurationData Core.LogonToleranceIsHardLimit -SettingValue $true`。

创建交付组

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

> 交付组是从一个或多个计算机目录中选择的计算机集合。交付组定义了哪些用户可以访问这些计算机，以及他们可以使用的应用程序和桌面。

创建交付组是设置站点和计算机目录之后的下一步。您可以稍后修改初始设置或根据需要创建其他交付组。

某些功能和设置仅在编辑现有交付组时可配置。有关详细信息，请参阅管理交付组

开始之前

在创建交付组之前：

- 查看本文以了解所需的选项和信息。
- 确保您已创建与管理计算机的管理程序、云服务或其他资源的连接。
- 确保包含虚拟或物理计算机的计算机目录可用。

要创建交付组：

1. 如果您已创建站点和计算机目录但未创建交付组，Web Studio 会引导您到正确的起始位置来创建一个。

向导页面

如果您已创建站点和计算机目录但尚未创建交付组，Web Studio 会引导您到正确的起点来创建一个。

如果您已创建交付组并希望创建另一个，请按照以下步骤操作：

1. 选择**交付组**。
2. 在操作窗格中，选择**创建交付组**。
3. 要组织交付组，您可以在默认的“**交付组**”文件夹下创建文件夹。有关详细信息，请参阅创建文件夹。
4. 选择要创建组的文件夹，然后单击“**创建交付组**”。组创建向导随即打开。
5. 向导从“**简介**”页面开始，您可以选择在将来启动时跳过此页面。然后，它会引导您完成多个页面，如下表所述。完成每个页面后，单击“**下一步**”继续，直到到达最后一页。

	多会话操作系统	单会话操作系统静态（已分配）	单会话操作系统共享（池化）	远程电脑访问
页面	计算机	计算机	计算机	计算机

	多会话操作系统	单会话操作系统静态（已分配）	单会话操作系统共享（池化）	远程电脑访问
	负载平衡	交付类型	用户	用户
	用户	用户	应用程序	应用程序
	应用程序	应用程序	桌面	桌面分配规则
	桌面	桌面分配规则	应用程序保护	应用程序保护
	应用程序保护	应用程序保护	作用域	作用域
	作用域	作用域	许可协议	许可协议
	许可协议	许可协议	策略集	策略集
	策略集	策略集	本地主机缓存	摘要
	摘要	摘要	摘要	

注意：

- 如果所选的单会话操作系统静态计算机目录中有任何可用的已分配计算机，您会看到**计算机分配**页面（紧随**计算机**页面之后）。
- 本地主机缓存设置页面仅适用于包含电源管理单会话池化计算机的交付组。

计算机页面

1. 要创建仅包含单会话可挂起 VM 的交付组，请选择 **为此交付组启用挂起功能**。

   注意：

   此功能仅适用于单会话可挂起计算机。

2. 选择一个计算机目录，然后选择要从该目录使用的计算机数量。

重要注意事项

- 选择目录时，列表中仅显示至少包含一台未使用计算机的目录。
- 一个目录可以为多个交付组提供计算机。一台计算机只能用于一个交付组。当您向交付组添加更多计算机时，Web Studio 默认会建议使用同一目录。
- 一个交付组可以使用来自多个目录的计算机；但是，这些目录必须包含相同的计算机类型（多会话操作系统、单会话操作系统或远程电脑访问）。交付组中的所有计算机必须具有相同的分配类型（池化或静态）。换句话说，您不能在交付组中混合使用计算机类型。
- Citrix 建议在所有计算机上使用最新版本的 VDA。
- 对于**远程电脑访问**，当您创建站点时，会自动创建一个名为**远程电脑访问计算机**的目录和一个名为**远程电脑访问桌面**的交付组。**远程电脑访问计算机**目录中的每台计算机都会自动与一个交付组关联。
- 执行以下兼容性检查：
  - MinimumFunctionalLevel 必须兼容
  - SessionSupport 必须兼容
  - SingleSession 的 AllocationType 必须兼容
  - 远程电脑访问仅与远程电脑访问目录兼容

计算机分配页面

如果在**计算机**页面上选择的单会话操作系统静态计算机目录中存在任何可用的已分配计算机，则**计算机分配**页面可用。

使用此页面，管理此交付组中计算机的用户分配和桌面显示名称。

- 使用**显示名称**字段管理桌面显示名称。
- 单击**浏览**并选择用户或组。

负载平衡页面

计算机上的负载平衡会话页面适用于多会话操作系统计算机。

使用此页面，配置此交付组要使用的负载平衡设置。默认情况下，交付组使用站点范围设置。

1. 要为此交付组配置负载平衡设置，请选中**覆盖站点范围**设置复选框。
2. 根据需要选择**水平负载平衡**或**垂直负载平衡**选项。有关水平和垂直负载平衡方法的信息，请参阅负载平衡计算机。

创建交付组时的负载平衡设置(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/load-balancing.png)

如果选择**垂直负载平衡**，请确保并发登录容忍度和最大会话数策略已正确配置。

交付类型页面

交付类型页面仅适用于单会话操作系统静态（已分配）计算机。

使用此页面，配置目录中的计算机，以便向用户交付桌面或应用程序。

1. 选择**应用程序**或**桌面**。不能同时启用两者。

> **注意：**
>
> 如果从多会话操作系统或单会话操作系统随机（池）目录中选择计算机，则交付类型假定为应用程序和桌面。您可以交付应用程序、桌面或两者。

用户页面

用户页面适用于所有计算机类型。但是，该页面的选项因计算机类型而异。

使用此页面，指定用户如何访问交付组中的资源。

用户访问控制的工作原理

在创建或编辑访问设置时，交付组中的用户访问权限通过指定的用户列表进行控制。

- 满足以下*所有*条件的用户可以访问交付组中的**应用程序**：
  - 有权访问此交付组中的资源（应用程序和桌面）。默认情况下，访问权限由部署的用户访问列表（Active Directory 中的用户）确定，该列表不是通过 Studio 配置的。请参阅在交付组中添加或删除用户。
  - 访问此组中的应用程序。默认情况下，应用程序授权策略规则包括所有人。有关详细信息，请参阅 PowerShell SDK `BrokerAppEntitlementPolicyRule` cmdlet。
  - 有权访问包含此应用程序的应用程序组。
- 满足以下*两个*条件的用户可以访问交付组中的桌面：
  - 有权访问此交付组中的资源（应用程序和桌面）。默认情况下，访问权限由部署的用户访问列表（Active Directory 中的用户）确定，该列表不是通过 Studio 配置的。您可以从默认用户范围添加或删除用户。请参阅在交付组中添加或删除用户。

◦ 有权访问此组中的桌面。有关详细信息，请参阅桌面（或桌面分配规则页面）。

配置步骤

1. 选择以下选项之一以允许或限制交付组中资源的使用：

   - **允许任何经过身份验证的用户使用资源：** 要访问应用程序和桌面，您按名称指定的用户和组成员必须向 StoreFront™ 或 Citrix Workspace™ 应用程序提供凭据，例如智能卡或用户名和密码。（对于包含单会话操作系统计算机的交付组，您可以通过编辑交付组稍后导入用户数据（用户列表）。）
   - **限制资源使用：** 另外，您可以通过将用户或用户组添加到**允许列表**来限制交付组的使用。只有**允许列表**中的用户才能访问交付组中的应用程序和桌面。您还可以通过单击**添加阻止列表**将用户和用户组添加到阻止列表，这会阻止用户使用所选交付组中的应用程序和桌面。阻止列表仅在用于阻止允许列表中的用户时才有意义。

2. 选择用户登录会话的身份类型：

   - **Active Directory**：允许用户使用 Active Directory 凭据登录到交付组中的资源。
   - **Microsoft Entra 混合身份**：允许用户使用 Active Directory 或 Microsoft Entra 混合身份登录到交付组中的资源。

   > **注意：**
   >
   > 如果未配置Microsoft Entra 单一登录 (SSO)，则**Microsoft Entra 混合身份**选项不可用。

3. 对于多会话操作系统计算机，如果您希望用户无需向 StoreFront 或 Citrix Workspace 应用程序提供凭据即可访问应用程序和桌面，请选择**授予未经身份验证（匿名）用户访问权限；无需凭据**。例如，在自助服务终端，应用程序可能需要凭据，但 Citrix 访问门户和工具不需要。

   - 未经身份验证的用户帐户在会话启动时按需创建，并命名为 AnonXYZ，其中 XYZ 是一个唯一的三位数值。
   - 未经身份验证的用户会话的默认空闲超时为 10 分钟，并且在客户端断开连接时会自动注销。不支持重新连接、客户端之间漫游和 Workspace Control。

4. 选择**要求会话在用户的主区域中启动（如果已配置）**，以防止在用户的主区域具有足够资源的情况下，会话默认启动到其他可用区域。
5. 如果您希望会话随用户移动，无论设备如何或是否存在当前会话，请选择**允许会话在客户端设备之间随用户漫游**。请参阅会话漫游。

下表描述了您在**用户**页面上的选择：

启用访问权限	添加/分配用户和用户组？	启用“授予未经身份验证的用户访问权限”复选框？
仅限经过身份验证的用户	是	否
仅限未经身份验证的用户	否	是
已验证和未验证用户	是	是

应用程序页面

“**应用程序**”页面适用于所有计算机类型。但是，可以添加的应用程序因计算机类型而异。

使用此页面，您可以将打包的应用程序添加到此组中的桌面。

重要注意事项

- 您可以将打包的应用程序添加到交付组。每次用户登录其桌面或远程电脑时，包含这些应用程序的软件包都会自动装载。
- 默认情况下，您添加的新应用程序会放置在名为“应用程序”的文件夹中。您可以指定其他文件夹。有关详细信息，请参阅应用程序文章。
- 您可以在将应用程序添加到交付组时或之后更改其属性。有关详细信息，请参阅应用程序文章。
- 如果您尝试添加一个应用程序，并且该文件夹中已存在同名应用程序，系统会提示您重命名要添加的应用程序。如果您拒绝，则会为该应用程序添加一个后缀，使其在该应用程序文件夹中是唯一的。
- 当您将应用程序添加到多个交付组时，如果您没有权限在所有这些交付组中查看该应用程序，则可能会出现可见性问题。在这种情况下，请咨询具有更高权限的管理员，或者扩展您的范围以包括添加了该应用程序的所有交付组。
- 如果您向同一用户发布两个同名应用程序，请更改“应用程序名称（面向用户）”属性。否则，用户将在 Citrix Workspace 应用程序中看到重复的名称。

配置步骤

1. 选择“**添加**”菜单以显示应用程序源。
    - **从“开始”菜单”：** 应用程序通过分配给交付组的当前注册 VDA 之一发现。当您选择此源时，将启动一个新页面，其中包含发现的应用程序列表；选择要添加的应用程序，然后选择“**确定**”。

- **手动：** 位于交付组中的 VDA 上或网络中其他位置的应用程序。选择此源将打开一个新页面，您可以在其中通过以下方式指定要添加的应用程序：
  - 键入可执行文件的路径、工作目录、可选命令行参数以及管理员和用户的显示名称。
  - 从交付组中的 VDA 选择一个应用程序。为此，请单击**浏览**，输入访问 VDA 的凭据，等待连接到 VDA，然后从 VDA 中选择一个应用程序。所选应用程序的属性会自动填充页面上的字段。
- **现有：** 以前添加到部署中的应用程序，可能在另一个交付组中。当您选择此源时，将启动一个新页面，其中包含发现的应用程序列表；选择要添加的应用程序，然后选择“**确定**”。
- **应用程序包：** App-V、MSIX、MSIX app attach 或 FlexApp 应用程序包中的应用程序。当您选择此源时，将启动“**从包中添加应用程序**”页面。选择一个应用程序包源，从结果显示中选择要添加的应用程序，然后选择“**确定**”。

> **注意：**
>
> - 如果未为站点配置任何应用程序包，则此选项将变灰。
>
> \> - 要发布 MSIX 或 MSIX app attach 应用程序，交付组的功能级别必须为 2106 或更高版本。对于 FlexApp 应用程序，功能级别必须为 2206 或更高版本。如果未满足功能级别要求，则“**应用程序包源**”下拉列表中的相应选项将变灰。

- **应用程序组：** 部署中存在的应用程序组。

如果应用程序源或应用程序不可用或无效，则它不可见或无法选择。例如，如果部署中未添加任何应用程序，则“**现有**”源不可用。或者，应用程序可能与所选计算机目录中计算机上支持的会话类型不兼容。

桌面（或桌面分配规则）页面

此页面的标题取决于您之前在向导中选择的计算机目录：

- 如果您选择的目录包含多会话或池化单会话计算机，则此页面标题为 **Desktops**。
- 如果您选择的目录包含单会话静态计算机，并且在 **Delivery Type** 页面上指定了“Desktops”，则此页面标题为 **Desktop Assignment Rules**。

> **注意：**

> 如果您选择的目录包含单会话静态计算机，并且在 **Delivery Type** 页面上指定了“Applications”，则您不会看到此页面。

1. (可选) 要更新默认桌面图标，请选择**更改**。浏览以从本地计算机或 VDA 计算机中选择 `.ico` 或 `.exe` 文件。支持的最大图标文件大小为 500 KB。此图标将覆盖组中所有桌面的默认图标，除非为单个桌面设置了不同的图标。
2. 选择 **Add**。在对话框中：
   a. 在 **Display name** 和 **Description** 字段中，键入要在 Citrix Workspace 应用程序中显示的信息。
   b. 对于多会话或池化单会话操作系统计算机：要向桌面添加标记限制，请选择 **Restrict launches to machines with this tag**，然后从菜单中选择标记。
   c. 使用单选按钮，您可以选择：
      i. **允许有权访问此交付组的所有人使用桌面。** 交付组中的所有用户都可以启动桌面（对于具有池化计算机的组），或者在启动桌面时被分配一台计算机（对于具有单会话静态计算机的组）。
      ii. 通过将用户和用户组添加到**允许列表**来**限制桌面使用**。只有**允许列表**中的用户才能访问桌面。您还可以通过单击**添加阻止列表**将用户和用户组添加到阻止列表，这会阻止用户使用所选交付组中的桌面。阻止列表仅在用于阻止允许列表中的用户时才有意义。
   d. 如果组包含单会话静态计算机，请指定每个用户的最大桌面数。此值必须大于或等于一。此设置不是强制性的。您可以手动分配计算机，或使用 RemotePC 自动分配计算机。
   e. (可选) 选择**更改**以更新池桌面或单会话静态桌面的桌面图标分配规则。浏览以从本地计算机或 VDA 计算机中选择 `.ico` 或 `.exe` 文件中的图标。支持的最大图标文件大小为 500 KB。指定的图标将覆盖在交付组级别设置的默认图标。
   f. 启用或禁用桌面（对于多会话计算机）或桌面分配规则（对于单会话静态计算机）：禁用桌面会停止桌面交付。禁用桌面分配规则会停止向用户自动分配桌面。
   g. 完成对话框后，选择 **确定**。

站点中桌面的最大实例数（仅限 PowerShell）

要配置站点中桌面的最大实例数（仅限 PowerShell）：

- 在 PowerShell 中，使用相应的 BrokerEntitlementPolicyRule cmdlet 和 MaxPerEntitlementInstances 参数。例如，以下 cmdlet 修改 `tsvda-desktop` 规则，将站点中

允许的最大并发桌面实例数设置为两个。当有两个桌面实例正在运行时，如果第三个订阅者尝试启动桌面，则会发生错误。

```
Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
-MaxPerEntitlementInstances 2
```

- 有关指导，请使用 Get-Help cmdlet。例如，`Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`。

应用程序保护页面

应用程序保护页面适用于所有计算机类型。

使用此页面，您可以为 Citrix 发布的应用程序和桌面提供增强的安全性。

以下信息是对 Citrix Workspace 应用程序文档中 `<https://docs.citrix.com/zh-cn/citrix-workspace-app/app-protection.html>` 处的“应用程序保护”文章的补充。

- 您必须拥有有效的应用程序保护授权。要购买应用程序保护功能，请联系您的 Citrix 销售代表。
- 应用程序保护需要 XML 信任。要启用 XML 信任，请转到**设置 > 启用 XML 信任**。

在以下条件下应用保护：

- **防屏幕截图**：
  - 在 Windows 和 macOS 上，只有受保护内容的窗口是空白的。当受保护的窗口未最小化时，应用程序保护处于活动状态。
  - 在 Linux 上，整个捕获是空白的。无论受保护的窗口是否最小化，应用程序保护都处于活动状态。
- **防键盘记录**：当受保护的窗口处于焦点时启用。要禁用保护，请将焦点切换到另一个窗口。

作用域页面

作用域页面适用于所有计算机类型。

使用此页面，您可以根据您的组织需求对对象（例如，连接、目录和交付组）进行分组。

许可证分配页面

“**许可证分配**”页面适用于所有计算机类型。

使用此页面，指定交付组要使用的许可证。默认情况下，交付组使用站点许可证。有关详细信息，请参阅多类型许可。

策略集页面

“**策略集**”页面适用于所有计算机类型。

使用此页面，指定此交付组要使用的策略集。

本地主机缓存设置页面

此页面仅适用于包含电源管理的单会话池化计算机的交付组。

默认情况下，处于本地主机缓存 (LHC) 模式时，由于数据泄露风险，已进行电源管理的池计算机不可用。要更改默认行为并在 LHC 模式下使其可用于新的用户连接，请选择**保持资源可用**。

或者，您可以使用 PowerShell 命令更改默认行为。有关详细信息，请参阅应用程序和桌面支持。

> **重要提示：**
>
> 启用对电源管理的单会话池化计算机的访问可能会导致来自先前用户会话的数据和更改出现在后续会话中。

本地主机缓存中的一次性使用池化桌面

在本地主机缓存 (LHC) 中断期间，池化桌面可以一次性使用。这是通过向具备能力的 VDA 发送卫生 Blob 并启动重新启动来实现的。此过程可确保桌面在从中断中恢复后处于干净状态。对于不具备能力或旧版计算机，只有在明确启用重用时才会参与。 此功能通过在中断期间使可用性更加无缝来改善客户体验。

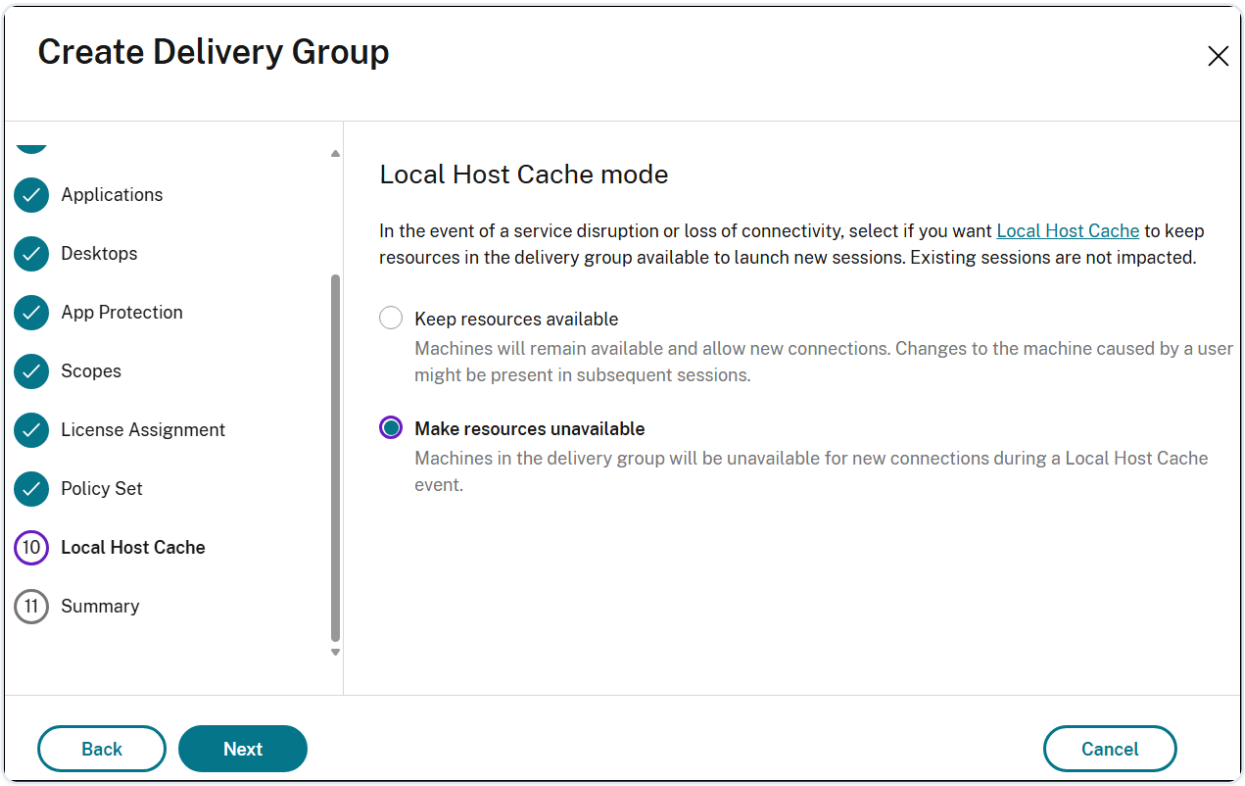
先决条件

- VDA 版本 2407 或更高版本，以实现完全卫生强制。旧版 VDA（VDA 版本 2407 之前）只能在启用重用时使用。这些 VDA 不会接收卫生 Blob 或强制重新启动。
- 具有单会话计算机的计算机目录。

配置池桌面的一次性使用

1. 使用 VDA 版本 2407 或更高版本创建包含单会话计算机的 MCS 目录。
2. 创建相应的交付组。通过远程 PowerShell 将交付组的 `ReuseMachinesWithoutShutdownInOutage` 桌面组设置设置为 `false`，或者在 Web Studio 的**本地主机缓存模式**页面上创建交付组时选择**使资源不可用**。

```
Set-BrokerDesktopGroup -Name "name"
-ReuseMachinesWithoutShutdownInOutage $false
```



3. 完成配置后，在 LHC 中断模式下，计算机可供一次性使用。退出 LHC 中断模式后，受污染的计算机将重新启动并可再次使用。

> **注意：**
>
> 一旦用户会话在其最近一次开机后启动，该计算机就被归类为受污染的计算机。未受污染的计算机是指自上次开机事件以来未启动任何用户会话的计算机。

摘要页面

输入交付组的名称。您还可以（可选）输入说明，该说明将显示在 Citrix Workspace 应用程序和 Studio 中。

查看摘要信息，然后单击**完成**。

限制

将桌面分配给客户端 IP 地址仅适用于非常有限的客户端类型和配置。基于客户端 IP 地址执行访问筛选会使用云客户端的公共 IP 地址。

使用合并组启用金丝雀部署（预览版）

使用合并组为您的应用程序和桌面资源实施金丝雀部署模型。此功能允许您发布同一资源的多个版本，同时以单个图标的形式呈现给最终用户。

合并组允许您将特定用户组定向到同一资源的不同实现版本。您可以指定一定比例的用户（例如 5%）测试新版本，而其他用户则继续使用稳定版本。如果新版本出现问题，您可以轻松地将用户故障转移到稳定版本，而不会中断他们的体验。此功能支持高可用性和灾难恢复场景，无需重新枚举或更改配置。

用法示例

为了在应用程序的不同版本可用时简化用户体验，请考虑使用合并组功能。例如，如果您有 Microsoft Word 2016 和 Microsoft Word 2019，则可以将其分组为一个图标，而不是显示两个单独的图标。通过使用合并组功能，系统可以确定为特定用户启动哪个版本的应用程序（例如 Word 2016 或 Word 2019）。

限制

当合并组中用户首选的资源暂时不可用（例如，处于维护模式）时，Broker 会在备用资源上启动会话。如果首选资源在用户重新连接之前再次可用，Broker 将在首选资源上创建新会话，而不是重新连接到备用资源上的现有会话。

影响：用户将有两个活动会话，每个资源上一个，但只能访问首选资源上的会话。备用资源上断开连接的会话将无法访问。

解决方法：管理员可以从 Studio 注销孤立会话或重新启动托管该会话的计算机。

配置合并组的命令

> **注意：**
>
> 有关详细的命令说明，请参阅 SDK 文档。

操作	命令	描述
创建合并组	`New-BrokerMergeGroup`	创建具有指定名称和描述（可选）的合并组。
设置合并组	`Set-BrokerMergeGroup`	设置合并组的名称、描述、MergeGroupSetUid 和 DefaultResourceUid。DefaultResource 是合并组的图标资源。在 Citrix

操作	命令	描述
		Workspace 应用程序中，合并组继承此资源的图标。
删除合并组	`Remove-BrokerMergeGroup`	删除指定的合并组。如果合并组包含合并资源，则删除失败。要删除此类合并组，您需要 `Force` 参数 – 它会删除合并组及其在合并组中关联的 `MergedResources` 。
创建合并资源	`New-BrokerMergedResource`	在站点中创建新的合并资源。创建具有 applicationUid 或 EntitlementPolicyRuleUid （共享/随机桌面组）的合并资源。这只是应用程序资源或授权策略规则之上的一个包装器。删除合并资源不会删除应用程序或授权策略规则。
设置合并资源	`Set-BrokerMergedResource`	设置 `MergedResource` 对象的属性。Users 参数会删除与合并资源关联的任何以前的用户，并将新列表（或单个用户）设置为此合并资源的用户列表。如果要向现有用户列表添加更多用户，可以使用 `AddUsers` 参数。如果要从现有用户列表中删除用户，可以使用 `RemoveUsers` 参数。
删除合并资源	`Remove-BrokerMergedResource`	删除指定的合并资源。

更多信息

- 管理交付组

- 应用程序

管理交付组

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 唯一的管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

简介

本文介绍了从管理控制台管理交付组的步骤。除了更改创建组时指定的设置外，您还可以配置创建交付组时不可用的其他设置。

过程类别包括：常规、用户、计算机和会话。有些任务跨越多个类别。例如，“阻止用户连接到计算机”在计算机类别中描述，但它也影响用户。如果您在一个类别中找不到任务，请检查相关类别。

其他文章也包含相关信息：

- 应用程序 包含有关管理交付组中应用程序的信息。
- 管理交付组需要交付组管理员内置角色权限。有关详细信息，请参阅 委派管理。

常规

- 查看组详细信息
- 更改首选属性
- 更改交付类型
- 更改 StoreFront™ 地址
- 更改功能级别
- 管理远程电脑访问交付组
- 使用文件夹组织交付组
- 管理应用程序保护
- 更改交付组的挂起功能

查看组详细信息

1. 使用搜索功能查找特定的交付组。有关说明，请参阅搜索实例。
2. 根据需要从搜索结果中选择一个组。
3. 有关组列的说明，请参阅下表。
4. 单击底部详细信息窗格中的选项卡，以获取有关此组的更多信息。

列	说明
交付组	组名称和会话类型。会话类型包括单会话操作系统和多会话操作系统。
交付内容	从此组交付的资源类型。可能的值包括应用程序、桌面以及应用程序和桌面。如果交付组由专用计算机组成，则显示“静态计算机分配”。
使用中的会话	已设置的计算机数量和处于断开连接状态的计算机数量。
已分配计数	分配给交付组的目录中的计算机数量。
文件夹	**交付组**树中组的位置。它显示组所在的文件夹名称（包括尾随反斜杠），如果组位于根级别，则显示 `-`。

更改首选属性

首选属性控制用户如何从交付组访问和启动资源。要更改交付组的首选属性，请执行以下步骤：

1. 在 Studio 的左窗格中，选择**交付组**。
2. 选择一个组，然后在操作栏中选择**编辑**。
3. 在**首选项**页面上，更改下表中的任何设置。
4. 选择**应用**以应用所做的任何更改并保持窗口打开。或者，选择**确定**以应用更改并关闭窗口。

设置	描述
描述	Citrix Workspace™（或 StoreFront）使用并显示给用户的文本。
启用交付组	交付组是否已启用。

设置	描述	
时区	此交付组中的计算机所在的时区。此设置会自动显示为新创建的交付组在 **设置 > 日期和时间** 中设置的时区。如果需要，您可以为交付组选择不同的时区。下拉菜单列出了站点支持的时区。 **注意：** 更改交付组上的时区可能会重新启动该交付组中的计算机。为避免这种情况，请务必在非生产时间更改时区设置。	
启用 Secure ICA®	使用 SecureICA 保护交付组中计算机之间的通信，SecureICA 会加密 ICA 协议。默认级别为 128 位。可以使用 SDK 更改级别。Citrix® 建议在遍历公共网络时使用更多加密方法，例如 TLS 加密。此外，SecureICA 不会检查数据完整性。	

更改交付组的交付类型

交付类型指示组可以交付的内容：应用程序、桌面或两者。

在将“**仅应用程序**”或“**桌面和应用程序**”类型更改为“**仅桌面**”类型之前，请从组中删除所有应用程序。

1. 在左侧窗格中选择“**交付组**”。
2. 选择一个组，然后单击操作栏中的 **编辑**。
3. 在 **交付类型** 页面上，选择所需的交付类型。
4. 单击“**应用**”以应用所做的任何更改并保持窗口打开。或者，单击“**保存**”以应用更改并关闭窗口。

更改 StoreFront 地址

1. 在左侧窗格中选择“**交付组**”。
2. 选择一个组，然后单击操作栏中的 **编辑**。

3. 在“**StoreFront**”页面上，选择或添加 StoreFront URL。这些 URL 由 Citrix Workspace™ 应用程序使用，该应用程序安装在交付组中的每台计算机上。
4. 单击“**应用**”以应用所做的任何更改并保持窗口打开。或者，单击“**保存**”以应用更改并关闭窗口。

您还可以通过在左侧窗格中选择“**StoreFront**”来指定 StoreFront 服务器地址。

更改功能级别

在升级交付组中使用的计算机上的 VDA 以及包含这些计算机的计算机目录后，更改交付组的功能级别。

开始之前：

- 如果您使用 Citrix Provisioning™（以前称为 Provisioning Services），请在 Citrix Provisioning 控制台中升级 VDA 版本。
- 启动包含已升级 VDA 的计算机，以便它们可以向交付控制器注册。此过程会告知控制台交付组中需要升级的内容。
- 如果您必须继续使用较早的 VDA 版本，则无法使用较新的产品功能。有关详细信息，请参阅升级文档。

要更改交付组的功能级别：

1. 在左侧窗格中选择**交付组**。
2. 选择一个组，然后单击操作栏中的**更改功能级别**。**更改功能级别**操作仅在检测到已升级的 VDA 时显示。
3. 单击**更改**。

显示屏会指示您哪些（如果有）计算机无法更改为功能级别以及原因。然后，您可以取消更改操作，解决计算机问题，然后再次执行更改操作。

更改完成后，您可以将计算机恢复到以前的状态。选择交付组，然后在操作栏中选择 **撤消功能级别更改**。

管理远程电脑访问交付组

如果远程电脑访问计算机目录中的计算机未分配，则该计算机将临时分配给与该目录关联的交付组。此临时分配使计算机以后可以分配给用户。

交付组到计算机目录的关联具有优先级值。优先级决定了计算机在向系统注册时或用户需要计算机分配时所分配的交付组。值越低，优先级越高。如果远程电脑访问计算机目录具有多个交付组分配，则软件会选择优先级最高的匹配项。使用 PowerShell SDK 设置此优先级值。

首次创建时，远程电脑访问计算机目录与交付组关联。稍后添加到目录的计算机帐户或组织单位可以添加到交付组。此关联可以关闭或打开。

要添加或删除远程电脑访问计算机目录与交付组的关联：

1. 在左侧窗格中选择**交付组**。
2. 选择一个远程电脑访问组。
3. 在**详细信息**部分中，单击**计算机目录**选项卡，然后选择一个远程电脑访问目录。
4. 要添加或恢复关联，请单击**添加桌面**。要删除关联，请单击**删除关联**。

使用文件夹组织交付组

您可以创建文件夹以组织交付组，以便于访问。

> **提示：**
>
> 您可以通过单击操作栏右上角的**文件夹**图标，为交付组节点设置首选默认视图（文件夹视图或列表视图）。

所需角色

默认情况下，您需要具有以下内置角色才能创建和管理交付组文件夹：云管理员、完全管理员或交付组管理员。如有必要，您可以自定义用于创建和管理交付组文件夹的角色。有关详细信息，请参阅所需权限。

创建交付组文件夹

在开始之前，请规划如何组织交付组。请考虑以下事项：

- 您可以嵌套文件夹最多五级（不包括默认根文件夹）。
- 文件夹可以包含交付组和子文件夹。
- Web Studio 中的所有节点（例如**计算机目录**、**交付组**、**应用程序**和**应用程序组**）在后端共享相同的文件夹树。为避免在重命名或移动文件夹时发生名称冲突，请为不同节点中的一级文件夹使用唯一的名称。

  如果您使用 `New-BrokerAdminFolder` SDK cmdlet 创建文件夹并希望它显示在“**交付组**”节点下，则必须使用 `Set-BrokerAdminFolderMetadata` cmdlet 添加 `ContainsDeliveryGroups` 元数据。

  示例：

```
Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
ContainsDeliveryGroups -Value true
```

要创建交付组文件夹，请执行以下步骤：

1. 在左侧窗格中选择**交付组**。
2. 在文件夹层次结构中，选择一个文件夹，然后在**操作**栏中选择**创建文件夹**。
3. 输入新文件夹的名称，然后单击**完成**。

提示：

如果将文件夹创建在意外位置，可以将其拖动到正确位置。

移动交付组

您可以在文件夹之间移动交付组。详细步骤如下：

1. 在左侧窗格中选择**交付组**。
2. 按文件夹查看组。您还可以打开文件夹层次结构上方的**查看全部**以一次性查看所有组。
3. 右键单击一个组，然后选择**移动交付组**。
4. 选择要将组移动到的文件夹，然后单击**完成**。

提示：

您可以将组拖动到文件夹。

管理交付组文件夹

您可以删除、重命名和移动交付组文件夹。

请注意，只有当文件夹及其子文件夹不包含交付组时，才能删除该文件夹。

要管理文件夹，请执行以下步骤：

1. 在左侧窗格中选择 **交付组**。
2. 在文件夹层次结构中，选择一个文件夹，然后根据需要选择**操作**栏中的一个操作：
   - 要重命名文件夹，请选择**重命名文件夹**。

- 要删除文件夹，请选择**删除文件夹**。
- 要移动文件夹，请选择**移动文件夹**。

3. 按照屏幕上的说明完成剩余步骤。

所需权限

下表列出了对交付组文件夹执行操作所需的权限。

操作	所需权限
创建交付组文件夹	创建交付组文件夹
删除交付组文件夹	移除交付组文件夹
移动交付组文件夹	移动交付组文件夹
重命名交付组文件夹	编辑交付组文件夹
将交付组移动到文件夹	编辑交付组文件夹和编辑交付组属性

管理应用程序保护

以下信息是对 `<https://docs.citrix.com/zh-cn/citrix-workspace-app/app-protection.html>` 处的应用程序保护文章的补充。请注意以下详细信息：

- 您必须拥有有效的应用程序保护授权。要购买应用程序保护功能，请联系您的 Citrix 销售代表。
- 应用程序保护需要 XML 信任。要启用 XML 信任，请转至 **设置 > 启用 XML 信任**。
- 关于防屏幕捕获：
  - 在 Windows 和 macOS 上，只有受保护内容的窗口是空白的。当受保护的窗口未最小化时，应用程序保护处于活动状态。
  - 在 Linux 上，整个捕获都是空白的。无论受保护的窗口是否最小化，应用程序保护都处于活动状态。

要为交付组选择应用程序保护方法，请执行以下步骤：

1. 在左侧窗格中选择 **交付组**。
2. 选择一个组，然后在操作栏中选择**编辑**。
3. 在 **应用程序保护** 页面上，您可以看到以下选项：

选项	描述
不应用	选择此选项以不应用该设置。
应用于此交付组	选择**防键盘记录**和/或**防按键捕获**选项。将鼠标悬停在每个设置上可阅读工具提示中的详细信息。
按上下文应用	要应用此设置，请在**访问策略设置**页面中配置访问策略。
	1. 在左侧窗格中单击**访问策略**，然后单击**添加**。
	1. 在**添加策略**页面上，执行以下操作
	- i. 输入**策略名称**并根据需要配置设置。
	- ii. 在**筛选器**和**值**字段中输入详细信息，然后单击**完成**。新策略将列在**应用程序保护**页面中。为此策略启用所需的设置。
	- iii. 单击**保存**。

4. 在**交付组**页面上，选择**交付组**，然后单击底部的**详细信息**选项卡。将显示已应用的新**应用程序保护**设置。

更改交付组的挂起功能

将交付组的挂起功能设置为必需或可选：

- **必需** - 交付组只能包含那些支持挂起的 VM。
- **可选** - 交付组可以包含支持或不支持挂起的 VM。

开始之前

只有当交付组中存在的所有 VM 都支持挂起时，才能将交付组的挂起功能更改为 `Required`。

要更改交付组的挂起功能：

1. 从 Web Studio，转到左侧窗格中的**交付组**。
2. 选择一个组，然后单击操作栏中的**更改挂起功能**。
3. 单击**是**以确认您的操作。

用户

本节涵盖以下主题：

- 添加或删除用户
- 限制用户访问交付组中的桌面和应用程序
- 限制对交付组中资源的访问
- 限制用户访问所有交付组中的资源
- 配置访问策略的用户范围

在交付组中添加或删除用户

有关用户的详细信息，请参阅用户。

1. 在左侧窗格中选择**交付组**。
2. 选择一个组，然后单击操作栏中的 **编辑**。
3. 在**用户**页面上：
    - 要添加用户，请单击**添加**，然后指定要添加的用户。
    - 要删除用户，请选择一个或多个用户，然后单击**删除**。
    - 选中或清除此复选框以允许未经身份验证的用户访问。
4. 单击**应用**以应用所做的任何更改并保持窗口打开。或者，单击**保存**以应用更改并关闭窗口。

导入或导出用户列表

对于包含物理单会话操作系统计算机的交付组，您可以在创建交付组后从 .csv 文件导入用户信息。您还可以将用户信息导出到 .csv 文件。.csv 文件可以包含来自以前产品版本的数据。

CSV 文件中的第一行必须包含两个列标题，用逗号分隔。请确保第一个标题是 `Machine Account`，第二个标题是 `User Names`。（您可以包含其他标题，但不支持这些标题。）文件中的后续行包含逗号分隔的数据。`Machine Account` 条目可以是计算机 SID、FQDN 或域和计算机名称对。

要导入或导出用户信息：

1. 在左侧窗格中选择**交付组**。
2. 选择一个组，然后单击操作栏中的 **编辑**。
3. 在**计算机分配**页面上，选择**导入**列表或**导出**列表，然后浏览到文件位置。
4. 点击 **应用** 以应用您所做的任何更改并保持窗口打开。或者，点击 **保存** 以应用更改并关闭窗口。

限制交付组中桌面和应用程序的访问

您可以通过执行以下任务来管理用户对交付组中资源的访问：

- 将桌面访问权限限制给特定用户
- 将应用程序访问权限限制给特定用户

将桌面访问权限限制给特定用户

满足以下*两个*条件的用户可以访问交付组中的桌面：

- 拥有此交付组中资源（应用程序和桌面）的访问权限。

  默认情况下，访问权限由部署的用户访问列表决定，该列表未通过 Studio 配置。您可以从默认用户范围中添加或删除用户。请参阅 在交付组中添加或删除用户。

- 拥有此组中桌面的访问权限。

  有关详细信息，请参阅 步骤 8. 桌面（或桌面分配规则）。

要将桌面访问权限限制为特定用户，请参阅 在创建和编辑交付组时限制桌面使用。

将应用程序访问权限限制给特定用户

满足以下*所有*条件的用户可以访问交付组中的应用程序：

- 拥有此交付组中资源（应用程序和桌面）的访问权限。

  默认情况下，访问权限由部署的用户访问列表决定，该列表未通过 Studio 配置。您可以从默认用户范围中添加或删除用户。请参阅 在交付组中添加或删除用户。

- 访问此组中的应用程序。

  默认情况下，应用程序授权策略规则包括所有人。有关详细信息，请参阅 PowerShell SDK `BrokerAppEntitlementPolicyRule` cmdlet。如有需要，您可以使用本节中描述的步骤限制用户对交付组中应用程序的访问。

- 访问包含此应用程序的应用程序组。

要在交付组级别限制特定用户对应用程序的访问，请执行以下步骤：

1. 在 Studio 中，在左侧窗格中选择 **交付组**。
2. 选择一个交付组，然后在操作栏中选择 **编辑**。
3. 要限制应用程序访问，请执行以下步骤：

   a. 在左侧窗格中，单击 **应用程序分配规则**。

b. 要允许特定用户访问应用程序，请选择 **限制应用程序使用**，然后在 **允许列表** 区域中单击 **添加** 并指定要包含的用户或用户组。

c. 要阻止特定用户访问应用程序，请在 **阻止列表** 区域中单击 **添加** 并指定要排除的用户或用户组。

注意：

- 如果您选择 **限制应用程序使用** 但将允许列表和阻止列表都留空，则此组中的任何用户都无法使用应用程序。
- 如果您选择 **限制应用程序使用** 并将允许列表留空，则除 **阻止列表** 中的用户外，所有用户都可以使用应用程序。

限制对交付组中资源的访问

您对限制用户访问交付组中资源所做的任何更改都将覆盖以前的设置，无论您使用何种方法。您可以：

- **使用委派管理范围限制管理员访问：** 您可以创建并分配一个允许管理员访问所有应用程序的范围，以及另一个仅提供对某些应用程序访问权限的范围。有关详细信息，请参阅 委派管理。
- **通过智能访问策略表达式限制用户访问：** 您可以配置访问策略规则来控制用户对特定交付组的访问。示例包括：
  - 限制对部分用户的访问并指定允许的用户设备。
  - 限制通过 Workspace（而非 StoreFront）连接的用户访问。
  - 限制通过特定 Workspace URL 连接的用户访问。

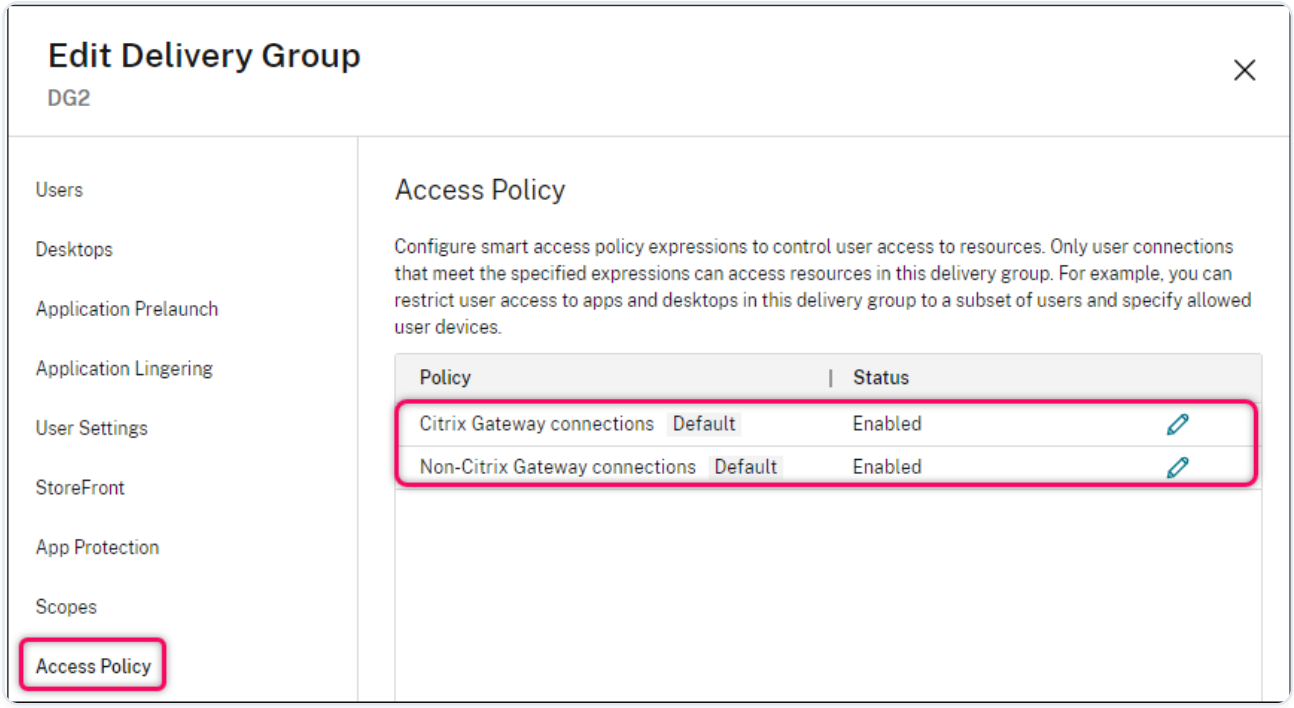
本节指导您如何通过访问策略规则限制用户对交付组的访问：

- 关于访问策略规则
- 添加访问策略规则
- 使用 Web Studio 管理访问策略规则
- 使用 PowerShell 添加和优化策略规则

关于访问策略规则

您可以为交付组配置多个访问策略规则。当用户的连接与您为交付组定义的任何访问策略规则匹配时（无论顺序如何），交付组中的应用程序和桌面都会显示在用户的 StoreFront 或 Workspace 中。

每个规则都可以单独启用或禁用。禁用规则在评估访问策略时将被忽略。



在 Web Studio 中，“访问策略”列表包含以下默认 SmartAccess 策略规则。您可以根据需要添加更多。

- **Citrix Gateway 连接。** 此策略仅允许通过 Citrix Gateway 建立的用户连接访问交付组中的资源。当启用设备状态或网络位置功能时，通过 Workspace 建立的用户连接也被视为通过 Citrix Gateway 的连接。
- **非 Citrix Gateway 连接。** 此策略仅允许不通过 Citrix Gateway 建立的用户连接访问交付组中的资源。

注意：

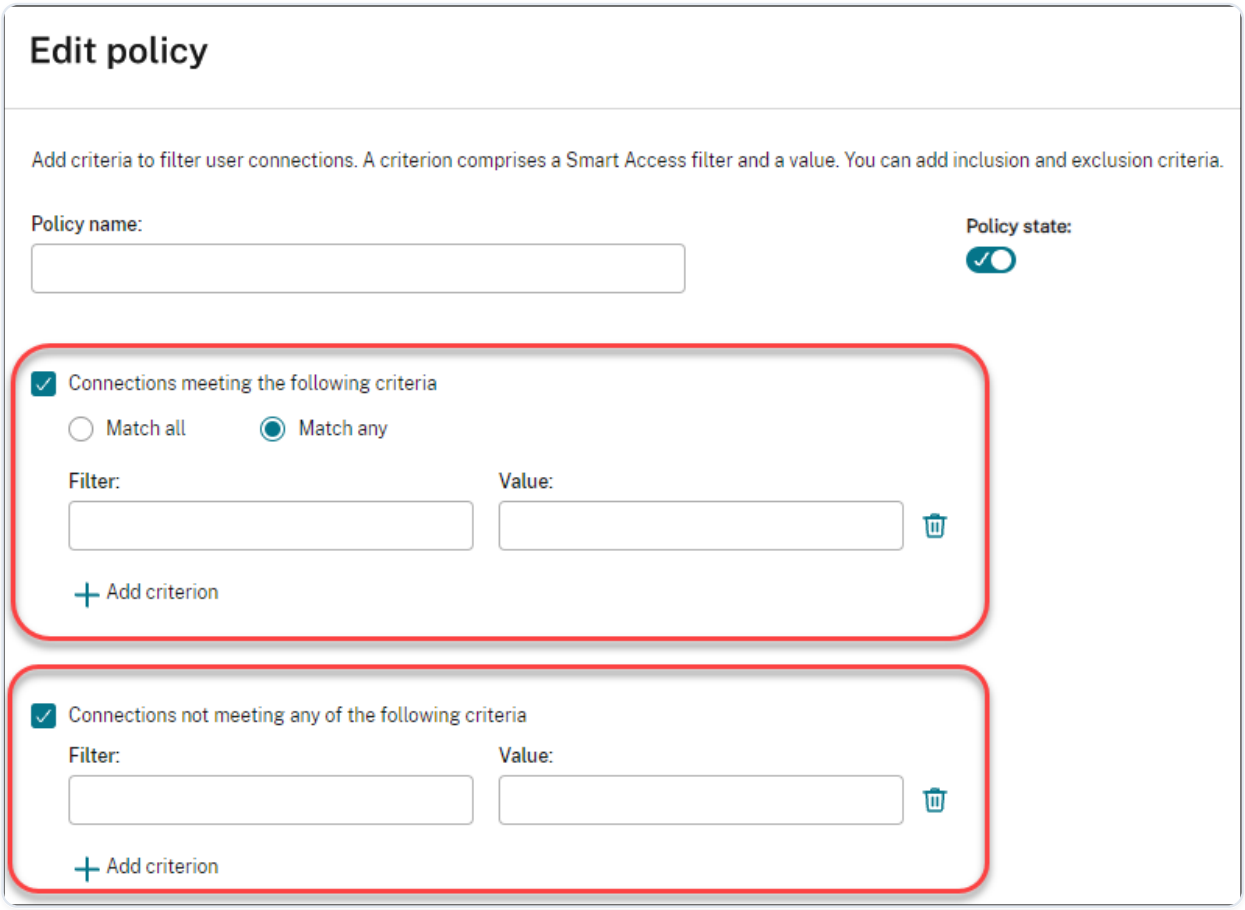
- 为防止默认规则覆盖新配置的规则，您必须禁用默认规则或对其进行优化，以排除新策略中使用的筛选器。
- 默认策略无法删除，但可以禁用。要禁用策略，请单击 **编辑** 图标，然后将 **策略状态** 更改为 **已禁用**。
- 策略列表还显示使用 PowerShell 命令添加的规则。这些策略可以删除，但不能在 Web Studio 中编辑。

使用 WEB STUDIO 添加访问策略规则

访问策略规则包含一组筛选器。有关筛选器的详细信息，请参阅本文。添加访问策略规则时，您可以根据需要向规则添加多个条件筛选器。

要使用 Web Studio 为交付组添加策略，请执行以下步骤：

1. 在控制台中，选择左侧窗格中的**交付组**。
2. 选择一个组，然后单击操作栏中的 **编辑**。
3. 在 **访问策略** 页面上，单击 **添加**。此时将显示 **添加策略** 页面。



4. 在 **策略名称** 字段中，键入策略的描述性名称。该名称在您的部署中必须是唯一的。
5. 要定义允许的用户连接条件，请执行以下步骤：

   a. 选择 **符合以下条件的连接**。

   b. 点击 **添加条件**。

   c. 在“**筛选器**”字段中，键入要使用的筛选器名称。在“**值**”字段中，键入筛选器的所需值。例如，若要仅允许通过 Workspace（而非 StoreFront）连接的用户访问此交付组中的资源，请在“**筛选器**”中键入 `Citrix-Via-Workspace`，在“**值**”中键入 `True`。

   d. 要添加更多条件，请重复步骤 b-c。

e. 选择条件之间的关系：

- **匹配任意**。仅当传入用户连接符合任何已配置的筛选条件时才允许访问。
- **匹配所有**。仅当传入用户连接符合所有已配置的筛选条件时才允许访问。

6. 要定义禁止的用户连接条件，请执行以下步骤：

a. 选择 **不符合以下任何条件的连接**。

b. 点击 **添加条件**。

c. 在**筛选器**字段中，键入要使用的筛选器名称。在**值**字段中，键入筛选器的所需值。例如，要禁止通过 `example.cloud.com` Workspace URL 连接的用户访问此交付组中的资源。为**筛选器**键入 `Citrix.Workspace.UsingDomain`，为**值**键入 `example.cloud.com`。

d. 要添加更多条件，请重复步骤 b-c。

> **注意：**
>
> 符合任何已配置条件的用户连接被禁止访问此交付组中的资源。

7. 点击 **完成**。

新策略将显示在策略列表中。

8. 审查并完善默认策略规则，以避免与此新策略涵盖的连接发生无意重叠。要完善现有策略，请使用以下方法：

- 禁用默认策略规则。
- 配置默认策略规则以排除您添加到新策略的包含条件中的 SmartAccess 筛选器。有关详细信息，请参阅使用 Web Studio 管理策略规则 和使用 PowerShell 添加和管理访问策略规则。

> **重要提示：**
>
> 如 (#about-access-policy-rules) 中所述，当用户的连接与交付组中的一个或多个策略规则匹配时，用户将获得对其资源的访问权限。因此，在创建规则后，您必须仔细审查并完善现有规则，以避免与新规则涵盖的连接发生任何无意重叠。

使用 WEB STUDIO 管理访问策略规则

您可以使用包含和排除条件来完善默认策略。例如，要限制对这些连接子集的访问，请执行以下步骤：

1. 编辑默认策略。
2. 选择**满足以下任一条件的连接**。
3. 添加、编辑或删除允许的用户访问方案的 SmartAccess 策略表达式。

有关详细信息，请参阅 Citrix Gateway 文档。

使用 POWERSHELL 添加和管理访问策略规则

您可以使用以下 PowerShell cmdlet 添加和管理交付组的访问策略规则：

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- 重命名 Broker 访问策略规则
- 移除 Broker 访问策略规则

有关详细信息，请参阅 Citrix Developer Documentation 中的相关文章。

限制用户对所有交付组中资源的访问

您可以配置资源筛选规则，以控制用户对所有交付组中的应用程序和桌面的访问。这些规则允许您指定资源类型、应用基于标记的限制，并根据网络位置和 Store 连接上下文等因素强制执行访问条件。

所需权限

要执行此任务，您必须是具有“**管理资源筛选器**”权限的管理员角色。

添加资源筛选规则

要添加资源筛选规则，请完成以下步骤：

1. 转到“**交付组 > 设置**”。
2. 在“**资源筛选器**”磁贴中选择“**管理**”。
3. 在“**管理资源筛选规则**”对话框中，单击“**添加**”。
4. 为规则输入“**名称**”和“**描述**”。
5. 选择规则适用的资源类型：
    - **应用程序**

- **桌面**
- **两者**

6. 选择标识规则所适用的资源的标签。

> **注意：**
>
> 如果选择**两者**作为资源类型，则必须选择一个标签。

7. 配置 **Smart Access 筛选器**以定义筛选资源的条件。
8. 单击**添加**以保存规则。

配置访问策略的用户范围

默认情况下，交付组中的所有访问策略都适用于同一组用户。您可以使用 Studio、PowerShell 或 Rest API 配置访问策略以应用于特定用户。

要使用 Studio 将访问策略应用于指定用户，请执行以下步骤：

1. 在 Studio 中，在左侧窗格中选择**交付组**。
2. 选择一个组，然后在操作栏中选择**编辑交付组**。
3. 在**用户**页面上，选择**使用上下文访问**。
4. 选择要配置的访问策略，然后单击“**用户访问范围**”。此时将显示“**用户访问范围**”页面。
5. 要定义此策略适用于哪些经过身份验证的用户：
   - 要将此策略应用于*任何*经过身份验证的用户，请选择“**允许任何经过身份验证的用户使用资源**”。
   - 要将此策略应用于特定用户，请保持选中“**限制资源使用**”。然后，使用允许列表和阻止列表为此策略添加或删除用户。
6. 要将此访问策略应用于未提供凭据的用户，请选择“**授予未经身份验证（匿名）用户访问权限；无需凭据**”。

计算机

- 管理计算机的用户分配(#manage-user-assignments-for-machines)
- 更改计算机到用户的分配
- 为电源管理的单会话池式 VDA 启用本地主机缓存

- 更改每个用户的最大计算机数
- 更新计算机(#update-a-machine-in-a-delivery-group)
- 添加、更改或删除桌面的标签限制(#add-change-or-remove-a-tag-restriction-for-a-desktop)
- 删除计算机(#remove-a-machine-from-a-delivery-group)
- 阻止用户连接到计算机（维护模式）(#prevent-users-from-connecting-to-a-machine-maintenance-mode-in-a-delivery-group)
- 关闭并重新启动计算机(#shut-down-and-restart-machines-in-a-delivery-group)
- 创建和管理计算机的重新启动计划(#create-and-manage-restart-schedules-for-machines-in-a-delivery-group)
- 启用一次性重新启动计划
- 电源管理计算机

管理计算机的用户分配

管理交付组中计算机的用户分配。为交付组配置桌面分配规则后，计算机将在首次启动桌面时随机分配给用户，并保持分配给用户，除非其用户分配被修改。如果要手动将未分配的计算机分配给特定用户，或者更改计算机的现有用户分配，请按照本主题中描述的步骤进行更改。使用这些步骤，您还可以修改 Citrix Workspace 应用程序中为分配给用户的计算机显示的名称。

详细步骤如下：

1. 在 Studio 中，从左侧窗格中选择**交付组**。
2. 选择一个组，然后在操作栏中选择**编辑**。
3. 在左侧窗格中，选择**计算机分配**。组中每台计算机的以下详细信息将显示：
   - **计算机名称：** 显示计算机的名称。
   - **显示名称：** 显示计算机在 Citrix Workspace 应用程序中的显示名称。
   - **用户：** 显示分配给此计算机的用户。如果配置了桌面分配规则，计算机将在首次启动桌面时随机分配给用户，并且除非修改其用户分配，否则将保持分配给这些用户。
4. 找到一台计算机，然后将用户分配给它或更改其用户分配：
   - 单击**浏览器**以浏览用户。
   - 在 **用户** 列中，输入以分号分隔的用户名列表。
   - 单击 **从 CSV 文件导入** 以使用 CSV 文件导入设置详细信息。
   - 单击**更改**以更新计算机的桌面图标。浏览以从本地计算机或 VDA 计算机中选择 `.ico` 或 `.exe` 文件。指定的图标仅在计算机级别覆盖默认图标集。

5. （可选）如果计算机已分配给用户，请根据需要修改其显示名称。

> **注意：**
>
> “显示名称”字段仅在计算机分配给用户时启用：
>
> - 如果计算机根据桌面分配规则分配给用户，则此字段显示在该规则中配置的显示名称。
> - 如果计算机是手动分配给用户的，并且该字段留空，则交付组的已发布名称（如果已指定）将用作计算机的显示名称。如果未指定已发布名称，则使用交付组的名称。请注意，您只能通过 PowerShell 为交付组指定已发布名称。

6. 选择 **应用** 以应用更改并保持窗口打开。或者，选择 **确定** 以应用更改并关闭窗口。

更改交付组中计算机到用户的分配

您可以更改使用 MCS 预配的单会话操作系统计算机的分配。您无法更改多会话操作系统计算机或使用 Citrix Provisioning 预配的计算机的分配。

1. 在左侧窗格中选择**交付组**。
2. 选择一个组，然后单击操作栏中的 **编辑**。
3. 在**桌面**或**桌面分配规则**页面（页面标题取决于交付组使用的计算机目录类型）上，指定新用户。
4. 单击**应用**以应用所做的任何更改并保持窗口打开。或者，单击**保存**以应用更改并关闭窗口。

为电源管理的单会话池式 VDA 启用本地主机缓存

默认情况下，电源管理的单会话池式计算机在本地主机缓存模式下不可用。您可以按交付组覆盖默认行为。详细步骤如下：

1. 在 Studio 的左窗格中，选择**交付组**。

   在组列表中，包含由 MCS 或 Citrix Provisioning 预配的单会话池式计算机的组会显示警告图标。

2. 根据需要选择一个组，然后在操作栏中选择 **编辑**。
3. 在**本地主机缓存**页面上，选择**保持资源可用**。
4. 选择**应用**以应用所做的任何更改并保持窗口打开。或者，选择**确定**以应用更改并关闭窗口。

或者，您可以使用 PowerShell 命令覆盖默认行为。有关详细信息，请参阅应用程序和桌面支持。

> **重要提示：**
>
> 启用对电源管理的单会话池化计算机的访问可能会导致来自先前用户会话的数据和更改出现在后续会话中。

更改交付组中每个用户的最大计算机数

1. 在左侧窗格中选择**交付组**。
2. 选择一个组，然后单击操作栏中的 **编辑**。
3. 在**桌面分配规则**页面上，设置每个用户的最大桌面数。
4. 单击**应用**以应用所做的任何更改并保持窗口打开。或者，单击**保存**以应用更改并关闭窗口。

更新交付组中的计算机

1. 在左侧窗格中选择**交付组**。
2. 选择一个组，然后单击操作栏中的**查看计算机**。
3. 选择一台计算机，然后单击操作栏中的**更新计算机**。

要选择其他映像，请选择**映像**，然后选择一个快照。

要应用更改并通知计算机用户，请选择**向最终用户推出通知**。然后指定：

- 何时更新主映像：立即更新还是在下次重新启动时更新
- 重新启动分发时间（开始更新组中所有计算机的总时间）
- 是否通知用户重新启动
- 用户收到的消息

添加、更改或删除桌面的标签限制

添加、更改和删除标签限制可能会对考虑启动的桌面产生意想不到的影响。请参阅标签中的注意事项和警告。

1. 在左侧窗格中选择“**交付组**”。
2. 选择一个组，然后单击操作栏中的 **编辑**。
3. 在“**桌面**”页面上，选择桌面，然后单击“**编辑**”。
4. 要添加标签限制，请选择 **将启动限制到具有此标签的计算机**，然后选择该标签。
5. 要更改或删除标签限制，请执行以下操作之一：
    - 选择其他标签。

- 通过清除 **将启动限制到具有此标签的计算机** 来删除标签限制。

6. 单击“**应用**”以应用所做的任何更改并保持窗口打开。或者，单击“**保存**”以应用更改并关闭窗口。

从交付组中删除计算机

删除计算机会将其从交付组中删除。它不会将其从交付组使用的计算机目录中删除。因此，该计算机可用于分配给另一个交付组。

计算机必须先关闭才能删除。要在删除计算机时暂时阻止用户连接到该计算机，请在关闭计算机之前将其置于维护模式。

计算机可能包含个人数据，因此在将计算机分配给其他用户之前请务必谨慎。请考虑重新映像计算机。

1. 在左侧窗格中选择“**交付组**”。
2. 选择一个组，然后在操作栏中单击“**查看计算机**”。
3. 确保计算机已关闭。
4. 选择计算机，然后在操作栏中单击“**从交付组中删除**”。

您还可以通过计算机使用的连接从交付组中删除计算机。

阻止用户连接到交付组中的计算机（维护模式）

当您需要暂时停止与计算机建立新连接时，可以为交付组中的一台或所有计算机启用维护模式。您可以在应用修补程序或使用管理工具之前执行此操作。

- 当多会话操作系统计算机处于维护模式时，用户可以连接到现有会话，但无法启动新会话。
- 当单会话操作系统计算机（或使用远程电脑访问的电脑）处于维护模式时，用户无法连接或重新连接。当前连接将保持连接状态，直到用户断开连接或注销。

要启用或禁用维护模式：

1. 在左侧窗格中选择“**交付组**”。
2. 选择一个组。
3. 要为交付组中的所有计算机启用维护模式，请在操作栏中单击“**启用维护模式**”。

   要为一台计算机启用维护模式，请在操作栏中单击“**查看计算机**”。选择一台计算机，然后在操作栏中单击“**启用维护模式**”。
4. 要为交付组中的一台或所有计算机禁用维护模式，请按照上述说明操作，但在操作栏中单击“**禁用维护模式**”。

Windows 远程桌面连接 (RDC) 设置也会影响多会话操作系统计算机是否处于维护模式。在以下任何一种情况下，维护模式都处于启用状态：

- 维护模式已设置为启用，如前所述。
- RDC 设置为**不允许连接到此计算机**。
- RDC 未设置为“**不允许连接到此计算机**”。“**远程主机配置用户登录模式**”设置是“**允许重新连接，但阻止新登录**”或“**允许重新连接，但阻止新登录直到服务器重新启动**”。

您还可以为以下各项启用或禁用维护模式：

- 连接，这会影响使用该连接的计算机。
- 计算机目录，这会影响该目录中的计算机。

关闭并重新启动交付组中的计算机

远程电脑访问计算机不支持此过程。

1. 在左侧窗格中选择“**交付组**”。
2. 选择一个组，然后在操作栏中单击“**查看计算机**”。
3. 选择计算机，然后在操作栏中单击以下条目之一：
    - **强制关机：** 强制关闭计算机电源并刷新计算机列表。
    - **重新启动：** 请求操作系统关闭然后再次启动计算机。如果操作系统无法执行此操作，则计算机将保持其当前状态。
    - **强制重新启动：** 强制关闭操作系统，然后重新启动计算机。
    - **暂停：** 暂停计算机而不将其关闭，并刷新计算机列表。
    - **关机：** 请求操作系统关机。

对于非强制操作，如果计算机在 10 分钟内未关机，则会断电。如果 Windows 在关机期间尝试安装更新，则存在更新完成前计算机断电的风险。

Citrix 建议您阻止单会话操作系统计算机用户在会话中选择**关机**。有关详细信息，请参阅 Microsoft 策略文档。

您还可以在连接上关闭并重新启动计算机。

创建和管理交付组中计算机的重新启动计划

> **注意：**

- 当重新启动计划应用于启用了 Autoscale™ 的交付组时，其计算机只会断电，并留待 Autoscale 开启它们。
- 当重新启动计划应用于随机单会话计算机时，这些计算机将断电而不是重新启动，以节省成本。建议您使用 Autoscale 启动计算机。
- 更改交付组上的时区可能会重新启动该交付组中的计算机。为避免这种情况，请务必在非生产时间更改时区设置。

重新启动计划指定交付组中的计算机何时定期重新启动。您可以为一个交付组创建一个或多个计划。计划可以影响：

- 组中的所有计算机。
- 组中的一台或多台（但不是全部）计算机。计算机通过您应用于计算机的标记进行标识。这称为标记限制，因为标记将操作限制为仅具有该标记的项目。

例如，假设您的所有计算机都在一个交付组中。您希望每周重新启动每台计算机一次，并希望每天重新启动会计团队使用的计算机。为此，请为所有计算机设置一个计划，并为会计部门的计算机设置另一个计划。

计划包括重新启动开始的日期和时间以及持续时间。

您可以启用或禁用计划。禁用计划在测试期间、特殊时间间隔期间或在需要之前准备计划时会很有帮助。

您不能使用计划从管理控制台进行自动开机或关机，只能用于重新启动。

计划重叠

多个计划可以重叠。在上面的示例中，两个计划都影响会计机器。这些机器可能在周日重新启动两次。调度代码旨在避免比预期更频繁地重新启动同一台机器，但这无法保证。

- 如果计划在开始时间和持续时间上精确一致，则更有可能只重新启动计算机一次。
- 计划在开始时间和持续时间上的差异越大，则越有可能发生多次重新启动。
- 受计划影响的机器数量也会影响重叠的可能性。在此示例中，影响所有机器的每周计划可能会比会计机器的每日计划更快地启动重新启动，具体取决于为每个计划指定的持续时间。

有关重新启动计划的深入了解，请参阅重新启动计划内部机制。

查看重新启动计划

1. 在左侧窗格中选择 **交付组**。

2. 选择一个组，然后单击操作栏中的 **编辑**。
3. 选择 **重新启动计划** 页面。

重新启动计划 页面包含每个已配置计划的以下信息：

- 计划名称
- 使用的标记限制（如果有）
- 计算机重新启动的频率
- 计算机用户是否收到通知
- 计划是否已启用

添加（应用）标签

配置使用标记限制的重新启动计划时，请确保已将标记添加到受计划影响的计算机。在上面的示例中，会计团队使用的每台计算机都应用了一个标记。有关详细信息，请参阅标记。

尽管您可以将多个标签应用到一台计算机，但重新启动计划只能指定一个标签。

1. 在左侧窗格中选择 **交付组**。
2. 选择包含由计划控制的计算机的组。
3. 单击 **查看计算机**，然后选择要添加标签的计算机。
4. 在操作栏中单击 **管理标签**。
5. 如果标签已存在，请选中标签名称旁边的复选框。如果标签不存在，请单击 **创建**，然后指定标签的名称。创建标签后，选中新创建的标签名称旁边的复选框。
6. 在 **管理标签** 对话框中单击 **保存**。

创建重新启动计划

> **注意：**
>
> 重新启动计划可应用于所有电源管理和非电源管理的多会话计算机。

1. 在左侧窗格中选择 **交付组**。
2. 选择一个组，然后单击操作栏中的 **编辑**。
3. 在 **重新启动计划** 页面上，单击 **添加**。
4. 在**添加重新启动计划**页面上：

- 要启用此计划，请选择**是**。要禁用此计划，请选择**否**。
- 键入计划名称和描述。
- 对于**限制为标签**，应用标签限制。
- 对于**包括维护模式下的计算机**，选择是否在此计划中包括处于维护模式的计算机。要改用 PowerShell，请参阅维护模式下计算机的计划重新启动。
- 对于**重新启动频率**，选择重新启动发生的频率：每天、每周、每月或一次。如果选择**每周**或**每月**，可以指定一个或多个特定日期。
- 对于**重复间隔**，指定希望计划运行的频率。
- 对于**开始日期**，指定计划首次发生的开始日期。
- 对于**开始重新启动时间**，以 24 小时制格式指定一天中开始重新启动的时间。
  - 对于**重新启动持续时间**：
  - 要强制重新启动具有无响应会话的计算机，请选择**强制重新启动**，然后选择以下选项之一：
    - **立即重新启动所有计算机**
    - **在一段时间内重新启动所有计算机**，并通过**小时**或**分钟**指定时间。
  - 要在重新启动前等待所有会话耗尽，请选择**正常重新启动**。

    启动配置为使用平稳重启的重启计划时：
    - 属于交付组的所有空闲计算机将立即重新启动。
    - 属于具有一个或多个活动会话的交付组的每台计算机将在所有会话注销后重新启动。

    > **注意：**
    >
    > 平稳重启计划只能重启电源管理的计算机。

- 在**向用户发送通知**中，确定是否在重启开始前在适用的计算机上显示通知消息。默认情况下，不显示任何消息。
- 如果您选择在重启开始前 15 分钟显示消息，则可以选择在初始消息显示后每五分钟重复一次该消息。默认情况下，消息不重复。
- 输入通知标题和文本。没有默认文本。

如果您希望消息包含重启倒计时，请包含变量 **%m%**。除非您选择同时重启所有计算机，否则消息将在重启前的适当时间显示在每台计算机上。

5. 单击**完成**以应用更改并关闭**添加重启计划**窗口。
6. 单击 **应用** 以应用所做的更改并保持窗口打开。或者，单击 **保存** 以应用更改并关闭窗口。

排空后重新启动

使用 PowerShell 创建或更新计算机重新启动计划时（`New-BrokerRebootSchedulev2` 或 `Set-BrokerRebootSchedulev2`），可以使用另一个重新启动持续时间值。

使用 `-UseNaturalReboot <Boolean>` 参数启用排空后重新启动功能时，所有计算机将在排空所有会话后重新启动。当达到重新启动时间时，计算机将进入排空状态，然后在所有会话注销后重新启动。

此功能支持包含单会话或多会话计算机的交付组。您可以将此选项用于已进行电源管理的计算机以及未进行电源管理的计算机。

在本地环境中，此功能仅在使用 PowerShell 时受支持。Web Studio 中不提供此功能。

编辑、删除、启用或禁用重新启动计划

1. 在左侧窗格中选择**交付组**。
2. 选择一个组，然后单击操作栏中的 **编辑**。
3. 在**重新启动计划**页面上，选中某个计划的复选框。
   - 要编辑计划，请单击**编辑**。根据创建重新启动计划中的指导更新计划配置。
   - 要启用或禁用计划，请单击**编辑**。选中或清除**启用重新启动计划**复选框。
   - 要删除计划，请单击**删除**。确认删除。删除计划不会影响应用于受影响计算机中任何计算机的标记。

由于数据库中断，计划的重新启动延迟

> **注意：**
>
> 此功能仅在 PowerShell 中可用。
>
> 如果在交付组中计算机 (VDA) 的计划重新启动开始之前发生站点数据库中断，则重新启动将在中断结束时开始。这可能会导致意外结果。

例如，假设您已将交付组的重新启动计划为在非生产时间（从 03:00 开始）进行。在计划重新启动开始前一小时（02:00）发生站点数据库中断。中断持续六小时（直到 08:00）。当 Delivery Controller 与站点数据库之间的连接恢复时，重新启动计划开始。VDA 重新启动现在比原始计划晚了五个小时，导致 VDA 在生产时间内重新启动。

为避免这种情况，您可以将 `MaxOvertimeStartMins` 参数用于 `New-BrokerRebootScheduleV2` 和 `Set-BrokerRebootScheduleV2` cmdlet。该值指定重启计划可以在计划开始时间之后开始的最大分钟数。

- 如果在此时间（计划时间 + `MaxOvertimeStartMins`）内恢复数据库连接，则 VDA 重启开始。
- 如果在此时间内未恢复数据库连接，则 VDA 重启不会开始。
- 如果省略此参数或其值为零，则无论中断持续时间如何，计划重启都会在数据库连接恢复时开始。

有关详细信息，请参阅 cmdlet 帮助。此功能仅在 PowerShell 中可用。在 Web Studio 中配置重新启动计划时，无法设置此值。

维护模式下计算机的计划重启

> **注意：**
>
> 此功能仅在 PowerShell 中可用。Citrix Virtual Apps and Desktops™ 7 2006 及更高版本支持选项 `IgnoreMaintenanceMode`。
>
> 要指示重新启动计划是否影响处于维护模式的计算机，请将 `IgnoreMaintenanceMode` 选项与 `BrokerRebootScheduleV2` cmdlet 结合使用。

例如，以下 cmdlet 创建一个重新启动处于维护模式的计算机（以及不处于维护模式的计算机）的计划。

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup>
-IgnoreMaintenanceMode $true
```

以下 cmdlet 修改现有重启计划。

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

有关详细信息，请参阅 cmdlet 帮助。此功能仅在 PowerShell 中可用。

启用一次性重新启动计划

如果要使用 PowerShell 启用一次性重启计划，请使用以下 `BrokerCatalogRebootSchedule` PowerShell 命令来创建、修改和删除重启计划：

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- 移除-代理目录重启计划
- 重命名-代理目录重启计划

限制：

- 与未配置时区的目录关联的目录重新启动计划已创建，但未启动。
- 创建目录重新启动计划后，该重新启动计划仅在属于交付组的目录 VM 上运行。

示例，

- 创建名为 **BankTellers** 的目录中 VM 的重启计划，该计划于 Feb 3, 2022 上午 2 点至上午 4 点之间开始。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -CatalogName
BankTellers  -StartDate "2022-02-03" -StartTime "02:00" -Enabled $true
-RebootDuration 120
```

- 创建目录中UID为17的VM的重启计划，于 Feb 3, 2022 凌晨1点至5点之间开始。在重启前十分钟，每台VM都会在每个用户会话中显示一个消息框，标题为 **警告：即将重启**，消息内容为 **保存您的工作**。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot'
-CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -Enabled
$true -RebootDuration 240 -WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
```

- 将名为 **Old Name** 的目录重启计划重命名为 **New Name**。

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName
"New Name"
```

- 显示所有 UID 为 1 的目录重启计划，然后将 UID 为 1 的目录重启计划重命名为 **New Name**。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- 将名为 **Accounting** 的目录重启计划设置为在每台VM重启前十分钟显示标题为 **警告：即将重启**，消息内容为 **保存您的工作** 的消息。该消息将显示在该VM的每个用户会话中。

```
C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage
"Save your work" -WarningDuration 10 -WarningTitle "WARNING: Reboot
pending"
```

- 显示所有已禁用的重启计划，然后启用所有已禁用的重启计划。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
BrokerCatalogRebootSchedule -Enabled $true
```

- 将UID为17的目录重启计划设置为在每台VM重启前十五、十和五分钟显示消息 **%m% 分钟后重启**。

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
%m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
```

- 配置名为 **MyCatalog** 的目录的时区。

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone &lt;TimeZone>
```

交付组中的计算机电源管理

您只能对虚拟单会话操作系统计算机进行电源管理，而不能对物理计算机（包括远程PC访问计算机）进行电源管理。具有GPU功能的单会话操作系统计算机无法暂停，因此关机操作会失败。对于多会话操作系统计算机，您可以创建重启计划。

在包含池化计算机的交付组中，虚拟单会话操作系统计算机可以处于以下状态之一：

- 随机分配且正在使用
- 未分配且未连接

在包含静态计算机的交付组中，虚拟单会话操作系统计算机可以：

- 永久分配且正在使用

- 永久分配且未连接（但已就绪）
- 未分配且未连接

在正常使用期间，静态交付组通常包含永久分配的计算机和未分配的计算机。最初，所有计算机都未分配，除非在创建交付组时手动分配。随着用户连接，计算机将永久分配。您可以完全电源管理这些交付组中的未分配计算机，但只能部分管理永久分配的计算机。

- **池和缓冲区：** 对于池交付组和包含未分配计算机的静态交付组，池（在此情况下）是一组处于开机状态的未分配或临时分配的计算机，可供用户连接。用户登录后会立即获得一台计算机。池大小（保持开机状态的计算机数量）可按一天中的时间进行配置。对于静态交付组，请使用 SDK 配置池。

  缓冲区是额外的备用未分配计算机集，当池中的计算机数量低于阈值时会开启。阈值是交付组大小的百分比。对于大型交付组，当超过阈值时，可能会开启大量计算机。因此，请仔细规划交付组大小，或使用 SDK 调整默认缓冲区大小。
- **电源状态计时器：** 您可以使用电源状态计时器在用户断开连接指定时间后挂起计算机。例如，如果用户断开连接至少 10 分钟，则计算机在办公时间之外会自动挂起。

  您可以为工作日和周末以及高峰和非高峰时段配置计时器。
- **永久分配计算机的部分电源管理：** 对于永久分配的计算机，您可以设置电源状态计时器，但不能设置池或缓冲区。计算机在每个高峰期开始时开启，并在每个非高峰期开始时关闭。您无法像管理未分配计算机那样对可用计算机的数量进行精细控制，以弥补已消耗的计算机。

电源管理虚拟单会话操作系统计算机

1. 在左侧窗格中选择**交付组**。
2. 选择一个组，然后在操作栏中单击**编辑交付组**。
3. 在**电源管理**页面上，在**电源管理计算机**中选择**工作日**。默认情况下，工作日为周一至周五。
4. 对于随机交付组，在**要开机的计算机**中，单击**编辑**，然后指定工作日期间的池大小。然后，选择要开机的计算机数量。
5. 在**高峰时段**中，设置每天的高峰和非高峰时段。
6. 设置工作日期间高峰和非高峰时段的电源状态计时器：在**高峰时段 > 断开连接时**，指定在挂起交付组中任何断开连接的计算机之前的延迟（以分钟为单位），然后选择**挂起**。在**非高峰时段 > 断开连接时**，指定在关闭交付组中任何已注销的计算机之前的延迟，然后选择**关机**。此计时器不适用于包含随机计算机的交付组。
7. 在**电源管理计算机**中选择**周末**，然后配置周末的高峰时段和电源状态计时器。
8. 单击“**应用**”以应用所做的任何更改并保持窗口打开。或者，单击“**保存**”以应用更改并关闭窗口。

使用 SDK 执行以下操作：

- 响应电源状态计时器时关闭（而不是挂起）计算机，或者，如果您希望计时器基于注销而不是断开连接。
- 更改默认工作日和周末定义。
- 禁用电源管理。请参阅 CTX217289。

电源管理在会话断开连接的情况下转换到不同时间段的 VDI 计算机

> **重要提示：**
>
> 此增强功能仅适用于会话已断开连接的 VDI 计算机。它不适用于会话已注销的 VDI 计算机。

> 在早期版本中，VDI 计算机转换到需要执行操作（断开连接操作 =“**挂起**”或“**关机**”）的时间段时，会保持开机状态。如果计算机在不需要执行任何操作（断开连接操作 =“**无**”）的时间段（高峰或非高峰时段）断开连接，则会发生此情况。

从 Citrix Virtual Apps and Desktops 7 1909 开始，当指定的断开连接时间过去后，计算机将挂起或关机，具体取决于为目标时间段配置的断开连接操作。

例如，为 VDI 交付组配置以下电源策略：

- 将 `PeakDisconnectAction` 设置为“无”
- 将 `OffPeakDisconnectAction` 设置为“关机”
- 将 `OffPeakDisconnectTimeout` 设置为“10”

有关电源策略中断开连接操作的详细信息，请参阅 https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy 和 https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/。

在早期版本中，会话在高峰时段断开连接的 VDI 计算机在从高峰时段转换到非高峰时段时会保持开机状态。从 Citrix Virtual Apps and Desktops 7 1909 开始，在时段转换时，`OffPeakDisconnectAction` 和 `OffPeakDisconnectTimeout` 策略操作将应用于 VDI 计算机。因此，计算机在转换到非高峰时段 10 分钟后会关机。

如果您想恢复到以前的行为（即，对从高峰期过渡到非高峰期或从非高峰期过渡到高峰期且会话已断开连接的计算机不采取任何操作），请执行以下操作之一：

- 将 `LegacyPeakTransitionDisconnectedBehaviour` 注册表值设置为 `1`，这相当于 *true*，可启用以前的行为。默认情况下，该值为 `0` 或 *false*，这会在周期转换时触发断开连接电源策略操作。
  - 路径：`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - 名称: `LegacyPeakTransitionDisconnectedBehaviour`
  - 类型: `REG_DWORD`
  - 数据: `0x00000001 (1)`
- 使用 `Set-BrokerServiceConfigurationData` PowerShell 命令配置设置。例如：
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

在周期转换时对其应用电源策略操作之前，计算机必须满足以下条件：

- 具有断开连接的会话。
- 没有待处理的电源操作。
- 属于过渡到不同时间段的 VDI（单会话）交付组。
- 具有在特定时间段（高峰期或非高峰期）断开连接并过渡到分配了电源操作的期间的会话。

更改目录中处于通电状态的 VDA 百分比

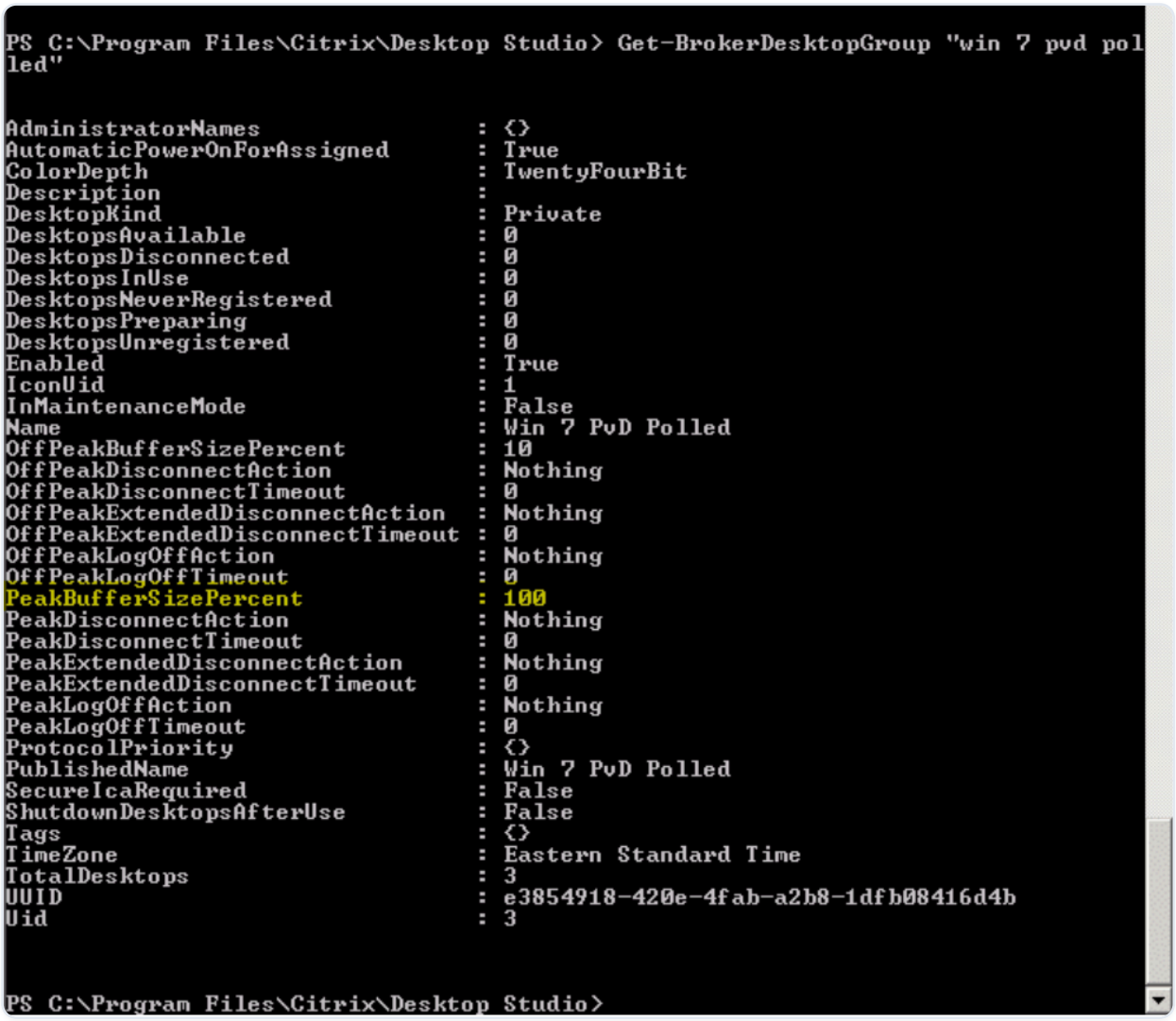
1. 从交付组的“**电源管理**”部分调整交付组的高峰时段。
2. 记下桌面组名称。
3. 使用管理员权限启动 PowerShell 并运行以下命令。将“Desktop Group Name”替换为您的桌面组名称，该桌面组的正在运行的 VDA 百分比已更改。

   ```
   asnp Citrix*
   ```

   ```
   # Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100
   ```

   值为 100 表示 100% 的 VDA 处于就绪状态。
4. 通过运行以下命令验证解决方案：

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```



更改可能需要长达一小时才能生效。

要在用户注销后关闭 VDA，请输入：

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

要在高峰时段重新启动 VDA，以便在用户注销后它们可供用户使用，请输入：

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

会话

- 注销或断开会话，或向用户发送消息
- 配置会话预启动和会话保留
- 控制维护模式下从计算机断开连接时的会话重新连接
- 配置会话漫游

注销或断开会话

1. 在左侧窗格中选择**交付组**。
2. 选择一个交付组，然后在操作栏中选择**查看计算机**。
3. 在中间窗格中，选择计算机，然后在操作栏中选择**查看会话**，然后选择一个会话。
   - 或者，在中间窗格中，选择**会话**选项卡，然后选择一个会话。
4. 要注销会话，请在操作栏中选择**注销**。会话将关闭，用户将注销。除非计算机分配给特定用户，否则它将可供其他用户使用。
5. 要断开会话，请在操作栏中选择**断开连接**。应用程序将继续在该会话中运行，并且计算机仍分配给该用户。用户可以重新连接到同一台计算机。

您可以为单会话操作系统计算机配置电源状态计时器，以自动处理未使用的会话。有关详细信息，请参阅电源管理计算机。

向交付组发送消息

1. 在左侧窗格中选择**交付组**。
2. 选择一个交付组，然后在操作栏中选择**查看计算机**。
3. 在中间窗格中，选择要向其发送消息的计算机。
4. 在操作栏中，选择 **查看会话**。
5. 在中间窗格中，选择所有会话，然后在操作栏中选择 **发送消息**。
6. 键入您的消息，然后单击 **确定**。如果需要，可以指定严重性级别。选项包括 **严重**、**问题**、**警告** 和 **信息**。

此外，您还可以使用 Citrix Director 发送消息。有关详细信息，请参阅向用户发送消息。

在交付组中配置会话预启动和会话保持

这些功能仅在多会话操作系统计算机上受支持。

会话预启动和会话保留功能通过在请求会话之前启动会话（会话预启动）以及在用户关闭所有应用程序后保持应用程序会话处于活动状态（会话保留）来帮助指定用户快速访问应用程序。

默认情况下，不使用会话预启动和会话保持。当用户启动应用程序时，会话会启动，并保持活动状态，直到会话中最后一个打开的应用程序关闭。

注意事项：

- 交付组必须支持应用程序，并且计算机必须运行适用于多会话操作系统的 VDA，最低版本为 7.6。

- 这些功能仅在使用适用于 Windows 的 Citrix Workspace 应用程序时受支持，并且还需要额外的 Citrix Workspace 应用程序配置。有关说明，请在适用于您的 Windows 版 Citrix Workspace 应用程序的产品文档中搜索“会话预启动”。
- 不支持适用于 HTML5 的 Citrix Workspace 应用程序。
- 使用会话预启动时，如果用户的计算机进入挂起或休眠模式，则预启动不起作用（无论会话预启动设置如何）。用户可以锁定其计算机/会话。但是，如果用户从 Citrix Workspace 应用程序注销，则会话将结束，并且预启动不再适用。
- 使用会话预启动时，物理客户端计算机无法使用挂起或休眠电源管理功能。客户端计算机用户可以锁定其会话，但不得注销。
- 预启动和保留会话会占用并发许可证，但仅在连接时占用。如果使用用户/设备许可证，则许可证有效期为 90 天。默认情况下，未使用的预启动和保留会话会在 15 分钟后断开连接。此值可以在 PowerShell 中配置（`New/Set-BrokerSessionPreLaunch` cmdlet）。
- 仔细规划和监控用户的活动模式对于调整这些功能以使其相互补充至关重要。最佳配置可在为用户提供更早的应用程序可用性优势与保持许可证使用和资源分配的成本之间取得平衡。
- 您还可以在 Citrix Workspace 应用程序中为预定时间配置会话预启动。

未使用的预启动和会话保留会话保持活动状态的时长

有多种方法可以指定如果用户未启动应用程序，未使用的会话保持活动状态的时长：配置的超时和服务器负载阈值。您可以配置所有这些。首先发生的事件会导致未使用的会话结束。

- **超时：** 配置的超时指定未使用的预启动或会话保留会话保持活动状态的分钟数、小时数或天数。如果配置的超时时间过短，预启动会话将在为用户提供更快应用程序访问的优势之前结束。如果配置的超时时间过长，则传入的用户连接可能会被拒绝，因为服务器没有足够的资源。

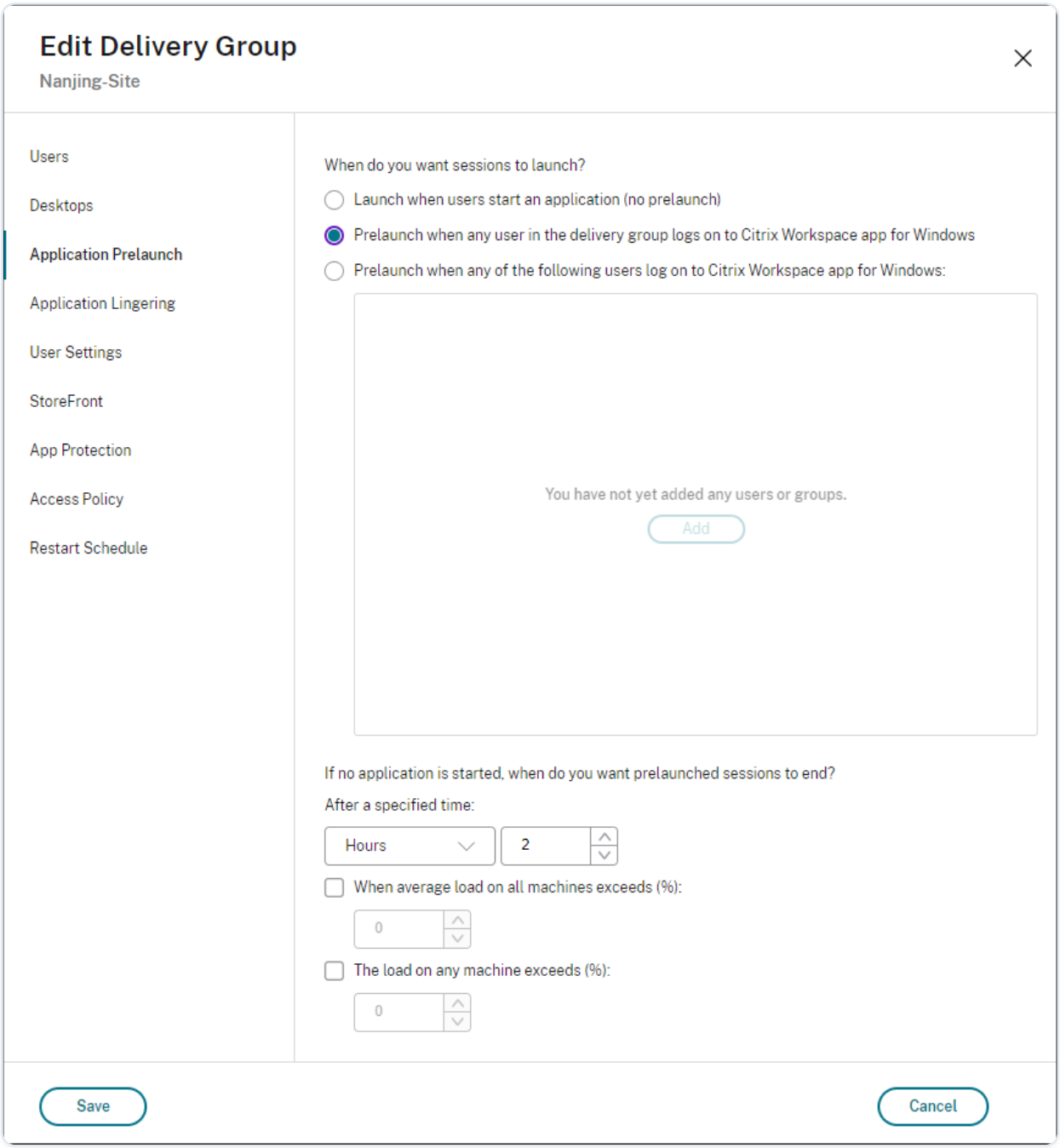
  您只能通过 SDK 启用此超时 (`New/Set-BrokerSessionPreLaunch` cmdlet)，而不能通过管理控制台启用。如果禁用超时，则它不会显示在该交付组的控制台显示中或“**编辑交付组**”页面中。
- **阈值：** 根据服务器负载自动结束预启动和会话保留会话可确保会话尽可能长时间保持打开状态，前提是服务器资源可用。未使用的预启动和会话保留会话不会导致连接被拒绝，因为当新用户会话需要资源时，它们会自动结束。

  您可以配置两个阈值：交付组中所有服务器的平均负载百分比，以及组中单个服务器的最大负载百分比。当超过阈值时，处于预启动或会话保留状态时间最长的会话将结束。会话将以分钟为间隔逐个结束，直到负载降至阈值以下。当超过阈值时，不会启动新的预启动会话。

未向 Controller 注册 VDA 的服务器以及处于维护模式的服务器被视为已满载。计划外中断会导致预启动和会话保留会话自动结束以释放容量。

启用会话预启动

1. 选择一个组，然后在操作栏中单击 **编辑交付组**。
2. 在**应用程序预启动**页面上，通过选择会话启动时间来启用会话预启动：
   - 当用户启动应用程序时。这是默认设置。会话预启动已禁用。
   - 当交付组中的任何用户登录到适用于 Windows 的 Citrix Workspace 应用程序时。
   - 当用户和用户组列表中的任何人登录到适用于 Windows 的 Citrix Workspace 应用程序时。如果选择此选项，请务必同时指定用户或用户组。



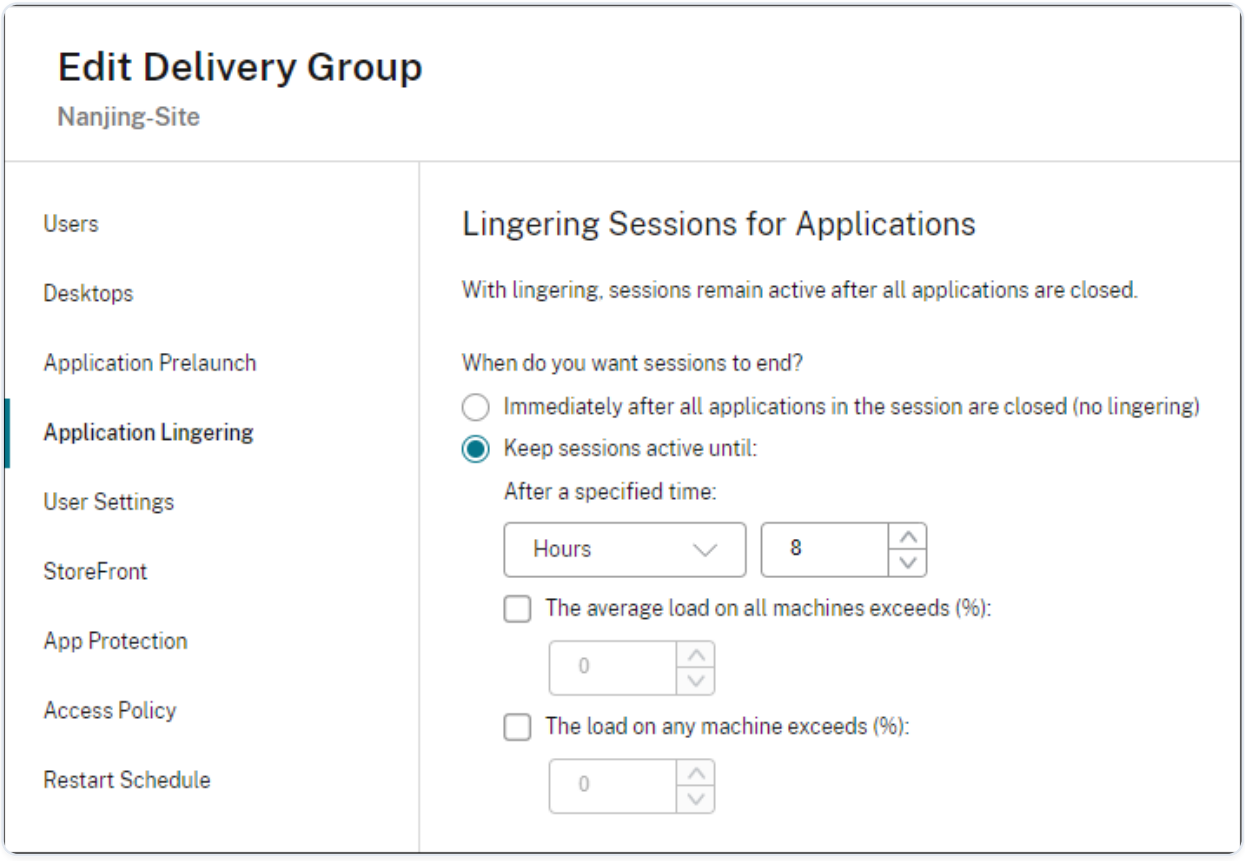
3. 当用户启动应用程序时，预启动会话将替换为常规会话。如果用户未启动应用程序（预启动会话未使用），则以下设置会影响该会话保持活动状态的时间。

- 当指定的时间间隔过去时。您可以更改时间间隔（1-99 天、1-2376 小时或 1-142,560 分钟）
- 当交付组中所有计算机的平均负载超过指定百分比 (1–99%) 时
- 当交付组中任何计算机的负载超过指定百分比 (1–99%) 时

总结：预启动会话将保持活动状态，直到发生以下事件之一：用户启动应用程序、指定时间过去或超过指定的负载阈值。

启用会话延迟

1. 在左侧窗格中选择 **交付组**。
2. 选择一个组，然后在操作栏中单击 **编辑交付组**。
3. 在**应用程序延迟**页面上，通过选择**保持会话活动直到**来启用会话延迟。



4. 如果用户未启动其他应用程序，则有多个设置会影响滞留会话保持活动状态的时长。

- 当指定的时间间隔过去时。您可以更改时间间隔：1–99 天、1–2376 小时或 1–142,560 分钟。
- 当交付组中所有计算机的平均负载超过指定百分比时：1–99%。
- 当交付组中任何计算机的负载超过指定百分比时：1–99%。

总结：滞留会话保持活动状态，直到发生以下事件之一：用户启动应用程序、指定时间过去或超过指定负载阈值。

控制维护模式下从计算机断开连接时的会话重新连接

> **注意：**
>
> 此功能仅在 PowerShell 中可用。

> 您可以控制在维护模式下从计算机断开连接的会话是否允许重新连接到交付组中的计算机。

在 2106 版本之前，对于已从维护模式下的计算机断开连接的单会话池桌面会话，不允许重新连接。从 2106 版本开始，您可以配置交付组以允许或禁止在从维护模式下的计算机断开连接后重新连接（无论会话类型如何）。

创建或编辑交付组时（`New-BrokerDesktopGroup`，`Set-BrokerDesktopGroup`），使用 `-AllowReconnectInMaintenanceMode <boolean>` 参数来允许或禁止从维护模式下的计算机断开连接的计算机重新连接。

- 当设置为 true 时，会话可以重新连接到组中的计算机。
- 当设置为 false 时，会话无法重新连接到组中的计算机。

默认值：

- 单会话：已禁用
- 多会话：已启用

配置会话漫游

默认情况下，交付组会启用会话漫游。会话会随用户在客户端设备之间漫游。当用户启动会话然后移动到另一台设备时，将使用相同的会话，并且应用程序在两台设备上同时可用。您可以在多台设备上查看应用程序。无论设备如何或是否存在当前会话，应用程序都会跟随。通常，分配给应用程序的打印机和其他资源也会跟随。或者，您可以使用 PowerShell。有关详细信息，请参阅会话漫游。

为应用程序配置会话漫游

要为应用程序配置会话漫游，请执行以下步骤：

1. 在控制台中，选择左侧窗格中的**交付组**。
2. 选择一个组，然后在操作栏中选择**编辑交付组**。

3. 在**用户**页面上，选中**会话随用户在设备之间移动而漫游**复选框以启用会话漫游。
    - 启用后，如果用户启动应用程序会话然后移动到另一台设备，则使用相同的会话并在两台设备上可用。禁用后，会话不再在设备之间漫游。
4. 选择**确定**以应用更改并关闭窗口。

配置桌面会话漫游

要为桌面配置会话漫游，请执行以下步骤：

1. 在控制台中，选择左侧窗格中的**交付组**。
2. 选择一个组，然后在操作栏中选择**编辑**。
3. 在 **桌面** 页面上，选择桌面，然后选择 **编辑**。
4. 选中**会话漫游**复选框以启用会话漫游。

- 启用后，如果用户启动桌面然后移动到另一台设备，则会使用相同的会话，并且应用程序在两台设备上都可用。禁用后，会话将不再在设备之间漫游。

选择 **确定** 以应用更改并关闭窗口。

应用程序

查看应用程序并将其添加到交付组。

1. 在控制台中，选择左侧窗格中的**交付组**。
2. 选择一个组。如果此组包含应用程序，则操作栏中会显示 **查看应用程序**。
3. 选择 **查看应用程序**。您将转到 **应用程序** 节点，其中显示此组中所有可用的应用程序。
4. 要向此组添加更多应用程序，请转到 **交付组** 节点，选择该组，然后在操作栏中选择 **添加应用程序**。

从 VDA 上的 Citrix Secure Access™ 客户端无缝登录

您可以从 VDA 上的 Citrix Secure Access (CSA) 客户端使用单点登录 (SSO) 无缝登录到 Citrix Workspace，以访问 Citrix Secure Private Access。此功能适用于单会话和多会话 VDA。

实现此目的的步骤如下：

1. 编辑现有交付组以启用 SPA SSO。例如，

```
Set-BrokerDesktopGroup -Name &lt;String> -SpaSsoEnabled 1
```

2. 使用 Get -BrokerDesktopGroup PowerShell 命令检查交付组的 SPA SSO 状态。例如：

```
Get-BrokerDesktopGroup -Name &lt;String> -property 'SpaSsoEnabled'
```

3. 在 SPA 中，创建应用程序和策略。请参阅配置 TCP/UDP 应用程序和配置应用程序的访问策略。
4. 通过 RDP 连接到单会话或多会话 VDA 并安装最新的 CSA 代理。
5. 打开 Citrix Workspace 并登录到单会话或多会话 VDA。

故障排除

- 未向 Delivery Controller 注册的 VDA 在启动代理会话时不会被考虑。这会导致原本可用的资源利用率不足。VDA 未注册的原因有很多，其中许多管理员都可以进行故障排除。详细信息显示在目录创建向导中以及将目录添加到交付组后提供故障排除信息。

  创建交付组后，交付组的详细信息窗格会指示可以注册但未注册的计算机数量。例如，一台或多台计算机已开机且未处于维护模式，但当前未向 Controller 注册。查看“未注册但应注册”的计算机时，请查看详细信息窗格中的**故障排除**选项卡，以了解可能的原因和建议的纠正措施。

  有关功能级别消息，请参阅VDA 版本和功能级别。

  有关 VDA 注册故障排除的信息，请参阅CTX136668。
- 在交付组的显示中，详细信息窗格中的 **已安装的 VDA 版本** 可能与计算机上安装的实际版本不同。计算机的 Windows 程序和功能显示屏会显示实际的 VDA 版本。
- 对于状态为 **电源状态未知** 的计算机，请参阅 CTX131267 以获取指导。

创建应用程序组

注意：

从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

简介

应用程序组允许您管理应用程序集合。为跨不同交付组共享的应用程序创建应用程序组。或者，为交付组中由部分用户使用的应用程序创建应用程序组。应用程序组是可选的；它们提供了一种替代

方法，无需将相同的应用程序添加到多个交付组。将交付组与多个应用程序组关联，并将应用程序组与多个交付组关联。

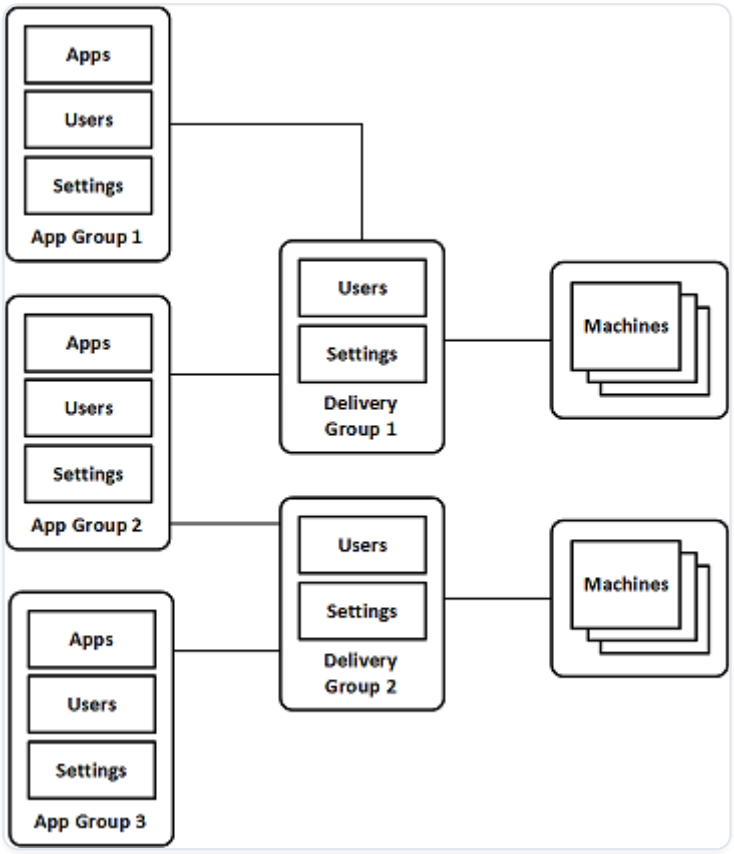
与使用更多交付组相比，使用应用程序组可以在应用程序管理和资源控制方面提供优势：

- 应用程序及其设置的逻辑分组允许您将这些应用程序作为一个单元进行管理。例如，您不必一次一个地将相同的应用程序添加到（发布到）各个交付组。
- 应用程序组之间的会话共享可以节省资源消耗。在其他情况下，禁用应用程序组之间的会话共享可能是有益的。
- 您可以使用标签限制功能从应用程序组发布应用程序，仅考虑所选交付组中的一部分计算机。通过标签限制，您可以将现有计算机用于多个发布任务，从而节省部署和管理额外计算机的成本。标签限制可以被认为是细分（或分区）交付组中的计算机。在隔离和排查交付组中一部分计算机的问题时，使用带有标签限制的应用程序组或桌面会很有帮助。

示例配置

示例 1：

下图显示了包含应用程序组的 Citrix Virtual Apps and Desktops™ 部署：



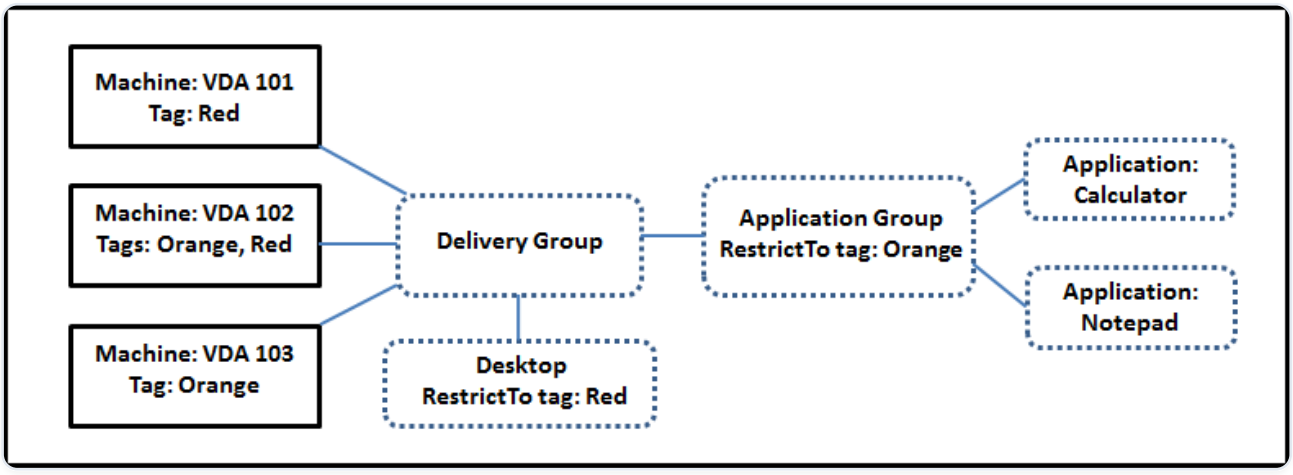
在此配置中，应用程序被添加到应用程序组，而不是交付组。交付组指定使用哪些计算机。（尽管未显示，但这些计算机位于计算机目录中。）

应用程序组 1 与交付组 1 关联。应用程序组 1 中的应用程序由应用程序组 1 中指定的用户访问。只有当这些组也位于交付组 1 的用户列表中时，它们才会出现。此配置遵循以下指导原则：应用程序组的用户列表是关联交付组用户列表的子集（一种限制）。应用程序组 1 中的设置（例如应用程序组之间的应用程序会话共享、关联的交付组）适用于该组中的应用程序和用户。交付组 1 中的设置适用于应用程序组 1 和 2 中的用户，因为这些应用程序组已与该交付组关联。

应用程序组 2 与两个交付组（1 和 2）关联。这些交付组中的每一个都在应用程序组 2 中被分配了一个优先级，指示在启动应用程序时检查交付组的顺序。优先级相同的交付组会进行负载平衡。应用程序组 2 中的应用程序由应用程序组 2 中指定的用户访问。但是，他们也必须出现在交付组 1 和交付组 2 的用户列表中。

示例 2：

这种简单的布局使用标签限制来限制哪些计算机被考虑用于某些桌面和应用程序启动。该站点有一个共享交付组、一个已发布的桌面和一个配置了两个应用程序的应用程序组。



标签已添加到三台计算机（VDA 101–103）中的每一台。

应用程序组是使用“Orange”标签限制创建的。它的每个应用程序都只在该交付组中具有“Orange”标签的计算机（VDA 102 和 103）上启动。

有关在应用程序组（以及桌面）中使用标签限制的更全面的示例和指导，请参阅标签。

指导和注意事项

Citrix 建议将应用程序添加到应用程序组或交付组，但不要同时添加到两者。否则，在两种组类型中都包含应用程序会增加复杂性，从而使其更难管理。

默认情况下，应用程序组处于启用状态。创建应用程序组后，您可以编辑该组以更改此设置。请参阅管理应用程序组。

默认情况下，应用程序组之间的应用程序会话共享处于启用状态。请参阅应用程序组之间的会话共享。

Citrix 建议将交付组升级到当前版本。此过程需要：

1. 升级交付组中使用的计算机上的 VDA。
2. 升级包含这些计算机的计算机目录。
3. 升级交付组。

有关详细信息，请参阅管理交付组。

要使用应用程序组，您的核心组件最低版本必须为 7.9。

创建应用程序组需要交付组管理员内置角色的委派管理权限。有关详细信息，请参阅委派管理。

本文指的是将应用程序“关联”到多个应用程序组。它将此操作与从可用源添加该应用程序的实例区分开来。同样，交付组与应用程序组关联，而不是彼此的附加项或组件。

与应用程序组的会话共享

启用应用程序会话共享后，所有应用程序都在同一应用程序会话中启动。这节省了启动更多应用程序会话的成本，并允许使用涉及剪贴板的应用程序功能，例如复制粘贴操作。但是，在某些情况下，您可以禁用会话共享。

使用应用程序组时，您可以通过以下三种方式配置应用程序会话共享，这些方式扩展了仅使用交付组时可用的标准会话共享行为：

- 应用程序组之间启用会话共享。
- 仅在同一应用程序组中的应用程序之间启用会话共享。
- 会话共享已禁用。

应用程序组之间的会话共享

您可以在应用程序组之间启用应用程序会话共享，也可以禁用它，将应用程序会话共享仅限于同一应用程序组中的应用程序。

- **启用应用程序组之间会话共享的有用示例：**

  应用程序组 1 包含 Microsoft Office 应用程序，例如 Word 和 Excel。应用程序组 2 包含其他应用程序，例如记事本和计算器，并且两个应用程序组都连接到同一个交付组。拥有两个应用程序组访问权限的用户通过启动 Word 来开始应用程序会话，然后启动记事本。如果控制器发现用户运行 Word 的现有会话适合运行记事本，则记事本将在现有会话中启动。如果无法从现有会话运行记事本（例如，如果标签限制排除了会话正在运行的计算机），则会在合适的计算机上创建新会话，而不是使用会话共享。

- **禁用应用程序组之间会话共享的有用示例：**

一种配置，其中一组应用程序与安装在同一台计算机上的其他应用程序无法很好地互操作。例如，同一软件套件的两个不同版本或同一 Web 浏览器的两个不同版本。您不希望允许用户在同一会话中启动这两个版本。

为软件套件的每个版本创建一个应用程序组，并将软件套件每个版本的应用程序添加到相应的应用程序组。如果这些应用程序组中的每个组都禁用了组间会话共享，则这些组中指定的用户可以在同一会话中运行相同版本的应用程序。用户仍然可以同时运行其他应用程序，但不能在同一会话中运行。当启动其中一个不同版本的应用程序，或任何不包含在应用程序组中的应用程序时，该应用程序将在新会话中启动。

此应用程序组之间的会话共享功能不是安全沙盒功能。它并非万无一失，也无法阻止用户通过其他方式（例如，通过 Windows 资源管理器）在其会话中启动应用程序。

如果计算机已满负荷，则不会在其上启动新会话。新应用程序将根据需要使用会话共享在该计算机的现有会话中启动。

您只能将预启动会话提供给允许应用程序会话共享的应用程序组。（使用会话延迟功能的会话可用于所有应用程序组。）这些功能必须在与应用程序组关联的每个交付组中启用和配置。您无法在应用程序组中配置它们。

默认情况下，在创建应用程序组时，应用程序组之间的应用程序会话共享处于启用状态。创建组时无法更改此设置。创建应用程序组后，您可以编辑该组以更改此设置。请参阅管理应用程序组。

禁用应用程序组内的会话共享

您可以阻止同一应用程序组中的应用程序之间进行应用程序会话共享。

- **禁用应用程序组内的会话共享有帮助的示例：**

  您希望用户在单独的显示器上访问应用程序的多个同时全屏会话。

  您创建一个应用程序组并向其中添加应用程序。

默认情况下，当您创建应用程序组时，应用程序会话共享处于启用状态。创建组时无法更改此设置。创建应用程序组后，您可以编辑该组以更改此设置。请参阅 管理应用程序组。

创建应用程序组

要创建应用程序组，请执行以下操作：

1. 登录 Web Studio。
2. 在左侧窗格中选择 **应用程序**，然后选择 **应用程序组** 选项卡。

3. 要使用文件夹组织应用程序组，请在**应用程序组**根文件夹下创建文件夹。有关详细信息，请参阅使用文件夹组织应用程序组。
4. 选择要创建组的文件夹，然后单击“**创建应用程序组**”。组创建向导将启动并显示“**简介**”页面。您可以从该向导的未来启动中删除此页面。
5. 按照向导在以下页面上配置设置。完成每个页面后，选择“**下一步**”，直到到达“**摘要**”页面。

步骤 1. 交付组

“**交付组**”页面列出了所有交付组，以及每个组包含的计算机数量。

- “**兼容交付组**”列表包含您可以选择的交付组。兼容交付组包含随机（非永久或静态分配）多会话或单会话操作系统计算机。
- “**不兼容交付组**”列表包含您无法选择的交付组。每个条目都解释了其不兼容的原因，例如包含静态分配的计算机。

应用程序组可以与包含可交付应用程序的共享（非专用）计算机的交付组关联。

如果满足以下两个条件，您还可以选择包含仅交付桌面的共享计算机的交付组：

- 交付组包含共享计算机，并且是使用早于 7.9 版本的 XenDesktop 创建的。
- 您具有“编辑交付组”权限。

提交应用程序组创建向导时，交付组类型会自动转换为“桌面和应用程序”。

尽管您可以创建一个没有关联交付组的应用程序组（可能用于组织应用程序或用作当前未使用的应用程序的存储），但该应用程序组在指定至少一个交付组之前无法用于交付应用程序。此外，如果未指定交付组，则无法从“**从‘开始’菜单**”源向应用程序组添加应用程序。

您选择的交付组指定用于交付应用程序的计算机。选中要与应用程序组关联的交付组旁边的复选框。

要添加标记限制，请选择“**将启动限制为具有该标记的计算机**”，然后从下拉列表中选择该标记。

步骤 2. 用户

在应用程序组中指定应用程序用户。可以允许上一页中选择的交付组中的所有用户和用户组，也可以从这些交付组中选择特定的用户和用户组。如果将使用限制为指定用户，则只有交付组中指定的用户（即应用程序组）才能访问此组中的应用程序。本质上，应用程序组中的用户列表提供了对交付组中用户列表的筛选。

启用或禁用未经身份验证的用户使用应用程序仅在交付组中可用，而不在应用程序组中可用。

有关部署中指定用户列表的位置的信息，请参阅 指定用户列表的位置。

步骤 3. 应用程序

须知：

- 默认情况下，您添加的新应用程序将放置在名为“**应用程序**”的文件夹中。您可以指定其他文件夹。如果您尝试添加应用程序，并且该文件夹中已存在同名应用程序，系统会提示您重命名要添加的应用程序。如果您同意建议的唯一名称，则会以该新名称添加应用程序。否则，您必须自行重命名才能添加。有关详细信息，请参阅管理应用程序文件夹。
- 您可以在添加应用程序时或之后更改其属性（设置）。请参阅更改应用程序属性。如果您向同一用户发布两个同名应用程序，请在 Web Studio 中更改“**应用程序名称（面向用户）**”属性。否则，用户会在 Citrix Workspace 应用程序中看到重复的名称。
- 当您将应用程序添加到多个应用程序组时，如果您没有足够的权限在所有这些组中查看该应用程序，则可能会出现可见性问题。在这种情况下，请咨询具有更高权限的管理员，或者扩展您的范围以包括添加了该应用程序的所有组。

单击下拉菜单中的“**添加**”以显示应用程序源。

- **从“开始”菜单：** 在所选交付组中的计算机上发现的应用程序。选择此源时，将启动一个新页面，其中包含发现的应用程序列表。选中要添加的应用程序的复选框，然后单击“**确定**”。

  如果选择了以下任何一项，则无法选择此源：

  - 没有关联交付组的应用程序组。
  - 关联交付组中不包含任何计算机的应用程序组。
  - 不包含任何计算机的交付组。

- **手动定义：** 位于站点中或网络其他位置的应用程序。选择此源时，将启动一个新页面，您可以在其中键入可执行文件的路径、工作目录、可选命令行参数以及管理员和用户的显示名称。输入此信息后，单击“**确定**”。
- **现有：** 以前添加到站点的应用程序。选择此源时，将启动一个新页面，其中包含发现的应用程序列表。选中要添加的应用程序的复选框，然后单击“**确定**”。如果站点没有应用程序，则无法选择此源。
- **App-V：** App-V 软件包中的应用程序。选择此源时，将启动一个新页面，您可以在其中选择“**App-V 服务器**”或“**应用程序库**”。在结果显示中，选中要添加的应用程序的复选框，然后单击“**确定**”。有关详细信息，请参阅部署和交付 App-V 应用程序。如果未为站点配置 App-V，则无法选择此源（或可能不显示）。

如前所述，如果不存在该类型的有效源，则“**添加**”下拉菜单中的某些条目将不可选。不兼容的源根本不会列出（例如，您不能将应用程序组添加到应用程序组，因此在创建应用程序组时不会列出该源）。

步骤 4. 作用域

此页面仅在您之前创建了自定义作用域时显示。默认情况下，将选择**所有**作用域。有关详细信息，请参阅委派管理。

步骤 5. 摘要

输入应用程序组的名称。您还可以（可选）输入描述。

查看摘要信息，然后单击**完成**。

管理应用程序组

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

简介

本文介绍如何管理您创建的应用程序组。

有关在应用程序组或交付组中管理应用程序的信息，请参阅应用程序，包括如何：

- 在应用程序组中添加或删除应用程序。
- 更改应用程序组关联。

管理应用程序组需要交付组管理员内置角色的委派管理权限。有关详细信息，请参阅委派管理。

启用或禁用应用程序组

启用应用程序组后，它可以交付已添加到其中的应用程序。禁用应用程序组会禁用该组中的每个应用程序。但是，如果这些应用程序也与其他已启用的应用程序组关联，则可以从其他组交付这些应用程序。如果应用程序已明确添加到与应用程序组关联的交付组中，则禁用应用程序组不会影响这些交付组中的应用程序。

创建应用程序组时，该组处于启用状态。创建组时无法更改此配置。

1. 在左侧窗格中选择**应用程序**，然后选择**应用程序组**选项卡。
2. 选择一个应用程序组，然后在操作栏中选择**编辑应用程序组**。

3. 在**设置**页面上，选中或清除**启用应用程序组**复选框。
4. 单击**应用**以保持窗口打开，或单击**保存**以应用更改并关闭窗口。

启用或禁用应用程序组之间的应用程序会话共享

应用程序组之间的会话共享在创建应用程序组时启用。创建组时无法更改此配置。有关详细信息，请参阅与应用程序组共享会话。

1. 在左侧窗格中选择**应用程序**，然后选择**应用程序组**选项卡。
2. 选择一个应用程序组，然后在操作栏中选择**编辑应用程序组**。
3. 在**设置**页面上，选中或清除**启用应用程序组之间的应用程序会话共享**复选框。
4. 单击**应用**以保持窗口打开，或单击**保存**以应用更改并关闭窗口。

禁用应用程序组内的应用程序会话共享

在创建应用程序组时，同一应用程序组中应用程序之间的会话共享默认启用。如果禁用应用程序组之间的应用程序会话共享，则同一应用程序组中应用程序之间的会话共享仍保持启用状态。

您可以使用 PowerShell SDK 配置应用程序组，使其包含的应用程序之间禁用应用程序会话共享。在某些情况下，此选项是可取的。例如，您可能希望用户在单独的显示器上以全尺寸应用程序窗口启动非无缝应用程序。

当您禁用应用程序组内的应用程序会话共享时，该组中的每个应用程序都会在新应用程序会话中启动。如果存在运行相同应用程序的合适断开连接会话，则会重新连接该会话。例如，当启动记事本时，如果存在运行记事本的断开连接会话，则会重新连接该会话，而不是创建新会话。当存在多个合适的断开连接会话时，会以随机但确定性的方式选择其中一个会话进行重新连接。当在相同情况下再次出现此情况时，会选择相同的会话，但否则会话不一定可预测。

使用 PowerShell SDK 禁用现有应用程序组中所有应用程序的应用程序会话共享，或创建禁用应用程序会话共享的组。

PowerShell cmdlet 示例

要禁用会话共享，请使用 Broker PowerShell cmdlet `New-BrokerApplicationGroup` 或 `Set-BrokerApplicationGroup`，并将参数 `SessionSharingEnabled` 设置为 `False`，将参数 `SingleAppPerSession` 设置为 `True`。

- 例如，要创建禁用组中所有应用程序的应用程序会话共享的应用程序组：

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

- 例如，要禁用现有应用程序组中所有应用程序之间的应用程序会话共享：

```
Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False
-SingleAppPerSession $True
```

注意事项

- 要启用 `SingleAppPerSession` 属性，必须将 `SessionSharingEnabled` 属性设置为 False。这两个属性不能同时启用。`SessionSharingEnabled` 参数指的是应用程序组之间的会话共享。
- 应用程序会话共享仅适用于与应用程序组关联但未与交付组关联的应用程序。所有直接与交付组关联的应用程序默认共享会话。
- 如果一个应用程序分配给多个应用程序组，请确保这些组没有冲突的设置。例如，一个组的选项设置为 `True`，而另一个组的选项设置为 `False` 会导致不可预测的行为。

重命名应用程序组

1. 在左侧窗格中选择**应用程序**，然后选择**应用程序组**选项卡。
2. 选择一个应用程序组，然后在操作栏中选择**重命名应用程序组**。
3. 指定新的唯一名称，然后单击**确定**。

添加、删除或更改交付组与应用程序组关联的优先级

应用程序组可以与包含可交付应用程序的共享（非专用）计算机的交付组关联。

如果满足以下两个条件，您还可以选择包含仅交付桌面的共享计算机的交付组：

- 交付组包含共享计算机，并且是使用早于 7.9 的版本创建的。
- 您具有“编辑交付组”权限。

提交**编辑应用程序组**对话框时，交付组类型会自动转换为“桌面和应用程序”。

1. 在左侧窗格中选择**应用程序**，然后选择**应用程序组**选项卡。
2. 选择一个应用程序组，然后在操作栏中选择**编辑应用程序组**。
3. 选择**交付组**页面。
4. 要添加交付组，请单击**添加**。选中可用交付组的复选框。（无法选择不兼容的交付组。）完成选择后，单击**确定**。
5. 要删除交付组，请选中要删除的组的复选框，然后单击**删除**。出现提示时确认删除。
6. 要更改交付组的优先级，请选中交付组的复选框，然后单击**编辑优先级**。输入优先级（0 = 最高），然后单击**确定**。
7. 点击“**应用**”以应用所做更改并保持窗口打开，或点击“**保存**”以应用更改并关闭窗口。

在应用程序组中添加、更改或删除标记限制

添加、更改和删除标记限制可能会对哪些计算机被考虑用于启动应用程序产生意想不到的影响。请查看 标记 中的注意事项和警告。

1. 在左窗格中选择“**应用程序**”，然后选择“**应用程序组**”选项卡。
2. 选择一个应用程序组，然后在操作栏中选择“**编辑应用程序组**”。
3. 选择“**交付组**”页面。
4. 要添加标记限制，请选择“**将启动限制到具有该标记的计算机**”，然后从下拉列表中选择标记。
5. 要更改或删除标记限制，请选择其他标记，或通过清除“**将启动限制到具有此标记的计算机**”来完全删除标记限制。
6. 点击“**应用**”以应用所做更改并保持窗口打开，或点击“**保存**”以应用更改并关闭窗口。

在应用程序组中添加或删除用户

有关用户的详细信息，请参阅 创建应用程序组。

1. 在左窗格中选择“**应用程序**”，然后选择“**应用程序组**”选项卡。
2. 选择一个应用程序组，然后在操作栏中选择“**编辑应用程序组**”。
3. 选择“**用户**”页面。指示是否要允许关联交付组中的所有用户使用应用程序组中的应用程序，或者只允许特定用户和组使用。要添加用户，请点击“**添加**”，然后指定要添加的用户。要删除用户，请选择一个或多个用户，然后点击“**删除**”。
4. 点击“**应用**”以应用所做更改并保持窗口打开，或点击“**保存**”以应用更改并关闭窗口。

在应用程序组中添加、更改或删除应用程序图标

执行以下步骤以添加、更改或删除应用程序图标。

1. 在左侧窗格中选择 **应用程序**。
2. 在 **应用程序** 选项卡上，选择一个应用程序，然后选择 **属性**。

   要在应用程序组级别进行更改，请导航到 **应用程序组** 选项卡，选择组中的一个应用程序，然后选择 **属性**。
3. 选择 **交付** 页面，然后选择 **更改**。将显示 **选择图标** 窗口。
4. 在 **选择图标** 窗口中，执行以下任一操作：

   - 要添加图标，请选择 **添加**，然后浏览到该图标。
   - 要删除图标，请选择它，然后选择 **删除**。
   - 要更改图标，请为应用程序选择它。

重要提示：

- 您无法添加大小超过 200 KB 的图标。
- 您只能添加 .icon 文件。
- 您无法删除内置图标。
- 您无法删除正在使用的应用程序的图标。

5. 选择 **保存** 以应用更改并关闭窗口。

更改应用程序组中的范围

仅当您已创建范围时才能更改范围（您无法编辑“所有”范围）。有关详细信息，请参阅委派管理。

1. 在左侧窗格中选择**应用程序**，然后选择**应用程序组**选项卡。
2. 选择一个应用程序组，然后在操作栏中选择**编辑应用程序组**。
3. 选择**范围**页面。选中或清除范围旁边的复选框。
4. 单击**应用**以应用所做的任何更改并保持窗口打开，或者单击**保存**以应用更改并关闭窗口。

更改应用程序组中的范围

仅当您已创建范围时才能更改范围（您无法编辑“所有”范围）。有关详细信息，请参阅委派管理。

1. 在左侧窗格中选择**应用程序**，然后选择**应用程序组**选项卡。
2. 选择一个应用程序组，然后在操作栏中选择**编辑应用程序组**。
3. 选择**范围**页面。选中或清除要更改的范围旁边的复选框。
4. 选择**应用**以应用所做的任何更改并保持窗口打开，或者选择**保存**以应用更改并关闭窗口。

删除应用程序组

应用程序必须至少与一个交付组或应用程序组关联。如果删除应用程序组导致一个或多个应用程序不再属于任何组，则会警告您删除该组也会删除这些应用程序。然后，您可以确认或取消删除。

删除应用程序不会从其原始源中删除它。但是，如果您想再次使其可用，则必须再次添加它。

1. 在左侧窗格中选择 **应用程序**，然后选择 **应用程序组** 选项卡。
2. 选择一个应用程序组，然后在操作栏中选择 **删除组**。
3. 出现提示时确认删除。

使用文件夹组织应用程序组

您可以创建文件夹来组织应用程序组，以便于访问。

所需角色

默认情况下，如果您拥有以下内置角色之一，则可以为应用程序组创建和管理文件夹：

- 云管理员
- 完全管理员
- 应用程序组管理员

您可以通过创建自定义角色将管理操作委派给其他用户。下表列出了每个操作所需的权限。

操作	所需权限
创建应用程序组文件夹	创建应用程序组文件夹
删除应用程序组文件夹	删除应用程序组文件夹
移动应用程序组文件夹	移动应用程序组文件夹
重命名应用程序组文件夹	编辑应用程序组文件夹
将应用程序组移动到文件夹	编辑应用程序组文件夹，编辑应用程序组属性

有关详细信息，请参阅创建和管理角色。

创建和管理文件夹

您可以使用“操作”栏或右键单击菜单来创建和管理应用程序组文件夹。此外，您可以将应用程序组或文件夹拖动到文件夹树中的所需位置。

须知：

- 您可以嵌套文件夹，最多五级（不包括默认根文件夹）。
- 一个文件夹可以包含应用程序组和子文件夹。只有当文件夹及其子文件夹不包含应用程序组时，才能删除该文件夹。
- Web Studio 中的所有节点（例如**计算机目录**、**交付组**、**应用程序**和**应用程序组**）在后端共享相同的文件夹树。为避免在重命名或移动文件夹时出现名称冲突，请为不同节点中的一级文件夹使用唯一的名称。

如果您使用 `New-BrokerAdminFolder` SDK cmdlet 创建文件夹并希望它显示在**应用程序组**节点下，则必须使用 `Set-BrokerAdminFolderMetadata` cmdlet 添加 `ContainsApplicationGroups` 元数据。

示例：

```
Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
ContainsApplicationGroups -Value true
```

远程电脑访问

注意：

从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中移除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

远程电脑访问是 Citrix Virtual Apps and Desktops™ 的一项功能，它使组织能够轻松地允许员工以安全的方式远程访问公司资源。Citrix 平台通过让用户访问其物理办公电脑来实现这种安全访问。如果用户可以访问其办公电脑，他们就可以访问完成工作所需的所有应用程序、数据和资源。远程电脑访问消除了引入和提供其他工具以适应远程办公的需要。例如，虚拟桌面或应用程序及其相关基础结构。

远程电脑访问使用与交付虚拟桌面和应用程序相同的 Citrix Virtual Apps and Desktops 组件。因此，部署和配置远程电脑访问的要求和过程与部署 Citrix Virtual Apps and Desktops 以交付虚拟资源的要求和过程相同。这种一致性提供了统一的管理体验。用户通过使用 Citrix HDX™ 交付其办公电脑会话可获得最佳用户体验。

此功能包含一个类型为 **远程电脑访问** 的计算机目录，它提供以下功能：

- 能够通过指定组织单位 (OU) 添加计算机。此功能有助于批量添加电脑。
- 根据登录办公 Windows PC 的用户进行自动用户分配。我们支持单用户和多用户分配。默认情况下，我们会自动将多个用户分配给下一个未分配的计算机。要将自动分配限制为单个用户，请登录 Web Studio，转到 **设置** 并关闭 **为远程电脑访问启用多用户自动分配** 设置。

Citrix Virtual Apps and Desktops 可以通过使用其他类型的计算机目录来适应物理电脑的更多用例。这些用例包括：

- 物理 Linux 电脑
- 池化物理电脑（即随机分配，而非专用）

注意：

有关支持的操作系统版本的详细信息，请参阅 单会话操作系统 和 Linux VDA 的 VDA 系统要求。

对于本地部署，远程电脑访问仅适用于 Citrix Virtual Apps and Desktops Advanced 或 Premium 许可证。会话消耗许可证的方式与其他 Citrix Virtual Desktops™ 会话相同。对于 Citrix Cloud，远程电脑访问适用于 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）和 Workspace Premium Plus。

注意事项

虽然适用于 Citrix Virtual Apps and Desktops 的所有一般技术要求和注意事项也适用于远程电脑访问，但有些可能与物理 PC 用例更相关或专属于物理 PC 用例。

重要提示：

Windows 11 物理系统（以及一些运行 Windows 10 的系统）包含基于虚拟化的安全功能，导致 VDA 软件错误地将其检测为虚拟机。为缓解此问题，您有以下选项：

- 在 VDA 命令行安装中，将“/physicalmachine”选项与“/remotepc”选项一起使用
- 如果未使用前面提到的选项，请在安装 VDA 后添加以下注册表值 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - 名称: ForceEnableRemotePC
  - 类型: DWORD
  - 数据: 1

部署注意事项

在规划远程电脑访问的部署时，需要做出一些一般性决定。

- 您可以将远程电脑访问添加到现有的 Citrix Virtual Apps and Desktops 部署中。在选择此选项之前，请考虑以下事项：
  - 当前的 Delivery Controller 或 Cloud Connector 的大小是否合适，以支持与远程电脑访问 VDA 相关的额外负载？
  - 本地站点数据库和数据库服务器的大小是否合适，以支持与远程电脑访问 VDA 相关的额外负载？
  - 现有 VDA 和新的远程电脑访问 VDA 是否会超过每个站点支持的最大 VDA 数量？
- 您必须通过自动化过程将 VDA 部署到办公 PC。以下是可用选项：
  - 电子软件分发 (ESD) 工具（例如 SCCM）：使用 SCCM 安装 VDA。
  - 部署脚本：使用脚本安装 VDA。
- 查看远程电脑访问安全注意事项。

> **注意：**
>
> 在设计远程电脑访问时，您必须考虑连接到远程 PC 上 GPU 的物理显示器数量以及当前配置/运行的显示器数量。即使显示器未在 Citrix 会话中使用，但被 GPU 检测到，显示器的存在也会计入 GPU 支持的最大显示器限制。

计算机目录注意事项

所需的计算机目录类型取决于用例：

- 远程电脑访问计算机目录
  - Windows 专用 PC
  - Windows 专用多用户 PC。此用例适用于多个用户可以在不同班次远程访问的物理办公 PC。
  - 池化 Windows PC。此用例适用于多个随机用户可以访问的物理 PC，例如计算机实验室。
- 单会话操作系统计算机目录
  - 静态 - 专用 Linux PC
  - 随机 - 池化 Linux PC

确定计算机目录类型后，请考虑以下事项：

- 一台计算机一次只能分配给一个计算机目录。
- 为了方便委派管理，请考虑根据地理位置、部门或任何其他分组创建计算机目录，以便于将每个目录的管理委派给相应的管理员。
- 在选择计算机帐户所在的 OU 时，请选择较低级别的 OU 以获得更高的粒度。如果不需要这种粒度，可以选择较高级别的 OU。例如，在 Bank/Officers/Tellers 的情况下，选择 **Tellers** 以获得更高的粒度。否则，您可以根据需要选择 **Officers** 或 **Bank**。
- 将 OU 分配给远程电脑访问计算机目录后，移动或删除 OU 会影响 VDA 关联并导致未来分配出现问题。因此，请务必进行相应规划，以便在 Active Directory 更改计划中考虑计算机目录的 OU 分配更新。
- 如果由于 OU 结构的原因，选择要添加到计算机目录的 OU 不容易，则不必选择任何 OU。您可以在之后使用 PowerShell 将计算机添加到目录。如果桌面分配在交付组中配置正确，则用户自动分配将继续有效。一个用于将计算机和用户分配添加到计算机目录的示例脚本可在 GitHub 中找到。
- 集成的局域网唤醒功能仅适用于 **Remote PC Access** 类型的计算机目录。

Linux VDA 注意事项

以下是 Linux VDA 的具体注意事项：

- 仅在非 3D 模式下在物理机上使用 Linux VDA。由于 NVIDIA 驱动程序的限制，当启用 HDX 3D 模式时，PC 的本地屏幕无法变黑并显示会话活动。显示此屏幕存在安全风险。
- 对于物理 Linux 计算机，请使用单会话操作系统类型的计算机目录。
- Linux 计算机不支持自动用户分配。
- 如果用户已在本地登录其 PC，则从 StoreFront™ 启动 PC 的尝试将失败。
- Linux 计算机不支持电源管理选项。

技术要求和注意事项

本节包含物理 PC 的技术要求和注意事项。

- 不支持以下各项：
  - KVM 切换器或其他可能断开会话的组件。
  - 混合型 PC，包括一体机和 NVIDIA Optimus 笔记本电脑及 PC。
  - 双启动计算机。
- 将键盘和鼠标直接连接到 PC。连接到显示器或其他可能关闭或断开连接的组件，可能会导致这些外围设备不可用。如果必须将输入设备连接到显示器等组件，请勿关闭这些组件。

- PC 必须加入 Active Directory 域服务域。
- 安全启动仅在 Windows 10 和 Windows 11 上受支持。
- PC 必须具有活动的网络连接。有线连接更可靠，带宽更高，因此是首选。
- 如果使用 Wi-Fi，请执行以下操作：

  a. 将电源设置配置为保持无线适配器开启。

  b. 配置无线适配器和网络配置文件，以允许在用户登录前自动连接到无线网络。否则，VDA 不会注册，直到用户登录。在用户登录之前，PC 无法用于远程访问。

  c. 确保可以从 Wi-Fi 网络访问 Delivery Controller 或 Cloud Connector。

- 您可以在笔记本电脑上使用远程电脑访问。确保笔记本电脑连接到电源，而不是使用电池运行。将笔记本电脑的电源选项配置为与台式电脑的选项匹配。例如：

  a. 禁用休眠功能。

  b. 禁用睡眠功能。

  c. 将合盖操作设置为 **不执行任何操作**。

  d. 将“按下电源按钮”操作设置为 **关机**。

  e. 禁用显卡和网卡节能功能。

- 远程电脑访问支持运行 Windows 10 的 Surface Pro 设备。请遵循前面提到的笔记本电脑相同准则。
- 如果使用扩展坞，可以对笔记本电脑进行取消坞接和重新坞接操作。当您取消坞接笔记本电脑时，VDA 会通过 Wi-Fi 重新向 Delivery Controller 或 Cloud Connector 注册。但是，当您重新坞接笔记本电脑时，除非您断开无线适配器，否则 VDA 不会切换到使用有线连接。某些设备提供内置功能，可在建立有线连接时断开无线适配器。其他设备需要自定义解决方案或第三方实用程序来断开无线适配器。请查看前面提到的 Wi-Fi 注意事项。

  要为远程电脑访问设备启用坞接和取消坞接，请执行以下操作：

  a. 在“**开始**”菜单中，选择“**设置 > 系统 > 电源和睡眠**”，然后将“**睡眠**”设置为“**从不**”。

  b. 在 **设备管理器 > 网络适配器 > 以太网适配器** 下，转到 **电源管理** 并取消选中 **允许计算机关闭此设备以节约电源**。确保选中 **允许此设备唤醒计算机**。

- 多个用户访问同一办公 PC 时，会在 Citrix Workspace 中看到相同的图标。当用户登录 Citrix Workspace 时，如果该资源已被其他用户使用，则该资源将显示为不可用。
- 在每个访问办公电脑的客户端设备（例如，家用电脑）上安装 Citrix Workspace 应用程序。

配置顺序

本节概述了在使用 **远程电脑访问** 类型计算机目录时如何配置远程电脑访问。有关如何创建其他类型计算机目录的信息，请参阅 创建计算机目录。

1. 仅限本地站点 - 要使用集成的局域网唤醒功能，请配置 局域网唤醒 中概述的先决条件。
2. 如果为远程电脑访问创建了新的 Citrix Virtual Apps and Desktops 站点：
   a. 选择 **Remote PC Access** 站点类型。
   b. 在 **电源管理** 页面上，选择为默认的远程电脑访问计算机目录启用或禁用电源管理。您可以通过编辑计算机目录属性稍后更改此设置。有关配置局域网唤醒的详细信息，请参阅 局域网唤醒。
   c. 填写 **用户** 和 **计算机帐户** 页面上的信息。

   完成这些步骤将创建一个名为 **Remote PC Access Machines** 的计算机目录和一个名为 **Remote PC Access Desktops** 的交付组。
3. 如果添加到现有 Citrix Virtual Apps and Desktops 站点：
   a. 创建 **远程电脑访问** 类型的计算机目录（向导的操作系统页面）。有关如何创建计算机目录的详细信息，请参阅 创建计算机目录。请务必分配正确的 OU，以便目标电脑可用于远程电脑访问。
   b. 创建一个交付组，为用户提供对计算机目录中 PC 的访问权限。有关如何创建交付组的详细信息，请参阅 创建交付组。请务必将交付组分配给包含需要访问其 PC 的用户的 Active Directory 组。
4. 将 VDA 部署到办公电脑。
   - 我们建议使用单会话操作系统核心 VDA 安装程序 (VDAWorkstationCoreSetup.exe)。
   - 您还可以使用带 `/remotepc/physicalmachine` 选项的单会话完整 VDA 安装程序 (VDAWorkstationSetup.exe)，这与使用核心 VDA 安装程序的效果相同。

   > **注意：**
   >
   > 对于 RemotePC 安装，请将 `/physicalmachine` 参数与 `/remotepc` 结合使用，以便 VDA 在某些用户场景中按预期运行。

- 考虑启用 Windows 远程协助，以允许技术支持团队通过 Citrix Director 提供远程支持。为此，请使用 `/enable_remote_assistance` 选项。有关详细信息，请参阅 使用命令行安装。
- 要在 Director 中查看登录持续时间信息，您必须使用单会话完整 VDA 安装程序并包含 **Citrix User Profile Management WMI Plugin** 组件。通过使用 `/includeadditional` 选项包含此组件。有关详细信息，请参阅 使用命令行安装。
- 有关使用 SCCM 部署 VDA 的信息，请参阅 使用 SCCM 安装 VDA。
- 有关通过部署脚本部署 VDA 的信息，请参阅 使用脚本安装 VDA。

成功完成步骤 2-4 后，用户在本地登录 PC 时将自动分配到其自己的计算机。

5. 指示用户在其用于远程访问办公电脑的每个客户端设备上下载并安装 Citrix Workspace 应用程序。Citrix Workspace 应用程序可从 `https://www.citrix.com/downloads/` 或支持的移动设备的应用商店获取。

通过注册表管理的功能

> **注意：**
>
> 错误编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。编辑注册表之前，请务必备份注册表。

禁用多用户自动分配

在每个 Delivery Controller™ 上，添加以下注册表设置：

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- 名称: AllowMultipleRemotePCAssignments
- 类型: DWORD
- 数据: 0

睡眠模式（最低版本 7.16）

要允许远程电脑访问计算机进入睡眠状态，请在 VDA 上添加此注册表设置，然后重新启动计算机。重新启动后，操作系统电源节省设置将生效。计算机在预配置的空闲计时器到期后进入睡眠模式。计算机唤醒后，它会重新向 Delivery Controller 注册。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名称: DisableRemotePCSleepPreventer
- 类型: DWORD
- 数据: 1

会话管理

默认情况下，当本地用户在该计算机上启动会话（通过按 CTRL+ALT+DEL）时，远程用户的会话会自动断开连接。要阻止此自动操作，请在办公电脑上添加以下注册表项，然后重新启动计算机。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名称: SasNotification
- 类型: DWORD
- 数据: 1

默认情况下，如果在超时期限内未确认连接消息，则远程用户优先于本地用户。要配置此行为，请使用以下设置：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名称: RpcaMode
- 类型: DWORD
- 数据:
  - 1 - 如果远程用户在指定的超时期限内未响应消息 UI，则远程用户始终具有优先权。如果未配置此设置，则此行为是默认行为。
  - 2 - 本地用户具有优先权。

默认情况下，强制执行远程电脑访问模式的超时时间为 30 秒。您可以配置此超时时间，但不要将其设置为低于 30 秒。要配置超时时间，请使用此注册表设置：

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 名称: RpcaTimeout
- 类型: DWORD
- 数据: 超时秒数（十进制值）

当用户想要强制获取控制台访问权限时：本地用户可以在 10 秒内两次按下 Ctrl+Alt+Del，以获取对远程会话的本地控制权并强制断开连接事件。

注册表更改并重新启动计算机后，如果本地用户在远程用户使用该电脑时按下 Ctrl+Alt+Del 登录，远程用户将收到提示。该提示询问是否允许或拒绝本地用户的连接。允许连接会断开远程用户的会话。

会话管理日志记录

远程电脑访问现在具有日志记录功能，可在有人尝试访问具有活动 ICA® 会话的电脑时进行记录。这使您能够监控环境中的不必要或意外活动，并在需要调查任何事件时能够审计此类事件。

事件使用 Windows 事件查看器记录，位于 **应用程序和服务 > Citrix > HostCore > ICA 服务 > 管理员** 中。

使用远程电脑访问时，会记录三个不同的事件。

Ctrl+Alt+Del 事件

当本地用户在具有活动远程会话的控制台键盘上按下 Ctrl+Alt+Del 时，将出现此事件。

事件详细信息

- 日志名称: 应用程序和服务
- 事件 ID: 43, 44, 45
- 来源：ICA 服务

事件 ID 43

当 SasNotification 注册表值不存在或 SasNotification 注册表值为 0 时，将显示此事件 ID。

- 消息：

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to automatically disconnect the
remote session.
```

事件 ID 44

当 SasNotification 注册表值为 1 且 RpcaMode 注册表值为 1 或 RpcaMode 注册表值不存在时，将显示此事件 ID。

- 消息：

```
Ctrl+Alt+Del has been pressed on the endpoint.
```

```
The session management behavior is set to notify the remote user. The
user preference is set to remote user.
```

事件 ID 45

当 SasNotification 注册表值为 1 且 RpcaMode 注册表值为 2 时，将显示此事件 ID。

- 消息：

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user.

The user preference is set to local user.
```

远程会话断开连接事件

当远程会话因各种原因断开连接时，将显示此事件。

事件详细信息

- 日志名称：应用程序和服务
- 事件 ID：46、47、48
- 来源：ICA 服务

事件 ID 46

当远程会话已断开连接，并且 SasNotification 注册表值不存在或 SasNotification 注册表值为 0 时，将显示此事件 ID。

- 消息：

```
The remote session for &lt;remoteUserName> has been disconnected.
```

事件 ID 47

当远程用户同意断开会话连接，并且 SasNotification 注册表值为 1 且 RpcaMode 注册表值为 1 或 RpcaMode 注册表值为 2 或 RpcaMode 注册表值不存在时，将显示此事件 ID。

- 消息：

```
The remote session for &lt;remoteUserName> has been disconnected
because the user accepted the request to disconnect the session.
```

事件 ID 48

当远程用户未在特定超时期限内拒绝断开连接请求，并且 SasNotification 注册表值为 1 且 RpcaMode 注册表值为 2 时，将显示此事件 ID。

- 消息：

```
The remote session for &lt;remoteUserName> has been disconnected
because the user did not decline the disconnection request within the
configured timeout period (&lt;timeout period>).
```

CTRL+ALT+DEL 按下两次事件

当在 10 秒内两次按下 Ctrl+Alt+Del 时，将显示此事件。

事件详细信息

- 日志名称：应用程序和服务
- 事件 ID：49
- 来源: ICA Service

事件 ID 49

当在 10 秒内按下两次 Ctrl+Alt+Del 时，会出现此事件 ID。

- 消息:

```
The remote session for &lt;remoteUserName> has been forcibly
disconnected.
```

局域网唤醒

远程电脑访问支持局域网唤醒，这使用户能够远程打开物理 PC。此功能使用户在不使用办公室 PC 时可以将其关闭，从而节省能源成本。当计算机意外关闭时，它还可以实现远程访问。

借助 Wake on LAN 功能，在交付控制器指示下，魔术包会直接从 PC 上运行的 VDA 发送到 PC 所在的子网。这使得该功能无需依赖额外的基础架构组件或第三方解决方案即可传输魔术包。

限制

带局域网唤醒功能的远程电脑访问不支持在高峰时段自动开机。

系统要求

以下是使用局域网唤醒功能的系统要求：

- 控制平面：
  - 思杰 DaaS™
  - Citrix Virtual Apps and Desktops 2009 或更高版本
- 物理 PC：
  - VDA 2009 或更高版本
  - Windows 10 或 Windows 11。有关支持性详细信息，请参阅 VDA 系统要求。
  - 在 BIOS/UEFI 中启用 Wake on LAN
  - 在 Windows 配置中，在网络适配器属性中启用 Wake on LAN

配置 Wake on LAN

使用 STUDIO 配置 WAKE ON LAN

要创建 Wake on LAN 连接：

1. 在左侧窗格中，选择“**托管**”节点。
2. 选择 **添加连接和资源**。
3. 在向导的“**连接**”页面上，提供以下信息:
   a. 连接类型: 远程电脑局域网唤醒
   b. 区域名称: 选择远程电脑访问目录所在的区域
   c. 连接名称: 输入局域网唤醒连接的名称
4. 完成“添加连接和资源”向导中的剩余步骤。

要将局域网唤醒连接添加到远程电脑访问计算机目录：

1. 如果您正在创建新的远程电脑访问计算机目录，则可以使用“计算机目录设置”向导的**计算机类型**页面上的下拉列表添加连接。
2. 如果要将局域网唤醒连接添加到现有计算机目录：
   a. 导航到左侧的**计算机目录**节点。
   b. 选择相应的远程电脑访问计算机目录。
   c. 右键单击计算机目录或选择上方的**更多**菜单。
   d. 选择**编辑计算机目录**。
   e. 在**电源管理**页面中，选择**是**。
   f. 从下拉列表中选择相应的连接。

g. 选择**保存**。

> **注意：**
>
> 通过 Studio 配置 Wake on LAN 目前仅适用于 Citrix DaaS。

使用 POWERSHELL 配置 WAKE ON LAN

要使用 PowerShell 配置 Wake on LAN，请执行以下操作：

1. 如果您尚未创建远程电脑访问计算机目录，请创建一个。
2. 如果您尚未创建 Wake on LAN 主机连接，请创建一个。
3. 检索 Wake on LAN 主机连接的唯一标识符。
4. 将 Wake on LAN 主机连接与计算机目录关联。

要创建 Wake on LAN 主机连接，请执行以下操作：

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `
```

```
                -ConnectionType Custom `

                -PluginId VdaWOLMachineManagerFactory `

                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid



# Wait for the connection to be ready before trying to use it

while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

}
```

当主机连接准备就绪时，运行以下命令以检索主机连接的唯一标识符：

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

检索到连接的唯一标识符后，运行以下命令将该连接与远程电脑访问计算机目录关联：

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

设计注意事项

当您计划将局域网唤醒 (Wake on LAN) 与远程电脑访问 (Remote PC Access) 结合使用时，请考虑以下事项：

- 多个计算机目录可以使用相同的局域网唤醒主机连接。
- 要使一台电脑唤醒另一台电脑，两台电脑必须位于同一子网中并使用相同的局域网唤醒主机连接。电脑是否在相同或不同的计算机目录中无关紧要。
- 主机连接分配给特定的区域。如果您的部署包含多个区域，则每个区域都需要一个局域网唤醒主机连接。这同样适用于计算机目录。
- 魔术包使用全局广播地址 255.255.255.255 进行广播。请确保该地址未被阻止。
- 对于每个局域网唤醒连接，子网中必须至少有一台电脑处于开机状态，才能唤醒该子网中的计算机。

操作注意事项

以下是使用局域网唤醒功能时的注意事项：

- VDA 必须至少注册一次，然后才能使用集成的局域网唤醒功能唤醒电脑。
- 局域网唤醒只能用于唤醒电脑。它不支持其他电源操作，例如重新启动或关机。
- 创建 Wake on LAN 连接后，它在 Web Studio 中可见。但是，如果在本地使用 Citrix Virtual Apps and Desktops，则不支持在 Web Studio 中编辑其属性。
- 魔术包通过以下两种方式之一发送：

  a. 当用户尝试启动其电脑会话且 VDA 未注册时

  b. 当管理员从 Web Studio 或 PowerShell 手动发送开机命令时

- 由于交付控制器不知道 PC 的电源状态，Web Studio 在电源状态下显示“**不支持**”。交付控制器使用 VDA 注册状态来确定 PC 是开机还是关机。

故障排除

显示器消隐不起作用

如果 Windows PC 的本地显示器在活动 HDX 会话期间未空白（本地显示器显示会话中发生的情况），这很可能是由于 GPU 供应商的驱动程序问题造成的。要解决此问题，请通过设置以下注册表值，使 Citrix 间接显示驱动程序 (IDD) 的优先级高于显卡供应商的驱动程序：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名称：CitrixIDD

- 类型: DWORD
- 数据: 3

有关显示适配器优先级和显示器创建的更多详细信息，请参阅知识中心文章 CTX237608。

在启用了会话管理通知的计算机上选择 Ctrl+Alt+Del 时会话断开连接

由 **SasNotification** 注册表值控制的会话管理通知仅在 VDA 上启用远程电脑访问模式时才有效。如果物理 PC 启用了 Hyper-V 角色或任何基于虚拟化的安全功能，则该 PC 会报告为虚拟机。如果 VDA 检测到它正在虚拟机上运行，它会自动禁用远程电脑访问模式。要启用远程电脑访问模式，请添加以下注册表值：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名称: ForceEnableRemotePC
- 类型: DWORD
- 数据: 1

重新启动 PC 以使设置生效。

诊断信息

有关远程电脑访问的诊断信息将写入 Windows 应用程序事件日志。信息性消息不受限制。错误消息通过丢弃重复消息来限制。

- 3300 (信息): 计算机已添加到目录
- 3301 (信息): 计算机已添加到交付组
- 3302 (信息): 计算机已分配给用户
- 3303 (错误): 异常

电源管理

如果启用了 Remote PC Access 的电源管理，子网定向广播可能无法启动与控制器位于不同子网上的计算机。如果您需要使用子网定向广播进行跨子网电源管理，并且 AMT 支持不可用，请尝试 Wake-up 代理或单播方法。确保在电源管理连接的高级属性中启用了这些设置。

活动远程会话记录本地触摸屏输入

当 VDA 启用远程电脑访问模式时，计算机在活动会话期间会忽略本地触摸屏输入。如果物理 PC 启用了 Hyper-V 角色或任何基于虚拟化的安全功能，则该 PC 会报告为虚拟机。如果 VDA 检测到它正在虚拟机上运行，它会自动禁用远程电脑访问模式。要启用远程电脑访问模式，请添加以下注册表设置：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名称: ForceEnableRemotePC
- 类型: DWORD
- 数据: 1

重新启动电脑以使设置生效。

更多资源

以下是用于远程电脑访问的其他资源：

- 解决方案设计指南: Remote PC Access Design Decisions。
- 远程电脑访问架构示例: Reference Architecture for Citrix Remote PC Access Solution。

Cloud Connector 独立 Citrix 安全票据颁发机构 (STA) 服务

如果将本地站点聚合与 Citrix Workspace™ 结合使用，或者将 Citrix Gateway Service 与 StoreFront 结合使用，Cloud Connector 会处理您的 Citrix Virtual Apps and Desktops™ 站点的安全票据颁发机构 (STA) 流量。独立 STA 服务使您能够更好地控制环境中 STA 票据的交付。

独立 Citrix STA 服务默认安装在资源位置中的每个 Cloud Connector 上。独立 STA 服务将 STA 票据颁发从 Citrix Cloud™ 票据颁发服务转移到 Cloud Connector，并标准化了正常模式和 LHC 模式下的票据颁发操作。独立 STA 服务减少了对云服务的依赖，并减少了间歇性 LHC 事件。

系统要求

- 如果使用本地 StoreFront™：版本 2311 或更高版本
- Delivery Controller™：2503 或更高版本

启用独立 STA 服务

要启用独立 STA 服务（该服务可将 Citrix Gateway Service 与本地 Delivery Controller 结合使用，并提高本地站点聚合到 Citrix Workspace 服务的弹性），请配置以下注册表项：

1. 在您的 Cloud Connector 上，将注册表项 `HKEY_LOCAL_MACHINE\Software\Citrix\XaXdCloudProxyPersist\StandaloneStaServiceForced` 设置为 `1`。

名称：`StandaloneStaServiceForced` 类型：DWORD 值：1

配置注册表项后，重新启动 Citrix Remote Broker Provider Service 以使更改生效。

重要注意事项

- 有关在本地环境中使用 Citrix Workspace 和本地 Citrix Gateway 的信息，请参阅在工作区中聚合虚拟应用和桌面。
- 有关将本地 StoreFront 与 Citrix Gateway Service 结合使用的信息，请参阅适用于 StoreFront 的 Citrix Gateway Service。
- 将本地 StoreFront 配置为使用 Cloud Connector 的 FQDN 作为 STA 服务器。本地 NetScaler® Gateway vServer 必须包含配置为 STA 的 Cloud Connector 的完整列表，并且与 StoreFront 中指定的列表匹配。
- 当您将 Citrix Workspace 与用于 ICA® 代理的本地 NetScaler Gateway vServer 结合使用时：将 NetScaler Gateway 配置为使用所有 Cloud Connector 作为 STA 服务器。

限制

- Citrix Workspace 不支持双 STA 票据兑换。
- 如果您的云租户中未配置 DaaS，配置同步将不会发生，并且事件日志中将记录 517 错误。

发布内容

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

> 您可以发布一个应用程序，该应用程序只是指向资源的 URL 或 UNC 路径，例如 Microsoft Word 文档或 Web 链接。此功能称为发布内容。发布内容的能力增加了向用户交付内容的灵活性。您可以受益于现有的应用程序访问控制和管理。您还可以指定是使用本地应用程序还是已发布的应用程序来打开内容。

发布的内容在 StoreFront™ 和 Citrix Workspace™ 应用程序中与其他应用程序一样显示。用户访问它的方式与访问应用程序的方式相同。在客户端上，资源照常打开。

- 如果本地安装的应用程序合适，则会启动它来打开资源。
- 如果已定义文件类型关联，则会启动已发布的应用程序来打开资源。

您可以使用 PowerShell SDK 发布内容。您不能使用 Web Studio 发布内容。但是，您可以在发布后使用 Web Studio 编辑应用程序属性。

配置概述和准备

发布内容使用 `New-BrokerApplication` cmdlet，并具有以下关键属性。（有关所有 cmdlet 属性的说明，请参阅 cmdlet 帮助。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType` 属性必须为 `PublishedContent`。

`CommandLineExecutable` 属性指定发布内容的位置。支持以下格式，限制为 255 个字符。

- HTML 网站地址（例如，`<http://www.citrix.com>`）
- Web 服务器上的文档文件（例如，`https://www.citrix.com/press/pressrelease.doc`）
- FTP 服务器上的目录（例如，`ftp://ftp.citrix.com/code`）
- FTP 服务器上的文档文件（例如，`ftp://ftp.citrix.com/code/Readme.txt`>）
- UNC 目录路径（例如，`file://myServer/myShare or \\\\myServer\\myShare`）
- UNC 文件路径（例如，`file://myServer/myShare/myFile.asf` 或 `\\myServer\myShare\myFile.asf`）

确保您拥有正确的 SDK。

- 对于 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）部署，下载 并安装 Citrix Virtual Apps and Desktops 远程 PowerShell SDK。
- 对于本地 Citrix Virtual Apps and Desktops 部署，请使用随 Delivery Controller 安装的 PowerShell SDK。添加已发布的内容应用程序需要最低版本为 7.11 的 Delivery Controller。

以下过程使用示例。在示例中：

- 已创建计算机目录。
- 已创建名为 `PublishedContentApps` 的交付组。该组使用目录中的多会话操作系统计算机。WordPad 应用程序已添加到该组。
- 已为交付组名称、`CommandLineExecutable` 位置和应用程序名称进行分配。

入门

在包含 PowerShell SDK 的计算机上，打开 PowerShell。

以下 cmdlet 添加相应的 PowerShell SDK 管理单元，并分配返回的交付组记录。

`Add-PsSnapin Citrix* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

如果您使用的是 Citrix DaaS，请通过输入您的 Citrix Cloud™ 凭据进行身份验证。如果存在多个客户，请选择一个。

发布 URL

分配位置和应用程序名称后，以下 cmdlet 将 Citrix 主页发布为应用程序。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"



New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

验证成功：

- 打开 StoreFront 并以可以访问 PublishedContentApps 交付组中应用程序的用户身份登录。显示屏包含新创建的带有默认图标的应用程序。要了解如何自定义图标，请参阅 `<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`。
- 单击 **Citrix 主页**应用程序。URL 将在本地运行的默认浏览器实例的新选项卡中启动。

发布位于 UNC 路径的资源

在此示例中，管理员已创建了一个名为 `PublishedResources` 的共享。分配位置和应用程序名称后，以下 cmdlet 将该共享中的 RTF 和 DOCX 文件发布为资源。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"
```

```
New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

验证成功：

- 刷新 StoreFront 窗口以查看新发布的文档。
- 单击 **PublishedRTF** 和 **PublishedDOCX** 应用程序。每个文档都会在本地运行的写字板中打开。

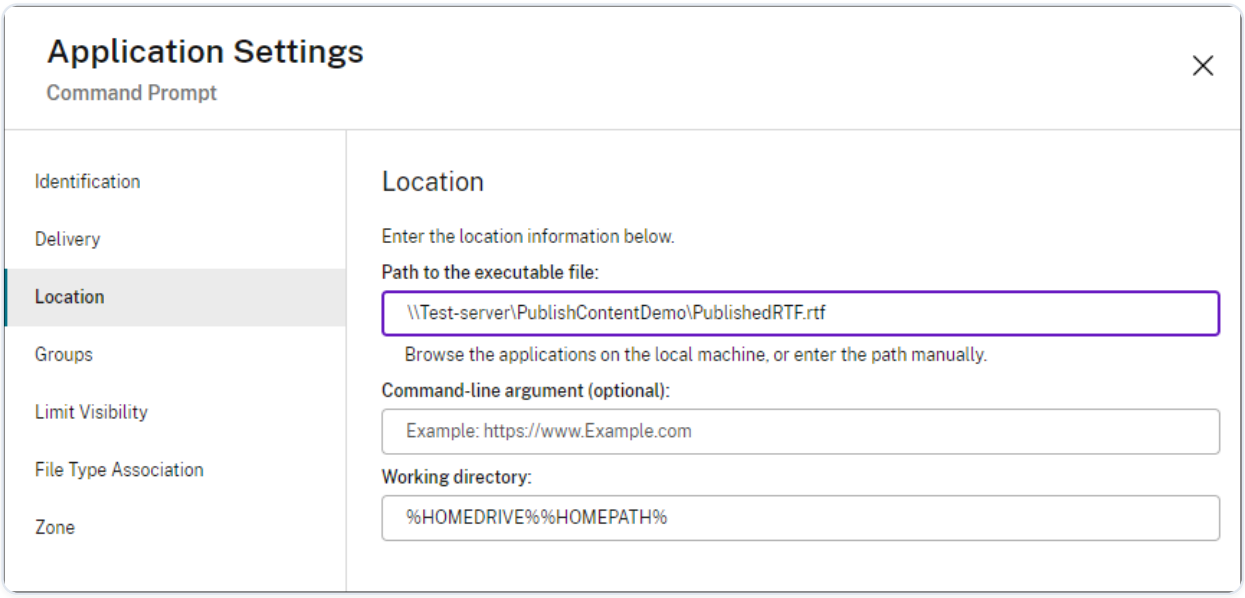
查看和编辑 PublishedContent 应用程序

您可以使用管理其他应用程序类型的方法来管理已发布的内容。

要查看和编辑 `PublishedContent` 应用程序，请执行以下步骤：

1. 登录 Web Studio 并在左侧窗格中选择**应用程序**。
2. 在**应用程序**选项卡上，选择一个 PublishedContent 应用程序，然后选择**属性**。

   应用程序属性（例如用户可见性、组关联和快捷方式）适用于已发布的内容。但是，您无法在**位置**页面上更改命令行参数或工作目录属性。
3. 要更改资源，请修改该页面上的**可执行文件路径**字段。



4. 要使用已发布的应用程序打开 `PublishedContent` 应用程序（而不是本地应用程序），请执行以下步骤：

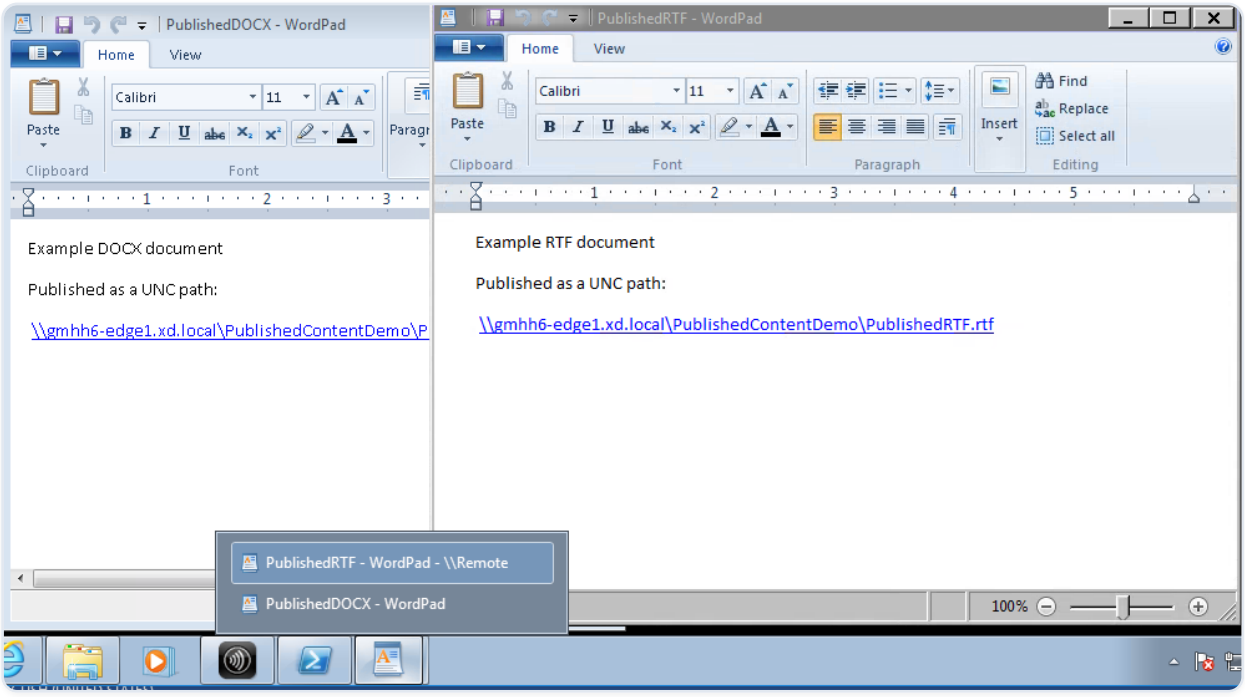
   在此示例中，编辑已发布的写字板应用程序以创建 .rtf 文件的文件类型关联。

   a. 为交付组启用维护模式。

   b. 编辑“**文件类型关联**”属性。

   c. 完成后，禁用维护模式。

   d. 刷新 StoreFront 以加载文件类型关联更改，然后单击“**PublishedRTF**”和“**PublishedDOCX**”应用程序。请注意区别。“**PublishedDOCX**”仍将在本地写字板中打开。但是，由于文件类型关联，“**PublishedRTF**”现在将在已发布的写字板中打开。



更多信息

- 创建计算机目录
- 创建交付组
- 更改应用程序属性

服务器 VDI

使用服务器 VDI（虚拟桌面基础结构）功能，从服务器操作系统为单个用户交付桌面。

- 企业管理员可以将服务器操作系统作为 VDI 桌面交付，这对于工程师和设计师等用户来说很有价值。
- 服务提供商可以从云端提供桌面。这些桌面符合 Microsoft 服务提供商许可协议 (SPLA)。

支持：

- 在 Citrix 虚拟应用和桌面™ 和 Citrix DaaS（以前称为 Citrix 虚拟应用和桌面服务）部署中，服务器 VDI 支持 Windows Server 2022、Windows Server 2019 和 Windows Server 2025。
- 所有服务器 VDI 部署都支持用户个性化层技术。
- 要使服务器 VDI 与扫描仪等 TWAIN 设备配合使用，必须安装 Windows Server 桌面体验功能。
- 以下功能不能与服务器 VDI 一起使用：
  - 托管应用程序
  - 本地应用程序访问
  - 直接（非代理）桌面连接
  - 远程电脑访问

安装和配置服务器 VDI

1. 准备 Windows 服务器以进行安装。
   - 使用 Windows Server Manager 确保未安装远程桌面服务角色服务。如果以前安装过，请将其删除。如果安装了这些角色服务，VDA 安装将失败。
   - 确保已启用“**将每个用户限制为单个会话**”属性。在 Windows 服务器上，编辑注册表以配置终端服务器设置：

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

     `DWORD fSingleSessionPerUser = 1`

2. 使用 Citrix Virtual Apps and Desktops 安装程序的命令行界面在受支持的服务器或服务器主映像上安装 VDA，并指定 `/servervdi` 选项。（默认情况下，安装程序的图形界面会阻止在服务器操作系统上安装 Windows 单会话操作系统 VDA。使用命令行可以覆盖此行为。）请使用以下命令之一：

   - 思杰虚拟应用和桌面™ 部署：
     - `XenDesktopVdaSetup.exe /servervdi`
     - `VDAWorkstationSetup.exe /servervdi`
   - Citrix DaaS™ 部署：
     - `VDAWorkstationSetup.exe /servervdi`

   其他选项：

   - 使用 `/controllers` 指定交付控制器或云连接器。
   - 使用 `/enable_hdx_ports` 在防火墙中打开端口，除非防火墙要手动配置。
   - 如果您要在映像上安装 VDA，并使用 MCS 从该映像创建服务器 VM，请使用 `/mastermcsimage`（或 `/masterimage`）。
   - 有关所有选项的详细信息，请参阅 使用命令行安装。

3. 为 Server VDI 创建计算机目录。在目录创建向导中：

   - 在“**操作系统**”页面上，选择“**单会话操作系统**”。
   - 在“**摘要**”页面上，为管理员指定一个计算机目录名称和描述，以明确将其标识为 Server VDI。这是 Studio 中指示该目录支持 Server VDI 的唯一标志。

   在 Studio 中使用搜索时，Server VDI 目录显示在“**单会话操作系统计算机**”选项卡上，即使 VDA 安装在多会话计算机上。

4. 创建交付组并选择您创建的 Server VDI 目录。

如果您在 VDA 安装期间未指定 Delivery Controller 或 Cloud Connector，请记住在之后指定它们。有关详细信息，请参阅 VDA 注册。

用户个性化层

> **注意：**

> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。有关 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

> Citrix Virtual Apps and Desktops 的用户个性化层功能扩展了非持久性计算机目录的功能，以在会话之间保留用户数据和本地安装的应用程序。用户个性化层功能由底层 Citrix App Layering 技术提供支持，在非持久性计算机目录中支持 Citrix Provisioning 和 Machine Creation Services™ (MCS)。

您将用户个性化层组件与 Virtual Delivery Agent 一起安装在主映像中。VHD 文件存储本地用户安装的应用程序。挂载在映像上的 VHD 充当用户自己的虚拟硬盘。

> **重要提示：**

> 您可以在 Citrix Virtual Apps and Desktops™ 中部署用户个性化层，或在映像模板中启用 App Layering 用户层，但不能同时部署。请勿在 App Layering 中的层上安装用户个性化层功能。

> 此功能取代了 Personal vDisk (PvD)，同时还为非持久性（池化）桌面环境中的用户提供了持久的工作区体验。

要部署用户个性化层功能，请按照文章中详述的步骤进行安装和配置。

应用程序支持

除了以下例外情况，用户在桌面上本地安装的所有应用程序都受用户个性化层支持。

例外情况

以下应用程序是例外，不支持在用户个性化层上使用：

- 企业应用程序，例如 MS Office 和 Visual Studio。
- 修改网络堆栈或硬件的应用程序。示例：VPN 客户端。
- 具有启动级驱动程序的应用程序。示例：病毒扫描程序。
- 驱动程序使用驱动程序存储的应用程序。示例：打印机驱动程序。

> **注意：**

> 您可以使用 Windows 组策略对象 (GPO) 使打印机可用。

*不要*允许用户在本地安装任何不受支持的应用程序。而是直接在主映像上安装这些应用程序。

需要本地用户或管理员帐户的应用程序

当用户在本地安装应用程序时，该应用程序会进入其用户层。如果用户随后添加或编辑本地用户或组，则这些更改在会话结束后不会保留。

> **重要提示：**
>
> 在主映像中添加任何所需的本地用户或组。

要求

用户个性化层功能需要以下组件：

- Citrix Virtual Apps and Desktops 7 1909 或更高版本
- Virtual Delivery Agent (VDA)，版本 1912 或更高版本
- Citrix Provisioning™，版本 1909 或更高版本
- Windows 文件共享 (SMB)，或启用了本地 AD 身份验证的 Azure 文件

当操作系统部署为单会话时，您可以在以下 Windows 版本上部署用户个性化层功能。支持仅限于单个会话上的单个用户。

- Windows 11 企业版 x64
- Windows 10 Enterprise x64，版本 1607 或更高版本
- Windows Server 2019（支持 Azure 文件）
- Windows Server 2022（支持 Azure 文件）

对于 Citrix Virtual Apps and Desktops 7，在 Windows Server 2022、Windows Server 2019 和 Windows 10 客户端上支持将 Azure 文件与用户个性化层结合使用。

> **注意：**
>
> 如果您使用的是服务器操作系统，则仅支持 Server VDI。有关部署详细信息，请参阅 Server VDI 文章。

> 用户个性化层一次仅支持每台计算机一个用户，然后计算机必须重新启动才能重置磁盘。您不能将用户个性化层与多会话服务器操作系统一起使用，只能与单会话服务器系统一起使用。用户个性化层仅支持非持久性桌面。

> 如果已安装用户个性化层功能，请将其卸载。在安装最新版本之前，请重新启动主映像。

设置文件共享

用户个性化层功能需要 Windows 服务器消息块 (SMB) 存储。要创建 Windows 文件共享，请按照您所用 Windows 操作系统的常规步骤进行操作。

有关将 Azure 文件与基于 Azure 的目录结合使用的更多信息，请参阅 为用户个性化层设置 Azure 文件存储。

建议

请遵循本节中的建议，以成功部署用户个性化层。

微软系统中心配置管理器 (SCCM)

如果您将 SCCM 与用户个性化层功能结合使用，请遵循 Microsoft 准则在 VDI 环境中准备映像。有关详细信息，请参阅这篇 Microsoft TechNet 文章。

用户层大小

用户层是精简预配的磁盘，会随着磁盘空间的使用而扩展。用户层允许的默认大小为 10 GB，这是我们建议的最小值。

> **注意：**

> 在安装过程中，如果该值设置为零 (0)，则默认用户层大小设置为 10 GB。

> 如果要更改用户层大小，可以为 **User Layer Size** 策略输入不同的值。请参阅**步骤 5：创建交付组自定义策略**，在**可选：单击“以 GB 为单位的用户层大小”旁边的“选择”**下。

用于覆盖用户层大小的工具（可选）

您可以使用 Windows 工具在用户层文件共享上定义配额来覆盖用户层大小。

使用以下 Microsoft 配额工具之一，在名为 **Users** 的用户层目录上设置硬配额：

- 文件服务器资源管理器 (FSRM)

- 配额管理器

> **注意：**
>
> 增加配额会影响新的用户层并扩展现有用户层。减少配额仅影响新的用户层。现有用户层的大小永远不会减小。

部署用户个性化层

部署用户个性化功能时，您可以在 Web Studio 中定义策略。然后，将策略分配给绑定到部署该功能的计算机目录的交付组。

如果主映像没有用户个性化层配置，则服务将保持空闲状态，并且不会干扰创作活动。

如果在主映像中设置策略，则服务会尝试在主映像中运行并装载用户层。主映像会表现出意外行为和不稳定。

要部署用户个性化层功能，请按以下顺序完成以下步骤：

- 步骤 1：验证 Citrix Virtual Apps and Desktops 环境的可用性。
- 步骤 2：准备主映像。
- 步骤 3：创建计算机目录。
- 步骤 4：创建交付组。
- 步骤 5：创建交付组自定义策略。

> **注意：**
>
> 在映像上升级 Windows 10 后首次登录所需的时间比平时长。用户的层需要更新以适应新版本的 Windows 10，这会增加登录时间。

步骤 1：验证 Citrix Virtual Apps and Desktops 环境是否可用

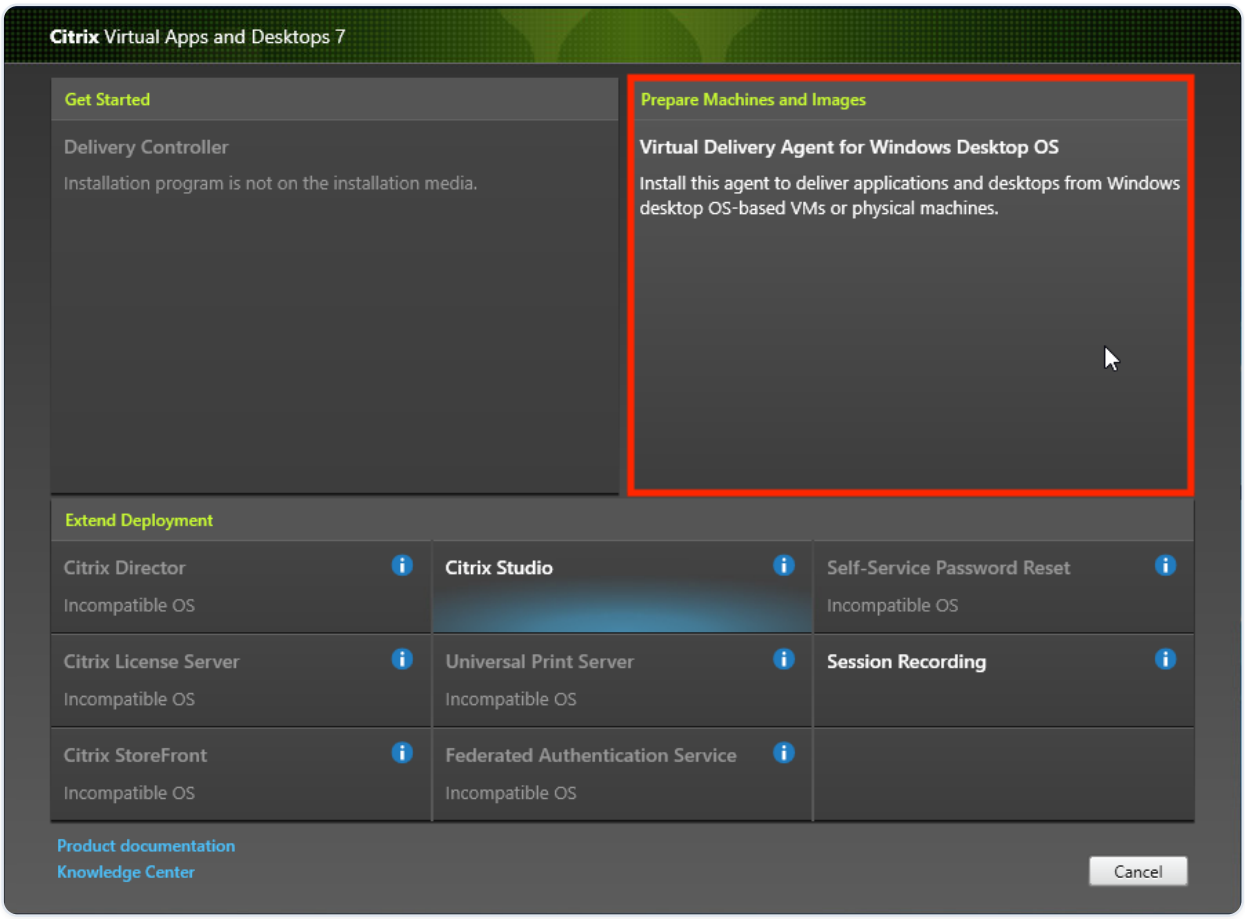
确保您的 Citrix Virtual Apps and Desktops 环境可用于此新功能。有关设置详细信息，请参阅安装和配置 Citrix Virtual Apps and Desktops。

步骤 2：准备主映像

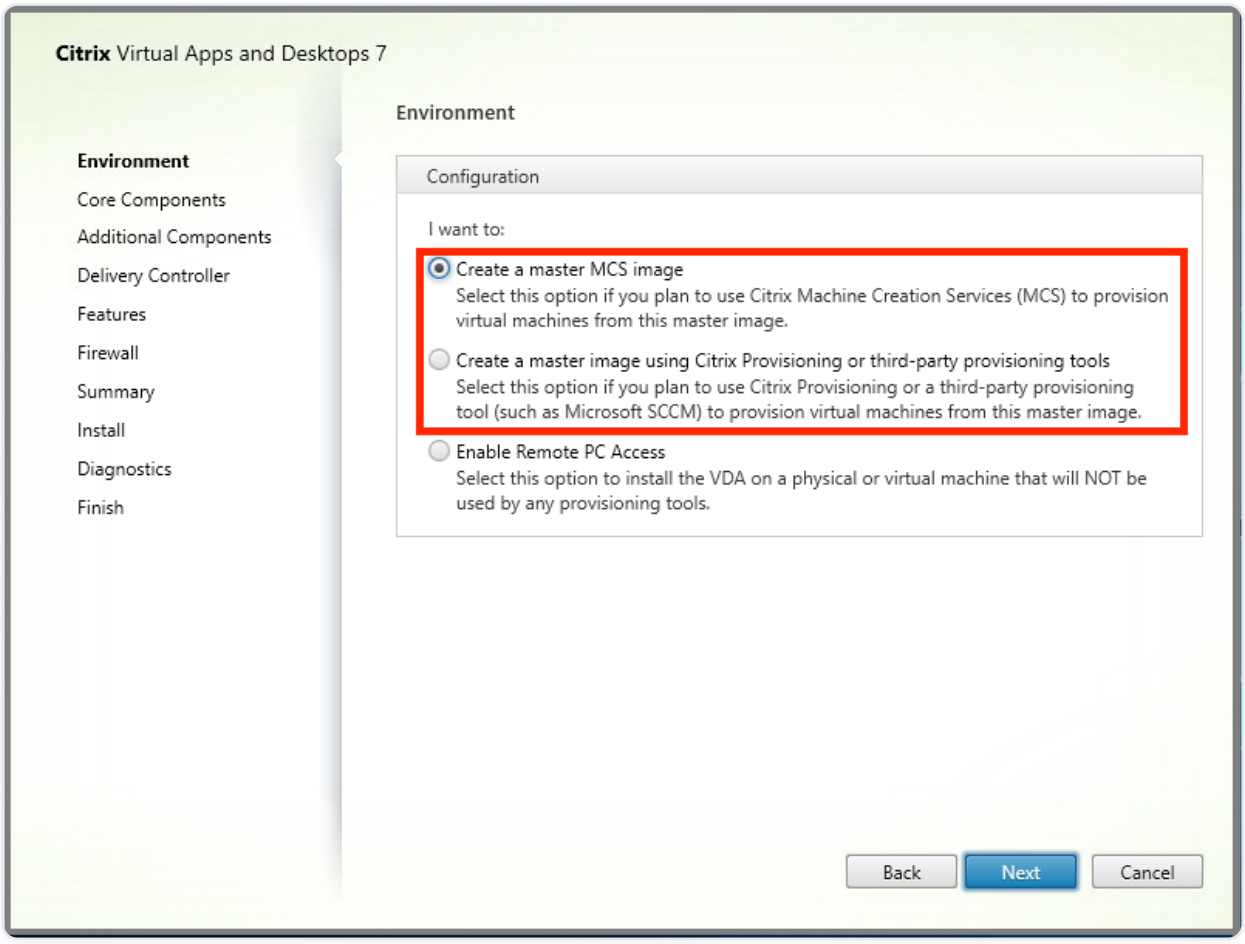
要准备主映像，请执行以下操作：

1. 找到主映像。安装您组织的业务应用程序以及用户通常认为有用的任何其他应用程序。
2. 如果您正在部署 Server VDI，请按照Server VDI 文章中的步骤操作。请务必包含可选组件 **User personalization layer**。有关详细信息，请参阅用于安装 VDA 的命令行选项。
3. 如果您使用的是 Windows 10，请安装 Virtual Delivery Agent (VDA) 1912 或更高版本。如果已安装旧版本的 VDA，请先卸载旧版本。安装新版本时，请务必选择并安装可选组件 **Citrix User Personalization Layer**，如下所示：

   a. 单击**适用于 Windows 桌面操作系统的虚拟投递代理**磁贴：

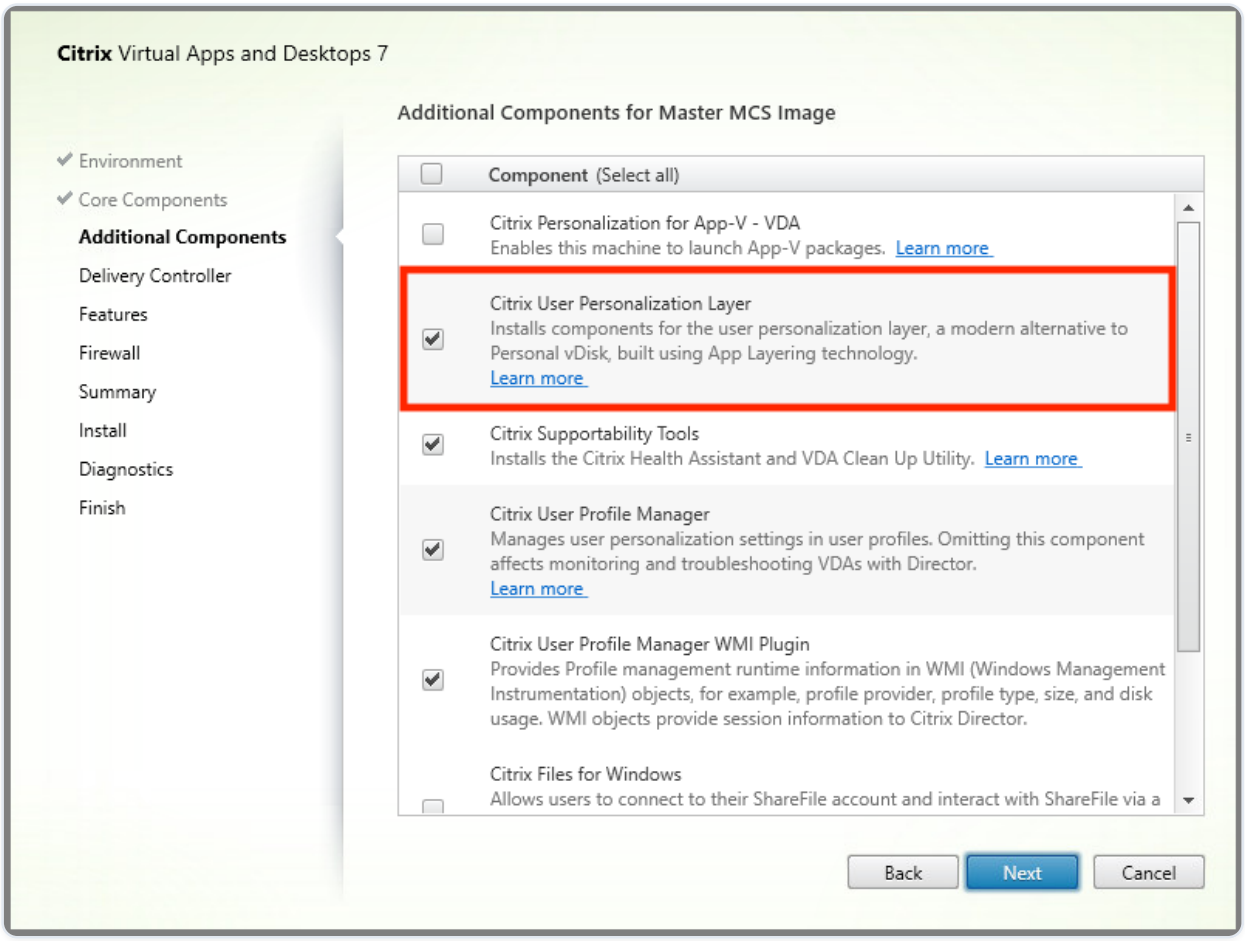


   a. **环境：** 选择“**创建 MCS 主映像**”或“**使用 Citrix Provisioning 或第三方预配工具创建主映像**”。



a. **核心组件：** 单击“**下一步**”。

b. **附加组件：** 选中“**Citrix User Personalization Layer**”。



a. 单击其余安装屏幕，根据需要配置 VDA，然后单击“**安装**”。映像在安装过程中会重启一次或多次。

4. 保持 **Windows 更新** 禁用。用户个性化层安装程序会禁用映像上的 Windows 更新。保持更新禁用状态。

映像已准备好供您上传到 Web Studio。

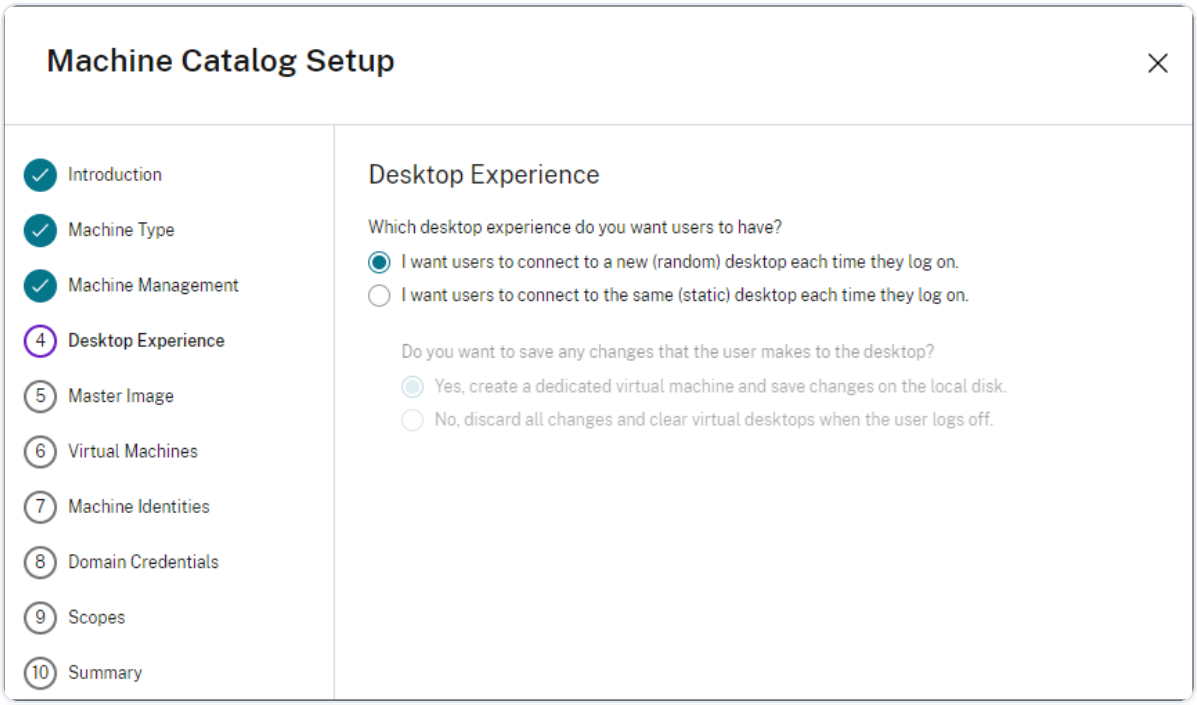
> **注意：**
>
> 如果您只想升级用户个性化层 (UPL)，可以使用较新版本的 UPL 和独立软件包进行升级。您无需升级 VDA。

步骤 3：创建计算机目录

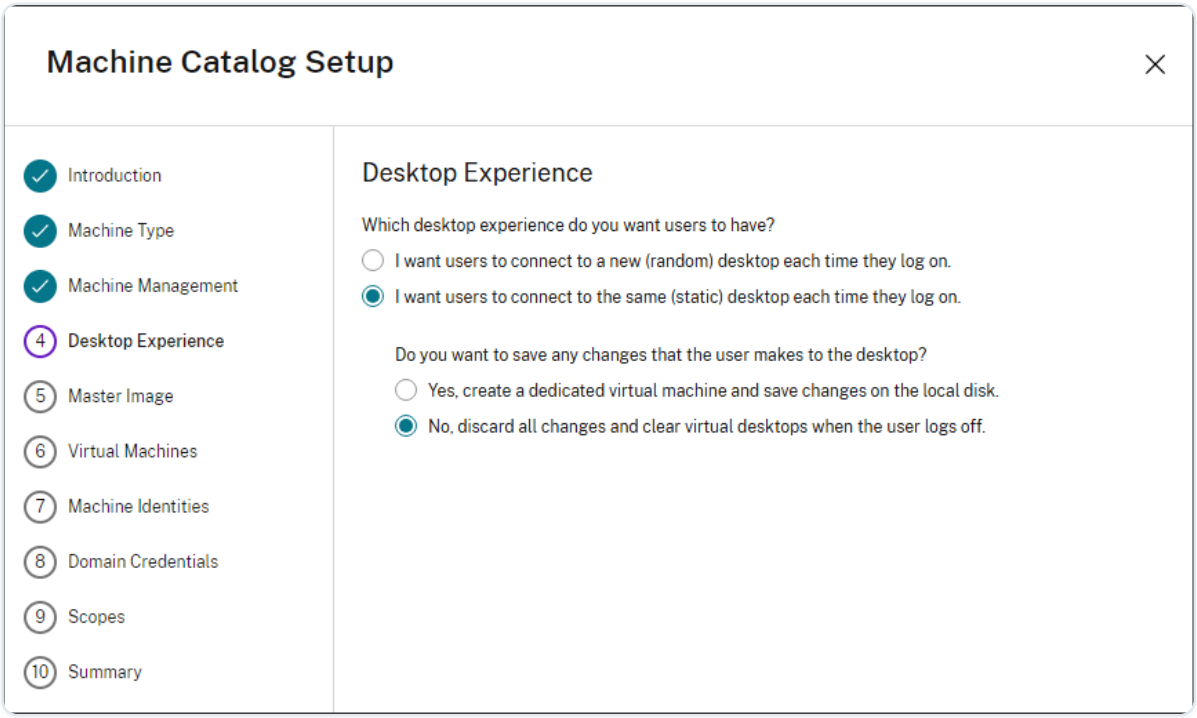
在 Web Studio 中，按照步骤创建计算机目录。在目录创建过程中使用以下选项：

1. 选择 **操作系统** 并将其设置为 **单会话操作系统**。
2. 选择 **计算机管理** 并将其设置为 **已进行电源管理的计算机**。例如，虚拟机或刀片式 PC。
3. 选择 **桌面体验** 并将其设置为 **随机池** 或 **静态池** 目录类型，如以下示例所示：

- **随机池：**



- **静态池：** 如果您选择静态池，请配置桌面以在用户注销时丢弃所有更改并清除虚拟桌面，如以下屏幕截图所示：



注意：

用户个性化层不支持配置为使用 Citrix Personal vDisk 或分配为专用虚拟机的静态池目录。

4. 如果您正在使用 MCS，请选择 **映像** 和上一节中创建的映像的快照。
5. 根据您的环境需要配置其余目录属性。

步骤 4：创建交付组

创建并配置**交付组**，包括您创建的计算机目录中的计算机。有关详细信息，请参阅创建交付组。

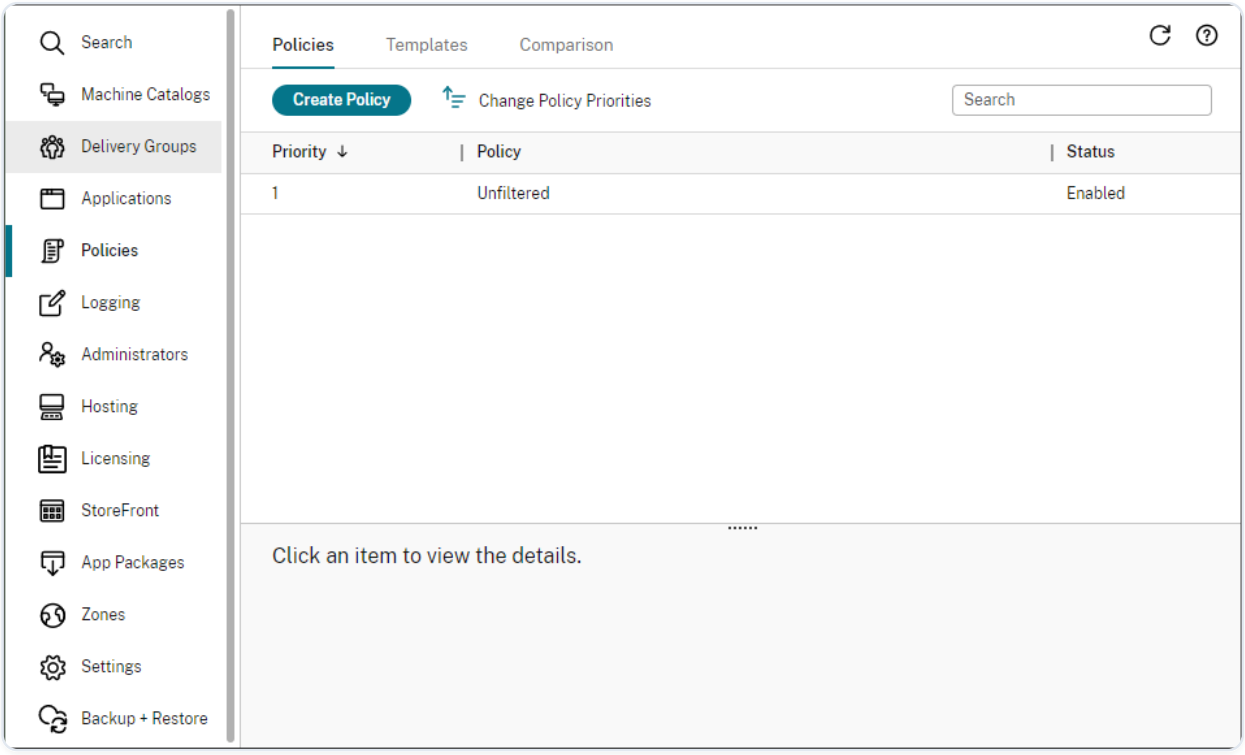
步骤 5：创建交付组自定义策略

要在 Virtual Delivery Agent 中启用用户层装载，请使用配置参数指定：

- 在网络上的何处访问用户层。
- 允许用户层磁盘增长到多大。

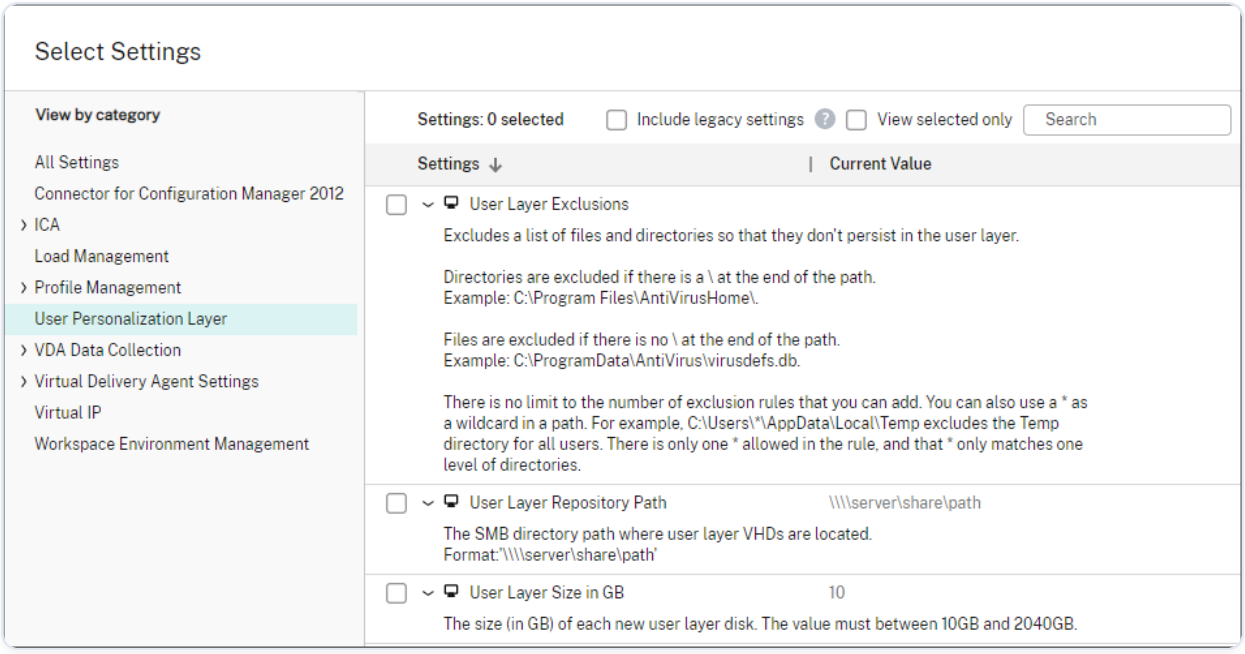
在 Web Studio 中将参数定义为自定义 Citrix 策略，并将其分配给您的交付组。

1. 登录 Web Studio 并在左侧窗格中选择**策略**：



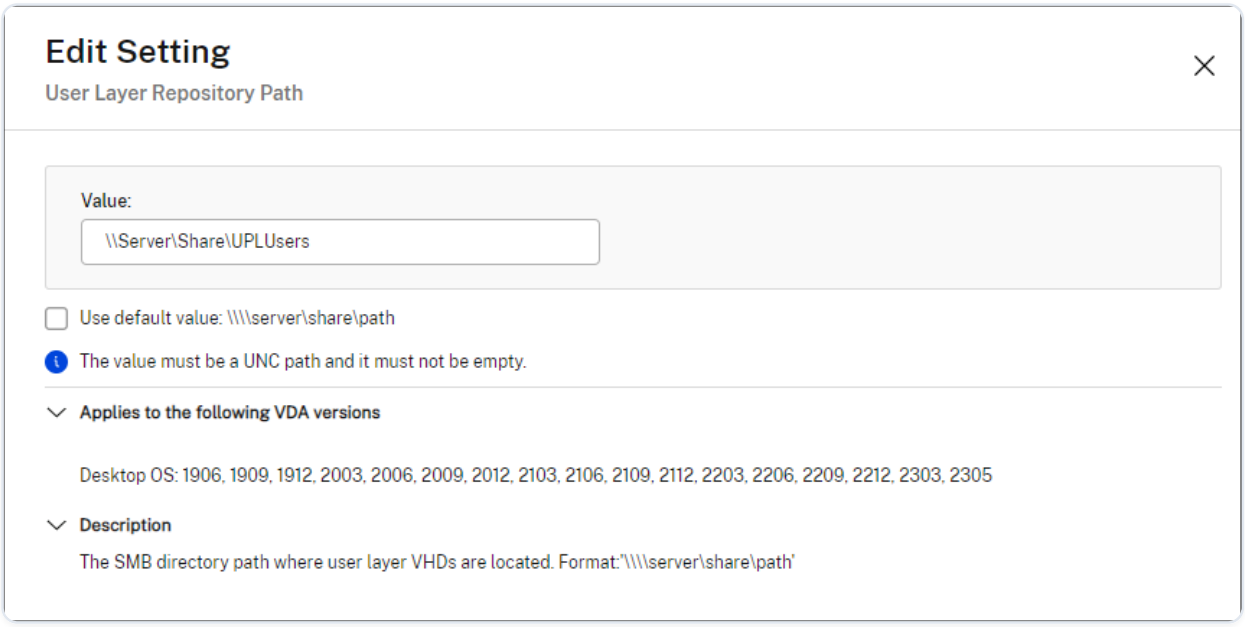
2. 在操作栏中选择**创建策略**。此时将显示“创建策略”窗口。
3. 在搜索字段中键入 `user layer`。以下三个策略将显示在可用策略列表中：
   - 用户层排除项
   - 用户层存储库路径
   - 用户层大小 (GB)

> **注意：**
>
> 增大大小会影响新的用户层并扩展现有用户层。减小大小仅影响新的用户层。现有用户层的大小永远不会减小。



4. 选中“**用户层存储库路径**”旁边的复选框，然后单击“**编辑**”。此时将显示“**编辑设置**”窗口。
5. 在“**值**”字段中输入路径，然后单击“**保存**”：

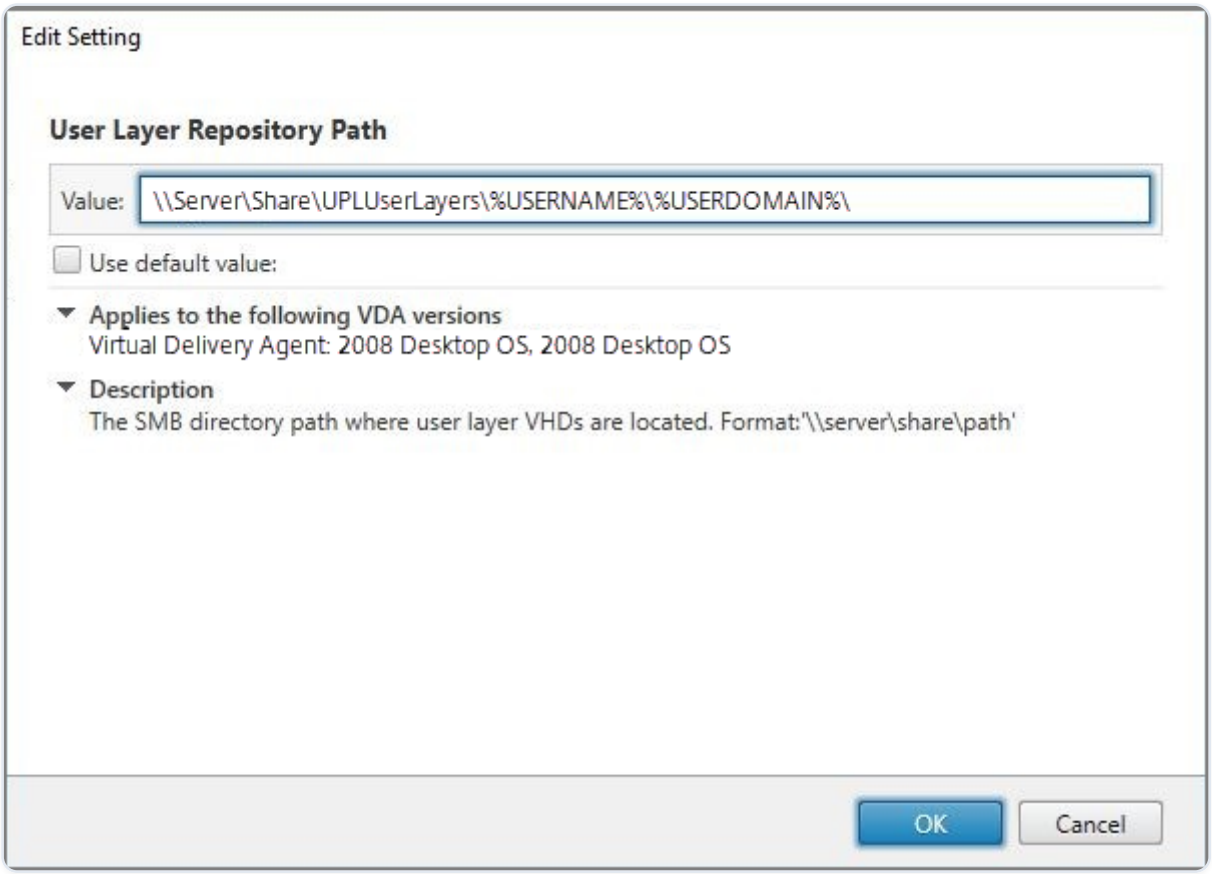
   - **路径格式：** `\\server-name-or-address\share-name\folder`
   - **路径示例：** `\\Server\Share\UPLUsers`
   - **结果路径示例：**对于 **CoolCompanyDomain** 中名为 **Alex** 的用户，路径为：`\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`



您可以使用 `%USERNAME%` 和 `%USERDOMAIN%` 变量、计算机环境变量和 Active Directory (AD) 属性来自定义路径。展开后，这些变量将生成显式路径。

环境变量示例：

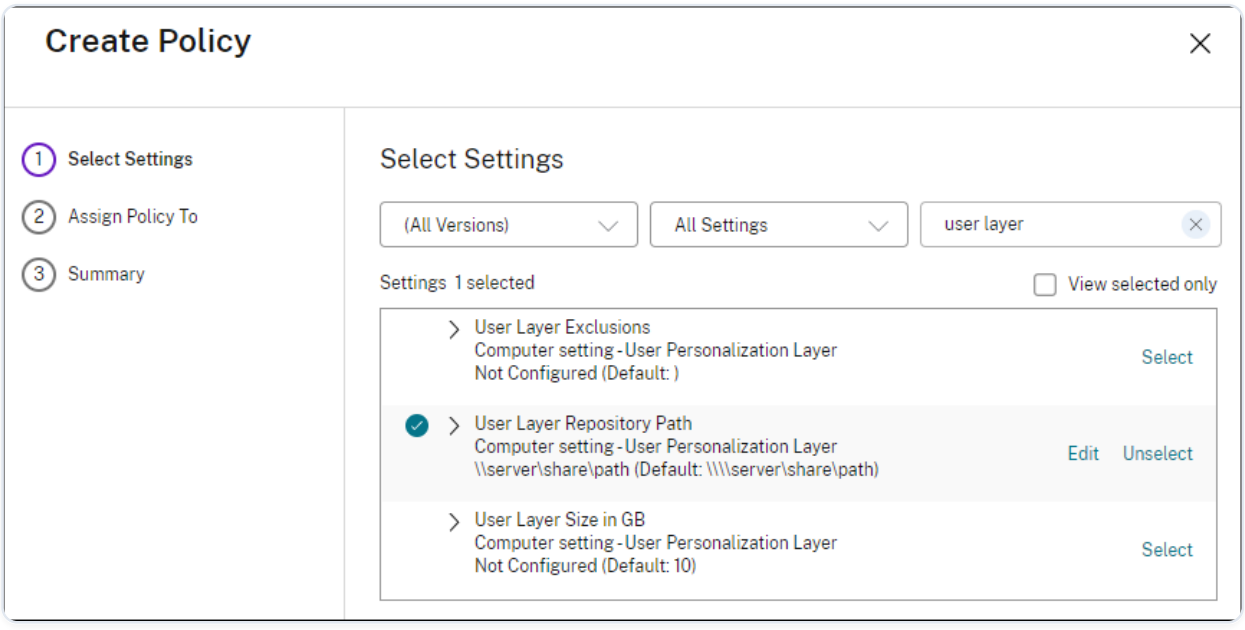
- **路径格式**：`\\Server-name-or-address\share-name\folder-with-environment-variables`
- **路径示例**：`\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **结果路径示例**：对于 **CoolCompanyDomain** 中名为 **Alex** 的用户，路径将为：`\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`



自定义 AD 属性示例：

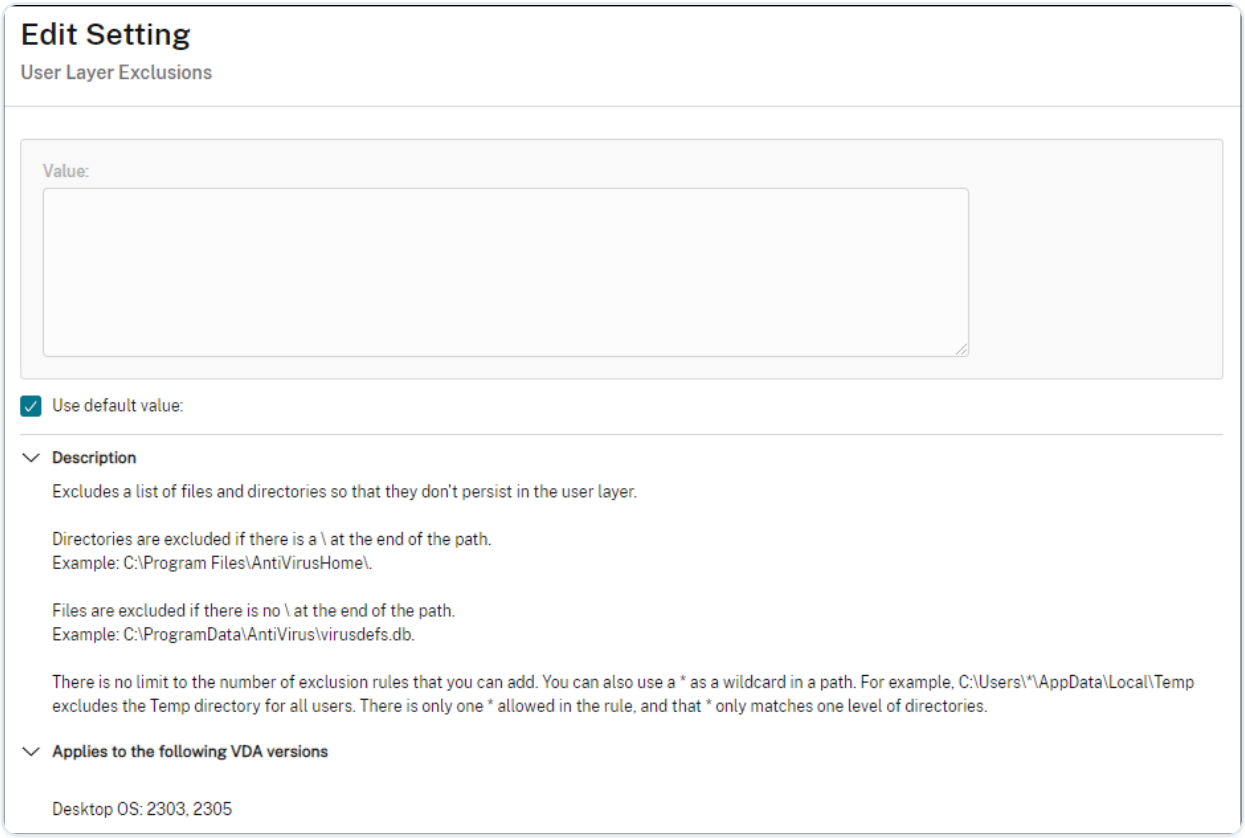
- 路径格式：`\\Server-name-or-address\share-name\AD-attribute`
- 路径示例：`\\Server\share#sAMAccountName#`
- 结果路径示例：`\\Server\share\JohnSmith`（如果 #sAMAccountName# 为当前用户解析为 JohnSmith）

6. 可选：选中“**用户层大小（GB）**”旁边的复选框，然后单击“**编辑**”：

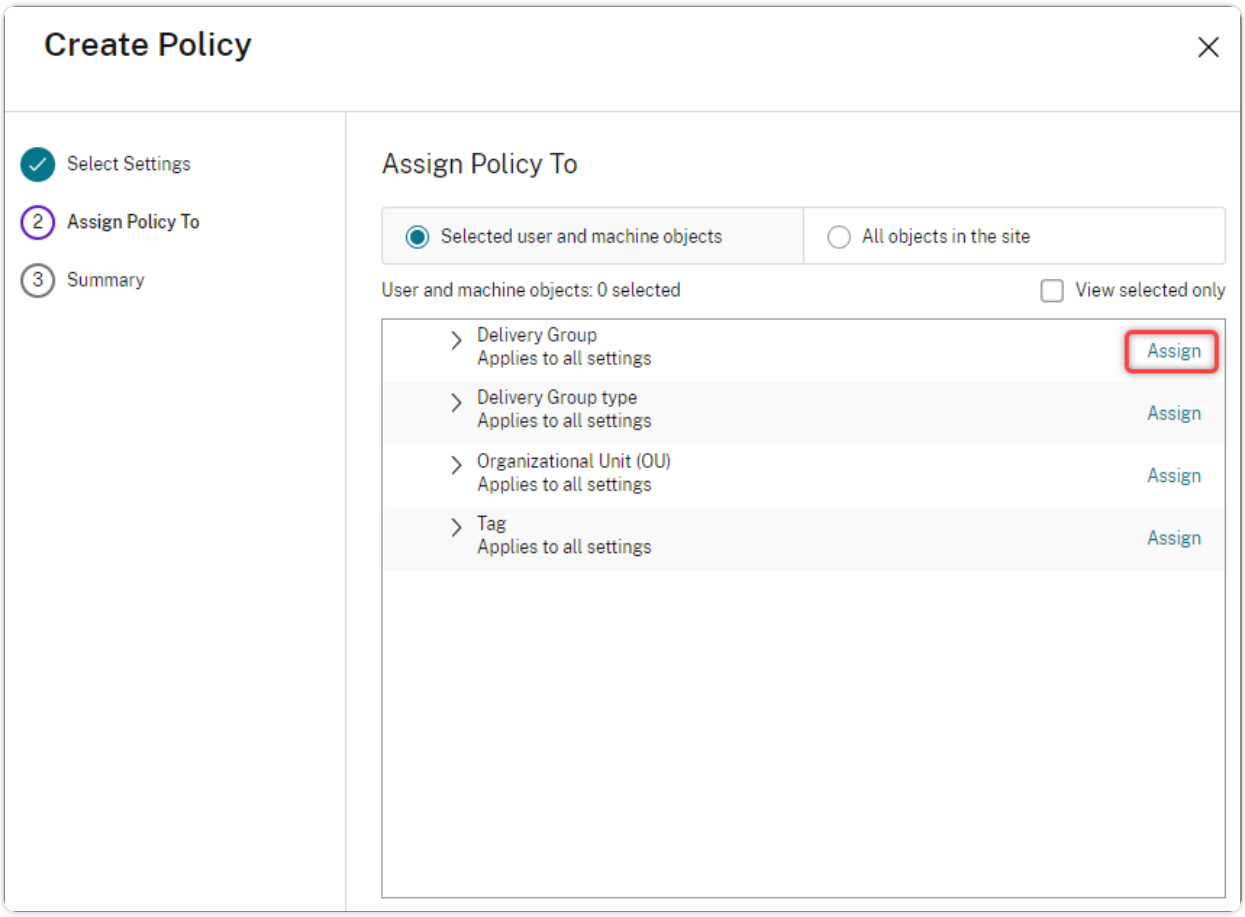


"编辑设置"窗口随即显示。

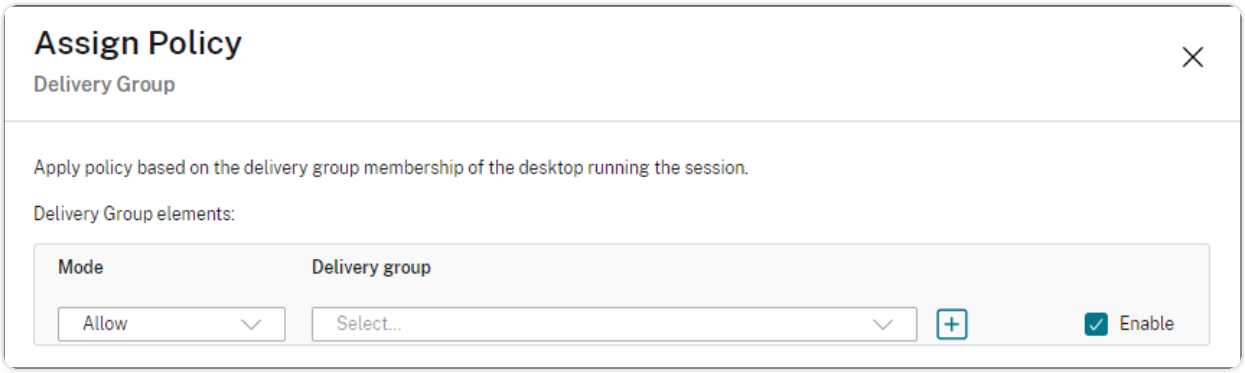
7. 可选：将默认值"**10 GB**"更改为每个用户层可增长的最大大小。单击"**保存**"。
8. 可选：选中"**用户层排除项**"旁边的复选框，然后单击"**编辑**"。



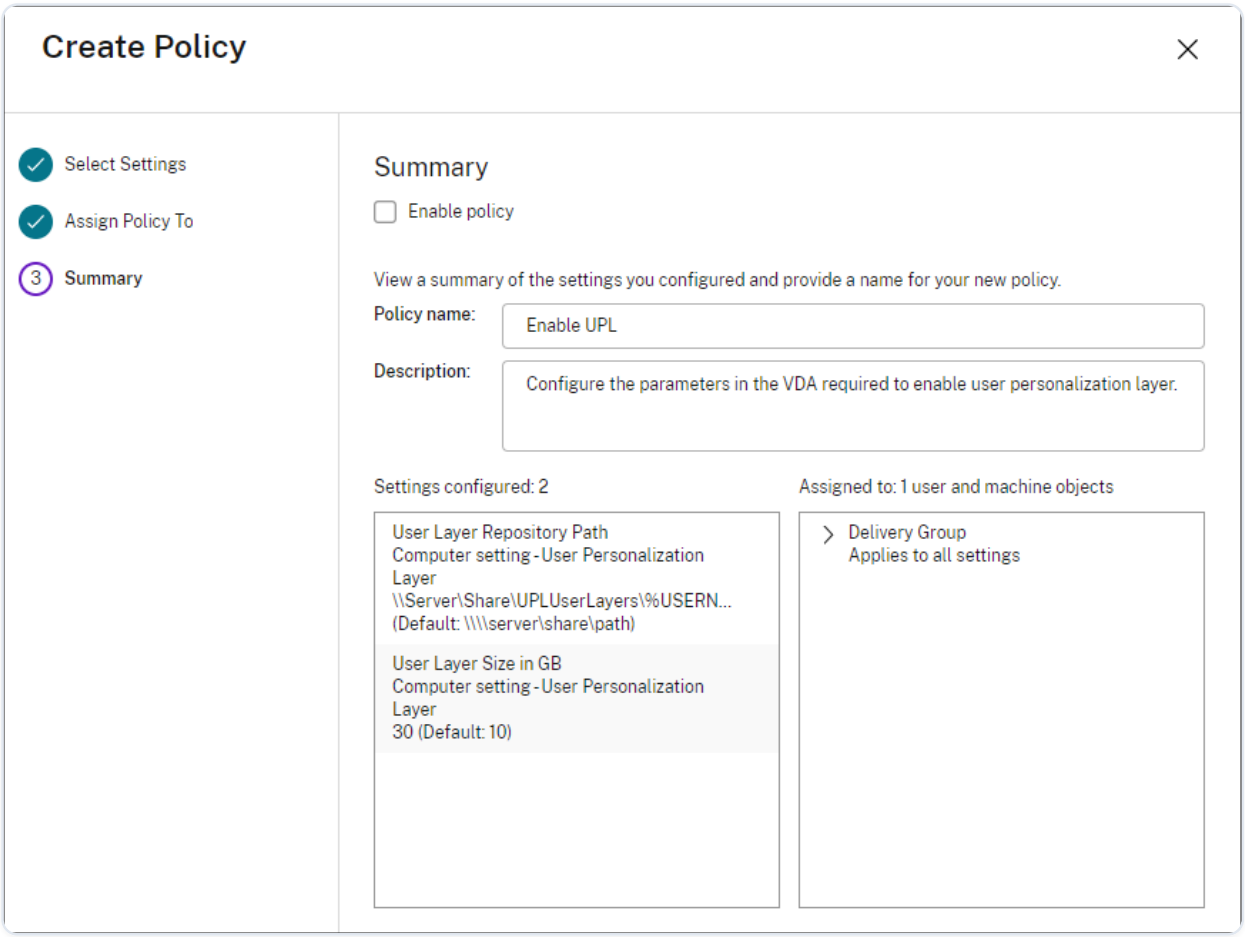
9. 可选：指定要排除的文件和文件夹，然后单击"**保存**"。有关详细信息，请参阅 Citrix App Layering 文档。
10. 单击"**下一步**"以配置要分配的用户和计算机。单击此图像中突出显示的"**交付组分配**"链接：



11. 在“**交付组**”菜单中，选择上一节中创建的交付组。单击“**确定**”。



12. 输入策略名称。选中复选框以启用策略，然后单击“**完成**”。



配置用户层文件夹上的安全设置

作为域管理员，您可以为用户层指定多个存储位置。为每个存储位置（包括默认位置）创建一个 `\Users` 子文件夹。使用以下设置保护每个位置。

设置名称	值	应用于	
创建者所有者	修改	仅子文件夹和文件	
所有者权限	修改	仅子文件夹和文件	
用户或组：	创建文件夹/追加数据；遍历文件夹/执行文件；列出文件夹/读取数据；读取属性	仅选定文件夹	
系统	完全控制	选定的文件夹、子文件夹和文件	
域管理员和选定的管理员组	完全控制	选定的文件夹、子文件夹和文件	

用户层消息

当用户无法访问其用户层时，他们会收到以下通知消息之一。

- **用户层正在使用中**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **用户层不可用**

  `We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **用户注销后系统未重置**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`.

故障排除时要使用的日志文件

日志文件 ulayersvc.log 包含用户个性化层软件的输出，其中记录了更改。

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

用户层/UPL 空间回收

您可以使用**用户层/UPL 空间回收**在用户每次注销时自动压缩 VHDX 文件。 有关详细信息，请参阅用户层/UPL 空间回收

限制

安装和使用用户个性化层功能时，请记住以下限制。

- 请*勿*尝试在 App Layering 中的层上部署用户个性化层软件。要么在 Citrix Virtual Apps and Desktops 中部署用户个性化层，要么在 App Layering 映像模板中启用用户层，两者不可兼得。这两种过程都会生成您所需的用户层。
- 请*勿*将用户个性化层功能与持久性计算机目录一起配置。
- *不要*使用会话主机。
- *不要*使用运行新操作系统安装的映像（即使是相同版本的 Windows 10）更新计算机目录。最佳做法是在创建计算机目录时使用的同一主映像中应用操作系统更新。

- *不要*使用启动时驱动程序或任何其他早期启动个性化设置。
- *不要*将 PvD 数据迁移到用户个性化层功能。
- *不要*将现有用户层从完整的 App Layering 产品迁移到用户个性化层功能。
- *不要*更改用户层 SMB 路径以访问使用不同主操作系统映像创建的用户层。
- 当用户注销会话并再次登录时，新会话将在池中的另一台计算机上运行。在 VDI 环境中，Microsoft Software Center 会将应用程序在第一台计算机上列为 **Installed**，但在第二台计算机上显示为 **Unavailable**。

  要查找应用程序的真实状态，请指示用户在 Software Center 中选择该应用程序并单击 **Install**。然后 SCCM 会将状态更新为真实值。
- 在启用了用户个性化层功能的 VDA 中，Software Center 有时会在启动后立即停止。为避免此问题，请遵循 Microsoft 关于在 XenDesktop VDI 环境中实施 SCCM 的建议。此外，请确保在启动 Software Center 之前 `ccmexec` 服务正在运行。
- 在组策略（计算机设置）中，用户层设置会覆盖应用于主映像的设置。因此，您使用 GPO 在计算机设置中所做的更改并非总是在用户下次会话登录时出现。

  为解决此问题，请创建一个发出以下命令的用户登录脚本：

  ```
  gpupdate /force
  ```

  例如，一位客户设置了以下命令在每次用户登录时运行：

  ```
  gpudate /Target:Computer /force
  ```

  为获得最佳结果，请在用户登录后，直接在用户层上应用对计算机设置的更改。
- 域用户帐户不得是最后登录到主映像的用户。否则，从该映像预配的计算机可能会出现问题。
- 在纯 Microsoft Entra 环境中启用 UPL 时，自定义证书不会持久存在，这是由于 Windows 在 Azure 上运行的底层问题所致。如果 Microsoft 在未来的增强功能中修复此问题，我们将更新本文。

删除组件

要删除组件，Citrix® 建议使用 Windows 的“删除或更改程序”功能。或者，您可以使用命令行或安装介质上的脚本来删除组件。

删除组件时，不会删除必备项，也不会更改防火墙设置。例如，当您删除 Delivery Controller™ 时，SQL Server 软件和数据库不会被删除。

如果您从包含 Web Interface 的早期部署升级了 Controller，则必须单独删除 Web Interface 组件。您不能使用安装程序来删除 Web Interface。

有关删除下面未提及的功能的信息，请参阅该功能的文档。

准备工作

在删除 Controller 之前，请将其从站点中删除。有关详细信息，请参阅删除 Controller。

在删除 Studio 和 Director 之前，请关闭它们。

使用 Windows 的删除或更改程序功能删除组件

从 Windows 的删除或更改程序功能中：

- 要删除 Controller、Studio、Director、License Server 或 StoreFront，请右键单击 **Citrix Virtual Apps *version*** 或 **Citrix Virtual Apps and Desktops™ *version***，然后选择**卸载**。安装程序将启动。选择要删除的组件。

  或者，您可以通过右键单击 **Citrix StoreFront** 并选择**卸载**来删除 StoreFront™。
- 要删除 VDA，请右键单击 **Citrix Virtual Delivery Agent *version***，然后选择**卸载**。安装程序将启动，您可以选择要删除的组件。默认情况下，计算机在删除后会自动重新启动。
- 要删除 Universal Print Server，请右键单击 **Citrix Universal™ Print Server**，然后选择**卸载**。

使用命令行删除核心组件

从 `\x64\XenDesktop Setup` 目录运行 `XenDesktopServerSetup.exe` 命令。

- 要删除一个或多个组件，请指定 `/remove` 和 `/components` 选项。
- 要删除所有组件，请指定 `/removeall` 选项。

有关命令和参数的详细信息，请参阅使用命令行安装。

例如，以下命令将删除 Web Studio。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components webstudio
```

如果在升级时，您首先使用命令 `\x64\Licensing\CitrixLicensing.exe /quiet` 或 `\x64\Licensing\CitrixLicensing.exe /quiet /l install.log` 安装了许可证服务器，然后安装了核心组件，则请按照相同的顺序进行卸载：

1. 使用命令行卸载许可证服务器：

```
CitrixLicensing.exe /quiet /uninstall /l uninstall.log
```

2. 使用 GUI 或命令行卸载组件。有关信息，请参阅删除组件。

如果您使用命令行 `XenDesktopServerSetup.exe` 或 `removeall` 卸载许可证服务器和组件，请清理注册表项和剩余文件。

清理注册表项：

1. 搜索注册表项 `Citrix Licensing` 并删除该条目。通常，您可以在以下位置找到该条目：

```
"Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\
```

2. 删除注册表项中 **Uninstall String** 指向的文件夹。

使用命令行删除 VDA

从 `\x64\XenDesktop Setup` 目录运行 `XenDesktopVdaSetup.exe` 命令。

- 要删除一个或多个组件，请使用 `/remove` 和 `/components` 选项。例如，要删除 VDA 和 Citrix Workspace 应用程序，请使用 `/remove /components vda,plugin`。
- `/removeall` 选项仅删除 VDA。它不会删除 Citrix Workspace 应用程序。

有关命令和参数的详细信息，请参阅使用命令行安装。

默认情况下，计算机在删除后会自动重新启动。

要使用 Active Directory 中的脚本删除 VDA，请参阅使用脚本安装或删除 VDA。

升级和迁移

本部分涵盖两项任务：将现有部署升级到较新版本，以及从早期部署迁移数据。

本节内容

- 升级：将现有部署升级到较新版本的 Citrix Virtual Apps and Desktops™，而无需设置新计算机或站点。包括准备工作、升级过程以及数据库和站点升级。
- 迁移：将本地部署迁移到云，或查找旧版 XenApp 6.x 迁移资源。

升级部署

升级会将您的部署更改为 Citrix Virtual Apps and Desktops™ 7 的较新版本，而无需设置新计算机或站点。此方法称为就地升级。

升级可让您访问符合条件的最新功能和技术。升级还可以包含早期版本中的修复、澄清和增强功能。

要开始升级，请运行新版本中的安装程序。安装程序会升级以前安装的核心组件、VDA 和某些其他组件。然后，您将升级数据库和站点。

升级概述

1. 在开始升级之前，请查看本文中的信息。本文是了解如何准备和实施升级的主要信息来源。
2. 确保您当前的 Customer Success Services 日期有效且未过期。有关详细信息，请参阅 Customer Success Services 续订许可证 文章。
3. 完成准备指南。
4. 运行安装程序以升级核心组件。
5. 升级系统数据库和站点。
6. 升级映像上的 VDA（或直接在计算机上升级）。
7. 升级其他组件。

每个准备和升级步骤都在 本节中 列出的文章中进行了详细说明。

升级前

在开始升级之前，请完成以下检查：

- 确认您可以升级哪些版本。请参阅您可以升级的版本。
- 确保您当前的客户成功服务日期有效且未过期。有关详细信息，请参阅客户成功服务续订许可证文章。
- 开始之前，请查看本文中的所有信息。

您可以升级的版本

您可以从以下版本升级到 Citrix Virtual Apps and Desktops™ 2507 LTSR：

- Virtual Apps and Desktops 2402 LTSR（含或不含 CU，最高包括 CU2）
- Virtual Apps and Desktops 2203 LTSR（含或不含 CU，最高包括 CU6）
- 当前支持的 Citrix Virtual Apps and Desktops CR 版本

> 注意：
>
> - 在启动升级过程之前，Citrix® 建议客户在受控环境中测试升级，并验证其是否满足特定要求。此外，我们建议查阅所有相关产品文档，包括弃用列表和已知问题，以确保平稳过渡。此方法有助于减轻对生产系统的潜在中断，并增强整体升级体验。 有关支持版本列表的更多信息，请参阅产品兼容性列表。

可以升级的内容

使用以下准则确定可以升级的内容以及在哪里查找指导：

- 当提供新版本时，完整产品安装程序或独立 VDA 安装程序可以安装的任何组件。
- 对于未随完整产品安装程序安装的组件（例如 Citrix Provisioning™ 和 Profile Management），请参阅该组件的文档以获取指导。
- 有关主机升级，请参阅相应的文档。

升级期间的预期

规划容量减少和短暂的服务中断。在安排升级之前，请了解其影响：

- **站点可用性：** 如果您首先升级一半的 Delivery Controller，用户仍然可以访问站点。VDA 会向剩余的 Controller 注册。当可用 Controller 较少时，站点可能会以降低的容量运行。

- **单 Controller 站点：** 如果您的站点只有一个 Controller，则在升级期间站点将无法运行。
- **数据库升级：** 在数据库升级期间，产品服务将被禁用。服务禁用期间，Controller 无法为站点代理新连接。
- **新连接：** 在数据库升级的最后步骤中，建立新的客户端连接时预计会出现短暂中断。在整个站点升级完成之前，已升级的 Controller 无法处理请求。

开始之前备份数据库。请参阅备份数据库。

本节内容

从端到端序列的升级过程开始。该过程的步骤 1 会引导您完成必须首先完成的准备任务。以下文章支持升级：

- 升级过程：按照分步序列升级您的组件、数据库和站点。从此处开始。
- 注意事项和限制：查看限制、混合环境指南和操作系统支持。
- 准备工作：完成升级前检查表和准备任务，包括 SQL Server 版本检查、初步站点测试以及删除 PvD、AppDisks 和不受支持的主机。准备工作是升级过程的步骤 1。
- 升级数据库和站点：完成详细的数据库和站点升级，无论是自动还是手动。
- 常见问题：查找有关升级顺序、版本、许可和权限的常见问题解答。

更多信息

长期服务版本 (LTSR)

长期服务版本 (LTSR) 部署更新使用累积更新 (CU)。CU 会更新 LTSR 的基线组件，并且每个 CU 都包含其自己的元安装程序。

每个 CU 都具有专门的文档。例如，对于 2203 LTSR，请在该 LTSR 的“**新增功能**”页面上查看链接以获取最新的 CU。每个 CU 页面都包含支持的版本信息、说明以及 CU 下载包的链接。

升级过程

大多数主要产品组件都可以通过在包含该组件的计算机上运行产品安装程序进行升级。如果一台计算机包含多个组件（例如 Studio 和许可证服务器），则如果产品介质包含其软件的较新版本，该计算机上的所有组件都将升级。

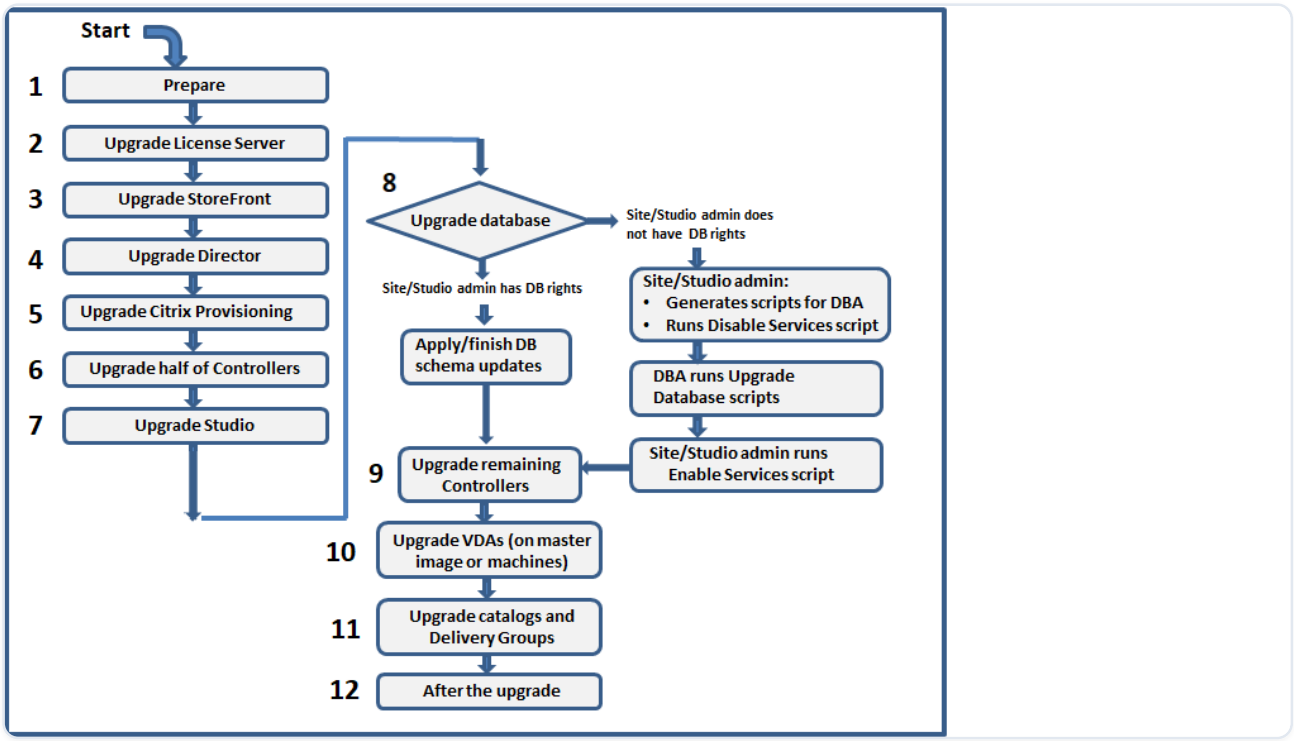
要使用安装程序：

- 要运行完整产品安装程序的图形界面，请登录到计算机，然后插入介质或装载新版本的 ISO 驱动器。双击 **AutoSelect**。

- 要使用命令行界面，请发出相应的命令。请参阅使用命令行安装。

升级顺序

下图显示了升级顺序中的步骤。图表后面的步骤包含每个步骤的详细信息。



步骤 1：准备

在开始升级之前，请查看先决条件并完成升级前检查表。准备任务包括验证许可证、备份数据库以及选择安装程序。有关详细信息，请参阅准备。

步骤 2：升级许可证服务器

如果安装包含新版本的 Citrix 许可证服务器软件，请先升级此组件，然后再升级任何其他组件。

如果您尚未确定您的许可证服务器是否与新版本兼容，则必须在升级任何其他核心组件之前在许可证服务器上运行安装程序。

步骤 3：升级 StoreFront™

如果安装介质包含新版本的 StoreFront 软件，请在包含 StoreFront 服务器的计算机上运行安装程序。

- 在图形界面中，从“**扩展部署**”部分选择 **Citrix StoreFront**。
- 从命令行运行 `CitrixStoreFront-x64.exe`，该文件位于 Citrix Virtual Apps and Desktops 安装介质的 `x64` 文件夹中。

步骤 4：升级 Director

如果安装介质包含新版本的 Director 软件，请在包含 Director 的计算机上运行安装程序。

步骤 5：升级 Citrix Provisioning

Citrix Provisioning 安装介质与 Citrix Virtual Apps and Desktops 安装介质是分开提供的。要了解如何安装和升级 Citrix Provisioning 服务器和目标设备软件，请参阅 Citrix Provisioning 产品文档。

步骤 6：升级一半的 Delivery Controller

例如，如果您的站点有四个 Controller，请在其中两个上运行安装程序。

保持一半的 Controller 处于活动状态可让用户访问站点。VDA 可以向其余 Controller 注册。有时，由于可用的 Controller 较少，站点的容量可能会降低。升级仅在最终数据库升级步骤中导致建立新客户端连接的短暂中断。升级后的 Controller 无法处理请求，直到整个站点升级完成。

如果您的站点只有一个 Controller，则在升级期间它将无法运行。

实际升级开始之前，将在第一个 Controller 上运行初步站点测试。有关详细信息，请参阅 运行初步站点测试。

> **注意：**
>
> Site Manager 会随 Delivery Controller 一起自动升级。

步骤 7：升级 Web Studio

如果您尚未升级 Web Studio（因为它与另一个组件位于同一台计算机上），请在包含 Studio 的计算机上运行安装程序。

> **注意：**
>
> 升级 Web Studio 后，版本信息可能不会立即更新。即使 Web Studio 已是最新版本，系统也可能会提示您升级它。要解决此问题，请转到 Web Studio 服务器，打开 Internet Information Services (IIS) Manager，导航到“开始页”>“站点”>“默认网站”，然后在“**管理网站**”窗格中选择“**重新启动**”。

步骤 8：升级数据库和站点

> **注意：**
>
> 为避免故障，您必须在执行任何与预配和交付组相关的任务（例如创建新的计算机目录、删除计算机目录、更新交付组中的计算机等）之前，升级所有 Delivery Controller 和数据库。

> 升级 Delivery Controller 后，升级数据库和站点。您可以自动或手动升级，具体取决于您的数据库权限：

- 如果您有权更新 SQL Server 数据库架构，请启动自动升级。
- 如果您没有足够的权限，请启动使用脚本的手动升级。在数据库管理员的帮助下完成升级。

Citrix 强烈建议您在升级前备份数据库。在数据库升级期间，产品服务将禁用。在此期间，Controller 无法为站点代理新连接，因此请仔细规划。

有关详细步骤，请参阅 升级数据库和站点。

步骤 9：升级剩余的 Delivery Controller

升级剩余的 Delivery Controller。完成升级后，关闭并重新打开 Site Manager。Site Manager 可能会提示您执行额外的站点升级，以将 Delivery Controller 的服务注册到站点。

步骤 10：升级 VDA

> **重要提示：**
>
> 如果您要将 VDA 升级到版本 1912 或更高版本，请参阅 将 VDA 升级到 1912 或更高版本。

> 在包含 VDA 的计算机上运行产品安装程序。

如果您使用 Machine Creation Services™ 和主映像创建了计算机，请转到您的主机并升级主映像上的 VDA。您可以使用任何可用的 VDA 安装程序。

- 有关图形界面指导，请参阅 安装 VDA。
- 有关命令行指导，请参阅 使用命令行安装。

如果您使用 Citrix Provisioning 创建了计算机，请参阅 Citrix Provisioning 产品文档 以获取有关升级的指导。

步骤 11：更新计算机目录和交付组

升级 VDA 后，更新使用这些计算机的计算机目录和交付组。请执行以下任务：

- 更新使用已升级 VDA 的计算机的目录。
- 升级使用已升级 VDA 的计算机的目录。
- 升级使用已升级 VDA 的计算机的交付组。

步骤 12：升级后

升级部署中的其他组件。有关指导，请参阅以下产品文档：

- StoreFront
- AppDNA
- Citrix 应用分层
- HDX 实时优化包
- 配置文件管理
- Citrix 预配
- 会话录制
- 工作区环境管理

如果您需要将 Microsoft SQL Server Express LocalDB 软件替换为更高版本，请参阅替换 SQL Server Express LocalDB。

升级注意事项和限制

开始升级之前，请查看这些限制和相关注意事项。它们会影响您可以升级的组件以及支持的操作系统。

以下限制适用于升级：

- **选择性组件安装：** 如果您将任何组件安装或升级到新版本，但选择不升级需要升级的其他组件（在不同的计算机上），Studio 会提醒您。例如，假设升级包括新版本的 Controller 和 Studio。您升级了 Controller，但未在安装 Studio 的计算机上运行安装程序。Studio 将不允许您继续管理站点，直到您升级 Studio。

  您不必升级 VDA，但 Citrix 建议升级所有 VDA，以便您可以使用所有可用功能。
- **早期版本或技术预览版本：** 您无法从早期版本、技术预览版或预览版进行升级。
- **早期操作系统上的组件：** 您无法在 Microsoft 或 Citrix 不再支持的操作系统上安装当前 VDA。有关详细信息，请参阅早期操作系统。

- **混合环境/站点：** 如果您必须继续运行早期版本站点和当前版本站点，请参阅混合环境注意事项。
- **产品选择：** 从早期版本升级时，您无需选择或指定在安装期间设置的产品（Citrix Virtual Apps 或 Citrix Virtual Apps and Desktops）。

早期操作系统

假设您在运行受支持的操作系统 (OS) 版本的计算机上安装了某个组件的早期版本。现在，您想使用较新的组件版本，但该操作系统不再受当前组件版本支持。

例如，假设您在 Windows Server 2016 计算机上安装了服务器 VDA。现在您想将该 VDA 升级到当前版本，但 Windows Server 2016 不受您要升级到的当前版本支持。

如果您尝试在不再允许的操作系统上安装或升级组件，则会显示错误消息，例如“无法在此操作系统上安装”。

这些注意事项适用于升级当前版本和长期服务版本。（这些注意事项不影响将 CU 应用于 LTSR 版本。）

单击链接以了解支持哪些操作系统：

- Citrix 虚拟应用和桌面 (当前版本):
  - 交付控制器、Studio、Director、VDA、通用打印服务器
  - 联合身份验证服务
  - 对于 StoreFront、自助密码重置 和 会话录制，请参阅当前版本的系统要求文章。
- 对于 LTSR，请参阅您的 LTSR 版本和 CU 的组件列表。（从主要的 Citrix Virtual Apps and Desktops 产品文档页面中选择您的 LTSR 版本。）

无效的操作系统

下表列出了当前版本中不适用于安装/升级组件的早期操作系统。它指出了每个列出的操作系统支持的最新有效组件版本，以及安装和升级变得无效的组件版本。

表中的操作系统包括 Service Pack 和更新。

操作系统	组件/功能	最新有效版本	从该版本起无法安装/升级
Windows 7 和 Windows 8 操作系统	VDA	7.15 LTSR	7.16

操作系统	组件/功能	最新有效版本	从该版本起无法安装/升级
Windows 7 和 Windows 8 操作系统	其他安装程序组件	7.17	7.18
早于 1607 的 Windows 10 版本	VDA	7.15 LTSR	7.16
Windows 10 x86 版本	VDA	1906.2.0	1909
Windows 服务器 2008 R2	VDA	7.15 LTSR	7.16
Windows 服务器 2008 R2	其他安装程序组件	7.17	7.18
Windows 服务器 2012	VDA	7.15 LTSR	7.16
Windows 服务器 2012	其他安装程序组件	7.17	7.18
Windows 服务器 2012 R2	其他安装程序组件 *	1912 LTSR	2003
Windows 服务器 2012 R2	服务器 VDI	7.15 LTSR	7.16
Windows 服务器 2016	服务器 VDI	7.15 LTSR	7.16

Windows XP 和 Windows Vista 不适用于任何 7.x 组件或技术。

* 适用于 交付控制器、管理控制台、监控器 和 VDA。

您可以执行的操作

您有多种选择。您可以：

- 继续使用当前操作系统
- 重新创建映像或升级计算机
- 添加新计算机，然后删除旧计算机

继续使用当前操作系统

这些方法适用于 VDA。如果您想继续使用早期操作系统的计算机，可以选择以下方法之一：

- 继续使用已安装的组件版本。
- 下载最新的有效组件版本，然后将组件升级到该版本。（此选项假定尚未安装最新的有效组件版本。）

例如，您在 Windows 7 SP1 计算机上有一个 7.14 VDA。Windows 7 操作系统计算机上最新的有效 VDA 版本是 XenApp and XenDesktop 7.15 LTSR。您可以继续使用 7.14，也可以下载 7.15 LTSR VDA，然后将 VDA 升级到该版本。这些较早的 VDA 版本可在包含较新版本 Delivery Controller 的部署中运行。例如，7.15 LTSR VDA 可以连接到 Citrix Virtual Apps and Desktops 7 1808 Controller。

重新创建映像或升级计算机

这些方法适用于 VDA 和未安装核心组件（例如 Delivery Controller）的其他计算机。请选择以下方法之一：

- 将计算机停用（开启维护模式并允许所有会话关闭）后，您可以将其重新映像到受支持的 Windows 操作系统版本，然后安装最新版本的组件。
- 要在不重新映像的情况下升级 VDA 计算机中的操作系统，您必须首先安装您要升级到的操作系统所支持的 VDA 版本，或者在升级操作系统后升级 VDA。否则，Citrix 软件将不受支持。在不卸载 VDA 的就地升级过程中，您可以升级到以下最低操作系统版本：
  - Windows 11，安装了 2023-07 Cumulative Update for Windows 11 (KB5028185) 或更高版本（内部版本 22621.1992 或更高版本）。
  - 安装了 适用于 Windows 10 的 2023 年 7 月动态更新 (KB5028311) 的 Windows 10。
- 如果您计划升级到的 Windows 版本不符合上述准则，则必须在升级操作系统之前卸载 VDA，然后在操作系统升级完成后安装受支持的 VDA 版本。

添加新计算机，然后移除旧计算机

如果您必须升级包含 Delivery Controller™ 或其他核心组件的计算机上的操作系统，此方法是可行的。

Citrix 建议站点中的所有控制器都使用相同的操作系统。以下升级顺序可最大程度地缩短不同控制器使用不同操作系统的时间间隔。

1. 对站点中的所有 Delivery Controller 进行快照，然后备份站点数据库。
2. 在新服务器上安装新的 Delivery Controller，并使用受支持的操作系统。
3. 将新控制器添加到站点。

4. 移除在当前版本不支持的操作系统上运行的控制器。请遵循 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/manage-deployment/delivery-controllers.html) 中有关移除控制器的建议。

混合环境注意事项

升级时，Citrix 建议您升级所有组件和 VDA，以便您可以使用您的版本中的所有新增和增强功能。

例如，尽管您可以在包含早期控制器版本的部署中使用当前 VDA，但当前版本中的新功能可能不可用。使用非当前版本时，也可能会出现 VDA 注册问题。

在某些环境中，您可能无法将所有 VDA 升级到最新版本。在这种情况下，当您创建计算机目录时，可以指定安装在计算机上的 VDA 版本。（此设置称为功能级别。）默认情况下，此设置指定建议的最低 VDA 版本。默认值足以满足大多数部署。仅当目录包含早于默认版本的 VDA 时，才考虑将设置更改为更早的版本。不建议在计算机目录中混合使用 VDA 版本。

如果使用默认的最低 VDA 版本设置创建目录，并且一台或多台计算机的 VDA 版本早于默认版本，则这些计算机将无法向 Controller 注册，并且无法正常工作。

有关详细信息，请参阅 VDA 版本和功能级别。

具有不同版本的多个站点

当您的环境包含具有不同产品版本的站点（例如，XenDesktop 7.18 站点和 Citrix Virtual Apps and Desktops 1909 站点）时，Citrix 建议使用 StoreFront 聚合来自不同产品版本的应用程序和桌面。有关详细信息，请参阅 StoreFront 文档。

在混合环境中，继续使用每个版本的 Studio 和 Director，但请确保将不同版本安装在单独的计算机上。

准备工作

在开始升级之前，请查看以下信息并完成必要的任务。

> **注意：**
>
> 尽管 VDA 升级在 升级过程 中稍后进行，但最好在开始升级之前选择安装程序并查看该过程，以便您了解预期情况。

升级前检查清单

在开始升级之前完成以下任务。每个项目都链接到其详细信息：

- 确认您的客户成功服务日期对新版本有效。请参阅 验证您的 Citrix 许可。

- 验证您的许可证服务器与新版本兼容。请参阅 验证许可证服务器兼容性。
- 如果您拥有混合权利许可证，请 更新混合权利许可证。
- 备份站点、监视和配置日志记录数据库。请参阅 备份数据库。
- 确认您的 SQL Server 版本受支持。请参阅 检查 SQL Server 版本。
- 备份所有 StoreFront 修改。请参阅 备份所有 StoreFront 修改。
- 删除 PvD、AppDisks 和不受支持的主机连接。请参阅 删除 PvD、AppDisks 和不受支持的主机。
- 关闭控制台和 PowerShell 会话，并停止第三方监视代理。请参阅 关闭应用程序和控制台。
- 确认您具有所需的权限。请参阅 验证您的权限。
- 选择安装程序和界面。请参阅 选择安装程序和界面。

选择安装程序和界面

使用产品 ISO 中的完整产品安装程序升级组件。您可以使用完整产品安装程序或独立 VDA 安装程序之一升级 VDA。所有安装程序都提供图形界面和命令行界面。

有关详细信息，请参阅安装程序。

安装详情： 完成所有准备工作并准备好启动安装程序后，安装文章将向您展示您将看到的内容（如果您使用的是图形界面）或要键入的内容（如果您使用的是命令行界面）。

- 使用图形界面安装/升级核心组件
- 使用命令行安装/升级核心组件
- 使用图形界面安装/升级 VDA
- 使用命令行安装/升级 VDA

对于单会话操作系统，有四种不同的安装程序可用。Citrix 建议在 Citrix VDA 的整个生命周期（包括安装、升级和卸载）中始终使用一致的安装程序类型。有关详细信息，请参阅使用单会话 VDA 安装程序的最佳实践

将 VDA 升级到当前版本时，在升级过程中会发生计算机重新启动。（此要求始于 7.17 版本。）无法避免重新启动。重新启动后，升级会自动恢复（除非您在命令行中指定 `/noresume`）。

验证您的 Citrix 许可

有关管理 Citrix 许可的全面信息，请参阅激活、升级和管理 Citrix 许可证。

您可以使用完整产品安装程序升级许可证服务器。或者，您可以单独下载和升级许可证组件。请参阅升级。

升级之前，请确保您的客户成功服务/软件维护/订阅权益日期对新产品版本有效。日期必须至少为 2021.11.15。

验证许可证服务器兼容性

确保您的 Citrix 许可证服务器与新版本兼容。有两种方法可以验证兼容性：

- 在升级任何其他 Citrix 组件之前，请在包含 Delivery Controller 的计算机上从 ISO 布局运行 `XenDesktopServerSetup.exe` 安装程序。如果存在任何不兼容问题，安装程序会报告并提供建议的解决步骤。
- 在安装介质的 `XenDesktop Setup` 目录中，运行命令：`.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`。显示屏会指示许可证服务器是否兼容。如果许可证服务器不兼容，请升级许可证服务器。

更新混合权利许可证

混合权利许可证是基于期限的订阅许可证，当客户从永久许可证过渡或升级到云服务订阅时，除了云服务订阅之外，还会提供此类许可证。您还可以随 DaaS 订阅购买混合权利附加组件。

具有 SaaS 属性的混合权利许可证

当您升级到 Citrix Virtual Apps and Desktops™ LTSR 2203 及更高版本时，您将有资格获得 LTSR 1912 不具备的功能。这些功能包括在 Microsoft Azure、AWS EC2 和 Google Cloud 等公共云中预配和托管工作负载。在部署新的许可证文件之前，请将您的许可证服务器更新到最新版本。如果您跳过此先决条件，更新将阻止 Citrix Virtual Apps and Desktops 站点升级和站点创建。

不带 SaaS 属性的混合权利许可证

请按照以下步骤获取具有 SaaS 属性的新混合权利许可证：

> **注意：**
>
> - 您会收到一封包含新许可证代码的电子邮件。有关详细信息，请参阅使用许可证访问代码。
> - 您现有的许可证已被撤销。撤销的许可证必须从许可证服务器中删除，然后才能安装新许可证。有关详细信息，请参阅删除许可证文件。

1. 转到 citrix.com 管理许可证门户，下载已启用云预配权限（SaaS 属性）的新混合权利许可证文件。有关详细信息，请参阅下载许可证。下图显示了“增量”部分中具有 SaaS 属性的混合权利许可证文件。

```
INCREMENT XDT_PLT_CCS CITRIX 2022.1201 01-dec-2022 5 \
    VENDOR_STRING=;LT=RetailS;GP=720;PSL=10;CL=VDS,VDA,VDE,VDP,SaaS:SA=0;ODP=0;NUDURMIN=2880;NUDURMAX=525600;AP=ADMIN/INT/14
    OVERDRAFT=1 DUP_GROUP=V ISSUED=18-dec-2005 NOTICE="Citrix \
    Systems Inc." SN=RetailSSaaS SIGN="..."
```

2. 在许可证服务器上安装混合权利许可证文件。有关详细信息，请参阅安装许可证。
3. 如果许可证版本或模型发生更改，请确保运行 broker 命令来设置版本和模型，然后开始就地升级。有关 Broker 命令的详细信息，请参阅Broker PowerShell SDK 部分。

有关 Citrix Virtual Apps and Desktops 当前版本和长期服务版本对公共云支持的更多信息，请参阅 CTX270373。

备份数据库

备份站点、监视和配置日志数据库。请按照 CTX135207 中的说明进行操作。如果在升级后发现任何问题，可以还原备份。

有关升级不再受支持的 SQL Server 版本的信息，请参阅检查 SQL Server 版本。（SQL Server 版本检查是指用于站点、监视和配置日志数据库的 SQL Server。）

Microsoft SQL Server Express LocalDB 会自动安装，以用于本地主机缓存。如果需要替换早期版本，新版本必须是 SQL Server Express LocalDB 2019。有关在升级组件和站点后用新版本替换 SQL Server Express LocalDB 的详细信息，请参阅替换 SQL Server Express LocalDB。

检查 SQL Server 版本

成功的 Citrix Virtual Apps and Desktops 部署需要受支持的 Microsoft SQL Server 版本用于站点、监视和配置日志数据库。使用不再受支持的 SQL Server 版本升级 Citrix 部署可能会导致功能问题，并且站点将不受支持。

要了解您要升级到的 Citrix 版本支持哪些 SQL Server 版本，请参阅该版本的系统要求文章。

升级 Controller 时，Citrix 安装程序会检查用于站点、监视和配置日志数据库的当前安装的 SQL Server 版本。

- 如果检查确定当前安装的 SQL Server 版本不是您要升级到的 Citrix 版本中支持的版本：
  - 图形界面：升级将暂停并显示一条消息。单击**我理解**，然后单击**取消**以关闭 Citrix 安装程序。（您无法继续升级。）
  - 命令行界面：命令失败（即使您在命令中包含了 `/ignore_db_check_failure` 选项）。

  升级 SQL Server 版本，然后再次启动 Citrix 升级。
- 如果检查无法确定当前安装的 SQL Server 版本，请查看您当前安装的版本是否在您要升级到的版本中受支持（系统要求）。

- 图形界面：升级将暂停并显示一条消息。
  - 如果当前安装的 SQL Server 版本受支持，请单击**我理解**以关闭消息，然后单击**下一步**以继续 Citrix 升级。
  - 如果当前安装的 SQL Server 版本不受支持，请单击**我理解**以关闭消息，然后单击**取消**以结束 Citrix 升级。将 SQL Server 升级到受支持的版本，然后再次启动 Citrix 升级。
- 命令行界面：命令失败并显示消息。关闭消息后：
  - 如果当前安装的 SQL Server 版本受支持，请使用 `/ignore_db_check_failure` 选项再次运行该命令。
  - 如果当前安装的 SQL Server 版本不受支持，请将 SQL Server 升级到受支持的版本。再次运行该命令以启动 Citrix 升级。

升级 SQL Server

如果您部署新的 SQL Server 服务器并迁移站点数据库，则必须更新连接字符串。

如果站点当前使用 SQL Server Express 作为站点数据库（Citrix 在站点创建期间自动安装）：

1. 安装最新版本的 SQL Server Express。
2. 分离数据库。
3. 将数据库附加到新的 SQL Server Express。
4. 迁移连接字符串。

有关详细信息，请参阅配置连接字符串 和 Microsoft SQL Server 产品文档。

备份所有 StoreFront 修改

在开始升级之前，如果您修改了 `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data` 中的文件（例如 *default.ica* 和 *usernamepassword.tfrm*），请为每个应用商店备份这些文件。升级后，您可以还原这些文件以恢复您的修改。

删除 PvD、AppDisks 和不受支持的主机

以下技术和主机类型在 Citrix Virtual Apps and Desktops 7 Current Release 部署中不受支持：

- **Personal vDisks (PvD)**，用于在目录中用户的 VM 旁边存储数据。用户个性化层功能现在处理用户持久性。
- **AppDisks**，用于管理交付组中使用的应用程序。
- **主机类型：** Azure Classic、CloudPlatform（原始 Citrix 产品）。

- 有关此版本中支持的主机类型，请参阅系统要求。

如果您的当前部署使用 PvD 或 AppDisks，或者连接到不受支持的主机类型（例如 Microsoft Azure Classic），则只有在删除使用这些技术的项目后，才能升级到版本 2006（或更高版本）。如果您的当前部署使用公共云主机连接（例如 AWS），请确保在升级前拥有混合权利许可证。当安装程序检测到一种或多种不受支持的技术或没有混合权利许可证的主机连接时，升级将暂停或停止，并显示一条解释性消息。安装程序日志中包含详细信息。

为确保成功升级，请查看并遵循有关删除不受支持项目的适用指南。

- 删除 PvD
- 删除 AppDisks
- 删除不受支持的主机项目
- 从 VDA 中删除 PvD 或 AppDisks 组件

即使您在部署中未使用 PvD 或 AppDisks，相关的 MSI 也可能已包含在较早的 VDA 安装或升级中。在将 VDA 升级到版本 2006（或更高版本）之前，您必须删除该软件，即使您从未使用过它。使用图形界面时，可以为您完成此删除操作，或者在使用 CLI 时包含删除选项。有关详细信息，请参阅从 VDA 中删除 PvD 或 AppDisks 组件。

删除 PvD

在删除所有配置为使用 PvD 的计算机之前，部署升级无法成功。此删除会影响目录和交付组。

要从组和目录中删除 PvD：

1. 在 Studio 中，如果交付组包含使用 PvD 的目录中的计算机，请(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/delivery-groups-manage.html#remove-a-machine-from-a-delivery-group)。
2. 在 Studio 中，(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/machine-catalogs-manage.html#delete-a-catalog)包含使用 PvD 的计算机的所有目录。

VDA 升级： 部署升级不会检测 VDA 是否安装了 AppDisk 或 PvD 组件。但是，VDA 安装程序会检测。有关详细信息，请参阅(#remove-pvd-or-appdisks-components-from-vdas)。

如果您计划使用 App Layering 而不是 PvD，请参阅(/zh-cn/citrix-virtual-apps-desktops/1912-ltsr/install-configure/personal-vdisk/migrate-to-app-layering.html)以了解有关移动数据的信息。

删除 AppDisk

在您从所有使用 AppDisk 的交付组中删除 AppDisk，然后删除 AppDisk 本身之前，部署升级无法继续。

1. 在 Studio 导航窗格中选择 **交付组**。
2. 选择一个组，然后在“操作”窗格中单击**管理 AppDisk**。
3. 单击从组中删除 AppDisk 的操作。
4. 对每个使用 AppDisk 的交付组重复步骤 2 和 3。
5. 在 Studio 导航窗格中选择**AppDisk**。
6. 选择一个 AppDisk，然后单击删除该 AppDisk 的操作。
7. 对每个 AppDisk 重复步骤 5 和 6。

VDA 升级： 部署升级不会检测 VDA 是否安装了 AppDisk 或 PvD 组件。但是，VDA 安装程序会检测。有关详细信息，请参阅(#remove-pvd-or-appdisks-components-from-vdas)。

删除不受支持的主机项

如果站点连接到不受支持的主机类型（例如 Citrix CloudPlatform 或 Microsoft Azure Classic），则无法升级到版本 2006（或更高受支持版本）。在尝试升级之前，请完成以下任务。

在 Studio 中：

- 删除所有连接 到不支持的主机。
- 如果交付组包含使用来自不支持主机的主映像创建的目录中的计算机，请从组中删除这些计算机。
- 删除所有目录，这些目录是使用来自不支持主机的主映像创建的。

从 VDA 中删除 PvD 或 AppDisks 组件

如果启用了 PvD 和 AppDisks 技术的组件安装在 VDA 上，则在删除这些组件之前，该 VDA 无法升级。即使您从未使用过 PvD 或 AppDisks，此限制也适用。

> **注意：**
>
> 升级到版本 1912 时，您必须卸载当前 VDA，然后安装新的 VDA。在此版本中，系统会询问您是否希望 Citrix 删除组件，然后继续升级。
>
> AppDisk 和 PvD 组件可能已在早期 VDA 版本中安装，即使您从未使用过这些技术：

- 图形界面：在 VDA 安装程序中，**附加组件**页面包含 **Citrix AppDisk / Personal vDisk** 选项。7.15 LTSR 和更早的 7.x 版本默认启用此选项。因此，如果您接受了默认设置（或在提供此选项的任何版本中明确启用了此选项），则会安装该组件。

- 命令行界面：指定 `/baseimage` 选项会安装该组件。

删除组件

如果 VDA 安装程序未在当前安装的 VDA 中检测到 AppDisks 或 PvD 组件，则升级照常进行。

如果安装程序在当前安装的 VDA 中检测到 AppDisks 或 PvD 组件：

- 图形界面：升级暂停。一条消息会询问您是否要自动删除不支持的组件。如果您单击 **OK**，组件将自动删除，然后升级继续进行。
- 命令行界面：为避免命令失败，请在命令中包含以下选项：
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

继续在早期 WINDOWS 版本上使用 PVD

如果您想在 Windows 10（1607 及更早版本，未更新）计算机上继续使用 PvD，VDA 7.15 LTSR 是最新支持的版本。

> **注意：**
>
> *我可以在 XenApp and XenDesktop 7.15 LTSR 中将 Personal vDisk 与 Windows 7 桌面结合使用吗？*
>
> Citrix 于 2016 年 1 月宣布将 Personal vDisk (PvD) 从 XenApp and XenDesktop 7.6 LTSR 中排除。此外，Citrix 已宣布弃用 PvD 技术，并建议客户今后开始使用 Citrix App Layering。Citrix App Layering（版本 4.4 及更高版本）是 XenApp and XenDesktop 7.15 LTSR 的兼容组件。但是，为了帮助客户将 Windows 7 上现有的 PvD 部署迁移到 Citrix App Layering 技术，Citrix 已决定通过 XenApp and XenDesktop 7.15 LTSR 累积更新 (CU) 为 Windows 7 桌面上的 PvD 部署提供限时支持，直至 Jan 14, 2020。PvD 组件将从 LTSR CU 中删除，并且在 Jan 14, 2020 之后将不再受支持。此外，在 Jan 14, 2020 之后将 PvD 用于 Windows 7 将导致 LTSR 站点不合规。此外，适用于 Windows 10 的 PvD 仍被排除在 7.15 LTSR 之外。因此，客户不得将其与 7.15 LTSR 站点一起使用。

关闭应用程序和控制台

在开始升级之前，请关闭所有可能导致文件锁定的程序，包括管理控制台和 PowerShell 会话。

重新启动计算机可确保清除所有文件锁定，并且没有待处理的 Windows 更新。

在开始升级之前，请停止并禁用任何第三方监控代理服务。

验证您的权限

除了是域用户之外，您还必须是正在升级产品组件的计算机上的本地管理员。

站点数据库和站点可以自动或手动升级。对于自动数据库升级，Studio 用户的权限必须包括更新 SQL Server 数据库架构的能力（例如，`db_securityadmin` 或 `db_owner` 数据库角色）。有关详细信息，请参阅数据库。

如果 Studio 用户没有这些权限，则启动手动数据库升级会生成脚本。Studio 用户从 Studio 运行部分脚本。数据库管理员使用 SQL Server Management Studio 等工具运行其他脚本。

运行初步站点测试

升级 Delivery Controller 和站点时，在实际升级开始之前会运行初步站点测试。这些测试验证：

- 站点数据库可访问且已备份
- Citrix 基本服务的连接正常工作
- Citrix 许可证服务器地址可用
- 可以访问配置日志数据库
- 如果要添加公共云主机连接（例如 AWS），请确保您拥有混合权利许可证。否则，初步站点测试将暂停或停止，并显示一条解释性消息。

测试运行后，您可以查看结果报告。然后，您可以修复检测到的任何问题，并再次运行测试。未能运行初步站点测试并解决任何问题可能会影响站点的运行方式。

包含测试结果的报告是一个 HTML 文件 (`PreliminarySiteTestResult.html`)，位于与安装日志相同的目录中。如果该文件不存在，则会创建该文件。如果该文件存在，则其内容将被覆盖。

运行测试

- 当您使用安装程序的图形界面进行升级时，向导中包含一个页面，您可以在其中启动测试并显示报告。测试运行后，查看报告并解决发现的任何问题后，可以重新运行测试。测试成功完成后，单击“下一步”继续向导。
- 当您使用命令行界面进行升级时，测试会自动运行。默认情况下，如果测试失败，则不执行升级。查看报告并解决问题后，重新运行命令。

Citrix 建议始终运行初步站点测试，然后解决任何问题，再继续 Controller 和站点升级。运行测试所花费的几分钟时间非常值得。但是，您可以覆盖此建议操作。

- 使用图形界面升级时，您可以选择跳过测试并继续升级。

- 从命令行升级时，无法跳过测试。默认情况下，站点测试失败会导致安装程序失败，而不执行升级。通常，如果包含 `/ignore_site_test_failure` 选项，则会忽略任何测试失败并继续升级。（有关例外情况，请参阅检查 SQL Server 版本。）

升级多个 Controller

当您在一个 Controller 上启动升级，然后在同一站点中启动另一个 Controller 的升级时（在第一个升级完成之前）：

- 如果在第一个 Controller 上完成了初步站点测试，则初步站点测试页面不会显示在其他 Controller 的向导中。
- 如果第一个 Controller 上的测试正在进行，而您在另一个 Controller 上启动升级，则站点测试页面会出现在另一个 Controller 上的向导中。但是，如果第一个 Controller 上的测试完成，则只保留第一个 Controller 的测试结果。

解决与站点运行状况无关的测试失败

- 如果初步站点测试因内存不足而失败，请提供更多内存，然后重新运行测试。
- 如果您有权升级，但无权运行站点测试，则初步站点测试将失败。要解决此问题，请使用有权运行测试的用户帐户重新运行安装程序。

完成其他准备任务

- 如有需要，备份模板并升级管理程序
- 完成业务连续性计划规定的任何其他准备任务。

升级数据库和站点

在升级 Delivery Controller 后，您需要升级数据库和站点。有关高级概述，请参阅步骤 8：升级数据库和站点。

检查验证您的权限，了解更新 SQL Server 数据库架构所需的权限。根据您的数据库权限选择升级方法：

- **自动升级。** 如果您有权更新 SQL Server 数据库架构，请运行自动升级。请参阅自动升级数据库和站点。
- **手动升级。** 如果您没有这些权限，请运行使用脚本的手动升级。与拥有所需权限的数据库管理员合作。请参阅手动升级数据库和站点。

  在手动升级中，任务分为两个角色：

  - 站点管理员用户生成脚本。然后，该用户运行启用和禁用服务的脚本。

- 数据库管理员运行更新数据库架构的脚本。管理员使用 SQLCMD 实用程序或 SQL Server Management Studio 的 SQLCMD 模式。

> **注意：**
>
> 在多区域部署中，请在托管站点 SQL Server 数据库的同一区域中运行自动 dbschema 升级。否则，自动升级可能会失败。

> 在升级之前，请备份数据库。请参阅CTX135207。在数据库升级期间，产品服务将被禁用。在禁用期间，控制器无法为站点代理新连接，因此请仔细规划。

查看数据库架构升级

更新部署时，可以升级多个数据库架构。下表列出了已升级的架构：

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

该表使用以下术语：

- **站点：** 站点数据存储。架构更新将应用于站点数据存储。
- **监控：** 监控数据存储。架构更新将应用于监控数据存储。
- **配置：** 配置表。Studio 版本、许可信息或两者都在配置表中更新。
- **日志记录：** 日志记录数据存储。架构更新将应用于日志记录数据存储。

自动升级数据库和站点

您可以使用 Site Manager 或 PowerShell SDK cmdlet 自动升级数据库和站点。

使用 Site Manager 自动升级

1. 在已升级的 Delivery Controllers 上启动 Site Manager。
2. 指示您要自动启动站点升级并确认您已准备就绪。

使用 PowerShell cmdlet 自动升级

作为使用 Site Manager 的替代方法，请使用 PowerShell SDK cmdlet `Update-XDSite` 自动升级数据库和站点。有关详细信息，请参阅 Citrix Virtual Apps and Desktops SDK Guide。

1. 在第二个 Delivery Controller 上，打开 PowerShell 会话。

2. 运行 `Update-XDSite` cmdlet。

该 cmdlet 自动检测所有需要升级的组件并执行以下操作：

- 断开数据库连接，更新必要的数据库表，然后重新连接服务。如果数据库已通过其他脚本或独立工具升级，则跳过此步骤。
- 运行环境所需的任何其他升级步骤。已完成的全局级别升级将被跳过。

手动升级数据库和站点

1. 在已升级的 Delivery Controller 上启动 Site Manager。
2. 指示您要手动升级站点。向导会检查许可证服务器兼容性并请求确认。
3. 确认您已备份数据库。

   向导会生成并显示脚本以及升级步骤清单。如果数据库的架构自产品升级版本以来未发生更改，则不会生成该脚本。例如，如果日志记录数据库架构未更改，则不会生成 `UpgradeLoggingDatabase.sql` 脚本。
4. 按所示顺序运行以下脚本。

   - `DisableServices.ps1`：Site Manager 用户在 Controller 上运行此 PowerShell 脚本以禁用产品服务。
   - `UpgradeSiteDatabase.sql`：数据库管理员在包含站点数据库的服务器上运行此 SQL 脚本。
   - `UpgradeMonitorDatabase.sql`：数据库管理员在包含 Monitor 数据库的服务器上运行此 SQL 脚本。
   - `UpgradeLoggingDatabase.sql`：数据库管理员在包含配置日志记录数据库的服务器上运行此 SQL 脚本。仅当此数据库发生更改时（例如，应用修补程序后）才运行此脚本。
   - `EnableServices.ps1`：Site Manager 用户在 Controller 上运行此 PowerShell 脚本以启用产品服务。

   数据库升级完成且产品服务启用后，Site Manager 会自动测试环境和配置，然后生成 HTML 报告。如果发现问题，可以还原数据库备份。解决问题后，可以再次升级数据库。
5. 完成清单任务后，单击 **完成升级**。

替换 SQL Server Express 本地数据库

Microsoft SQL Server Express LocalDB 是 SQL Server Express 的一项功能，本地主机缓存独立使用此功能。本地主机缓存不需要 SQL Server Express 的任何组件，只需 SQL Server Express LocalDB。

将 Delivery Controller 升级到 Citrix Virtual Apps and Desktops 2203 LTSR 或更高版本时，支持的版本是 SQL Server Express LocalDB 2019 或 SQL Server Express LocalDB 2022。

更新 SQL Server Express LocalDB 的方法有两种：

- 自动更新
- 手动更新

自动更新

升级 Delivery Controller 时，元安装程序会自动安装最新兼容版本的 SQL Server Express LocalDB。元安装程序不会卸载旧的 LocalDB 版本。确认新版本正常运行后，您必须手动卸载旧版本。

验证新的 SQL SERVER EXPRESS LOCALDB 安装

在卸载旧版本之前，请验证新的 SQL Server Express LocalDB 安装是否正常运行：

1. 使用命令提示符导航到 SqlLocalDB 实例：
   - 对于 SQL LocalDB 2014：`cd C:\Program Files\Microsoft SQL Server\120\Tools\Binn`
   - 对于 SQL LocalDB 2017：`cd C:\Program Files\Microsoft SQL Server\140\Tools\Binn`
   - 对于 SQL LocalDB 2019：`cd C:\Program Files\Microsoft SQL Server\150\Tools\Binn`
   - 对于 SQL LocalDB 2022：`cd C:\Program Files\Microsoft SQL Server\160\Tools\Binn`
2. 运行 `SqlLocalDB i`。

   您应该会看到两个文件：CitrixHA 和 MSSQLLocalDB。

手动更新

先决条件

- Citrix 虚拟应用和桌面 安装介质。
- Windows Sysinternals 工具箱中的 PsExec 工具。

过程

1. 完成 Citrix Virtual Apps and Desktops 组件、数据库和站点的升级。（这些数据库升级会影响站点、监视和配置日志记录数据库。它们不影响使用 SQL Server Express LocalDB 的本地主机缓存数据库。）
2. 登录到要更新 SQL Server Express LocalDB 的 Delivery Controller。
3. 从 Microsoft 下载 PsExec 并将其放置在该 Delivery Controller 上易于访问的位置，例如 C:\Temp。
4. 从 Windows 系统服务中停止 Delivery Controller 上的 Citrix High Availability Service。
5. 在 Delivery Controller 上打开命令提示符，导航到 PsExec 所在的位置（例如 `C:\Temp`），然后运行以下命令以使用 Network Service 帐户提升命令提示符的权限：

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
   ```

6. 运行 `whoami` 以确认命令提示符正在以 Network Service 帐户运行。您必须获得以下输出：`nt authority\networkservice`。
7. 使用命令提示符导航到 SQL LocalDB 实例：
   - 如果从 SQL LocalDB 2014 升级：

     ```
     cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
     ```

   - 如果从 SQL LocalDB 2017 升级：

     ```
     cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
     ```

   - 如果从 SQL LocalDB 2019 升级：

     ```
     cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
     ```

8. 停止并删除 SQL LocalDB 实例：`CitrixHA`。

   ```
   SqlLocalDB stop CitrixHA
   ```

```
SqlLocalDB delete CitrixHA
```

9. 从 Delivery Controller 中删除以下文件：

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*

C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if
exists)

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.*
(if exists)
```

10. 使用 Windows 本机程序删除功能从 Delivery Controller 卸载现有的 SQL LocalDB SQL Server Express。
11. 卸载完成后，重新启动 Delivery Controller。
12. 从 Windows 系统服务中停止 Delivery Controller 上的 Citrix High Availability Service。
13. 将 Citrix Virtual Apps and Desktops 安装介质装载到您的 Delivery Controller。
14. 以管理员身份在 Delivery Controller 上安装 SQL Server Express LocalDB 2022。
    a. 使用 Citrix Virtual Apps and Desktops 安装介质的 `Support > SQLLocalDB` 文件夹中的 `sqllocaldb.msi` 文件。例如，如果安装介质装载到 `E drive` 盘符，则该文件位于 `E:\Support\SQLLocalDB\sqllocaldb.msi`。需要重新启动才能完成安装。
    b. 新的 SQL LocalDB 必须位于 `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` 中。
15. 从 Windows 系统服务中启动 Delivery Controller 上的 Citrix High Availability Service。
16. 在 Delivery Controller 的命令提示符中，导航到 `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` 并运行 `SqlLocalDB i` 以确认已创建 CitrixHA 实例。返回的实例列表中必须包含 `CitrixHA`。

> **注意：**
>
> 启动 Citrix High Availability Service 后，可能需要长达 15 分钟才能创建 CitrixHA 数据库。

17. 确保已创建本地主机缓存数据库文件，以确认高可用性服务（辅助代理）可在需要时接管。

    a. 在 Delivery Controller 上，浏览到 `C:\Windows\ServiceProfiles\NetworkService`。

    b. 验证 `HaDatabaseName.mdf` 和 `HaDatabaseName_log.ldf` 已创建。

18. 在其余 Delivery Controller 上重复这些步骤。

常见问题

本节回答了有关升级 Citrix Virtual Apps and Desktops 的一些常见问题。

- **升级 Virtual Apps and Desktops 环境的正确顺序是什么？**

  有关建议升级顺序的图示和说明，请参阅升级顺序和升级过程。

- **我的站点有多个 Delivery Controller（位于不同区域）。如果我只升级其中一部分，会发生什么？我是否必须在同一维护时段内升级站点中的所有 Controller？**

  最佳实践是在同一维护时段内升级所有 Delivery Controller，因为每个 Controller 上的各种服务会相互通信。保留不同版本可能会导致问题。在维护时段内，我们建议您先升级一半的 Controller，然后升级站点，再升级剩余的 Controller。有关详细信息，请参阅升级过程。

- **我可以直接升级到最新版本，还是必须进行增量升级？**

  您几乎总是可以直接升级到最新版本并跳过中间版本，除非您要升级到的版本的**新增功能**文章中明确说明。

- **客户可以从长期服务版本 (LTSR) 环境升级到当前版本吗？**

  可以。客户无需长期停留在长期服务版本。客户可以根据业务需求和功能，将 LTSR 环境迁移到当前版本。

- **是否允许混合使用不同版本的组件？**

  在每个站点中，Citrix 建议将所有组件升级到同一版本。尽管您可以使用某些组件的早期版本，但最新版本中的所有功能可能无法使用。有关详细信息，请参阅混合环境注意事项。

- **当前版本必须多久升级一次？**

  当前版本在发布日期后 6 个月达到维护终止 (EOM)。Citrix 建议客户采用最新的当前版本。当前版本在发布日期后 18 个月达到生命周期终止 (EOL)。

- **建议：升级到 LTSR 还是 CR？**

  当前版本 (CR) 提供最新、最具创新性的应用程序、桌面和服务器虚拟化功能。这使您能够保持领先技术，并在竞争中保持优势。

长期服务版本 (LTSR) 非常适合希望在较长时间内保留相同基础版本的大型企业生产环境。

- **我需要升级我的许可证吗？**

  确保当前许可证日期未过期，并且对您要升级到的版本有效。请参阅 CTX111618。有关续订的信息，请参阅 客户成功服务续订许可证。

- **升级需要多长时间？**

  升级部署所需的时间因基础架构和网络而异。因此，我们无法提供确切的时间。

- **最佳实践是什么？**

  确保您理解并遵循 准备指南。

- **Citrix Virtual Apps and Desktops 站点升级是否需要 sysadmin 权限？**

  否。对于使用 Windows 身份验证（默认）的标准站点升级，现有数据库（站点、日志记录和监视）上的 db_owner 权限足以让站点管理器更新架构。sysadmin 主要仅在初始站点创建或进程必须自动创建新数据库和服务器级登录时才需要。

- **为什么站点管理器在升级期间有时会提示提升权限？**

  如果升级需要服务器级操作，站点管理器可能会检查提升的权限，例如：

  - 添加新的 Delivery Controller：这需要为 Delivery Controller 的计算机身份创建新的 SQL 登录。
  - 修改登录：需要 `securityadmin` 或 `dbcreator` 角色的操作通常简化为对 sysadmin 的请求。
  - 自动创建：如果站点管理器负责自动创建新的数据库结构或映射用户，而不是使用预先准备的脚本。

- **在不授予 Citrix 管理员 sysadmin 权限的情况下，我可以升级数据库吗？**

  可以，您可以通过执行手动升级来升级。Citrix 管理员使用站点管理器获取升级 SQL 脚本，然后将脚本提供给数据库所有者以执行数据库升级。数据库升级后，Citrix 管理员返回站点管理器以完成整个升级过程。

- **为什么 Citrix 服务在计算机帐户下运行？**

  Citrix 服务默认在网络服务帐户下运行，因为它允许服务器使用其自己的身份（例如，计算机帐户 DOMAIN\SERVER$）与其他服务器和 SQL 数据库安全通信，而无需手动密码管理。此设置依赖于 Windows 身份验证，这是连接到 SQL 最安全和推荐的方法，因为它使用 Active Directory 中现有的信任。

- **支持哪些操作系统？**

您要升级到的版本的系统要求文章列出了支持的操作系统。

如果您的当前部署使用不再支持的操作系统，请参阅早期操作系统。

- **支持哪些版本的 VMware vSphere (vCenter + ESXi)？**

  CTX131239列出了支持的主机和版本，以及已知问题的链接。

- **我的版本何时终止生命周期 (EOL)？**

  请查看产品矩阵。

- **最新版本有哪些已知问题？**

  - Citrix 虚拟应用和桌面
  - StoreFront
  - Citrix 预配
  - Citrix 许可证服务器
  - 适用于 Windows 的 Citrix Workspace 应用程序(/zh-cn/citrix-workspace-app-for-windows/about.html#known-issues)

迁移

迁移将数据从早期部署移动到较新版本或云。选择适合您目标的路径：将本地部署迁移到云，或查找旧版 XenApp 6.x 迁移的资源。

迁移到云

您可以使用适用于 Citrix Virtual Apps and Desktops 的自动化配置工具将本地部署迁移到云。有关详细信息，请参阅 迁移到云。

迁移旧版部署

迁移将数据从早期部署移动到较新版本。该过程包括安装较新的组件并创建新站点、从旧场导出数据，然后将数据导入新站点。

没有支持的工具或脚本用于迁移 XenApp 和 XenDesktop 版本，或迁移早期 Citrix Virtual Apps and Desktops 版本。本产品文档中描述的 Citrix Virtual Apps and Desktops 版本支持*升级*。

有关早期 XenApp 6.x 迁移内容，请参阅以下内容。脚本和文章均不受支持或维护。

- XenApp 6.x 版本的开源迁移脚本可在 `<https://github.com/citrix/xa65migrationtool>` 获取。Citrix 不支持或维护这些迁移脚本。

- 7.x 中的更改
- 将 XenApp 6.5 工作程序升级到新的 VDA
- 迁移 XenApp 6.x

安全

Citrix Virtual Apps and Desktops™ 提供了一种安全设计解决方案，可让您根据安全需求定制环境。

IT 面临的移动工作人员安全问题之一是数据丢失或被盗。通过托管应用程序和桌面，Citrix Virtual Apps and Desktops™ 将所有数据保留在数据中心，从而将敏感数据和知识产权与终端设备安全地分离。当启用策略以允许数据传输时，所有数据都将加密。

Citrix Virtual Apps and Desktops 数据中心还通过集中式监控和管理服务简化了事件响应。Director 允许 IT 监控和分析网络中正在访问的数据，而 Studio 允许 IT 在数据中心修补和修复大多数漏洞，而不是在每个最终用户设备上本地解决问题。

Citrix Virtual Apps and Desktops 还简化了审计和法规遵从性，因为调查人员可以使用集中式审计跟踪来确定谁访问了哪些应用程序和数据。Director 通过访问配置日志和 OData API 收集有关系统更新和用户数据使用情况的历史数据。

委派管理允许您设置管理员角色，以精细控制对 Citrix Virtual Apps and Desktops 的访问。这使您的组织能够灵活地为某些管理员提供对任务、操作和范围的完全访问权限，而其他管理员则具有有限的访问权限。

Citrix Virtual Apps and Desktops 通过在网络的不同级别（从本地级别到组织单位级别）应用策略，为管理员提供了对用户的精细控制。这种策略控制决定了用户、设备或用户和设备组是否可以连接、打印、复制/粘贴或映射本地驱动器，从而最大程度地减少了与第三方临时工作人员相关的安全问题。管理员还可以使用 Desktop Lock 功能，以便最终用户只能使用虚拟桌面，同时阻止对最终用户设备本地操作系统的任何访问。

管理员可以通过将站点配置为使用控制器或最终用户与虚拟投递代理 (VDA) 之间的传输层安全 (TLS) 协议来增强 Citrix Virtual Apps 或 Citrix Virtual Desktops 的安全性。该协议还可以在站点上启用，以提供服务器身份验证、数据流加密和 TCP/IP 连接的消息完整性检查。

Citrix Virtual Apps and Desktops 还支持 Windows 或特定应用程序的多重身份验证。多重身份验证还可用于管理 Citrix Virtual Apps and Desktops 交付的所有资源。这些方法包括：

- 令牌
- 智能卡
- RADIUS

- Kerberos (科尔贝罗斯)
- 生物识别

Citrix Virtual Desktops 可以与许多第三方安全解决方案集成，从身份管理到防病毒软件。支持的产品列表可在 `<http://www.citrix.com/ready>` 找到。

Citrix Virtual Apps and Desktops 的部分版本已通过通用准则标准认证。有关这些标准的列表，请访问 `<https://www.commoncriteriaportal.org/cc/>`。

联合身份验证服务

Citrix 联合身份验证服务 (FAS) 允许用户在通过 SAML 或 OpenID Connect (OIDC) 等不提供 Windows 密码的现代身份提供程序进行身份验证的环境中，对 Citrix 虚拟桌面和应用程序进行单点登录 (SSO)，从而确保对已加入 Active Directory 域的会话主机进行无缝访问。

有关使用联合身份验证服务保护部署的更多信息，请参阅其自己的文档中的 联合身份验证服务 文档。

FIDO2 和 WebAuthn 身份验证

使用 FIDO2 和 WebAuthn 进行本地授权和虚拟身份验证

用户可以使用 FIDO2 安全密钥以及集成 TPM 2.0 和 Windows Hello 的生物识别设备，在其虚拟会话中对利用 FIDO2 或 WebAuthn 的应用程序进行身份验证。

有关 FIDO2 的更多信息，请参阅 FIDO2: WebAuthn & CTAP。

有关使用此功能的信息，请参阅 FIDO2 重定向。

> **注意**
>
> 请注意，此功能不支持使用 WebAuthn 或 FIDO2 登录虚拟会话。此功能仅允许在虚拟会话中的应用程序中使用这些身份验证方法。

先决条件和配置

支持性矩阵

会话主机操作系统	WEB 应用程序身份验证	UWP 应用程序身份验证
Windows 服务器 2016	通过 USB 重定向支持	不支持
Windows 服务器 2019	受支持	不支持
Windows 服务器 2022	受支持	受支持
Windows 服务器 2025	受支持	受支持
Windows 10 系统	受支持	受支持
Windows 十一	受支持	受支持

注意：

对上述身份验证方法的支持取决于底层操作系统的功能。例如，由于操作系统限制，Windows Server 2019 不支持 UWP 应用程序。

有关更多信息，请查看以下要求。

Web 应用程序身份验证

要求

以下是使用 FIDO2 和 WebAuthn 身份验证与 Web 应用程序的要求：

CITRIX® 控制平面

- Citrix Virtual Apps and Desktops™ 2203 或更高版本

会话主机

- 操作系统
  - Windows 10 22H2 或更高版本
  - Windows 十一
  - Windows Server 2019 或更高版本

- VDA
  - Windows：版本 2203 或更高版本

客户端设备

- 操作系统
  - Windows 10 22H2 或更高版本
  - Windows 十一
  - Linux：请参阅适用于 Linux 的 Workspace 应用程序的系统要求
  - Mac：请参阅适用于 Mac 的 Workspace 应用程序的系统要求
- Workspace 应用程序
  - Windows: 2402 版本或更高版本
  - Linux: 2303 或更高版本
  - Mac: 2307 或更高版本

WEB 浏览器要求

- 32 位和 64 位浏览器

支持的身份验证方法

- FIDO2 安全密钥
- Windows 哈啰
  - TPM 2.0
  - 集成生物识别技术
    - 面部识别
    - 指纹扫描仪
  - WebAuthn
- 通行密钥

> **注意：**
>
> - 对上述身份验证方法的支持取决于底层客户端操作系统的功能。

- 通行密钥在 Windows 10 客户端设备和/或会话主机上不受支持。

UWP 应用程序身份验证

随着 Citrix Virtual Apps and Desktops™ 2112 的发布，Citrix 支持 UWP 应用程序中的 WebAuthn 和 FIDO2 身份验证。

Microsoft Teams、Microsoft Outlook for Office 365 和 OneDrive 等应用程序使用 UWP 应用程序进行身份验证，作为与 Microsoft Entra ID 的链接。Citrix 现在支持使用 FIDO2 对这些应用程序进行身份验证。

要求

以下是使用 FIDO2 和 WebAuthn 身份验证与 UWP 应用程序的要求：

CITRIX 控制平面

- Citrix Virtual Apps and Desktops 2112 或更高版本

会话主机

- 操作系统
  - Windows 10 22H2 或更高版本
  - Windows 十一
  - Windows Server 2022 或更高版本
- VDA
  - Windows：版本 2203 或更高版本

客户端设备

- 操作系统
  - Windows 10 22H2 或更高版本
  - Windows 十一
  - Linux：请参阅适用于 Linux 的 Workspace 应用程序的系统要求
  - Mac：请参阅适用于 Mac 的 Workspace 应用程序的系统要求
- Workspace 应用程序
  - Windows：版本 2402 或更高版本
  - Linux：2303 或更高版本

- Mac：2307 或更高版本

UWP 应用程序要求

- 32 位和 64 位应用程序

支持的身份验证方法

- FIDO2 安全密钥
- Windows 你好
  - TPM 2.0
  - 集成生物识别
    - 面部识别
    - 指纹扫描仪
  - WebAuthn
  - 密钥

> **注意：**
>
> 对上述身份验证方法的支持取决于底层操作系统的功能。

> 在客户端、VDA 或操作系统不支持 FIDO2 重定向功能而导致 FIDO2 重定向不可用的情况下，可以使用 USB 重定向来重定向基于 USB 的 FIDO2 密钥。 在 FIDO2 重定向可用的情况下，也可以使用 USB 重定向来重定向基于 USB 的 FIDO2 密钥。在这种情况下，您必须禁用 FIDO2 重定向并配置相应的 USB 重定向规则。 有关如何使用 USB 重定向规则配置 FIDO2 密钥的详细信息，请参阅 USB 重定向设备规则 文档。

配置

FIDO2 重定向默认启用。无需额外配置即可对在 Chrome、Edge、Brave 和 Firefox 浏览器中运行的应用程序进行身份验证。有关相关策略设置的信息，请参阅 FIDO2 重定向设置。

对于使用任何其他需要 FIDO2 身份验证的应用程序的企业，需要在注册表中进行额外配置。有关详细信息，请参阅 高级配置。

> **注意：**

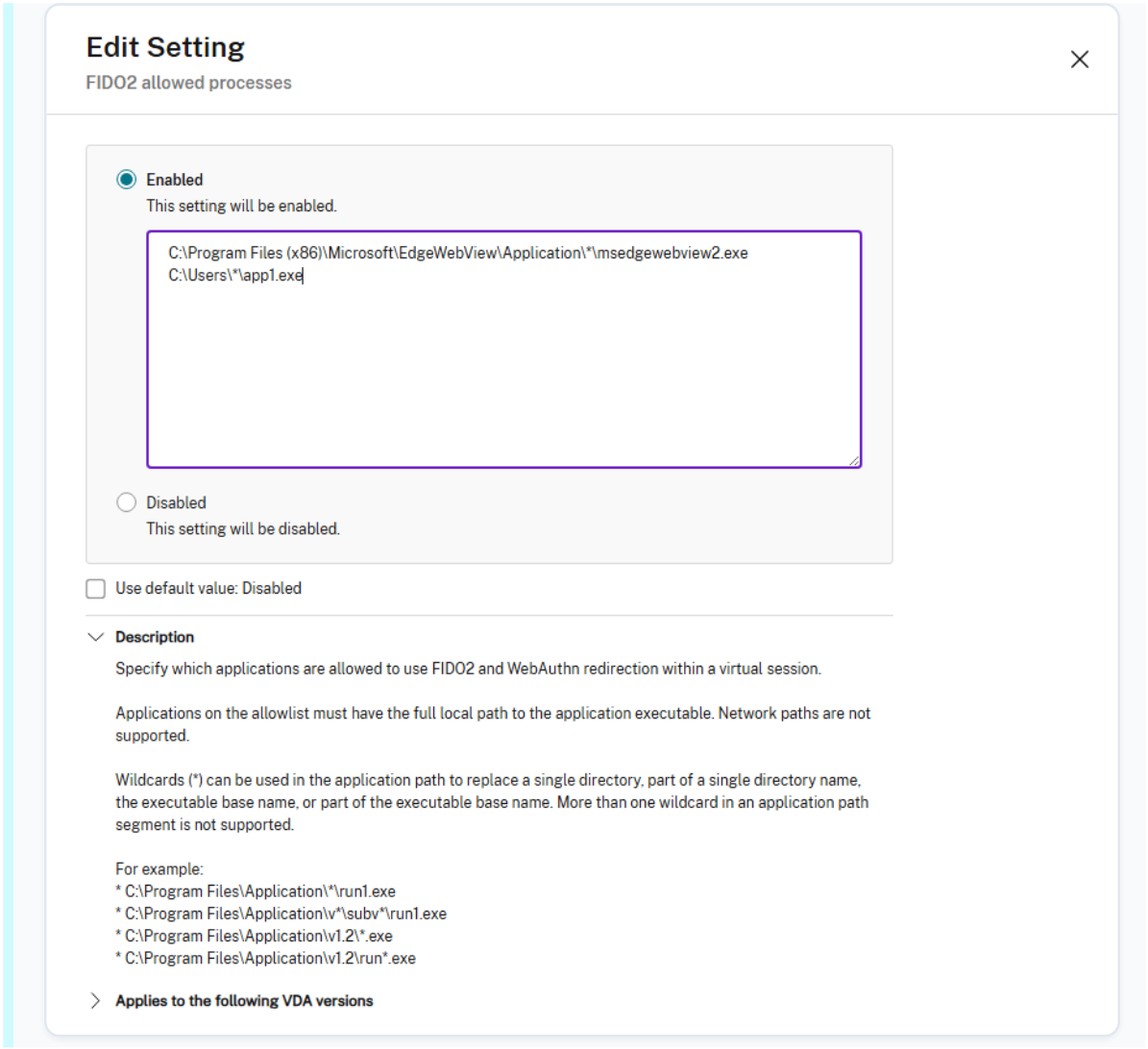
> FIDO2 重定向在双跳场景中受支持，只要安装在中间跳 VDA 上的适用于 Windows 的 Citrix Workspace 应用程序版本为 2503 或更高。此外，这仅在第二跳连接通过 ICA 进行时受支持。

自定义应用程序的高级配置

对于拥有任何其他 Web 应用程序（即非 Chrome、Edge、Firefox 或 Brave）的企业，需要进行以下更改才能使 FIDO2 重定向在 HDX 会话中工作：

1. 在 Studio 中配置 **FIDO2 允许的进程**策略设置。
    - 在文本字段中添加应用程序的完整路径。有关策略设置用法的更多详细信息，请参阅策略部分。

      > **注意：**
      >
      > 支持使用通配符 (*)。当目录或可执行文件的名称根据应用程序版本而变化，或者应用程序安装在用户配置文件中时，可以使用通配符。



2. 添加以下注册表项和值：

   a. 对于 64 位应用程序（例如“app1.exe”）：

      - 键：

        `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\app1.exe`

   b. 对于 32 位应用程序：

      - 键：

        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHo`

3. 设置注册表值后，重新启动 VDA，以使 FIDO2 重定向对 app1.exe 启用。

> **注意：**

- `msedgewebview2.exe` 仅需在 Studio 策略设置中配置。对于 `msedgewebview2.exe`，不需要步骤 2 和 3。
- 错误地编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix 无法.
- 保证可以解决因错误使用注册表编辑器而导致的问题。
- 使用注册表编辑器风险自负。请务必在编辑注册表之前备份注册表。
- 在步骤 2 中配置的注册表项在 VDA 升级后仍然保留。

FIDO2 诊断工具

`CtxFido2Diagnostics.exe` 是 VDA 上的一个命令行工具，可帮助 Citrix 管理员和支持工程师诊断和解决 HDX 会话中的 FIDO2 重定向配置问题。该工具以 JSON 格式收集并显示关键配置数据，从而能够快速识别策略配置错误、缺少应用程序挂钩和版本不匹配等问题。

该工具位于：`C:\Program Files\Citrix\HDX\bin\CtxFido2Diagnostics.exe`

该工具的路径在 VDA 安装期间已包含在系统环境变量中，因此您可以通过键入 `CtxFido2Diagnostics.exe` 从任何目录运行它。

要求

会话主机

- **操作系统：** Windows 10 1809 或更高版本、Windows 11 21H2 或更高版本、Windows Server 2019 或更高版本

客户端设备

- **操作系统：** Windows 10 1809 或更高版本

显示的信息

当您在 HDX 会话中运行 `CtxFido2Diagnostics.exe` 时，该工具会输出一个包含以下诊断信息的 JSON 对象：

CVAD 版本

显示会话主机上安装的 Citrix Virtual Apps and Desktops 版本。使用此信息可验证 VDA 版本是否支持 FIDO2 重定向以及您的部署所需的特定 WebAuthn 功能。

示例：

```
"CVAD Version": "2607.0.100.407"
```

CWA 版本

显示客户端设备上安装的 Citrix Workspace 应用程序版本。VDA 和 Citrix Workspace 应用程序都必须满足最低版本要求，FIDO2 重定向才能正常运行。

示例：

```
"CWA Version": "CWA for Windows, 26.3.10.69"
```

Fido2策略已启用

指示当前会话的 FIDO2 重定向策略是已启用 (`true`) 还是已禁用 (`false`)。当此值为 `false` 时，无论其他配置设置如何，FIDO2 重定向都无法运行。

管理员通过 Citrix Studio 或 Citrix 组策略在 **ICA > FIDO2** 下配置此策略。

示例：

```
"Fido2PolicyEnabled": true
```

会话 ID

显示当前 HDX 会话的 ID。此值有助于在故障排除期间将诊断输出与 Director 中的会话日志或事件查看器条目相关联。

示例：

```
"Session ID": 2
```

WebAuthn API 版本

显示当前 CVAD 和 CWA 组合支持的 WebAuthn API 版本。API 版本决定了哪些 FIDO2/WebAuthn 功能可用于重定向。

示例：

```
"WebAuthn API Version": 7
```

FIDO2 允许的进程注册表设置

列出通过会话主机上的注册表配置的、允许使用 FIDO2 重定向的应用程序进程路径。这些路径对应于以下注册表值：

`HKLM\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\`

此列表通常包括受支持的浏览器（Chrome、Edge、Firefox、Brave）、Azure AD Broker 插件以及 Citrix ICA 客户端本身。FIDO2 诊断工具可执行文件也包含在内，以便它可以执行诊断调用。

FIDO2 允许的进程 Studio 策略设置

列出管理员通过 Citrix Studio 策略设置配置的、允许使用 FIDO2 重定向的其他应用程序进程路径。这些条目补充了基于注册表的列表，并允许管理员添加自定义应用程序（例如第三方身份验证器实用程序），而无需直接修改注册表。

FIDO2 重定向可挂钩应用程序

列出 FIDO2 挂钩模块已成功识别并可拦截以进行 WebAuthn API 重定向的应用程序可执行文件名称。只有在此列表中出现的应用程序，其 FIDO2 身份验证请求才会被重定向到客户端设备。

如果应用程序出现在允许的进程列表中但未在此处显示，则挂钩模块无法附加到它。这可能表示兼容性问题、应用程序当前未运行或配置问题。

相关信息

有关解决此工具识别出的 FIDO2 重定向问题的详细指导，请参阅排查 FIDO2 重定向问题。

故障排除

以下步骤应遵循以解决 FIDO2 重定向问题：

1. **检查系统要求**
    a. 根据 Citrix 官方文档，验证 FIDO2 重定向的系统要求是否得到满足。
2. **验证设备连接**
    a. 对于物理 FIDO2 密钥：
        i. 确保 FIDO2 密钥已正确插入并在客户端端点上可见。
        ii. 使用您的操作系统设备管理器（例如，Windows 上的设备管理器，macOS 上的系统信息）确认设备已被识别并正常运行。
        iii. 如果设备未被检测到：
            i. 尝试重新插入密钥或使用不同的 USB 端口。

ii. 在另一台设备上测试密钥，以排除硬件问题。

b. 对于内置身份验证器（例如 Windows Hello 等）-

i. 确认该功能已在您的客户端设备上启用和配置。

c. 这很重要，因为如果客户端设备无法识别 FIDO2 密钥，Citrix 将无法将其重定向到 HDX 会话。

3. **验证 Citrix 策略设置和配置**

a. 检查 Citrix 策略中的 FIDO2/WebAuthn 重定向和 USB 重定向设置。

i. FIDO2 重定向策略已启用。

ii. 如果正在使用 EdgeWebView2 或自定义桌面应用程序，则在 **FIDO2 允许的进程** 策略设置中添加了相应的文件路径。

iii. **未**设置设备规则，以使用通用 USB 重定向来重定向 FIDO2 密钥设备。

b. 如果 Citrix 组件最近已更新，请验证您的配置是否与新版本保持一致。

4. **使用 HDX Monitor 进行诊断**

a. 启动 HDX 会话并打开 Web 浏览器或 UWP 应用程序，然后导航到身份验证页面。

b. 选择安全密钥、Webauthn 或 FIDO2 作为登录方法。您应该会看到 wfica32.exe 进程弹出的对话框提示，这是 FIDO2 调用被重定向的结果（请参阅随附的屏幕截图）。如果不是这种情况：

i. 确保未使用通用 USB 虚拟通道重定向密钥。如果密钥在 HDX 会话中被重定向，您可能会看到一个对话框提示，显示“将您的安全密钥插入 USB 端口”。要解决此问题，请禁用 USB 重定向或确保安全密钥未在 HDX 会话中重定向。

ii. 在 HDX 会话中打开 HDX Monitor 并导航到 **FIDO2 - Webauthn 重定向** 节点。

iii. 确保 FIDO2 允许重定向策略设置为 **True** 并且需要 FIDO2/WebAuthn 身份验证的应用程序已列在 **FIDO2 重定向挂钩应用程序**中。如果应用程序不存在，请根据 高级配置 中的信息将其添加到相应的注册表位置。

iv. 确保需要 FIDO2/WebAuthn 身份验证的应用程序的完整路径已列在 **FIDO2 允许的进程** 策略设置中。如果完整路径不存在，请将其添加到 Studio 中的 **FIDO2 允许的进程** 策略设置中。有关其他信息，请参阅 配置部分。

v. （旧版）如果使用基于旧版注册表的设置配置了 FIDO2 重定向，请将您的配置迁移到 Studio 中的 **FIDO2 允许的进程** 策略设置，并确保包含需要 FIDO2/WebAuthn 身份验证的应用程序的完整路径。有关其他信息，请参阅 配置部分。

注意：

如果您的会话主机上尚未安装 HDX Monitor，您可以从 Citrix Virtual Apps and Desktops 安装程序的 Support 文件夹中安装它。

1. **收集日志并联系技术支持**
    a. 如果在执行上述步骤后问题仍然存在 —
        i. 收集 HDX Monitor 输出、Citrix Workspace 应用程序和 VDA CDF 日志。
        ii. 记录您已采取的所有故障排除步骤以及遇到的任何错误消息。
        iii. 联系您的 IT 支持团队或 Citrix 支持，提供收集到的信息以加快解决速度。

常见问题和解决方案

1. **使用 Microsoft Edge 浏览器打开的网页可能无法进行 FIDO2 身份验证**
    a. **可能的原因**：带有 AppContainer 的 Edge 沙盒实例不允许 Citrix 挂钩到进程中，这会阻止 WebAuthn 调用的重定向正常工作。
    b. **解决方案**：可以通过在组策略编辑器中或通过 Intune 更新相应设置来解决此问题。有关此内容的更多信息，请参阅此处。或者，将 **DynamicCodeSettings** 注册表值设置为 0 也应有助于解决此问题。
        - **项**：`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\`
        - **值名称**：`DynamicCodeSettings`
        - **值类型**：`DWORD`
        - **值数据**：0
2. **FIDO2（例如 Yubikey）重定向在 Web 浏览器中不起作用**
    a. **可能的原因**：与浏览器相关的 FSLogix 配置文件管理 AppMasking 规则可能会阻止 Citrix FIDO2 服务查看和验证浏览器安装的文件路径。
    b. **解决方案**：禁用 FSLogix 中使 Chrome 文件路径对 Citrix FIDO2 服务不可见的隐藏规则，将确保 Yubikey 成功重定向并显示在浏览器中。

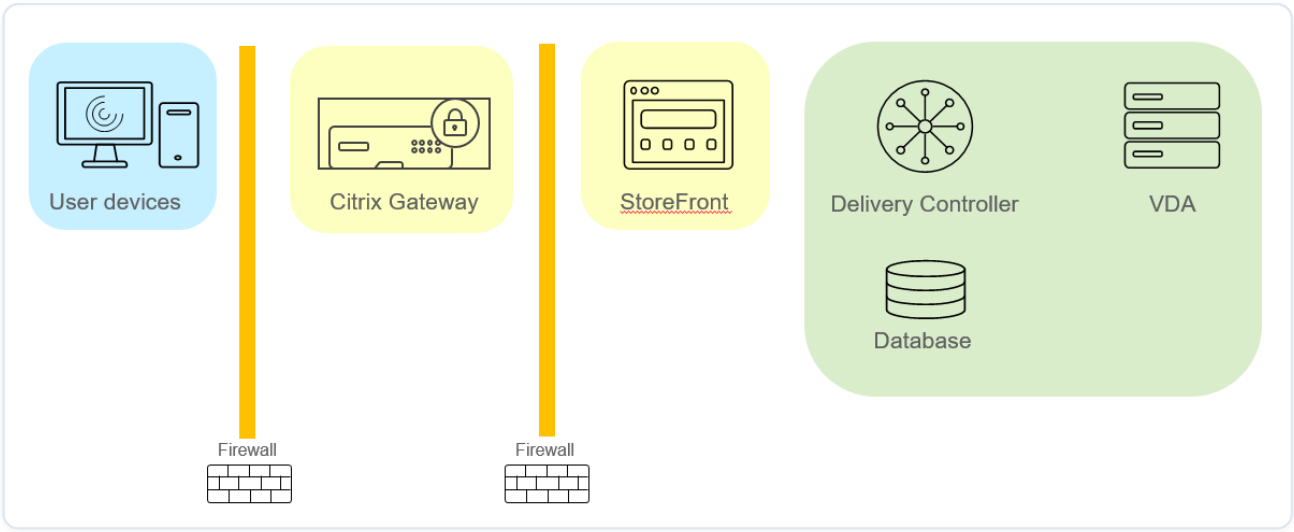
集成 思杰虚拟应用和桌面™ 与 思杰网关

StoreFront™ 服务器已部署并配置，以管理对已发布的资源和数据的访问。对于远程访问，建议在 StoreFront 前添加 Citrix Gateway。

注意：

有关如何集成 Citrix Virtual Apps and Desktops 与 Citrix Gateway 的详细配置步骤，请参阅 StoreFront 文档。

下图展示了一个包含 Citrix Gateway 的简化 Citrix 部署示例。Citrix Gateway 与 StoreFront 通信，以保护由 Citrix Virtual Apps and Desktops™ 交付的应用程序和数据。用户设备运行 Citrix Workspace™ 应用程序，以创建安全连接并访问其应用程序、桌面和文件。



用户使用 Citrix Gateway 登录并进行身份验证。Citrix Gateway 部署在 DMZ 中并受到保护。已配置双因素身份验证。根据用户凭据，用户将获得相关的资源和应用程序。应用程序和数据位于适当的服务器上（图中未显示）。针对安全敏感的应用程序和数据使用单独的服务器。

安全注意事项和最佳实践

注意：

您的组织可能需要满足特定的安全标准以符合法规要求。本文档不涵盖此主题，因为此类安全标准会随时间变化。有关安全标准和 Citrix 产品的最新信息，请查阅 Citrix 信任中心。

防火墙

使用外围防火墙保护环境中的所有计算机，包括在适当情况下保护安全区域边界。

环境中的所有计算机都必须受到个人防火墙的保护。安装核心组件和 VDA 时，如果检测到 Windows 防火墙服务（即使防火墙未启用），您可以选择自动打开组件和功能通信所需的端口。您也可以选择手动配置这些防火墙端口。如果使用其他防火墙，则必须手动配置。有关所需端口的更多信息，请参阅 技术白皮书：Citrix 技术使用的通信端口。

如果您要将传统环境迁移到此版本，可能需要重新定位现有外围防火墙或添加新的外围防火墙。例如，假设数据中心中传统客户端和数据库服务器之间存在外围防火墙。使用此版本时，必须放置该外围防火墙，以便虚拟桌面和用户设备位于一侧，而数据中心中的数据库服务器和 Delivery Controller 位于另一侧。因此，请考虑在数据中心内创建一个安全区域以包含数据库服务器和控制器。此外，还要考虑在用户设备和虚拟桌面之间提供保护。

> **注意：**
>
> TCP 端口 1494 和 2598 用于 ICA 和 CGP，因此很可能在防火墙上打开，以便数据中心外部的用户可以访问它们。Citrix 建议您不要将这些端口用于其他任何用途，以避免无意中将管理界面暴露于攻击的可能性。端口 1494 和 2598 已在互联网号码分配机构 (http://www.iana.org/) 正式注册。

与 Delivery Controller™ 的安全通信

使用 HTTPS 加密通信

StoreFront 和 NetScaler Gateway 通过 HTTP 或 HTTPS 与在 Delivery Controller 上运行的 XML 服务通信。根据配置，VDA 可以使用 WebSocket 与 Delivery Controller 通信。Director 使用 OData 通过 HTTP 或 HTTPS 与监视数据通信。建议您启用 HTTPS 并禁用 HTTP。这要求您 在 Delivery Controller 上启用 TLS。

- 要配置 StoreFront 以使用 HTTPS 连接，请参阅 为 Citrix Virtual Apps and Desktops 添加资源源 和 添加 Citrix Gateway 设备。
- 要配置 NetScaler Gateway 以使用 HTTPS 连接到 Delivery Controller，请参阅 在 NetScaler Gateway 上配置安全票证颁发机构。

安全密钥

您可以使用 安全密钥 来确保只有授权的 StoreFront 和 NetScaler 服务器才能通过云连接器连接到 DaaS。如果您已启用 XML 信任，这一点尤其重要。

XML 信任

默认情况下，当 StoreFront 连接到 Delivery Controller 以执行枚举和启动等操作时，StoreFront 必须传递用户的 Active Directory 凭据，以便 DaaS 可以对用户进行身份验证并检查用户的组成员身份。但是，当使用其他身份验证方法（例如域直通、智能卡或 SAML）时，StoreFront 不会拥有 Active Directory 密码。在这种情况下，您必须启用“XML 信任”。启用 XML 信任后，Citrix Virtual Apps and Desktops 允许 StoreFront 代表用户执行操作，例如枚举和启动应用程序，而无需验证用户的密码。在启用 XML 信任之前，请使用 安全密钥 或其他机制（例如防火墙或 IPsec）来确保只有受信任的 StoreFront 服务器才能连接到 Delivery Controller。

使用 Citrix Virtual Apps and Desktops PowerShell SDK 检查、启用或禁用 XML 信任设置。

- 要检查 XML 信任设置的当前值，请运行 `Get-BrokerSite` 并检查 `TrustRequestsSentToTheXMLServicePort` 的值。
- 要启用或禁用 XML 信任，请运行 `Set-BrokerSite` 并使用参数 `TrustRequestsSentToTheXmlServicePort`。

VDA 与 Delivery Controller 之间的通信

VDA 与控制器通信有两种机制。

- Windows 通信基础

  Windows Communication Foundation (WCF) 消息级保护可保护 Delivery Controller 与 VDA 之间的通信。这消除了使用 TLS 进行额外传输层保护的需要。VDA 与 Delivery Controller 之间通信的默认端口是 80。但是，您可以自定义端口。有关信息，请参阅 自定义 VDA。

  有关 WCF 中消息安全的信息，请参阅 Microsoft 文档 WCF 中的消息安全。

  WCF 配置使用 Kerberos 在 Controller 和 VDA 之间进行相互身份验证。加密使用具有 256 位密钥的 CBC 模式 AES。消息完整性使用 SHA-1。

  根据 Microsoft 的说法，WCF 使用的安全 协议 符合 OASIS（结构化信息标准促进组织）的标准，包括 WS-SecurityPolicy 1.2。此外，Microsoft 表示 WCF 支持 安全策略 1.2 中列出的所有算法套件。

  Controller 和 VDA 之间的通信使用 basic256 算法套件，其算法如前所述。

  WCF 配置使用基于 HTTP 协议的 SOAP 以及消息级安全加密。

- WebSockets

这是 WCF 的现代替代方案。它提供了一个优势，即 VDA 到 Delivery Controller 的通信仅使用 TLS 端口 443。目前，它仅适用于 MCS 预配的计算机。有关详细信息，请参阅 VDA 与 Delivery Controller 之间的 WebSocket 通信。

Delivery Controller 与许可证服务器之间的安全通信

Delivery Controller 通过 HTTPS 与许可证服务器通信。默认情况下，它使用自签名证书，但建议您将其替换为企业或公共证书颁发机构颁发的证书。有关详细信息，请参阅 手动安装 Citrix 许可管理器和许可 Web 服务使用的证书。

Web 浏览器与 Web Studio 和 Director 之间的安全通信

Web Studio 和 Director 可以安装在与 Delivery Controller 相同的计算机上，也可以安装在单独的计算机上。用户使用 Web 浏览器连接到 Web Studio 和 Director。默认情况下，Web Studio 使用自签名证书启用 HTTPS，而独立安装的 Director 不配置 HTTPS。建议您(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/secure/tls-studio.html)，并使用适当的证书。

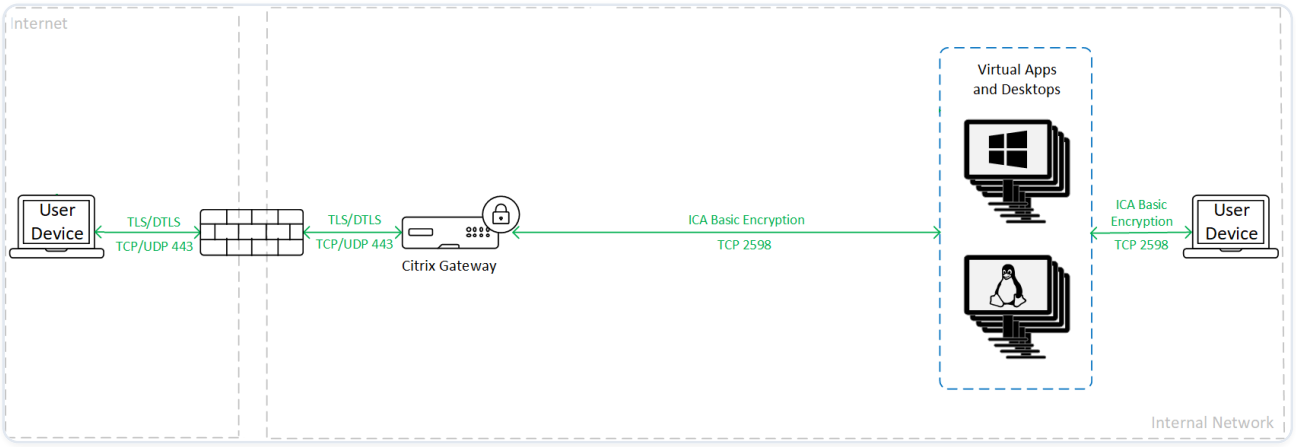
保护 ICA® 通信

Citrix Virtual Apps and Desktops™ 提供了多种选项来保护客户端与 VDA 之间的 ICA 流量。以下是可用的选项：

- **基本加密：** 默认设置。
- **SecureICA：** 允许使用 RC5 (128 位) 加密会话数据。
- **VDA TLS/DTLS：** 允许使用 TLS/DTLS 进行网络级加密。

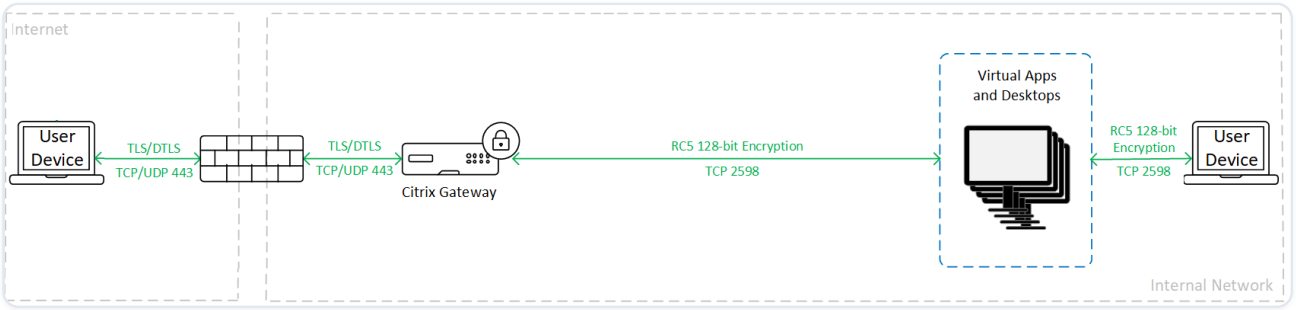
基本加密

使用基本加密时，流量会按以下图形所示进行加密。



SecureICA

使用 SecureICA 时，流量会按以下图形所示进行加密。



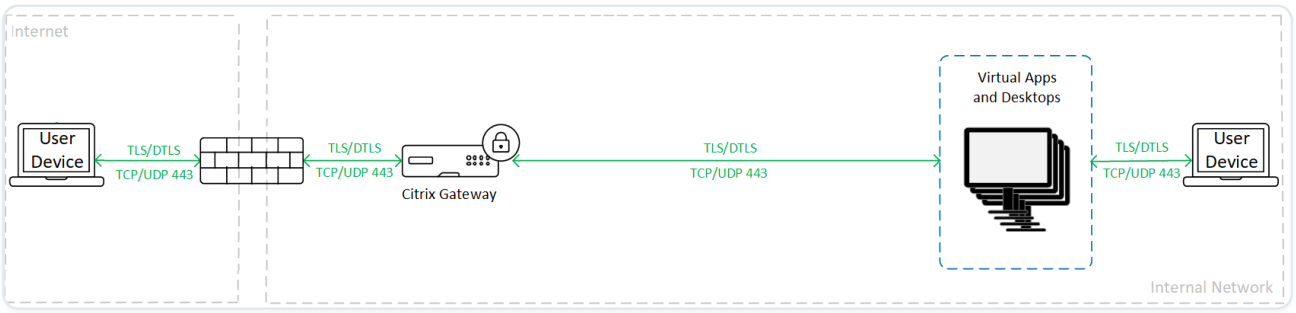
有关详细信息，请参阅(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/policies/reference/ica-policy-settings/security-policy-settings.html)

> **注意 1：**
>
> 当使用适用于 HTML5 的 Workspace 应用程序时，不支持 SecureICA。

> **注意 2：**
>
> Citrix SecureICA 是 ICA/HDX 协议的一部分，但它不是像传输层安全性 (TLS) 那样的符合标准的网络安全协议。

VDA TLS/DTLS

使用 VDA TLS/DTLS 加密时，流量会按以下图形所示进行加密。



要配置 VDA TLS/DTLS，请参阅(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/secure/tls-vda.html)。

虚拟通道

使用(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/secure/virtual-channel-security.html)来控制环境中允许哪些非 Citrix 虚拟通道。

与打印服务器的安全通信

您可以为虚拟投递代理 (VDA) 和通用打印服务器之间基于 TCP 的连接启用 TLS。有关详细信息，请参阅通用打印服务器上的传输层安全性 (TLS)。

与站点数据库的安全通信

有关为站点数据库启用 TLS 的信息，请参阅 CTX137556。

VDA 计算机安全性

一般建议

确保您的 VDA 及时更新最新的操作系统安全更新和防病毒软件。

应用程序安全性

为防止非管理员用户执行恶意操作，Citrix® 建议您为 VDA 主机上的安装程序、应用程序、可执行文件和脚本配置 Windows AppLocker 规则。

8.3 文件名

您可以在 VDA 上禁用 8.3 文件名。请参阅 Microsoft fsutil 文档。

数据存储注意事项

您的桌面环境可能包含各种类型的桌面，例如池桌面和专用桌面。用户绝不能将数据存储在用户之间共享的桌面（例如池桌面）上。如果用户将数据存储在专用桌面上，则如果该桌面稍后可供其他用户使用，则必须删除该数据。

用户帐户管理

应用 Windows 帐户管理最佳实践。在通过 Machine Creation Services 或 Provisioning Services 复制模板或映像之前，请勿在模板或映像上创建帐户。请勿使用存储的特权域帐户安排任务。请勿手动创建共享 Active Directory 计算机帐户。这些做法将有助于防止计算机攻击获取本地持久帐户密码，然后使用这些密码登录到属于其他用户的 MCS/PVS 共享映像。

仅授予用户所需的权限。Microsoft Windows 权限仍以常规方式应用于桌面：通过用户权限分配配置权限，并通过组策略配置组成员身份。此版本的一个优点是，可以授予用户对桌面的管理权限，而无需同时授予对存储桌面的计算机的物理控制权。

规划桌面权限时，请注意以下事项：

- 默认情况下，当非特权用户连接到桌面时，他们看到的是运行桌面的系统时区，而不是其自身用户设备的时区。有关如何允许用户在使用桌面时查看其本地时间的信息，请参阅“管理交付组”文章。
- 作为桌面管理员的用户对该桌面拥有完全控制权。如果桌面是池化桌面而非专用桌面，则必须信任该用户，使其能够与该桌面的所有其他用户（包括未来用户）共享。该桌面的所有用户都需要了解这种情况对其数据安全造成的潜在永久风险。此注意事项不适用于仅有一个用户的专用桌面；该用户不应是任何其他桌面的管理员。
- 作为桌面管理员的用户通常可以在该桌面上安装软件，包括潜在的恶意软件。该用户还可能监视或控制连接到桌面的任何网络上的流量。

管理登录权限

用户帐户和计算机帐户都需要登录权限。与 Microsoft Windows 权限一样，登录权限仍以常规方式应用于桌面：通过用户权限分配配置登录权限，并通过组策略配置组成员身份。

Windows 登录权限包括：本地登录、通过远程桌面服务登录、通过网络登录（从网络访问此计算机）、作为批处理作业登录以及作为服务登录。

对于计算机帐户，仅授予计算机所需的登录权限。交付控制器计算机帐户需要“从网络访问此计算机”登录权限。

对于用户帐户，仅授予用户所需的登录权限。

根据 Microsoft 的说法，默认情况下，远程桌面用户组被授予“允许通过远程桌面服务登录”的登录权限（域控制器除外）。

您组织的安全策略可能会明确规定应从该登录权限中删除此组。请考虑以下方法：

- 适用于多会话操作系统的虚拟投递代理 (VDA) 使用 Microsoft 远程桌面服务。您可以将远程桌面用户组配置为受限组，并通过 Active Directory 组策略控制该组的成员身份。有关详细信息，请参阅 Microsoft 文档。
- 对于 Citrix Virtual Apps and Desktops™ 的其他组件，包括适用于单会话操作系统的 VDA，不需要远程桌面用户组。因此，对于这些组件，远程桌面用户组不需要“允许通过远程桌面服务登录”的登录权限；您可以将其删除。此外：
    - 如果您通过远程桌面服务管理这些计算机，请确保所有此类管理员都已是 Administrators 组的成员。
    - 如果您不通过远程桌面服务管理这些计算机，请考虑在这些计算机上禁用远程桌面服务本身。

尽管可以将用户和组添加到登录权限“拒绝通过远程桌面服务登录”，但通常不建议使用拒绝登录权限。有关详细信息，请参阅 Microsoft 文档。

交付控制器安全性

交付控制器上的 Windows 服务

交付控制器安装会创建以下 Windows 服务：

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService)：管理虚拟机的 Microsoft Active Directory 计算机帐户。
- Citrix Analytics (NT SERVICE\CitrixAnalytics)：如果站点管理员已批准此收集，则收集站点配置使用信息供 Citrix 使用。然后将此信息提交给 Citrix，以帮助改进产品。
- Citrix App Library (NT SERVICE\CitrixAppLibrary)：支持 AppDisks 的管理和预配、AppDNA 集成以及 App-V 的管理。
- Citrix Broker Service (NT SERVICE\CitrixBrokerService)：选择可供用户使用的虚拟桌面或应用程序。
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging)：记录管理员对站点所做的所有配置更改和其他状态更改。
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService)：用于共享配置的全站点存储库。
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin)：管理授予管理员的权限。
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest)：管理其他交付控制器服务的自检。
- Citrix Host Service (NT SERVICE\CitrixHostService)：存储有关 Citrix Virtual Apps 或 Citrix Virtual Desktops 部署中使用的虚拟机管理程序基础结构的信息，并提供控制台用于枚举虚拟机管理程序池中资源的功能。
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService)：协调桌面虚拟机的创建。
- Citrix Monitor Service (NT SERVICE\CitrixMonitor)：收集 Citrix Virtual Apps 或 Citrix Virtual Desktops 的指标，存储历史信息，并为故障排除和报告工具提供查询界面。
- Citrix StoreFront Service (NT SERVICE\ CitrixStorefront)：支持 StoreFront 的管理。（它本身不是 StoreFront 组件的一部分。）

- Citrix StoreFront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService)：支持 StoreFront 的特权管理操作。（它本身不是 StoreFront 组件的一部分。）
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService)：将配置数据从主站点数据库传播到本地主机缓存。
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService)：当主站点数据库不可用时，选择可供用户使用的虚拟桌面或应用程序。

Delivery Controller 安装还会创建以下 Windows 服务。这些服务在与其他 Citrix 组件一起安装时也会创建：

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc)：支持收集诊断信息供 Citrix 支持人员使用。
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService)：收集诊断信息供 Citrix 分析，以便管理员可以查看分析结果和建议，从而帮助诊断站点问题。

Delivery Controller 安装还会创建以下 Windows 服务。此服务目前未使用。如果已启用，请将其禁用。

- Citrix 远程代理提供程序 (NT SERVICE\XaXdCloudProxy)

Delivery Controller 安装还会创建以下 Windows 服务。这些服务目前未使用，但必须启用。请勿禁用它们。

- Citrix 编排服务 (NT SERVICE\CitrixOrchestration)
- Citrix 信任服务 (NT SERVICE\CitrixTrust)

除了 Citrix StoreFront™ Privileged Administration Service 之外，这些服务都被授予“作为服务登录”的登录权限以及“调整进程内存配额”、“生成安全审核”和“替换进程级别令牌”的特权。您无需更改这些用户权限。Delivery Controller 不使用这些特权，并且它们会自动禁用。

除了 Citrix StoreFront Privileged Administration service 和 Citrix Telemetry Service 之外，前面列出的 Delivery Controller Windows 服务都配置为以 NETWORK SERVICE 身份登录。请勿更改这些服务设置。

Citrix 配置同步服务需要 NETWORK SERVICE 帐户属于 Delivery Controller 上的本地管理员组。这允许本地主机缓存正常工作。

Citrix StoreFront 特权管理服务配置为以本地系统 (NT AUTHORITY\SYSTEM) 身份登录。这是 Delivery Controller StoreFront 操作所必需的，这些操作通常对服务不可用（包括创建 Microsoft IIS 站点）。请勿更改其服务设置。

Citrix 遥测服务配置为以其自己的服务特定身份登录。

您可以禁用 Citrix 遥测服务。除了此服务以及已禁用的服务之外，请勿禁用任何其他 Delivery Controller Windows 服务。

管理登录权限

VDA 的计算机帐户必须具有登录权限“从网络访问此计算机”。请参阅基于 Active Directory OU 的控制器发现。

客户端访问

客户端访问通常通过部署 Citrix StoreFront 提供。有关保护 StoreFront 的更多信息，请参阅 StoreFront 文档。

为允许远程用户安全连接到 StoreFront 和 VDA，请部署 NetScaler® 网关。

Citrix 建议客户端使用 Citrix Workspace 应用程序连接到 StoreFront。有关更多信息，请参阅适用于每个操作系统的 Citrix Workspace 应用程序的文档的安全部分。或者，用户可以使用 Web 浏览器访问 StoreFront。

考虑为用户提供瘦客户端，其中用户运行 Citrix Workspace™ 应用程序以外的应用程序的能力有限。如果设备由您的组织管理，您应该制定策略以确保部署操作系统安全更新和防病毒软件。然而，在许多情况下，用户需要能够从组织控制之外的非托管设备进行连接。请考虑使用以下功能：

- 端点分析 用于扫描端点以获取安全信息（例如操作系统和防病毒软件），并拒绝不符合您安全要求的客户端的访问。
- 应用程序保护 阻止键盘记录器和屏幕捕获。

混合版本环境

混合版本环境，例如 VDA 版本与 Delivery Controller 版本不同，在某些升级过程中是不可避免的。请遵循最佳实践，并尽量缩短不同版本的 Citrix 组件共存的时间。在混合版本环境中，安全策略（例如）可能无法统一执行。

> **注意：**
>
> 这在其他软件产品中很常见。使用早期版本的 Active Directory 只能部分地对更高版本的 Windows 强制执行组策略。

以下场景描述了在特定混合版本 Citrix 环境中可能出现的一个安全问题。当使用 Citrix Receiver 1.7 连接到运行 XenApp and XenDesktop 7.6 Feature Pack 2 中 VDA 的虚拟桌面时，策略设置 **允许桌面和客户端之间传输文件** 在站点中已启用，但无法由运行 XenApp and XenDesktop 7.1 的 Delivery Controller 禁用。它无法识别此策略设置，因为该设置是在产品的更高版本中发布的。此策略设置允许用户将文件上传和下载到其虚拟桌面，这就是安全问题所在。要解决此问题，请将 Delivery Controller（或 Studio 的独立实例）升级到 7.6 Feature Pack 2 版本，然后使用组策略禁用该策略设置。或者，在所有受影响的虚拟桌面上使用本地策略。

远程电脑访问安全注意事项

远程电脑访问(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/remote-pc-access.html)实施以下安全功能：

- 支持智能卡使用。
- 当远程会话连接时，办公室电脑的显示器显示为空白。
- 远程电脑访问将所有键盘和鼠标输入重定向到远程会话，但 CTRL+ALT+DEL 以及支持 USB 的智能卡和生物识别设备除外。
- SmoothRoaming 仅支持单个用户。
- 当用户有连接到办公室电脑的远程会话时，只有该用户可以恢复对办公室电脑的本地访问。要恢复本地访问，用户在本地电脑上按 Ctrl-Alt-Del，然后使用远程会话所用的相同凭据登录。如果您的系统具有适当的第三方凭据提供程序集成，用户还可以通过插入智能卡或利用生物识别技术来恢复本地访问。可以通过组策略对象 (GPO) 启用快速用户切换或编辑注册表来覆盖此默认行为。

注意：

Citrix 建议您不要将 VDA 管理员权限分配给普通会话用户。

自动分配

默认情况下，远程电脑访问支持将多个用户自动分配给 VDA。在 XenDesktop 5.6 Feature Pack 1 中，管理员可以使用 RemotePCAccess.ps1 PowerShell 脚本覆盖此行为。此版本使用注册表项来允许或禁止多个自动远程电脑分配。此设置适用于整个站点。

注意：

> 错误编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。编辑注册表之前，请务必备份注册表。

> 要将自动分配限制为单个用户：

在站点中的每个 Controller 上，设置以下注册表项：

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple user assignment.
```

如果存在任何现有用户分配，请使用 SDK 命令将其删除，以便 VDA 随后有资格进行单个自动分配。

- 从 VDA 中删除所有已分配的用户：`$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- 从交付组中移除 VDA：`$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

重新启动物理办公电脑。

管理证书

TLS 使用证书在双方之间建立信任。您必须在提供服务的每台服务器上安装合适的证书，并确保连接到该服务器的机器信任该证书。证书签名有以下选项：

- 自签名证书。不推荐使用这些证书。它们难以管理，因为您必须手动将此证书复制到任何其他必须信任该证书的机器上。
- 企业证书颁发机构。如果您已部署现有 PKI，那么这通常是用于内部设备之间签名的最简单选项。
- 公共证书颁发机构。这要求您向证书颁发机构证明域的所有权。它的优点是，非托管客户端设备通常预配置为信任来自主要公共证书颁发机构的证书。

创建新证书

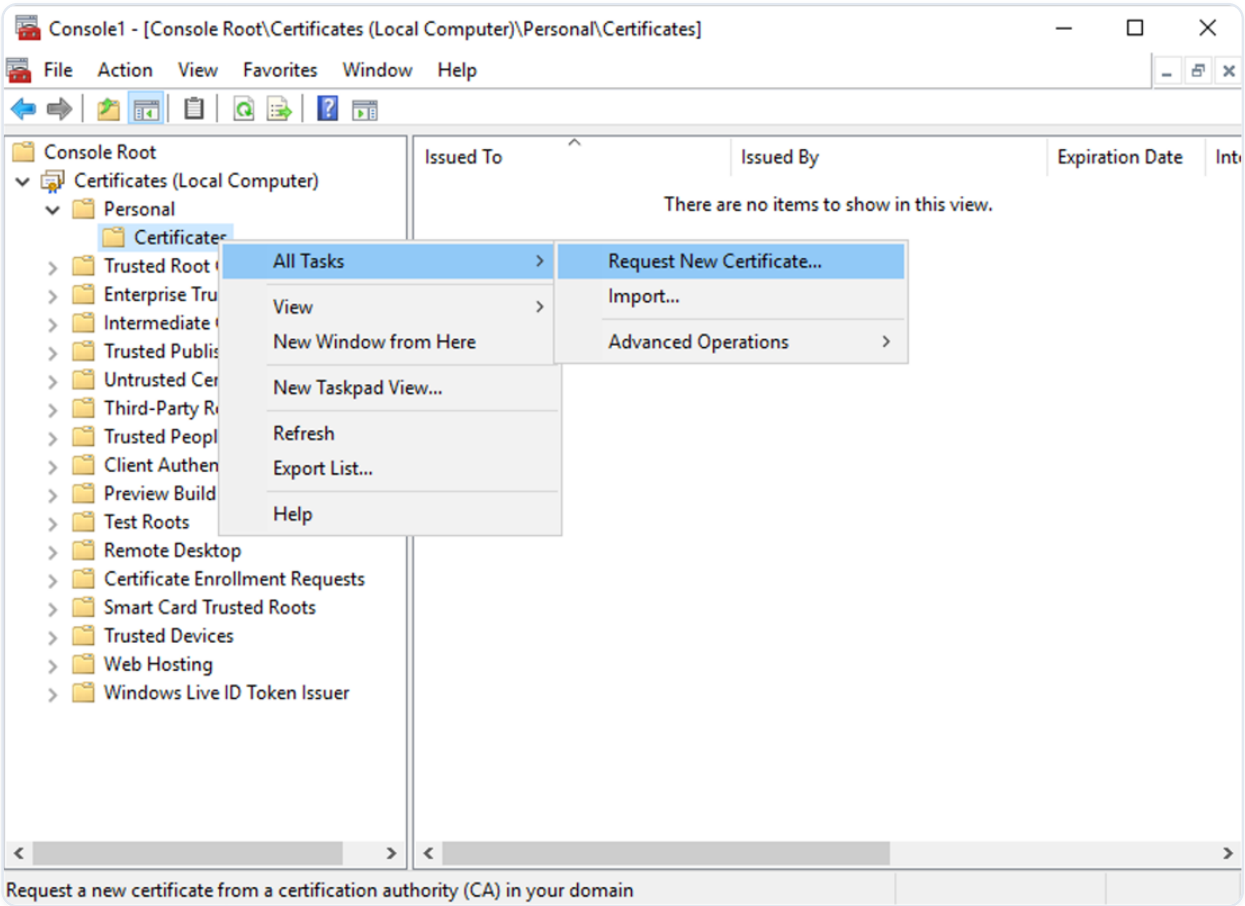
遵循您组织创建证书的策略和程序。

使用 Microsoft 证书颁发机构创建证书

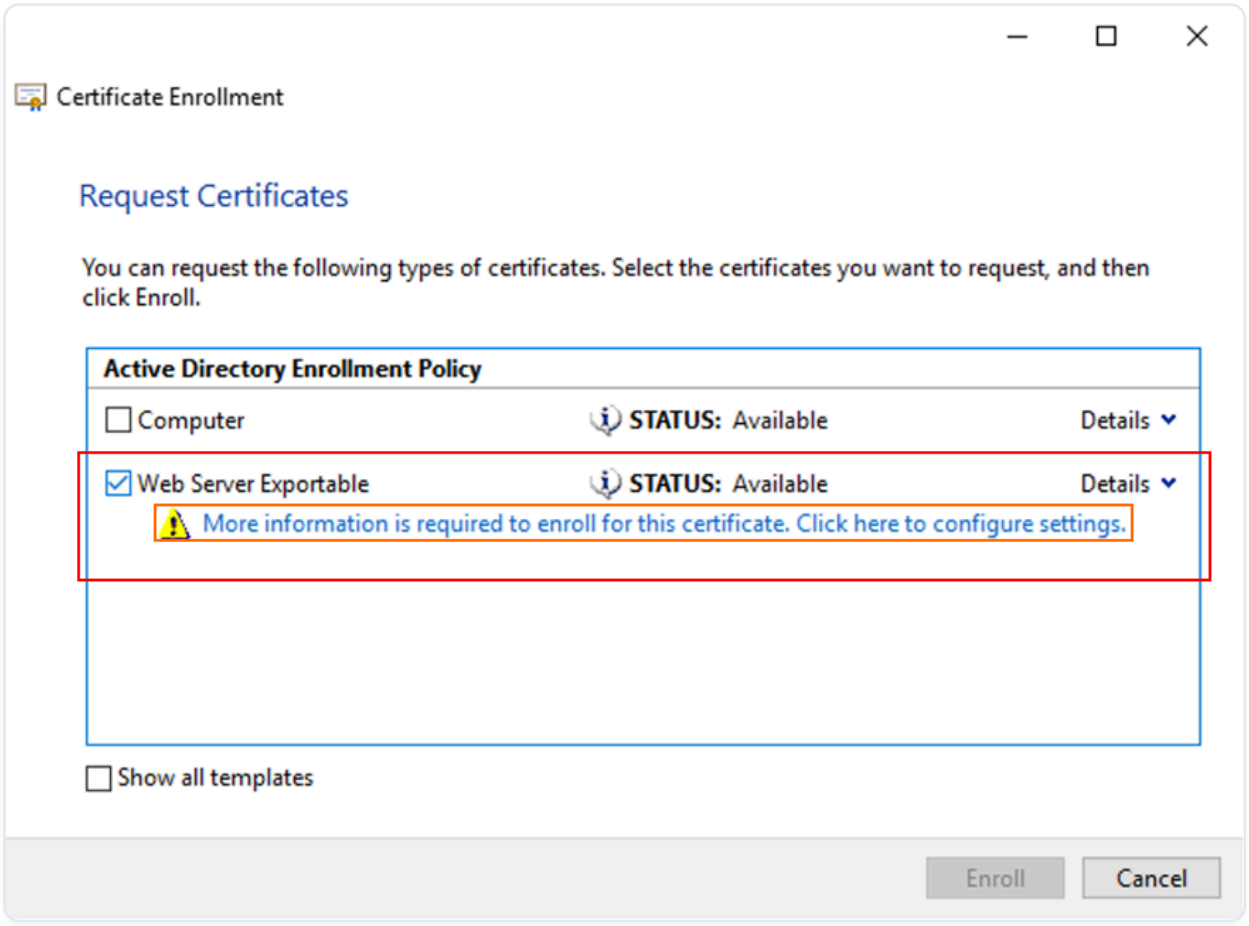
如果 Microsoft 证书颁发机构已集成到 Active Directory 域或交付控制器所加入的受信任林中，您可以从“证书”MMC 管理单元的“证书注册向导”中获取证书。Microsoft 证书颁发机构需要发布适用于 Web 服务器的证书模板。

根证书使用组策略自动部署到域中的其他机器。因此，域中的所有其他机器都信任使用 Microsoft 证书颁发机构创建的证书。如果您的机器不在域中，则需要导出根证书颁发机构证书并将其导入到这些机器中。

1. 在服务器上，打开 MMC 控制台并添加“证书”管理单元。出现提示时，选择“计算机帐户”。
2. 展开“**个人 > 证书**”，然后使用“**所有任务 > 请求新证书**”上下文菜单命令。



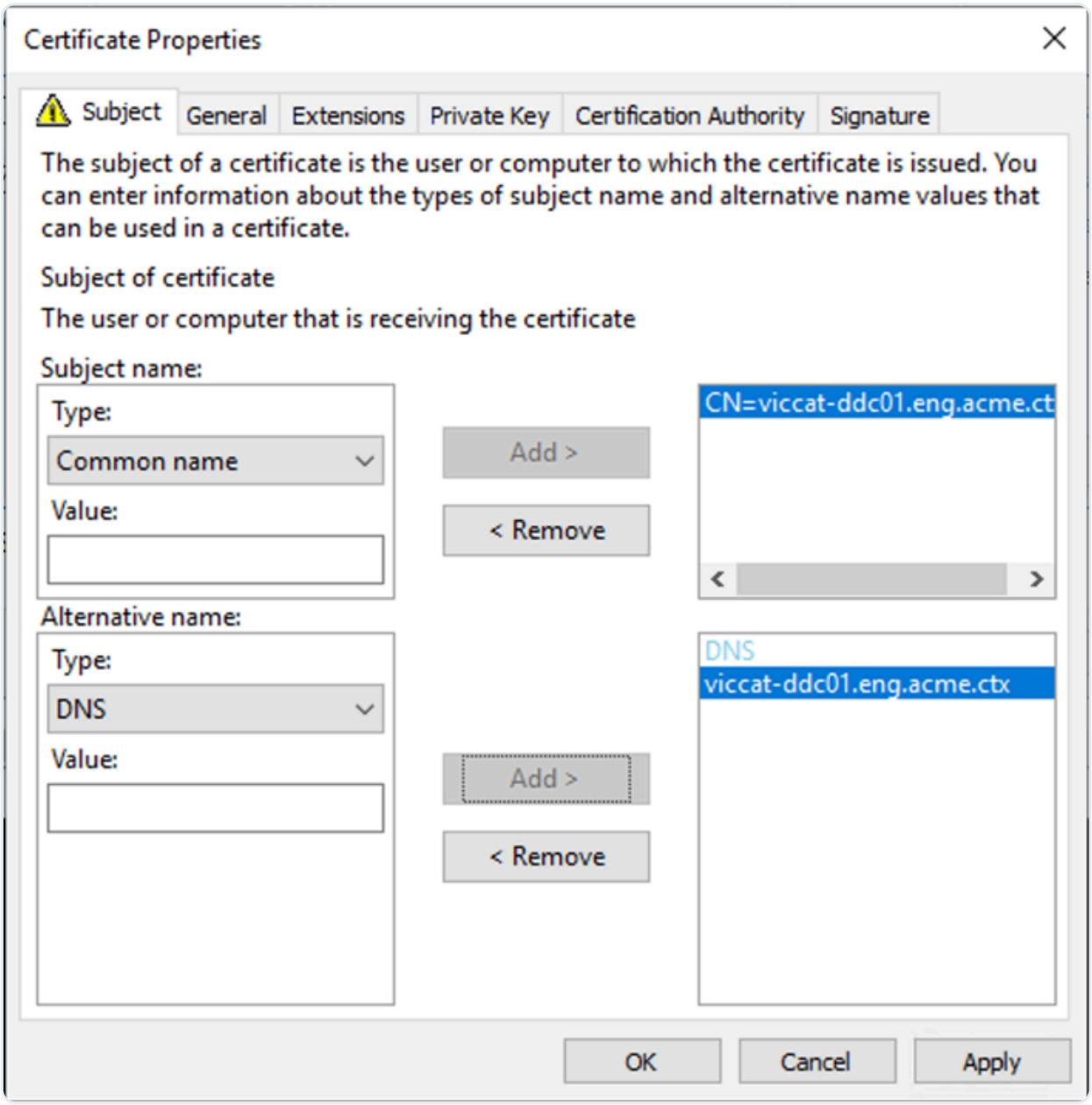
3. 单击“**下一步**”开始，然后单击“**下一步**”确认您正在从 Active Directory 注册获取证书。
4. 选择合适的模板，例如 **Web 服务器可导出**。如果模板已设置为自动提供主题的值，则无需提供更多详细信息即可单击“**注册**”。否则，单击“**需要更多信息才能注册此证书。单击此处配置设置。**”.



5. 要为证书模板提供更多详细信息，请单击“**详细信息**”箭头按钮并配置以下内容：

   主题名称：选择“公用名”并添加服务器的 FQDN。

   备用名称：选择“DNS”并添加服务器的 FQDN。



6. 按“**确定**”。
7. 按“**注册**”以创建证书。它将显示在证书列表中。

   个人证书的屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/personal-certificates.png)

使用 IIS 创建证书请求

如果服务器上安装了 IIS，请完成以下步骤：

1. 打开 **Internet 信息服务 (IIS) 管理器**
2. 在“连接”列表中选择服务器节点。
3. 打开 **服务器证书**。 指示“服务器证书”位置的屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/iis-server-certificates.png)

4. 在“**操作**”窗格中，选择“**创建证书请求...**”。 突出显示“创建证书请求”的操作菜单屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/iis-create-certificate-request.png)
5. 输入“**可分辨名称属性**”。 可分辨名称属性屏幕的屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/iis-request-certificate-properties.png)
6. 在“**加密服务提供程序属性**”屏幕上，将“**加密服务提供程序**”保留为默认值。选择 **2048** 或更高的密钥大小。 加密服务提供程序属性屏幕的屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/iis-request-certificate-crypto.png)
7. 选择文件名，然后按“**完成**”。 文件名屏幕的屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/iis-request-certificate-file-name.png)
8. 将您的 CSR 上传到您的证书颁发机构。
9. 收到证书后，在“**操作**”窗格中，选择“**完成证书请求...**”。 突出显示“完成证书请求”的操作菜单屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/iis-complete-certificate-request.png)
10. 选择证书，提供“**友好名称**”，然后按“**确定**”。 完成证书响应窗口的屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/iis-certificate-authority-response.png)

无法设置主题备用名称。因此，证书仅限于使用通用名称指定的服务器。

从证书管理单元创建证书签名请求

在证书 MMC 管理单元中，您可以创建证书签名请求。这将生成一个文件，您可以将其发送给证书颁发机构，由其提供证书。然后，您必须导入该证书以将其与本地私钥结合。

1. 在服务器上，打开 MMC 控制台并添加“证书”管理单元。出现提示时，选择“计算机帐户”。
2. 展开 **个人** > **证书**
3. 选择 **所有任务** > **高级操作** > **创建自定义请求**。
4. 在 **开始之前** 页面上，选择 **下一步**。
5. 在 **选择证书注册策略** 屏幕上，选择一个合适的现有策略，或选择 **不使用注册策略继续**。
6. 在 **自定义请求** 屏幕上，如果使用注册策略，请选择一个合适的模板（如果可用），例如 **Web 服务器可导出**。
7. 在 **证书信息** 屏幕上，展开 **详细信息** 并选择 **属性**。
8. 在 **证书属性** 窗口的 **常规** 选项卡上，输入一个合适的友好名称。
9. 在 **主题** 选项卡上：
    a. 在 **主题名称** 下，选择 **公用名** 并输入服务器的 FQDN。您可以输入通配符。选择 **添加**。
    b. 在 **主题名称** 下，为组织、组织单位、地区、省/市/自治区、国家/地区添加相应的值。

c. 在 **备用名称** 下，选择 **DNS**。添加服务器 FQDN。您可以添加多个服务器 FQDN 或通配符 FQDN。

10. 在 **扩展** 选项卡上：
    - 在 **密钥用法** 下，添加 **数字签名** 和 **密钥加密**。
    - 在 **扩展密钥用法（应用程序策略）** 下，添加 **服务器身份验证** 和 **客户端身份验证**。
11. 在 **私钥** 选项卡上。
    - 在 **选择加密服务提供商 (CSP)** 下，选择一个合适的提供商。
    - 在 **密钥选项** 下，选择一个合适的密钥大小。对于 RSA 提供商，至少使用 2048 的密钥大小。为了更高的安全性，您可能希望选择 4096，但这会对性能产生轻微影响。
    - 在 **密钥选项** 下，选择 **使私钥可导出**。
12. 选择“**确定**”。
13. 选择“**下一步**”。
14. 选择 **浏览** 并保存您的请求。
15. 选择 **完成**。
16. 将您的 CSR 上传到您的证书颁发机构。
17. 收到证书后，在同一服务器上导入它，以便将其与私钥关联。

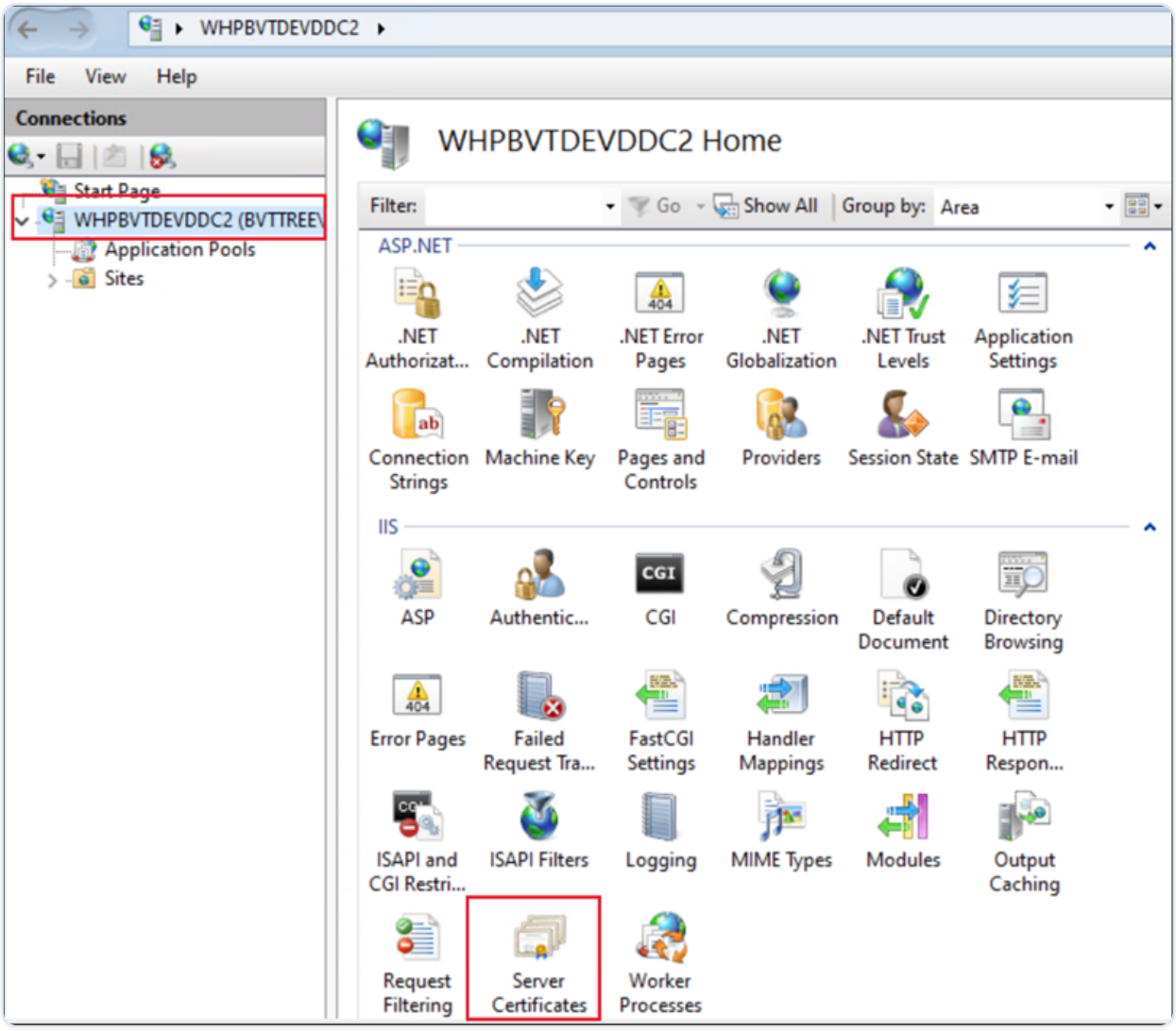
创建新的自签名证书

在安装 delivery controller™ 和 web studio 期间会创建一个自签名证书。您可以生成一个新的自签名证书并用它替换现有的证书。

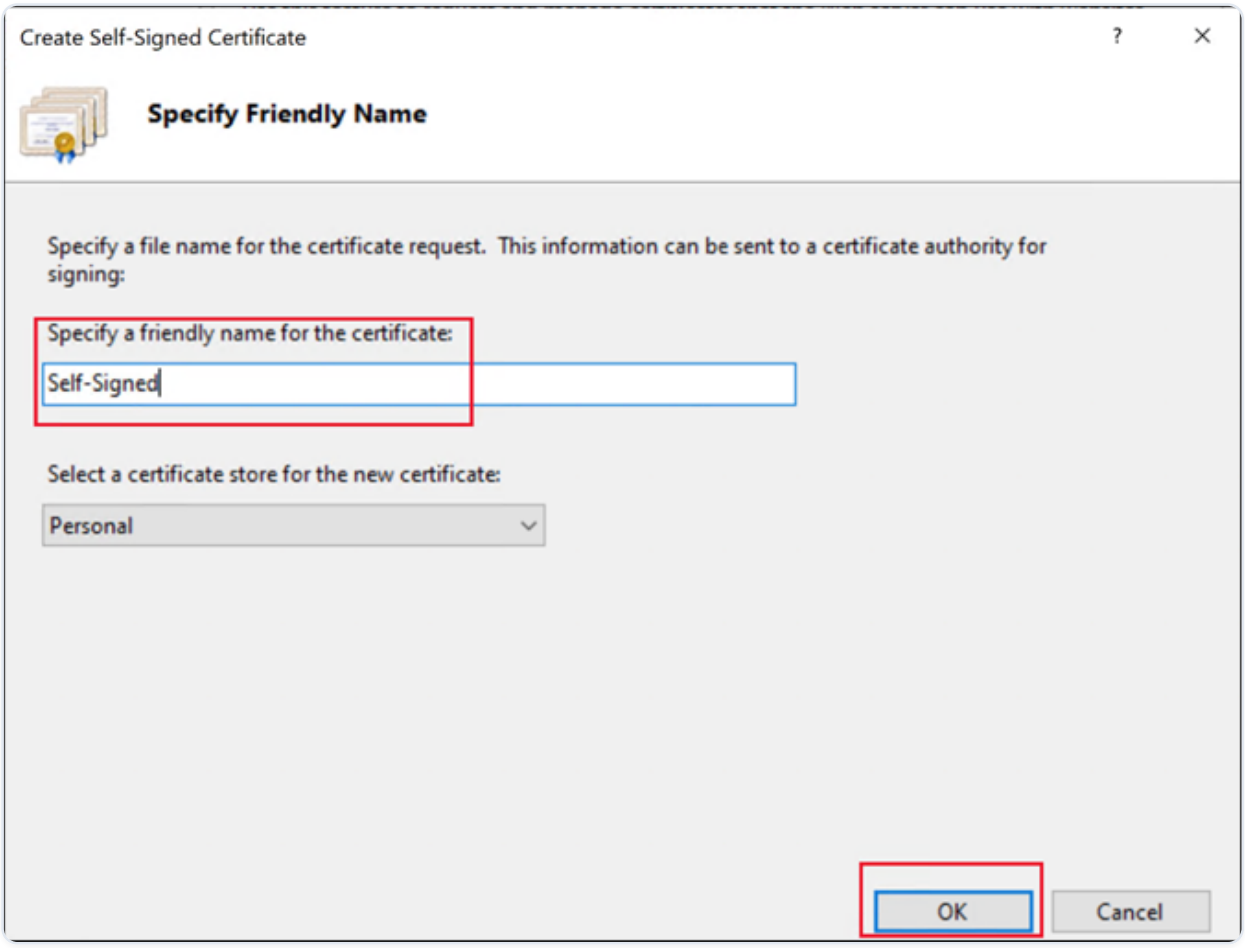
使用 IIS 管理器

如果服务器上安装了 IIS，则可以执行以下步骤：

1. 以管理员身份登录到服务器。
2. 打开 IIS 管理器
3. 打开 **服务器证书**
4. 在**操作**窗格中，选择**创建自签名证书**。



5. 在**创建自签名证书**中，输入证书名称，然后单击**确定**。然后创建自签名证书。



使用 PowerShell

您可以使用 PowerShell 创建自签名证书：

```
$certSubject = "CN=myddc.example.com" # The FQDN of the server.

$friendlyName = "Self-Signed-3"

$expireYears = 5



## Create new self-signed certificate under LocalMachine\My

$certificate = New-SelfSignedCertificate -Subject $certSubject
-CertStoreLocation "Cert:\LocalMachine\My\" -KeyExportPolicy Exportable
-KeySpec Signature -KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256
-FriendlyName $friendlyName -NotAfter $
([System.DateTime]::Now.AddYears($expireYears))
```

```
# Add to trusted root certificates

$rootCertStore = Get-Item "Cert:\LocalMachine\Root\"

$rootCertStore.Open([System.Security.Cryptography.X509Certificates.OpenFlags]::ReadWrite)

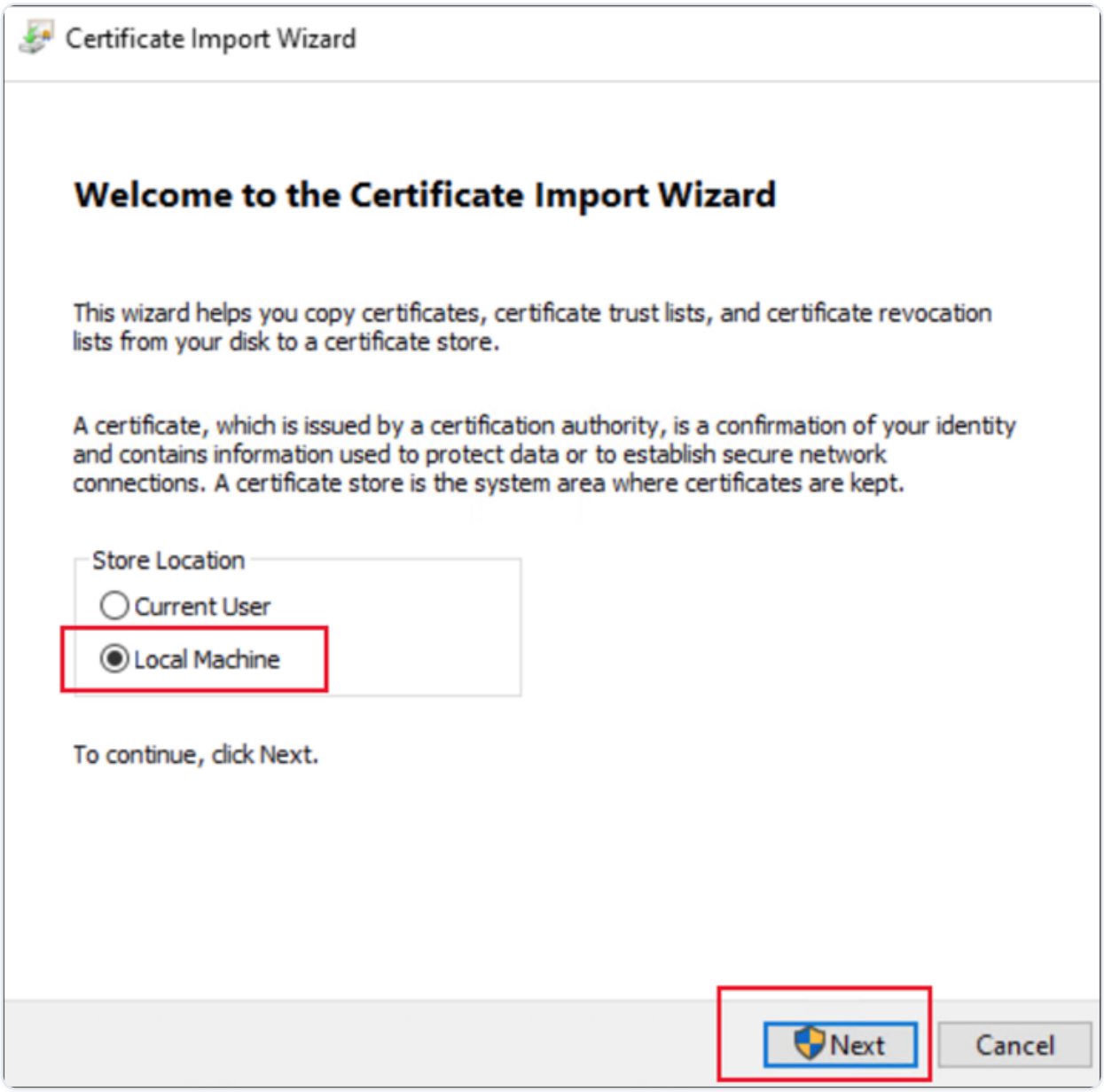
$rootCertStore.Add($certificate)
```

导入现有证书

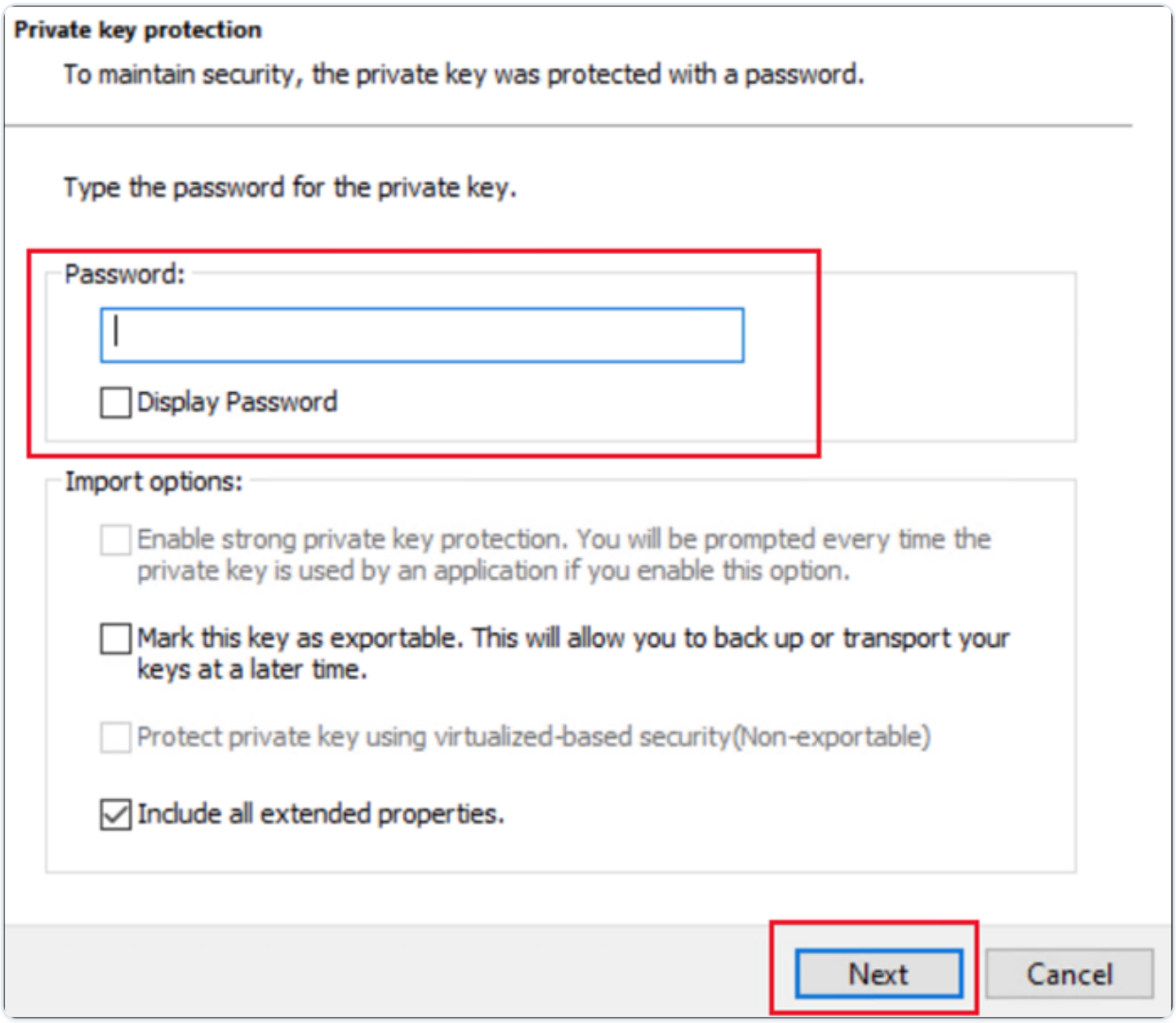
您可以使用以下任一方法将现有证书导入服务器。

证书导入向导

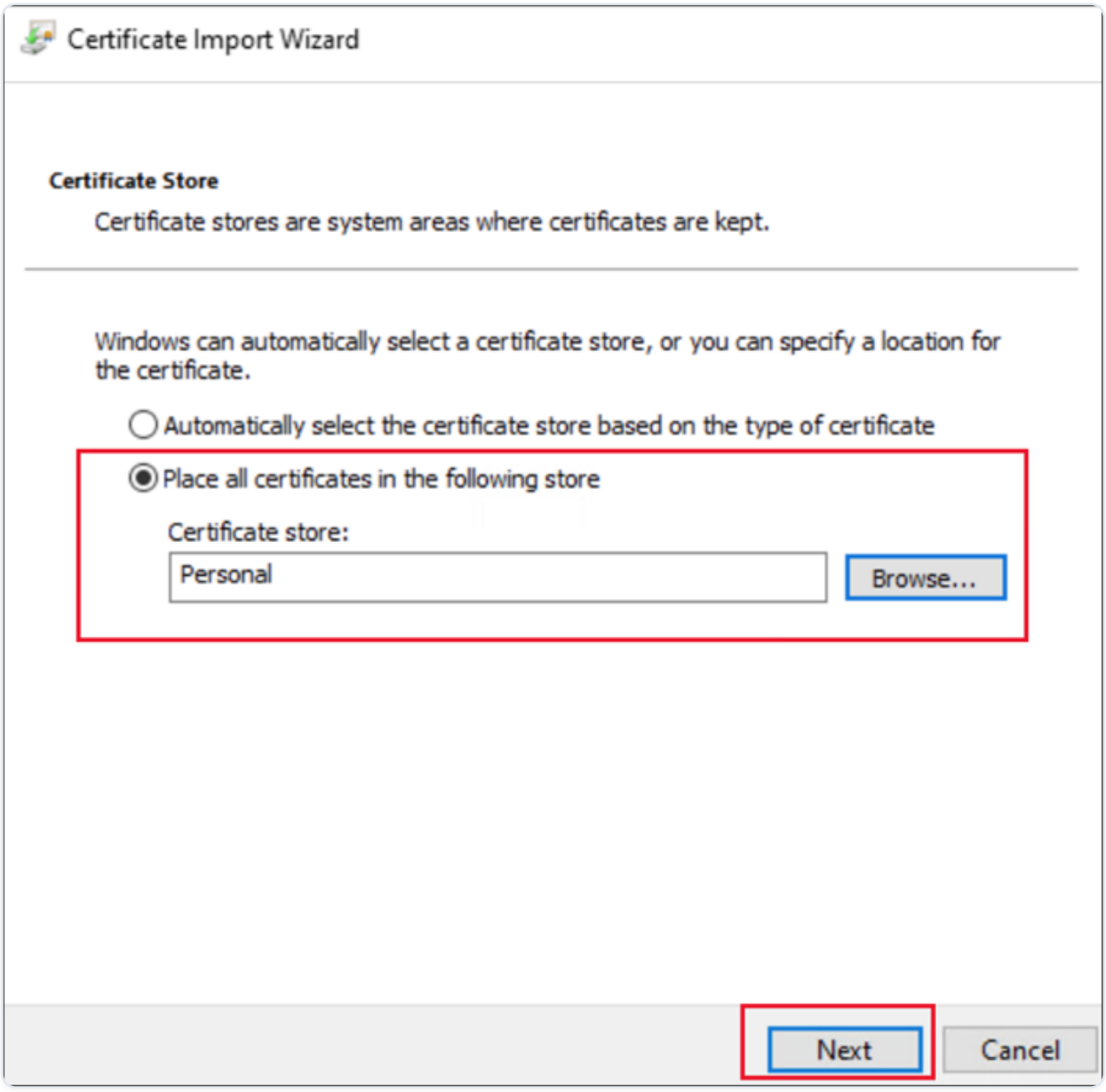
1. 双击 PFX 文件，或右键单击该文件并选择**安装 PFX**。这将打开**证书导入向导**。
2. 对于**存储位置**，选择**本地计算机**。


Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel

3. 如果需要，请输入密码。

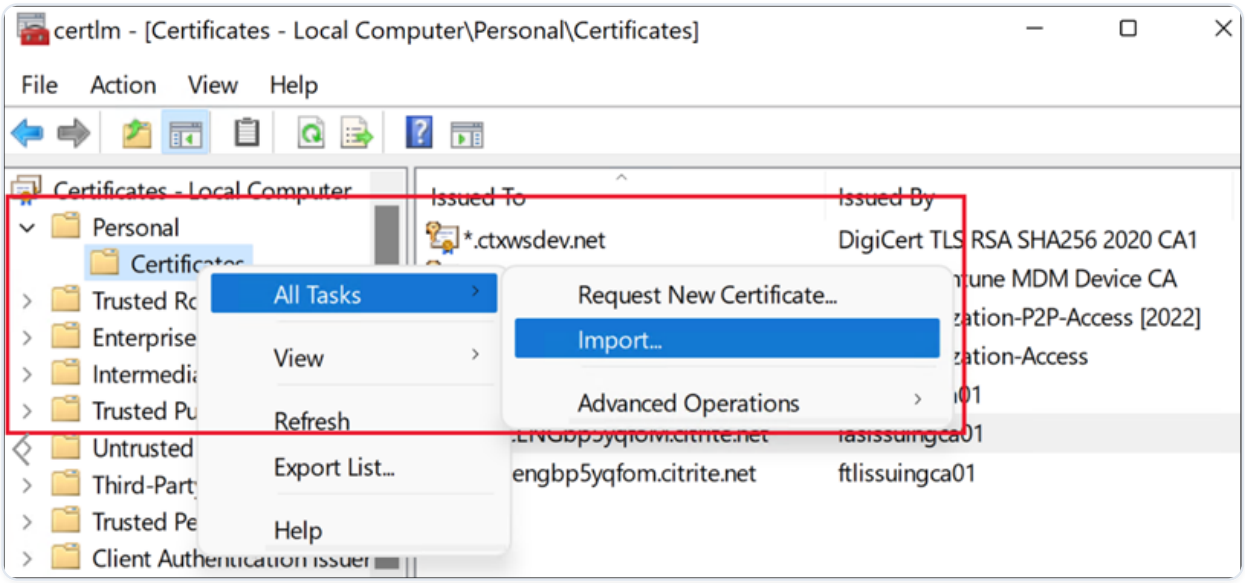


4. 选择**证书存储**。对于服务器证书，选择**个人**。如果这是您希望此计算机信任的根证书或自签名证书，则选择**受信任的根证书颁发机构**。



使用管理计算机证书控制台

1. 打开管理计算机证书控制台并导航到相应的证书存储。对于服务器证书，通常是**个人** > **证书**。要信任根证书或自签名证书，请选择**受信任的根证书颁发机构** > **证书**。
2. 右键单击证书，然后选择 > **所有任务** > **导入...**。



3. 选择 **浏览...** 并选择文件。
4. 如果需要，输入密码。

使用 PowerShell

要导入证书，请使用 PowerShell cmdlet Import-PfxCertificate。例如，要将证书 `certificate.pfx` 和密码 `123456` 导入个人证书存储，请运行以下命令：

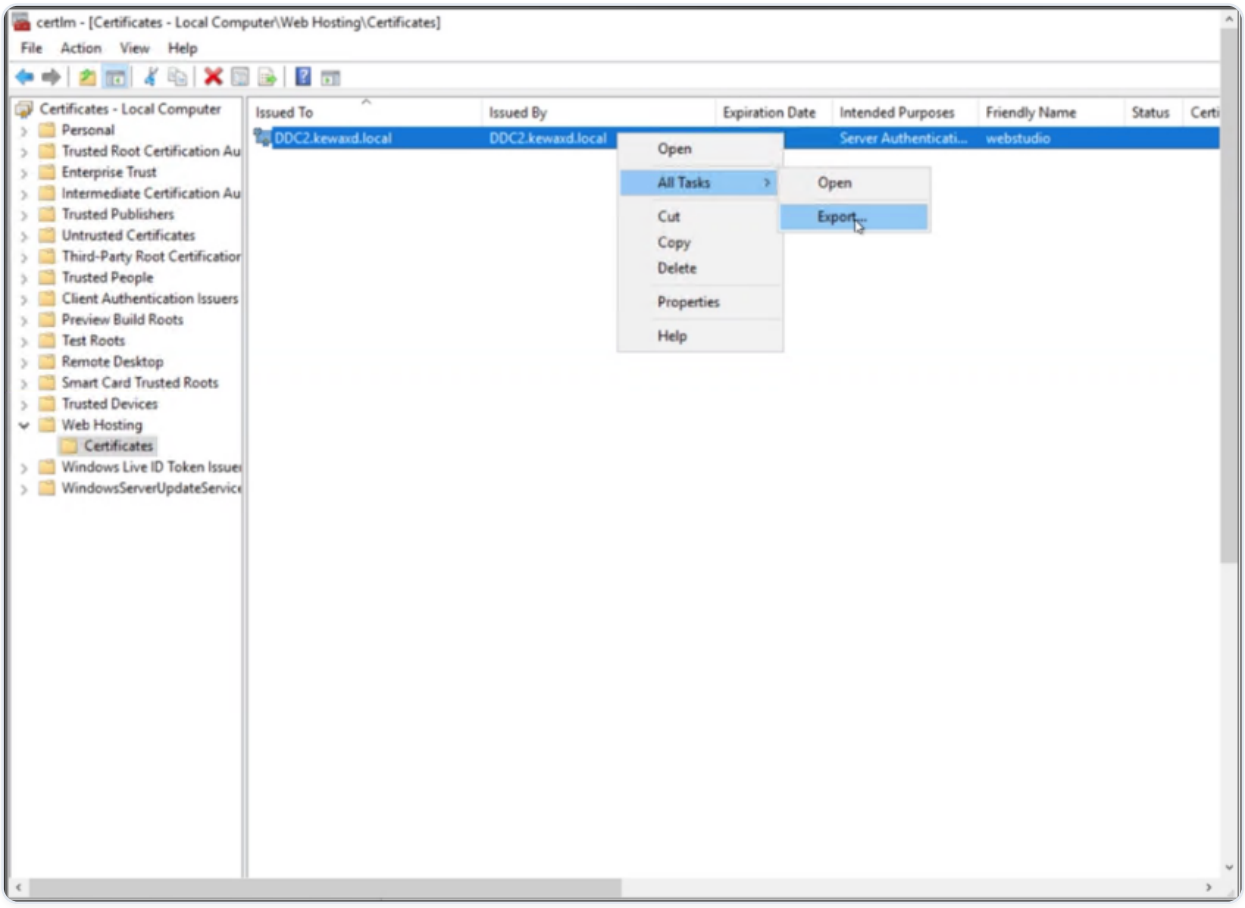
```
Import-PfxCertificate -Password $(ConvertTo-SecureString -String "123456"
-AsPlainText -Force) -CertStoreLocation Cert:\LocalMachine\My\ -FilePath .
\Desktop\certificate.pfx
```

要导入受信任的根证书，请将 `CertStoreLocation` 设置为 `Cert:\LocalMachine\Root\`。

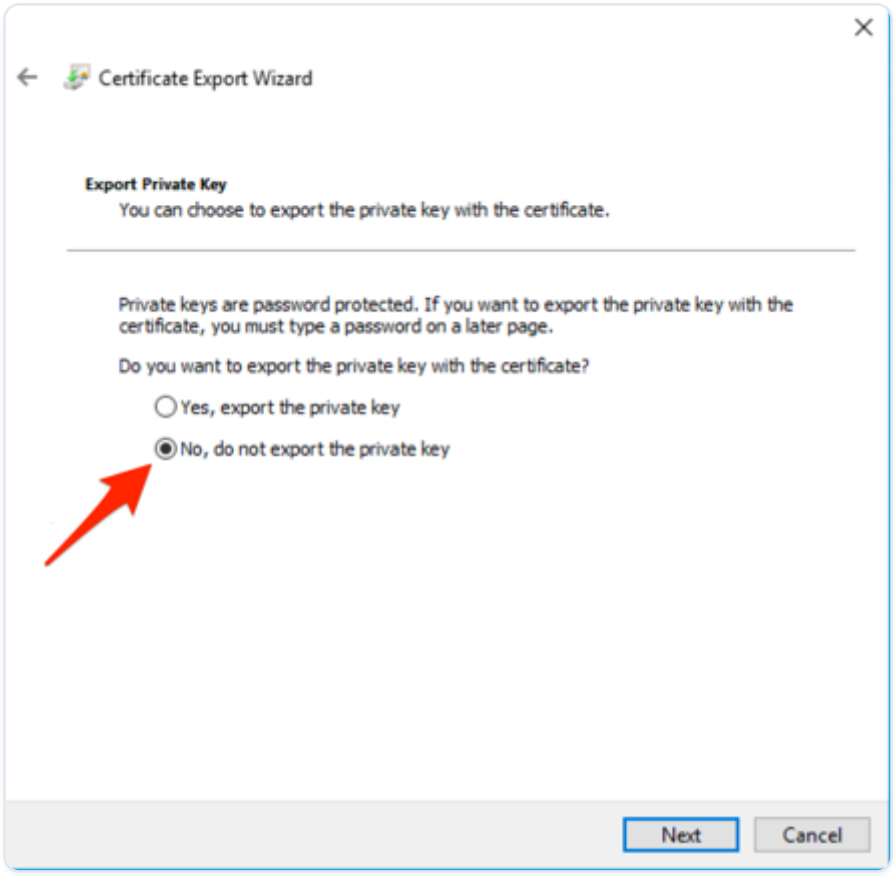
导出不带私钥的证书

要导出证书以便可以将其导入其他设备以信任该证书，应排除私钥。

1. 打开“管理计算机证书”。导航到 **个人** > **证书**，然后选择要导出的证书。
2. 从 **操作** 菜单中，选择 **所有任务**，然后选择 **导出**。

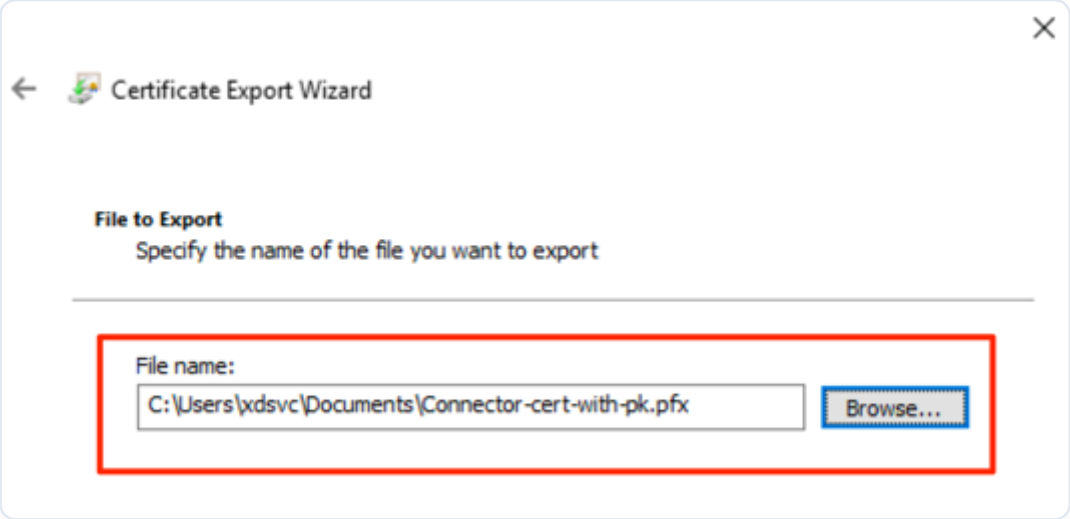


3. 选择 **否，不导出私钥**，然后按 **下一步**。



4. 选择格式 **DER 编码的二进制 X.509 (.CER)**（默认），然后按 **下一步**。

5. 输入文件名，然后按 **下一步**。



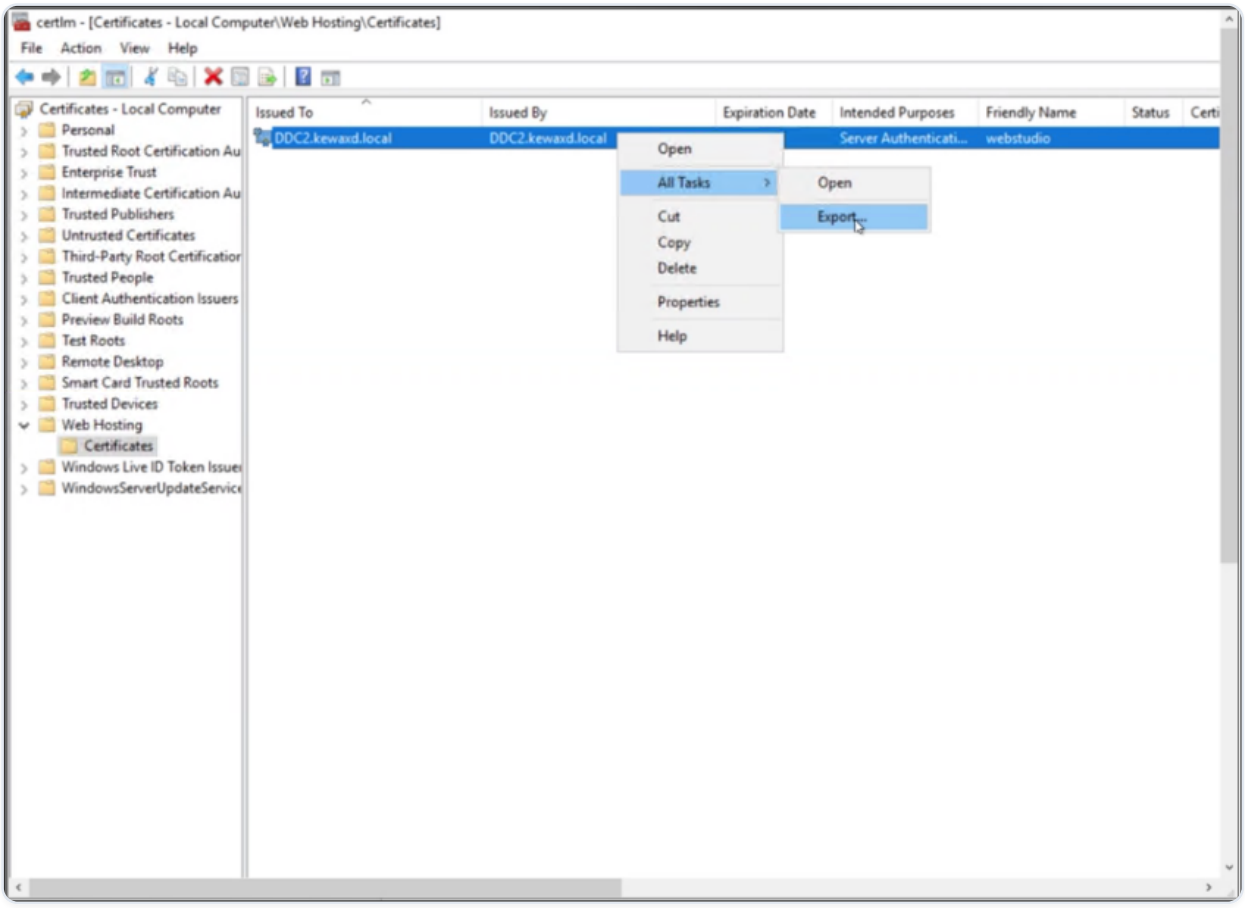
6. 选择**完成**。



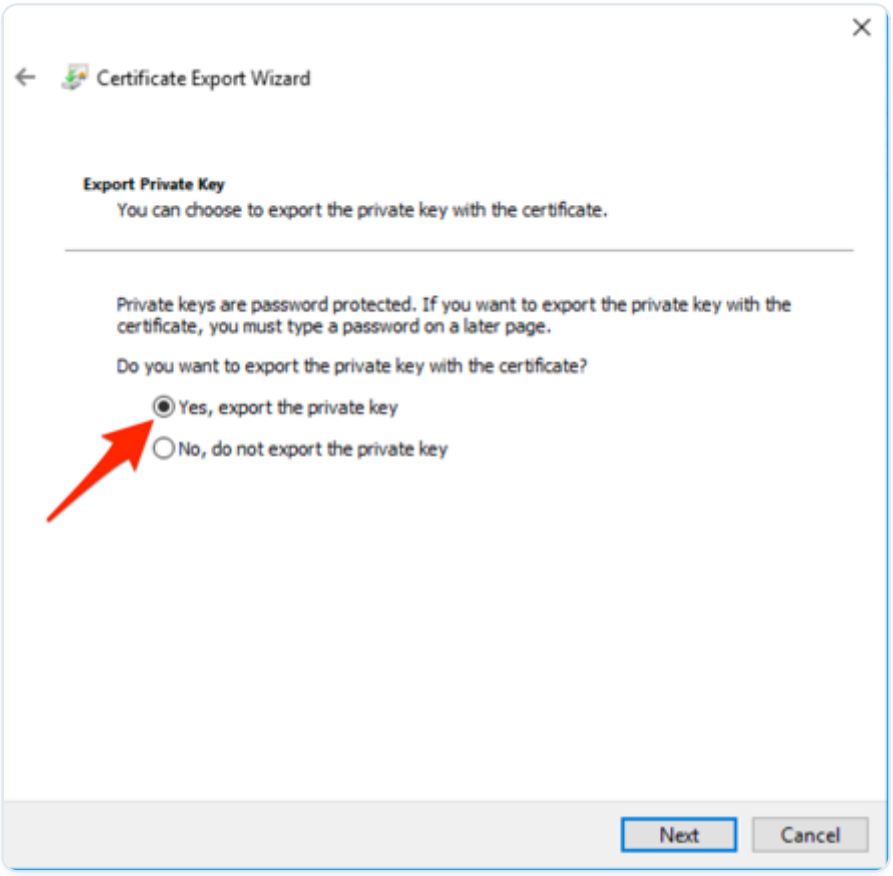
导出带私钥的证书

要导出证书以便您可以在其他服务器上使用，您必须包含私钥。

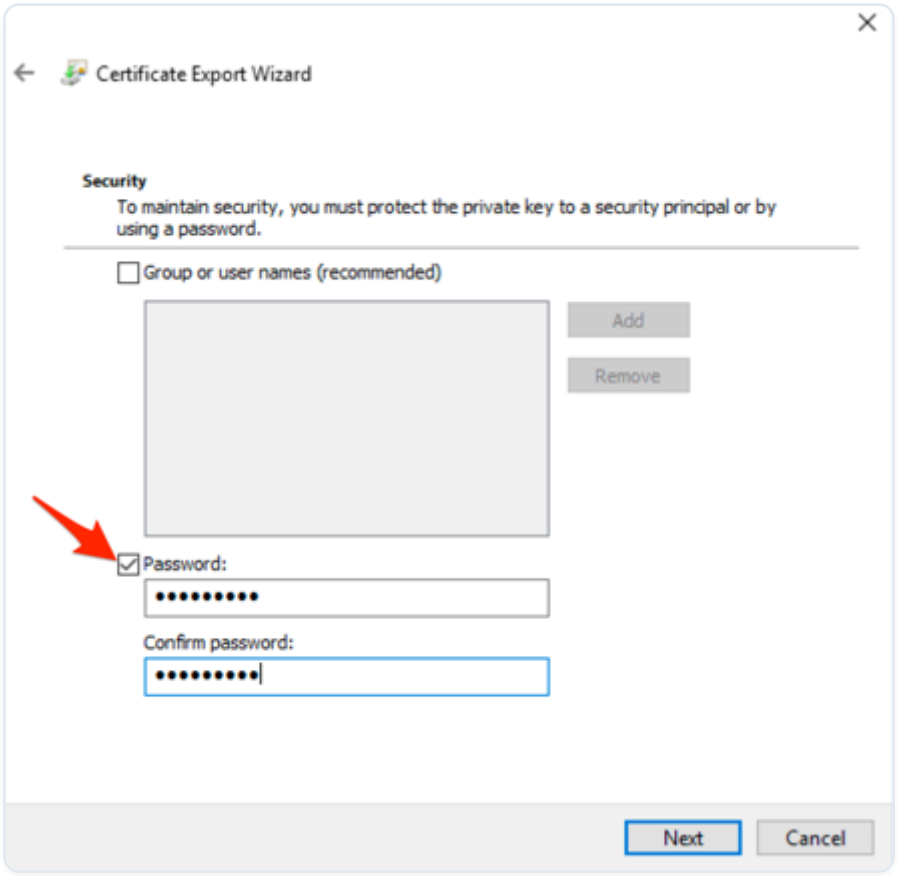
1. 打开“管理计算机证书”。导航到**个人** > **证书**并选择您要导出的证书。
2. 从**操作**菜单中，选择**所有任务**，然后选择**导出**。



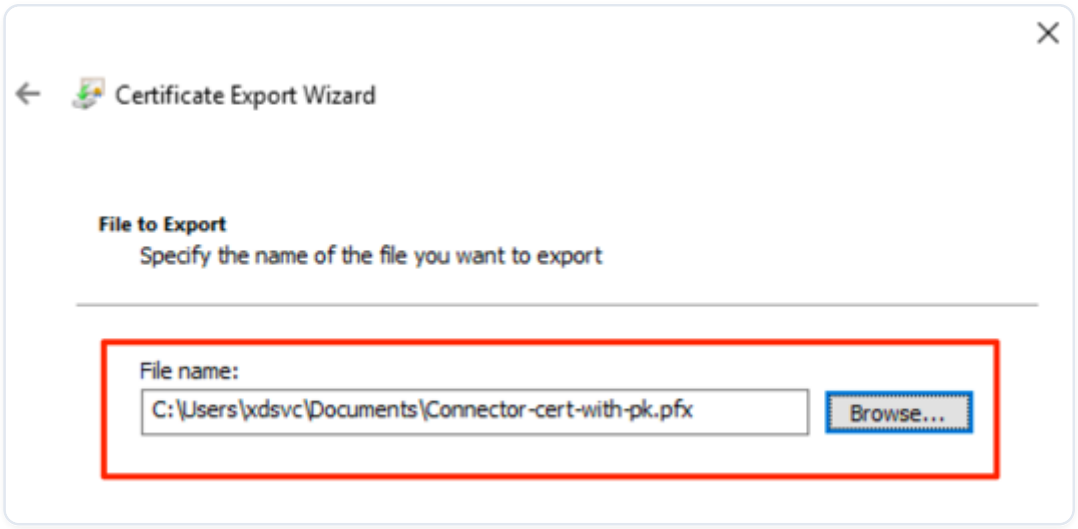
3. 选择**是，导出私钥**，然后选择**下一步**。



4. 在**安全**选项卡上，输入密码，然后选择**下一步**。



5. 输入文件名并选择**下一步**。



6. 选择**完成**。



将证书转换为 PEM 格式

默认情况下，Windows 以 PKCS#12 格式导出证书，生成包含私钥的 .pfx 文件。要在 NetScaler® Gateway 或许可证服务器上使用证书，必须将证书和私钥提取到 PEM 格式的单独文件中。您可以使用 openssl 来完成此操作。

要以 PEM 格式导出证书，请运行：

```
openssl pkcs12 -in name.pfx -clcerts -nokeys -out name.cer
```

它会要求您输入现有密码和新密码短语

要以 PEM 格式导出密钥，请运行：

```
openssl pkcs12 -in name.pfx -nocerts -out name.key
```

信任证书

- 如果您使用来自公共证书颁发机构的证书，则设备通常会预配置根证书。
- 如果您使用企业证书颁发机构，则必须将根证书部署到任何必须信任该证书的设备中。如果使用 Active Directory 证书服务，根证书也会通过组策略部署到域中的所有计算机。您必须手动将根证书导入到非域加入的计算机上，例如您的 NetScaler 网关或其他域上的计算机。
- 如果您使用的是自签名证书，则必须将其手动安装到任何需要信任该证书的计算机上。

要从 Windows 导出自签名或受信任的根证书，请参阅导出不带私钥的证书。

要使 Windows 信任该证书，您必须将证书导入到**受信任的根证书颁发机构**存储中。如果使用 PowerShell，请输入存储 **Cert:\\LocalMachine\Root**。

要使 NetScaler 信任该证书，首先将证书转换为 PEM 格式，然后安装根证书。

智能卡

智能卡和等效技术在本文所述的指导原则范围内受支持。要在 Citrix Virtual Apps 或 Citrix Virtual Desktops™ 中使用智能卡，请执行以下操作:

- 了解贵组织有关智能卡使用的安全策略。例如，这些策略可能会说明智能卡如何颁发以及用户必须如何保护它们。这些策略的某些方面可能需要在 Citrix Virtual Apps™ 或 Citrix Virtual Desktops 环境中重新评估。
- 确定哪些用户设备类型、操作系统和已发布的应用程序将与智能卡一起使用。
- 熟悉智能卡技术以及您选择的智能卡供应商的硬件和软件。
- 了解如何在分布式环境中部署数字证书。

> **注意：**
>
> 智能卡注册不支持 快速智能卡。当快速智能卡禁用时，智能卡注册可能有效，但这取决于智能卡和中间件的类型。请联系您的智能卡和中间件供应商，了解其与 Citrix Virtual Apps and Desktops 的集成以及对通过虚拟会话进行智能卡注册的支持信息。

智能卡类型

企业和消费者智能卡具有相同的尺寸、电气连接器，并适用于相同的智能卡读卡器。

企业用途的智能卡包含数字证书。这些智能卡支持 Windows 登录，也可用于应用程序的数字签名以及文档和电子邮件的加密。Citrix Virtual Apps and Desktops™ 支持这些用途。

消费者用途的智能卡不包含数字证书；它们包含共享密钥。这些智能卡可以支持支付（例如芯片签名或芯片 PIN 信用卡）。它们不支持 Windows 登录或典型的 Windows 应用程序。需要专门的 Windows 应用程序和合适的软件基础设施（例如，连接到支付卡网络）才能使用这些智能卡。请联系您的 Citrix 代表，了解在 Citrix Virtual Apps 或 Citrix Virtual Desktops 上支持这些专用应用程序的信息。

对于企业智能卡，存在可以类似方式使用的兼容等效物。

- 智能卡等效 USB 令牌直接连接到 USB 端口。这些 USB 令牌通常与 USB 闪存驱动器大小相同，但也可以小到手机中使用的 SIM 卡。它们表现为智能卡加上 USB 智能卡读卡器的组合。
- 使用 Windows 可信平台模块 (TPM) 的虚拟智能卡表现为智能卡。这些虚拟智能卡支持 Windows 8 和 Windows 10，使用 Citrix Workspace 应用程序（最低版本 Citrix Receiver 4.3）。
    - 早于 XenApp and XenDesktop 7.6 FP3 的 Citrix Virtual Apps and Desktops 版本（以前称为 XenApp and XenDesktop）不支持虚拟智能卡。
    - 有关虚拟智能卡的更多信息，请参阅 虚拟智能卡概述。

    注意： 术语“虚拟智能卡”也用于描述存储在用户计算机上的数字证书。这些数字证书与智能卡并非严格等同。

Citrix Virtual Apps and Desktops 智能卡支持基于 Microsoft 个人计算机/智能卡 (PC/SC) 标准规范。最低要求是智能卡和智能卡设备必须受底层 Windows 操作系统支持，并且必须获得 Microsoft Windows 硬件质量实验室 (WHQL) 的批准，才能在运行合格 Windows 操作系统的计算机上使用。有关硬件 PC/SC 合规性的更多信息，请参阅 Microsoft 文档。其他类型的用户设备可能符合 PS/SC 标准。有关详细信息，请参阅 Citrix Ready 计划。

通常，每个供应商的智能卡或等效设备都需要单独的设备驱动程序。但是，如果智能卡符合 NIST 个人身份验证 (PIV) 标准等标准，则可能可以使用单个设备驱动程序来支持一系列智能卡。设备驱动程序必须安装在用户设备和虚拟投递代理 (VDA) 上。设备驱动程序通常作为 Citrix 合作伙伴提供的智能卡中间件软件包的一部分提供；智能卡中间件软件包提供高级功能。设备驱动程序也可以描述为加密服务提供程序 (CSP)、密钥存储提供程序 (KSP) 或微型驱动程序。

Citrix 已测试以下适用于 Windows 系统的智能卡和中间件组合，作为其类型的代表性示例。但是，也可以使用其他智能卡和中间件。有关 Citrix 兼容智能卡和中间件的更多信息，请参阅 `<http://www.citrix.com/ready>`。

中间件	匹配的卡
Gemalto .NET 卡微型驱动程序	Gemalto .NET v2及以上

有关智能卡与其他类型设备一起使用的信息，请参阅该设备的 Citrix Workspace™ 应用程序文档。

远程电脑访问

智能卡仅支持远程访问运行 Windows 10、Windows 8 或 Windows 7 的物理办公电脑。

以下智能卡已通过远程电脑访问进行测试：

中间件	匹配的卡
Gemalto .NET 微型驱动程序	Gemalto .NET v2及以上

快速智能卡

快速智能卡是对现有基于 HDX PC/SC 的智能卡重定向的改进。它在智能卡用于高延迟 WAN 环境时提高了性能。当延迟较高时，性能改进可能非常显著（例如，Windows 快速智能卡登录需要 15 秒，而基于 PC/SC 的智能卡重定向则需要 1 分钟以上）。

快速智能卡在运行当前支持的 Windows VDA 的主机上默认启用。要在主机端禁用快速智能卡（例如，出于诊断目的），请将“Disable Cryptographic Redirection”注册表设置设置为任何非零值：

```
HKLM\SOFTWARE\Citrix\SmartCard

CryptographicRedirectionDisable (DWORD)
```

在客户端，要启用快速智能卡，请在关联的 StoreFront 站点的 *default.ica* 文件中包含 SmartCardCryptographicRedirection ICA 参数：

```
[WFClient]

SmartCardCryptographicRedirection=On
```

此外，在客户端，可以使用以下注册表设置强制启用或强制禁用快速智能卡（例如，出于诊断目的）：

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (作为非零 DWORD)

或者

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (作为非零 DWORD)

如果客户端计算机是 64 位，则必须指定 32 位注册表配置单元（使用 `WOW6432Node`）。

限制：

- 只有适用于 Windows 的 Citrix Workspace 应用程序支持快速智能卡。如果在 default.ica 文件中配置了快速智能卡，非 Windows 版本的 Citrix Workspace 应用程序仍将使用现有的 PC/SC 重定向。
- 快速智能卡唯一支持的双跳方案是在两个跳上都启用了快速智能卡的 ICA® > ICA。由于快速智能卡不支持 ICA > RDP 双跳方案，因此这些方案不起作用。
- 快速智能卡不支持下一代加密技术 (Cryptography Next Generation)。因此，快速智能卡不支持椭圆曲线加密 (ECC) 智能卡。
- 快速智能卡仅支持只读密钥容器操作。
- 快速智能卡不支持更改智能卡 PIN。

从 VDA 2203 版和适用于 Windows 的 Citrix Workspace 应用程序 2202 版（或更高版本）开始，快速智能卡与下一代加密技术 (CNG) 兼容。此外，椭圆曲线加密 (ECC) 智能卡支持以下曲线：P-256、P-384、P-521 位，适用于 ECDSA 和 ECDH。

从 VDA 2203 版开始，快速智能卡增加了在同一用户登录会话中的应用程序之间缓存智能卡 PIN 的功能。例如，如果启用了 **会话 PIN 缓存** 并且最终用户之前已将智能卡 PIN 提供给 Outlook，当 Word 用于签署文档时，Word 会使用已缓存的智能卡 PIN（已提交给 Outlook）。**会话 PIN 缓存** 通过减少用户输入智能卡 PIN 的次数来改善用户体验。此外，如果智能卡用于登录 VDA，Windows 智能卡登录 PIN 可以选择保存到 **会话 PIN 缓存** 中。这可以进一步改善用户体验。

会话 PIN 缓存 默认禁用。可以在 VDA 上使用以下注册表设置启用和控制它：

在 HKLM\SOFTWARE\Citrix\SmartCard 中:

- `EnablePinSessionCache` 作为 DWORD (非零表示启用)
- `EnableLogonPinSessionCache` 作为 DWORD (非零表示启用)
- `PinSessionCacheEntryStaleTimeout` 作为 DWORD (条目失效前的秒数，默认为 1 小时)

智能卡读卡器类型

智能卡读卡器可能内置于用户设备中，也可能单独连接到用户设备（通常通过 USB 或蓝牙）。支持符合 USB 芯片/智能卡接口设备 (CCID) 规范的接触式读卡器。它们包含一个插槽或刷卡口，用户可将智能卡插入其中。德国信贷经济 (DK) 标准定义了四类接触式读卡器。

- 1 类智能卡读卡器最常见，通常包含一个插槽。支持 1 类智能卡读卡器，通常随操作系统提供标准 CCID 设备驱动程序。
- 2 类智能卡读卡器还包含一个安全键盘，用户设备无法访问该键盘。2 类智能卡读卡器可能内置于带有集成安全键盘的键盘中。对于 2 类智能卡读卡器，请联系您的 Citrix 代表；可能需要读卡器特定的设备驱动程序才能启用安全键盘功能。

- 3 类智能卡读卡器还包含一个安全显示屏。不支持 3 类智能卡读卡器。
- 4 类智能卡读卡器还包含一个安全事务模块。不支持 4 类智能卡读卡器。

注意：

智能卡读卡器类别与 USB 设备类别无关。

智能卡读卡器必须在用户设备上安装相应的设备驱动程序。

有关支持的智能卡读卡器的信息，请参阅您正在使用的 Citrix Workspace 应用程序的文档。在 Citrix Workspace 应用程序文档中，支持的版本列在智能卡文章或系统要求文章中。

用户体验

智能卡支持已集成到 Citrix Virtual Apps and Desktops 中，使用默认启用的特定 ICA/HDX 智能卡虚拟通道。

重要提示：请勿将通用 USB 重定向用于智能卡读卡器。智能卡读卡器默认禁用此功能，如果启用则不受支持。

可以在同一用户设备上使用多张智能卡和多个读卡器，但如果使用直通身份验证，则用户启动虚拟桌面或应用程序时只能插入一张智能卡。当智能卡在应用程序中使用时（例如，用于数字签名或加密功能），可能会出现其他提示，要求插入智能卡或输入 PIN 码。如果同时插入了多张智能卡，则可能会发生这种情况。

- 如果智能卡已在读卡器中，但系统仍提示用户插入智能卡，则用户必须选择“取消”。
- 如果系统提示用户输入 PIN 码，则用户必须再次输入 PIN 码。

您可以使用卡管理系统或供应商实用程序重置 PIN 码。

重要提示：

在 Citrix Virtual Apps 或 Citrix Virtual Desktops 会话中，不支持将智能卡与 Microsoft 远程桌面连接应用程序配合使用。这有时被称为“双跳”使用。

部署智能卡之前

- 获取智能卡读卡器的设备驱动程序并将其安装在用户设备上。许多智能卡读卡器可以使用 Microsoft 提供的 CCID 设备驱动程序。
- 从智能卡供应商处获取设备驱动程序和加密服务提供程序 (CSP) 软件，并将其安装在用户设备和虚拟桌面上。驱动程序和 CSP 软件必须与 Citrix Virtual Apps and Desktops 兼容；请查阅供应商文档以了解兼容性。对于使用支持并使用微型驱动程序模型的智能卡的虚拟桌面，智能卡微型驱动程序会自动下载，但您也可以从 http://catalog.update.microsoft.com 或从您的供应商处获取它们。此外，如果需要 PKCS#11 中间件，请从卡供应商处获取。
- 重要提示：Citrix 建议您在安装 Citrix 软件之前，先在物理计算机上安装并测试驱动程序和 CSP 软件。
- 对于在 Windows 10 中使用 Internet Explorer 的智能卡用户，将 Citrix Receiver™ for Web URL 添加到“受信任站点”列表。在 Windows 10 中，Internet Explorer 默认情况下不会为受信任站点在保护模式下运行。
- 确保您的公钥基础结构 (PKI) 配置正确。这包括确保为 Active Directory 环境正确配置了证书到帐户的映射，并且可以成功执行用户证书验证。
- 确保您的部署符合与智能卡一起使用的其他 Citrix 组件（包括 Citrix Workspace 应用程序和 StoreFront）的系统要求。
- 确保可以访问站点中的以下服务器：
    - 与智能卡上的登录证书关联的用户帐户的 Active Directory 域控制器
    - 交付控制器™
    - 思杰 StoreFront
    - Citrix 网关/Citrix 访问网关 10.x
    - VDA
    - (远程电脑访问可选)：Microsoft Exchange Server

启用智能卡使用

步骤 1. 根据您的卡片颁发策略向用户颁发智能卡。

步骤 2. (可选) 设置智能卡以启用用户进行远程电脑访问。

步骤 3. 安装并配置 Delivery Controller 和 StoreFront（如果尚未安装），以用于智能卡远程处理。

步骤 4. 启用 StoreFront 以使用智能卡。有关详细信息，请参阅 StoreFront 文档中的“配置智能卡身份验证”。

步骤 5. 启用 Citrix Gateway/Access Gateway 以使用智能卡。有关详细信息，请参阅 NetScaler 文档中的“配置身份验证和授权”以及“通过 Web 界面配置智能卡访问”。

步骤 6. 启用 VDA 以使用智能卡。

- 确保 VDA 具有所需的应用程序和更新。
- 安装中间件。
- 设置智能卡远程处理，以实现在用户设备上的 Citrix Workspace 应用程序与虚拟桌面会话之间智能卡数据的通信。

步骤 7. 启用用户设备（包括已加入域或未加入域的计算机）以使用智能卡。有关详细信息，请参阅 StoreFront 文档中的“配置智能卡身份验证”。

- 将证书颁发机构根证书和颁发证书颁发机构证书导入设备的密钥库。
- 安装供应商的智能卡中间件。
- 安装并配置适用于 Windows 的 Citrix Workspace 应用程序，务必使用组策略管理控制台导入 icaclient.adm 并启用智能卡身份验证。

步骤 8. 测试部署。通过使用测试用户的智能卡启动虚拟桌面，确保部署已正确配置。测试所有可能的访问机制（例如，通过 Internet Explorer 和 Citrix Workspace 应用程序访问桌面）。

跟踪智能卡读卡器插入计数

通过智能卡远程处理，您可以使用 SCardGetStatusChange 函数跟踪智能卡插入或从读卡器中移除的次数。该函数会更新一个 SCARD_READERSTATE 数据结构数组，每个您监控的读卡器对应一个。每个 SCARD_READERSTATE 的 dwEventState 字段的高字（16 位）包含读卡器计数。有关详细信息，请参阅 Microsoft 文章 SCardGetStatusChangeA function 和 SCARD_READERSTATEA structure。

“**读卡器插入计数报告**”设置默认处于禁用状态。要启用跟踪，请添加以下注册表项：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

名称: EnableReaderInsertCountReporting

类型: DWORD

值: 任何非零值

会话断开连接时，计数将重置为零。

“**读卡器插入计数报告**”与第三方智能卡中间件兼容。

智能卡部署

此产品版本以及包含此版本的混合环境支持以下类型的智能卡部署。其他配置可能有效，但不受支持。

类型	STOREFRONT™ 连接
本地已加入域的计算机	直接连接
从已加入域的计算机进行远程访问	通过 Citrix Gateway 连接
未加入域的计算机	直接连接
从未加入域的计算机进行远程访问	通过 Citrix Gateway 连接
访问 Desktop Appliance 站点的未加入域的计算机和瘦客户端	通过 Desktop Appliance 站点连接
通过 XenApp® Services URL 访问 StoreFront 的已加入域的计算机和瘦客户端	通过 XenApp Services URL 连接

部署类型由智能卡读卡器所连接的用户设备的特性决定：

- 设备是已加入域还是未加入域。
- 设备如何连接到 StoreFront。
- 用于查看虚拟桌面和应用程序的软件是什么。

此外，这些部署中可以使用支持智能卡的应用程序，例如 Microsoft Word 和 Microsoft Excel。这些应用程序允许用户对文档进行数字签名或加密。

双模式身份验证

在这些部署中，Receiver 尽可能通过向用户提供使用智能卡或输入其用户名和密码的选择来支持双模式身份验证。如果智能卡无法使用（例如，用户将其遗忘在家中或登录证书已过期），此功能会很有用。

由于未加入域的设备用户直接登录到 Receiver for Windows，因此您可以让用户回退到显式身份验证。如果配置双模式身份验证，用户最初会收到使用智能卡和 PIN 登录的提示，但如果他们的智能卡出现任何问题，他们可以选择显式身份验证。

如果部署 Citrix Gateway，用户将登录其设备，并且 Receiver for Windows 会提示他们向 Citrix Gateway 进行身份验证。这适用于已加入域和未加入域的设备。用户可以使用其智能卡和 PIN 或显式凭据登录到 Citrix Gateway。这使您能够为 Citrix Gateway 登录提供双模式身份验证。配置从

Citrix Gateway 到 StoreFront 的直通身份验证，并将凭据验证委托给 Citrix Gateway 以供智能卡用户使用，以便用户可以静默地向 StoreFront 进行身份验证。

多个 Active Directory 林注意事项

在 Citrix 环境中，智能卡在单个林中受支持。跨林的智能卡登录需要与所有用户帐户建立直接的双向林信任。不支持涉及智能卡的更复杂的多林部署（即，信任仅为单向或不同类型的部署）。

您可以在包含远程桌面的 Citrix 环境中使用智能卡。此功能可以本地安装（在智能卡连接到的用户设备上）或远程安装（在用户设备连接到的远程桌面上）。

智能卡移除策略

产品上设置的智能卡移除策略决定了在会话期间从读卡器中移除智能卡时会发生什么。智能卡移除策略通过 Windows 操作系统进行配置和处理。

策略设置	桌面行为
无操作	无操作。
锁定工作站	桌面会话已断开连接，虚拟桌面已锁定。
强制注销	用户被强制注销。如果网络连接丢失且此设置已启用，会话可能会被注销，用户可能会丢失数据。
如果是远程终端服务会话，则断开连接	会话已断开连接，虚拟桌面已锁定。

证书吊销检查

如果启用了证书吊销检查，并且用户将带有无效证书的智能卡插入读卡器，则用户无法进行身份验证或访问与该证书相关的桌面或应用程序。例如，如果无效证书用于电子邮件解密，则电子邮件仍将保持加密状态。如果卡上的其他证书（例如用于身份验证的证书）仍然有效，则这些功能将保持活动状态。

部署示例：已加入域的计算机

此部署涉及运行 Desktop Viewer 并直接连接到 StoreFront 的已加入域的用户设备。

部署示例：已加入域的计算机(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/smartcard1_1.png)

用户使用智能卡和 PIN 登录设备。Receiver 使用集成 Windows 身份验证 (IWA) 对用户向 StoreFront 服务器进行身份验证。StoreFront 将用户安全标识符 (SID) 传递给 Citrix Virtual Apps 或 Citrix Virtual Desktops。当用户启动虚拟桌面或应用程序时，由于 Receiver 上配置了单点登录功能，因此不会再次提示用户输入 PIN。

通过添加第二个 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展为双跳。虚拟桌面中的 Receiver 向第二个 StoreFront 服务器进行身份验证。此第二个连接可以使用任何身份验证方法。第一个跳中显示的配置可以在第二个跳中重复使用，或者仅在第二个跳中使用。

部署示例：从已加入域的计算机进行远程访问

此部署涉及运行 Desktop Viewer 并通过 Citrix Gateway/Access Gateway 连接到 StoreFront 的已加入域的用户设备。

部署示例：从已加入域的计算机进行远程访问(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/smartcard2_1.png)

用户使用智能卡和 PIN 登录到设备，然后再次登录到 Citrix Gateway/Access Gateway。第二次登录可以使用智能卡和 PIN，也可以使用用户名和密码，因为在此部署中 Receiver 允许双模式身份验证。

用户自动登录到 StoreFront，StoreFront 将用户安全标识符 (SID) 传递给 Citrix Virtual Apps™ 或 Citrix Virtual Desktops。当用户启动虚拟桌面或应用程序时，不会再次提示用户输入 PIN，因为 Receiver 上已配置单点登录功能。

此部署可以通过添加第二个 StoreFront 服务器和托管应用程序的服务器来扩展为双跳。虚拟桌面中的 Receiver 向第二个 StoreFront 服务器进行身份验证。此第二个连接可以使用任何身份验证方法。为第一跳显示的配置可以在第二跳中重复使用，或者仅在第二跳中使用。

部署示例：未加入域的计算机

此部署涉及运行 Desktop Viewer 并直接连接到 StoreFront 的未加入域的用户设备。

部署示例：未加入域的计算机(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/smartcard3_1.png)

用户登录到设备。通常，用户输入用户名和密码，但由于设备未加入域，因此此登录的凭据是可选的。由于在此部署中可以进行双模式身份验证，因此 Receiver 会提示用户输入智能卡和 PIN 或用户名和密码。然后 Receiver 向 StoreFront 进行身份验证。

StoreFront 将用户安全标识符 (SID) 传递给 Citrix Virtual Apps 或 Citrix Virtual Desktops。当用户启动虚拟桌面或应用程序时，会再次提示用户输入 PIN，因为此部署中不提供单点登录功能。

此部署可以通过添加第二个 StoreFront 服务器和托管应用程序的服务器来扩展为双跳。虚拟桌面中的 Receiver 向第二个 StoreFront 服务器进行身份验证。此第二个连接可以使用任何身份验证方法。为第一跳显示的配置可以在第二跳中重复使用，或者仅在第二跳中使用。

部署示例：从未加入域的计算机进行远程访问

此部署涉及运行 Desktop Viewer 并直接连接到 StoreFront 的未加入域的用户设备。

部署示例：从未加入域的计算机进行远程访问(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/smartcard4_1.png)

用户登录到设备。通常，用户输入用户名和密码，但由于设备未加入域，因此此登录的凭据是可选的。由于在此部署中可以进行双模式身份验证，因此 Receiver 会提示用户输入智能卡和 PIN 或用户名和密码。然后 Receiver 向 StoreFront 进行身份验证。

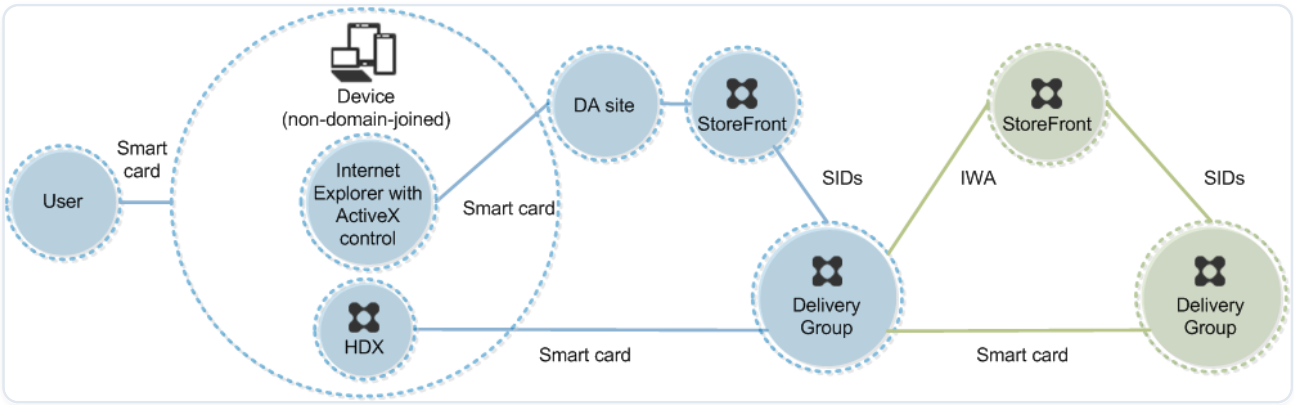
StoreFront 将用户安全标识符 (SID) 传递给 Citrix Virtual Apps 或 Citrix Virtual Desktops。当用户启动虚拟桌面或应用程序时，由于此部署中不提供单点登录功能，用户将再次被要求输入 PIN。

通过添加第二个 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展为双跳。虚拟桌面中的 Receiver 向第二个 StoreFront 服务器进行身份验证。此第二个连接可以使用任何身份验证方法。第一个跳中显示的配置可以在第二个跳中重复使用，或者仅在第二个跳中使用。

部署示例：非域加入计算机和瘦客户端访问桌面设备站点

此部署涉及非域加入的用户设备，这些设备可能运行 Desktop Lock 并通过桌面设备站点连接到 StoreFront。

Desktop Lock 是一个单独的组件，随 Citrix Virtual Apps、Citrix Virtual Desktops 和 VDI-in-a-Box 一起发布。它是 Desktop Viewer 的替代方案，主要为重新利用的 Windows 计算机和 Windows 瘦客户端设计。Desktop Lock 会替换这些用户设备中的 Windows shell 和任务管理器，从而阻止用户访问底层设备。使用 Desktop Lock，用户可以访问 Windows Server Machine 桌面和 Windows Desktop Machine 桌面。Desktop Lock 的安装是可选的。



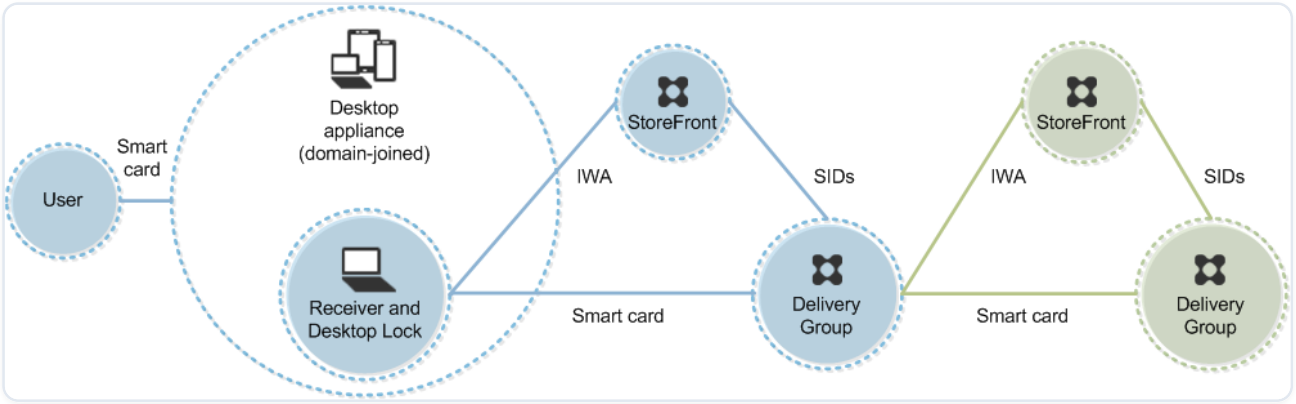
用户使用智能卡登录设备。如果设备上运行 Desktop Lock，则设备配置为通过在 Kiosk 模式下运行的 Internet Explorer 启动桌面设备站点。站点上的 ActiveX 控件会提示用户输入 PIN，并将其发送到 StoreFront。StoreFront 将用户安全标识符 (SID) 传递给 Citrix Virtual Apps 或 Citrix Virtual Desktops。分配的桌面组中按字母顺序排列的第一个可用桌面将启动。

通过添加第二个 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展为双跳。虚拟桌面中的 Receiver 向第二个 StoreFront 服务器进行身份验证。此第二个连接可以使用任何身份验证方法。第一个跳中显示的配置可以在第二个跳中重复使用，或者仅在第二个跳中使用。

部署示例：域加入计算机和瘦客户端通过 XenApp Services URL 访问 StoreFront

此部署涉及运行 Desktop Lock 并通过 XenApp Services URL 连接到 StoreFront 的域加入用户设备。

Desktop Lock 是一个单独的组件，随 Citrix Virtual Apps、Citrix Virtual Desktops 和 VDI-in-a-Box 一起发布。它是 Desktop Viewer 的替代方案，主要为重新利用的 Windows 计算机和 Windows 瘦客户端设计。Desktop Lock 会替换这些用户设备中的 Windows shell 和任务管理器，从而阻止用户访问底层设备。使用 Desktop Lock，用户可以访问 Windows Server Machine 桌面和 Windows Desktop Machine 桌面。Desktop Lock 的安装是可选的。



用户使用智能卡和 PIN 登录设备。如果设备上运行 Desktop Lock，它会使用集成 Windows 身份验证 (IWA) 对用户向 StoreFront 服务器进行身份验证。StoreFront 将用户安全标识符 (SID) 传递给 Citrix Virtual Apps 或 Citrix Virtual Desktops。当用户启动虚拟桌面时，由于 Receiver 上配置了单点登录功能，用户不会再次被要求输入 PIN。

通过添加第二个 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展为双跳。虚拟桌面中的 Receiver 向第二个 StoreFront 服务器进行身份验证。此第二个连接可以使用任何身份验证方法。第一个跳中显示的配置可以在第二个跳中重复使用，或者仅在第二个跳中使用。

智能卡直通身份验证和单点登录

直通身份验证

智能卡直通身份验证到虚拟桌面在运行 Windows 10、Windows 8 和 Windows 7 SP1 企业版和专业版的用户设备上受支持。

智能卡直通身份验证到托管应用程序在运行 Windows Server 2012 和 Windows Server 2008 R2 SP1 的服务器上受支持。

要将智能卡直通身份验证用于托管应用程序，请确保在将智能卡直通配置为站点的身份验证方法时启用 Kerberos。

注意：智能卡直通身份验证的可用性取决于许多因素，包括但不限于：

- 您的组织关于直通身份验证的安全策略。
- 中间件类型和配置。
- 智能卡读卡器类型。
- 中间件 PIN 缓存策略。

智能卡直通身份验证在 Citrix StoreFront 上配置。有关详细信息，请参阅 StoreFront 文档。

单点登录

单点登录是 Citrix 的一项功能，它通过虚拟桌面和应用程序启动实现直通身份验证。您可以在已加入域、直接连接到 StoreFront 以及已加入域、NetScaler 连接到 StoreFront 的智能卡部署中使用此功能，以减少用户输入 PIN 的次数。要在这些部署类型中使用单点登录，请编辑 StoreFront 服务器上 default.ica 文件中的以下参数：

- 已加入域、直接连接到 StoreFront 的智能卡部署 — 将 DisableCtrlAltDel 设置为 Off
- 已加入域、NetScaler 连接到 StoreFront 的智能卡部署 — 将 UseLocalUserAndPassword 设置为 On

有关设置这些参数的更多说明，请参阅 StoreFront 或 Citrix Gateway 文档。

单点登录功能的可用性取决于多种因素，包括但不限于：

- 您组织关于单点登录的安全策略。
- 中间件类型和配置。
- 智能卡读卡器类型。
- 中间件 PIN 缓存策略。

注意：

当用户在连接了智能卡读卡器的计算机上登录到 Virtual Delivery Agent (VDA) 时，可能会出现一个 Windows 磁贴，表示之前成功的身份验证模式，例如智能卡或密码。因此，当启用单点登录时，可能会出现单点登录磁贴。要登录，用户必须选择 **切换用户** 以选择另一个磁贴，因为单点登录磁贴将不起作用。

在交付控制器上启用 TLS

默认情况下，HTTP 和 HTTPS 均已启用。HTTPS 使用自签名证书，该证书使用服务器的 FQDN 作为公用名，StoreFront™ 或 Web 浏览器不信任该证书。

要在交付控制器™上启用 TLS，您必须：

- 在所有交付控制器上获取、安装和注册服务器证书。有关详细信息，请参阅请求和安装证书。
- 使用 TLS 证书配置端口。有关详细信息，请参阅安装证书。
- 为监视服务启用 HTTPS。
- 通过禁用 HTTP 来强制执行 HTTPS 流量。有关详细信息，请参阅仅强制执行 HTTPS 流量。
- （可选）您可以更改控制器用于侦听 HTTP 和 HTTPS 流量的端口。有关详细信息，请参阅更改 HTTP 或 HTTPS 端口。

请求和安装证书

要使用 TLS，您必须安装一个证书，其公用名或主题备用名称与服务器的 FQDN 匹配。如果您在交付控制器前使用负载均衡器，则将服务器和负载均衡器的 FQDN 都包含为主题备用名称。有关详细信息，请参阅证书。StoreFront 要连接到交付控制器，您必须使用 RSA 数字签名算法。StoreFront 不支持使用 ECDSA 算法的证书。

配置 SSL/TLS 侦听器端口

如果 IIS Windows 组件安装在同一服务器上（作为 Web Studio 和 Director 的一部分安装），则可以使用 IIS 配置 TLS。有关详细信息，请参阅在 Web Studio 和 Director 上启用 TLS。否则，要使用 PowerShell 配置证书：

1. 要检查是否存在已绑定的证书，请打开命令提示符并运行 `netsh http show sslcert`：

```
netsh http show sslcert
```

2. 如果存在现有绑定，请将其删除。

```
netsh http delete sslcert ipport=0.0.0.0:443
```

如果现有绑定中指定了特定的 IP 地址和端口，请将 `0.0.0.0:443` 替换为该 IP 地址和端口。

3. 查找您之前安装的证书的指纹。要查看指纹，请打开**管理计算机证书**，浏览到该证书并将其打开，然后转到**详细信息**选项卡。

证书属性显示指纹的屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/certificate-thumbprint.png)

或者，您可以使用 PowerShell。例如，以下脚本查找其公用名与服务器主机名匹配的证书并打印缩略图：

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

如果证书公用名与主机名不匹配，则此操作将失败。如果主机名有多个证书，则此操作将返回多个连接在一起的指纹，您必须选择相应的指纹。

以下示例按友好名称查找证书：

```
$friendlyName = "My certificate name"

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $friendlyName: $
($Thumbprint)" -Foreground Yellow
```

如果有多个具有指定友好名称的证书，则此操作将返回多个连接在一起的指纹，您必须选择相应的指纹。

4. 要将证书绑定到端口，请使用 `netsh http add sslcert` 命令：

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`：IP 地址和端口。使用 0.0.0.0:443 将其应用于所有 IP 地址。您可以改为指定特定的 IP 地址。
- `certhash`：您在上一步中确定的证书指纹。
- `appid`：Citrix Broker Service 的全局唯一标识符。

> **注意：**
>
> 续订证书或重新绑定时，请使用与 Broker Service 关联的特定 `appid`，而不是任意 GUID。 要查找 Citrix Broker Service 的正确 `appid`：

a. 以管理员身份打开 PowerShell 命令窗口并运行以下命令：

```
Get-WmiObject -Class Win32_Product | Select-String -Pattern
"broker"
```

b. 在输出中找到 Citrix Broker Service 的 IdentifyingNumber (GUID)（例如，`{D333C884-187F-447C-8C67-463F33989C8F}`）。将此 GUID 用于 `appid` 参数。

- `disablelegacytls=enable`：禁用旧版 TLS。此参数在 Windows 2022 及更高版本上可用。在 Windows 2022 上，它禁用 TLS 1.0 和 1.1。在 Windows 2025 上，这没有必要，因为 TLS 1.0 和 1.1 默认是禁用的。

例如，运行以下命令将指纹为 `bc96f958848639fd101a793b87915d5f2829b0b6` 的证书绑定到所有 IP 地址上的端口 `443`：

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

一旦启用 HTTPS，请配置任何 StoreFront 部署 和 NetScaler 网关以使用 HTTPS 而不是 HTTP 连接到交付控制器。

为 HTTPS 配置监视服务 OData API

监视服务提供 OData v3 和 v4 API，以允许 Citrix® 和第三方应用程序查询数据。Director 使用 OData API V3 连接到监视服务。要为 HTTPS 配置监视 OData API，请完成以下步骤：

1. 运行以下 PowerShell：

```
$serviceGroup = Get-ConfigRegisteredServiceInstance -ServiceType
Monitor | Select -First 1 ServiceGroupUid

Remove-ConfigServiceGroup -ServiceGroupUid
$serviceGroup.ServiceGroupUid

& 'C:\Program Files\Citrix\Monitor\Service\citrix.monitor.exe'
-ConfigureFirewall -RequireODataTls –OdataPort 443 -RequireODataSdkTls
–OdataSdkPort 443

get-MonitorServiceInstance | register-ConfigServiceInstance

Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-
MonitorServiceGroupMembership
```

2. 使用文本编辑器打开文件 `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config`。找到元素 `<add key="owin:baseAddress" value="http://localhost/citrix/monitor/odata/v4" />` 并将其更改为 `<add key="owin:baseAddress" value="https://localhost/citrix/monitor/odata/v4" />`。

配置密码套件

密码套件顺序列表必须包含 `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` 或 `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` 密码套件（或两者）；并且这些密码套件必须位于任何 `TLS_DHE_` 密码套件之前。

1. 使用 Microsoft 组策略编辑器，浏览到 **计算机配置 > 管理模板 > 网络 > SSL 配置设置**。
2. 编辑策略“SSL 密码套件顺序”。默认情况下，此策略设置为“未配置”。将此策略设置为“已启用”。
3. 按正确顺序排列套件。删除任何您不想使用的密码套件。

确保 `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` 或 `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` 位于任何 `TLS_DHE_` 密码套件之前。

在 Microsoft Learn 上，另请参阅 配置 TLS 密码套件顺序。

仅强制执行 HTTPS 流量

建议您将 XML Service 配置为忽略 HTTP 流量。

1. 运行 `regedit`
2. 打开 `HKLM\Software\Citrix\DesktopServer\`
3. 创建一个名为 `XmlServicesEnableNonSsl` 的新 DWORD 值，并将其设置为 0。
4. 重新启动 Broker Service。

您可以创建一个相应的注册表 DWORD 值 `XmlServicesEnableSsl` 来忽略 HTTPS 流量。请确保其未设置为 0。

更改 HTTP 或 HTTPS 端口

默认情况下，Controller 上的 XML Service 侦听端口 80 以处理 HTTP 流量，侦听端口 443 以处理 HTTPS 流量。尽管您可以使用非默认端口，但请注意将 Controller 暴露给不受信任网络的安全风险。部署独立的 StoreFront 服务器优于更改默认设置。

要更改 Controller 使用的默认 HTTP 或 HTTPS 端口，请从 Studio 运行以下命令：

```
BrokerService.exe -StoreFrontPort <http-port> -StoreFrontTlsPort <https-port>
```

其中：

- `<http-port>` 是 HTTP 流量的端口号
- `<https-port>` 是 HTTPS 流量的端口号。

注意：

更改端口后，Studio 可能会显示有关许可证兼容性和升级的消息。要解决此问题，请使用以下 PowerShell cmdlet 序列重新注册服务实例：

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS |

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
```

```
Register-ConfigServiceInstance
```

在 Web Studio 和 Director 上启用 TLS

我们建议始终通过启用 HTTPS 来使用 TLS 保护与 Web Studio 和 Director 的连接。本文介绍了如何配置 Web Studio 和 Director 以使用受信任的证书并确保通过 HTTPS 进行安全访问。

默认行为

安装 Web Studio 时，安装程序会创建一个自签名证书并将其绑定到当前服务器上的端口 443。您可以通过本地服务器上的 Web 浏览器通过 HTTPS 访问 Web Studio 和 Director。

但是，如果您尝试从另一台计算机通过 HTTPS 访问 Web Studio 或 Director，浏览器会显示安全错误，因为它不信任该证书。

注意：

如果您在未安装 Web Studio 的情况下安装 Director，则安装程序不会创建自签名证书。

启用通过 HTTPS 的安全访问

要允许从 Web Studio 服务器以外的计算机通过 HTTPS 访问 Web Studio 或 Director，请执行以下步骤：

1. 创建或导入受信任的证书。
2. 在 IIS 中将证书绑定到端口 443。
3. （可选）启用 HTTP 严格传输安全 (HSTS)。
4. 如果 Web Studio 未配置为代理（客户端计算机连接到 Web Studio 和 Delivery Controller），请在 Delivery Controller 上启用 TLS。

注意：

不建议使用自签名证书，因为它需要在每台计算机上进行手动配置。有关详细信息，请参阅使用自签名证书。

创建或导入受信任的证书

我们建议使用来自企业或公共证书颁发机构的证书，该证书应受连接到服务器的计算机信任。

有关详细信息，请参阅 创建新证书 和 导入现有证书。证书的公用名或主题备用名称必须与用户用于连接 Web Studio 或 Director 的 FQDN 匹配。如果服务器前面部署了负载均衡器，请使用负载均衡器的 FQDN。

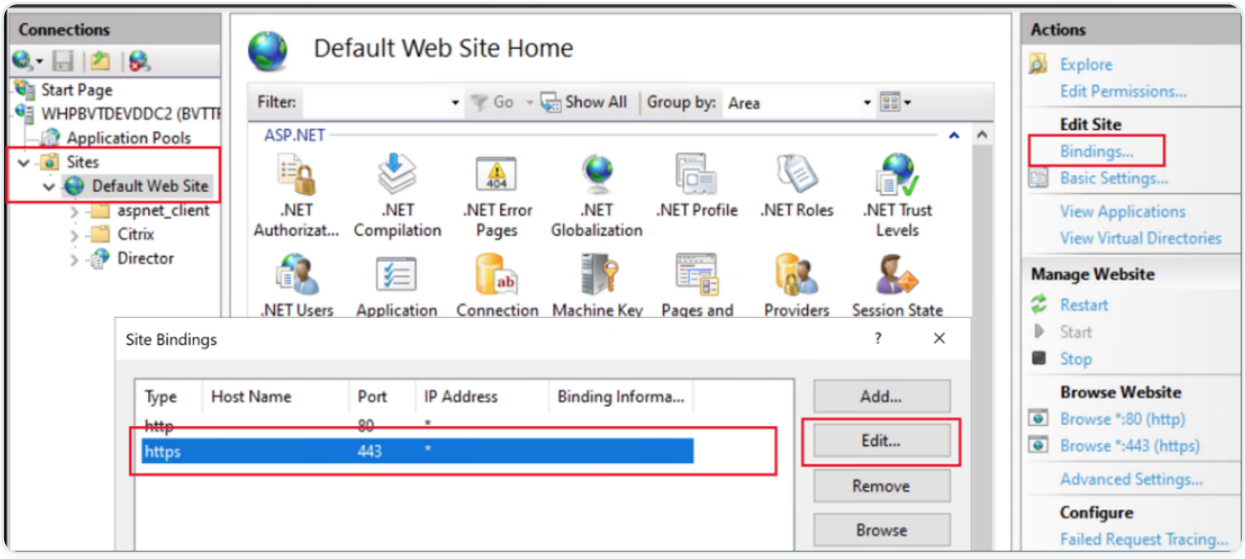
将证书绑定到端口 443

创建或导入受信任的证书后，将其绑定到 IIS 中的端口 `443`。您可以在安装之前或之后执行此操作。如果已为端口 `443` 配置了证书绑定，则安装程序不会进行任何更改。

> **注意：**
>
> 默认情况下，Web Studio 和 Director 使用端口 443 进行安全的 HTTPS 访问。如果需要，您可以更改端口号。有关详细信息，请参阅 更改默认端口号。

要将证书绑定到端口 `443`，请按照以下步骤操作：

1. 以管理员身份登录服务器。
2. 打开 IIS 管理器，然后导航到 **站点 > 默认网站 > 绑定**。
3. 如果存在类型为 **https** 的现有绑定，请选择它并单击 **编辑...**。如果没有 **https** 绑定，请单击 **添加**。



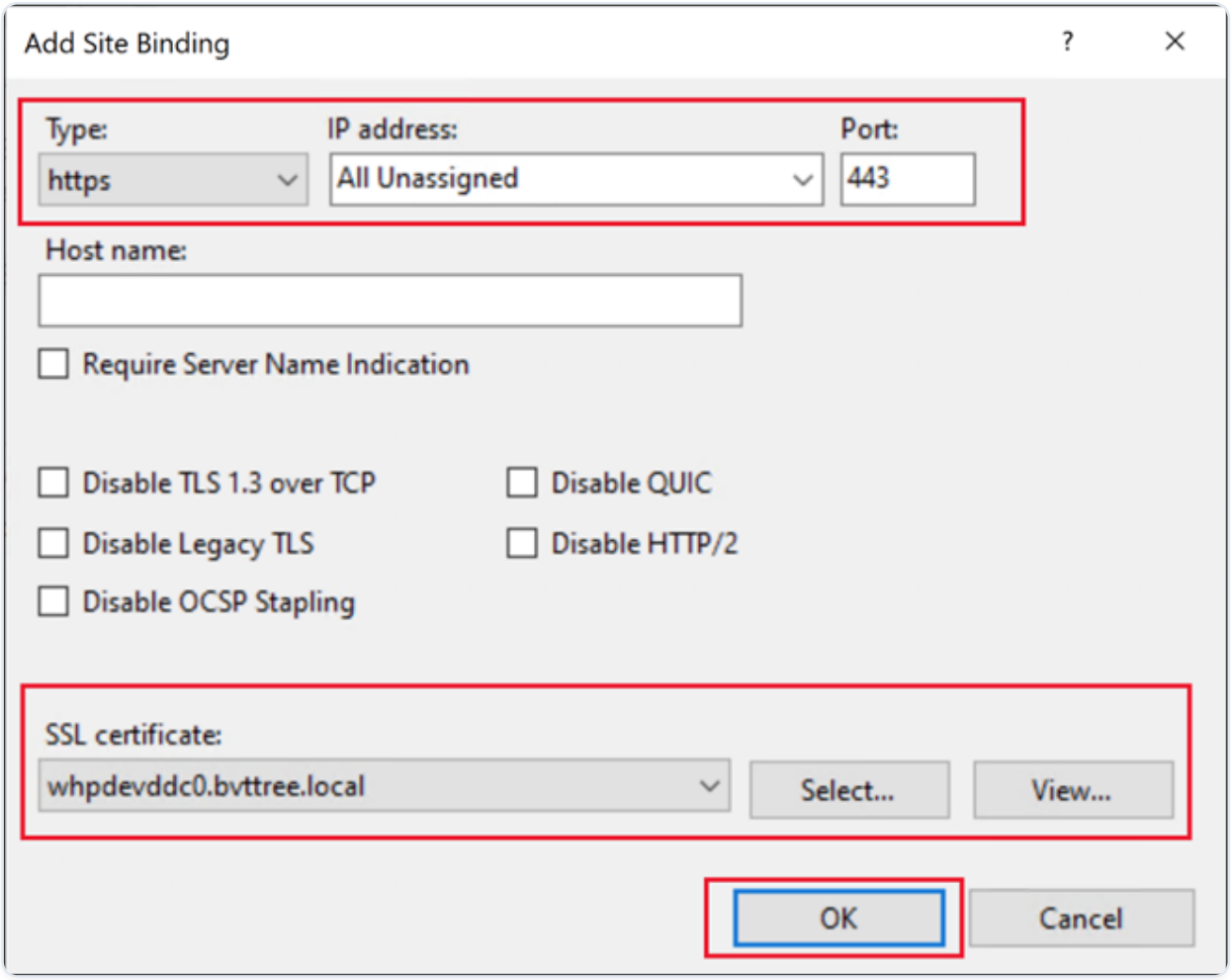
4. 创建或编辑站点绑定：

   a. 对于新绑定，将类型设置为 **https**，端口设置为 `443`。

b. 选择相应的 SSL 证书。

c. 在 Windows Server 2022 或更高版本上，可以选择 **禁用旧版 TLS**，以确保用户只能使用现代 TLS 版本进行连接。

d. 单击**确定**。



或者，您可以使用 PowerShell 更改证书。例如，以下脚本会查找具有给定公用名的证书，并将其绑定到所有 IP 地址、端口 443，并禁用旧版 TLS 版本。

```
$certSName = 'CN=whpdevddc0.bvttree.local'  # The subject name of the
certificate

$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {$_.Subject
-eq $certSName}

netsh http add sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint) certstorename=My appid="{91fe7386-e0c2-471b-
a252-1e0a805febac}" disablelegacytls=enable
```

请注意，`appid` 是一个任意 GUID，可用于标识是哪个应用程序添加了证书。

使用自签名证书

您可以使用现有的自签名证书，但不建议这样做，因为它需要手动配置访问服务器的每台计算机。

要在需要连接到 Web Studio 的计算机上安装自签名证书，请执行以下操作：

1. 从 Web Studio 和 Delivery Controller 服务器导出 现有的自签名证书。
2. 将证书导入 到必须访问服务器的计算机的**受信任的根证书**存储中。

（可选）启用 HTTP 严格传输安全 (HSTS)

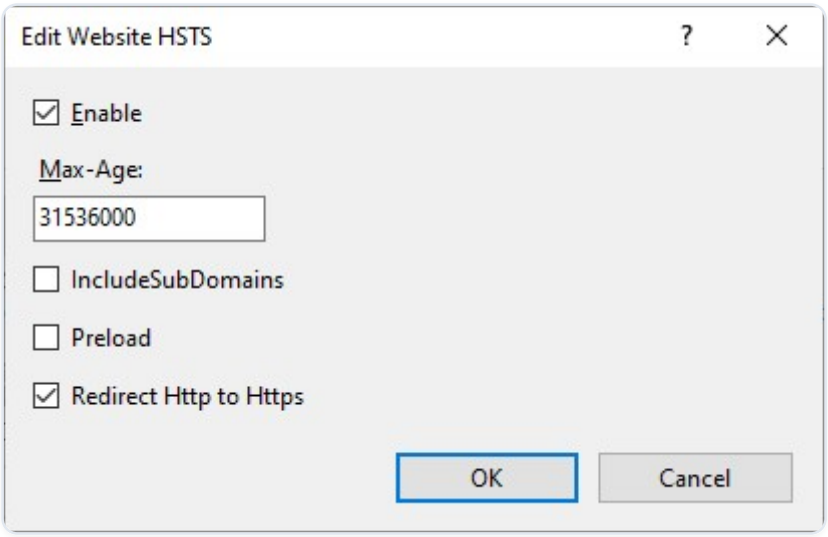
HTTP 严格传输安全 (HSTS) 告知 Web 浏览器在访问站点时仅使用 HTTPS。如果用户尝试使用 HTTP 访问 URL，浏览器会自动切换到 HTTPS。此设置可确保客户端和服务器端的安全连接验证。浏览器会在配置的期限内保持此验证。

在 Windows Server 2019 及更高版本上，您可以在 IIS 中配置 HSTS：

1. 打开 **Internet Information Services (IIS) 管理器**。
2. 选择**默认网站**（或相应的网站）。
3. 在右侧的**操作**窗格中，选择 **HSTS...**。
4. 选择**启用**并输入最大期限，例如一年为 31536000。
5. 选择**将 Http 重定向到 Https**。

> **注意：**
>
> 访问 Studio 网站时，Web Studio 会自动配置**URL 重写**规则以将 HTTP 重定向到 HTTPS。但是，此选项也适用于 Director 和 IIS 站点上的任何其他应用程序。

6. 单击 **确定**。



(可选) 更改默认端口号

默认情况下，Web Studio 和 Director 使用端口 443 进行安全的 HTTPS 访问。要更改此端口号，请按照以下步骤在 `Default Web Site` 上为所需端口创建站点绑定。

步骤：

1. 在托管 Web Studio 的服务器上，打开 **Internet Information Services (IIS) Manager**。
2. 在 **Connections** 窗格中，展开服务器节点，然后在 **Sites** 下选择 **Default Web Site**。
3. 在右侧的 **Actions** 窗格中，单击 **Bindings**。
4. 在 **Site Bindings** 窗口中，单击 **Add**。
5. 在 Add Site Binding 窗口中，为新绑定设置以下内容：
   a. **Type**：选择 **https**。
   b. **IP address**：选择适当的 IP 地址，如果适用，则保留为 All Unassigned。
   c. **Port**：输入所需的端口号（例如，444）。
   d. **SSL certificate**：选择用于安全通信的相应 SSL 证书。

> **注意：**
>
> 如果 Delivery Controller™ 和 Web Studio 安装在不同的计算机上，并且服务器没有部署其他服务或网站，则可以删除端口 443。否则，请保留此端口以避免与 Orchestration 服务和其他 FMA 服务发生通信问题。

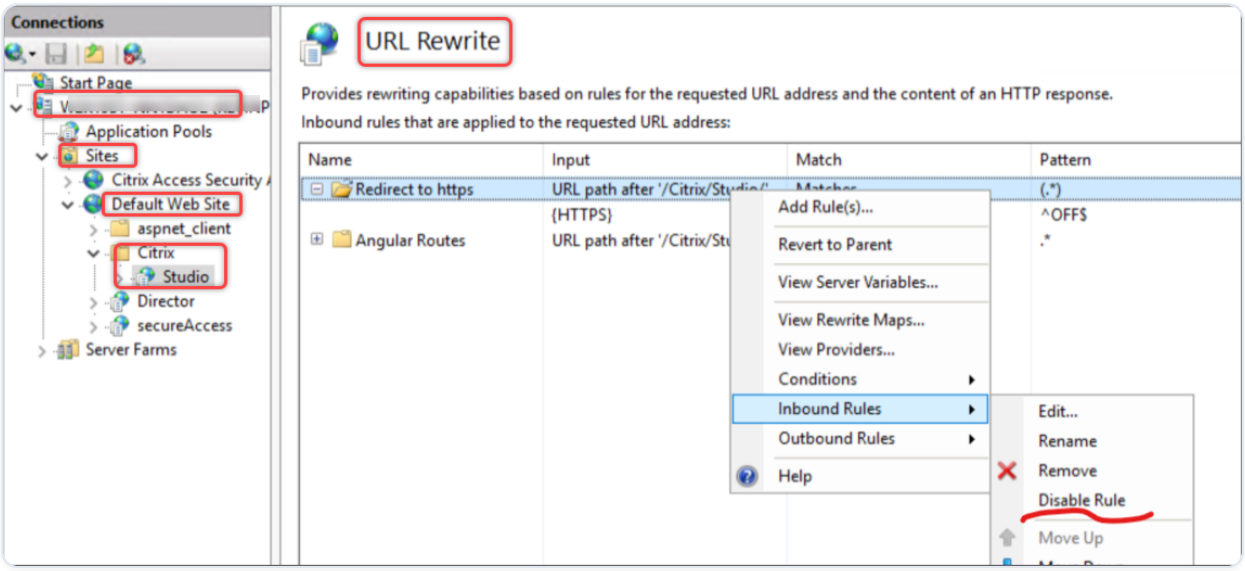
6. 单击 **OK** 保存绑定，然后关闭 **Site Bindings** 窗口。

7. 在 **IIS 管理器**中，单击服务器节点，然后在**操作**窗格中，单击**重新启动**以应用新绑定。

(可选) 禁用 HTTPS 重定向

安装 Web Studio 时，默认情况下，任何 HTTP 访问都会自动重定向到 HTTPS。可以禁用此重定向以允许 HTTP 访问。仅当您已采取其他措施阻止 HTTP 访问时，才建议采用此方法。如果您在 Web Studio 前面有一个 TLS 终止负载平衡器，仍然建议在负载平衡器和 Web Studio 之间使用 HTTPS。

1. 登录到 Web Studio 服务器。
2. 打开 **Internet 信息服务 (IIS) 管理器**，并导航到 *Server_name* **> 站点 > 默认网站 > URL 重写**。
3. 禁用**入站规则**中的**重定向到 https**，如下图所示。



如果您已在 IIS 中启用 HSTS，则还必须清除**将 Http 重定向到 Https**。

在 VDA 上启用 TLS / DTLS

通过完成以下任务，在 Citrix Workspace™ 应用程序和 Virtual Delivery Agent (VDA) 之间启用 TLS 连接：

- 在 VDA 上安装证书。有关详细信息，请参阅 (#requesting-and-installing-a-certificate)
- 在安装了 VDA 的计算机上配置 TLS。（为方便起见，以后凡提及安装了 VDA 的计算机，均简称为“VDA”。）强烈建议您使用 Citrix 提供的 PowerShell 脚本来配置 TLS/DTLS。有关详细信息，请参阅 (#configure-tls-on-a-vda-using-the-powershell-script)。但是，如果您想手动配置 TLS/DTLS，请参阅 (#manually-configure-tls-on-a-vda)。
- 通过在 Studio 中运行一组 PowerShell cmdlet，在包含 VDA 的交付组中配置 TLS。有关详细信息，请参阅 (#configure-tls-on-delivery-groups)。

要求和注意事项：

- 在安装组件、创建站点、创建计算机目录和创建交付组之后，在交付组和 VDA 上配置 TLS。
- 要在交付组中配置 TLS，您必须具有更改 Controller 访问规则的权限。完全管理员拥有此权限。
- 要在 VDA 上配置 TLS，您必须是安装 VDA 的计算机上的 Windows 管理员。
- 在由 Machine Creation Services™ 或 Provisioning Services 预配的池化 VDA 上，VDA 计算机映像会在重新启动时重置，导致以前的 TLS 设置丢失。每次 VDA 重新启动时运行 PowerShell 脚本以重新配置 TLS 设置。

交付组不能混合配置了 TLS 的 VDA 和未配置 TLS 的 VDA。在为交付组配置 TLS 之前，请确保已为该交付组中的所有 VDA 配置了 TLS。

在 VDA 上配置 TLS 时，已安装的 TLS 证书的权限会发生更改，从而授予 ICA® Service 对证书私钥的读取访问权限，并通知 ICA Service 以下信息：

- 证书存储中用于 TLS 的证书。
- 用于 TLS 连接的 TCP 端口号。

  必须配置 Windows 防火墙（如果已启用）以允许在此 TCP 端口上进行入站连接。当您使用 PowerShell 脚本时，此配置会自动完成。
- 允许的 TLS 协议版本。

  > **重要提示：**
  >
  > Citrix 建议使用 TLS 1.2 或更高版本。SSL 和旧版 TLS 已弃用。
  >
  > 支持的 TLS 协议版本遵循以下层次结构（从低到高）：SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2 和 TLS 1.3。指定允许的最低版本；使用该版本或更高版本的所有协议连接都将被允许。

  例如，如果将 TLS 1.1 指定为最低版本，则允许 TLS 1.1、TLS 1.2 和 TLS 1.3 协议连接。如果将 SSL 3.0 指定为最低版本，则允许所有受支持版本的连接。如果将 TLS 1.3 指定为最低版本，则只允许 TLS 1.3 连接。
- 允许的 TLS 密码套件。

  密码套件选择用于连接的加密。客户端和 VDA 可以支持不同的密码套件集。当客户端 (Citrix Workspace app) 连接并发送受支持的 TLS 密码套件列表时，VDA 会将客户端的密码套件之一与其自身配置的密码套件列表中的一个密码套件进行匹配，并接受连接。如果没有匹配的密码套件，VDA 将拒绝连接。

VDA 支持三组密码套件（也称为合规模式）：GOV（政府）、COM（商业）和 ALL。可接受的密码套件还取决于 Windows FIPS 模式；有关 Windows FIPS 模式的信息，请参阅 `<http://support.microsoft.com/kb/811833>`。下表列出了每组中的密码套件：

密码套件	ALL	COM	GOV	ALL	COM	GOV
FIPS 模式	关闭	关闭	关闭	开	开	开
TLS_AES_256_GCM_SHA384	X		X	X		X
TLS_AES_128_GCM_SHA256	X			X		X
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

注意：

> VDA 不支持 DHE 密码套件（例如，TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CBC_SHA、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 和 TLS_DHE_RSA_WITH_AES_128_CBC_SHA）。如果由 Windows 选择，连接将失败。

> 如果您使用的是 NetScaler Gateway，请参阅 NetScaler 文档，了解有关后端通信的密码套件支持信息。有关 TLS 密码套件支持的信息，请参阅 Citrix ADC 设备上可用的密码。有关 DTLS 密码套件支持的信息，请参阅 DTLS 密码支持。

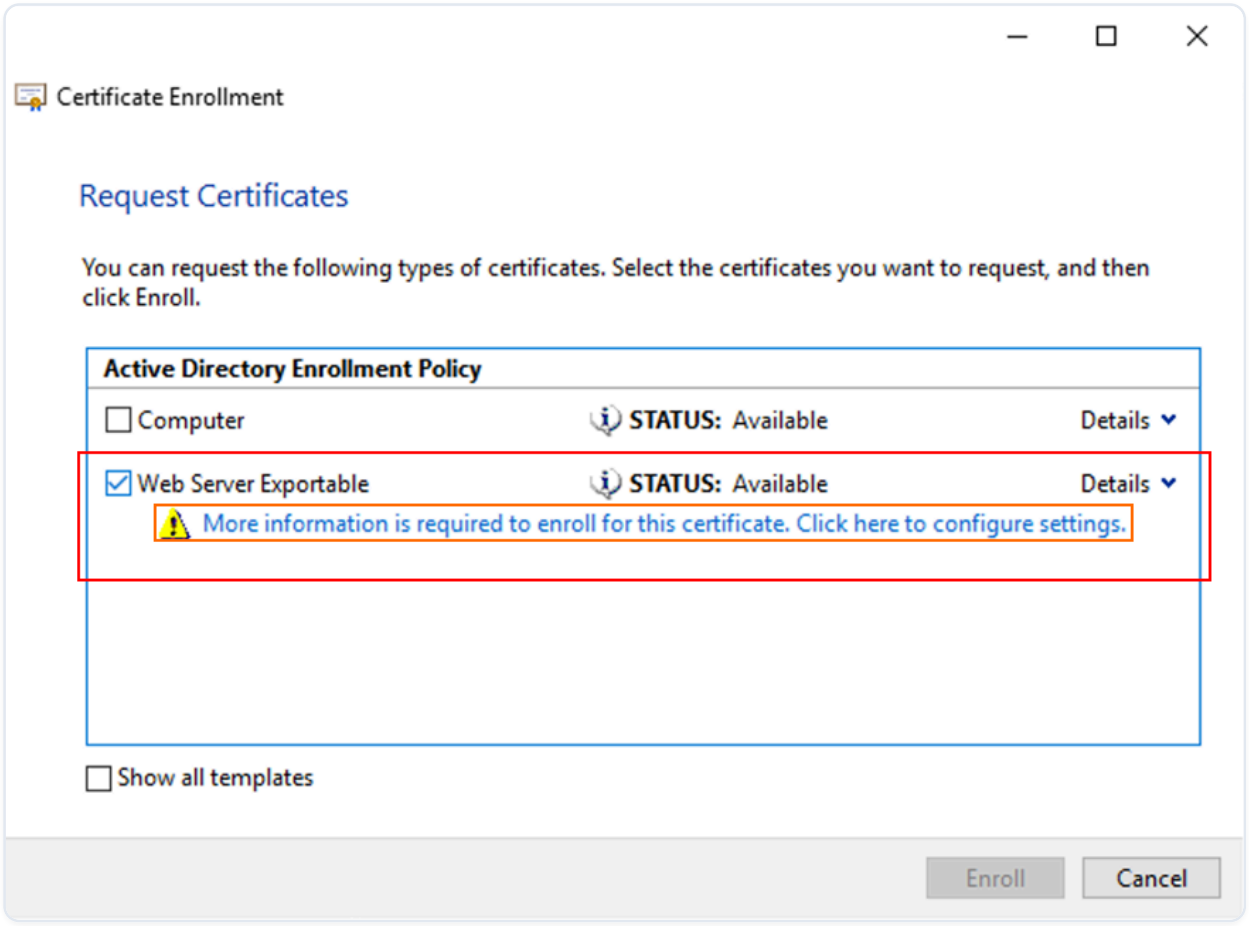
请求和安装证书

要使用 TLS，您必须安装一个其备用名称包含 VDA FQDN 的证书。该证书必须受直接连接到 VDA（而非通过 Citrix Gateway）的任何客户端信任。要允许无法轻松部署证书的非托管设备连接到 VDA，请考虑部署 NetScaler® Gateway。

使用 Microsoft 证书颁发机构创建证书

如果您的客户端和 VDA 位于受信任的林中，并且该林具有 Microsoft 证书颁发机构，则可以从“证书”MMC 管理单元的“证书注册向导”中获取证书。

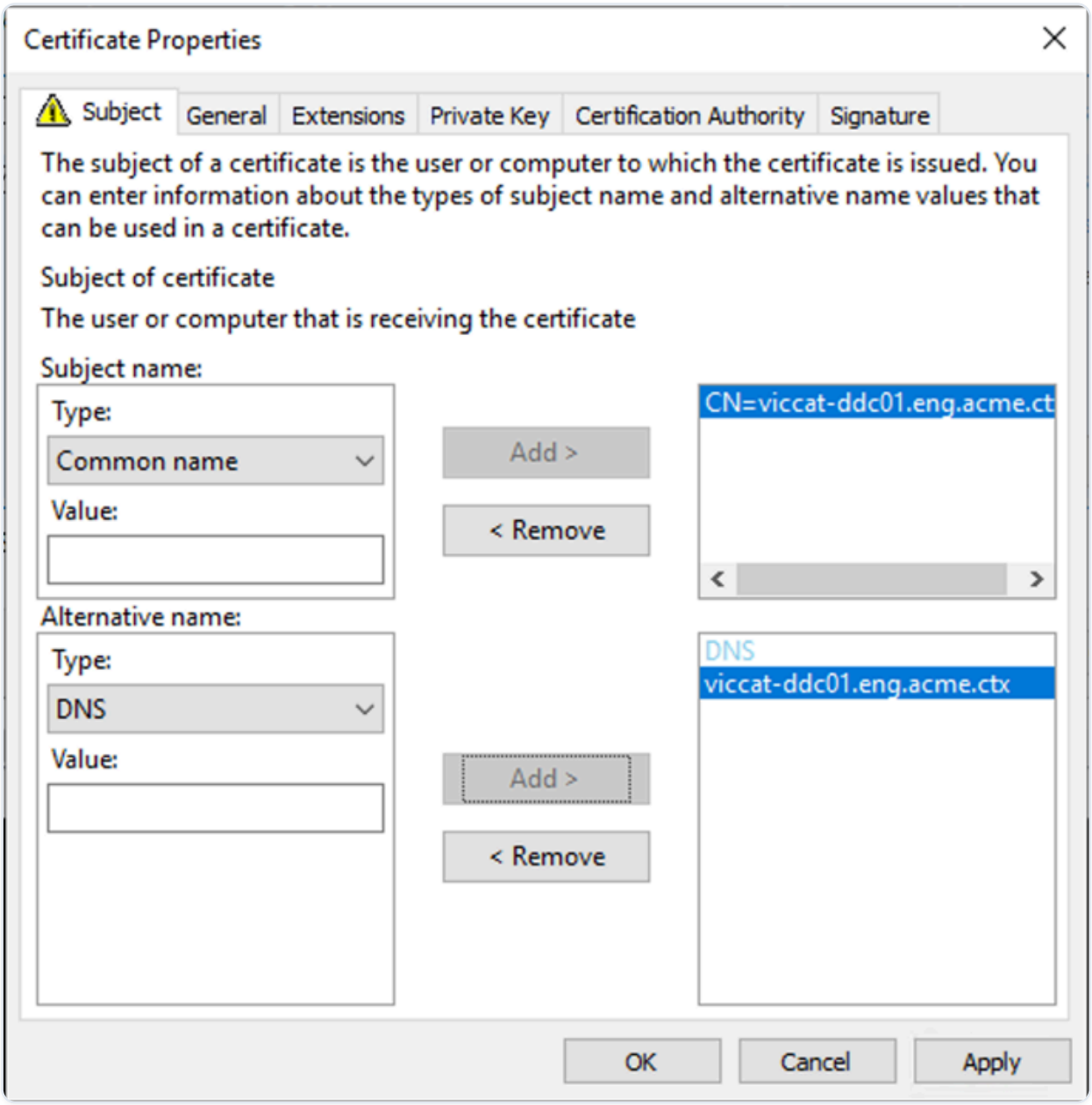
1. 在 VDA 上，打开 MMC 控制台并添加“证书”管理单元。出现提示时，选择“计算机帐户”。
2. 展开 **个人 > 证书**，然后使用上下文菜单命令 **所有任务 > 请求新证书**。
3. 单击“**下一步**”开始，然后单击“**下一步**”确认您正在从 Active Directory 注册获取证书。
4. 选择服务器身份验证证书的模板。默认的 Windows **计算机** 或 **Web 服务器可导出** 均可接受。如果模板已设置为自动提供主题的值，则无需提供更多详细信息即可单击 **注册**。



5. 要为证书模板提供更多详细信息，请单击 **详细信息** 并配置以下内容：

   主题名称 — 选择类型 **公用名** 并添加 VDA 的 FQDN

   备用名称 — 选择类型 **DNS** 并添加 VDA 的 FQDN



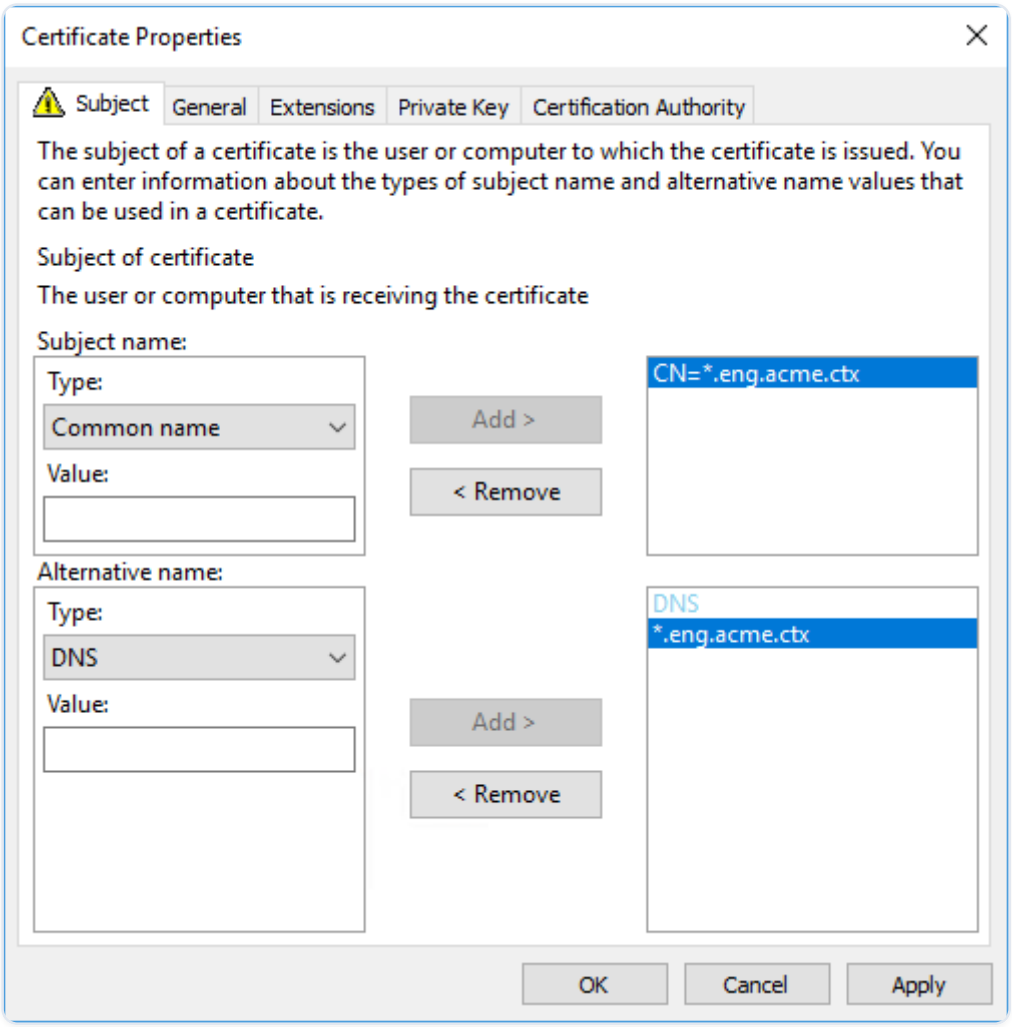
注意：

使用 Active Directory 证书服务证书自动注册来自动向 VDA 颁发和部署证书。这在 (#enable-certificate-auto-enrollment) 中有所描述。

您可以使用通配符证书来允许单个证书保护多个 VDA：

主题名称 — 选择类型 **通用名称** 并输入 VDA 的 *.primary.domain

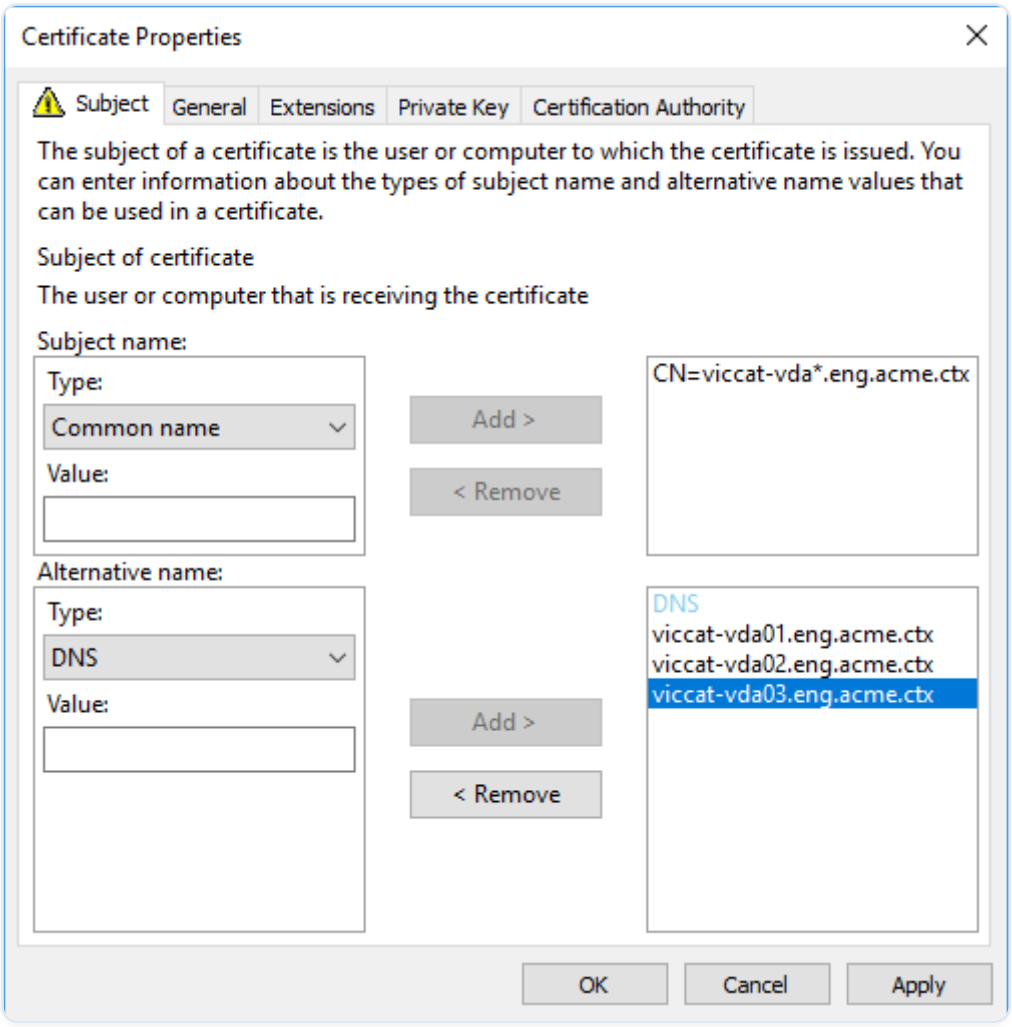
备用名称 — 选择类型 **DNS** 并添加 VDA 的 *.primary.domain



您可以使用 SAN 证书来允许单个证书保护多个特定的 VDA：

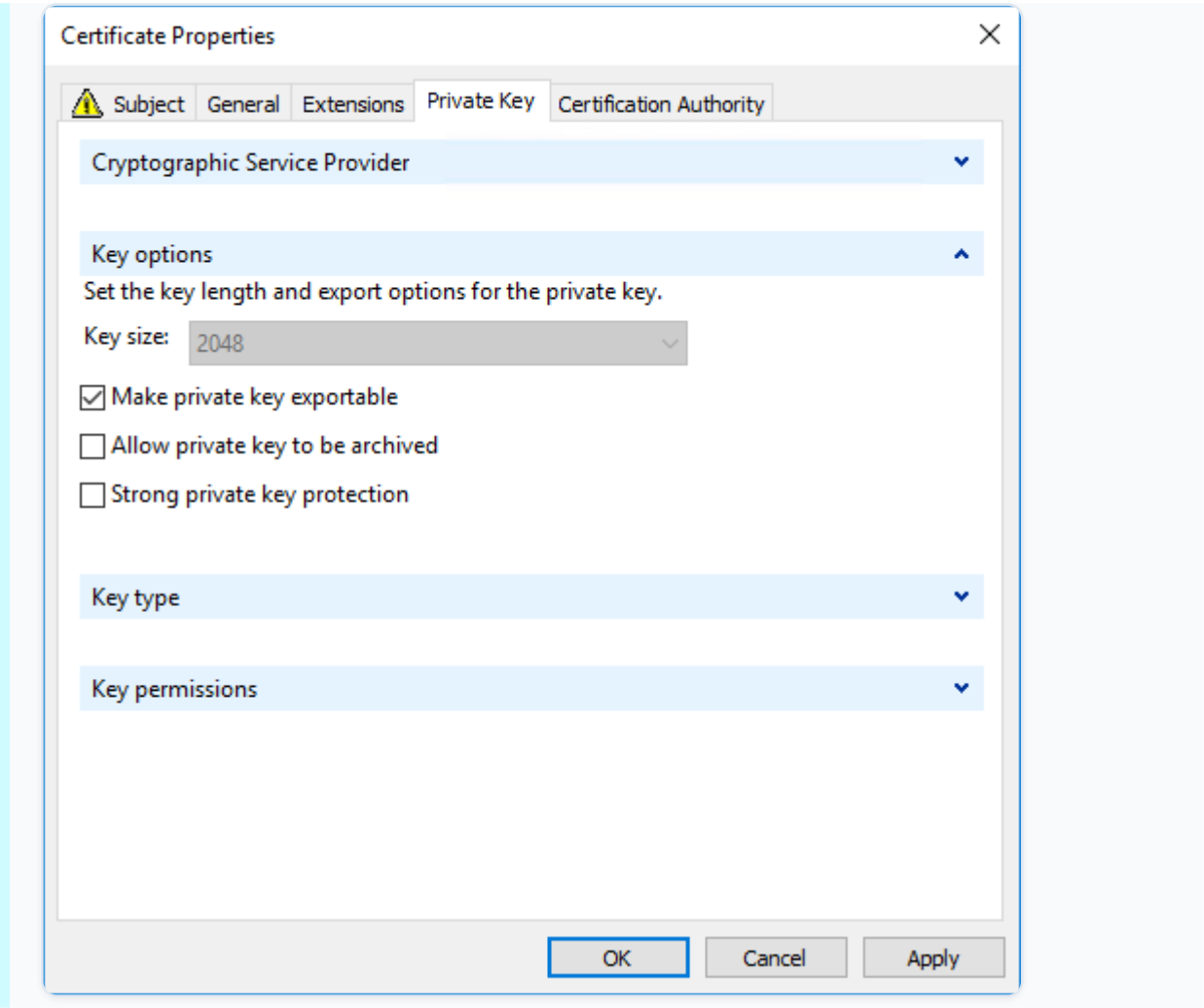
主题名称 — 选择类型 **通用名称** 并输入一个字符串以帮助识别证书用途

备用名称 — 选择类型 **DNS** 并为每个 VDA 的 FQDN 添加一个条目。将备用名称的数量保持在最低限度，以确保最佳的 TLS 协商。



注意：

通配符证书和 SAN 证书都要求在“私钥”选项卡上选择 **允许导出私钥**：



使用 PowerShell 脚本在 VDA 上配置 TLS

将 TLS 证书安装在证书存储的“本地计算机”>“个人”>“证书”区域中。如果该位置存在多个证书，请向 PowerShell 脚本提供证书的指纹。

> **注意：**
>
> 从 XenApp and XenDesktop 7.15 LTSR 开始，PowerShell 脚本会根据 VDA 的 FQDN 查找正确的证书。当 VDA FQDN 只有一个证书时，您无需提供指纹。

> Enable-VdaSSL.ps1 脚本用于在 VDA 上启用或禁用 TLS 侦听器。此脚本位于安装介质的 *Support* > *Tools* > *SslSupport* 文件夹中。

启用 TLS 时，DHE 密码套件将被禁用。ECDHE 密码套件不受影响。

启用 TLS 时，脚本会禁用指定 TCP 端口的所有现有 Windows 防火墙规则。然后，它会添加一条新规则，允许 ICA 服务仅在 TLS TCP 和 UDP 端口上接受传入连接。它还会禁用以下 Windows 防火墙规则：

- Citrix ICA（默认值：1494）
- Citrix CGP（默认值：2598）
- Citrix WebSocket（默认值：8008）

结果是用户只能使用 TLS 或 DTLS 进行连接。如果没有 TLS 或 DTLS，他们将无法使用 ICA/HDX、带有会话可靠性的 ICA/HDX 或通过 WebSocket 的 HDX。

> **注意：**
>
> DTLS 不支持通过 UDP 实时传输的 ICA/HDX 音频，也不支持 ICA/HDX Framehawk。
>
> 请参阅网络端口。

该脚本包含以下语法说明以及其他示例；您可以使用 Notepad++ 等工具查看此信息。

> **重要提示：**
>
> 指定 Enable 或 Disable 参数以及 CertificateThumbPrint 参数。其他参数是可选的。

语法

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]
```

参数	描述
启用	在 VDA 上安装并启用 TLS 侦听器。此参数或 Disable 参数是必需的。
禁用	禁用 VDA 上的 TLS 侦听器。此参数或 Enable 参数是必需的。如果指定此参数，则其他参数无效。

参数	描述
证书指纹 "<thumbprint>"	证书存储中 TLS 证书的指纹，用引号引起来。脚本使用指定的指纹选择要使用的证书。如果省略此参数，则会选择不正确的证书。
SSL端口 <port>	TLS 端口。默认值：443
SSL最低版本 "<version>"	最低 TLS 协议版本，用引号括起来。有效值：`SSL_3.0`、`TLS_1.0`（默认）、`TLS_1.1`、`TLS_1.2` 和 `TLS_1.3`。`TLS_1.3` 需要 Windows 11 或 Windows Server 2022 或更高版本。
SSL密码套件 "<suite>"	TLS 密码套件，用引号引起来。有效值：“GOV”、“COM”和“ALL”（默认）。

示例

以下脚本安装并启用 TLS 协议版本值。指纹（在此示例中表示为“12345678987654321”）用于选择要使用的证书。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

以下脚本安装并启用 TLS 侦听器，并指定 TLS 端口 400、GOV 密码套件和最低 TLS 1.2 协议值。指纹（在此示例中表示为“12345678987654321”）用于选择要使用的证书。

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.2"

-SSLCipherSuite "All"
```

以下脚本禁用 VDA 上的 TLS 侦听器。

```
Enable-VdaSSL -Disable
```

在 VDA 上手动配置 TLS

在 VDA 上手动配置 TLS 时，您需要为每个 VDA 上的相应服务授予 TLS 证书私钥的通用读取权限：对于适用于 Windows 单会话操作系统的 VDA，为 NT SERVICE\PorticaService；对于适用于 Windows 多会话操作系统的 VDA，为 NT SERVICE\TermService。在安装 VDA 的计算机上：

步骤 1。启动 Microsoft 管理控制台 (MMC)：开始 > 运行 > mmc.exe。

步骤 2。将“证书”管理单元添加到 MMC：

1. 选择“文件”>“添加/删除管理单元”。
2. 选择“证书”，然后单击“添加”。
3. 当系统提示“此管理单元将始终管理以下对象的证书:”时，选择“计算机帐户”，然后单击“下一步”。
4. 当系统提示“选择此管理单元要管理的计算机”时，选择“本地计算机”，然后单击“完成”。

步骤 3。在“证书 (本地计算机)”>“个人”>“证书”下，右键单击证书，然后选择“所有任务”>“管理私钥”。

步骤 4。访问控制列表编辑器显示“（友好名称）私钥的权限”，其中（友好名称）是您的 TLS 证书的名称。添加以下服务之一并为其授予“读取”访问权限：

- 对于 Windows 单会话操作系统 VDA，“PORTICASERVICE”
- 对于 Windows 多会话操作系统 VDA，“TERMSERVICE”

步骤 5。双击已安装的 TLS 证书。在证书对话框中，选择“详细信息”选项卡，然后滚动到底部。单击“指纹”。

步骤 6。运行 regedit 并转到 HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd。

1. 编辑 SSL Thumbprint 密钥，并将 TLS 证书指纹的值复制到此二进制值中。您可以安全地忽略“编辑二进制值”对话框中的未知项（例如“0000”和特殊字符）。
2. 编辑 SSLEnabled 密钥并将 DWORD 值更改为 1。（要稍后禁用 SSL，请将 DWORD 值更改为 0。）
3. 如果要更改默认设置（可选），请在同一注册表路径中使用以下内容：

   SSLPort DWORD – SSL 端口号。默认值：443。

   SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2, 5 = TLS 1.3。默认值：2 (TLS 1.0)。

SSLCipherSuite DWORD – 1 = GOV，2 = COM，3 = ALL。默认值：3 (ALL)。

步骤 7. 如果 TLS TCP 和 UDP 端口不是默认的 443，请确保它们在 Windows 防火墙中处于打开状态。（在 Windows 防火墙中创建入站规则时，请确保其属性中选中了“允许连接”和“已启用”条目。）

步骤 8. 确保没有其他应用程序或服务（例如 IIS）正在使用 TLS TCP 端口。

步骤 9. 对于多会话 VDA，请重新启动计算机以使更改生效。（您无需重新启动单会话 VDA 计算机。）

步骤 10. 修改 Windows 密码套件首选项，使 VDA 支持的密码套件具有最高优先级，以避免连接问题。

> **重要提示：**
>
> 下面概述的组策略更改仅在系统重新启动后生效。
>
> 如果您使用的是通过 MCS 或 PVS 预配的非持久性会话主机，则必须在主映像中应用这些设置。
>
> 选项 1：

使用组策略编辑器，转到“计算机配置”>“策略”>“管理模板”>“网络”>“SSL 配置设置”>“SSL 密码套件顺序”。确保以下密码套件位于列表顶部：

```
TLS_AES_256_GCM_SHA384_P384

TLS_AES_256_GCM_SHA384_P256

TLS_AES_128_GCM_SHA256_P384

TLS_AES_128_GCM_SHA256_P256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
```

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

注意：

TLS_AES_256_GCM_SHA384 和 TLS_AES_128_GCM_SHA256 仅适用于 Windows 11 和 Windows Server 2022 或更高版本。如果您使用的是较旧的操作系统，请不要在列表中包含这些密码套件。

请注意，列出的密码套件还指定了椭圆曲线 P384 或 P256，以确保不选择“curve25519”。FIPS 模式不会阻止使用“curve25519”。

无需从列表中删除任何密码套件。请注意，这些设置适用于整个系统，因此如果您决定删除任何密码套件，则必须确保您的会话主机上运行的任何应用程序或服务都不需要它们。

选项 2：

使用组策略编辑器，转到“计算机配置”>“策略”>“管理模板”>“网络”>“SSL 配置设置”>“SSL 密码套件顺序”。确保以下密码套件位于列表顶部：

```
TLS_AES_256_GCM_SHA384

TLS_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

注意：

TLS_AES_256_GCM_SHA384 和 TLS_AES_128_GCM_SHA256 仅适用于 Windows 11 和 Windows Server 2022 或更高版本。如果您使用的是较旧的操作系统，请不要在列表中包含这些密码套件。

无需从列表中删除任何密码套件。请注意，这些设置适用于整个系统，因此如果您决定删除任何密码套件，则必须确保您的会话主机上运行的任何应用程序或服务都不需要它们。

使用组策略编辑器，转到“计算机配置”>“策略”>“管理模板”>“网络”>“SSL 配置设置”>“ECC 曲线顺序”。启用该设置并在列表中包含以下曲线：

```
NistP384

NistP256
```

注意：

这可确保不选择“curve25519”。FIPS 模式不会阻止使用“curve25519”。

VDA 仅在以下两个列表中都出现时才选择密码套件：组策略列表和所选合规模式（COM、GOV 或 ALL）的列表。密码套件还必须出现在客户端 (Citrix Workspace app) 发送的列表中。

在交付组上配置 TLS

对于包含已配置为 TLS 连接的 VDA 的每个交付组，请完成此过程。

1. 从 Studio 打开 PowerShell 控制台。
2. 运行 **Get-BrokerAccessPolicyRule -DesktopGroupName '\<*delivery-group-name*>' \| Set-BrokerAccessPolicyRule -HdxSslEnabled $true**。
3. 运行 **Set-BrokerSite -DnsResolutionEnabled $true**。

使用自动注册为池化 VDA 启用 SSL

使用池化 VDA 时，如果将证书添加到主映像，则所有 VDA 共享同一映像。您可以使用通配符证书，但缺点是，如果任何一个 VDA 受到威胁，此功能强大的证书将意味着所有 VDA 的 HDX™ 连接都将面临风险。

相反，一种安全的替代方法是利用 Microsoft Active Directory 证书服务通过组策略自动预配证书。您可以在 VDA 上使用启动脚本来动态预配新证书并为 VDA 启用 SSL。

请注意，此方法仅适用于单会话桌面 VDA。对于多会话 VDA，ICA 侦听器在启动过程中过早启动，无法自动预配证书。

由于 Active Directory 证书服务使用内部企业证书颁发机构，因此并非所有 Windows 安装都会自动信任它。如果客户端由公司管理并且是域林的一部分，则可以使用组策略自动分发受信任的 CA 证书。对于 BYOD 和其他未加入域的设备，您需要通过其他机制（例如提供下载链接）将受信任的 CA 证书分发给用户，或者使用 NetScaler 网关。

启用证书自动注册

首先，请确保在 VDA 域林中的服务器上安装了 Active Directory 证书服务角色，并提供企业 CA，否则将无法进行自动注册。

请注意，这可能会给您的企业 CA 带来比平时更高的负载，因为 VDA 将在每次启动时提交证书请求。请务必在 CA 服务器上分配足够的 CPU 和内存以应对负载，并一如既往地在投入生产之前在实验室环境中测试部署的可伸缩性。

在组策略管理编辑器中，创建一项新策略，该策略适用于将包含已启用 SSL 的池化 VDA 的组织单位，如下所示：

1. 展开“计算机配置”->“策略”->“Windows 设置”->“安全设置”->“公钥策略”
2. 编辑“证书服务客户端 – 自动注册策略”对象属性
3. 按照以下屏幕截图所示进行配置。
4. 右键单击“自动证书请求”容器，然后选择“新建”->“自动证书请求...”.
5. 在“自动证书请求设置向导”中，单击“下一步”
6. 确保已选择“计算机”证书模板，然后单击“下一步”
7. 单击“完成”

注册策略的屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/ssltask-autoenrollment-policy.png)

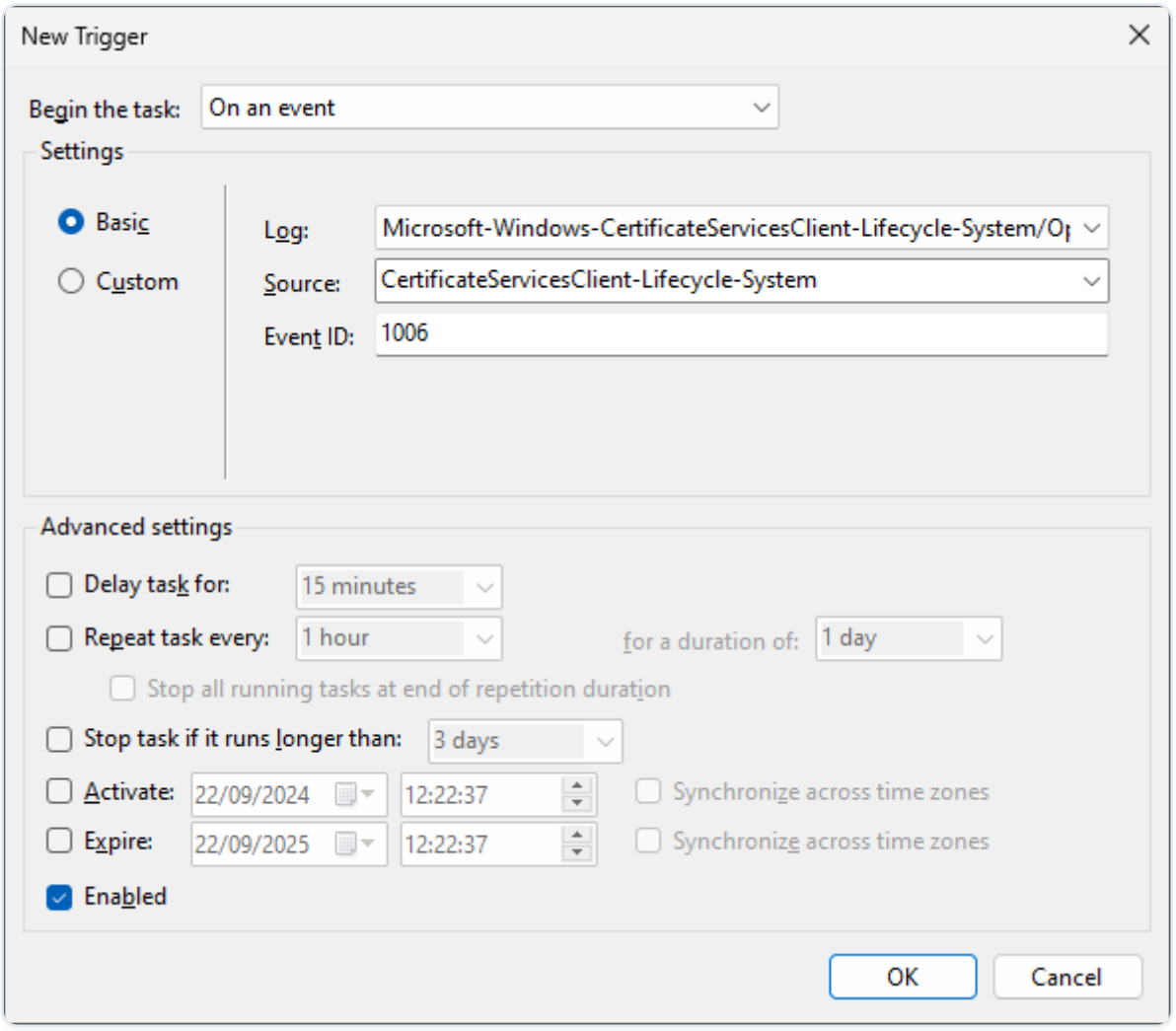
准备 Windows 主映像

将产品安装介质 `Support\Tools\SslSupport` 文件夹中的 Enable-VdaSsl.ps1 脚本复制到 VDA 主映像。请注意，主映像不应包含任何用于 HDX SSL 连接的证书。证书将在创建 MCS 或 PVS 计算机目录时进行预配。现在，按如下方式创建新的计划任务（暂时不要运行该计划任务）：

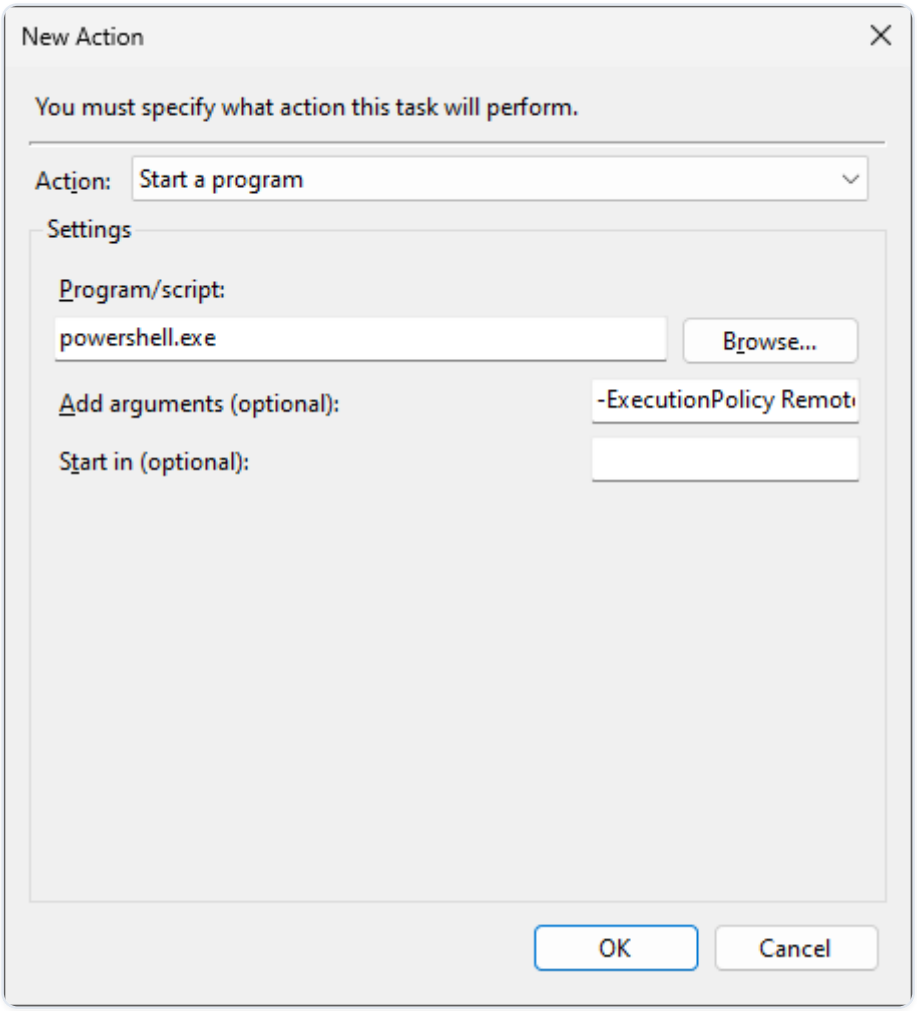
1. 打开“任务计划程序”。

2. 在“**操作**”窗格中，按“**创建任务...**”.
3. 在“常规”选项卡上：
   - 输入一个“**名称**”，例如 `Enable VDA SSL`
   - 单击“**更改用户或组...**”，然后在“选择用户或组”对话框中输入 `SYSTEM` 并单击“**确定**”

   创建任务“操作”选项卡的屏幕截图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/ssltask-general.png)
4. 选择“触发器”选项卡
5. 单击“**新建...**”。在“**新建触发器**”对话框中：
   a. 将 **开始任务** 设置为 **在事件发生时**
   b. 将 **日志** 设置为 **Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational**
   c. 将 **源** 设置为 **微软-Windows-证书服务客户端-生命周期-系统**
   d. 将 **事件 ID** 设置为 `1006`
   e. 单击 **确定** 以保存触发器



6. 选择 **操作** 选项卡
7. 单击 **新建...**
8. 在 **新建操作** 对话框中：
    a. 将 **操作** 设置为 **启动程序**
    b. 在“程序/脚本”字段中，输入 `powershell.exe`
    c. 在“添加参数”字段中，输入 `-ExecutionPolicy RemoteSigned Enable-VdaSsl.ps1 -Enable -Confirm:$False`，包括 PowerShell 脚本的路径。
    d. 按 **确定** 以保存操作



9. 按 **确定** 以保存任务

故障排除

如果发生连接错误，请检查 VDA 上的系统事件日志。

使用适用于 Windows 的 Citrix Workspace 应用程序时，如果收到指示 TLS 错误的连接错误，请禁用 Desktop Viewer，然后尝试重新连接。尽管连接仍然失败，但可能会提供有关底层 TLS 问题的解释。（例如，在向证书颁发机构请求证书时指定了不正确的模板。）

大多数使用 HDX 自适应传输的配置都可以成功地与 DTLS 配合使用，包括使用最新版本的 Citrix Workspace 应用程序、Citrix Gateway 和 VDA 的配置。某些在 Citrix Workspace 应用程序和 Citrix Gateway 之间以及在 Citrix Gateway 和 VDA 之间使用 DTLS 的配置需要采取额外措施。

在以下情况下需要额外操作：

- Citrix Receiver 版本支持 HDX 自适应传输和 DTLS：适用于 Windows 的 Receiver (4.7, 4.8, 4.9)、适用于 Mac 的 Receiver (12.5, 12.6, 12.7)、适用于 iOS 的 Receiver (7.2, 7.3.x) 或适用于 Linux 的 Receiver (13.7)

并且以下任一情况也适用：

- Citrix Gateway 版本支持到 VDA 的 DTLS，但 VDA 版本不支持 DTLS（版本 7.15 或更早版本），
- VDA 版本支持 DTLS（版本 7.16 或更高版本），但 Citrix Gateway 版本不支持到 VDA 的 DTLS。

为避免 Citrix Receiver™ 连接失败，请执行以下操作之一：

- 将 Citrix Receiver 更新到适用于 Windows 的 Receiver 4.10 或更高版本、适用于 Mac 的 Receiver 12.8 或更高版本，或适用于 iOS 的 Receiver 7.5 或更高版本；或者，
- 将 Citrix Gateway 更新到支持到 VDA 的 DTLS 的版本；或者，
- 将 VDA 更新到 7.16 或更高版本；或者，
- 在 VDA 上禁用 DTLS；或者，
- 禁用 HDX 自适应传输。

> **注意：**
>
> 适用于 Linux 版 Receiver 的相应更新尚未推出。Android 版 Receiver（版本 3.12.3）不支持通过 Citrix Gateway 使用 HDX 自适应传输和 DTLS，因此不受影响。

> 要在 VDA 上禁用 DTLS，请修改 VDA 防火墙配置以禁用 UDP 端口 443。请参阅网络端口。

TLS 与 HTML5 视频重定向以及浏览器内容重定向

您可以使用 HTML5 视频重定向和浏览器内容重定向来重定向 HTTPS 网站。注入到这些网站中的 JavaScript 必须与在 VDA 上运行的 Citrix HDX HTML5 视频重定向服务建立 TLS 连接。为此，HTML5 视频重定向服务会在 VDA 上的证书存储中生成两个自定义证书。停止服务会删除这些证书。

HTML5 视频重定向策略默认处于禁用状态。

浏览器内容重定向默认处于启用状态。

有关 HTML5 视频重定向的详细信息，请参阅多媒体策略设置。

在通用打印服务器上启用 TLS

通用打印服务器支持虚拟投递代理 (VDA) 与通用打印服务器之间基于 TCP 的连接的传输层安全 (TLS) 协议。

> **警告：**
>
> 对于涉及 Windows 注册表操作的任务（例如编辑注册表），不正确地编辑注册表可能会导致严重问题，甚至可能需要重新安装操作系统。Citrix® 无法保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。编辑注册表之前，请务必备份注册表。

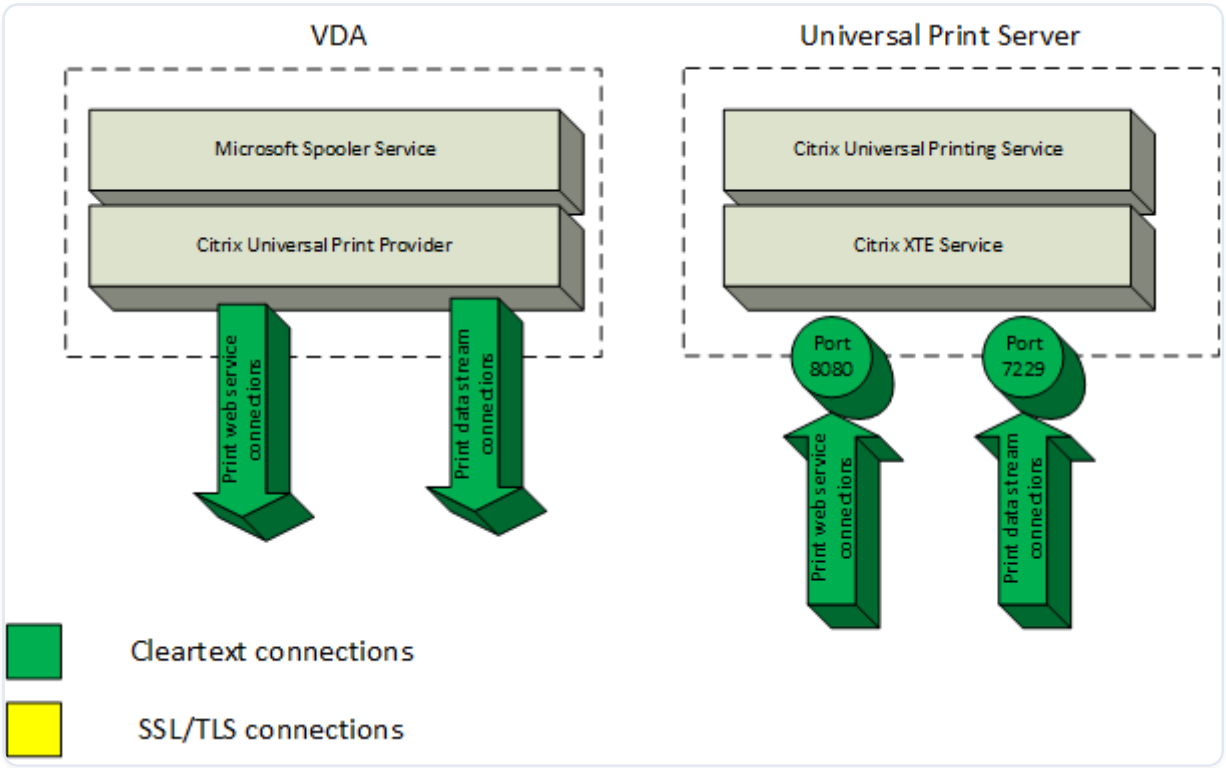
VDA 与通用打印服务器之间的打印连接类型

明文连接

以下与打印相关的连接源自 VDA，并连接到通用打印服务器上的端口。仅当 **SSL enabled** 策略设置为 **Disabled**（默认值）时，才会建立这些连接。

- 明文打印 Web 服务连接（TCP 端口 8080）
- 明文打印数据流 (CGP) 连接（TCP 端口 7229）

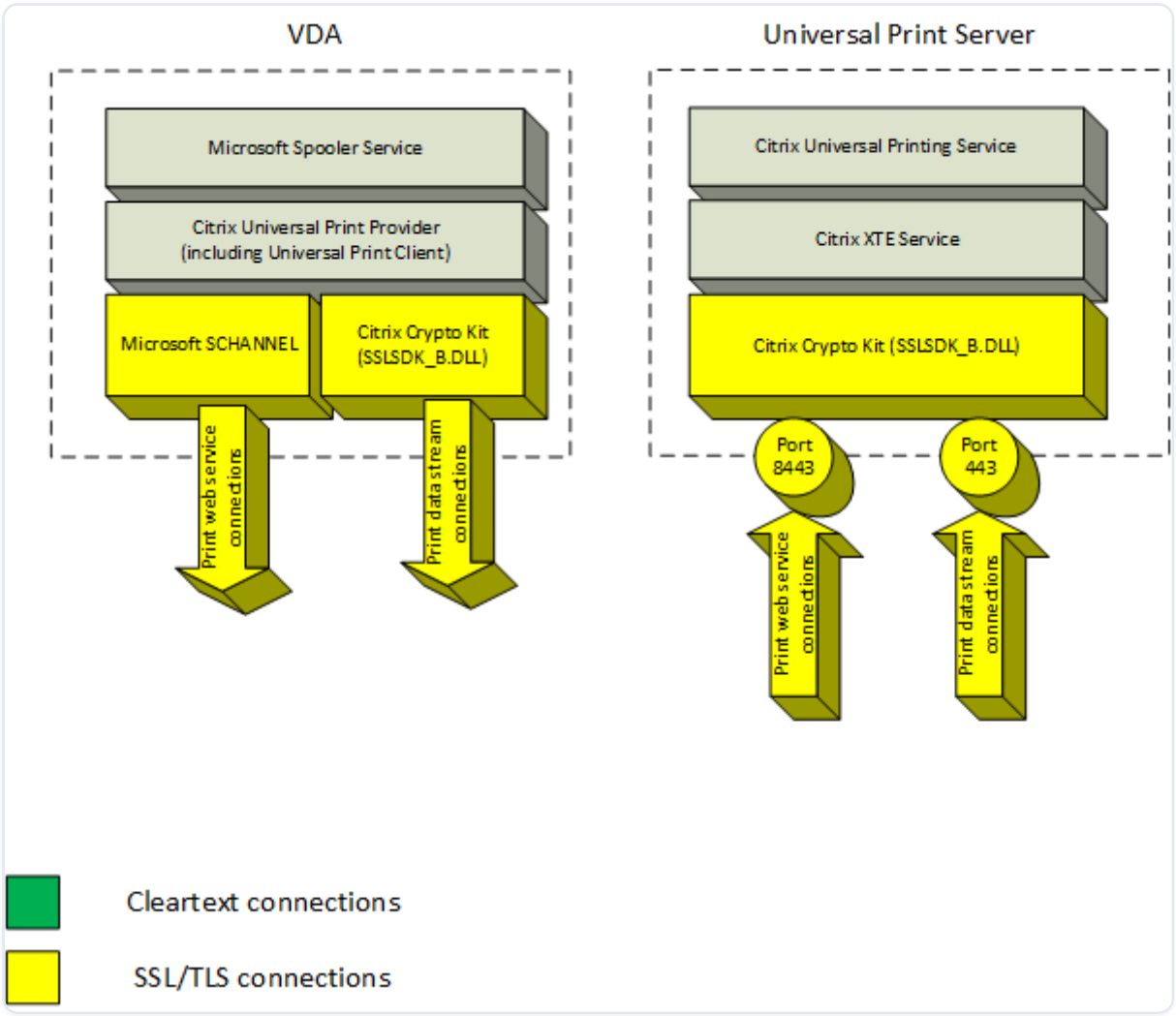
Microsoft 支持文章 Service overview and network port requirements for Windows 介绍了 Microsoft Windows 打印后台处理程序服务使用的端口。本文档中的 SSL/TLS 设置不适用于 Windows 打印后台处理程序服务建立的 NetBIOS 和 RPC 连接。如果 **Universal Print Server enable** 策略设置为 **Enabled with fallback to Windows' native remote printing**，则 VDA 会使用 Windows 网络打印提供程序 (win32spl.dll) 作为备用方案。



加密连接

这些与打印相关的 SSL/TLS 连接源自 VDA，并连接到通用打印服务器上的端口。仅当 **SSL enabled** 策略设置为 **Enabled** 时，才会建立这些连接。

- 加密打印 Web 服务连接（TCP 端口 8443）
- 加密打印数据流 (CGP) 连接（TCP 端口 443）



SSL/TLS 客户端配置

VDA 充当 SSL/TLS 客户端。

使用 Microsoft 组策略和注册表配置 Microsoft SCHANNEL SSP，以用于加密的打印 Web 服务连接（TCP 端口 8443）。Microsoft 支持文章 TLS 注册表设置 介绍了 Microsoft SCHANNEL SSP 的注册表设置。

在 VDA 上使用组策略编辑器，转到**计算机配置 > 管理模板 > 网络 > SSL 配置设置 > SSL 密码套件顺序**。当设置 TLS 1.3 时，选择以下顺序：

TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

当设置 TLS 1.2 时，选择以下顺序：

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **注意：**

> 配置此组策略设置后，VDA 仅当连接同时出现在以下两个 SSL 密码套件列表中时，才会为加密的打印 Web 服务连接（默认端口：8443）选择密码套件：

> - 组策略 SSL 密码套件顺序列表
> - 与所选 SSL 密码套件策略设置（COM、GOV 或 ALL）对应的列表

> 此组策略配置还会影响 VDA 上的其他 TLS 应用程序和服务。如果您的应用程序需要特定的密码套件，您可能需要将它们添加到此组策略密码套件顺序列表中。

> **重要提示：**

> TLS 配置的组策略更改仅在操作系统重新启动后生效。

> 使用 Citrix 策略配置加密打印数据流 (CGP) 连接（TCP 端口 443）的 SSL/TLS 设置。

SSL/TLS 服务器配置

Universal Print Server 充当 SSL/TLS 服务器。

使用 `Enable-UpsSsl.ps1` PowerShell 脚本配置 SSL/TLS 设置。

在通用打印服务器上安装 TLS 证书

对于 HTTPS，您必须在通用打印服务器上安装一个受 VDA 信任的 SSL 服务器证书。使用 Microsoft Active Directory 证书服务或其他证书颁发机构为通用打印服务器请求证书。

使用微软活动目录证书服务注册/请求证书时，请记住以下注意事项：

1. 将证书放置在本地计算机的 **个人** 证书存储中。
2. 将证书主题可分辨名称 (Subject DN) 的 **公用名** 属性设置为通用打印服务器的完全限定域名 (FQDN)。在证书模板中指定此项。

3. 将用于生成证书请求和私钥的加密服务提供程序 (CSP) 设置为 **Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**。在证书模板中指定此项。
4. 将密钥大小设置为至少 2048 位。在证书模板中指定此项。

有关创建和安装证书的更多信息，请参阅管理证书。

在通用打印服务器上配置 SSL

通用打印服务器上的 XTE 服务侦听传入连接。启用 SSL 后，它将充当 SSL 服务器。传入连接有两种类型：包含打印命令的打印 Web 服务连接，以及包含打印作业的打印数据流连接。可以在这些连接上启用 SSL。SSL 可保护这些连接的机密性和完整性。默认情况下，SSL 处于禁用状态。

用于配置 SSL 的 PowerShell 脚本位于安装介质上，文件名为：`\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

在通用打印服务器上配置侦听端口号

以下是 XTE 服务的默认端口：

- 明文打印 Web 服务 (HTTP) TCP 端口：8080
- 明文打印数据流 (CGP) TCP 端口: 7229
- 加密打印 Web 服务 (HTTPS) TCP 端口: 8443
- 加密打印数据流 (CGP) TCP 端口: 443

要更改 Universal Print Server 上 XTE 服务使用的端口，请以管理员身份在 PowerShell 中运行以下命令（有关 Enable-UpsSsl.ps1 PowerShell 脚本用法的说明，请参阅后面的部分）：

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` 或 `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

Universal Print Server 上的 TLS 设置

如果您在负载平衡配置中拥有多个 Universal Print Server，请确保所有 Universal Print Server 上的 **TLS** 设置配置一致。

在 Universal Print Server 上配置 TLS 时，已安装的 TLS 证书的权限会更改，从而授予 Universal Printing Service 对证书私钥的读取访问权限，并通知 Universal Printing Service 以下信息：

- 证书存储中用于 TLS 的证书。

- 用于 TLS 连接的 TCP 端口号。

必须配置 Windows 防火墙（如果已启用）以允许这些 TCP 端口上的传入连接。使用 Enable-UpsSsl.ps1 PowerShell 脚本时，将为您完成此配置。

- 允许的 TLS 协议版本。

Universal Print Server 支持 TLS 协议版本 1.3 和 1.2。请指定允许的最低版本。

默认 TLS 协议版本为 1.2。

> **注意：**
>
> 从 Citrix Virtual Apps and Desktops 2311 版开始，不再支持 TLS 1.1 和 1.0。

- 允许的 TLS 密码套件。

密码套件选择用于连接的加密算法。VDA 和 Universal Print Server 可以支持不同的密码套件集。当 VDA 连接并发送支持的 TLS 密码套件列表时，Universal Print Server 会将客户端的密码套件之一与其自身配置的密码套件列表中的一个密码套件进行匹配，并接受连接。如果没有匹配的密码套件，Universal Print Server 将拒绝连接。

Universal Print Server 支持以下密码套件集，这些套件集针对 OPEN、FIPS 和 SP800-52 本机 Crypto Kit 模式命名为 GOV（政府）、COM（商业）和 ALL。可接受的密码套件还取决于 **SSL FIPS Mode** 策略设置和 Windows FIPS Mode。有关 Windows FIPS Mode 的信息，请参阅这篇 Microsoft 支持文章。

密码套件（按优先级降序排列）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_G	X		X	X		X	X		X

密码套件（按优先级降序排列）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
CM_SHA384									
TLS_ECDHE_RSA_AES256_CBC_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA	X	X		X	X		X	X	

使用 PowerShell 脚本在通用打印服务器上配置 TLS

将 TLS 证书安装到证书存储的 **本地计算机 > 个人 > 证书** 区域。如果该位置存在多个证书，请向 `Enable-UpsSsl.ps1` PowerShell 脚本提供证书的指纹。

> **注意：**
>
> PowerShell 脚本根据通用打印服务器的 FQDN 查找正确的证书。如果通用打印服务器 FQDN 只有一个证书，则无需提供证书指纹。

`Enable-UpsSsl.ps1` 脚本启用或禁用从 VDA 到通用打印服务器的 TLS 连接。此脚本位于安装介质的 **Support > Tools > SslSupport** 文件夹中。

启用 TLS 时，脚本会禁用通用打印服务器 TCP 端口的所有现有 Windows 防火墙规则。然后，它会添加新规则，允许 XTE 服务仅在 TLS TCP 和 UDP 端口上接受传入连接。它还会禁用以下 Windows 防火墙规则：

- 明文打印 Web 服务连接（默认值：8080）
- 明文打印数据流 (CGP) 连接（默认值：7229）

结果是 VDA 只能在使用 TLS 时建立这些连接。

注意：

启用 TLS 不会影响源自 VDA 并流向通用打印服务器的 Windows 打印后台处理程序 RPC/SMB 连接。

重要提示：

将 **Enable** 或 **Disable** 指定为第一个参数。如果本地计算机个人证书存储中只有一个证书具有通用打印服务器的 FQDN，则 CertificateThumbprint 参数是可选的。其他参数是可选的。

语法

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort &lt;port>] [-CGPPort &lt;port>] [-HTTPSPort &lt;port>] [-CGPSSLPort &lt;port>] [-SSLMinVersion &lt;version>] [-SSLCipherSuite &lt;name>] [-CertificateThumbprint &lt;thumbprint>] [-FIPSMode &lt;Boolean>] [-ComplianceMode &lt;mode>]

Enable-UpsSSL.ps1 -Disable [-HTTPPort &lt;portnum>] [-CGPPort &lt;portnum>]
```

参数	描述
启用	在 XTE 服务器上启用 SSL/TLS。此参数或 Disable 参数是必需的。

参数	描述
禁用	在 XTE 服务器上禁用 SSL/TLS。此参数或 Enable 参数是必需的。
证书指纹 `"<thumbprint>"`	本地计算机个人证书存储中 TLS 证书的指纹，用引号括起来。脚本使用指定的指纹来选择您要使用的证书。
HTTP 端口 `<port>`	明文打印 Web 服务 (HTTP/SOAP) 端口。默认值: 8080
CGP 端口 `<port>`	明文打印数据流 (CGP) 端口。默认值: 7229
HTTPS 端口 `<port>`	加密打印 Web 服务 (HTTPS/SOAP) 端口。默认值: 8443
CGP SSL 端口 `<port>`	加密打印数据流 (CGP) 端口。默认值: 443
SSL 最低版本 `"<version>"`	最低 TLS 协议版本，用引号括起来。有效值: “TLS_1.2” 和 “TLS_1.3”。默认值: TLS_1.2。
SSL 密码套件 `"<name>"`	TLS 密码套件包的名称，用引号括起来。有效值: “GOV”、“COM” 和 “ALL”（默认值）。
FIPS 模式 `<Boolean>`	在 XTE 服务器中启用或禁用 FIPS 140 模式。有效值：$true 启用 FIPS 140 模式，$false 禁用 FIPS 140 模式。

示例

以下脚本启用 TLS。指纹（在此示例中表示为“12345678987654321”）用于选择要使用的证书。

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

以下脚本禁用 TLS。

```
Enable-UpsSsl.ps1 –Disable
```

配置 FIPS 模式

启用美国联邦信息处理标准 (FIPS) 模式可确保通用打印服务器加密连接仅使用符合 FIPS 140 的加密技术。

在客户端上配置 FIPS 模式之前，请先在服务器上配置 FIPS 模式。

有关启用/禁用 Windows FIPS 模式的信息，请查阅 Microsoft 的文档站点。

在客户端上启用 FIPS 模式

在 Delivery Controller™ 上，运行 Web Studio 并将 **UPS FIPS 模式** Citrix 策略设置设为**已启用**。启用 Citrix 策略。

在每个 VDA 上执行以下操作：

1. 启用 Windows FIPS 模式。
2. 重新启动 VDA。

在服务器上启用 FIPS 模式

在每个通用打印服务器上执行以下操作：

1. 启用 Windows FIPS 模式。
2. 以管理员身份运行此 PowerShell 命令: `stop-service CitrixXTEServer, UpSvc`
3. 使用 `-Enable -FIPSMode $true` 参数运行 `Enable-UpsSsl.ps1` 脚本。
4. 重新启动 Universal Print Server。

在客户端禁用 FIPS 模式

在 Web Studio 中，将 **UPS FIPS Mode** Citrix 策略设置设为 **Disabled**。启用 Citrix 策略。您也可以删除 **UPS FIPS Mode** Citrix 策略设置。

在每个 VDA 上执行以下操作：

1. 禁用 Windows FIPS 模式。
2. 重新启动 VDA。

在服务器上禁用 FIPS 模式

在每个 Universal Print Server 上执行以下操作：

1. 禁用 Windows FIPS 模式。
2. 以管理员身份运行此 PowerShell 命令: `stop-service CitrixXTEServer, UpSvc`
3. 使用 `-Enable -FIPSMode $false` 参数运行 `Enable-UpsSsl.ps1` 脚本。
4. 重新启动 Universal Print Server。

> **注意：**
>
> 当 SSL 协议版本设置为 TLS 1.3 时，不支持 FIPS 模式。

配置 SSL/TLS 协议版本

默认的 SSL/TLS 协议版本是 TLS 1.2。TLS 1.2 和 TLS 1.3 是生产环境中推荐的 SSL/TLS 协议版本。为了进行故障排除，可能需要在非生产环境中临时更改 SSL/TLS 协议版本。

Universal Print Server 不支持 SSL 2.0 和 SSL 3.0。

在服务器上设置 SSL/TLS 协议版本

在每台 Universal Print Server 上执行以下操作：

1. 以管理员身份运行此 PowerShell 命令：`stop-service CitrixXTEServer, UpSvc`
2. 运行 `Enable-UpsSsl.ps1` 脚本，并使用 `-Enable -SSLMinVersion` 版本参数。请记住，测试完成后将其设置回 TLS 1.2 或 TLS 1.3。
3. 重新启动 Universal Print Server。

在客户端上设置 SSL/TLS 协议版本

在 Studio 中，将 **SSL Protocol Version** 策略设置设为所需的协议版本并启用该策略。

确保 VDA 的操作系统支持所选的 TLS 版本。有关 Windows 上支持的 TLS 版本，请参阅 Microsoft Learn - TLS 协议版本支持。要配置注册表以覆盖默认设置，请参阅 Microsoft Learn - TLS、DTLS 和 SSL 协议版本设置。

故障排除

如果发生连接错误，请检查 Universal Print Server 上的 C:\Program Files (x86)\Citrix\XTE\logs\error.log 文件。

如果 SSL/TLS 握手失败，此日志文件中将显示错误消息 **SSL handshake from client failed**。如果 VDA 和 Universal Print Server 上的 SSL/TLS 协议版本不匹配，则可能会发生此类故障。

在包含 Universal Print Server 主机名的以下策略设置中使用 Universal Print Server FQDN：

- 会话打印机
- 打印机分配
- 用于负载平衡的通用打印服务器

确保通用打印服务器和 VDA 上的系统时钟（日期、时间、时区）正确。

虚拟通道允许列表

虚拟通道允许列表是一项功能，可让您控制环境中允许哪些非 Citrix 虚拟通道。默认情况下，虚拟通道允许列表功能处于启用状态。因此，只有 Citrix 虚拟通道才允许在 Citrix Virtual Apps and Desktops™ 会话中打开。如果需要使用自定义虚拟通道（无论是自行开发还是来自第三方），则需要将其显式添加到允许列表中。

配置

虚拟通道允许列表默认处于启用状态。您可以使用 Citrix 策略中的以下设置来配置此功能：

- **虚拟通道允许列表**：用于启用或禁用该功能并将虚拟通道添加到列表中。
- **虚拟通道允许列表日志限制**：设置虚拟通道允许列表事件日志记录的限制周期。
- **虚拟通道允许列表日志记录**：设置虚拟通道允许列表的日志记录级别。

将虚拟通道添加到允许列表

要将虚拟通道添加到允许列表，您需要以下信息：

1. 代码中定义的虚拟通道名称，最多可包含七个字符。例如，`CTXCVC1`。
2. 在 VDA 计算机上打开虚拟通道的进程路径。例如，`C:\Program Files\Application\run.exe`。

获得所需信息后，您必须使用虚拟通道允许列表策略设置将虚拟通道添加到允许列表。要将虚拟通道添加到列表中，请输入虚拟通道名称，后跟逗号，然后是访问虚拟通道的进程路径。如果有多个进程，可以通过用逗号分隔每个进程来添加这些进程。

对于单个进程

使用前面的示例，将以下条目添加到列表中：

```
CTXCVC1,C:\Program Files\Application\run.exe
```

对于多个进程

如果存在多个进程，请将以下条目添加到列表中：

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

使用通配符

支持使用通配符 (*)。当目录或可执行文件的名称根据应用程序版本而变化，或者第三方组件安装在用户配置文件中时，可以使用通配符。

您可以在以下场景中使用通配符：

- 替换完整的目录名称。 例如：`C:\Program Files\Application*\run1.exe`
- 替换目录名称的一部分。 例如：`C:\Program Files\Application\v*\run1.exe`
- 替换可执行文件的名称。 例如：`C:\Program Files\Application\v1.2*.exe`
- 替换可执行文件名称的一部分。 例如：`C:\Program Files\Application\v1.2\run*.exe`

适用以下限制：

- 通配符只能用于替换单个目录。例如，如果可执行文件位于 `C:\Program Files\Application\v1.2\run1.exe`
  - 允许：`C:\Program Files\Application*\run1.exe`
  - 不允许：`C:\Program Files*\run1.exe`
- 条目必须包含文件扩展名。
  - 允许：`C:\Program Files\Application\v1.2*.exe`
  - 不允许：`C:\Program Files\Application\v1.2*`
- 所有路径都必须是本地路径。

> **注意：**
>
> - 不允许使用网络路径。
> - 通配符支持从 Citrix Virtual Apps and Desktops™ 2206 开始提供。
> - Citrix Virtual Apps and Desktops 2203 LTSR 从 CU2 开始支持通配符。

使用系统环境变量

您可以使用系统环境变量来简化允许列表中受信任进程的定义。您可以使用任何开箱即用的变量，例如 `%programfiles%`、`%programfiles(x86)%`、`%systemdrive%` 和 `%systemroot%`。

只要在系统级别定义了自定义环境变量，您也可以使用它们。

以下示例描述了开箱即用的环境变量：

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

以下示例描述了自定义系统环境变量：

- 自定义变量名称：`app`
- 自定义变量值：`%programfiles%\Application\`
- 允许列表条目：`CTXCVC1,%app%\run.exe`

> **注意：**
>
> 不支持用户环境变量。
>
> 环境变量支持从 Citrix Virtual Apps and Desktops 2209 版开始提供。

获取虚拟通道名称和进程

获取虚拟通道名称以及在 VDA 计算机上打开该通道的进程的最简单方法是，从提供该虚拟通道的开发人员或第三方供应商处获取信息。

或者，您可以通过应用功能的日志并按照以下步骤获取信息：

1. 自定义虚拟通道的客户端和服务器组件就位后，启动虚拟应用程序或虚拟桌面。
2. 在 VDA 计算机的系统事件日志中，查找自定义虚拟通道的名称以及尝试打开它的进程。有关可用事件的更多信息，请参阅事件日志。
3. 从会话中注销。
4. 在虚拟通道允许列表策略设置中为已识别的虚拟通道和进程添加条目。
5. 重新启动计算机。
6. VDA 注册后，运行虚拟应用程序或虚拟桌面以验证自定义虚拟通道是否成功打开。

Citrix 虚拟通道的注意事项

所有内置的 Citrix 虚拟通道都受信任，无需进一步配置即可打开。但是，以下两个功能由于外部依赖项，需要在允许列表中明确条目：

- 多媒体重定向
- 适用于 Skype for Business 的 HDX RealTime 优化包

多媒体重定向

如果您使用 Windows Media Player 以外的媒体播放器作为系统媒体播放器，则需要将其作为受信任的进程添加到允许列表中。允许列表条目需要以下信息：

- 虚拟通道名称：`CTXMM`
- 进程：VDA 计算机中使用的媒体播放器的路径。例如，`C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 允许列表条目：`CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

适用于 Skype for Business 的 HDX RealTime 优化包

允许列表条目需要以下信息：

- 虚拟通道名称：`CTXRMEP`
- 进程：VDA 计算机中 Skype for Business 可执行文件的路径，该路径可能因 Skype for Business 的版本或您是否使用了自定义安装路径而异。例如，`C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 允许列表条目：`CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

VDA 与 Delivery Controller™ 之间的 WebSocket 通信

本文介绍了如何设置 WebSocket 连接，以便在 VDA 和 Delivery Controller 之间进行通信，作为使用 WCF 通信的替代方案。其优点是，VDA 到 Delivery Controller 的通信只需使用 TLS 端口 443。

工作原理

以下部分介绍了 Delivery Controller 与 VDA 之间 WebSocket 连接的工作流程：

正常代理操作期间

1. Citrix Virtual Apps and Desktops™ 管理员通过使用 Machine Creation Service (MCS) 预配 VDA 来启动此过程。
2. 在 MCS 预配过程中，MCS 为每个 VDA 生成公钥-私钥对，并将公钥注册到 Delivery Controller 上的 FMA 信任服务。MCS 将公钥-私钥对作为文件保存在 VDA 上的身份磁盘下。

3. 当 VDA 计算机启动时，安装在 VDA 计算机上的 MCS 代理从身份磁盘读取密钥对，并将此信息写入 VDA 注册表位置。
4. 安装在 VDA 上的代理程序从注册表读取密钥对，并向 Delivery Controller 生成一个启用 SSL 的 WebSocket 请求，其中服务密钥由私钥签名。
5. Delivery Controller 使用来自 FMA 信任服务的公钥验证已签名的服务密钥授权标头。
6. 验证完成后，系统在 VDA 和 Delivery Controller 之间建立 WebSocket 连接。

LHC 模式何时激活

如果为 LHC 启用 Websocket 支持，则在 LHC 模式下，当 VDA 尝试与高可用性服务建立 Websocket 连接时，高可用性服务会使用本地数据库中的公钥验证已签名的服务密钥授权标头。这会验证 Websocket 连接，并且 VDA 与 Delivery Controller 之间的 WebSocket 连接即使在 LHC 模式下也能成功。

WebSocket 支持

开始之前

1. 配置您的站点。有关详细信息，请参阅 创建站点。
2. 在 Delivery Controller 上安装 TLS 证书。有关详细信息，请参阅 在 Controller 上安装 TLS 服务器证书。
3. 在 VDA 上安装根 CA 和中间 CA 以信任 Delivery Controller。

过程

按照说明设置 WebSocket 连接：

1. 在 Delivery Controller 上启用 WebSocket 连接。在站点中的每个 Delivery Controller 上运行以下命令：

   `New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy" -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force`

2. 启用 WebSocket 后，重新启动 Broker Service。
3. 为 LHC 模式启用 WebSocket 支持。在站点中的每个 Delivery Controller 上运行以下命令：

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\LHC" -Name "WebSocketEnabledLhc" -PropertyType "DWord" -Value 1 -Force
```

4. 为使用 MCS 预配的已加入 AD 的 VDA 创建计算机目录。有关详细信息，请参阅创建计算机目录。
5. 创建交付组并将 VDA 添加到其中。有关详细信息，请参阅创建交付组。
6. 在 VDA 上启用 WebSocket 连接。在 VDA 上运行以下 PowerShell 命令：

```
New-ItemProperty
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent
\WebSocket" -Name "Enabled" -PropertyType "DWord" -Value 1 -Force
```

- 要检查 WebSocket 是否已启用，请检查以下注册表项值。`Enabled` 的值必须为 1。

  键：

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAge
  nt\WebSocket
  ```

  名称：Enabled

  类型：REG_DWORD

  值：1

HDX™ 连接性

Citrix HDX 代表一系列广泛的技术，旨在为集中式应用程序和桌面的用户在任何设备上并通过任何网络提供高清体验。

HDX 围绕以下三个技术原则设计：

- 智能重定向
- 自适应压缩
- 数据去重

以不同组合应用时，它们优化了 IT 和用户体验，降低了带宽消耗，并提高了每个托管服务器的用户密度。

在 HDX 产品中，您可以通过独特的专有传输协议进行连接，在建立会话时利用最大传输单元，并通过 Citrix SD-WAN 优化连接性。

自适应传输

自适应传输是 Citrix Virtual Apps and Desktops™ 中的一种机制，允许使用首选传输协议为 HDX 会话建立连接，同时，如果首选协议的连接不可用，则提供回退到 TCP 的机制。

支持以下传输协议：

- 智能数据传输 (EDT)
- 传输控制协议 (TCP)

配置

自适应传输默认启用。您可以将自适应传输配置为在以下模式下运行：

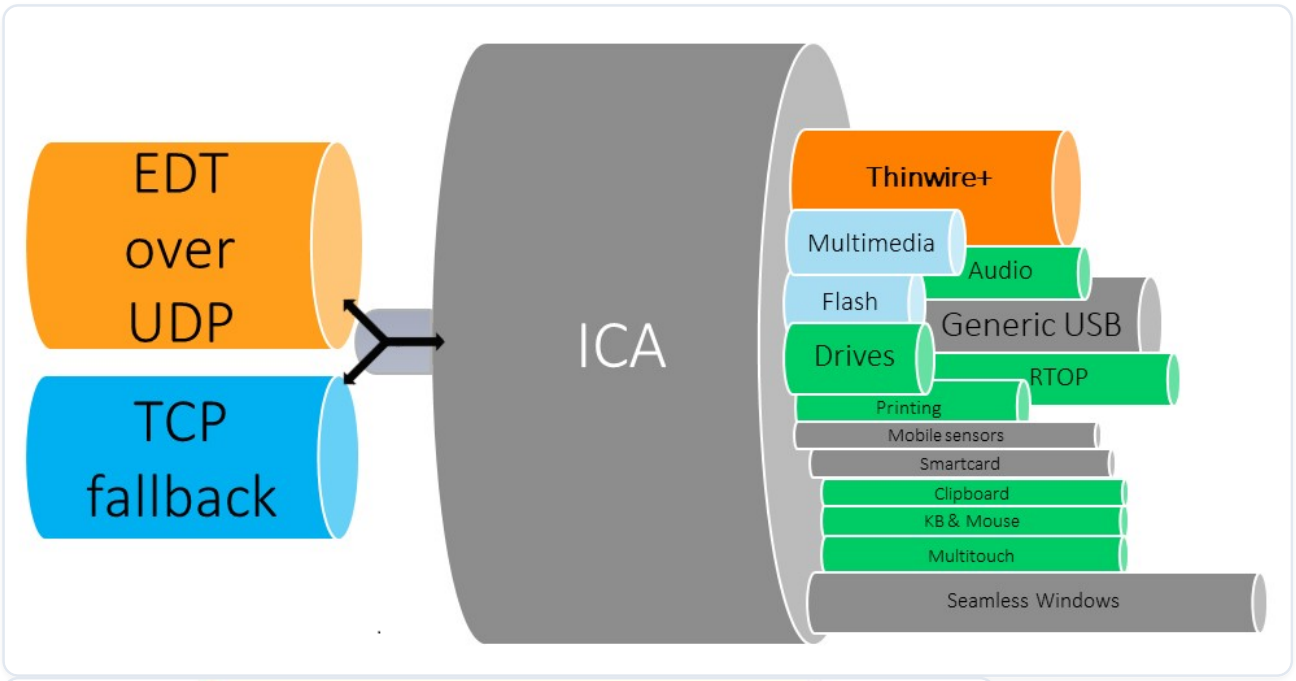
- **首选**：(默认) 客户端尝试使用首选协议连接，如果首选协议连接不可用，则回退到 TCP。
- **诊断模式**：客户端仅尝试使用首选协议连接。禁用回退到 TCP。
- **关闭**：客户端仅尝试使用 TCP 连接。

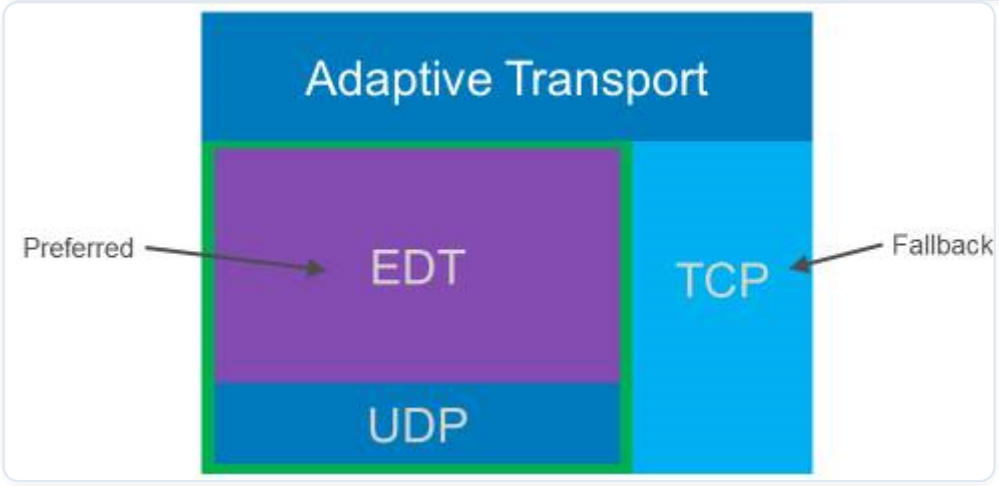
工作原理

当**自适应传输**设置为 `Preferred` 时，客户端会同时尝试使用首选协议和 TCP 连接到会话。如果无法使用首选协议连接且客户端必须回退到使用 TCP，这有助于优化连接时间。如果使用 TCP 建立连接，客户端会每五分钟在后台尝试使用首选协议连接。

当**自适应传输**设置为 `Diagnostic mode` 时，客户端仅使用首选协议连接到会话。如果客户端无法使用首选协议建立连接，则不会回退到使用 TCP，并且连接会失败。

当**自适应传输**设置为 `Off` 时，**自适应传输**被禁用，并且客户端仅使用 TCP 连接到会话。





系统要求

以下是使用自适应传输和 EDT 的要求：

- 控制平面

  - Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops™ 服务）
  - Citrix Virtual Apps and Desktops：当前支持的版本
- 虚拟投递代理
  - Windows：当前支持的版本 (建议使用 2402 或更高版本)
  - Linux：当前支持的版本 (建议使用 2402 或更高版本)
- Citrix Workspace™ 应用程序
  - Windows：当前支持的版本 (建议使用 2402 或更高版本)
  - Linux：当前支持的版本 (建议使用 2402 或更高版本)
  - Mac: 当前支持的版本（建议使用 2402 或更高版本）
  - iOS: Apple App Store 中提供的最新版本
  - Android: Google Play 中提供的最新版本
- Citrix NetScaler® 网关
  - 14.1.12.30 或更高版本（推荐）
  - 13.1.17.42 或更高版本（建议使用 13.1-52.19 或更高版本）

> **注意：**
>
> 有关 Linux VDA 的详细信息，请参阅 Linux Virtual Delivery Agent 文档。

网络要求

以下部分是使用 EDT 和自适应传输的网络要求：

会话主机

如果您的会话主机有防火墙（例如 Windows Defender 防火墙），则必须允许以下入站流量用于内部连接。

描述	源	协议	端口
内部连接 - 会话可靠性已启用	客户端	UDP	2598

描述	源	协议	端口
内部连接 - 会话可靠性已禁用			1494
内部连接 - HDX™ Direct 或 VDA SSL			443

注意：

VDA 安装程序会将相应的入站规则添加到 Windows Defender 防火墙。如果您使用不同的防火墙，则必须添加上述规则。

内部网络

下表描述了在您的网络中使用 EDT 所需的防火墙规则：

描述	协议	源	目标	目标端口
直接内部连接 - 会话可靠性已启用	UDP	客户端网络	VDA 网络	2598
直接内部连接 - 会话可靠性已禁用				1494
直接内部连接 - HDX Direct 或 VDA SSL				443
NetScaler 网关		NetScaler SNIP		2598
NetScaler 网关 - VDA SSL				443

注意：

如果您正在使用 Citrix Gateway Service，则必须启用 **Rendezvous** 才能使用 EDT 作为传输协议。有关系统和网络要求，请参阅 Rendezvous 文档。

客户端网络

下表概述了客户端设备的连接要求：

描述	协议	源	目标	目标端口
内部连接 - 会话可靠性已启用	UDP	客户端 IP	VDA 网络	2598
内部连接 - 会话可靠性已禁用				1494
内部连接 - HDX Direct 或 SSL VDA				443
外部连接 - NetScaler Gateway			NetScaler Gateway 公共 IP 地址	443
外部连接 - Citrix Gateway Service			Citrix 网关服务	443

注意：

如果您正在使用 Citrix Gateway Service，客户端必须能够访问 `<https://*.*.nssvc.net>`。如果您无法使用 `<https://*.*.nssvc.net>` 允许所有子域，则可以使用 `<https://*.c.nssvc.net>` 和 `<https://*.g.nssvc.net>` 代替。有关详细信息，请参阅知识中心文章 CTX270584。

智能数据传输

Enlightened Data Transport (EDT) 是基于用户数据报协议 (UDP) 构建的 Citrix 专有传输协议。它在具有挑战性的长途连接上提供卓越的用户体验，同时保持服务器可伸缩性。EDT 提高了不可靠网络上所有 ICA® 虚拟通道的数据吞吐量，从而提供更好、更一致的用户体验。

启用**自适应传输**后，EDT 是首选协议。

须知事项

- 必须启用**会话可靠性**才能将 **MTU 发现**和 EDT 与 NetScaler® Gateway 和 Citrix Gateway Service 结合使用。
- 在某些情况下，数据包分段可能会导致性能下降，甚至无法打开会话。为防止出现这种情况，您必须将 EDT MTU 调整为适合您网络的值。您可以使用 EDT MTU 发现或 如何在具有非标准 MTU 的网络上使用 EDT 时配置 MSS 中所述的手动解决方法。
- 有关启用 EDT 与 NetScaler Gateway 结合使用的详细信息，请参阅 配置 NetScaler Gateway 以支持 Enlightened Data Transport。

EDT MTU 发现

MTU 发现允许 EDT 在建立会话时自动确定最大传输单元 (MTU)。这样做可以防止 EDT 数据包分段，否则可能会导致性能下降或无法建立会话。

MTU 发现默认处于启用状态。如果需要禁用它，请参阅 通过注册表管理的 HDX 功能 了解详细信息。

> **注意：**
>
> - 必须启用**会话可靠性**才能使 MTU 发现正常工作。
> - VDA 2209 及更高版本支持使用多流 ICA 的 MTU 发现。

EDT MTU 重新发现

MTU 重新发现允许 EDT 在初始连接后检测到较低的 MTU 时，自动调整活动会话的 MTU，从而确保最佳性能和可靠性。

可以使用以下设置通过 Citrix 策略配置 MTU 重新发现：

- **MTU 重新发现**：
  - 关闭：MTU 重新发现已禁用。
  - 静态：当检测到 MTU 降低时，会话的 MTU 将在会话的剩余时间内设置为 1200。
  - 动态：当在活动会话中检测到 MTU 降低时，将触发 MTU 发现以确定连接的最佳 MTU。

默认情况下，此设置处于禁用状态。

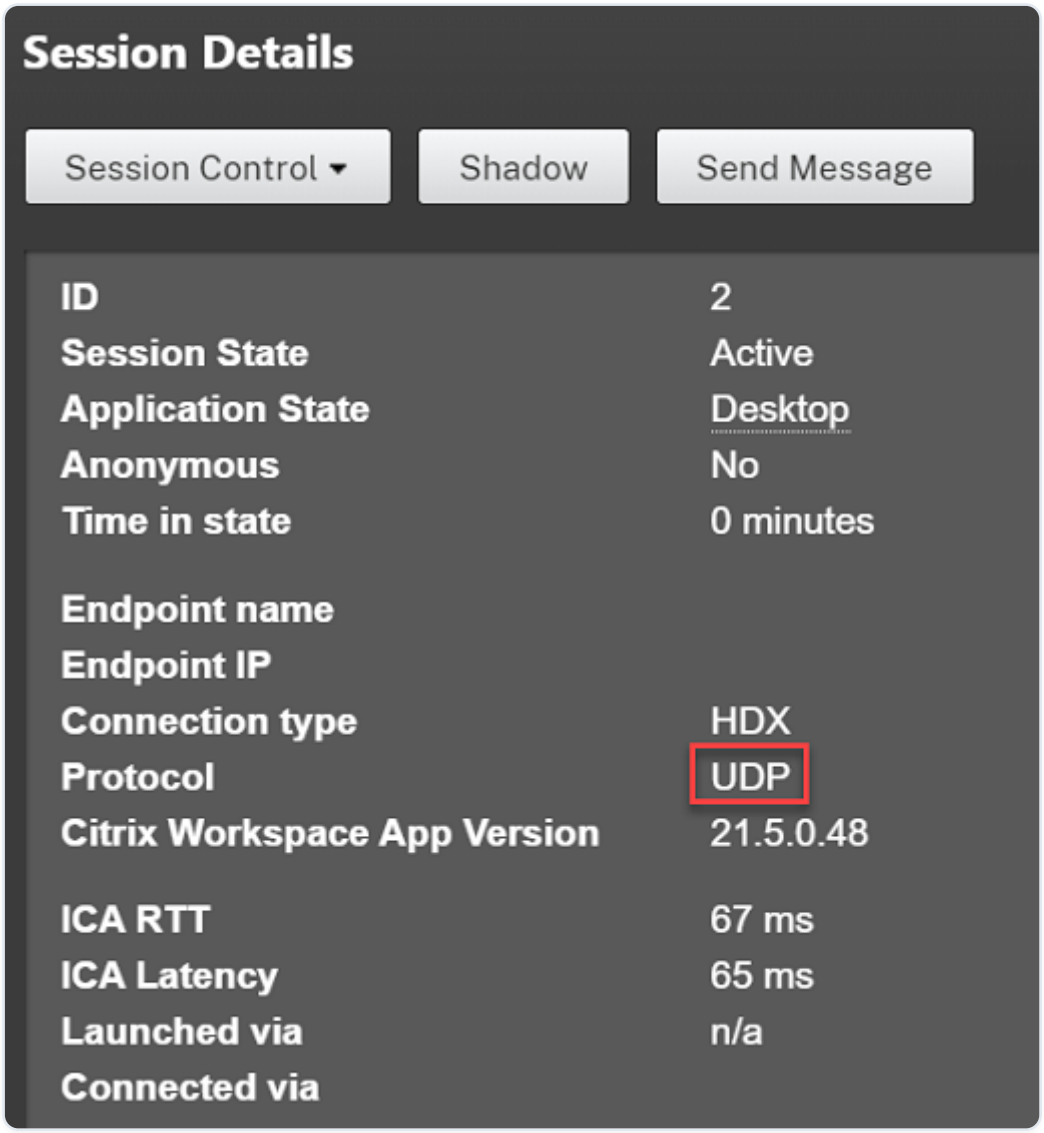
注意：

- 必须启用**会话可靠性**才能使 MTU 重新发现正常工作。
- MTU 重新发现需要适用于 Windows 2607 或更高版本的 Workspace 应用程序。
- 如果您之前通过注册表配置了 MTU 重新发现，则必须删除注册表配置才能使用策略设置配置 MTU 重新发现。

故障排除

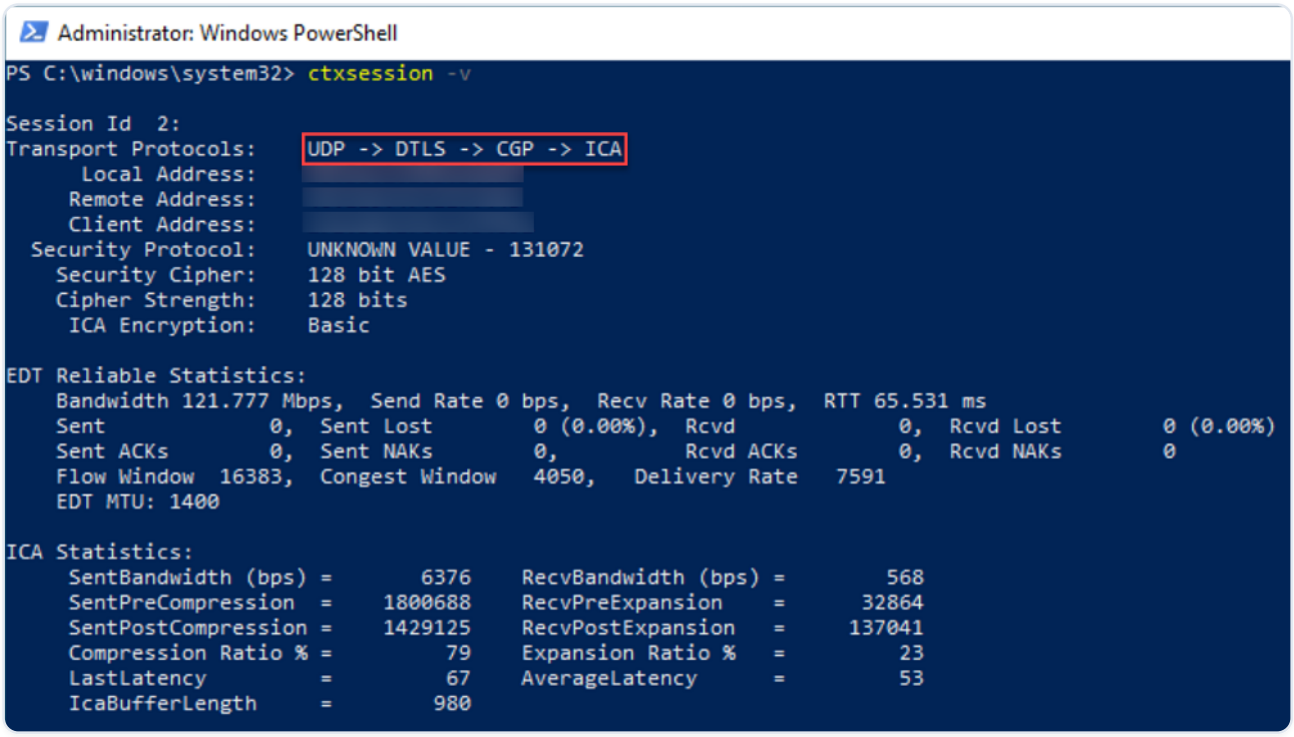
要确认 EDT 正用作会话的传输协议，您可以使用 Director 或 VDA 上的 `CtxSession.exe` 命令行实用程序。

在 Director 中，查找会话并选择**详细信息**。如果**连接类型**为 `HDX™` 且**协议**为 `UDP`，则 EDT 正用作会话的传输协议。



要使用 CtxSession.exe 实用程序，请在会话中启动命令提示符或 PowerShell 并运行 `ctxsession.exe`。要查看详细统计信息，请运行 `ctxsession.exe -v`。如果正在使用 EDT，则传输协议将显示以下其中一项：

- **UDP > ICA®**（会话可靠性已禁用）
- **UDP > CGP > ICA**（会话可靠性已启用）
- **UDP > DTLS > CGP > ICA**（ICA 已进行 DTLS 端到端加密）



当会话无法通过 EDT 连接时

要对**自适应传输**和 **EDT** 进行故障排除，我们建议执行以下操作：

1. 查看系统要求、网络要求、已知问题 和注意事项，并确保所有项目都已解决。
2. 检查 Studio 或 GPO 中是否存在覆盖所需 **HDX 自适应传输**设置的 Citrix® 策略。
3. 检查客户端上是否存在覆盖所需 HDX 自适应传输设置的设置。这可以是 GPO 首选项、使用可选的 Workspace 应用程序管理模板配置的设置，或者在注册表或客户端配置文件中手动配置的 **HDXoverUDP** 设置。
4. 在多会话 VDA 计算机上，确保 UDP 侦听器处于活动状态。在 VDA 计算机中打开命令提示符并运行 `netstat -a -p udp`。有关详细信息，请参阅如何确认 HDX Enlightened Data Transport 协议。
5. 检查网络防火墙和VDA机器上运行的防火墙是否已配置适当的防火墙规则。
6. 在内部启动一个直接会话，绕过NetScaler® Gateway或Citrix Gateway Service，并检查正在使用的协议。如果会话使用EDT，则VDA已准备好通过NetScaler Gateway或Citrix Gateway Service使用EDT进行外部连接。
7. 如果EDT适用于直接内部连接，但不适用于通过NetScaler Gateway或Citrix Gateway Service的会话：
   - 确保已启用**会话可靠性**。

- 如果使用NetScaler Gateway，请确保您的配置符合(/zh-cn/netscaler-gateway/current-release/hdx-enlightened-data-transport-support/configuring-citrix-gateway.html)中概述的所需配置，即。

8. 如果使用Citrix Gateway Service，请确保Rendezvous已启用并正常工作。
9. 检查您的用户连接是否需要非标准MTU。有效MTU低于1500字节的连接会导致EDT数据包分段，这反过来会影响性能，甚至导致会话启动失败。此问题在使用VPN、某些Wi-Fi接入点以及4G和5G等移动网络时很常见。请确保您已启用MTU发现，或者正在设置自定义MTU，如(https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX231821/how-to-configure-mss-when-using-edt-on-networks-with-nonstandard-mtu)中所述。

已知问题

- 不对称网络路径可能导致MTU发现对于不通过NetScaler Gateway或Citrix Gateway Service的连接失败。要解决此问题，请升级到VDA版本2103或更高版本。
- 使用NetScaler Gateway时，不对称网络路径可能导致MTU发现失败。这是由于Gateway上的一个问题，导致EDT数据包头中的“不分段 (DF)”位未传播。此问题的修复程序从固件版本13.1 build 17.42开始提供。有关如何启用修复程序的详细信息，请参阅(/zh-cn/netscaler-gateway/current-release/hdx-enlightened-data-transport-support/pmtud-support-on-citrix-gateway.html)文档。
- 对于通过DS-Lite网络连接的用户，MTU发现可能会失败。当启用数据包处理时，某些调制解调器无法遵守DF位，从而阻止MTU发现检测分段。在这种情况下，可用的选项如下：
  - 禁用用户调制解调器上的数据包处理。
  - 禁用**MTU发现**并使用硬编码MTU，如如何在非标准MTU网络上使用EDT时配置MSS所述。
  - 禁用**自适应传输**以强制会话使用TCP。如果只有一部分用户受到影响，请考虑在客户端禁用它，以便其他用户可以继续使用EDT。

HDX™ 直连

访问 Citrix 提供的资源时，如果直接通信可行，HDX Direct 允许内部和外部客户端设备与会话主机建立安全的直接连接。

系统要求

以下是使用 HDX Direct 的系统要求：

- 控制平面
  - 思杰 DaaS™

  - Citrix Virtual Apps and Desktops™ 2503 或更高版本
- 虚拟投递代理 (VDA)
  - Windows: 2503 或更高版本
- Workspace 应用程序
  - Windows: 2503 或更高版本
  - Linux：2411 或更高版本
  - Mac：2411 或更高版本
- 访问层
  - Citrix 工作区™
  - Citrix Storefront™ 2503 或更高版本
  - Citrix 网关服务
  - Citrix NetScaler® 网关

网络要求

以下是使用 HDX Direct 的网络要求。

会话主机

如果您的会话主机有防火墙（例如 Windows Defender 防火墙），则必须允许以下入站流量用于内部连接。

描述	源	协议	端口
直接内部连接	客户端	TCP	443
直接内部连接	客户端	UDP	443

> 注意：
>
> VDA 安装程序会将相应的入站规则添加到 Windows Defender 防火墙。如果您使用其他防火墙，则必须添加上述规则。

客户端网络

下表描述了适用于内部和外部用户的客户端网络。

内部用户

描述	协议	源	源端口	目标	目标端口
直接内部连接	TCP	客户端网络	1024–65535	VDA 网络	443
直接内部连接	UDP	客户端网络	1024–65535	VDA 网络	443

外部用户

描述	协议	源	源端口	目标	目标端口
STUN（仅限外部用户）	UDP	客户端网络	1024–65535	Internet（请参阅下面的注释）	3478, 19302
外部用户连接	UDP	客户端网络	1024–65535	数据中心的公共 IP 地址	1024–65535

数据中心网络

下表描述了内部用户和外部用户的数据中心网络。

内部用户

描述	协议	源	源端口	目标	目标端口
直接内部连接	TCP	客户端网络	1024–65535	VDA 网络	443
直接内部连接	UDP	客户端网络	1024–65535	VDA 网络	443

外部用户

描述	协议	源	源端口	目标	目标端口
STUN（仅限外部用户）	UDP	VDA 网络	1024–65535	互联网（参见下文注释）	3478, 19302
外部用户连接	UDP	DMZ / 内部网络	1024–65535	VDA 网络	55000–55250
外部用户连接	UDP	VDA 网络	55000–55250	客户端的公共 IP	1024–65535

注意：

VDA 和 Workspace 应用程序都尝试按相同顺序向以下服务器发送 STUN 请求：

- stun.cloud.com:3478
- stun.cloudflare.com:3478
- stun.l.google.com:19302

如果您使用 **HDX Direct 端口范围**策略设置更改外部用户连接的默认端口范围，则相应的防火墙规则必须与您的自定义端口范围匹配。

配置

HDX Direct 默认处于禁用状态。您可以使用 Citrix 策略中的 **HDX Direct** 设置配置此功能。

- **HDX Direct**：用于启用或禁用功能。
- **HDX Direct 模式**：确定 **HDX Direct** 是仅适用于内部客户端，还是同时适用于内部和外部客户端。
- **HDX Direct 端口范围**：定义 VDA 用于与外部客户端建立连接的端口范围。

如有需要，可以通过编辑以下注册表值来修改 HDX Direct 使用的 STUN 服务器列表：

- 项: HKLM\SOFTWARE\Citrix\HDX-Direct

- 值类型: REG_MULTI_SZ
- 值名称: STUNServers
- 数据: stun.cloud.com:3478 stun.cloudflare.com:3478 stun.l.google.com:19302

> **注意：**
>
> 外部用户的 HDX Direct 仅在使用 EDT (UDP) 作为传输协议时可用。因此，(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/hdx-transport/adaptive-transport.html) 必须启用。

注意事项

使用 HDX Direct 时需要考虑以下事项：

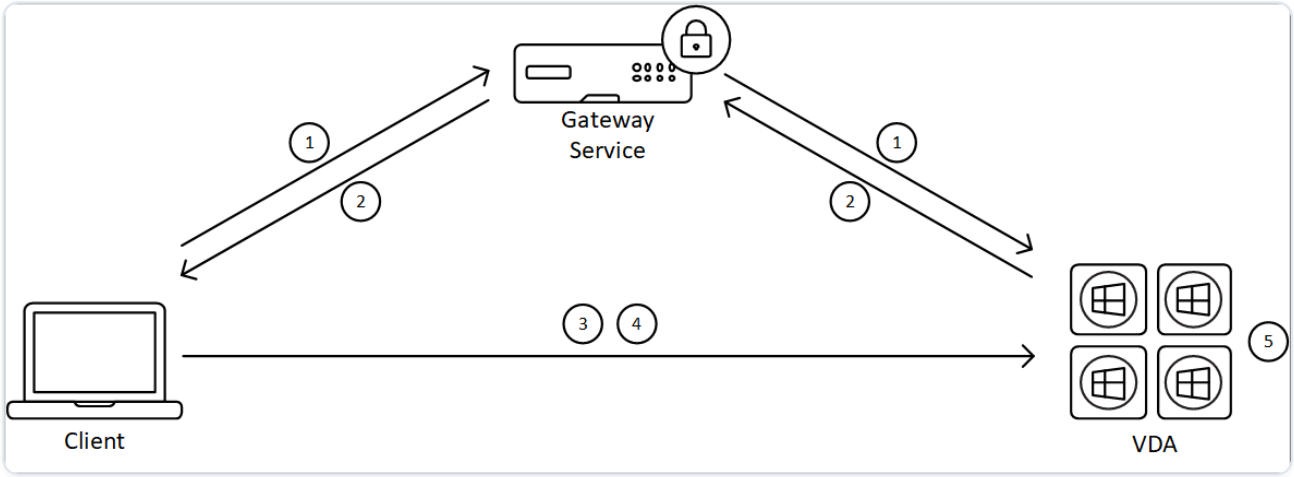
- 外部用户的 HDX Direct 仅在使用 EDT (UDP) 作为传输协议时可用。因此，必须启用 **自适应传输**。
- 如果您正在使用 **HDX Insight**，请注意，使用 **HDX Direct** 会阻止 HDX Insight 数据收集，因为会话将不再通过 NetScaler Gateway 代理。
- 在多会话主机环境中，HDX Direct 要求用户在一分钟内完成登录。如果登录时间超过此阈值，HDX Direct 将不会被触发，并且会话将保持通过网关连接。您可以增加 HDX Direct 超时时间以支持更长的登录时间。有关详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/policies/reference/hdx-registry-settings.html#hdx-direct)。

工作原理

当直接通信可用时，HDX Direct 允许客户端与会话主机建立直接连接。当使用 HDX Direct 建立直接连接时，将使用自签名证书通过网络级加密 (TLS/DTLS) 来保护直接连接。

内部用户

下图描述了内部用户的 HDX Direct 连接过程概述。



1. 客户端通过网关服务建立 HDX 会话。
2. 连接成功后，VDA 通过 HDX 连接向客户端发送 VDA 计算机的 FQDN、其 IP 地址列表以及 VDA 计算机的证书。
3. 客户端探测 IP 地址，以查看是否可以直接访问 VDA。
4. 如果客户端可以使用共享的任何 IP 地址直接访问 VDA，则客户端会与 VDA 建立直接连接，该连接使用与步骤 (2) 中交换的证书匹配的证书通过 (D)TLS 进行保护。
5. 直接连接成功建立后，会话将转移到新连接，并且与网关服务的连接将终止。

> **注意：**
>
> 在上述步骤 2 中建立连接后，会话处于活动状态。后续步骤不会延迟或干扰用户使用虚拟应用程序或桌面的能力。如果后续步骤中的任何一个失败，通过网关的连接将保持不变，而不会中断用户的会话。

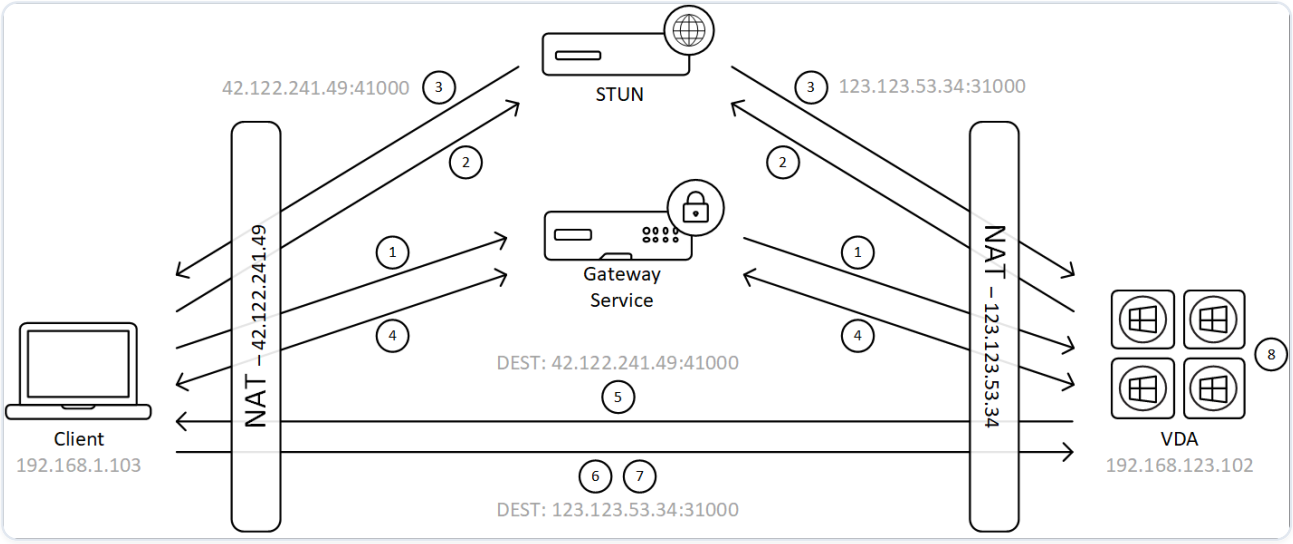
传统直接连接

当使用 Storefront、具有直接工作负载连接的 Workspace 或配置为仅限内部连接的 Workspace 时，客户端和会话主机之间会建立直接连接，而无需首先通过网关路由。

在这些情况下，由于连接本身就是直接的，因此不会触发 HDX Direct。但是，如果启用了 HDX Direct，这些连接将利用 HDX Direct 证书来保护会话。

外部用户

下图描绘了外部用户 HDX Direct 连接过程的概述：



1. 客户端通过网关服务建立 HDX 会话。
2. 连接成功后，客户端和 VDA 都会发送 STUN 请求以发现其公共 IP 地址和端口。
3. STUN 服务器向客户端和 VDA 响应其相应的公共 IP 地址和端口。
4. 通过 HDX 连接，客户端和 VDA 交换其公共 IP 地址和 UDP 端口，VDA 将其证书发送给客户端。
5. VDA 将 UDP 数据包发送到客户端的公共 IP 地址和 UDP 端口。客户端将 UDP 数据包发送到 VDA 的公共 IP 地址和 UDP 端口。
6. 收到来自 VDA 的消息后，客户端会响应一个安全连接请求。
7. 在 DTLS 握手期间，客户端会验证证书是否与步骤 (4) 中交换的证书匹配。验证后，客户端会发送其授权令牌。此时已建立安全的直接连接。
8. 直接连接成功建立后，会话将转移到新连接，并且与网关服务的连接将终止。

> **注意：**
>
> 在上述步骤 2 中建立连接后，会话处于活动状态。后续步骤不会延迟或干扰用户使用虚拟应用程序或桌面的能力。如果后续任何步骤失败，通过网关的连接将保持不变，而不会中断用户的会话。

证书管理

概述

HDX™ 直连通过网络级加密进行保护。为实现此目的，每个会话主机都具有唯一的自签名根 CA 证书和相应的服务器证书，该服务器证书由自签名根 CA 证书签名。

此解决方案具有以下优势：

- **简化安全性：** HDX 直连无需在环境中管理证书的管理开销即可获得保护。
- **减少攻击面：** 攻击面仅限于单个主机，因为每个主机都有一组唯一的密钥和证书。
- **增强非持久性环境的安全性：** 在具有非持久性会话主机的环境中，每次重新启动时都会生成新的密钥和证书，从而进一步增强了安全性。

会话主机

负责管理每个会话主机上证书的两个服务是 **Citrix ClxMtp Service** 和 **Citrix Certificate Manager Service**。ClxMtp Service 负责密钥生成和轮换，而 Certificate Manager Service 负责生成和管理证书。

将创建两个证书：自签名根 CA 和服务器证书。两者都具有两年有效期；但是，当密钥轮换时，它们会被替换。此外，每次非持久性计算机重新启动时都会生成新证书。

每个证书的详细信息如下：

- **自签名根 CA**
  - 颁发给：CA-Citrix-Certificate-Manager
  - 证书颁发机构：CA-Citrix-Certificate-Manager
  - 颁发者详细信息：组织为 Citrix Systems, Inc.
- **服务器证书**
  - 颁发给：\<主机 FQDN\>（例如，FTLW11-001.ctxlab.net）
  - 证书颁发机构：CA-Citrix-Certificate-Manager
  - 颁发者详细信息：组织为 Citrix Systems, Inc.

> **注意：**

> Citrix Certificate Manager Service 生成利用 2048 位密钥的 RSA 证书。

> 如果存在由 Citrix Certificate Manager Service 创建的现有计算机证书，并且主题名称与计算机的 FQDN 不匹配，则会生成新证书。

密钥轮换

Citrix ClxMtp Service 每六个月自动轮换密钥。但是，您可以通过增加会话主机注册表中的轮换计数器来手动触发密钥轮换。

要轮换密钥，请更新以下值：

- 键：SOFTWARE\Citrix\ClxMtpConnectorSvcRotateKeyPairs
- 值类型: DWORD
- 值名称：ClxMtpRotateRequestCounter
- 数据：整数（十进制）

> **注意：**

> 首次密钥轮换：

> 1. 创建 ClxMtpConnectorSvcRotateKeyPairs 键。
> 2. 创建 ClxMtpRotateRequestCounter 值并将其设置为 1。

> 对于后续密钥轮换，将 ClxMtpRotateRequestCounter 值增加 1。

> 值更新后， **Citrix ClxMtp Service** 将自动轮换密钥，无需重新启动。 **Citrix Certificate Manager Service** 在检测到新密钥后将自动生成新证书。

客户端设备

根 CA 证书通过已建立的安全可信连接路径由 Workspace 或 Storefront™ 发送到客户端。这消除了将 CA 证书分发到客户端设备的证书存储的需要，并确保客户端信任用于保护 HDX Direct 连接的证书。

使用自定义证书

HDX Direct 支持使用您自己的 PKI 颁发和管理的证书。以下步骤概述了如何安装证书、配置必要的权限、将其绑定到会话管理器服务以及启用所需的 TLS 侦听器。

1. 如果计算机上禁用了 HDX Direct，请继续执行步骤 2。如果启用了 HDX Direct，请按照以下步骤操作：

a. 打开注册表编辑器 (regedit.exe) 并导航到 **HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd**。
b. 将 **SSLEnabled** 值设置为 **0**。
c. 导航到 **HKLM\Software\Citrix\HDX-Direct**。
d. 将 **HdxDirectCaInTls** 值设置为 **0**。

2. 在计算机的证书存储中安装由您的 PKI 颁发的相应证书。
3. 授予会话管理器服务对证书私钥的读取访问权限。
   a. 启动 Microsoft 管理控制台 (**MMC**)：开始 > 运行 > mmc.exe。
   b. 导航到 **文件 > 添加/删除管理单元**。
   c. 选择 **证书**，然后单击 **添加**。
   d. 选择 **计算机帐户**，然后单击 **下一步**。
   e. 选择 **本地计算机**，然后单击 **完成**。
   f. 导航到 **证书 (本地计算机) > 个人 > 证书**。
   g. 右键单击相应的证书，然后选择 **所有任务 > 管理私钥**。
   h. 添加以下服务之一，并为其授予读取权限：
      - 对于 **单会话 VDA**：`NT SERVICE\PorticaService`
      - 对于 **多会话 VDA**：`NT SERVICE\TermService`
   i. 单击 **应用**，然后单击 **确定**。
4. 将证书绑定到会话管理器服务。
   a. 检索证书指纹（双击证书 > **详细信息** > **指纹**）。
   b. 打开注册表编辑器 (regedit.exe) 并导航到 **HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd**。
   c. 编辑 **SSLThumbprint** 值，并粘贴证书指纹。
5. 启用 Citrix TLS 侦听器。
   a. 在同一注册表位置，将 **SSLEnabled** 值设置为 **1**。
6. 启用 HDX Direct（在 Citrix 策略 中）。

Citrix Virtual Apps and Desktops 安装介质包含一个 PowerShell 脚本 (Enable-VdaSSL.ps1)，可自动执行其中几项任务：

- 设置证书密钥的权限
- 将证书绑定到会话管理器服务
- 启用 Citrix TLS 侦听器

此脚本位于 Support > Tools > SslSupport 目录中。有关详细信息，请参阅 使用 PowerShell 脚本在 VDA 上配置 TLS。

> **注意：**
>
> 如果您使用自己的证书，连接到会话主机的设备需要安装正确的根 CA 和中间 CA 证书。

NAT 兼容性

为了在外部用户设备和会话主机之间建立直接连接，HDX™ Direct 利用打洞技术进行 NAT 穿越，并使用 STUN 促进客户端设备和会话主机的公共 IP 地址和端口映射的交换。这类似于 VoIP、统一通信和 P2P 解决方案的工作方式。

只要防火墙和其他网络组件配置为允许 STUN 请求和 HDX 会话的 UDP 流量，外部用户的 HDX Direct 预计就能正常工作。但是，在某些情况下，用户和会话主机网络的 NAT 类型会导致不兼容的组合，从而导致 HDX Direct 失败。

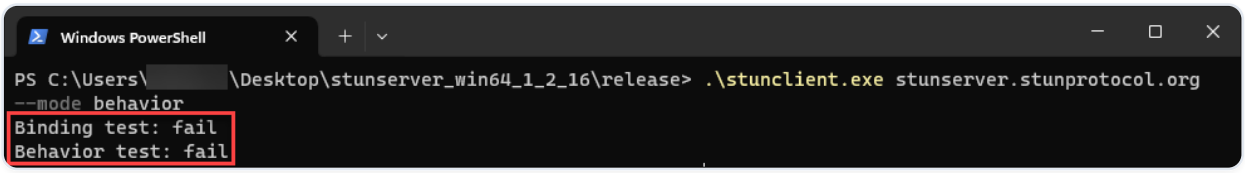
验证

您可以使用 STUNTMAN 的 STUN 客户端实用程序 验证客户端和会话主机上的 NAT 类型和过滤：

1. 从 stunprotocol.org 下载适用于目标平台的相应软件包，并解压内容。
2. 打开终端提示符并导航到内容解压的目录。
3. 运行以下命令执行 NAT 绑定和行为测试： `stunclient.exe stunserver2025.stunprotocol.org --mode behavior`
4. 如果绑定和行为测试成功，则**绑定测试**和**行为测试**都报告成功，并指定了 NAT 行为：



如果测试失败，则**绑定测试**和/或**行为测试**报告失败。



5. 运行以下命令执行 NAT 绑定和过滤测试：`stunclient.exe stunserver2025.stunprotocol.org --mode filtering`
6. 如果绑定和过滤测试成功，则**绑定测试**和**过滤测试**都报告成功，并指定了 NAT 过滤类型：

   如果测试失败，则**绑定测试**和/或**过滤测试**报告失败。

在执行上述测试后，请检查下表以确定外部用户的 HDX Direct 是否有望根据 NAT 行为和筛选组合工作：

客户端 NAT 行为	客户端 NAT 筛选	会话主机 NAT 行为	会话主机 NAT 筛选	预期会工作吗？
端点独立映射	任意	端点独立映射	任意	是
端点独立映射	端点无关过滤	地址相关映射	任意	是
端点独立映射	地址相关过滤	地址相关映射	任意	否
端点独立映射	地址和端口相关过滤	地址相关映射	任意	否
端点独立映射	端点无关过滤	地址和端口相关映射	端点无关过滤	是
端点独立映射	地址相关过滤	地址相关映射	任意	否
端点独立映射	地址和端口相关过滤	地址相关映射	任意	否
地址相关映射	任意	端点独立映射	端点无关过滤	是
地址相关映射	任意	端点独立映射	地址相关过滤	否
地址相关映射	任意	端点独立映射	地址和端口相关过滤	否
地址相关映射	任意	地址相关映射	任意	否

客户端 NAT 行为	客户端 NAT 筛选	会话主机 NAT 行为	会话主机 NAT 筛选	预期会工作吗？
地址相关映射	任意	地址和端口相关映射	任意	否
地址和端口相关映射	任意	端点独立映射	端点无关过滤	是
地址和端口相关映射	任意	端点独立映射	地址相关过滤	否
地址和端口相关映射	任意	端点独立映射	地址和端口相关过滤	否
地址和端口相关映射	任意	地址相关映射	任意	否
地址和端口相关映射	任意	地址和端口相关映射	任意	否
失败	任意	任意	任意	否
任意	任意	失败	任意	否
失败	任意	失败	任意	否

故障排除

要确认 **HDX Direct** 已成功建立直接连接，您可以在 VDA 计算机上使用 `CtxSession.exe` 实用程序。

要使用 `CtxSession.exe` 实用程序，请在会话中启动命令提示符或 PowerShell 并运行 `ctxsession.exe -v`。如果 **HDX Direct** 连接成功建立，则 **HDX Direct Status** 为 `Connected`。

HDX Direct 故障排除(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/hdx-direct-troubleshooting.png)

您还可以查看会话主机的事件日志，以了解 HDX™ Direct 连接是成功建立还是失败。有关详细信息，请参阅“**Event Logs**”部分。

> 注意：
>
> 根据环境以及会话主机可用的 IP 地址数量，HDX Direct 连接可能需要长达 5 分钟才能建立。

当 HDX Direct 无法建立直接连接时

如果 HDX Direct 无法建立直接连接，请查看以下步骤：

1. 确保所使用的 VDA 版本和 Workspace 应用程序版本根据系统要求支持该功能。
2. 确认已将策略应用于 VDA 以启用 HDX Direct，并且没有其他优先级更高的策略禁用该功能。
3. 确认已将策略应用于 VDA 以设置所需的 HDX Direct 模式，并且没有其他优先级更高的策略覆盖此配置。
4. 确保 Citrix ClxMtp Service 正在会话主机上运行。
5. 确保 Citrix Certificate Manager Service 正在会话主机上运行。如果未运行，请尝试手动启动它。如果 HDX Direct 被禁用，该服务将自动停止。
6. 检查会话主机是否具有其自签名根 CA 证书：
    a. 颁发给：`CA-Citrix-Certificate-Manager`
    b. 颁发者：`CA-Citrix-Certificate-Manager`
    c. 颁发者详细信息：组织为 Citrix Systems, Inc.
7. 检查会话主机是否具有其自签名服务器证书：
    a. 颁发给：`<host FQDN>`（例如，FTLW11-001.ctxlab.net）
    b. 颁发者：`CA-Citrix-Certificate-Manager`
    c. 颁发者详细信息：组织为 Citrix Systems, Inc.
8. 如果证书缺失，请联系 Citrix 技术支持。
9. 如果证书存在：
    a. 停止会话主机上的 Citrix Certificate Manager Service。
    b. 删除自签名根 CA 证书和自签名服务器证书。
    c. 启动会话主机上的 Citrix Certificate Manager Service。该服务启动后会创建新证书。
10. 对于内部用户：
    a. 确保会话主机的防火墙未阻止 UDP 443 或 TCP 443 上的入站流量，分别用于 HDX over EDT 和 HDX over TCP。

b. 确保您的网络防火墙未阻止客户端网络与会话主机网络之间 UDP 443 和 TCP 443 上的流量。

11. 对于外部用户：

a. 检查会话主机是否包含 STUN 服务器列表：

- 键: HKLM\SOFTWARE\Citrix\HDX-Direct
- 值类型: REG_MULTI_SZ
- 值名称: STUNServers
- 数据: stun.cloud.com:3478 stun.cloudflare.com:3478 stun.l.google.com:19302

b. 检查客户端和会话主机的 NAT 类型，并确保该组合能够正常工作。有关详细信息，请参阅 NAT 兼容性部分。

c. 如果 NAT 测试在客户端或会话主机上失败：

i. 如果系统上运行有防火墙，请确保它没有阻止通过 UDP 3478 的出站流量。

ii. 确保您的网络防火墙没有阻止通过 UDP 3478 的出站流量。

iii. 确保防火墙没有阻止 STUN 服务器的响应。

d. 确保您的网络防火墙已配置适当的规则以允许所有必要的流量。有关详细信息，请参阅网络要求部分。

e. 如果您使用 HDX Direct 端口范围策略设置更改了默认端口范围，请确保您的防火墙规则已针对自定义端口范围进行设置。

事件日志

以下事件记录在 VDA 计算机的事件日志中：

日志	ID	源	级别	描述
应用程序和服务日志 > Citrix-HostCore-HDX Direct/ Operational	1	HDX 直接	信息	内部用户 `<username>` 的 HDX Direct 连接已建立。
应用程序和服务日志 > Citrix-HostCore-HDX	2	HDX 直接	信息	外部用户 `<username>` 的 HDX Direct 连接已建立。

日志	ID	源	级别	描述
Direct/ Operational				
应用程序和服务日志 > Citrix-HostCore-HDX Direct/ Operational	3	HDX 直接	信息	用户 `<username>` 的 HDX Direct 连接失败。
应用程序和服务日志 > Citrix-HostCore-HDX Direct/ Operational	4	HDX 直接	信息	STUN 服务器 `<URL:PORT>` 为用户 `<username>` 提供了以下会话主机 IP 和端口映射：`<IP>:<PORT>` 。
应用程序和服务日志 > Citrix-HostCore-HDX Direct/ Operational	5	HDX 直接	信息	会话主机未从为用户 `<username>` 配置的任何 STUN 服务器接收到响应。
应用程序和服务日志 > Citrix-HostCore-HDX Direct/ Operational	6	HDX 直接	信息	客户端为用户 `<username>` 提供了 `<IP>:<PORT>` 作为外部映射。
应用程序和服务日志 > Citrix-HostCore-HDX Direct/ Operational	7	HDX 直接	信息	客户端未为用户 `<username>` 提供外部映射。

已知问题

- 如果 Rendezvous 被禁用，外部用户的 HDX Direct 在使用 Workspace with Gateway Service 的环境中可能会失败。要解决此问题，请确保 Rendezvous 已启用。
- 在对已启用 **HDX Direct** 的计算机执行 VDA 就地升级后，HDX Direct 可能会停止工作。要解决此问题，请完成以下步骤：

  a. 在会话主机上停止 Citrix Certificate Manager Service。

  b. 删除自签名根 CA 证书和自签名服务器证书。

  c. 打开注册表。

  d. 删除 `HKLM\Software\Citrix\HDX-Direct` 键。

  e. 转到 `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`。

  f. 将 **SSLEnabled** 值设置为 `0`。

  g. 删除 **SSLThumbprint** 值的内容。

  h. 启动 **Citrix 证书管理器服务**。

安全 HDX™

安全 HDX 是一种应用层加密 (ALE) 解决方案，可防止流量路径中的任何网络元素检查 HDX 流量。它通过在 Citrix Workspace™ 应用程序（客户端）和 VDA（会话主机）之间使用 AES-256-GCM 加密在应用层提供真正的端到端加密 (E2EE) 来实现此目的。

系统要求

以下列表描述了使用安全 HDX 的系统要求。

- 控制平面
  - 思杰 DaaS™
  - Citrix Virtual Apps and Desktops™ 2503 或更高版本
- 会话主机
  - 操作系统
    - Windows 10 22H2 版本
    - Windows 11 22H2 或更高版本
    - Windows Server 2019 或更高版本

    - 虚拟投递代理 (VDA)
        - Windows: 2503 或更高版本
        - Linux：版本 2407 或更高版本
- Workspace 应用程序
    - Windows: 2503 或更高版本
    - Linux: 2408 或更高版本
    - Mac: 2409 或更高版本
    - Chrome OS: 2409 或更高版本
    - HTML5: 2408 或更高版本
    - Android: 2503 或更高版本
    - iOS: 2503 或更高版本
- 访问层
    - 思杰工作区
    - Citrix StoreFront™ 2402 或更高版本

> **注意：**
>
> 有关使用 Linux VDA 配置 Secure HDX 的详细信息，请参阅 Linux VDA 文档。

配置

Secure HDX 默认处于禁用状态。您可以使用 Citrix 策略中的 Secure HDX 设置来配置此功能：

Secure HDX：定义是启用还是禁用此功能。

> **重要提示：**
>
> 如果要在要启用 Secure HDX 的交付组上启用了 Secure ICA®，则必须首先禁用 Secure ICA（编辑交付组 > 用户设置）。

HDX 洞察 和 智能控制

在启用 Secure HDX 的情况下，将 HDX Insight 和 SmartControl 与 NetScaler Gateway 结合使用的要求如下：

- NetScaler 14.1 Build 47.46 或更高版本。
- **网络遥测**必须在 Citrix 策略中启用。
- 必须启用**会话可靠性**。此设置默认启用，因此请确保没有禁用此设置的策略。

> **注意：**
>
> 带 Secure HDX 的 HDX Insight 和 SmartControl 仅在以下情况下可用：
>
> - 使用 TCP 作为传输协议的连接
> - 使用 IPv4 的连接
> - 使用以下 Workspace 应用程序版本的客户端：
>   - Windows: 2503 或更高版本
>   - Mac: 2505 或更高版本
>   - Linux: 2508 或更高版本

注意事项

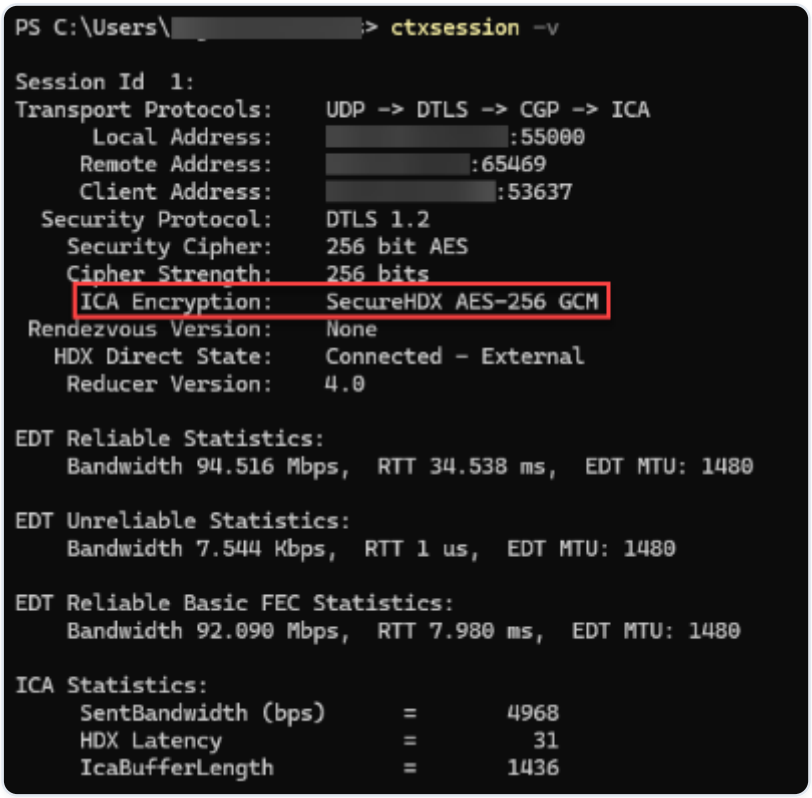
以下是使用 Secure HDX 的注意事项：

- 如果用户尝试使用不支持该功能的客户端连接到启用了 Secure HDX 的会话主机，则连接将被拒绝。
- 只有 无连接器工作负载的服务连续性 支持 Secure HDX。如果您使用的是标准版服务连续性，则在发生云服务中断时，将无法连接到任何启用了 Secure HDX 的会话主机。
- 启用 Secure HDX 时，不支持多流 ICA。
- 如果您使用任何依赖于检查 HDX 流量的第三方解决方案，那么在您启用 Secure HDX 后，它们将不再起作用，因为 HDX 流量已加密。

故障排除

要确认 Secure HDX 已激活，您可以在 VDA 计算机上使用 `ctxsession.exe` 实用程序。

要使用 `CtxSession.exe` 实用程序，请在会话中打开命令提示符或 PowerShell 并运行 `ctxsession.exe -v`。如果正在使用 Secure HDX，ICA 加密将显示 `SecureHDX AES-256 GCM`。



会话中未启用 Secure HDX 时

- 确保所使用的 VDA 版本根据系统要求支持该功能。
- 确认您已将启用 Secure HDX 的策略应用于 VDA，并且没有其他优先级更高的策略禁用该功能。
- 如果在配置 Secure HDX 时会话主机已在运行，请重新启动计算机以确保更改生效。

网络遥测

网络指标对于 Citrix 会话故障排除至关重要，因为 Citrix 会话的性能和稳定性在很大程度上取决于底层网络条件。与本地应用程序不同，Citrix 会话涉及通过网络流式传输交互式桌面或应用程序体验，这意味着任何网络不稳定或瓶颈都会直接影响用户对性能的感知。

有关 Citrix Monitor 和 Director 中可用的网络指标的详细信息，请参阅诊断会话性能问题。

系统要求

以下是使用网络遥测的系统要求：

- 控制平面
  - 思杰桌面即服务
  - Citrix Virtual Apps and Desktops 2503 或更高版本
- 虚拟交付代理 (VDA)
  - Windows：版本 2503 或更高版本
  - Linux：版本 2507 或更高版本
  - Mac：版本 2507 或更高版本
- Workspace 应用程序
  - Windows：版本 2503 或更高版本
  - Linux：版本 2508 或更高版本
  - Mac: 2505 版或更高版本
- 访问层
  - 思杰工作区
  - Citrix Storefront 2402 或更高版本
  - Citrix 网关服务
  - Citrix NetScaler Gateway 14.1 Build 47.46 或更高版本

网络要求

如果您使用的是 Citrix Gateway Service，则没有其他网络要求。但是，如果您使用的是 NetScaler Gateway，则使用网络遥测需要满足其他要求，如下所述。

会话主机

如果您的会话主机具有防火墙（例如 Windows Defender 防火墙），则必须允许来自 NetScaler Gateway 连接的以下入站流量。

描述	源	协议	端口
来自 NetScaler Gateway 的连接	NetScaler SNIP	TCP	443

> **注意：**

> VDA 安装程序会将相应的入站规则添加到 Windows Defender 防火墙。如果您使用其他防火墙，则必须添加上述规则。

内部网络

以下是您的内部网络的防火墙要求：

描述	协议	源	源端口	目标	目标端口
来自网关的连接	TCP	NetScaler SNIP	1024-65535	VDA 网络	443

配置

网络遥测默认禁用。您可以使用以下设置在 Studio 中通过 Citrix 策略配置此功能。

- **网络遥测：** 定义是启用还是禁用此功能。

注意事项

以下是使用网络遥测的注意事项：

- 为确保传输中的监控数据安全，启用网络遥测时，从 NetScaler Gateway 到会话主机的连接通过 TLS/DTLS 进行保护。因此，默认情况下，连接在 UDP 443 端口（通过 EDT 的 HDX）和 TCP 443 端口（通过 TCP 的 HDX）上建立。如果您希望更改端口号，请参阅通过注册表管理的 HDX 功能。
- 自管理证书用于促进会话连接的网络级加密。有关证书管理的详细信息，请参阅HDX Direct 证书管理。请注意，启用网络遥测不会启用 HDX Direct。
- 目前，当网络遥测启用时，NetScaler Gateway 不支持 EDT；启用网络遥测会强制会话使用 TCP。

虚拟通道允许列表

虚拟通道允许列表是一项功能，可让您控制环境中允许哪些非 Citrix 虚拟通道。默认情况下，虚拟通道允许列表功能处于启用状态。因此，只有 Citrix 虚拟通道才允许在 Citrix Virtual Apps and Desktops™ 会话中打开。如果需要使用自定义虚拟通道（无论是自行开发还是来自第三方），则需要将其显式添加到允许列表中。

配置

虚拟通道允许列表默认处于启用状态。您可以使用 Citrix 策略中的以下设置来配置此功能：

- **虚拟通道允许列表**：用于启用或禁用该功能并将虚拟通道添加到列表中。
- **虚拟通道允许列表日志限制**：设置虚拟通道允许列表事件日志记录的限制周期。
- **虚拟通道允许列表日志记录**：设置虚拟通道允许列表的日志记录级别。

将虚拟通道添加到允许列表

要将虚拟通道添加到允许列表，您需要以下信息：

1. 代码中定义的虚拟通道名称，最多可包含七个字符。例如，`CTXCVC1`。
2. 在 VDA 计算机上打开虚拟通道的进程路径。例如，`C:\Program Files\Application\run.exe`。

获得所需信息后，您必须使用虚拟通道允许列表策略设置将虚拟通道添加到允许列表。要将虚拟通道添加到列表中，请输入虚拟通道名称，后跟逗号，然后是访问虚拟通道的进程路径。如果有多个进程，可以通过用逗号分隔每个进程来添加这些进程。

对于单个进程

使用前面的示例，将以下条目添加到列表中：

```
CTXCVC1,C:\Program Files\Application\run.exe
```

对于多个进程

如果存在多个进程，请将以下条目添加到列表中：

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

使用通配符

支持使用通配符 (*)。当目录或可执行文件的名称根据应用程序版本而变化，或者第三方组件安装在用户配置文件中时，可以使用通配符。

您可以在以下场景中使用通配符：

- 替换完整的目录名称。 例如：`C:\Program Files\Application*\run1.exe`
- 替换目录名称的一部分。 例如：`C:\Program Files\Application\v*\run1.exe`
- 替换可执行文件的名称。 例如：`C:\Program Files\Application\v1.2*.exe`

- 替换可执行文件名称的一部分。 例如：`C:\Program Files\Application\v1.2\run*.exe`

适用以下限制：

- 通配符只能用于替换单个目录。例如，如果可执行文件位于 `C:\Program Files\Application\v1.2\run1.exe`
  - 允许：`C:\Program Files\Application*\run1.exe`
  - 不允许：`C:\Program Files*\run1.exe`
- 条目必须包含文件扩展名。
  - 允许：`C:\Program Files\Application\v1.2*.exe`
  - 不允许：`C:\Program Files\Application\v1.2*`
- 所有路径都必须是本地路径。

> **注意：**
>
> - 不允许使用网络路径。
> - 通配符支持从 Citrix Virtual Apps and Desktops™ 2206 开始提供。
> - Citrix Virtual Apps and Desktops 2203 LTSR 从 CU2 开始支持通配符。

使用系统环境变量

您可以使用系统环境变量来简化允许列表中受信任进程的定义。您可以使用任何开箱即用的变量，例如 `%programfiles%`、`%programfiles(x86)%`、`%systemdrive%` 和 `%systemroot%`。

只要在系统级别定义了自定义环境变量，您也可以使用它们。

以下示例描述了开箱即用的环境变量：

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

以下示例描述了自定义系统环境变量：

- 自定义变量名称：`app`

- 自定义变量值：`%programfiles%\Application\`
- 允许列表条目：`CTXCVC1,%app%\run.exe`

> **注意：**

> 不支持用户环境变量。

> 环境变量支持从 Citrix Virtual Apps and Desktops 2209 版开始提供。

获取虚拟通道名称和进程

获取虚拟通道名称以及在 VDA 计算机上打开该通道的进程的最简单方法是，从提供该虚拟通道的开发人员或第三方供应商处获取信息。

或者，您可以通过应用功能的日志并按照以下步骤获取信息：

1. 自定义虚拟通道的客户端和服务器组件就位后，启动虚拟应用程序或虚拟桌面。
2. 在 VDA 计算机的系统事件日志中，查找自定义虚拟通道的名称以及尝试打开它的进程。有关可用事件的更多信息，请参阅事件日志。
3. 从会话中注销。
4. 在虚拟通道允许列表策略设置中为已识别的虚拟通道和进程添加条目。
5. 重新启动计算机。
6. VDA 注册后，运行虚拟应用程序或虚拟桌面以验证自定义虚拟通道是否成功打开。

Citrix 虚拟通道的注意事项

所有内置的 Citrix 虚拟通道都受信任，无需进一步配置即可打开。但是，以下两个功能由于外部依赖项，需要在允许列表中明确条目：

- 多媒体重定向
- 适用于 Skype for Business 的 HDX RealTime 优化包

多媒体重定向

如果您使用 Windows Media Player 以外的媒体播放器作为系统媒体播放器，则需要将其作为受信任的进程添加到允许列表中。允许列表条目需要以下信息：

- 虚拟通道名称：`CTXMM`

- 进程：VDA 计算机中使用的媒体播放器的路径。例如，`C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 允许列表条目：`CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

适用于 Skype for Business 的 HDX RealTime 优化包

允许列表条目需要以下信息：

- 虚拟通道名称：`CTXRMEP`
- 进程：VDA 计算机中 Skype for Business 可执行文件的路径，该路径可能因 Skype for Business 的版本或您是否使用了自定义安装路径而异。例如，`C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 允许列表条目：`CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

第三方虚拟通道的注意事项

选定的第三方虚拟通道受信任，并允许在无需进一步配置的情况下打开。所有其他第三方虚拟通道都需要在允许列表中明确条目。受信任的第三方虚拟通道包括：

- 微软团队
- 适用于 VDI 的 Zoom Meetings

> **重要提示：**
>
> 仅当关联应用程序安装在其默认安装路径中时，受信任的第三方虚拟通道才会自动受信任。如果应用程序安装在不同的路径中，则必须将虚拟通道明确添加到允许列表中。

微软团队

以下是 Microsoft Teams 虚拟通道和进程的默认安装路径：

- 虚拟通道名称：`MSTEAMS`、`MSTEAM1` 和 `MSTEAM2`
- 进程：`ms-teams.exe`
- 默认安装路径：`C:\Program Files\WindowsApps\MSTeams.<app version>_x64_8wekyb3d8bbwe\`

有关 Microsoft Teams 虚拟通道的其他信息，请参阅Microsoft 文档。

适用于 VDI 的 Zoom Meetings

以下是适用于 VDI 的 Zoom Meetings 虚拟通道和进程的默认安装路径：

- 虚拟通道名称：`ZOOMHDX`、`ZOOMHDC`、`ZOOMPHX`、`ZOOMCVX`、`ZOOMCCX`、`ZOOMAUS`
- 进程：`Zoom.exe` 和 `ZoomVDITool.exe`
- 默认安装路径：
  - 32 位: `C:\Program Files (x86)\ZoomVDI\bin\`
  - 64 位: `C:\Program Files\ZoomVDI\bin\`

有关适用于 VDI 的 Zoom Meetings 虚拟通道的更多信息，请参阅 Zoom 文档。

故障排除

如果您的自定义虚拟通道无法打开，请查看以下步骤：

1. 确保您使用的是正确的 VDA 版本。
2. 确认您已将包含自定义虚拟通道的策略应用到 VDA 的虚拟通道允许列表中，并且没有其他优先级更高的策略覆盖此配置。
3. 检查 VDA 中的事件日志，确认报告的虚拟通道名称与允许列表中定义的名称匹配。
   a. 如果您有多个进程，请确保按照 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/secure/virtual-channel-security.html#adding-virtual-channels-to-the-allow-list) 中所述正确定义这些进程。
   b. 如果您在定义的进程路径中使用通配符，请确保您遵守 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/secure/virtual-channel-security.html#using-wildcards) 中的准则。
   c. 如果您在定义的进程路径中使用环境变量，请确保您遵守 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/secure/virtual-channel-security.html#using-system-environment-variables) 中的准则。

事件日志

以下事件记录在 VDA 计算机的事件日志中。

单会话 VDA

以下事件记录在单会话 VDA 计算机的事件日志中：

日志名称	ID	源	级别	描述
系统	2001	`Picadd`	信息	自定义虚拟通道 `<vcName>` 已

日志名称	ID	源	级别	描述
				由进程 `<processName>` 打开
系统	2002	`Picadd`	警告	自定义虚拟通道 `<vcName>` 无法由进程 `<processName>` 打开
系统	2003	`Picadd`	信息	`<username>` 打开了自定义虚拟通道 `<vcName>`
系统	2004	`Picadd`	警告	`<username>` 尝试打开自定义虚拟通道 `<vcName>`
系统	2005	`Picadd`	错误	策略 `<pathInPolicy>` 中给定的路径无法解析为进程路径
系统	2007	`Picadd`	信息	加载的进程路径为 `<processPath>`
系统	2008	`Picadd`	错误	在 VC 策略路径中找不到环境变量 `<varName>`

多会话 VDA

以下事件记录在多会话 VDA 计算机的事件日志中：

日志名称	ID	源	级别	描述
系统	13	`Rpm`	信息	自定义虚拟通道 `<vcName>` 已由进程 `<processName>` 打开
系统	14	`Rpm`	警告	自定义虚拟通道 `<vcName>` 无法由进程 `<processName>` 打开
系统	15	`Rpm`	信息	`<username>` 打开了自定义虚拟通道 `<vcName>`
系统	16	`Rpm`	警告	`<username>` 尝试打开自定义虚拟通道 `<vcName>`
系统	17	`Rpm`	错误	策略 `<pathInPolicy>` 中给定的路径无法解析为进程路径
系统	18	`Rpm`	信息	加载的进程路径为 `<processPath>`
系统	19	`Rpm`	错误	在 VC 策略路径中未找到环境变量 `<varName>`

已知第三方虚拟通道

以下是使用自定义 Citrix® 虚拟通道的已知第三方解决方案。此列表不包含所有使用自定义 Citrix 虚拟通道的解决方案。

- 赛纳
- ControlUp
- 思科 WebEx Teams
- 思科 WebEx Meetings 虚拟桌面软件
- 史诗曲速引擎
- 史诗弹射
- Imprivata 单点登录
- 微软团队
- Midmark IQPath 客户端扩展
- Nuance PowerMic 客户端扩展
- 纽昂斯 龙 医疗网络版 360 vSync
- Zoom VDI 会议
- 奥特玛 IA-Connect

要获取将相关虚拟通道添加到允许列表的详细信息，请联系解决方案供应商。或者，按照 获取虚拟通道名称和进程 部分中概述的步骤操作。

DVC 虚拟通道允许列表

您可以使用 DVC 虚拟通道允许列表来控制环境中允许哪些自定义动态虚拟通道。默认情况下，不允许任何动态虚拟通道。如果需要动态虚拟通道，则需要将其显式添加到允许列表中。

配置

DVC 虚拟通道允许列表默认启用。您可以使用 Citrix® 策略中的以下设置配置此功能：

- DVC 虚拟通道允许列表：用于启用或禁用此功能，并将动态虚拟通道添加到列表中。
- 虚拟通道允许列表日志节流：设置虚拟通道允许列表事件日志记录的节流周期。
- 虚拟通道允许列表日志记录：设置虚拟通道允许列表的日志记录级别。

将动态虚拟通道添加到允许列表

要将动态虚拟通道添加到允许列表，您需要以下信息：

1. 客户端上的 DVC 插件名称。例如，`DvcPlugin1.dll`。
2. DVC 侦听器名称。例如，`ListenerName1`。
3. 访问 VDA 计算机上动态虚拟通道的进程路径。例如，`C:\Program Files\Application\run.exe`。

获取所需信息后，您必须使用 DVC 虚拟通道允许 列表策略设置将动态虚拟通道添加到允许列表。要将动态虚拟通道添加到列表中，请输入会话主机中访问 DVC 的进程路径，后跟逗号，然后是客户端插件名称，后跟逗号，以及插件使用的侦听器名称。可以添加多个侦听器名称，用逗号分隔。

对于单个侦听器

使用前面的示例，将以下条目添加到列表中：`C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1`

对于多个侦听器

如果存在多个侦听器，请将以下条目添加到列表中：`C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1,ListenerName2`

使用通配符

支持使用通配符 (*)。当目录或可执行文件的名称根据应用程序版本而变化，或者第三方组件安装在用户配置文件中时，可以使用通配符。

您可以在以下场景中使用通配符：

- 替换完整的目录名称。例如：`C:\Program Files\App*\run1.exe`
- 替换目录名称的一部分。例如：`C:\Program Files\App\v*\run1.exe`
- 替换可执行文件的名称。例如：`C:\Program Files\App\v1.2*.exe`
- 替换可执行文件名称的一部分。例如：`C:\Program Files\App\v1.2\run*.exe`

适用以下限制：

- 通配符只能用于替换单个目录。例如，如果可执行文件位于 `C:\Program Files\App\v1.2\run1.exe`
  - 允许：`C:\Program Files\App*\run1.exe`
  - 不允许：`C:\Program Files*\run1.exe`
- 条目必须包含文件扩展名。
  - 允许：`C:\Program Files\App\v1.2*.exe`

    - 不允许：`C:\Program Files\App\v1.2*`

- 所有路径都必须是本地路径。

设备

HDX™ 可在任何设备、任何位置提供高清用户体验。“设备”部分中的文章介绍了以下设备：

- 扫描
- 通用 USB 设备
- 客户端驱动器映射
- 移动和触摸屏设备
- 串行设备
- 专用键盘
- 网络摄像头

优化型 USB 设备与通用型 USB 设备

优化型 USB 设备是指 Citrix Workspace™ 应用程序提供特定支持的设备。例如，能够使用 HDX 多媒体虚拟通道重定向网络摄像头。通用设备是指 Citrix Workspace 应用程序中没有特定支持的 USB 设备。

默认情况下，通用 USB 重定向无法重定向具有优化虚拟通道支持的 USB 设备，除非将其置于通用模式。

通常，USB 设备在优化模式下的性能优于通用模式。但是，在某些情况下，USB 设备在优化模式下无法提供完整功能。此时可能需要切换到通用模式才能完全访问其功能。

对于 USB 大容量存储设备，您可以使用客户端驱动器映射或通用 USB 重定向，或两者结合，具体由 Citrix® 策略控制。主要区别在于：

如果通用 USB 重定向和客户端驱动器映射策略都已启用，并且在大容量存储设备在会话开始之前或之后插入，则会使用客户端驱动器映射对其进行重定向。

当这些条件成立时，大容量存储设备将使用通用 USB 重定向：

- 通用 USB 重定向和客户端驱动器映射策略都已启用。
- 设备已配置为自动重定向。
- 大容量存储设备在会话开始之前或之后插入。

有关详细信息，请参阅 `<http://support.citrix.com/article/CTX123015>`。

功能	客户端驱动器映射	通用 USB 重定向
默认启用	是	否
可配置只读访问	是	否
加密设备访问	是，如果加密在设备于虚拟会话中访问之前已解锁。	仅适用于 Citrix Virtual Desktops™

扫描

扫描仪是一种设备，可以光学扫描图像、打印文本、手写内容或物体，并将其转换为数字图像。

如果您正在使用扫描仪，并且您的计算机运行的是 Windows 系统，您很有可能正在使用 WIA 扫描仪驱动程序。该驱动程序负责您的计算机和扫描仪之间的通信。

- **Windows 图像采集** (WIA) 是 Microsoft 的驱动程序模型和应用程序编程接口 (API)，它使软件能够与扫描仪等成像硬件进行通信。
- **TWAIN**（Windows 和 Mac）是另一种协议，它是一种扫描协议，通过提供标准接口将扫描仪和应用程序连接在一起。TWAIN 允许应用程序从符合 TWAIN 标准的设备（扫描仪、数码相机等）获取图像。
- **SANE**：扫描协议是一套标准和指南，允许软件应用程序与图像扫描仪进行通信和控制。SANE 代表 **S**canner **A**ccess **N**ow **E**asy（扫描仪现在易于访问），其协议定义了不同计算机系统上运行的软件如何访问、管理和控制扫描仪硬件。

TWAIN 重定向

简介

用户可以使用 Citrix HDX™ 会话中的应用程序扫描文档，使用连接到客户端端点的 TWAIN 兼容扫描仪。Citrix 扫描模块将扫描请求重定向到客户端端点以处理该请求。完成后，扫描的信息将发送回 VDA 主机。

要求

Citrix 控制平面

- Citrix Virtual Apps and Desktops™ 1912 或更高版本
- 思杰 DaaS™

会话主机

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows 十一
  - Windows Server 2022 或更高版本
- VDA
  - 版本 1912 或更高版本
- 应用程序
  - 32 位应用程序
  - 64 位应用程序

> **注意：**
>
> - 要在会话主机上为 64 位应用程序启用扫描功能，需要 64 位 TWAIN 数据源管理器 (twaindsm.dll)。操作系统不会预安装此组件。
> - 如果您的 64 位扫描应用程序不包含此文件，请联系应用程序供应商以获取 64 位 twaindsm.dll。
> - 获取后，管理员必须手动将文件复制到会话主机上的 **System32** 文件夹中，然后重新启动计算机。

客户端设备

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows 十一
- Workspace 应用程序
  - Windows：版本 1912 或更高版本
- 扫描仪
  - TWAIN 兼容扫描仪

- 在客户端端点上安装 TWAIN 驱动程序

配置

TWAIN 重定向默认启用。以下策略设置可用于配置 TWAIN 重定向并优化扫描体验。

- **客户端 TWAIN 设备重定向：** 用于启用或禁用 TWAIN 重定向。
- **TWAIN 压缩级别：** 用于设置从客户端传输到 VDA 的图像的压缩级别。

有关更多详细信息，请参阅TWAIN 设备策略设置。

故障排除

TWAIN 重定向功能可以使用公开可用的测试应用程序 Twacker 进行测试，该应用程序可从此URL下载。

请按照以下步骤验证 HDX 会话中的 TWAIN 功能：

1. 在 VDA 主机上安装 **Twacker**。
2. 启动 **Twacker**（32 位或 64 位版本）。
3. 单击**文件 > 选择源**，然后从列表中选择您的扫描仪。
4. 单击**文件 > 获取**。
5. 单击**扫描按钮**以测试您的扫描仪。

如果 **Twacker** 可以成功扫描，则表明 **Citrix Virtual Apps and Desktops™** 设置为：

- 已正确配置为使用 TWAIN 重定向
- 满足所有本地客户端设备要求

如果您在特定应用程序中仍然存在扫描问题，则很可能是软件问题。

WIA 设备

WIA 设备（例如数码相机和扫描仪）通过使用 WIA 框架与服务器托管的图像处理应用程序通信。

先决条件

- 扫描仪必须符合 WIA 标准。
- 在本地设备上安装 WIA 驱动程序。服务器上不需要这些驱动程序。
- 在本地连接扫描仪（例如，通过 USB）。
- 确保扫描仪使用的是本地 Windows 图像采集服务，而不是 TWAIN 驱动程序。

- 确保用于测试的用户帐户未应用任何策略，并且该策略未限制 ICA® 会话中的带宽。例如，客户端 USB 重定向带宽限制。

要求

会话主机

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows 十一
  - Windows Server 2022 或更高版本
- VDA
  - 版本 2511 或更高版本

客户端设备

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows 十一
- Workspace 应用程序
  - Windows: 版本 2411 或更高版本

配置

WIA 重定向默认处于禁用状态。可以在 Citrix® 策略中启用以下设置：

- WIA 重定向：此设置允许或禁止用户访问用户设备上的 WIA 设备。

在 Citrix Virtual Apps and Desktops 2511 或更高版本上，无需进行额外的 VDA 端注册表修改。

已知问题

有关策略设置的信息，请参阅 WIA 设备策略设置。

非 Windows 客户端平台上的扫描 - SANE 重定向

简介

用户可以从 ChromeOS 和 Linux 端点，在其 Citrix® 会话中的 TWAIN 应用程序内扫描文档。当用户尝试从应用程序扫描文档时，Citrix 扫描模块会将请求重定向到客户端端点，以实现从扫描仪进行扫描，并在扫描完成后将文件发送到 VDA。

要求

Citrix 控制平面

- Citrix Virtual Apps and Desktops™ 2411 或更高版本
- 思杰 DaaS™

会话主机

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows 十一
  - Windows Server 2019 或更高版本
- VDA
  - 版本 2411 或更高版本

客户端设备

- 操作系统
  - ChromeOS v129 或更高版本
- Workspace 应用程序
  - ChromeOS: 版本 2409 或更高版本
  - Linux: 版本 2508.10 或更高版本
- 扫描仪
  - 扫描仪必须受底层客户端操作系统支持。
  - 必须通过 USB 本地连接到客户端端点。

配置

无需额外配置即可启用此功能。此功能默认启用。

> **注意：**
>
> 要禁用此功能，请打开 Web Studio/DaaS 控制台。将 SANE 扫描仪重定向策略设置设为“已禁用”。

故障排除

事件日志

管理员可以查看各种与扫描相关的事件消息。

下面列出了将在 VDA 主机上的事件查看器中记录的各种与扫描相关的操作的事件消息。可以在 Windows 日志的“应用程序”部分下查看这些消息，事件源为 HDX™ Scanner。

事件 ID	事件文本	说明
2	AllowScannerSANERedirection 策略已禁用。扫描仪未重定向。	表示 SaneRedirection 策略已禁用。
3	扫描详细信息：页数 - '[pages]'，应用程序 - '[application]'，扫描仪 - '[scanner]'，用户 - '[user]'，每页平均时间 - '[time]' 毫秒。	扫描完成后生成。
101	未找到要扫描的页面。	未检测到文档时生成。
102	扫描失败 - 设备文档进纸器卡纸。	当扫描仪文档进纸器卡纸导致扫描失败时生成。
103	扫描失败 - '[failure]'。请关闭并重新启动扫描仪应用程序。	当扫描因不支持的操作、文件结束错误、访问被拒绝错误等原因失败时生成。
104	应用程序内存故障。请重启应用程序。	当扫描因内存不足而失败时生成。

事件 ID	事件文本	说明
201	用户取消了扫描操作。	当用户取消扫描操作时生成。
202	扫描时会话已断开连接。	当 HDX 会话在扫描时断开连接时生成。
203	TWAIN 和 SANE 之间对“[capability]”的转换不受支持。请检查扫描仪/应用程序是否受支持。	表示 TWAIN 和 SANE 之间对指定功能的转换不受支持。
205	无法将扫描仪“[scanner]”设置为活动状态。请检查扫描仪是否已开启并连接。	当无法打开与扫描仪的连接时生成。
206	未找到扫描仪。请检查扫描仪是否已开启并连接。	当客户端端点上未检测到扫描仪时生成。

已知限制

1. 不支持网络授权的扫描仪。
2. 某些专有扫描应用程序（例如 VDA 上的 Fujitsu Paperstream 应用程序）可能不会将重定向的扫描仪列为受支持。
3. 使用本机 UI 时，由于第三方 API 限制，某些扫描仪设置（例如页面宽度、页面高度、纸张尺寸、亮度和对比度）可能无法生效。

USB 设备

简介

通用 USB 重定向功能允许将 USB 设备从客户端计算机重定向到 HDX™ 会话，从而使用户能够在其 HDX 会话中与各种通用 USB 设备进行交互。这在用户需要使用没有优化支持或不适合的专用设备时非常有用。

> **注意：**
>
> 未针对虚拟通道支持进行优化的 USB 设备将回退到使用原始 USB 重定向的通用 USB 虚拟通道。

工作原理?

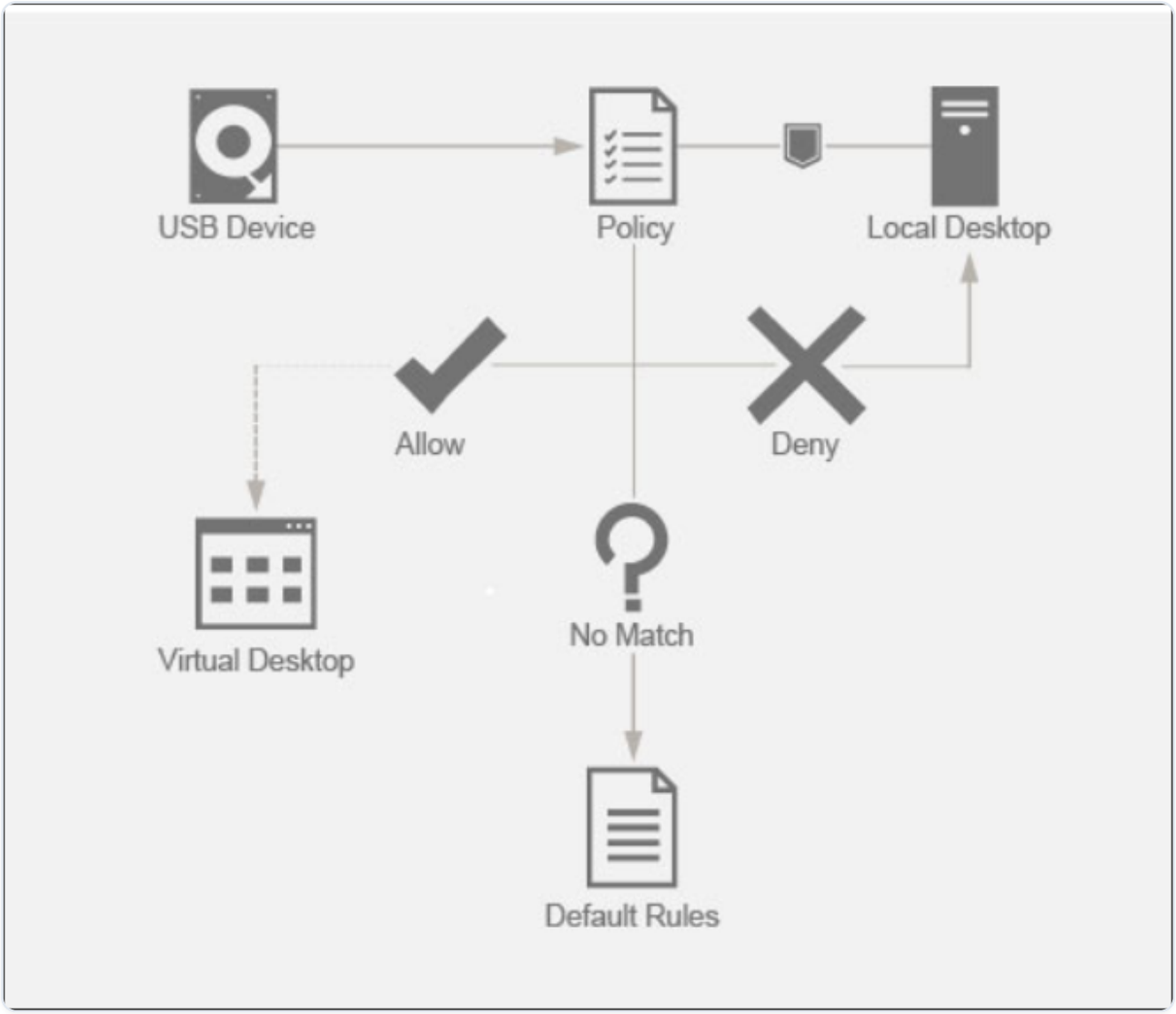
通用 USB 重定向在低级别工作，并在客户端计算机和 XenDesktop® 虚拟桌面之间重定向 USB 请求和响应消息。

它避免了客户端计算机上对兼容设备驱动程序的要求，并且驱动程序预计仅在虚拟桌面上受支持。USB 重定向策略规则遵循特定的优先级顺序，允许在评估和实施 DDC 策略规则后遵循客户端策略和默认规则。这允许 Citrix 管理员阻止任何未经授权/欺骗的设备在会话中被重定向。

此外，可以对尝试访问远程会话的未经授权设备的事件日志进行审计和标记，管理员可以采取额外措施来防止数据泄露。

当用户插入 USB 设备时，会话主机将根据每个策略规则连续检查该设备，直到找到匹配项。任何设备的第一个匹配项都被视为最终结果。

- 如果第一个匹配项是“允许”规则，则设备将重定向到虚拟桌面。
- 如果第一个匹配项是“拒绝”规则，则设备不会重定向到会话，并且只能在本地用户设备中使用。如果未找到匹配项，则使用默认规则。



与通用 USB 重定向的兼容性

以下 Citrix Workspace™ 应用程序支持通用 USB 重定向：

- 适用于 Windows 的 Citrix Workspace 应用程序，请参阅 适用于 Windows 的 Citrix Workspace 应用程序。
- 适用于 Mac 的 Citrix Workspace 应用程序，请参阅 适用于 Mac 的 Citrix Workspace 应用程序。
- 适用于 Linux 的 Citrix Workspace 应用程序，请参阅 适用于 Linux 的 Citrix Workspace 应用程序。
- 适用于 Chrome OS 的 Citrix Workspace 应用程序，请参阅适用于 Chrome 的 Citrix Workspace 应用程序。

对于 Citrix Workspace 应用程序版本，请参阅Citrix Workspace 应用程序功能矩阵。

配置

USB 重定向默认处于禁用状态。您可以使用 Citrix® 策略中的以下设置配置通用 USB 重定向：

- **客户端 USB 设备重定向**：用于启用或禁用 USB 重定向
- **客户端 USB 设备重定向规则**：用于指定特定的设备操作，即允许或拒绝访问特定设备
- **客户端 USB 设备重定向规则（版本 2）**：用于指定过滤、拆分和自动连接 USB 设备的规则
- **客户端 USB 设备优化规则**：用于禁用优化或更改优化模式
- **允许自动连接现有 USB 设备**：用于允许或阻止在 HDX™ 会话开始时自动连接连接到客户端端点的现有 USB 设备
- **允许自动检测新到达的 USB 设备**：用于允许或阻止在 HDX 会话期间自动连接连接到客户端端点的 USB 设备

请参阅 USB Policy Settings 了解更多详细信息。

如何配置 USB 重定向

默认情况下，USB 重定向配置处于禁用状态。要使用它，必须在 DDC 上启用并配置 USB 重定向策略和特定的重定向规则。

> **注意：**
>
> 如果您使用的任何组件版本低于 2212，或者您正在使用适用于 Linux/Mac 的 Workspace 应用程序，请参阅 Legacy USB Redirection Configuration 了解如何配置 USB 重定向的详细信息。

启用通用 USB 重定向

1. 打开 **Citrix Web Studio™ 策略**并单击“**策略**”选项卡。
2. 单击“**创建策略**”并展开“**ICA® > USB 设备策略**”。
3. 编辑“**客户端 USB 设备重定向策略**”。
4. 选择 **允许** 并点击 **保存**。

创建 USB 重定向策略规则

当用户尝试将 USB 设备重定向到虚拟桌面时，系统会依次对照每个 USB 策略规则进行检查，直到找到匹配项。任何设备的第一个匹配项都被视为最终结果。如果第一个匹配项是“**允许**”规则，则允许将匹配的设备重定向到虚拟桌面。如果第一个匹配项是“**拒绝**”规则，则匹配的设备仅在本地桌面中可用。如果未找到匹配项，则使用默认规则。

设备规则

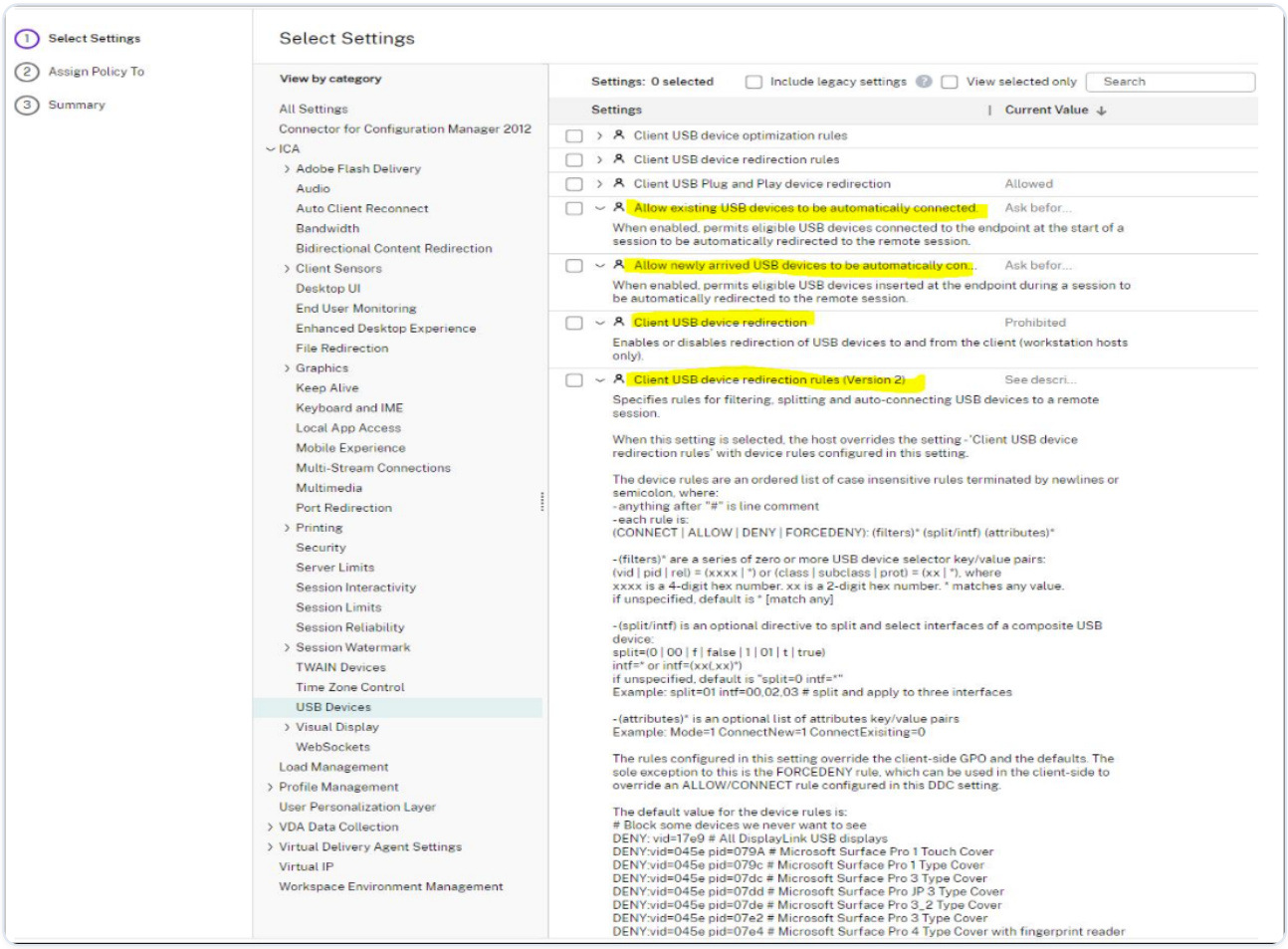
与常规 USB 设备一样，在策略或客户端 Citrix Workspace™ 应用程序配置中设置的设备规则会在端点上选择要转发的设备。Citrix Workspace 应用程序使用这些规则来决定允许或阻止哪些 USB 设备转发到远程会话。

每条规则都包含一个操作关键字（**允许、连接或拒绝**）、一个冒号 (:) 以及零个或多个与端点 USB 子系统中的实际设备匹配的筛选参数。这些筛选参数对应于每个 USB 设备用于标识自身的 USB 设备描述符元数据。

设备规则是纯文本，每条规则占一行，并且在 # 字符后可以跟一个可选注释。规则按从上到下（优先级降序）的顺序匹配。匹配设备或子接口的第一条规则将应用。忽略选择相同设备或接口的后续规则。

示例： 允许: VID=1050 PID=0421 #Device1 **示例：** 连接: VID=xxxx PID=yyyy Class=03 #Device2

关键字	描述
CONNECT	使用此关键字允许设备通过 USB 虚拟通道重定向，并使其能够在会话启动和插入时自动重定向。
ALLOW	使用此关键字允许设备通过 USB 虚拟通道重定向
DENY	使用此关键字拒绝设备通过 USB 虚拟通道重定向



在 DDC 上设置策略：

1. 打开 **Citrix Web Studio 策略**，然后单击**策略**选项卡。
2. 单击**创建策略**，然后展开 **ICA > USB 设备策略**。
3. 编辑**客户端 USB 设备重定向规则（版本 2）**。
4. 根据描述中为每个需要重定向的 USB 设备提供的示例设置值，然后单击“保存”。

   例如：允许: VID=056A PID=00A4 #STU-430 拒绝: Class=08 subclass=05 # Mass Storage

> **注意：**
>
> 如果 Citrix 管理员选中**使用默认值**并单击**保存**，则可以在 VDA 中的以下注册表中找到默认规则。

> **注意！**
>
> 在使用注册表编辑器之前，请参阅本文末尾的免责声明。

```
HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules
```

注意：

仍可以使用组策略设备规则在客户端设备上设置策略，但在较新版本的 CVAD 和 CWA 中不再需要这样做。

有关 USB 设备的旧版配置，请参阅旧版 USB 重定向配置。

配置 USB 设备的自动重定向（可选）

启用 USB 支持后，USB 设备将自动重定向。此外，USB 用户首选项设置也配置为自动连接 USB 设备。重定向所有 USB 设备并非总是最佳选择。用户可以从 USB 设备列表中显式重定向未自动重定向的设备。要阻止 USB 设备被列出或重定向，请在客户端端点或 DDC 策略上使用 DeviceRules。 此策略可以在 DDC 上、使用 GPO 在客户端上、使用 Citrix Workspace 首选项或 CDViewer 下的“连接”选项卡中设置。所有这些方法都将在下面进行描述：

在 DDC 上设置策略：

DDC 上可以设置两个策略，以允许 USB 设备自动重定向 -

- 允许现有 USB 设备自动连接
- 允许新插入的 USB 设备自动连接

a. 打开 **Citrix Web Studio 策略**，然后单击**策略**选项卡。

b. 单击**创建策略**，然后展开 **ICA > USB 设备策略**。

c. 编辑设置**允许**现有 USB 设备自动连接。

d. 清除**使用默认值**复选框，然后从下拉菜单中选择**自动重定向可用 USB 设备**，再单击**保存**。

e. 编辑设置**允许**新插入的 USB 设备自动连接。

f. 清除**使用默认值**复选框，然后从下拉菜单中选择**自动重定向可用 USB 设备**，再单击**保存**。

了解 USB 设备重定向规则

使用 Citrix 客户端 USB 重定向时，了解不同规则的优先级和应用方式非常重要。可以将其视为一组指令：系统会按特定顺序检查规则，并应用它为特定设备找到的第一个规则。列表中后续为**同一设备**找到的任何其他规则都将被忽略。

以下是评估设备规则的顺序：

- **客户端 USB 设备重定向规则（版本 2）**：此策略设置配置的设备规则具有最高优先级。如果在此处找到特定设备的规则，则应用该规则，并且不会考虑该特定设备的任何其他规则。
- **客户端 USB 设备重定向规则**：接下来是 Citrix Studio 中此旧版设置中定义的规则。如果在版本 2 策略中未找到设备的规则，系统将检查此策略设置中定义的规则。同样，如果在此处找到设备的规则，则应用该规则，并且系统将停止查找该特定设备的规则。

> **注意：**
>
> 仅当 Studio 中未设置**客户端 USB 设备重定向规则（版本 2）**或 **适用于 Windows 的 Citrix Workspace 应用程序**版本低于 2212 时，才应用上述策略设置。

- **客户端组策略对象 (GPO)**：如果设备在检查了两个 Studio 策略设置后仍没有应用规则，系统将转而使用通过客户端组策略对象配置的规则。
- **客户端注册表设置**：最后，客户端注册表设置以最低优先级应用。

此层次结构可确保更具体或更新的配置对给定设备具有优先权，从而提供一种清晰且可预测的方式来管理 USB 设备重定向。请务必记住，虽然层次结构决定了评估顺序，但为设备在较高级别找到的规则将阻止为**同一设备**在较低级别应用规则。 但是，在较低级别设置的规则并非完全被忽略；对于尚未应用规则的任何设备，它们仍会进行评估。

这种分层方法还保证了**向后兼容性**。从旧版 Citrix Virtual Apps and Desktops™ 或 Citrix Workspace 应用程序升级时，现有的客户端配置将得到保留。这让企业管理员有时间规划迁移到 Studio 中更高级的**版本 2 设备规则**策略设置的路径，而不会立即造成中断。

示例：

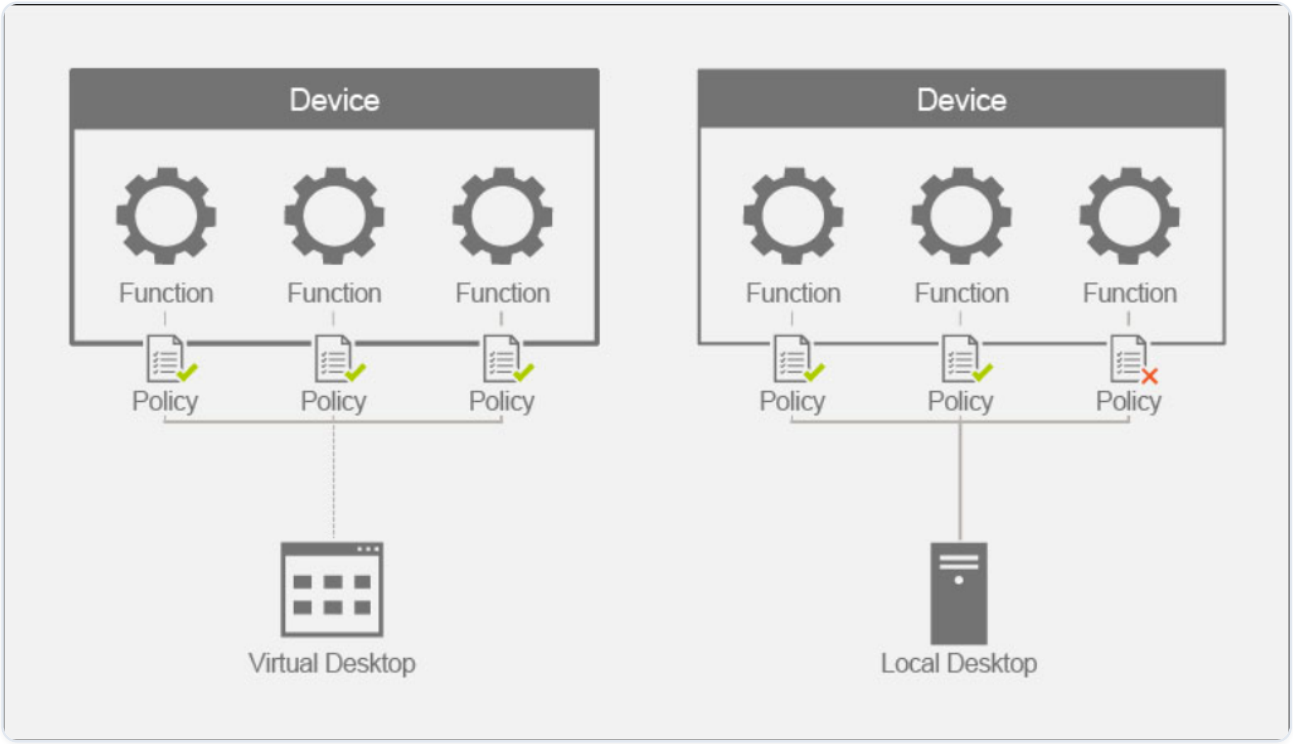
假设您有一个特定的 USB 设备，其供应商 ID (VID) 为 `xxxx`，产品 ID (PID) 为 `yyyy`。

- 在 Citrix Studio 的**客户端 USB 设备重定向规则（版本 2）**策略设置中，您有一个规则集 `CONNECT VID=xxxx PID=yyyy`。
- 另外，在客户端**组策略对象 (GPO)** 中，您为同一设备设置了一个 `DENY` 规则 `DENY: VID=xxxx PID=yyyy`。

当此设备连接到客户端端点时，系统将首先评估版本 2 Studio 策略中的规则。它会找到 `CONNECT` 规则 `VID=xxxx PID=yyyy`。由于此规则处于最高优先级级别，因此会立即应用。然后，系统会忽略此特定设备的任何其他规则。因此，即使客户端 GPO 中存在 `DENY` 规则，它也会被忽略，并且设备将成功重定向。

复合设备和设备拆分

复合 USB 设备是一种单一设备，其行为类似于连接到计算机的多个独立 USB 设备。它具有一个 USB 连接器，但可以向计算机公开多个接口，每个接口都有一组自己的功能。当用户插入复合 USB 设备时，主机设备会根据每个策略规则检查所有功能（接口）。如果任何功能（接口）的第一个匹配项是“拒绝”规则，则该规则被视为复合设备的最终规则，并且该设备被拒绝。如果某个功能（接口）的第一个匹配项是“允许”规则，则主机设备会继续根据下一个功能（接口）匹配规则。如果没有任何功能（接口）被策略规则拒绝，则允许该复合设备。如果复合设备的最终匹配项是“拒绝”规则，则该设备仅可用于本地桌面，否则该设备将远程连接到虚拟桌面。如果未找到匹配项，则使用默认规则。



我们可以使用“设备重定向规则（版本 2）”策略中的相应规则来拆分复合设备，以仅允许复合设备的特定功能。例如，我们可能只想使用 FIDO2 密钥的 HID 功能，而不使用智能卡功能。在这种情况下，我们将按如下所示设置规则：

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey 5 系列允许 FIDO2 HID 功能。
2. Deny: VID=1050 PID=0407 split=01 intf=02 # Yubikey 5 系列智能卡功能已阻止。

> **提示：**
>
> 创建新策略规则时，请参阅 USB 网站上提供的USB 类代码。

配置签名板

1. 在 VDA 主机上安装相应的设备驱动程序。
2. 在 **Citrix Web Studio™** 中启用**客户端 USB 设备重定向**策略设置。
3. 编辑**客户端 USB 设备重定向规则（版本 2）**策略设置。
    a. 设置需要重定向的签名板的 **VID** 和 **PID** 信息，然后单击**保存**。例如：**连接**：VID=06A8 PID=0057 class=03 #Topaz HSB
4. 编辑策略设置**客户端 USB 设备优化规则**。
    a. 设置模式以及其他设备信息。例如：Mode=00000004 VID=06A8 PID=0057 class=03 #在捕获模式下运行的输入设备
5. 编辑策略设置**允许自动连接现有 USB 设备**。
6. 取消选中“**使用默认值**”复选框，然后从下拉菜单中选择“**自动重定向可用 USB 设备**”，再单击“**保存**”。
7. 编辑策略设置“**允许自动连接新到达的 USB 设备**”。
8. 取消选中“**使用默认值**”复选框，然后从下拉菜单中选择“**自动重定向可用 USB 设备**”，再单击“**保存**”。

配置这些设置后，后续会话启动时，设备将自动重定向，并且不需要任何额外的最终用户操作。

> **注意：**
>
> 将 VID 和 PID 替换为要重定向设备的实际 VID 和 PID。

使用 USB 重定向配置 Bloomberg 键盘

1. 在 **Citrix Web Studio** 中启用“**客户端 USB 设备重定向**”策略设置。
2. Bloomberg 5 键盘在“**客户端 USB 设备重定向规则（版本 2）**”策略设置中默认已设置，无需额外的管理员操作。
3. 编辑策略设置“**允许自动连接现有 USB 设备**”。
4. 取消选中“**使用默认值**”复选框，然后从下拉菜单中选择“**自动重定向可用 USB 设备**”，再单击“**保存**”。
5. 编辑策略设置“**允许自动连接新到达的 USB 设备**”。

6. 取消选中“**使用默认值**”复选框，然后从下拉菜单中选择“**自动重定向可用 USB 设备**”，再单击“**保存**”。

配置这些设置后，Bloomberg 密钥将自动显示在后续 HDX™ 会话中，并且不需要任何额外的最终用户操作。

使用 USB 重定向配置 FIDO2 密钥

Citrix 建议使用 FIDO2 重定向在 HDX 会话中使用 FIDO2 密钥。但是，在某些情况下，您必须改用 USB 重定向来重定向 FIDO2 密钥。这些情况包括 FIDO2 重定向不可用，因为客户端、VDA 或操作系统（例如 Windows Server 2016）不支持该功能。

密钥可能启用了多种模式，但您只想在 HDX 会话中允许其中的一部分。例如，您可能希望允许 FIDO2 和 OTP，但阻止智能卡。

以下步骤说明了如何使用 USB 重定向配置 FIDO2 密钥（Yubikey vid=1050, pid=0407）。

1. 在 **Citrix Web Studio** 中启用**客户端 USB 设备重定向**策略设置。
2. 编辑**客户端 USB 设备重定向规则（版本 2）**策略设置。
    a. 设置要在会话中重定向的 FIDO2 密钥的 **VID** 和 **PID** 信息以及拆分设备配置，然后单击**保存**。
    b. **连接**：VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey series 5 允许的 FIDO2 HID 功能。
    c. **拒绝**：VID=1050 PID=0407 split=01 intf=02 # Yubikey series 5 智能卡功能已阻止。
3. 编辑策略设置**允许自动连接现有 USB 设备**。
4. 清除**使用默认值**复选框，然后从下拉菜单中选择**自动重定向可用 USB 设备**，然后单击**保存**。
5. 编辑策略设置**允许自动连接新到达的 USB 设备**。
6. 清除**使用默认值**复选框，然后从下拉菜单中选择**自动重定向可用 USB 设备**，然后单击**保存**。

配置这些设置后，FIDO2 键盘将自动显示在后续的 HDX 会话中，并且无需任何额外的最终用户操作。

使用 USB 重定向配置 3D 鼠标

目前，3dConnexion 空间鼠标驱动程序仅在工作站操作系统（Windows 10 和 Windows 11）上受支持。它们不适用于服务器操作系统。以下是在工作站操作系统上配置 SpaceMouse Enterprise 的步骤 (vid=046D, pid=C016)。

1. 在 VDA 主机上安装最新的 Windows 驱动程序。

2. 在 **Citrix Web Studio** 中启用**客户端 USB 设备重定向**策略设置。
3. 编辑**客户端 USB 设备重定向规则（版本 2）**策略设置。
    a. 添加需要重定向的签名板的 **VID** 和 **PID** 信息，然后单击**保存**。例如：**连接**：VID=046D PID=C016 #SpaceMouse Enterprise
4. 编辑策略设置**客户端 USB 设备优化规则**。
    a. 设置模式以及其他设备信息。例如：Mode=00000004 VID=046D PID=C016 class=03 #Input device operating in capture mode
5. 编辑策略设置**允许自动连接现有 USB 设备**。
6. 清除**使用默认值**复选框，并从下拉菜单中选择**自动重定向可用 USB 设备**，然后单击**保存**。
7. 编辑策略设置**允许自动连接新到达的 USB 设备**。
8. 清除**使用默认值**复选框，并从下拉菜单中选择**自动重定向可用 USB 设备**，然后单击**保存**。

使用不同的设备规则配置两个或更多设备以进行 USB 重定向

可以在 HDX 会话中重定向多个设备，并使用不同的设备规则。管理员可能希望自动重定向一个设备，同时为最终用户提供重定向另一个设备的选项。以下是使用不同规则配置两个设备的步骤。

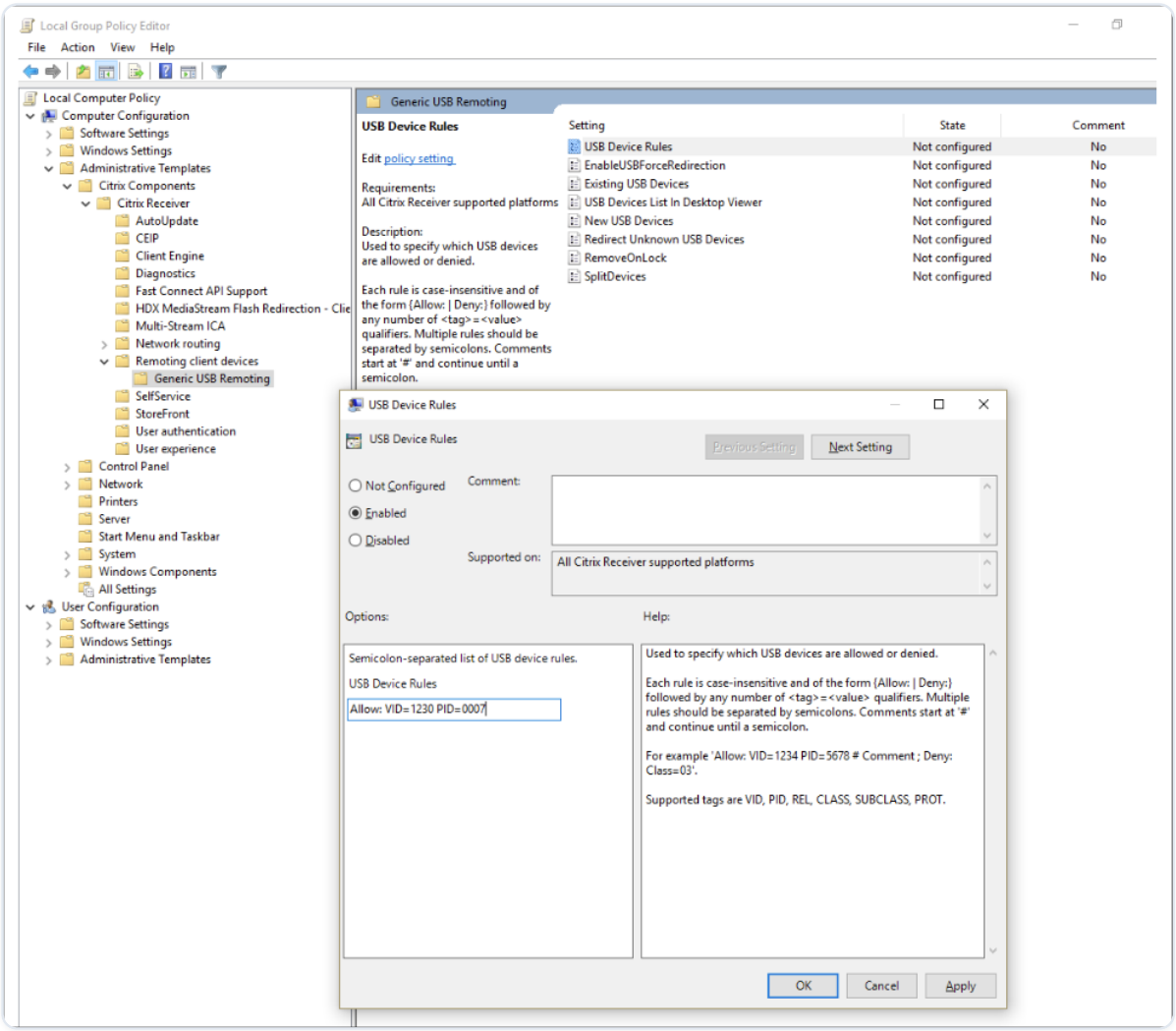
1. 在 **Citrix Web Studio** 中启用**客户端 USB 设备重定向**策略设置。
2. 编辑**客户端 USB 设备重定向规则（版本 2）**策略设置。
    a. 添加要重定向的两个设备的 **VID** 和 **PID** 信息以及会话中相应的设备规则，然后单击**保存**。
    b. **允许**：VID=0911 PID=0c1c #飞利浦语音麦克风。
    c. **连接**: VID=06A8 PID=0043 class=03 # Topaz HSB 签名板
3. 编辑策略设置 **允许现有 USB 设备自动连接**。
4. 清除 **使用默认值** 复选框，然后从下拉菜单中选择 **自动重定向可用 USB 设备**，然后单击 **保存**。
5. 编辑策略设置 **允许新到达的 USB 设备自动连接**。
6. 清除 **使用默认值** 复选框，然后从下拉菜单中选择 **自动重定向可用 USB 设备**，然后单击 **保存**。

这些设置配置完成后，Topaz HSB 签名板将自动显示在后续的 HDX 会话中，并且不需要任何额外的最终用户操作。另一方面，飞利浦语音麦克风将要求最终用户在连接中心或 CDViewer 的“设备”选项卡中启用重定向。

故障排除

以下步骤可用于排查 USB 重定向相关问题：

1. 验证 USB 重定向是否满足系统要求。这包括正确的 CVAD 和 CWA 版本、受支持的设备以及所考虑的操作系统平台上的设备驱动程序。
2. 确保配置与您环境中使用的组件版本和平台相符。有关需要(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/devices/usb-devices/legacy-usb-redirection-configuration.html)的组件的详细信息，请参阅旧版 USB 重定向配置中的说明。
3. 验证设备是否列在客户端已枚举的设备下。
    a. Workspace 首选项工具栏：查看 Workspace 应用程序首选项工具栏的“设备”选项卡中枚举的设备（右键单击 **CWA 图标 > 连接中心 > 首选项**… 单击“**设备**”选项卡）。
    b. `CtxUsbDiagnostics.exe`（推荐）：在命令提示符窗口中运行此工具。输出将为您提供特定会话的设备特定信息。它会告诉您设备是否正在重定向。它还会告诉您设备规则集是否导致设备未重定向。有关详细信息，请参阅诊断工具。
    c. USBView 或其他第三方工具：在端点/客户端计算机上运行 USBView 等第三方工具，以确保在端点检测到设备。
4. 如果您看到设备正在枚举：
    a. 如果您在 CtxUsbDiagnostics 工具输出中看到特定设备的拒绝规则，请检查 Studio 中配置的策略，并确保在版本 2 策略中正确设置了规则。如果拒绝规则未出现在 Studio 策略中，请按顺序检查客户端策略，最后检查客户端默认设置以查找匹配的拒绝规则。
    b. 如果 CtxUsbDiagnostics 输出中没有拒绝规则，则 CWA 将通过选中/单击“首选项”窗口的“设备”选项卡（设备 > 管理设备）中的相应按钮来允许重定向设备。设备重定向后将在会话中可用。这可以通过检查 HDX 会话中的设备管理器/USBView 或类似应用程序来验证。
5. 如果您没有看到设备在会话中显示：
    a. VDA 主机上可能未正确安装正确的设备驱动程序。确保 VDA 主机上正确安装了最新版本的设备驱动程序。某些设备驱动程序在终端服务器计算机上不受支持，因此请确保您尝试重定向的设备不存在这种情况。
    b. 确保设备未在客户端端点上使用。某些设备还需要在客户端端点上安装驱动程序，这可能会阻止它们在会话中重定向。
6. 验证客户端端点上是否正确设置了 USB 相关规则：
    a. **适用于 Windows 的 CWA**：
        i. 验证客户端上的组策略（为此添加更多详细信息和屏幕截图）是否已正确设置，并且不与 Studio 中设置的规则冲突。
        ii. 验证客户端注册表中的默认规则。



`(HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules) are appropriately set and not in conflict with the rules set in Studio and client group policy.`.

b. 适用于 Linux 的 CWA - 要对适用于 Linux 的 CWA 问题进行分类，请参阅适用于 适用于 Linux 的 CWA 的 USB 文档

c. 适用于 Mac 的 CWA - 要对适用于 Mac 的 CWA 问题进行分类，请参阅 适用于 Mac 的 CWA

注意：

- 在 TSVDA 上，默认情况下，音频设备被阻止使用 USB 重定向。使用这些设备的推荐方法是使用优化的 Audio VC。
- 有时，即使设置了正确的设备重定向规则来拆分设备，USB 复合设备也可能无法自动拆分。出现此问题是因为设备处于低功耗模式。在这种情况下，进入低功耗模式的子设备可能不会出现在设备列表中。您可以使用以下解决方法来解决此问题：

  - 断开会话，插入 USB 设备，然后重新连接到会话。
  - 拔下 USB 设备，然后重新插入。此操作将使设备脱离低功耗模式。
- 有时，可能会启用 USB 电池节电设置以优化电池续航时间。如果客户端端点进入睡眠状态，USB 设备可能会断开连接。在这种情况下，您可能需要断开并重新连接设备，以便在会话中再次呈现该设备。

事件日志

管理员现在可以监视用户可能尝试重定向的未经授权的设备，并可以采取适当的措施。以下是一些将在 VDA 主机上的事件查看器中记录的事件消息，适用于允许重定向的设备和不允许重定向的设备。

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

USB 诊断工具

`CtxUsbDiagnostics.exe` 是 VDA 上的一个命令行工具，可帮助 Citrix 管理员快速诊断和解决客户端上遇到的 USB 设备重定向问题。此实用工具收集了对连接到客户端但无法在 HDX 会话中重定向的 USB 设备相关的配置问题进行分类所需的重要信息。

> **注意：**
>
> - 需要以管理员身份运行命令提示符或 PowerShell，以确保该工具具有执行系统级操作所需的权限。
> - `CtxUsbDiagnostics.exe` 位于 `C:\Program Files\Citrix\HDX\bin\CtxUsbDiagnostics.exe`。 并且已是环境变量的一部分。您无需导航到此路径，可以直接在具有提升权限的命令提示符下运行此工具。

要求

会话主机

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows 11 21H2 或更高版本
  - Windows Server 2016 或更高版本
- VDA
  - Windows: Citrix Virtual Apps and Desktops™ 版本 2311 或更高版本

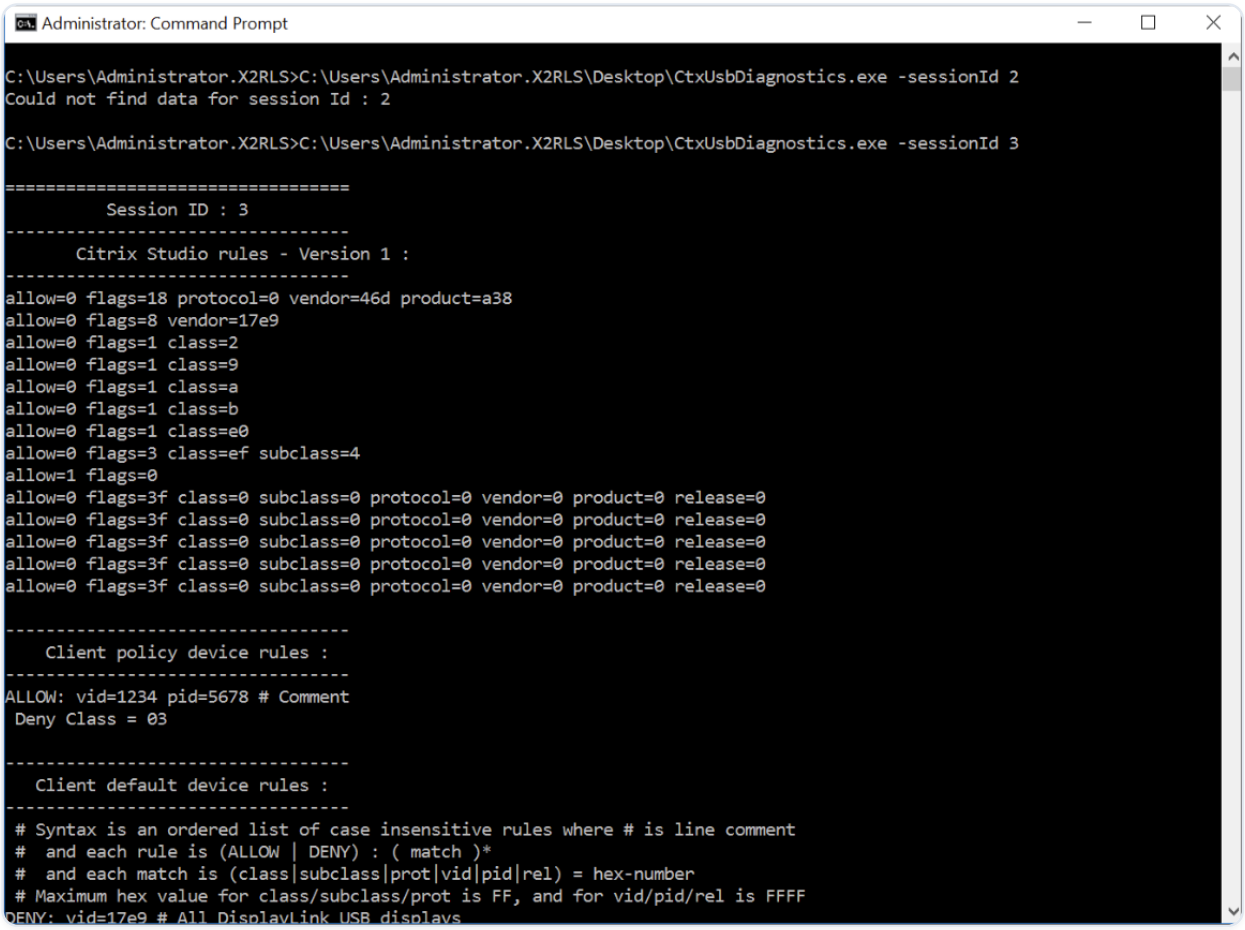
客户端设备

- 操作系统
  - Windows 10 1809 或更高版本
- Workspace 应用程序
  - Windows: 版本 2311 或更高版本

该工具的作用是什么?

该工具目前提供：

- 会话 ID
- VDA 设备策略（在 Studio 中设置的设备规则）
- 客户端设备和客户端设备策略（设备规则）
- 设备列表、其重定向状态以及允许或拒绝它们的原因



> **注意：**
>
> 管理员可以查看所有活动会话的设备信息。

显示的信息

- **Citrix Studio 规则 - 版本 1/2**
  - DDC 规则指示在 Studio 中使用旧版“**客户端 USB 设备重定向规则**”或“**客户端 USB 设备重定向规则（版本 2）**”策略。本节列出的信息包含 Citrix® 管理员配置的所有规则。

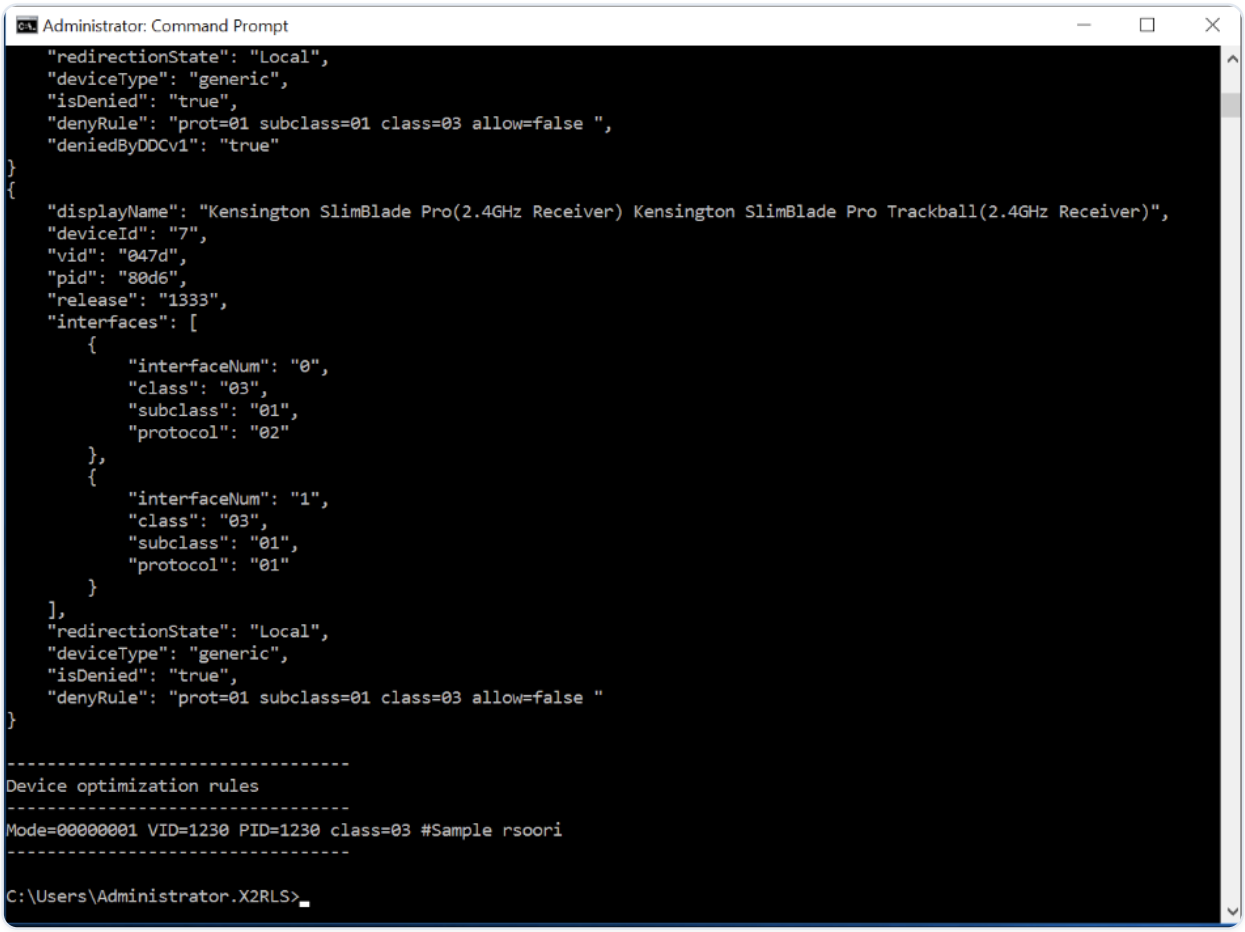
```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

---------------------------------
          Session ID : 1
---------------------------------
       Citrix Studio rules - Version 2 :
---------------------------------
DENY: vid=046D pid=0A38
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
```

- **客户端默认设备规则**
  - 本节列出了在客户端注册表中设置的规则。

```
---------------------------------
  Client default device rules :
---------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #  and each rule is (ALLOW | DENY) : ( match )*
 #  and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

- **设备优化规则**
  - 本节列出了在“客户端 USB 设备优化规则”中设置的设备优化规则。



设备列表

本节列出了有关连接到客户端端点的每个设备的有价值信息、硬件信息、设备是否正在重定向、是否设置了正确的设备重定向规则等等。

标签名称	描述
显示名称	列出设备的通用名称。
供应商 ID	供应商 ID
产品 ID	产品 ID
接口	如果复合设备已拆分为多个子设备，此子部分将列出所有接口。
接口编号	指示接口描述符的索引
类	类代码
子类	子类代码

标签名称	描述
协议	协议
redirectionState	**Local** 表示设备未在 ICA® 会话中重定向。**ThisSession** 表示设备已在 ICA 会话中重定向。**OtherSession** 表示设备已在另一个 ICA 会话中重定向。
deviceType	**generic** 表示设备没有优化的虚拟通道，并且流量正在通过 USB 虚拟通道传输。**optimized** 意味着与设备相关的数据传输正在通过专用虚拟通道进行。
isDenied	**true** 表示设备因管理员设置的策略规则而未重定向。`false` 表示设备因应用策略而重定向。
denyRule	如果 **isDenied** 设置为 `true`，此字段很有用。它会告知管理员策略中导致设备未重定向的具体规则集。
deviceDriver	此字段指示 VDI 主机上是否存在相应的驱动程序。

此外，每个设备都包含一个摘要部分，该部分可让用户了解设备在 HDX 会话中的可用性。

建议

本节简要概述了各种设备规则和问题（如有），这些问题需要纠正或调查。

传统 USB 重定向配置

如果您使用的任何组件版本低于 2212，或者您正在使用适用于 Linux 的 CWA，请按照本指南在您的环境中配置 USB 重定向。

启用通用 USB 重定向

1. 打开 **Citrix Web Studio™ 策略**，然后单击**策略**选项卡。
2. 单击**创建策略**，然后展开 **ICA® > USB 设备策略**。
3. 编辑**客户端 USB 设备重定向**策略设置。
4. 选择**允许**，然后单击**保存**。

创建 USB 重定向策略规则

当用户尝试将 USB 设备重定向到虚拟桌面时，系统会依次对照每个 USB 策略规则进行检查，直到找到匹配项。任何设备的第一个匹配项都被视为最终结果。如果第一个匹配项是“允许”规则，则允许将匹配的设备重定向到虚拟桌面。如果第一个匹配项是“拒绝”规则，则匹配的设备仅在本地桌面中可用。如果未找到匹配项，则使用默认规则。

在 Studio 控制台上设置适当的设备规则：

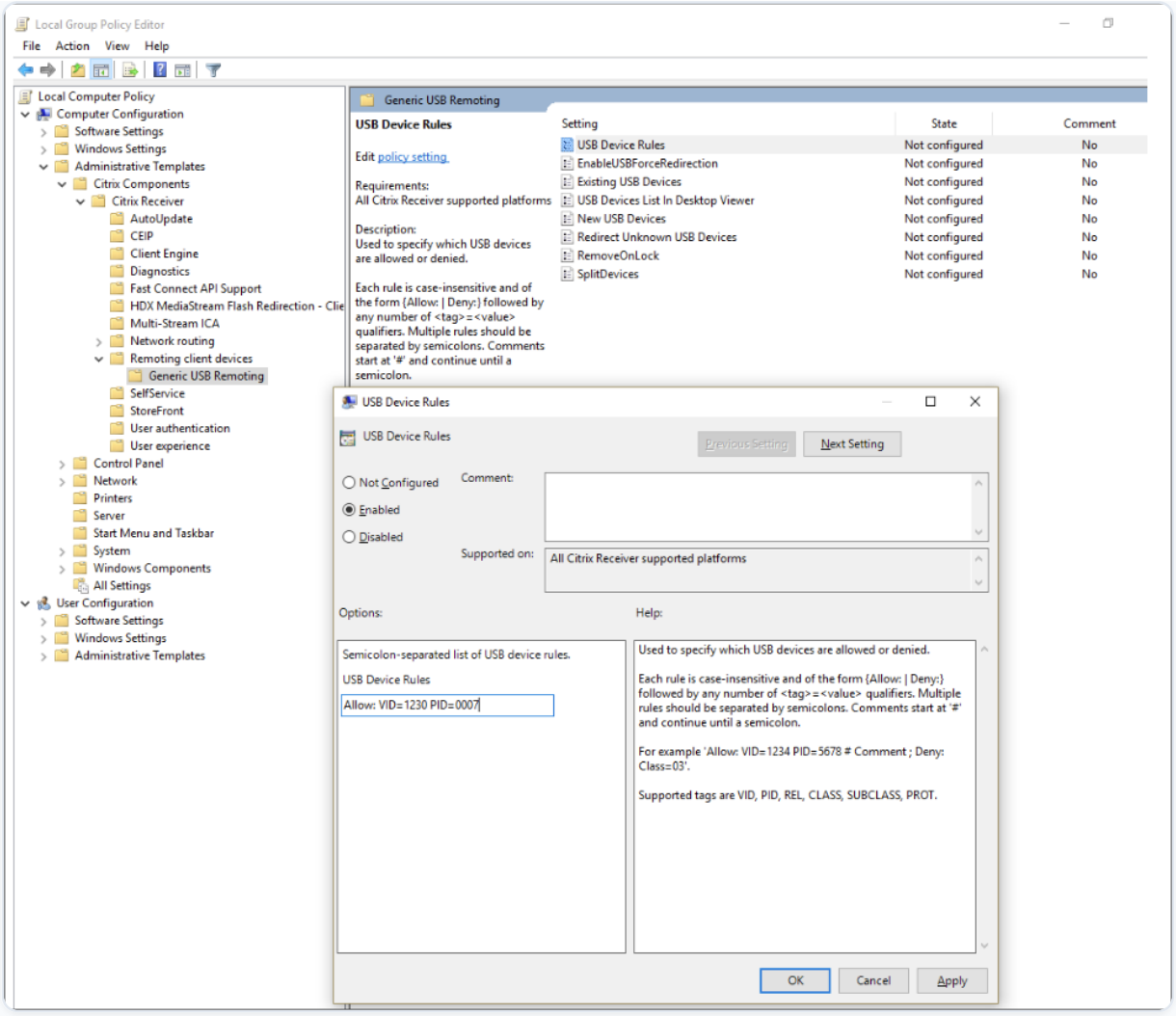
1. 打开 **Citrix Web Studio 策略**，然后单击**策略**选项卡。
2. 单击**创建策略**，然后展开 **ICA > USB 设备策略**。
3. 编辑**客户端 USB 设备重定向规则**策略设置。
4. 根据描述中为每个需要重定向的 USB 设备提供的示例设置值，然后单击“保存”。 例如： Allow: VID=056A PID=00A4 #STU-430 Deny: Class=08 subclass=05 # Mass Storage

> **注意：**
>
> 如果 Citrix® 管理员选中“使用默认值”并单击“保存”，则可以在 VDA 中的以下注册表中找到默认规则。
>
> **注意：**
>
> 在使用注册表编辑器之前，请参阅本文末尾的免责声明。
> `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

在客户端上设置适当的 GPO：

1. 打开**本地组策略编辑器**并导航到**管理模板 > Citrix 组件 > Citrix Receiver™ > 远程处理客户端设备 > 通用 USB 远程处理**。
2. 打开**USB 设备规则**设置并将其设置为**已启用**。按照此示例添加 USB 设备规则， 允许： VID=1230 PID=0007 规则允许供应商 ID 为 1230 且产品 ID 为 0007 的设备。

> **注意：**
>
> 当特定设备必须位于设备规则列表顶部时，请使用“允许：VID=xxxx PID=xxxx”规则。



注意：

诸如 USBView 或连接工具栏之类的工具可用于确定设备的详细信息，例如 VID 和 PID。

配置 USB 设备的自动重定向

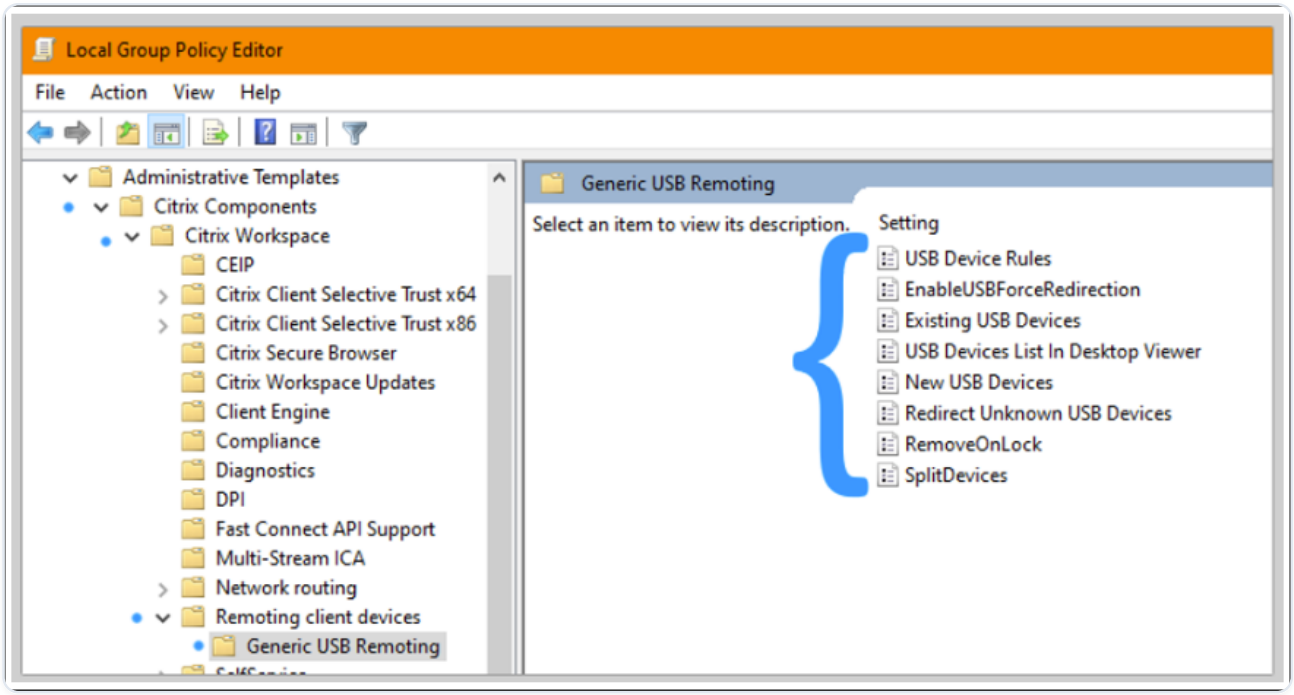
启用 USB 支持后，USB 设备将自动重定向。此外，USB 用户首选项设置也配置为自动连接 USB 设备。并非总是最好重定向所有 USB 设备。用户可以从 USB 设备列表中显式重定向未自动重定向的设备。为防止 USB 设备被列出或重定向，请在客户端端点上使用 DeviceRules 策略设置。

可以在客户端上使用 GPO、客户端注册表、Citrix Workspace™ 首选项或 CDViewer 下的“连接”选项卡来设置此策略。所有这些方法都将在下面介绍：

在客户端上使用 GPO：

1. 打开**本地组策略编辑器**并导航到**管理模板 > Citrix 组件 > Citrix Receiver > 远程处理客户端设备 > 通用 USB 远程处理**。

2. 打开**新建 USB 设备**，选择**已启用**，然后单击**确定**。
3. 打开**现有 USB 设备**，选择**已启用**，然后单击**确定**。

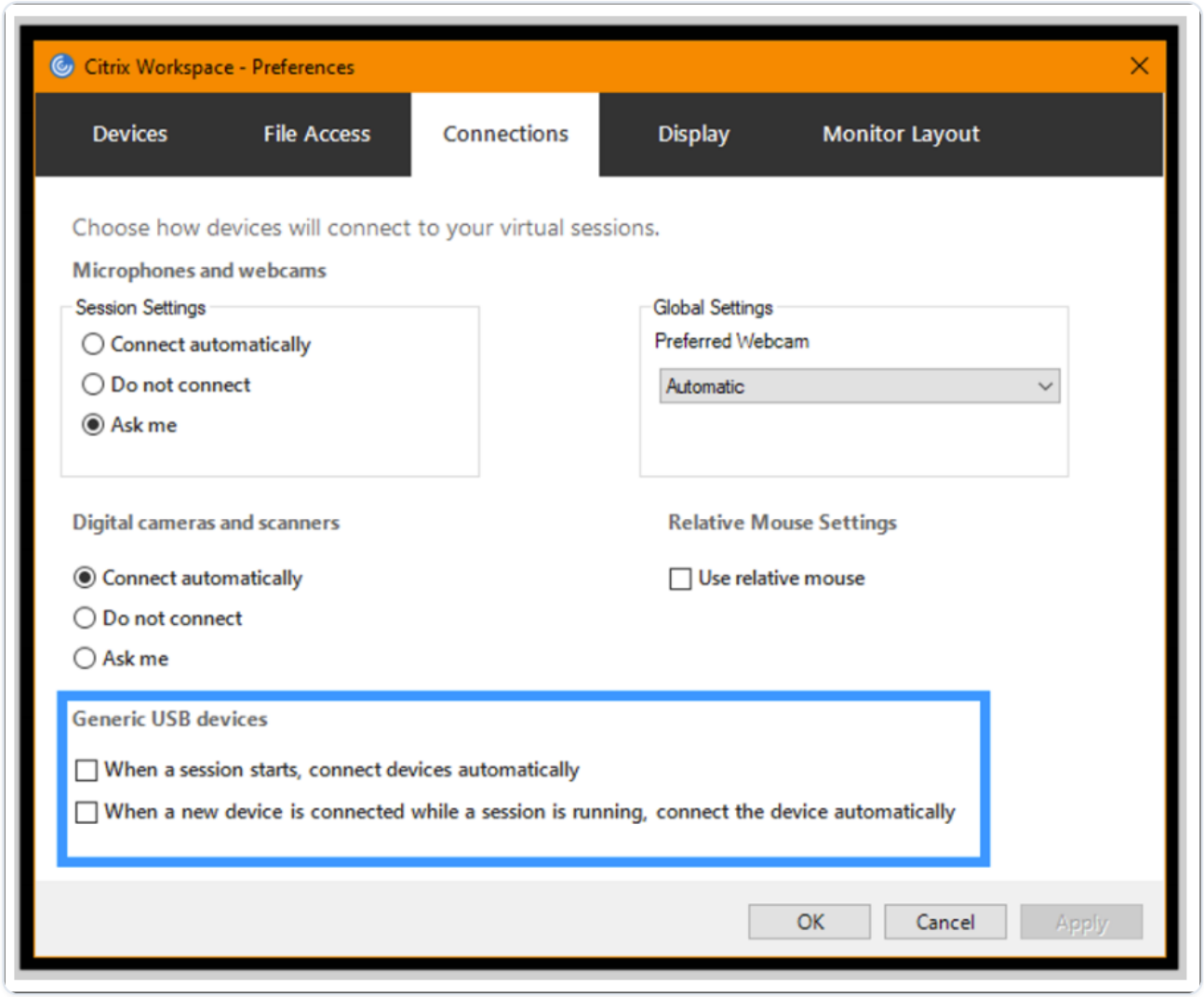


如何使用 Citrix Connection Center：

1. 前往 **Citrix Workspace 首选项 > 连接**。
2. 确保选中以下选项：
    a. 会话启动时，自动连接设备
    b. 会话运行时连接新设备时，自动连接该设备。
3. 单击 **确定**。

使用 CDViewer 连接工具栏：

1. 会话启动后，单击 **CDViewer** 下拉菜单并选择 **Citrix Workspace Preferences > Connections** 选项卡。
2. 确保选中以下选项：
    a. 会话启动时，自动连接设备
    b. 会话运行时连接新设备时，自动连接该设备。
3. 单击 **Apply** 和 **OK** 保存策略。



对于基于客户端的配置，注册表项在客户端设备上的以下位置设置：

> **注意：**
>
> 在使用注册表编辑器之前，请参阅本文末尾的免责声明。
>
> `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

使用具有不同设备规则的 USB 重定向配置两个或更多设备

多个设备可以使用不同的设备规则在 HDX™ 会话中进行重定向。管理员可能希望自动重定向一个设备，同时为最终用户提供重定向另一个设备的选项。以下是使用不同规则配置两个设备的步骤。

1. 在 **Citrix Web Studio** 中启用**客户端 USB 设备重定向**策略设置。
2. 编辑客户端 GPO 中的 **USB 设备规则**设置。
    a. 打开**本地组策略编辑器**，然后转到**管理模板 > Citrix 组件 > Citrix Receiver > 远程处理客户端设备 > 通用 USB 远程处理**。

b. 打开 **USB 设备规则设置**并启用该设置。按照此示例添加 USB 设备规则，**允许: VID=0911 PID=0c1c** 规则允许 **供应商 ID 0911** 和 **产品 ID 0c1c** 的设备，但它不会自动重定向。**连接: VID=06A8 PID=0043** 规则将自动重定向 **供应商 ID 06A8** 和 **产品 ID 0043** 的设备，前提是已设置步骤 3 中提到的自动重定向策略。

c. **允许**: VID=0911 PID=0c1c #Phillips 语音麦克风。

d. **连接**: VID=06A8 PID=0043 class=03 # Topaz HSB 签名板

3. 打开**本地组策略编辑器**，然后转到**管理模板 > Citrix 组件 > Citrix Receiver > 远程处理客户端设备 > 通用 USB 远程处理**。
4. 打开**新建 USB 设备**，选择**已启用**，然后单击**确定**。
5. 打开**现有 USB 设备**，选择**已启用**，然后单击**确定**。

配置这些设置后，Topaz 签名板将自动重定向到 HDX 会话中，并且需要最终用户执行额外操作（在连接中心或 CD Viewer 设备选项卡中选择“重定向”选项）才能在会话中重定向 Phillips 语音麦克风。

> **注意：**
>
> 步骤 2 和 3 中的上述设置可以直接应用于 GenericUSB 键 (HKLM\SOFTWARE\Wow6432Citrix\ICA Client\GenericUSB) 下的客户端注册表值 **DeviceRules**，但这不是推荐的方法。

通用 USB 重定向和客户端驱动器注意事项

HDX™ 技术为大多数常用 USB 设备提供**优化支持**。优化支持可提供更好的用户体验，并在 WAN 上实现更高的性能和带宽效率。优化支持通常是最佳选择，尤其是在高延迟或安全敏感的环境中。

HDX 技术为没有优化支持或不适合使用优化支持的专用设备提供**通用 USB 重定向**，例如：

- USB 设备具有不属于优化支持的更高级功能，例如具有更多按钮的鼠标或网络摄像头。
- 用户需要不属于优化支持的功能。
- USB 设备是专用设备，例如测试和测量设备或工业控制器。
- 应用程序需要以 USB 设备的形式直接访问该设备。
- USB 设备只有 Windows 驱动程序可用。例如，智能卡读卡器可能没有适用于 Android 版 Citrix Workspace™ 应用程序的驱动程序。
- Citrix Workspace 应用程序的版本不为此类 USB 设备提供任何优化支持。

使用通用 USB 重定向：

- 用户无需在用户设备上安装设备驱动程序。
- USB 客户端驱动程序安装在 VDA 计算机上。

重要提示：

- 通用 USB 重定向可以与优化支持一起使用。如果启用通用 USB 重定向，请为通用 USB 重定向和优化支持配置 Citrix USB 设备策略设置。
- 客户端 USB 设备优化规则 中的 Citrix 策略设置是针对特定 USB 设备的通用 USB 重定向的特定设置。它不适用于此处所述的优化支持。

USB 设备的性能注意事项

网络延迟和带宽会影响用户体验，以及在使用通用 USB 重定向时某些类型 USB 设备的运行。例如，对时序敏感的设备可能无法在高延迟、低带宽链路上正常运行。尽可能使用优化支持。

某些 USB 设备需要高带宽才能使用，例如 3D 鼠标（与通常也需要高带宽的 3D 应用程序一起使用）。如果无法增加带宽，您可以通过使用带宽策略设置调整其他组件的带宽使用情况来缓解此问题。有关详细信息，请参阅客户端 USB 设备重定向的带宽策略设置和多流连接策略设置。

USB 设备的安全性注意事项

某些 USB 设备本质上对安全性敏感，例如智能卡读卡器、指纹识别器和签名板。其他 USB 设备（例如 USB 存储设备）可用于传输可能敏感的数据。

USB 设备通常用于分发恶意软件。Citrix Workspace 应用程序和 Citrix Virtual Apps and Desktops™ 的配置可以降低但不能消除这些 USB 设备带来的风险。无论使用通用 USB 重定向还是优化支持，此情况都适用。

重要提示：

对于安全敏感的设备和数据，请始终保护 HDX 连接，请参阅客户端与 VDA 之间的通信。

仅启用您需要的 USB 设备支持。配置通用 USB 重定向和优化支持以满足此需求。

为用户提供安全使用 USB 设备的指导：

- 仅使用从可信来源获取的 USB 设备。
- 请勿将 USB 设备留在无人看管的开放环境中，例如，将闪存驱动器留在网吧。
- 解释在多台计算机上使用 USB 设备的风险。

USB 大容量存储设备的安全控制

为 USB 大容量存储设备提供优化支持。此支持是 Citrix Virtual Apps and Desktops 客户端驱动器映射的一部分。用户登录时，用户设备上的驱动器会自动映射到虚拟桌面上的驱动器盘符。这些驱动器显示为具有映射驱动器盘符的共享文件夹。要配置客户端驱动器映射，请使用**客户端可移动驱动器**设置。此设置位于 ICA 策略设置的文件重定向策略设置部分中。

对于 USB 大容量存储设备，您可以使用客户端驱动器映射或通用 USB 重定向，或两者都使用。使用 Citrix® 策略对其进行控制。主要区别在于：

功能	客户端驱动器映射	通用 USB 重定向
默认启用	是	否
可配置只读访问	是	否

注意：

USB 重定向支持较低带宽的连接，例如 50 Kbps。但是，复制大文件不起作用。

客户端驱动器映射 (CDM)

客户端驱动器映射使客户端端点上的存储驱动器在 Citrix HDX™ 会话中可用，从而允许文件和文件夹在客户端与会话主机之间传输。此功能默认启用，并具有读写权限。为防止用户在映射的客户端设备上添加或更改文件和文件夹，请启用**只读客户端驱动器访问**策略设置。将此设置添加到策略时，请确保**客户端驱动器重定向**设置已设置为**允许**，并且也已添加到策略中。

作为一项安全预防措施，默认情况下，端点驱动器在映射时没有运行权限。要允许用户直接从映射的客户端驱动器运行可执行文件，请编辑会话主机中的 **ExecuteFromMappedDrive** 注册表值。有关详细信息，请参阅**通过注册表管理的 HDX 功能**部分中的映射的客户端驱动器。

要求

使用 CDM 的要求如下：

Citrix 控制平面

- Citrix Virtual Apps and Desktops™ 1912 或更高版本
- 思杰 DaaS™

会话主机

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows Server 2016 或更高版本
  - Linux：请参阅 Linux VDA 系统要求
- VDA
  - Windows: 思杰虚拟应用和桌面™ 1912 或更高版本
  - Linux：请参阅 Linux VDA 文档

客户端设备

- 操作系统
  - Windows 10 1809 或更高版本
  - Linux: 请参阅适用于 Linux 的 Workspace 应用程序的系统要求

相关策略

有关 CDM 设置，请参阅策略设置参考部分。

双跳方案

CDM 支持双跳方案。默认情况下，客户端端点的驱动器映射到第二个跳会话，并且第一个跳的驱动器不可用。但是，可以进行设置，以便将第一个跳的驱动器映射到第二个跳的会话中，而不是客户端端点的驱动器。

要配置此功能，请编辑以下注册表值：

- 键：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive\
- 值名称：NativeDriveMapping
- 值类型：REG_SZ
- 值数据:

- 真 - 将第一跳会话的驱动器映射到第二跳会话中
- 假 - 将客户端端点的驱动器映射到第二跳会话中

注意：

不正确地编辑注册表可能会导致严重问题，甚至可能需要重新安装操作系统。Citrix 无法保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。编辑注册表之前，请务必备份注册表。

移动和触摸屏客户端设备支持

Citrix Virtual Apps and Desktops™ 允许用户通过移动和触摸屏客户端设备访问其发布的应用程序和桌面。

要求

Citrix® 控制平面

- Citrix Virtual Apps and Desktops™ 1912 或更高版本
- 思杰 DaaS™

会话主机

- 操作系统
  - Windows 10 1903 或更高版本
  - Windows 11 21H2 或更高版本
- VDA
  - Windows: Citrix Virtual Apps and Desktops 版本 7.15 或更高版本

客户端设备

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows 11 21H2 或更高版本
- 适用于 Windows 的 Citrix Workspace™ 应用程序 1808 或更高版本

使用 Windows Continuum 的触摸屏设备的平板电脑模式

Continuum 是 Windows 10 的一项功能，可根据客户端设备的使用方式进行调整。当 VDA 在支持触摸的客户端上检测到键盘或鼠标时，它会将客户端置于桌面模式。如果不存在键盘或鼠标，VDA 会将客户端置于平板电脑/移动模式。此检测在会话连接和重新连接时发生，并在会话中当键盘或鼠标连接或分离时也会发生。

此功能默认启用。要禁用此功能，请配置策略设置 平板电脑模式切换策略设置。

除了上述触屏设备的要求外，Windows Continuum 还需要满足以下条件：

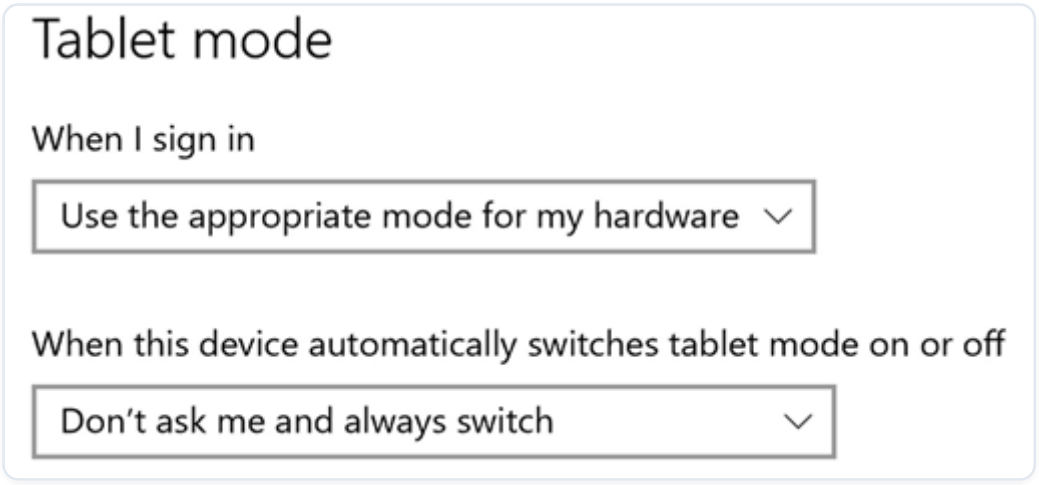
XenServer（以前称为 Citrix Hypervisor™）

- Citrix Hypervisor 8.2 或更高版本
- 请运行以下 XenServer CLI 命令以允许笔记本电脑/平板电脑切换： **xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1**

> **重要提示：**
>
> 更改元数据设置后更新现有计算机目录的基础映像不会影响任何以前预配的 VM。更改 XenServer VM 基础映像后，请创建目录，选择基础映像，然后预配新的 Machine Creation Services™ (MCS) 计算机。

会话主机

- 操作系统
  - Windows 10 1903 或更高版本
  - Windows 11 21H2 或更高版本
- VDA
  - Windows: 7.16 版或更高版本
  - **由于操作系统配置的当前限制，用户在启动第一个 ICA® 会话并重新启动 VDA 后，必须从下拉菜单中设置以下选项：**
    - **设置 > 系统 > 平板电脑模式**
      - 为我的硬件使用适当的模式
      - 不询问我并始终切换



平板电脑模式提供更适合触摸屏的用户界面：

- 按钮略大。
- “开始”屏幕和您启动的任何应用程序都以全屏模式打开。
- 任务栏包含一个返回按钮。
- 任务栏中的图标已删除。

您可以访问文件资源管理器。



Windows 10 根据此更新的 BIOS 在目标虚拟机上加载 GPIO 驱动程序。它用于在虚拟机内切换平板电脑模式和桌面模式。

适用于 HTML5 的 Citrix Workspace 应用程序不支持 Windows Continuum 功能。

桌面模式提供传统用户界面，您可以通过与使用 PC、键盘和鼠标相同的方式进行交互。

微软 Surface Pro 和 Surface Book 触控笔

我们支持基于 Windows Ink 的应用程序的标准触控笔功能。支持包括指向、擦除、笔压、蓝牙信号以及其他功能，具体取决于操作系统固件和触控笔型号。例如，笔压可达 4096 级。此功能默认启用。

触控笔功能支持的要求如下：

Citrix 控制平面

- Citrix Virtual Apps and Desktops 1903 或更高版本
- 思杰 DaaS

会话主机

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows 11 21H2 或更高版本
- VDA
  - 视窗：思杰虚拟应用和桌面 1903 或更高版本

客户端设备

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows 11 21H2 或更高版本
- 适用于 Windows 的 Citrix Workspace 应用程序版本 1902 或更高版本

要查看 Windows Ink 和笔功能的演示，请单击此图：



要禁用或启用此功能，请参阅通过注册表管理的特性列表中的 Microsoft Surface Pro 和 Surface Book 触控笔。

已知问题

以下是笔支持的已知问题：

- 由于 Windows Server 2k22 中的操作系统限制，用户在连接到 2k22 服务器应用程序或桌面时，将无法在控制面板中设置笔快捷方式或调整笔/墨迹设置。
- 由于操作系统限制，从启用了笔功能的 Windows 11 客户端发出的笔快捷方式未被识别。

串行端口

大多数新电脑没有内置串行 (COM) 端口。通过使用 USB 转换器可以轻松添加这些端口。适用于串行端口的应用程序通常涉及传感器、控制器、旧式支票读取器、手写板等。某些 USB 虚拟 COM 端口设备使用供应商专用驱动程序，而不是 Windows 提供的驱动程序 (usbser.sys)。这些驱动程序允许您强制指定 USB 设备的虚拟 COM 端口，使其即使连接到不同的 USB 插槽也不会更改。这可以通过**设备管理器 > 端口 (COM 和 LPT) > 属性**或控制设备的应用程序来完成。

客户端 COM 端口映射允许在虚拟会话期间使用连接到用户端点上 COM 端口的设备。您可以像使用任何其他网络映射一样使用这些映射。

对于每个 COM 端口，操作系统中的驱动程序会分配一个符号链接名称，例如 COM1 和 COM2。然后应用程序使用该链接访问端口。

> **重要提示：**

> 设备可以通过 USB 直接连接到端点，但这并不意味着它可以使用通用 USB 重定向进行重定向。某些 USB 设备充当虚拟 COM 端口，应用程序可以像访问物理串行端口一样访问它们。操作系统可以抽象化 COM 端口并将其视为文件共享。虚拟 COM 的两种常见协议是 CDC ACM 或 MCT。通过 RS-485 端口连接时，应用程序可能根本无法工作。获取 RS-485 到 RS232 转换器以将 RS-485 用作 COM 端口。 **重要提示：**

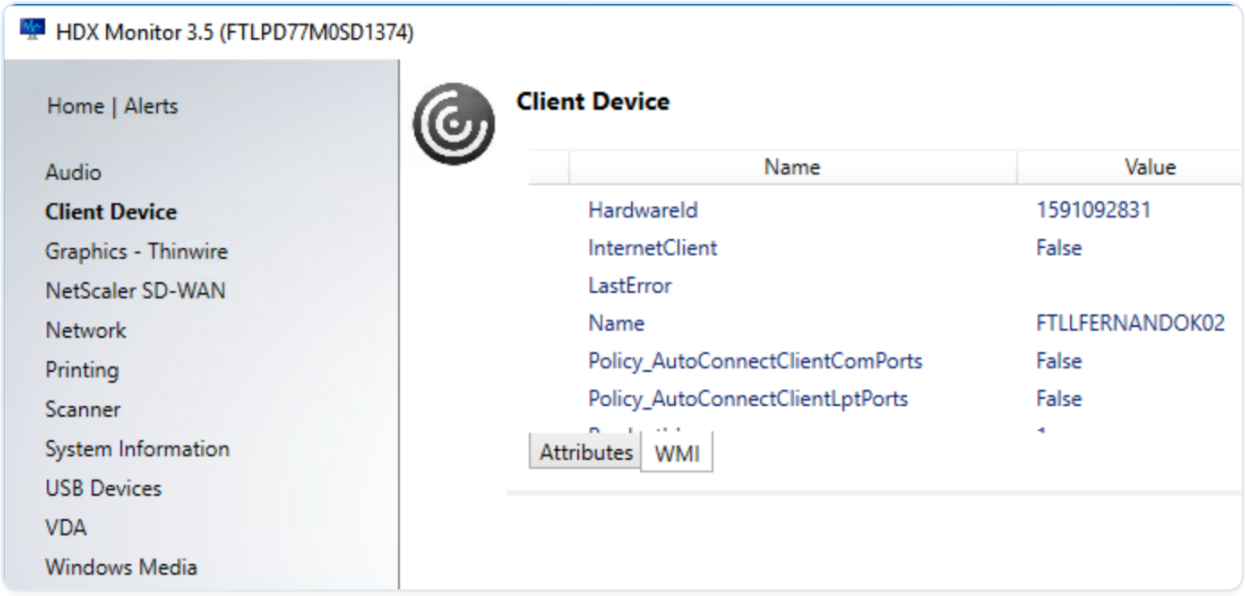
> 某些应用程序仅在设备（例如签名板）连接到客户端工作站上的 COM1 或 COM2 时才能始终如一地识别该设备。

将客户端 COM 端口映射到服务器 COM 端口

您可以通过以下三种方式将客户端 COM 端口映射到 Citrix® 会话：

- Studio 策略。有关策略的详细信息，请参阅端口重定向策略设置。
- VDA 命令行。
- 远程桌面（终端服务）配置工具。

1. 启用**客户端 COM 端口重定向**和**自动连接客户端 COM 端口 Studio**策略。应用后，HDX™ Monitor 中会提供一些信息。



2. 如果**自动连接客户端 COM 端口**未能映射端口，您可以手动映射端口或使用登录脚本。登录到 VDA，并在命令行窗口中键入：

   NET USE COMX: `\\CLIENT\COMZ`:

   或者

   NET USE COMX: `\\CLIENT\CLIENTPORT:COMZ`:

   X 是 VDA 上的 COM 端口号（端口 1 到 9 可用于映射）。**Z** 是您要映射的客户端 COM 端口号。

   要确认操作成功，请在 VDA 命令提示符下键入 **NET USE**。出现的列表包含映射的驱动器、LPT 端口和映射的 COM 端口。

```
C:\Windows\system32>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
             COM3      \\Client\COM3:            Citrix Client Network
```

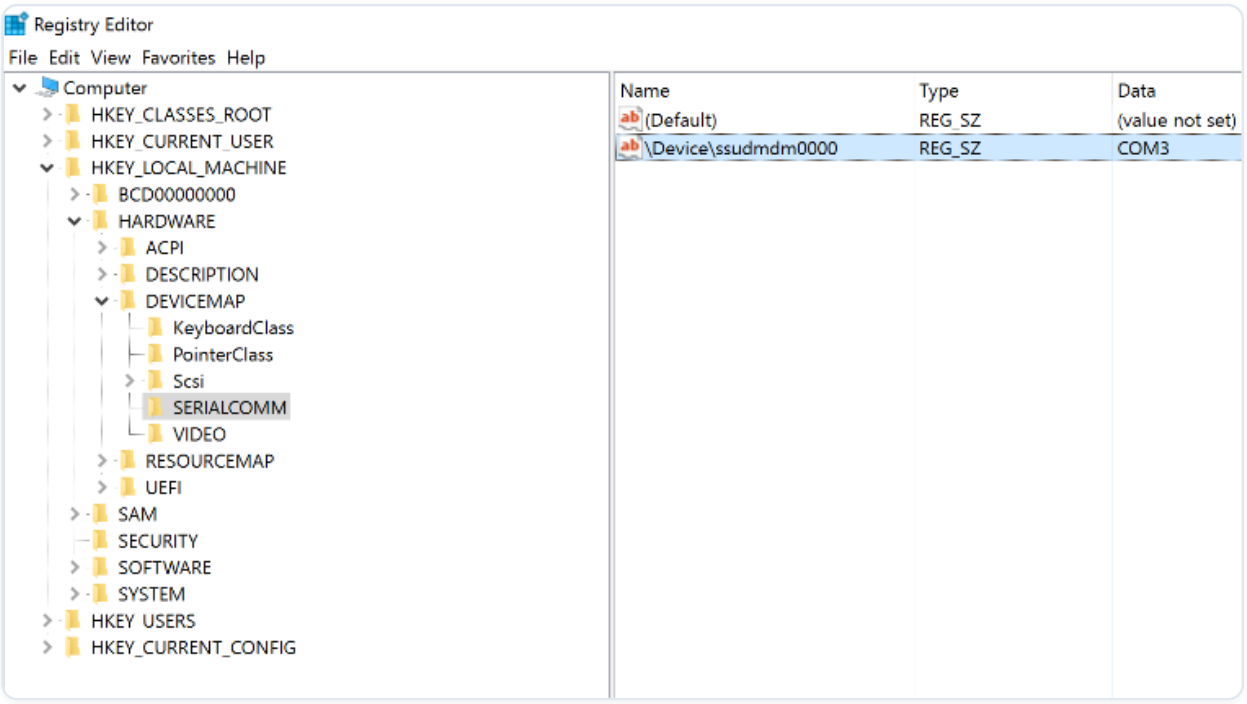
3. 要在虚拟桌面或应用程序中使用此 COM 端口，请安装您的用户设备应用程序并将其指向映射的 COM 端口名称。例如，如果您将客户端上的 COM1 映射到服务器上的 COM3，请在 VDA 中安装您的 COM 端口设备应用程序，并在会话期间将其指向 COM3。像使用用户设备上的 COM 端口一样使用此映射的 COM 端口。

重要提示：

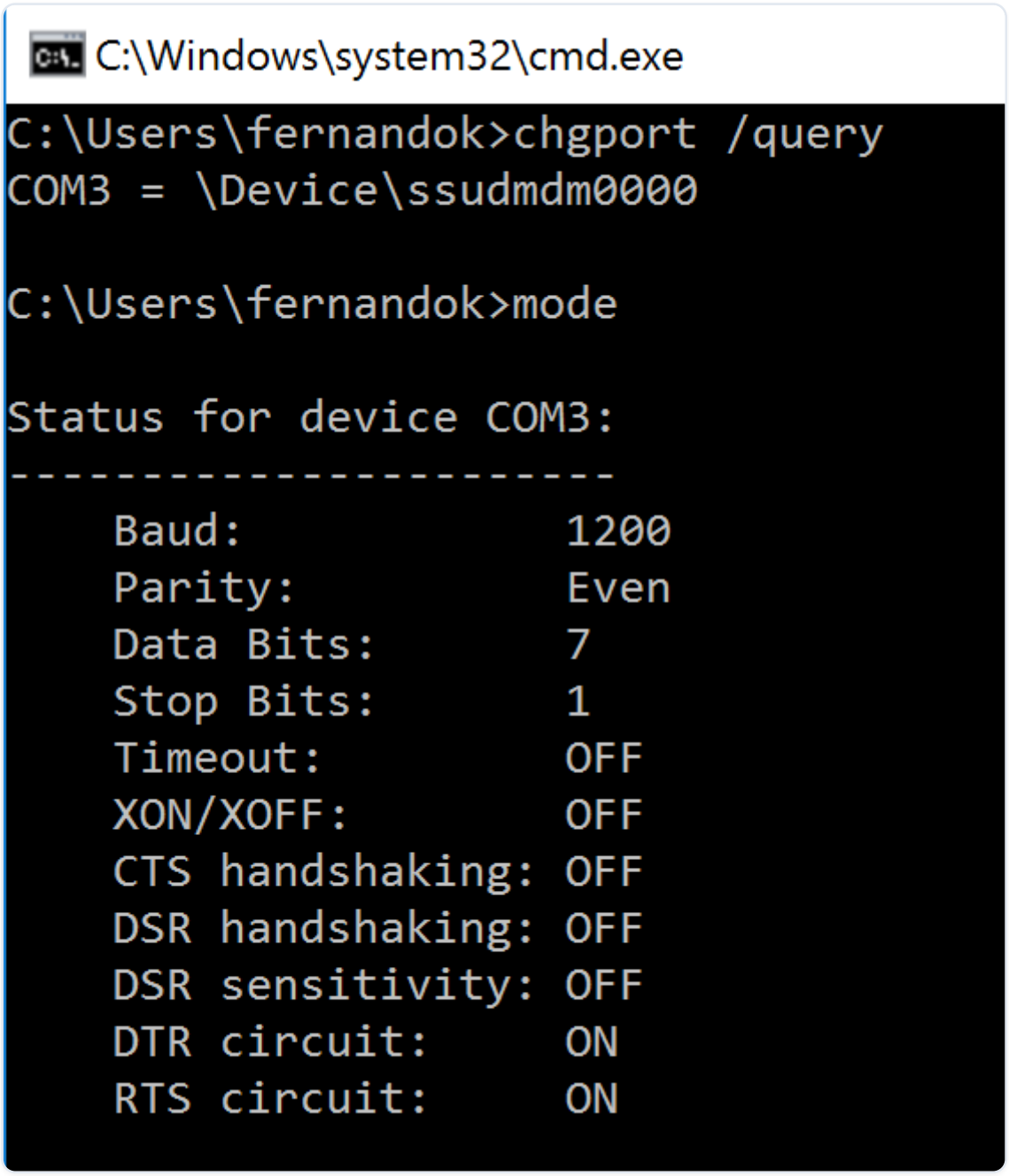
COM 端口映射与 TAPI 不兼容。您无法将 Windows 电话应用程序编程接口 (TAPI) 设备映射到客户端 COM 端口。TAPI 定义了一种标准方式，供应用程序控制数据、传真和语音呼叫的电话功能。TAPI 管理信令，包括拨号、接听和结束呼叫。此外，还包括保持、转接和电话会议等补充服务。

故障排除

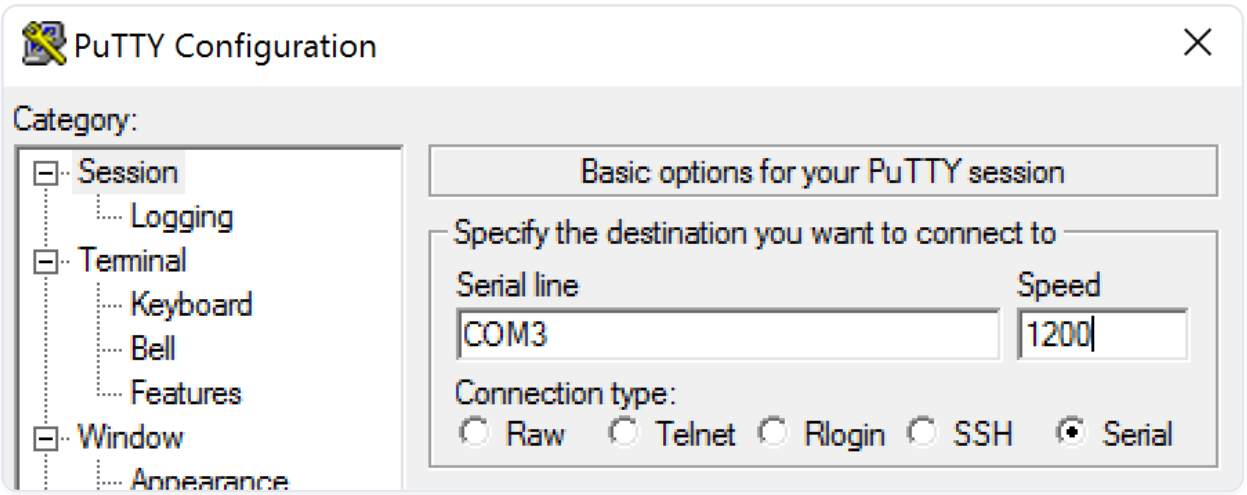
1. 确保您可以直接从端点访问设备，绕过 Citrix。当端口未映射到 VDA 时，您未连接到 Citrix 会话。请遵循设备随附的任何故障排除说明，并首先验证其在本地是否正常工作。 当设备连接到串行 COM 端口时，会在此处所示的配置单元上创建一个注册表项：



   您还可以通过在命令提示符下运行 **chgport /query** 来查找此信息。



如果设备没有故障排除说明，请尝试打开 PuTTY 会话。选择**会话**，并在**串行线路**中指定您的 COM 端口。



您可以在本地命令窗口中运行 **MODE**。输出可能会显示正在使用的 COM 端口以及波特率/奇偶校验/数据位/停止位，这些信息是您在 PuTTY 会话中需要的。如果 PuTTY 连接成功，请按 **Enter** 键查看设备的反馈。您键入的任何字符都可能会在屏幕上重复显示或得到响应。如果此步骤不成功，则无法从虚拟会话访问设备。

2. 将本地 COM 端口映射到 VDA（使用策略或 **NET USE COMX: `\\CLIENT\COMZ`:**），并重复上一步中相同的 PuTTY 过程，但这次是从 VDA PuTTY。如果 PuTTY 未能显示错误 **Unable to open connection to COM1. Unable to open serial port**，则可能是另一个设备正在使用 COM1。
3. 运行 **chgport /query**。如果 VDA 上的内置 Windows 串行驱动程序将 \Device\Serial0 自动分配给 VDA 的 COM1 端口，请执行以下操作： A. 在 VDA 上打开 CMD 并键入 **NET USE.**

   B. 删除 VDA 上任何现有映射（例如 COM1）。

   NET USE COM1 /DELETE

   C. 将设备映射到 VDA。

   NET USE COM1: `\\CLIENT\COM3`:

   D. 将 VDA 上的应用程序指向 COM3。

   最后，尝试将本地 COM 端口（例如 COM3）映射到 VDA 上的另一个 COM 端口（COM1 除外，例如 COM3）。确保您的应用程序指向它： **NET USE COM3: `\\CLIENT\COM3`**
4. 如果现在您确实看到端口已映射，PuTTY 正在工作但没有数据传输，则可能是竞态条件。应用程序可能在端口映射之前连接并打开端口，从而阻止其被映射。请尝试以下方法之一：

   - 打开在同一服务器上发布的第二个应用程序。等待几秒钟，直到端口被映射，然后打开尝试使用该端口的实际应用程序。
   - 从 Active Directory 中的组策略编辑器而不是 Studio 启用 COM 端口重定向策略。这些策略是 **Client COM port redirection** 和 **Auto connect client COM ports**。以这种方式应用的策略可能会在 Studio 策略之前处理，从而确保 COM 端口已映射。Citrix 策略被推送到 VDA 并存储在： `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
   - 为用户使用此登录脚本，或者不发布应用程序，而是发布一个 .bat 脚本，该脚本首先删除 VDA 上的任何映射，重新映射虚拟 COM 端口，然后启动应用程序：

   @echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: `\\CLIENT\COM1`: NET USE COM2: `\\CLIENT\COM2`: MODE COM1: BAUD=1200 (或所需的任何值) MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (或所需的任何值) START C:\Program Files\\\<Your Software Path>\\\<your_software.exe>

5. Sysinternals 的 Process Monitor 是最后的手段。在 VDA 上运行该工具时，查找并筛选 COM3、picaser.sys、CdmRedirector 等对象，尤其是 \<your_app\>.exe。任何错误都可能显示为 Access Denied 或类似内容。

专用键盘

彭博键盘

> **警告：**
>
> 不正确地编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix® 无法保证可以解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。在编辑注册表之前，请务必备份注册表。

Citrix Virtual Apps and Desktops™ 支持 Bloomberg model 5、model 4 Starboard 键盘（以及更早的 model 3）。此键盘使金融行业的客户能够使用键盘的特殊功能来访问金融市场数据并快速执行交易。

> **重要提示：**
>
> 我们建议您仅在一个会话中使用 Bloomberg 键盘。不建议在多个并发会话（一个客户端连接到多个会话）中使用该键盘。

Bloomberg 键盘是一个 USB 复合设备，在一个物理外壳中包含多个 USB 设备：

- 键盘。
- 指纹识别器。
- 带有用于增大和减小音量以及静音扬声器和麦克风的按键的音频设备。此设备包括板载扬声器、麦克风以及用于麦克风和耳机的插孔。
- 用于将所有这些设备连接到系统的 USB 集线器。

要求：

- Citrix Workspace™ 应用程序 for Windows 连接到的会话必须支持 USB 设备。
- Citrix Workspace 应用程序 2207 for Linux 或更高版本，以支持 Bloomberg 键盘 model 5。

- Citrix Workspace 应用程序 2109 for Windows 或更高版本，以支持 Bloomberg 键盘 model 5。
- Citrix Workspace 应用程序 1808 for Windows 或 Citrix Receiver for Windows 4.8 或更高版本，以支持 Bloomberg 键盘 model 3 和 4。
- Citrix Workspace 应用程序 1808 for Windows 或 Citrix Receiver for Windows 4.12 或更高版本，以将 KVM 模式（两根 USB 电缆，其中一根通过 KVM 路由）用于 Model 4。

有关在 Citrix Workspace 应用程序 for Windows 上配置 Bloomberg 键盘的信息，请参阅 配置 Bloomberg 键盘。

要启用 Bloomberg 键盘支持，请参阅注册表管理的特性列表中的 Bloomberg 键盘。

验证支持：

要确定 Citrix Workspace 应用程序中是否启用了 Bloomberg 键盘支持，请检查桌面查看器是否正确报告了 Bloomberg 键盘的设备。

桌面场景：

打开桌面查看器。如果启用了 Bloomberg 键盘支持，桌面查看器会在 USB 图标下显示三个设备：

对于 Bloomberg 5 键盘：

- Bloomberg LP Bloomberg 生物识别模块
- Bloomberg LP 键盘（具有两个接口的复合设备）
- Bloomberg LP 键盘音频（具有三个接口的复合设备）

对于 Bloomberg 3 和 4 键盘：

- Bloomberg 指纹扫描仪
- Bloomberg 键盘功能
- Bloomberg LP 键盘 2013

仅限无缝应用程序场景：

从 Citrix Workspace 应用程序通知区域图标打开**连接中心**菜单。如果启用了 Bloomberg 键盘支持，这三个设备将显示在**设备**菜单中。

这些设备旁边的复选标记表示它们已远程连接到会话。

在双跳场景中支持 Windows VDA 中的按键事件序列处理

此功能可确保当客户端设备为非 Windows 且在 Unicode 模式下运行时，按键事件在 Windows 虚拟桌面代理 (VDA) 中按顺序发送。它解决了特定的输入相关问题，包括

1. 以 RDP 作为第二跳的双跳场景。
    - 使用德语键盘布局时，按住 **AltGr** 键并按下 **q** 应该会输出 @。但是，如果没有此功能，实际输出将是 **q**。
2. 键盘快捷方式功能
    - 在使用适用于 Android 的 Citrix Workspace™ 应用程序 (CWA) 时，**Alt+Tab** 快捷方式在 Windows VDA 中可能无法正常工作。

启用此功能后，这些输入不一致问题将得到解决。这可确保准确的按键事件处理并提高可用性。

此功能默认禁用。此功能的切换在注册表设置中 `EnableSendUnicodeKeyQueue`。

如果值为 1，则使用新的注册表 `HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd\EnableSendUnicodeKeyQueue` DWORD = 0/1 来切换到新的实现。

默认情况下，该值为 0。

> **注意：**
>
> 在第一跳 Windows VDA 中设置上述注册表项，以用于双跳使用场景。

Windows - 键盘和 IME 支持工具

这是一个自助式命令行工具，可以诊断与键盘和输入法编辑器相关的各种问题。

为了满足各种用户需求、提供平台通用性并为用户提供个性化需求，键盘和输入法编辑器 (IME) 的功能依赖于 VDA 和 Citrix Workspace™ 应用程序中的不同配置和功能。

VDA 或客户端的错误设置可能会导致意外的输入行为。

但是，Citrix® 为一些常见使用场景提供了推荐设置，这些推荐设置也包含在诊断结果中。

使用此工具，可以识别以下类别的问题：

- **键盘类型不一致：** 将检查 VDA 键盘类型和客户端键盘类型，以确认是否存在不一致。例如，VDA 使用 101 英语键盘，但客户端使用日语 106 键盘。此诊断针对 JP 106/109 键盘和 KO 103/106 键盘用例。
- **键盘布局同步模式不一致：** 将检查键盘布局同步设置、注册表设置、组策略，并找出给定环境中同步模式配置中的问题。
- **客户端键盘布局与 VDA 键盘布局不一致：** 将检查客户端键盘布局是否与 VDA 键盘布局相同
- **远程语言栏未显示在应用程序会话中：** 将检查当最终用户启动应用程序会话并使用多个键盘布局时，远程语言栏是否显示。

此命令行工具托管在 Windows VDA - `CtxKbImeDiagnostics.exe` 中。 命令行接口如下：

接口	描述	注意
`CtxKbimeDiagnostics`	仅显示当前 ICA® 会话的诊断结果	如果用户具有管理员权限，则显示所有活动 ICA 会话的诊断结果。如果用户没有管理员权限，则显示当前用户 ICA 会话的诊断结果
`CtxKbimeDiagnostics [-v]`	显示当前会话的设置信息和诊断结果	如果用户具有管理员权限，它将显示所有活动的 ICA 会话的诊断信息
`CtxKbimeDiagnostics [-v] [-s Session_Id]`	显示此会话的设置信息和诊断结果	
`CtxKbimeDiagnostics [-s Session_Id]`	指定一个会话并显示此会话的相应诊断结果	管理员权限可以查询其他 ICA 会话。普通用户只能查询自己的 ICA 会话
`CtxKbimeDiagnostics [-s Session_Id] [-v]`	指定一个会话并显示此会话的所有设置信息和诊断结果	管理员权限可以查询其他 ICA 会话。普通用户只能查询自己的 ICA 会话
`CtxKbimeDiagnostics [-h]`	显示支持的参数和示例	“help” 接口
`CtxKbimeDiagnostics [-V]`	显示当前工具版本	

> **注意：**
>
> 在此版本中，仅支持 CWA Windows 作为客户端。

网络摄像头

高清网络摄像头流式传输

虚拟会话中运行的视频会议应用程序可以使用网络摄像头。服务器上的应用程序根据支持的格式类型选择网络摄像头的格式和分辨率。会话启动时，客户端会将网络摄像头信息发送到服务器。从视频会议应用程序中选择一个网络摄像头。当网络摄像头和应用程序都支持高清渲染时，应用程序将使用高清分辨率。我们支持高达 1920x1080 的网络摄像头分辨率。

此功能需要适用于 Windows 的 Citrix Receiver，最低版本为 4.10。有关支持 HDX 网络摄像头重定向的 Citrix Workspace 应用程序平台列表，请参阅 Citrix Workspace 应用程序功能矩阵。

有关高清网络摄像头流式传输的详细信息，请参阅 HDX 视频会议和网络摄像头视频压缩。

您可以使用注册表项禁用和启用此功能，然后配置特定的分辨率。有关详细信息，请参阅通过注册表管理的功能列表中的 高清网络摄像头流式传输和高清网络摄像头分辨率。

图形

Citrix HDX 图形包含一整套图形加速和编码技术，可优化从 Citrix Virtual Apps and Desktops 交付富图形应用程序的性能。这些图形技术在远程使用图形密集型虚拟应用程序时，提供了与使用物理桌面相同的体验。

您可以使用软件或硬件进行图形渲染。软件渲染需要一个名为软件光栅化器的第三方库。例如，Windows 包含用于基于 DirectX 的图形的 WARP 光栅化器。有时，您可能希望使用替代的软件渲染器。硬件渲染（硬件加速）需要图形处理器 (GPU)。

HDX™ Graphics 提供默认编码配置，针对最常见的用例进行了优化。通过使用 Citrix 策略，IT 管理员还可以配置各种图形相关设置，以满足不同的要求并提供所需的用户体验。

Thinwire 显示技术

Thinwire 是 Citrix Virtual Apps and Desktops™ 中使用的 Citrix 默认显示远程处理技术。

显示远程处理技术允许将一台计算机上生成的图形（通常通过网络）传输到另一台计算机进行显示。图形是用户输入（例如击键或鼠标操作）的结果。

HDX 3D Pro 图形技术

Citrix Virtual Apps and Desktops 中的 HDX 3D Pro 功能使您能够交付使用图形处理单元 (GPU) 进行硬件加速时性能最佳的桌面和应用程序。这些应用程序包括基于 OpenGL 和 DirectX 的 3D 专业图形应用程序。标准 VDA 仅支持 DirectX 的 GPU 加速。

适用于 Windows 单会话操作系统的 GPU 加速

通过使用 HDX 3D Pro，您可以交付图形密集型应用程序，作为单会话操作系统计算机上托管桌面或应用程序的一部分。HDX 3D Pro 支持物理主机计算机（包括桌面、刀片和机架工作站）以及 XenServer®、vSphere 和 Hyper-V（仅直通）管理程序提供的 GPU 直通和 GPU 虚拟化技术。

使用 GPU 直通，您可以创建对专用图形处理硬件具有独占访问权限的 VM。您可以在管理程序上安装多个 GPU，并以一对一的方式将 VM 分配给每个 GPU。

使用 GPU 虚拟化，多个虚拟机可以直接访问单个物理 GPU 的图形处理能力。

适用于 Windows 多会话操作系统的 GPU 加速

HDX 3D Pro 允许在 Windows 多会话操作系统会话中运行的图形密集型应用程序在服务器图形处理单元 (GPU) 上进行渲染。通过将 OpenGL、DirectX、Direct3D 和 Windows Presentation Foundation (WPF) 渲染移动到服务器 GPU，图形渲染不会降低服务器 CPU 的速度。此外，由于工作负载在 CPU 和 GPU 之间分配，服务器能够处理更多图形。

弗雷姆霍克

> **重要提示：**

> 自 Citrix Virtual Apps and Desktops 7 1903 起，不再支持 Framehawk。请改用启用了 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/hdx-transport/adaptive-transport.html) 的 (/zh-cn/xenapp-and-xendesktop/current-release/graphics/thinwire.html)。

> Framehawk 是一种显示远程处理技术，适用于使用宽带无线连接（Wi-Fi 和 4G/LTE 蜂窝网络）的移动工作人员。Framehawk 克服了频谱干扰和多径传播的挑战，为虚拟应用程序和桌面的用户提供了流畅且交互式的用户体验。

基于文本的会话水印

基于文本的会话水印有助于阻止和跟踪数据盗窃。此可追溯信息显示在会话桌面上，以阻止那些使用照片和屏幕截图窃取数据的人。您可以指定一个文本层水印。水印可以显示在整个会话屏幕上，而无需更改原始文档的内容。基于文本的会话水印需要 VDA 支持。

自适应刷新率

通过新的可扩展性改进，HDX 将虚拟显示器的刷新率与目标 FPS 策略设置相匹配。自适应刷新率 (ARR) 适用于单会话和多会话 VDA，并且适用于 GPU 加速和非 GPU 场景。

丢包容忍模式

容损模式经过彻底改造，以确保在检测到数据包丢失时会话仍保持交互性。

相关信息

- (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/graphics/introduction/hdx-3d-pro-introduction.html)
- (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/graphics/introduction/gpu-acceleration-introduction.html)
- (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/graphics/introduction/gpu-acceleration-introduction.html)

- 弗雷姆霍克
- (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/graphics/introduction/thinwire-introduction.html)
- (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/graphics/introduction/session-watermark-introduction.html)

思睿线

Thinwire 是 Citrix HDX 中的核心显示远程处理技术，负责在 Citrix Virtual Apps and Desktops™ 环境中提供流畅且交互式的视觉体验。

Thinwire 分析屏幕内容，识别更改，并对屏幕上的图形数据进行编码，以便从 VDA 到用户端点设备在网络上高效传输。这确保了信息尽可能高效地发送，最大限度地减少带宽消耗并优化性能，尤其是在具有挑战性的网络条件下。

由 Thinwire 提供支持的 HDX™ Graphics 是 Citrix 的高级显示技术，旨在提供高性能、自适应且高效的远程桌面和应用程序体验。通过智能分析和压缩图形数据，Thinwire 确保在各种网络条件和端点设备上实现最佳性能。

HDX Graphics 和 Thinwire 的主要功能

- **自适应显示压缩：** Thinwire 根据内容类型和网络条件动态调整压缩算法，确保图像质量和带宽效率之间的平衡。这种适应性即使在带宽受限的环境中也能实现流畅的性能。
- **图形处理单元：** HDX Graphics 将在 VDA 上可用时自动利用 GPU 功能进行硬件编码。
- **高效多媒体重定向：** 通过将多媒体内容直接重定向到端点进行本地渲染，Thinwire 减少了服务器端处理和网络负载，从而为用户带来了无缝的多媒体体验。
- **优化文本和图像渲染：** Thinwire 利用无损文本压缩和智能图像缓存等技术，提供清晰的文本和锐利的图像，增强可读性和视觉清晰度。
- **支持高分辨率显示器：** Thinwire 可高效处理高达 8 台显示器的高分辨率和多显示器设置，为用户提供跨各种显示配置的一致且高质量的视觉体验。
- **高帧率支持：** HDX 支持高达每秒 120 帧 (fps) 的帧率，确保高动态应用程序和场景的流畅响应性能。此功能可增强用户体验，尤其是在游戏、视频编辑和其他图形密集型工作负载中。
- **10 位高动态范围：** 借助 10 位高动态范围 (HDR) 虚拟桌面会话，您可以使用增强的编码和解码功能来渲染具有更宽广色彩范围、更高对比度和亮度的优质图像和视频。

与 Microsoft 的远程桌面协议 (RDP)、VMware 的 Blast Extreme 和 Amazon 的 NICE DCV 等其他行业解决方案相比，Citrix 的 HDX Graphics 和 Thinwire 通过提供一套全面的功能而脱颖而出，这些

功能旨在满足现代远程工作环境的需求。其适应不同网络条件的能力，结合高效的资源利用和卓越的图像质量，使其成为寻求强大灵活的远程显示解决方案的组织的首选。

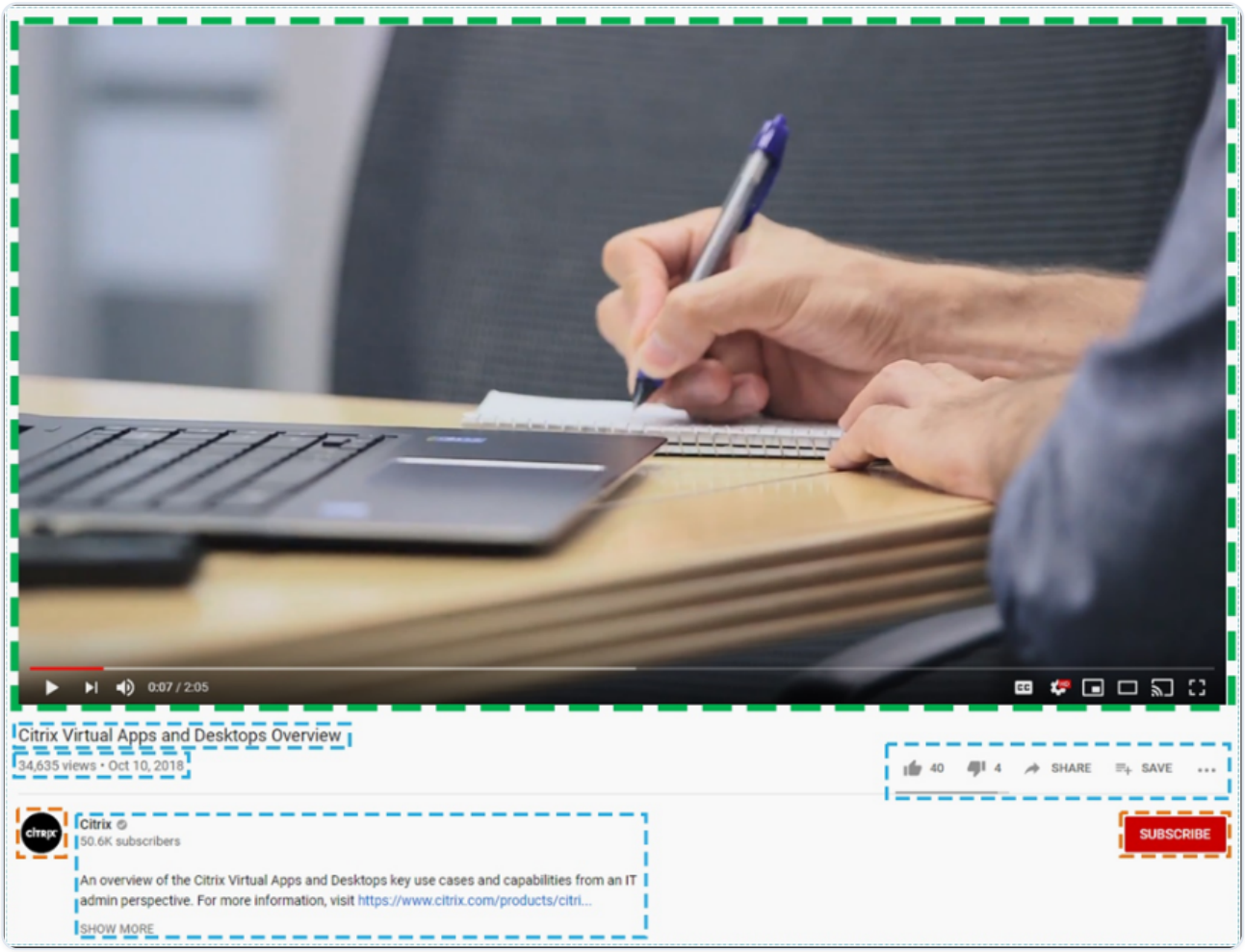
HDX Graphics 支持 VDA 上的服务器端图形处理单元 (GPU)，用于编码和渲染的硬件加速。HDX Graphics 将自动检测是否存在 GPU，并自动使用 GPU 的功能。

将 GPU 添加到 VDA 还可以帮助加速图形密集型应用程序，例如图形设计、视频渲染、3D CAD 以及数据处理和可视化应用程序。

Thinwire 分析

Thinwire 实时分析屏幕内容，并将显示数据动态分类为以下三种类型：

- 文本、简单图像和纯色
- 静态图像内容
- 动态（或流畅）图像



在上面所示的示例中，文本或简单图形以蓝色突出显示，静态图像以橙色突出显示，动态（或流畅）图像以绿色突出显示。

屏幕分析后，Thinwire 将根据 VDA 的功能和 Thinwire 配置策略，采用不同的方法尽可能高效地压缩和编码每种显示数据类别。

Thinwire 配置

Thinwire 可以根据其配置以不同的图形编码模式运行。Thinwire 的主要配置策略是“使用视频编解码器进行压缩”策略。

- 在首选时使用（默认）
- 对于活动变化区域
- 针对整个屏幕
- 不使用视频编解码器

以下部分将更详细地描述每种模式。

使用视频编解码器进行压缩设置	文本	图像	动态图像和视频	用例
在首选时使用 (GPU)	无损	JPEG	智能构建为无损/视频编解码器*	大多数工作负载的默认设置，包括图形密集型应用程序
在首选时使用（无 GPU）	无损	JPEG	视频编解码器	大多数工作负载的默认设置
对于活动变化区域	无损	JPEG	视频编解码器	
对于整个屏幕	视频编解码器	视频编解码器	视频编解码器	图形密集型应用程序（例如游戏），不首选“构建到无损”时
不使用视频编解码器	无损	JPEG	自适应 JPEG	当图像质量优于会话交互性时。由于 GPU 利用率最小化，可实现最佳可扩展性

*仅当满足特定条件时才使用智能构建到无损。

对于大多数用例，将 Thinwire 配置保留为默认设置将带来最佳性能和显示质量。

有关不同用例的更多信息，请参阅我们的 Techzone 文档：HDX 图形设计决策。

Thinwire 全屏编码器

概述

随着 Citrix Virtual Apps and Desktops™ 2503 及更高版本的发布，“优化 3D 图形工作负载”策略已被弃用并移除。

此策略已被全屏编码器取代，全屏编码器为某些图形密集型工作负载提供了增强的功能和改进的用户体验。

全屏编码器可以使用“对压缩使用视频编解码器”策略进行配置，并将其设置为“针对整个屏幕”。

全屏编码器简化了配置，同时为图形密集型工作负载提供了强大的性能。它确保使用视频编解码器对整个屏幕进行编码，放弃任何屏幕分析或带宽优化，以最大限度地提高帧速率和交互性。

此模式特别适用于 3D 应用程序和图形保真度至关重要的工作负载。

全屏编码器的主要优点是它能够利用 YUV444 颜色空间。此外，全屏编码可以提供尽可能高的帧速率，最高可达每秒 120 帧 (FPS)，而选择性编码器则不能，但因此会占用更多带宽和资源。

何时使用全屏编码器？

对于图形密集型应用程序，在尝试全屏编码器之前，应考虑“构建到无损”。可以通过将“视觉质量”策略设置为“构建到无损”，并将“使用视频编解码器进行压缩”策略保留为其默认设置“在首选时使用”来设置“构建到无损”。

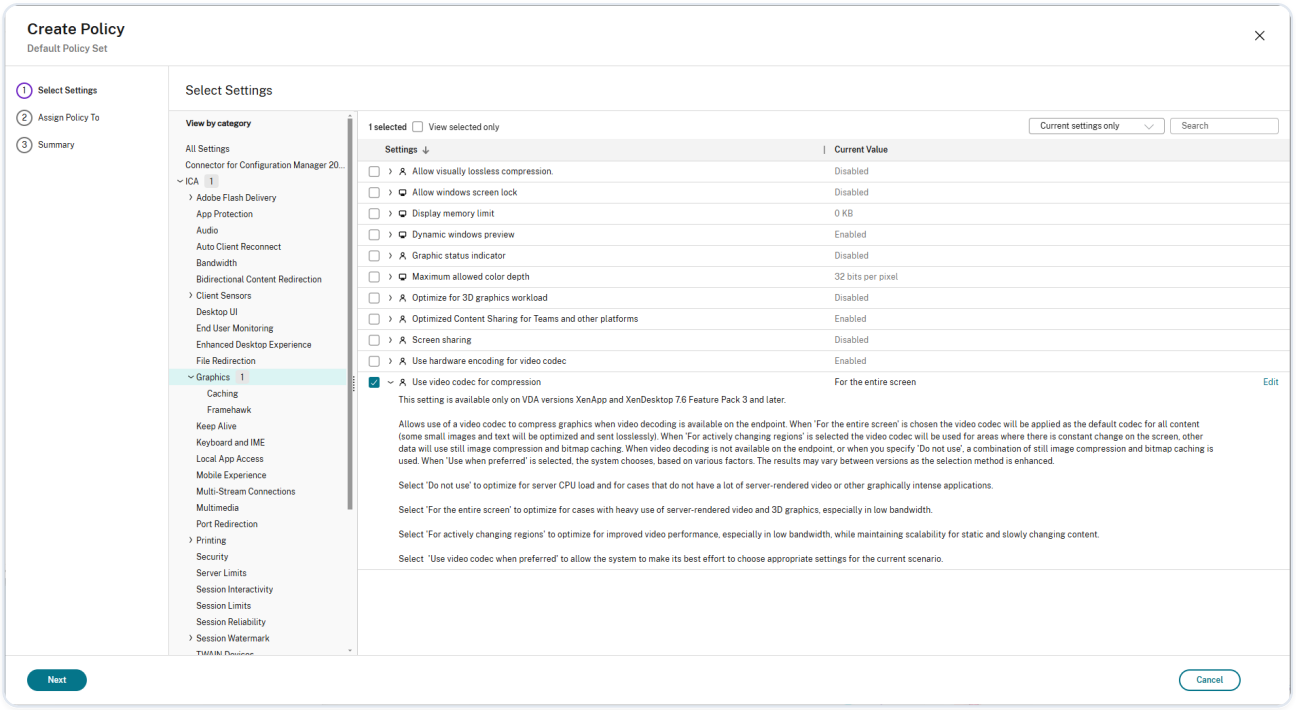
仅当需要更高的动态图像质量时才推荐使用全屏编码器，因为它支持 YUV444 颜色空间（请参阅“允许视觉无损”策略）。视频编辑是可能需要这种额外保真度的一个很好的例子，但是，这将带来相当高的带宽成本。

配置

要启用全屏编码器：

1. 导航到 Citrix Studio 中的图形策略设置。
2. 找到“使用视频编解码器进行压缩”策略。
3. 将策略设置为“用于整个屏幕”。
4. 应用策略更改并将其传播到您的交付组。

有关编解码器行为和配置的更多详细信息，请参阅自动视频编解码器配置文档。



监控

为了监控全屏编码器，可以在会话中使用图形状态指示器。目前，图形状态指示器默认未启用。

要启用图形状态指示器：

1. 导航到 Citrix Studio 中的图形策略设置。
2. 找到“图形状态指示器”策略。
3. 将策略设置为“已启用”。
4. 应用策略更改并将其传播到您的交付组。

图形编码器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/policy-enable-gsi.png)

图形状态指示器将在远程会话的任务栏中可用。

使用全屏编码器时，图形状态指示器将显示：

图形全屏(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/gsi-fs.png)

已弃用策略 - 优化 3D 图形工作负载

以前，“优化 3D 图形工作负载”策略提供了与全屏编码器类似的功能。但是，此策略缺乏高级功能。

此策略的移除简化了配置，并确保了在不同工作负载和环境中性能的一致性。

补充说明

对于利用高性能 GPU 的环境，全屏编码器可最大限度地发挥其潜力，确保复杂视觉应用程序的流畅交付。

请注意，与默认的 YUV420 相比，YUV444 提供更高的色彩保真度，但代价是增加了带宽使用量。有关更多信息，请参阅色彩空间部分。

Thinwire 选择性编码

选择性编码是 Thinwire 的默认操作模式。在此模式下，Thinwire 将实时分析屏幕内容，并选择最佳方法对屏幕的每个部分进行编码，以实现最佳视觉质量、会话保真度和带宽使用率。

选择性编码将使用：

- 文本：无损编码
- 简单图像和纯色：无损编码
- 复杂/照片图像：JPEG 编码
- 瞬态内容和动态图像：视频编解码器，采用 YUV 4:2:0 颜色模式的 H.264 / H.265 / AV1。

选择性编码具有以下特点：

- 自适应显示：Thinwire 中的自适应显示技术可识别动态图像（视频、动态 3D），并在图像移动的屏幕部分使用视频编解码器。
- 智能无损构建：当存在 GPU 时，智能无损构建可用于在检测到移动时提供最佳会话交互性，并在移动停止后提供保证的像素完美图像。Thinwire 会根据多种因素（包括响应时间监控和屏幕活动）自动为每个显示器启用智能无损构建。
- 硬件加速：如果虚拟投递代理 (VDA) 上存在 GPU，全屏编码器会利用 GPU 进行硬件加速编码，从而降低 CPU 使用率并提高性能。
- 自动视频编解码器选择：所使用的视频编解码器是根据 VDA 和客户端的功能动态选择的。支持的编解码器包括：
    - AV1：因其效率和高质量压缩而首选。
    - H.265 (HEVC)：用作不支持 AV1 的系统的备用方案。
    - H.264 (AVC)：用于旧版或低性能场景，或当 VDA 上不存在 GPU 时。

何时使用 Thinwire 选择性编码

此模式推荐用于大多数用例，并将根据可用带宽自动调整视觉质量。这些用例包括（但不限于）：

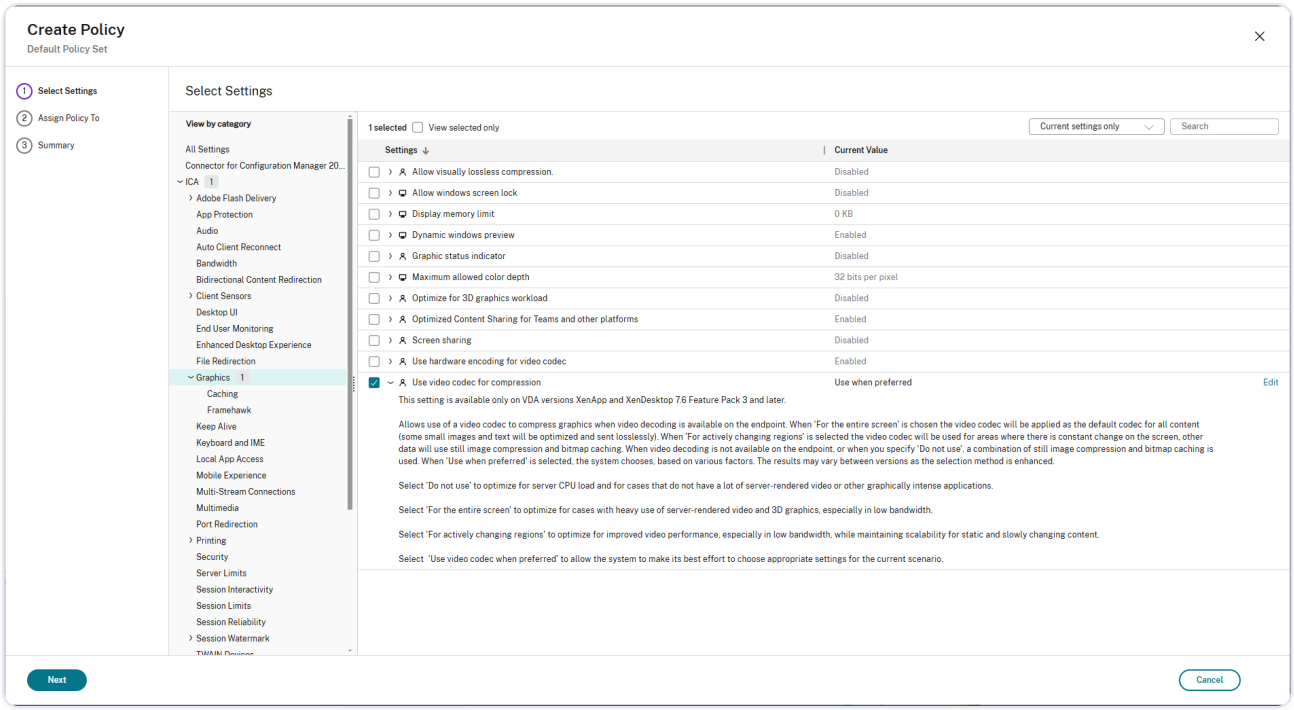
- 办公人员和开发人员。办公人员和开发人员受益于选择性编码器提供的高图像质量和清晰文本质量。
- 金融交易员：金融交易员通常使用多个高分辨率显示器。
- 2D CAD：对于 2D CAD 用例，清晰的线条和高分辨率至关重要。作为 Thinwire Selective Encoder 的一部分，智能无损构建 (Intelligent Build to Lossless) 将确保快速响应时间以及在停止移动时提供像素完美的图像。
- 医学影像：选择性编码可以与无损图像质量结合使用，为医学用例提供像素完美的图像。（待 FDA 批准）

配置

选择性编码是默认操作模式，因此无需额外配置。默认情况下，当服务器端 GPU 可用时，选择性编码将使用智能无损构建。

要显式设置选择性编码：

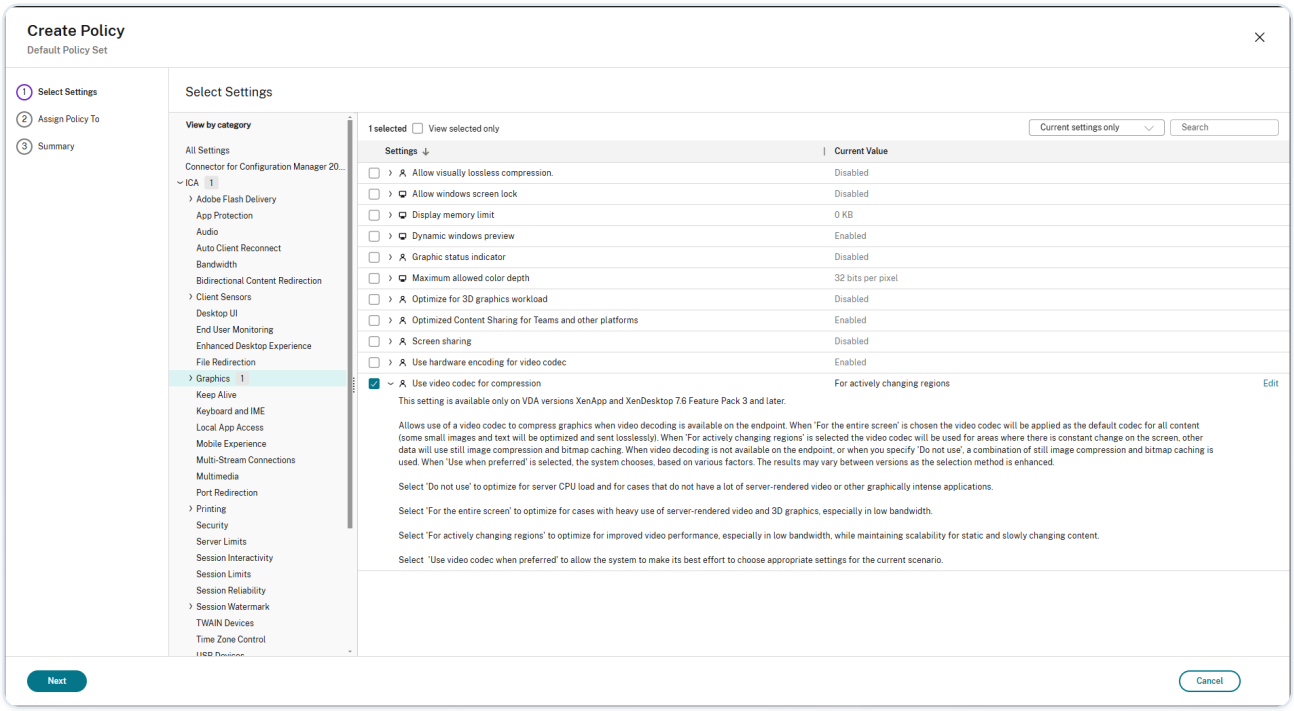
1. 导航到 Citrix Studio 中的图形策略设置。
2. 找到“使用视频编解码器进行压缩”策略。
3. 将策略设置为“在首选时使用”。
4. 应用策略更改并将其传播到您的交付组。



智能无损构建随 Citrix Virtual Apps and Desktops™ 2503 版引入。对于 2503 之前的 CVAD 版本，选择性编码将在没有智能无损构建的情况下工作。

要在没有智能无损构建的情况下对带有 GPU 的 VDA 使用选择性编码（以设置 2503 之前版本的旧版行为）：

1. 导航到 Citrix Studio 中的图形策略设置。
2. 找到“使用视频编解码器进行压缩”策略。
3. 将策略设置为“对于活动更改区域”。
4. 应用策略更改并将其传播到您的交付组。



请注意，对于 2503 之前的版本，“在首选时使用”和“对于活动更改区域”是相同的。在 2503 中，当 GPU 可用时，“在首选时使用”的默认设置包括智能无损构建。在没有 GPU 的情况下，“在首选时使用”与“对于活动更改区域”相同。

构建无损

构建无损是一种特殊的 Thinwire 配置，可优化图形交付以实现交互性和最终图像质量。您可以通过将视觉质量策略设置为“构建无损”来启用此设置。

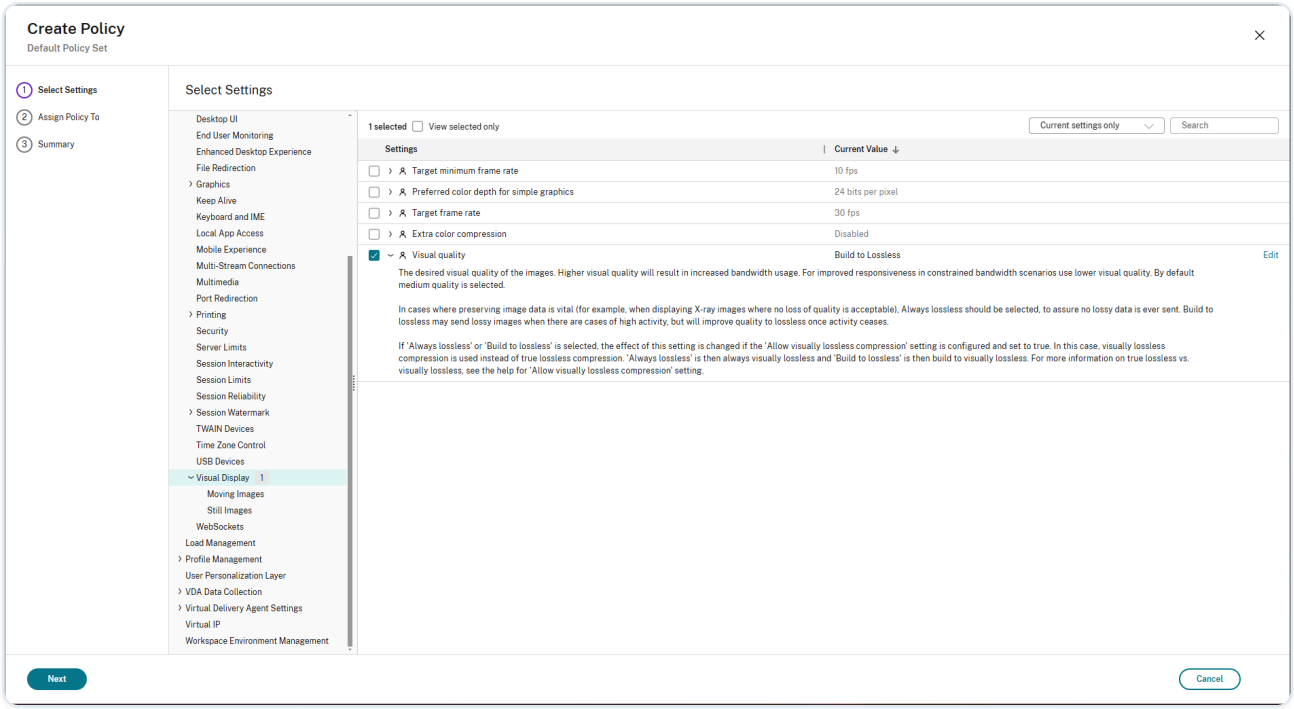
构建无损旨在尽可能轻量化，并将禁用常规选择性编码中执行的大部分 Thinwire 图像分析。它采用“模糊优先”方法，假设有损编解码器在移动图像方面会提供更好的性能，并且当运动停止时，将逐渐构建为保证无损的图像。

构建无损在屏幕活动期间使用所选视频编解码器（AV1、H.265 或 H.264）压缩屏幕，并在活动停止时锐化至像素完美（无损）。有损图像质量会根据可用资源进行调整，以保持最佳帧率。锐化步骤是逐步执行的，从鼠标光标向外辐射。这允许用户在锐化开始后不久开始屏幕活动时立即响应。例如，选择一个模型并旋转它。

对于常规的构建无损，启用后所有显示器都将在构建无损模式下运行。如果您正在寻找在选定显示器上运行构建无损的功能，请参阅下面我们新的智能构建无损功能。

可以通过使用视觉质量策略设置来启用构建无损。

1. 导航到 Citrix Studio 中的图形策略设置。
2. 找到“视觉质量”策略。
3. 将策略设置为“构建无损”。
4. 将策略更改应用并传播到您的交付组。



何时使用常规构建到无损？

常规构建到无损旨在用于以下用例

- 全屏 3D CAD
- 全屏 2D CAD
- 某些医学影像模式
- 金融/交易员

对于所有这些用例，当在 Citrix® 会话中使用多显示器时，请考虑使用智能构建到无损，而不是常规构建到无损。

智能无损构建

本文介绍了 Citrix HDX 的智能无损构建图形模式。它解释了该功能的工作原理、如何配置以及如何验证和监控其操作。它还将此模式与现有的无损构建和始终无损视觉质量设置进行了比较。

智能无损构建专为混合工作负载而设计，是 Thinwire 选择性编码的演进，也是新的默认图形模式。与现有的无损构建设置类似，智能无损构建在大型、活跃变化的屏幕区域上使用视频编解码器，以保持会话图形的流畅性。当屏幕活动停止时，它会逐步优化图像，直到达到像素完美。智能无损构建与现有无损构建设置的不同之处在于模式的切换方式：是否启用无损构建的选择不再仅仅是策略决策，而是基于屏幕活动和其他因素。此外，此决策是基于每个显示器做出的，这首次允许在同一会话中混合使用 Thinwire 选择性编码和无损构建。

对于 Citrix Virtual Apps and Desktops™ 2503 版及更高版本，当 VDA 上存在 GPU 时，智能无损构建默认启用。当 VDA 上不存在 GPU 时，将使用不带智能无损构建的选择性编码，这与 2503 版之前选择性编码的工作方式基本相同。

无需升级 Citrix Workspace™ 应用程序即可利用智能无损构建。

比较图形模式 - 智能BTL 对比 BTL 对比 始终无损

下表重点介绍了智能 BTL、BTL 和始终无损之间的主要区别：

功能	智能构建到无损（推荐）	构建到无损	始终无损
配置	默认启用，通过 GPU 启用的 VDA 上的“使用视频编解码器进行压缩”策略控制	视觉质量策略设置为“构建到无损”	视觉质量策略设置为“始终无损”
激活	动态。Thinwire 根据屏幕内容智能地激活和停用。	在整个会话期间始终开启。	在整个会话期间始终开启。
范围	按显示器。仅在需要“构建到无损”的显示器上实时激活和停用。	影响连接到会话的所有显示器，这可能导致生产力应用程序（例如电子邮件）以两次传递的方式呈现。	影响连接到会话的所有显示器。
带宽消耗	中等到低，取决于屏幕活动。	中等，取决于屏幕活动。	高。

功能	智能构建到无损（推荐）	构建到无损	始终无损
用例	GPU 启用型 VDA 上所有用例的默认模式。对于没有 GPU 的 VDA，将使用选择性编码，类似于 2503 之前的 VDA。	已被智能无损构建取代。不建议用于 GPU 启用型 VDA 的新部署。	在所有用例中，包括运动期间，每个帧都必须是无损的。

先决条件

智能无损构建是所有启用 GPU 的 VDA 用例的新默认模式。

VDA

智能无损构建适用于 Windows、Linux 和 Mac VDA。

请务必注意，CVAD 版本要求因操作系统而异。

- **Windows VDA：** CVAD 2503 或更高版本
- **Linux VDA：** CVAD 2503 或更高版本
- **macOS VDA：** 2507 或更高版本

VDA 硬件：需要服务器端 GPU（NVIDIA、AMD 或 Intel）。

有关更多信息，请参阅适用于 Linux VDA 的智能无损构建。

> **注意：**
>
> 智能无损构建在没有 GPU 的 VDA 上不可用。

Citrix Workspace™ 应用程序

Citrix Workspace 应用程序：所有当前支持的版本。

智能无损构建独立于客户端硬件，适用于所有客户端，无论它们是否具有客户端 GPU。

何时使用智能无损构建?

智能无损构建适用于所有工作负载和网络场景。它特别适合混合工作负载以及最终用户使用多个显示器和高分辨率显示器的用例，例如高端金融交易员。

对于运行 Citrix Virtual Apps and Desktops™ 2503 或更高版本并配备服务器端 GPU 的 VDA，智能无损构建默认启用。

没有额外的端点要求；但是，Citrix® 始终建议使用最新可用的 CWA 客户端版本。

VDA 版本	服务器端 GPU	智能无损构建
VDA 2503 之前的版本	是	否
VDA 2503 之前的版本	否	否
VDA 2503 或更高版本	**是**	**是**
VDA 2503 或更高版本	否	否

Citrix 建议在以下场景中使用智能无损构建：

医学影像：

用于查看诊断图像，例如 X 射线、MRI 或 CT 扫描，其中压缩伪影可能会模糊细节并损害临床准确性。

3D CAD/CAM 和工程：

在处理复杂精密的模型和蓝图时，精确的线条清晰度对于设计和制造都至关重要。

印前和平面设计：

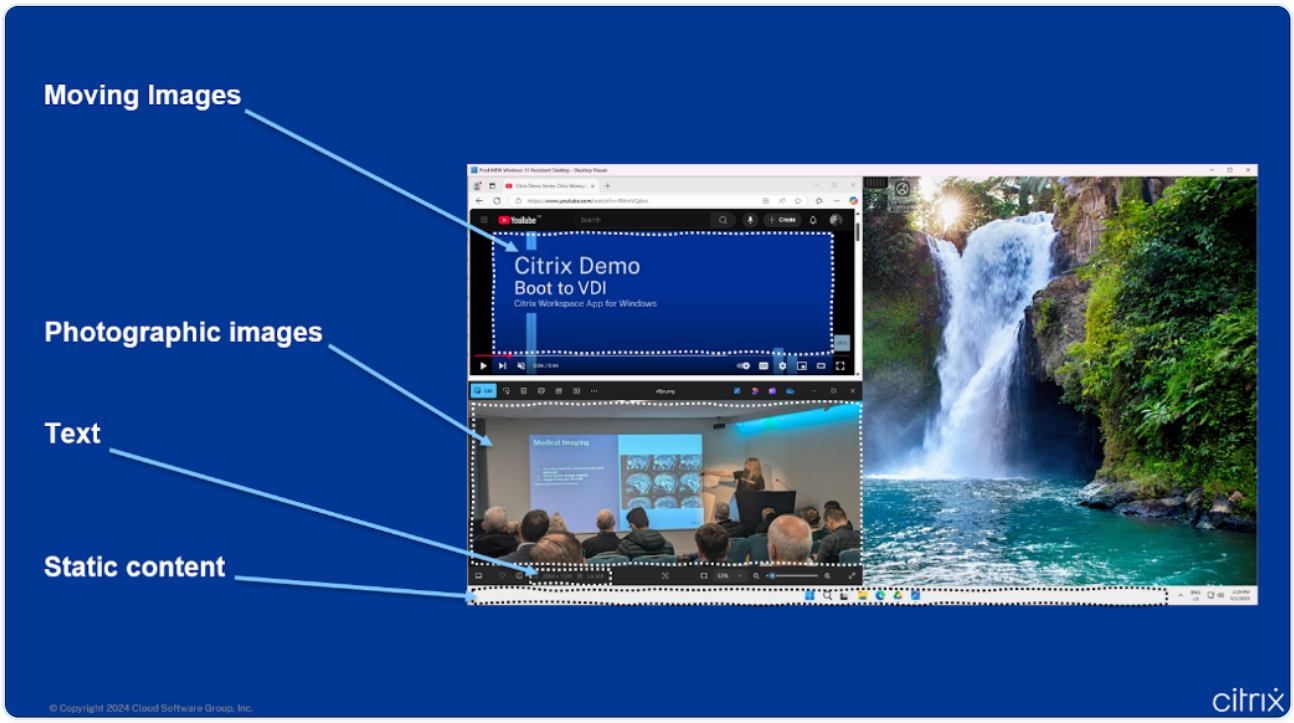
用于审阅彩色打样、高分辨率图像或文本布局，在这些情况下，需要查看实际的高质量源材料以进行质量控制。

金融服务：

用于在交易大厅显示密集的实时数据，在使用多个高分辨率显示器时，静态图表和数字的绝对清晰度对于分析至关重要。

工作原理?

该功能作为 HDX™ Thinwire 显示协议的一部分运行。



1. 一旦 Thinwire 检测到屏幕区域有移动图像，它会根据 VDA 和客户端的功能，使用配置的视频编解码器（H.264、H.265 或 AV1）对该区域进行编码。这优先考虑帧率和响应速度。
2. 当屏幕区域变为静态（即未检测到移动）时，Thinwire 将通过一系列针对静态区域的精细化更新，逐步将该区域构建为无损状态。

配置

在 Citrix Virtual Apps and Desktops™ 2503 及更高版本中，支持 GPU 的 VDA 默认启用 Intelligent Build to Lossless。您无需创建任何策略即可启用它。其行为由“使用视频编解码器进行压缩”策略的状态控制：

启用 Intelligent Build to Lossless（默认行为）

将“使用视频编解码器进行压缩”策略保留为 *未配置*。或者，您可以将 *使用视频编解码器进行压缩策略* 显式设置为 *在首选时使用*。

禁用 Intelligent Build to Lossless（不推荐）

将“使用视频编解码器进行压缩”策略显式设置为“用于活动更改区域”。

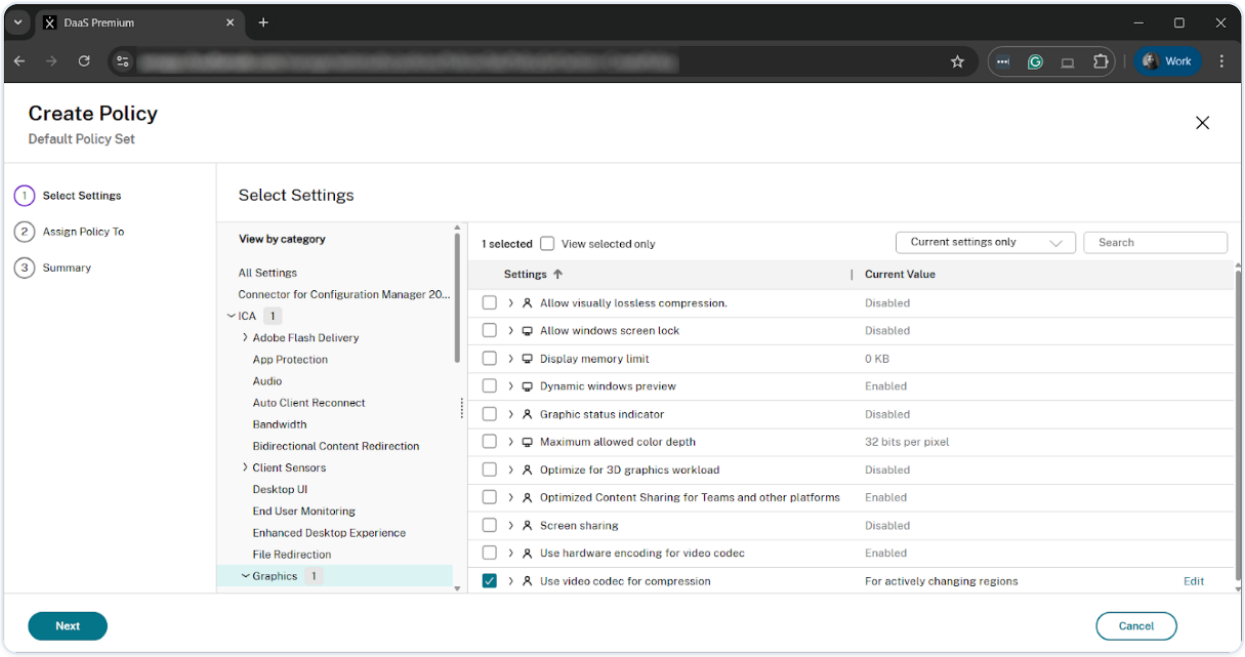
选择“用于活动更改区域”将导致 Thinwire 使用选择性编码，就像在 2503 之前的带有服务器端 GPU 的 VDA 中一样。

分步说明

要使用 Citrix Studio 显式禁用 Intelligent Build to Lossless 策略，请按照以下说明操作。

CITRIX STUDIO（图形用户界面）

1. **打开** Citrix Studio 应用程序。
2. 在左侧窗格中，导航到**策略**。
3. 单击**创建策略**或编辑适用于目标用户或交付组的现有策略。
4. 在策略配置窗口中，使用搜索栏查找**使用视频编解码器进行压缩**策略，该策略位于 **ICA®** > **图形**类别下。
5. **选择**该策略，然后单击**编辑**。
6. 默认情况下，此策略设置为**在首选时使用**。取消选中**使用默认值**选项。
7. 将值更改为用于主动更改的区域。
8. 单击 **确定** 以保存策略设置。
9. 确保策略已启用、优先级正确，并应用于相应的 **交付组** 或用户筛选器。



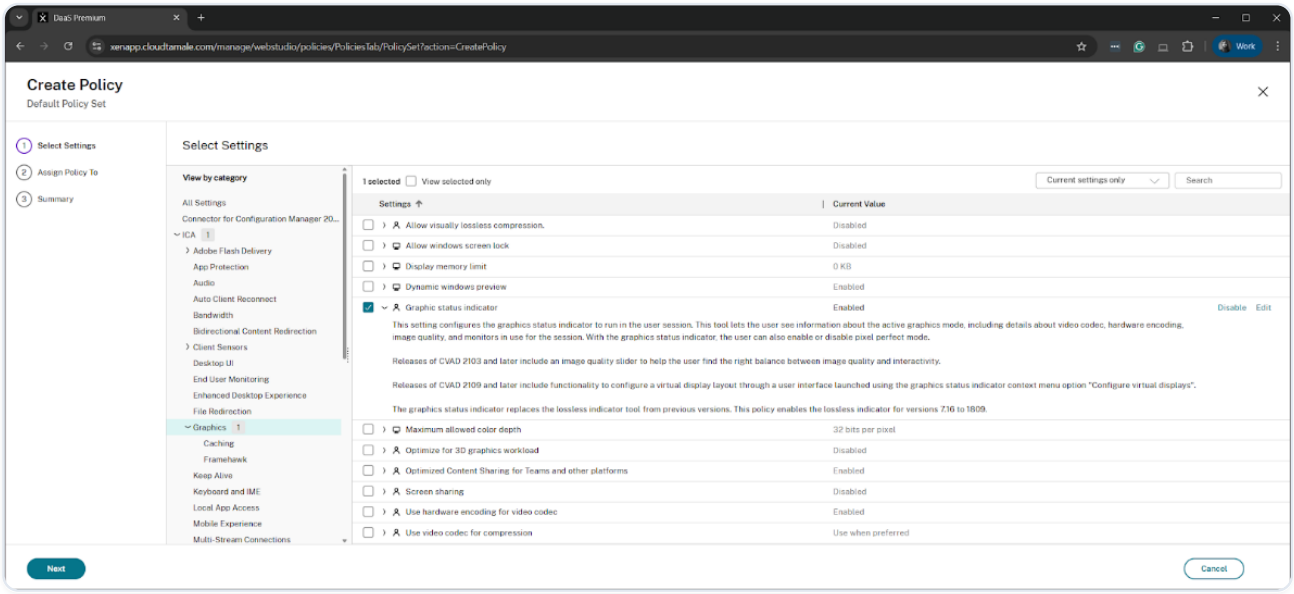
> **注意：**
>
> 如果视觉质量策略明确设置为“构建到无损”或“始终无损”，则这些设置将始终优先并覆盖新的智能构建到无损功能。为获得最佳效果，请将“视觉质量”策略和“使用视频编解码器进行压缩”设置保留为默认值。

监控智能无损构建

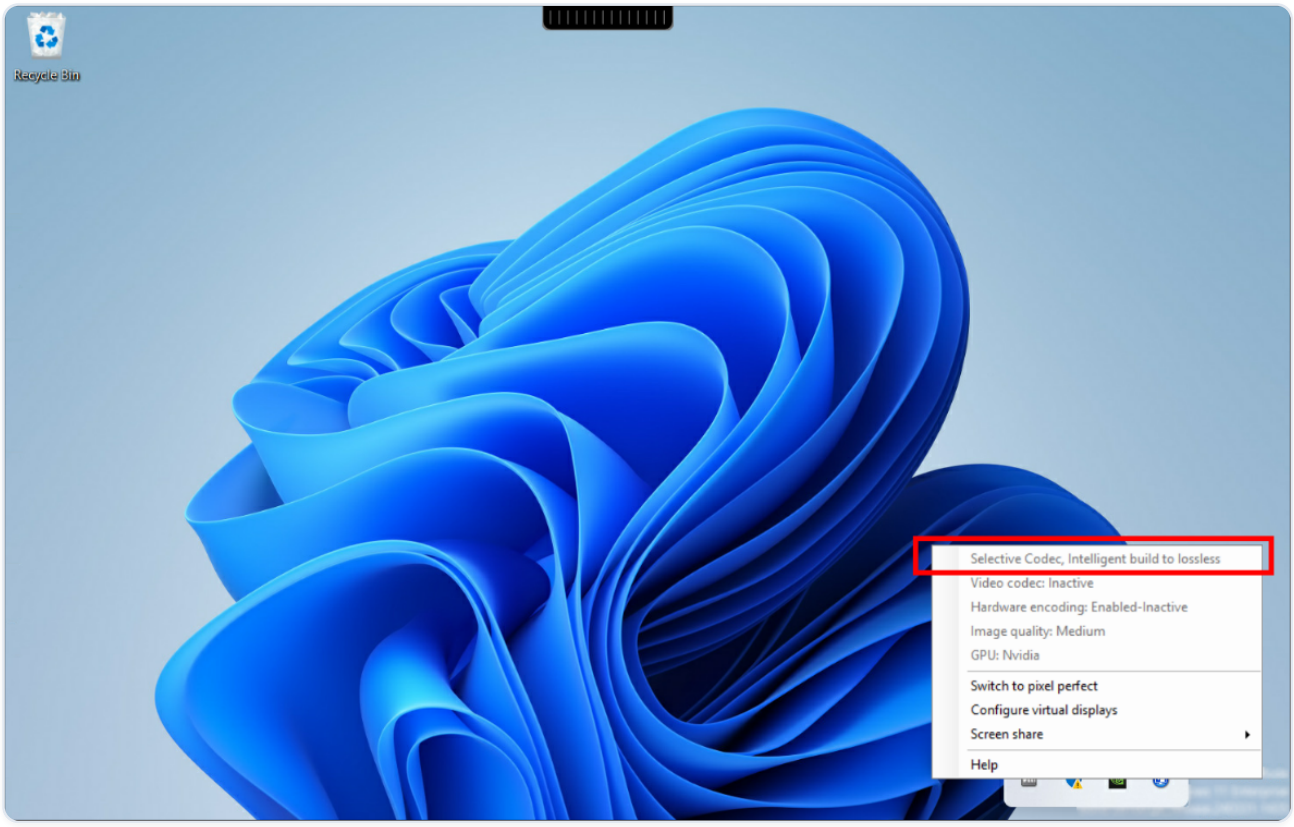
智能无损构建可以通过我们的图形状态指示器在 Citrix® 会话中进行监控。目前，图形状态指示器默认未启用。

启用图形状态指示器

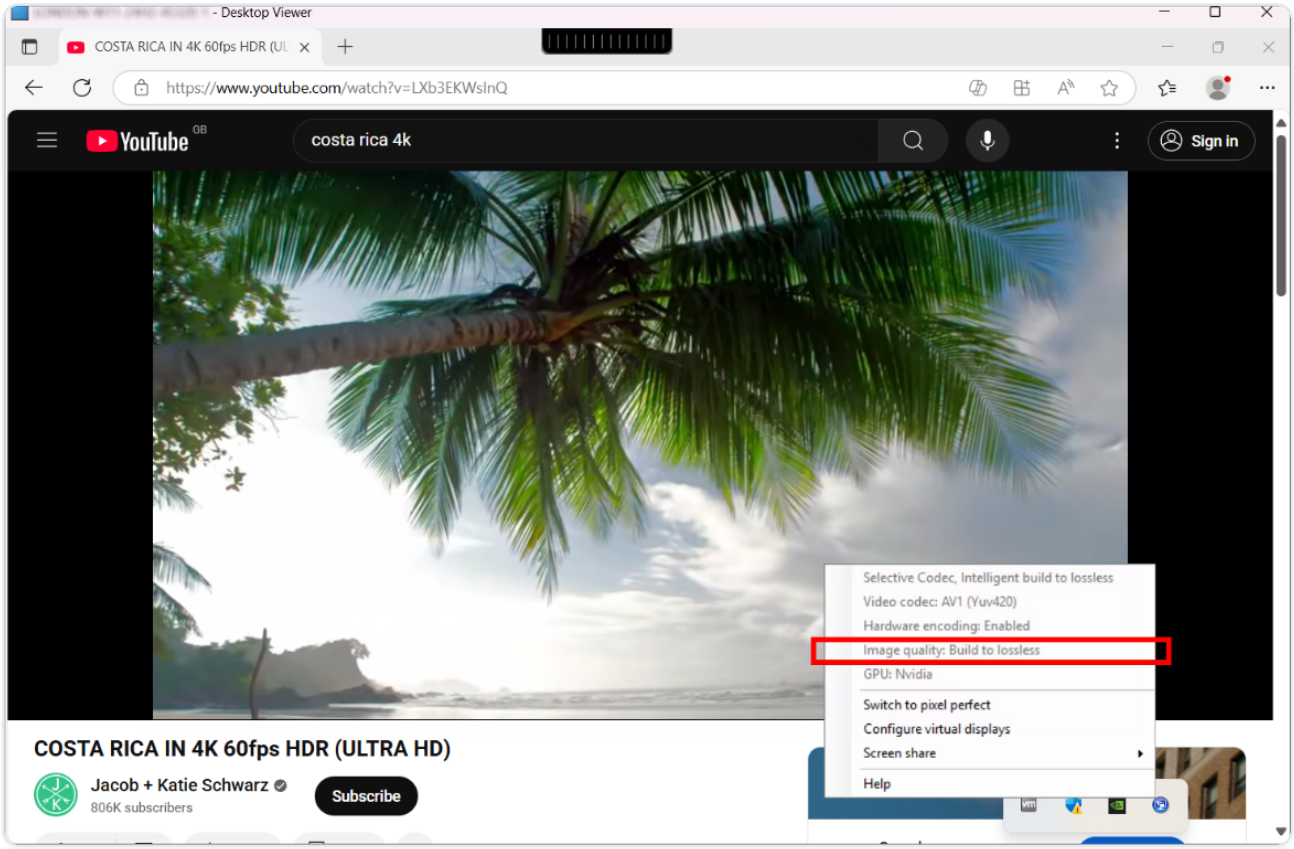
1. 打开 Citrix Studio。
2. 在左侧窗格中，导航到**策略**。
3. 单击**创建策略**或编辑适用于目标用户或交付组的现有策略。
4. 在策略配置窗口中，使用搜索栏查找**图形状态指示器**策略，该策略位于 **ICA® > 图形**类别下。
5. 选择该**策略**，然后单击**启用**。
6. 单击**确定**以保存策略设置。
7. 确保策略已启用、优先级正确，并应用于相应的**交付组**或用户筛选器。



当智能无损构建在用户会话中可用但尚未激活时，会话将使用常规选择性编码，图形状态指示器将在顶行显示为“选择性编解码器，智能无损构建”。由于智能无损构建尚未启用，“视觉质量”将列出当前配置的视觉质量，例如低、中或高。

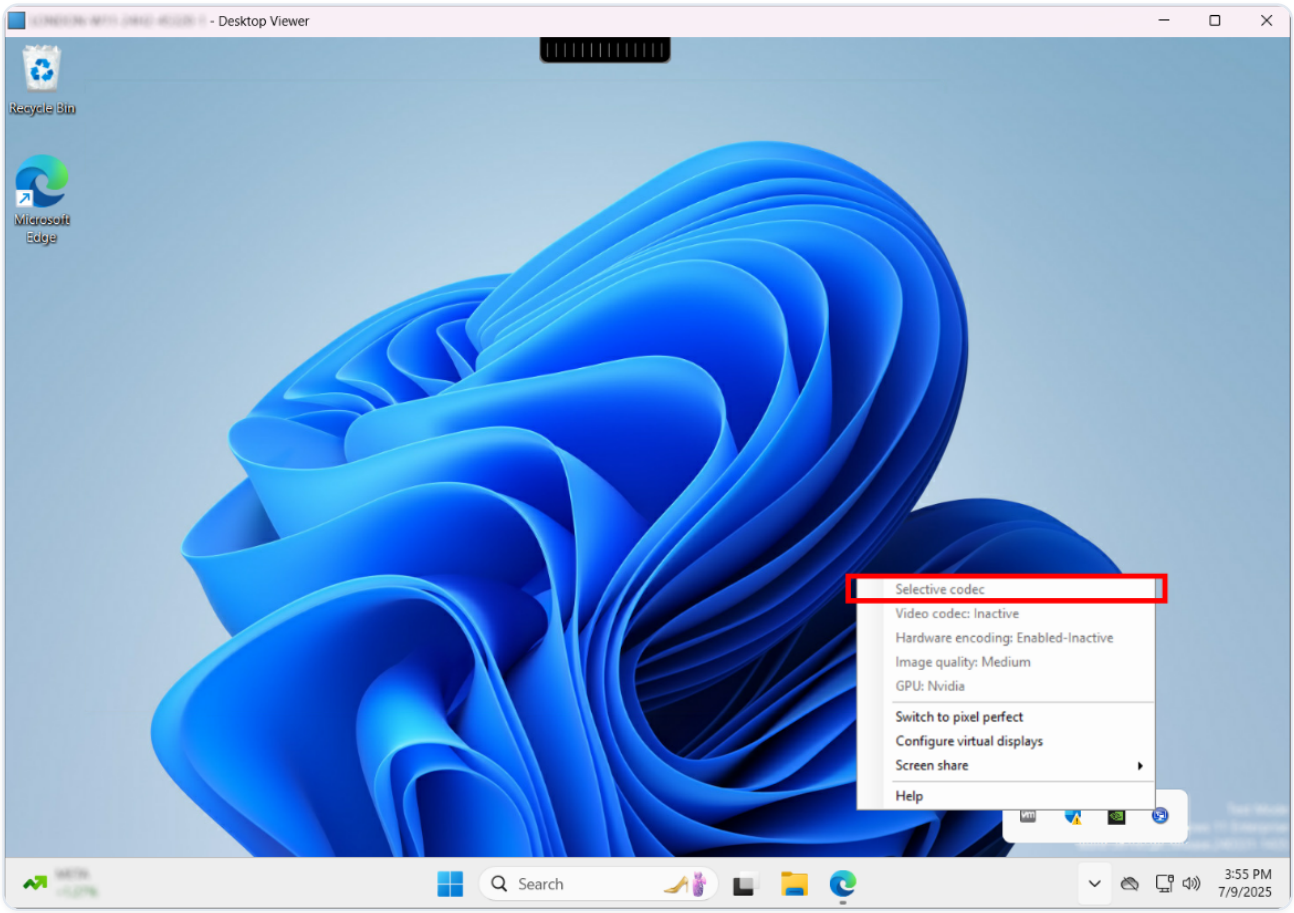


当 Thinwire 检测到有利于在一个或多个连接的显示器上启用智能无损构建的条件时，图形状态指示器会将第四行的“视觉质量”更改为“无损构建”。这是智能无损构建处于活动状态的主要指示。



当 Thinwire 确定不再需要无损构建时，它将逐渐构建出像素完美的图像，然后恢复到常规的选择性编码。图形状态指示器会将图像质量更改回配置的视觉质量模式，例如低、中或高。

如果智能无损构建不可用，例如，在使用 2503 之前的版本 VDA、没有服务器端 GPU 的 VDA，或者智能无损构建被明确禁用时，图形状态指示器将在顶行显示“选择性编解码器”：



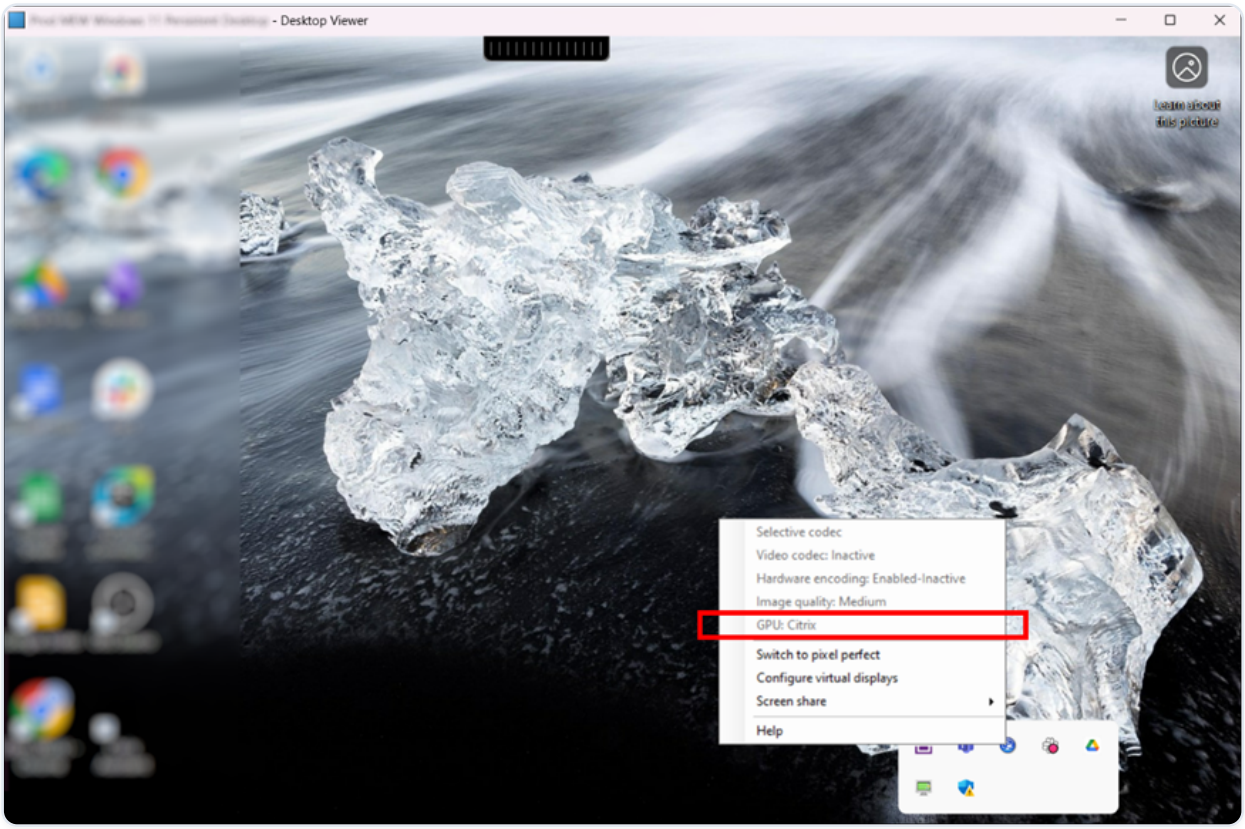
为了对智能无损构建进行更深入的测试和监控，您还可以启用一个逐显示器视觉指示器，该指示器将显示哪个显示器处于无损构建模式。

此设置仅用于测试和故障排除，不应在生产环境中使用。有关更多信息，请参阅知识库文章以启用智能无损构建视觉指示器。

故障排除

如果会话中无法使用智能无损构建，请检查以下要求：

1. 确保 VDA 运行版本 2503 或更高版本。
2. 确保会话中存在服务器端 GPU。验证此项最简单的方法是使用图形状态指示器，并检查 GPU 行是否显示 GPU 供应商名称，例如 NVIDIA、Intel 或 AMD。如果不存在可用 GPU，则 GPU 供应商名称将显示“Citrix”：



或者，您可以使用 Citrix Monitor 查看 VDA 的服务器端 GPU 是否存在，并排查 GPU 利用率。

3. 验证“使用视频编解码器进行压缩”策略是未设置（并使用默认值）还是设置为“在首选时使用”。

您可以使用 策略建模向导 来确定策略是否已正确应用于会话。

有关 DaaS 方面的更多信息，请参阅 策略流程。

不要使用视频编解码器

使用视频编解码器对远程会话进行编码有几个优点，它速度快且相对轻量。视频编解码器专为动态图像设计，并非常擅长处理动态图像，这在远程会话中很常见。

然而，在某些情况下，使用视频编解码器可能不是最佳解决方案，例如当图像质量或色彩准确性至关重要时。我们的选择性编码器在大多数情况下都能很好地确定屏幕的哪些部分受益于视频编解码器编码，您也可以强制 Thinwire 永不使用视频编解码器进行屏幕压缩。

当 Thinwire 设置为不使用视频编解码器时，Thinwire 将仅使用 JPEG 和无损 RLE 进行压缩，从而保持最佳图像质量。与使用选择性编码或全屏编码相比，Thinwire 将占用更多的带宽。

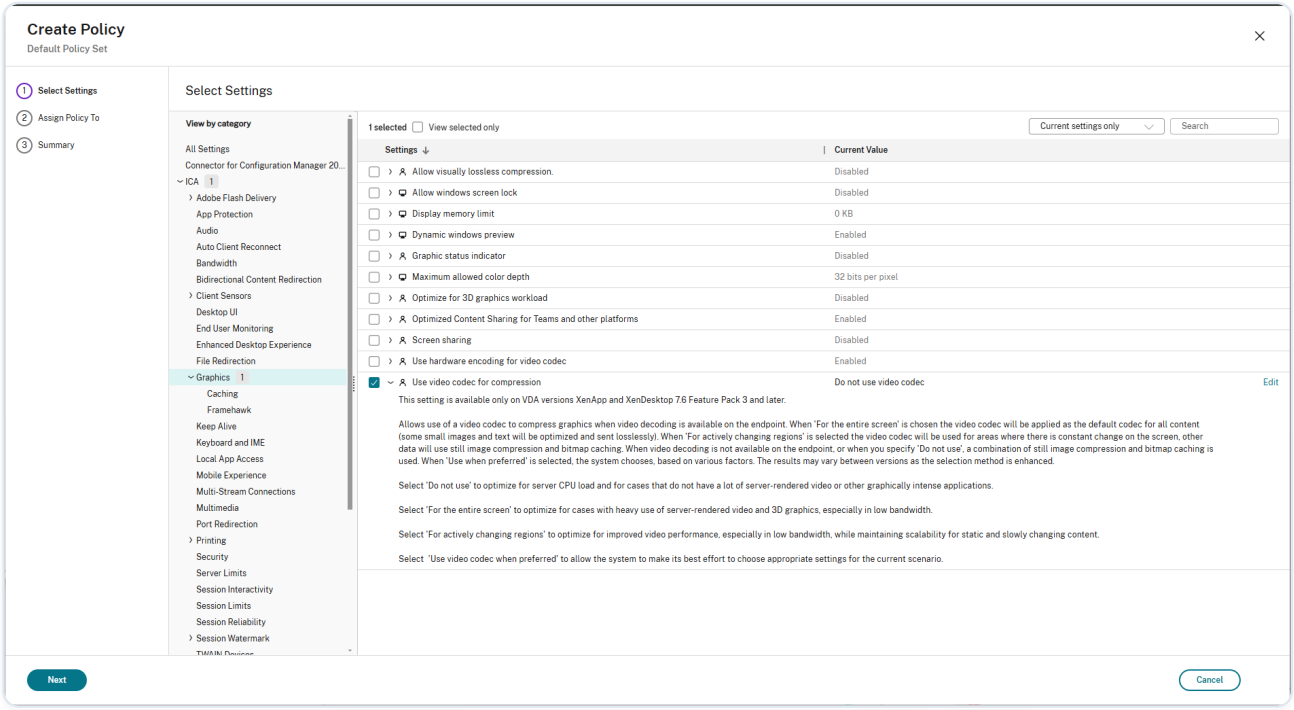
何时不使用视频编解码器

在图像质量与 VDA 可伸缩性相结合是重要因素的场景中，您可以考虑使用我们的 Thinwire 全屏编码器模式。不使用视频编解码器可以最大化 VDA 可伸缩性，因为它通常比使用视频编解码器进行压缩具有更低的 CPU 开销。

然而，在大多数情况下，我们的选择性编码器，尤其是在与无损构建或智能无损构建结合使用时，将提供与不使用视频编解码器压缩时相同的质量、更好的性能和更低的带宽。

配置

将 Thinwire 策略“使用视频编解码器进行压缩”设置为“不使用视频编解码器”

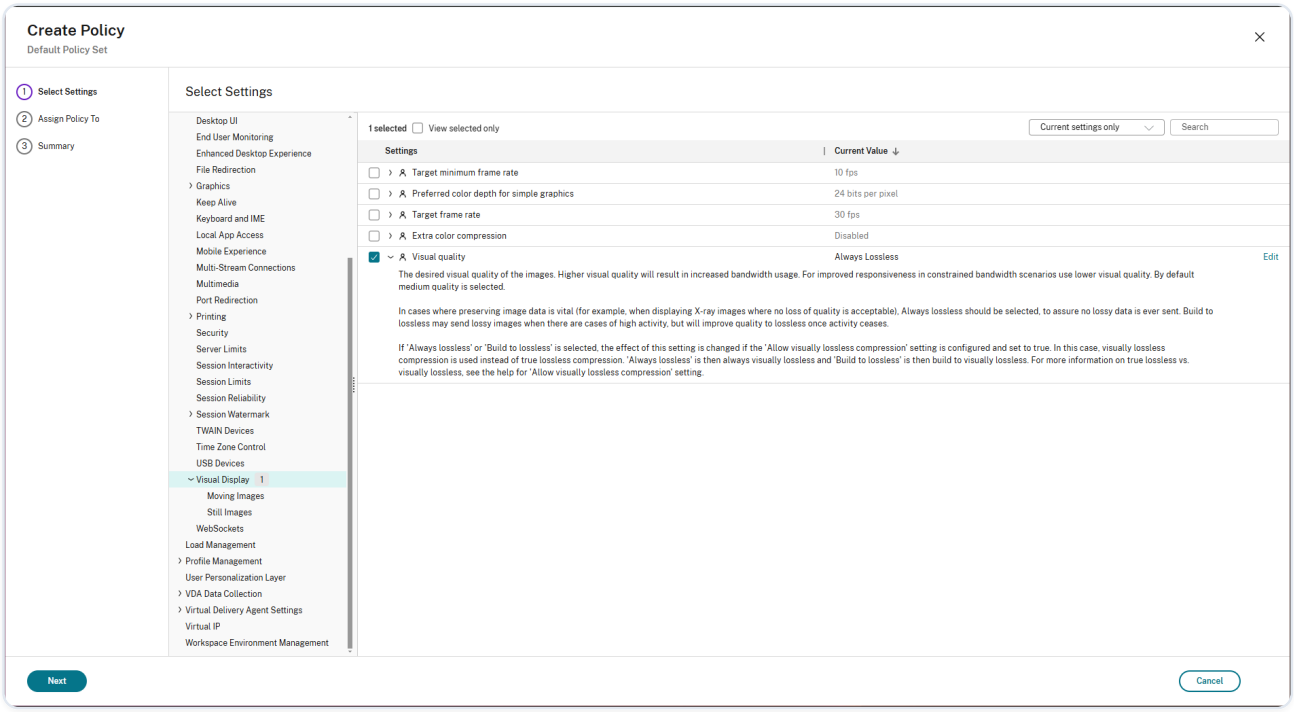


始终无损模式

使用始终无损模式可确保不会向客户端发送任何有损图像数据。这意味着每个帧都将仅使用无损编解码器进行编码，并且质量将达到像素级完美。

始终无损的压缩比远不如使用其他模式，并且设置始终无损模式将占用大量带宽。当可用带宽不足时，这会显著影响交互性。

Citrix® 仅建议在需要无损图像质量的特定用例（例如医学成像用例）中使用此设置。

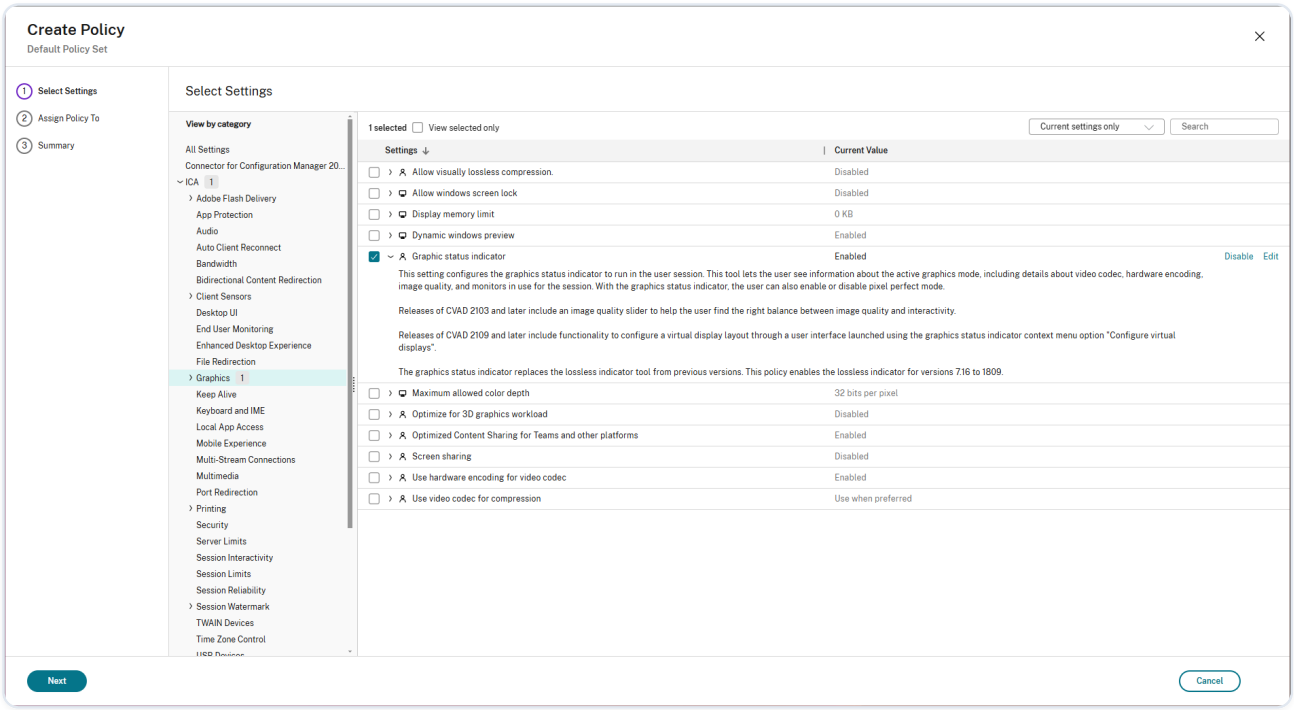


除了明确设置始终无损模式外，当图形状态指示器可用时，最终用户还可以在会话中切换无损模式。

目前，图形状态指示器默认未启用。

要启用图形状态指示器：

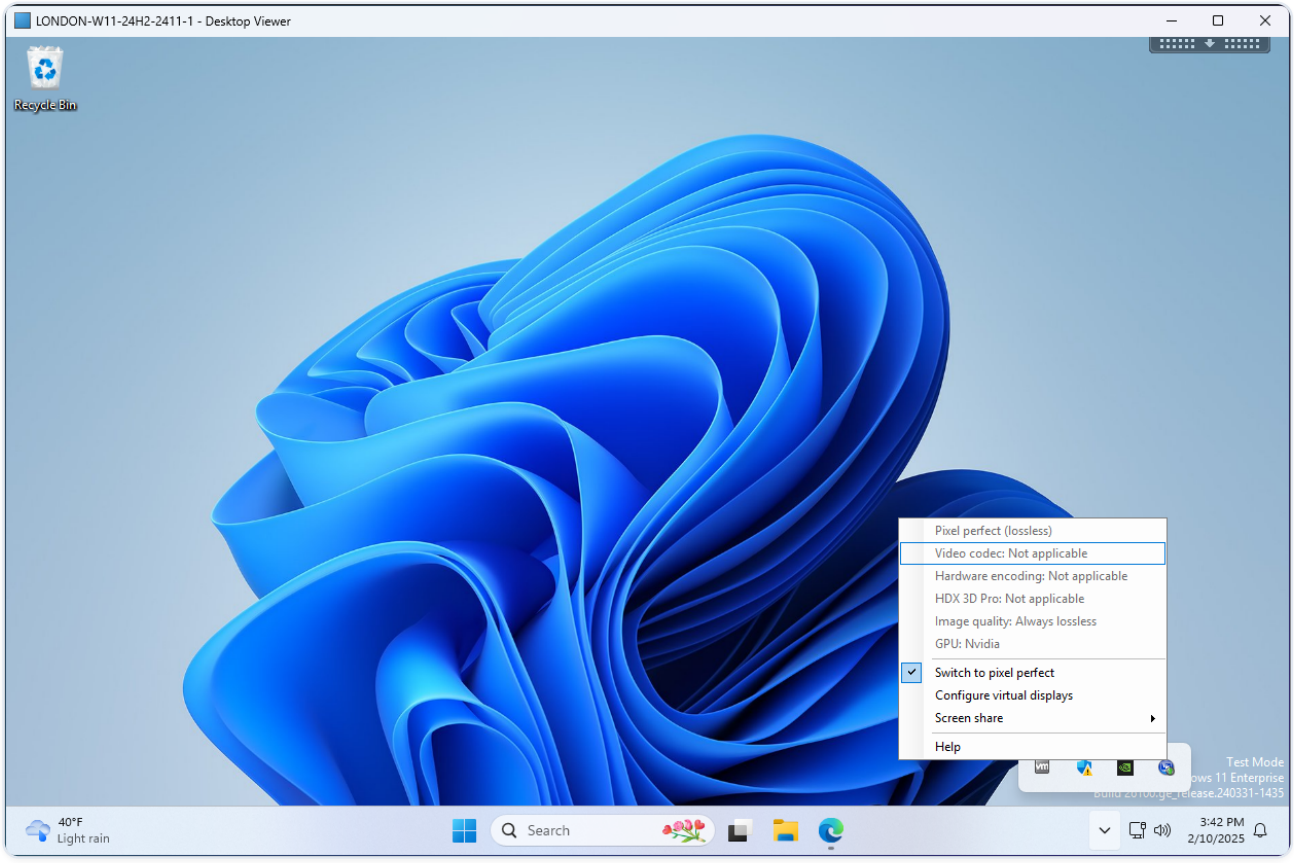
1. 导航到 Citrix Studio 中的图形策略设置。
2. 找到“图形状态指示器”策略。
3. 将策略设置为“已启用”。
4. 应用策略更改并将其传播到您的交付组。



作为最终用户切换始终无损模式：

1. 在任务栏中找到图形状态指示器。
2. 在 VDA 的任务栏中右键单击图形状态 1. 1. 指示器。
3. 选择“切换到像素完美”。

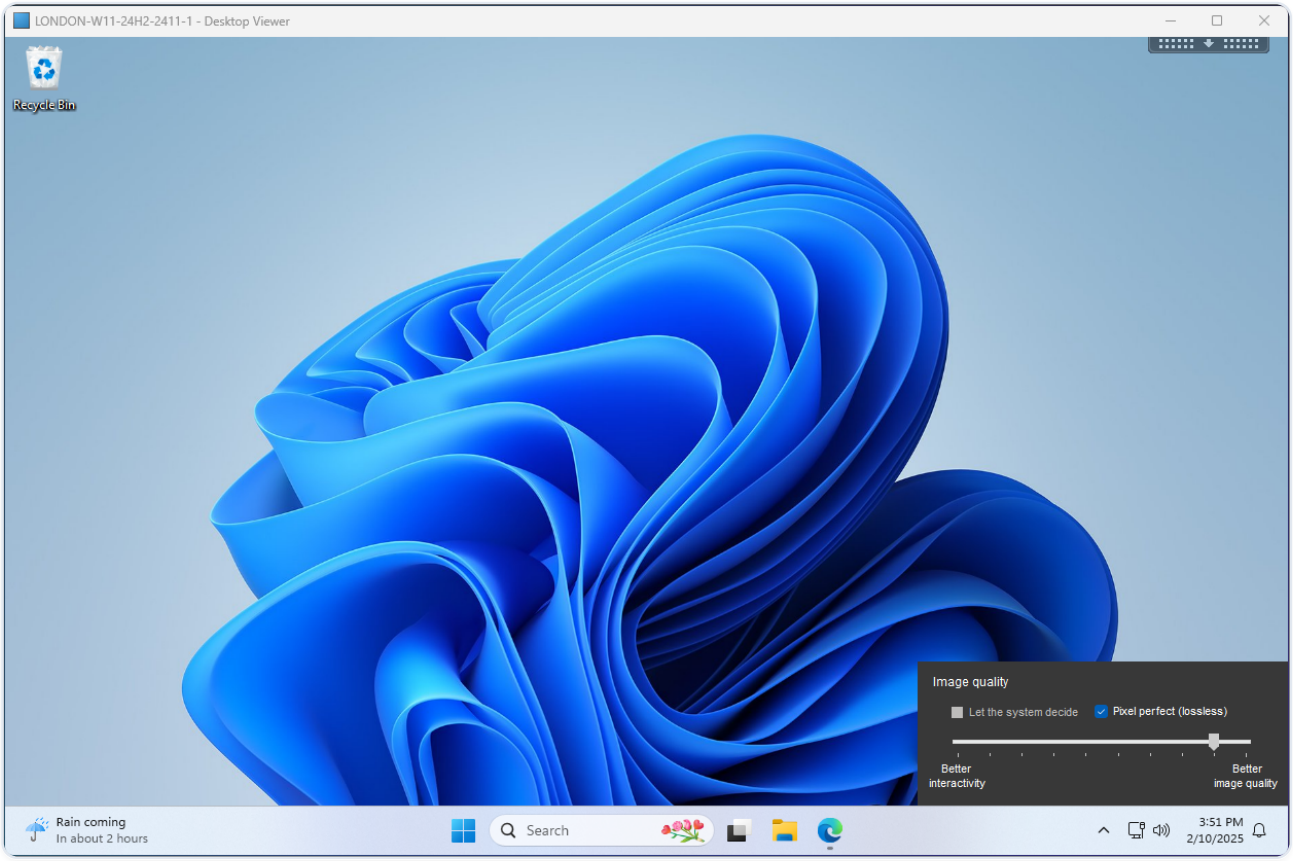
图形状态指示器将在图标中显示绿色指示器，以指示无损模式已启用。



或者：

1. 在任务栏中找到图形状态指示器。
2. 单击 VDA 任务栏中的图形状态指示器。
3. 取消选择“让系统决定”。
4. 选择“像素完美（无损）”。

图形状态指示器将在图标中显示绿色指示器，以指示无损模式已启用。



色彩空间

这是一个新章节，讨论 YUV 4:2:0 和 YUV 4:4:4 的色彩空间和色彩压缩设置。

概述

所选的色彩空间将决定 HDX™ Graphics 是否以及使用何种色彩压缩模式（也称为色度子采样）。默认情况下，HDX Graphics 使用 YUV 4:2:0 色度子采样。

色度子采样是一种用于减少从 VDA 到客户端传输视频数据所需带宽的技术。它通过减少传输的颜色信息量来实现，因为人眼对亮度（luminance）变化的敏感度高于对颜色（chrominance）变化的敏感度。

存在不同的色度子采样方案，由 4:2:0、4:2:2 和 4:4:4 等比率表示。这些比率表示相对于亮度信息采样的色度信息量。

4:4:4 - 无色度子采样。保留所有颜色信息。这提供了最高的图像质量和色彩准确性，但需要最大的带宽。

4:2:0 - 色度信息在水平和垂直方向上均以 2 倍因子进行子采样。这提供了最大的带宽减少，但可能会导致明显的颜色伪影。



Citrix HDX 图形利用色度子采样来优化虚拟桌面环境中的带宽使用。默认情况下，HDX 使用 YUV 4:2:0 对屏幕内容进行编码。这为典型的办公生产力应用程序/大多数用例提供了图像质量和带宽效率之间的良好平衡。

当整个屏幕使用视频编解码器（通过使用全屏编码器）进行编码时，色彩压缩会降低文本等高对比度细节的质量，使其变得模糊且难以阅读。

对于色彩准确性至关重要的场景，例如医学成像、视频编辑或 CAD/CAM 应用程序，HDX 也支持 YUV 4:4:4。

这确保了在编码过程中不会丢失任何颜色信息，从而提供最高的图像保真度和色彩准确性。请注意，YUV 4:4:4 比 YUV 4:2:0 使用的带宽要多得多。

在生产环境中启用 YUV 4:4:4 之前，请在测试场景中验证带宽使用情况，以避免与带宽拥塞相关的问题。

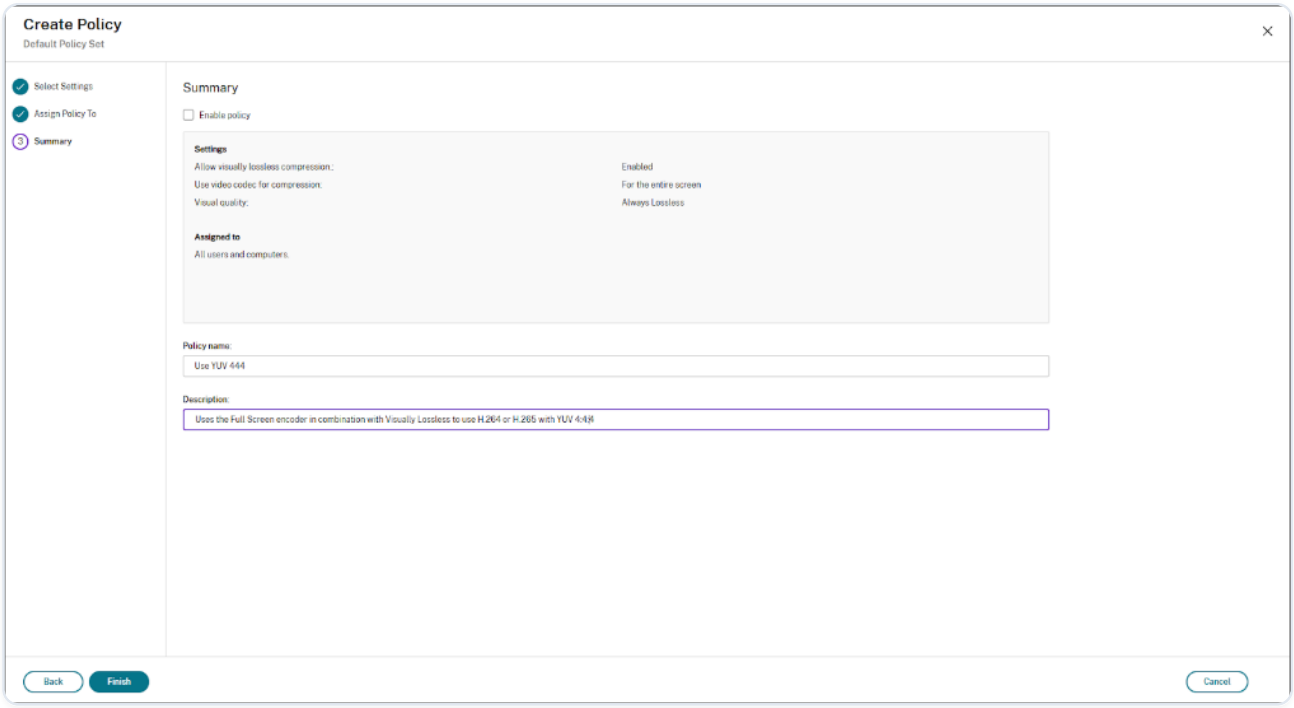
配置

为了使用 YUV 4:4:4 获得更高的图像质量和色彩准确度，启用 YUV 4:4:4 需要在 Citrix Studio 中调整多个 HDX™ 策略设置：

用于压缩的视频编解码器：将其设置为“用于整个屏幕”，以将视频编解码器（以及所选的色度子采样）应用于整个屏幕内容。

视觉质量：选择“构建到无损”或“始终无损”，以优先考虑图像质量而非带宽消耗。

允许视觉无损：启用此策略以允许视觉无损压缩。



默认情况下，Thinwire 使用 H.264 YUV 4:4:4；如果在客户端检测到兼容硬件，Thinwire 将自动使用 H.265 YUV 4:4:4 硬件解码。

使用 H.265 YUV 4:4:4，内部测试显示，与 H.264 4:4:4 相比，每秒帧数 (FPS) 增加了 4 倍；与 H.264 相比，每帧大小减少了 2.5 倍，这归因于 H.265 更高的效率。

要求

对于 H.264 的 YUV 4:4:4，没有额外要求。H.265 YUV 4:4:4 有以下客户端要求：

- 适用于 Windows 的 Citrix Workspace™ 应用程序 2305 或更高版本
- 启用 H.265 支持
- 支持 H.265 4:4:4 解码的客户端 GPU：
  - NVIDIA Turing 或更高版本
  - Intel 第 10 代或更高版本

> **注意：**
>
> 截至撰写本文时，AMD 不支持 H.265 4:4:4 解码。

> 当 VDA 配置为使用 YUV 4:4:4 并启用自动视频编解码器选择时，将自动使用 H.265 YUV 4:4:4。有关详细信息，请参阅 自动视频编解码器 文档。

高分辨率显示器

部署高分辨率显示器（6K、8K 和等效百万像素计数）的客户在使用 Citrix Virtual Apps and Desktops™ 时，可能会遇到性能问题，或者鼠标跟踪不一致、显示缩放和 DPI 相关问题。

典型办公显示器的传统分辨率是 4K、6K 或 8K 分辨率，其中“K”表示水平分辨率。

6K 显示器的示例包括 Apple Pro Display XDR 和 Dell UltraSharp U3224KB，分辨率分别为 6016 × 3384 和 6144 × 3456。

目前只有少数 8K 显示器可用，其中一个示例是 Dell UltraSharp UP3218K，分辨率为 7680 x 4320。

Barco 列出的显示器使用 MP 或百万像素计数，而不是分辨率。最新的 Barco 显示器是 32MP 显示器，其宣传分辨率为 6848 x 4560。

Citrix® 最多支持 8 台显示器，具体取决于硬件资源。根据所使用的 GPU，此最大值可能存在其他硬件限制。

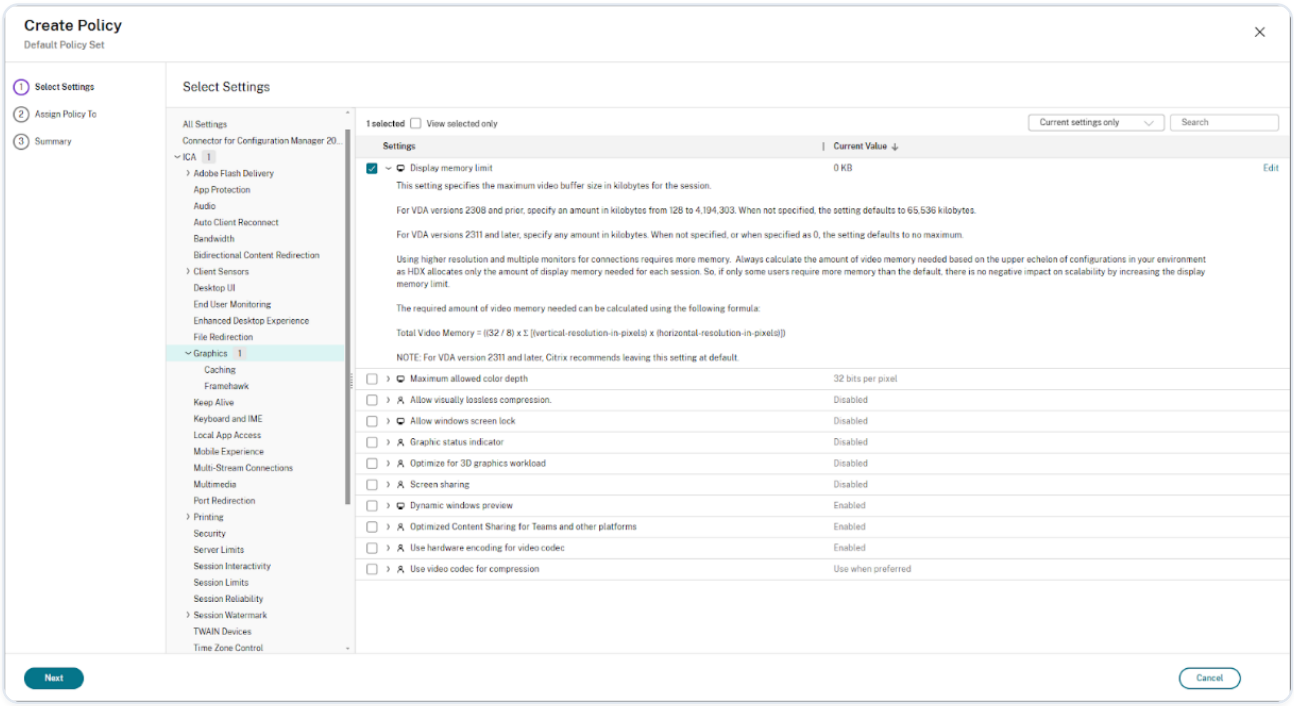
为了优化性能并缓解高分辨率显示器可能出现的问题，Citrix 建议使用 CVAD 2402。

VDA 2402 及更高版本

对于 VDA 2402 及更高版本，将“显示内存限制”策略保留为默认值 0，表示不限制显示内存。这允许 VDA 动态分配所需的显示内存。

旧版 VDA（2402 之前）

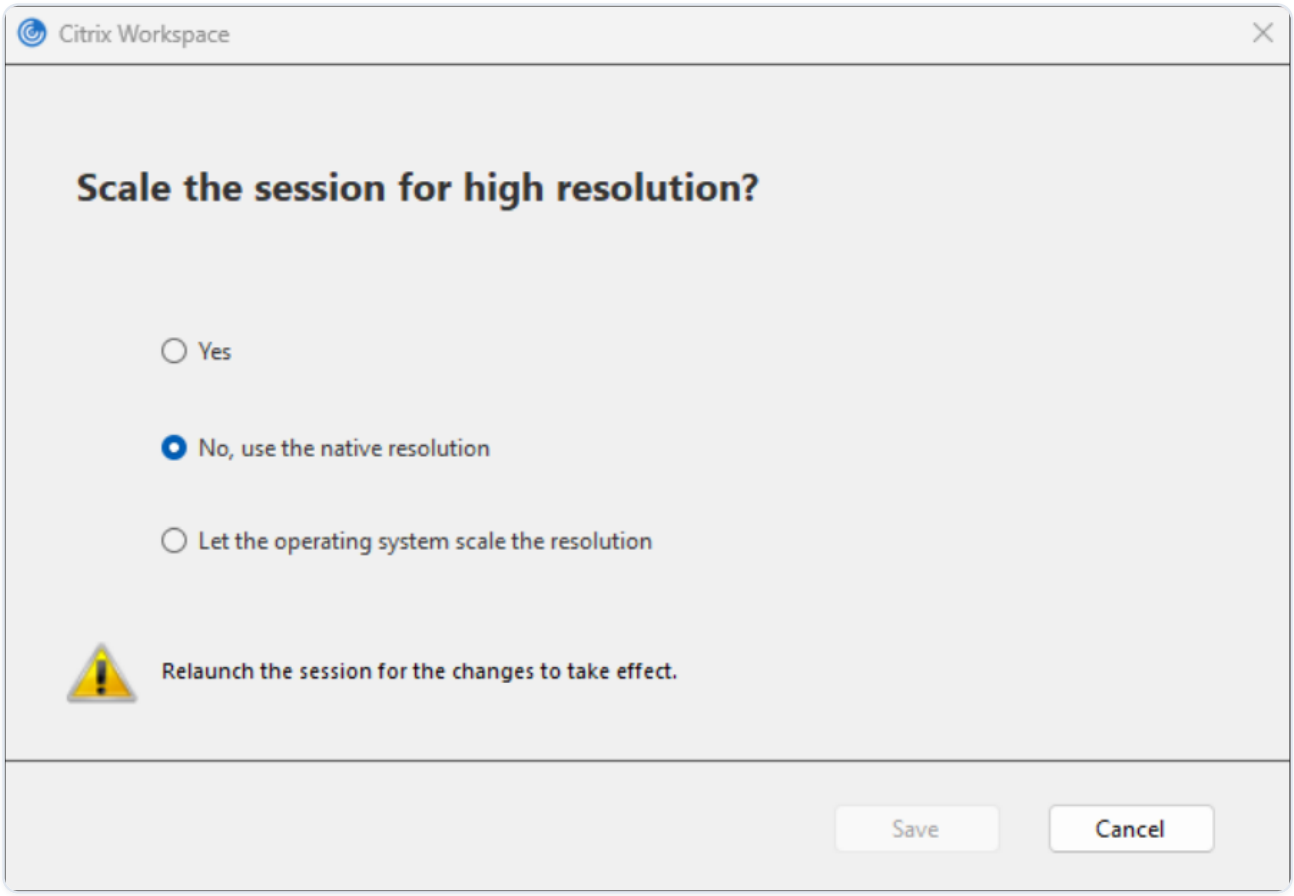
如果无法升级到 CVAD 2402 或更高版本，请将“显示内存限制”策略配置为其最大值 4,194,303 KB。这为 VDA 提供了最大可用显示内存。



DPI 缩放

适用于 Windows 的 CWA 会将本地 Windows 客户端的显示分辨率和 DPI 缩放设置与 Citrix® 会话匹配。这是满足以下系统要求的所有情况的推荐模式：

- Citrix Virtual Apps and Desktops™ 2203 LTSR 或更高版本
- 在 Windows Server 2019 或更高版本上运行的多会话操作系统 VDA
- 在 Windows 10 或更高版本上运行的单会话操作系统 VDA
- 适用于 Windows 的 CWA 2203 LTSR 或更高版本



Citrix 建议使用 Citrix Workspace™ App 2402 或更高版本。

有关详细信息，请参阅 Citrix Workspace 文档。

GPU

对于高分辨率显示器，请确保所使用的 GPU（VDA 和端点上）满足驱动高分辨率显示器的要求。请参阅您的 GPU 供应商文档，了解支持的分辨率和刷新率。

使用服务器端 GPU 时，Citrix® 建议以下最低 GPU 帧缓冲区大小：

显示器和分辨率	推荐的帧缓冲区大小
1 个 4K	2GB
4 个 1080p	2GB
2 个 4K	4GB
1 个 6K	4GB
1 个 8K	8GB
2 个 6K	8GB

显示器和分辨率	推荐的帧缓冲区大小
4 x 4K	8GB

注意：

这些是 HDX™ 图形编码的最低推荐帧缓冲区大小。请查阅应用程序帧缓冲区要求，并在进行规模调整时将其考虑在内。

有关 NVIDIA 规模调整指南 的更多信息，请参阅 NVIDIA GPU 的帧缓冲区大小调整。

有关 Intel 虚拟桌面基础架构 (VDI) 在 Intel® 数据中心 GPU Flex 系列白皮书上的性能 的更多信息，请参阅 Intel GPU 的 GPU 大小调整。

有关 更多信息，请参阅此处。

性能和可扩展性注意事项

更高的分辨率和显示器数量直接影响会话性能和服务器可扩展性。

带宽消耗将随着更高的分辨率和使用的多显示器而增加。带宽限制可能会限制帧速率并降低图像质量，从而影响会话交互性和用户体验。

端点设备必须具备足够的硬件资源来支持所需的显示配置。这可能意味着拥有足够的 CPU 资源，在某些情况下还需要能够处理图形工作负载的 GPU。

已知问题

结合全屏视频编解码器、H.265 编码以及高于 4096x4096 的分辨率时，NVIDIA GPU 存在一个已知问题。

请参阅此处以获取更多信息。

作为一种变通方法，请使用默认的**使用视频编解码器进行压缩”图形策略设置，或将策略明确设置为“让系统决定”或“活动更改区域**。

图形容错模式

图形容错模式可增强在高丢包率和高延迟网络上交互式会话的用户体验。

它通过动态调整图形数据传输策略来确保会话保持响应。图形容错模式默认启用。

何时使用图形的容忍丢包模式

当用户通过网络连接到虚拟应用程序和桌面时，如果网络条件具有挑战性，例如高数据包丢失和高延迟，他们的会话交互性和体验可能会受到严重影响。

这可能导致用户体验下降，表现为延迟和视觉卡顿，从而对生产力和用户满意度产生负面影响。

为了减轻这些不良网络条件的影响，图形的容错模式会自动将 Citrix® 图形编码器切换到更积极的数据包传输机制，当数据包丢失和延迟超过配置的阈值时。此模式会主动增加带宽使用量，其增加量与数据包丢失程度成比例，以确保数据有效传输并保持会话的交互性。

图形的容错模式具有以下优点：

- **改善用户体验：** 在具有挑战性的网络上提供更流畅、响应更快的图形体验。
- **无缝操作：** 该模式根据实时网络条件自动激活和停用，无需用户干预。
- **保持生产力：** 用户可以继续高效工作，而不会受到不良网络质量的阻碍。

系统要求

- Citrix Virtual Delivery Agent (VDA) 2311 或更高版本
- 适用于 Windows 2311 或更高版本的 Citrix Workspace™ 应用程序。

> **注意：**
>
> 必须同时启用图形策略的 **HDX™ 自适应传输 (EDT)** 和 **容错模式**，此功能才能正常工作。

重要要求注意事项

带宽阈值

从 CVAD 2507 版本开始，图形容错模式需要至少 30 Mbps 的带宽才能激活。即使满足延迟和数据包丢失阈值，如果可用的会话内带宽低于 30 Mbps，该功能也不会启用。此带宽阈值是一个硬编码值，无法配置。

配置

此功能通过 Web Studio 或组策略管理中的 Citrix® 策略进行管理。

图形的容错模式默认启用：

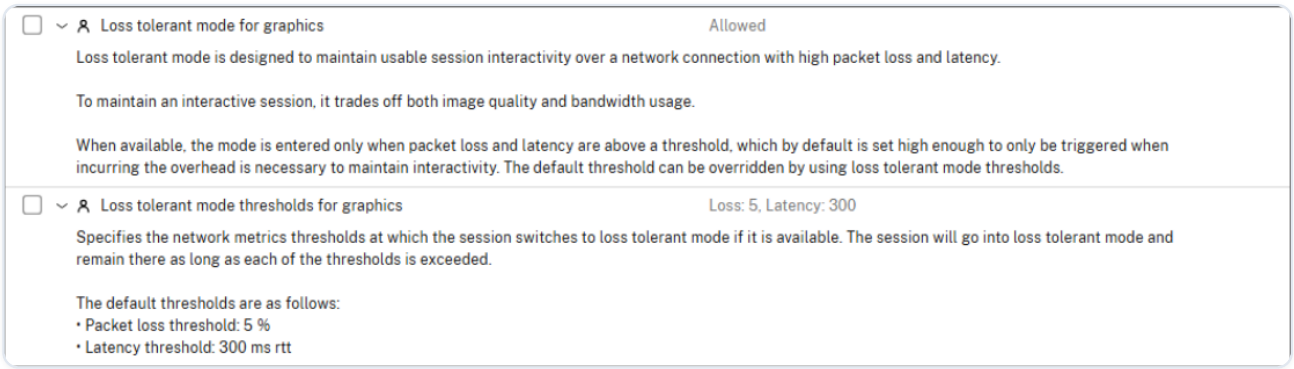
- 策略：图形的容错模式
- 默认值：已启用

将此策略设置为**已禁用**以关闭图形的容错模式功能。

要配置图形的容错模式阈值：

- 策略：图形的容错模式阈值
- 默认值：
  - 数据包丢失：5%
  - 延迟：300 毫秒

此策略允许您调整触发图形容错模式的网络条件阈值。当数据包丢失和延迟值都达到或超过，并且可用带宽至少为 30 Mbps 时，此模式将激活。



HDX 图形超分辨率升频

HDX 图形超分辨率升频

HDX 图形超分辨率是一种智能的客户端辅助技术，可减少图形密集型和多媒体繁重工作负载的带宽消耗，同时保持用户感知的视觉质量。

通过在编码期间对视频区域选择性地应用额外压缩，并使用客户端的图形处理单元 (GPU) 在端点上重建原始质量，HDX 图形超分辨率提高了会话效率，而不会增加服务器端 CPU 或 GPU 的利用率。

从 Citrix Virtual Apps and Desktops (CVAD) 2607 LTSR 开始，HDX 图形超分辨率已正式发布 (GA) 并默认启用。

主要优势

- 降低视频和高动态内容的带宽消耗
- 在带宽受限或可变网络上改善体验
- 无需服务器端 GPU

- 透明操作，无需用户交互
- 在自动模式下默认安全激活，并具有策略控制

HDX 图形超分辨率的工作原理

借助 HDX 图形超分辨率，Thinwire 首先识别会话中的视频或高动态区域（例如，视频播放或动画内容）。

虚拟投递代理 (VDA) 会有意地对这些区域应用额外压缩，并在编码期间以降低的有效分辨率对这些区域进行编码。 降低分辨率的区域使用显著更少的带宽进行传输。

在端点上，Citrix Workspace 应用程序使用客户端 GPU 将受影响的区域升频回其原始分辨率和视觉质量。 文本和静态区域不受影响，并继续以最佳质量交付。

这种方法在保持高质量用户体验的同时减少了带宽使用。

自动操作（默认行为）

在 CVAD 2607 LTSR 中，HDX 图形超分辨率默认启用并以自动模式运行。在自动模式下，Thinwire 实时监控可用带宽，以确定何时激活 HDX 图形超分辨率

此功能仅在满足以下两个条件时激活：

- 检测到兼容的客户端 GPU
- Citrix 确定网络状况不佳

当网络状况改善时，HDX 图形超分辨率会自动解除，确保在网络质量允许的情况下优先选择无损传输。

此自动模式允许管理员安全地保持此功能启用，无需手动调整。

策略配置

HDX 图形超分辨率通过“HDX 图形超分辨率”策略控制。

管理员可以通过使用 **HDX 图形超分辨率** Studio 策略更改 HDX 图形超分辨率的默认自动行为

HDX 图形超分辨率模式

模式	描述	推荐用途
自动（默认）	根据客户端功能和网络状况动态激活超分辨率	一般企业环境

模式	描述	推荐用途
开	超分辨率将用于所有视频区域	带宽受限或多媒体密集型环境
关闭	明确禁用超分辨率	无损、诊断或法规工作流

何时使用自动模式（推荐）

- 网络质量条件多变或不理想
- 用户工作负载混合
- 希望管理开销最小化

大多数环境无需配置

何时强制开启

- WAN 带宽持续受限
- 视频或高动态内容在工作负载中占主导地位
- 希望实现可预测的带宽减少

何时禁用超分辨率

- 需要法规或诊断无损成像
- 像素级完美审查工作流是强制性的
- 全屏编码是特意配置的

与其他 HDX 图形模式的兼容性

HDX 图形超分辨率与我们的默认选择性编码模式协同工作。

当通过将“使用视频编解码器进行压缩策略”设置为以下选项来使用全屏编码时，超分辨率不可用：

- 针对整个屏幕

当“视觉质量”设置为：

- 始终无损视觉质量

或者当使用视觉无损压缩时：

- 启用视觉无损压缩

这些策略设置与 HDX 图形超分辨率不兼容。启用它们将禁用超分辨率，无论 HDX 图形超分辨率是设置为 **自动** 还是 **已启用**。

自动视频编解码器选择

HDX 图形超分辨率与自动视频编解码器选择协同工作，使 VDA 能够根据服务器和客户端之间的兼容性选择最佳编解码器。如果没有可用的硬件编码（例如 VDA 没有服务器端 GPU），超分辨率仍将使用 H.264 视频编解码器运行。当存在服务器端 GPU 时，HDX 图形超分辨率将尽可能自动利用 H.265 或 AV1 进行硬件编码。

系统要求

虚拟投递代理 (VDA)

- Windows VDA 2607 LTSR 或更高版本
- 无需服务器端 GPU
- 无需额外 VDA 配置

客户端要求

- 适用于 Windows 的 Citrix Workspace 应用程序 2607 LTSR 或更高版本*
- 受支持的客户端 GPU

*请注意，Nvidia 客户端 GPU 需要 x64 Citrix Workspace 客户端

受支持的客户端 GPU

Intel GPU 支持

HDX 图形超分辨率与集成 GPU (iGPU) 和独立客户端 GPU 均兼容。

集成 GPU

受支持的集成 GPU (iGPU) 系列：

- Intel Iris Xe（第 11 代及更高版本）
- 英特尔锐炬 Xe Max
- 英特尔锐炬 Plus 显卡
- 英特尔 UHD 显卡 (710, 730, 750, 770, P750)
- 适用于第 11、12 和 13 代处理器的 Intel UHD Graphics

独立 GPU

- Intel Arc – 桌面
  - Arc A 系列: A310, A380, A580, A750, A770
  - Intel B 系列: B570, B580
- Intel Arc – 移动
  - Arc A 系列移动版: A350M, A370M, A530M, A550M, A570M, A730M, A77M
- Intel Arc – 工作站 (Arc Pro)
  - Arc Pro 系列: A30M, A40, A50, A60M, A60
  - Arc Pro B 系列: B50, B60

Nvidia GPU 支持

桌面 GPU

支持的系列：

- GeForce 20 系列 (Turing)
  - RTX 2050 – RTX 2080 桌面和移动版（包括 Ti 和 Super 型号）
  - 泰坦 RTX
- GeForce 30 系列 (Ampere)
  - RTX 3050 – RTX 3090 桌面和移动版（包括 Ti 和 Super 型号）
- GeForce 40 系列 (Ada Lovelace)
  - RTX 4050 – RTX 4090 桌面和移动版（包括 Ti 和 Super 型号）
- GeForce 50 系列 (Blackwell)
  - RTX 5050–5090 桌面和移动版

专业和工作站 GPU

- NVIDIA Quadro（旧品牌名称）
  - Quadro RTX 系列：3000、4000、5000、6000、8000（桌面和移动版）
  - Quadro T 系列：T400、T500、T600、T1000、T1200（桌面和移动版）

- NVIDIA RTX（原 Quadro）– Ampere 工作站
  - RTX A 系列：A1000–A6000 桌面和移动版
  - A800 主动
- NVIDIA RTX – Ada 代工作站
  - RTX Ada 系列：2000、4000、4000 SFF、4500、5000、5880、6000
  - RTX Ada 笔记本系列：RTX 500–5000 Ada（移动版）
  - RTX PRO 6000 Blackwell 工作站

这是一个非详尽的客户端 GPU 列表，它们应与 HDX 图形超分辨率兼容。请注意，此列表是根据供应商文档编译的，并非所有 GPU 都经过 Citrix 验证。

Citrix 建议使用 GPU 供应商提供的最新 GPU 驱动程序以获得最佳性能。

多 GPU 配置

在多 GPU 端点中，只有主 GPU 适配器将用于 HDX 图形超分辨率。 多 GPU 配置常见于专注于多媒体的笔记本电脑设备。

从 HDX 图形超分辨率预览版过渡

本节解释了从 HDX 图形超分辨率预览版升级时发生的变化以及管理员应期待什么。

区域	预览版行为 (CVAD 2507 和 2511)	CVAD 2607 LTSR 及更高版本
启用	VDA 和客户端上的手动注册表项	默认自动启用
控制模型	基于注册表	基于策略
默认状态	已禁用	默认自动启用
激活逻辑	启用后始终处于活动状态	根据网络条件有条件地启用（默认行为）*
支持的客户端 GPU	仅限部分 Intel GPU 和 iGPU	部分 Intel GPU 和部分 NVIDIA GPU

HDX 图形超分辨率现在通过 **HDX 图形超分辨率策略**进行控制。此策略取代了预览期间使用的所有基于注册表的启用方式。

所需操作

管理员可以安全地删除在公共技术预览版中启用超分辨率所需的 VDA 和客户端注册表项。升级到 CVAD 2607 LTSR 后，无需采取进一步操作即可启用 HDX 图形超分辨率。请确保客户端运行的是 Citrix Workspace App for Windows 2607 LTSR 或更高版本。

管理员可以选择性地审查或调整 HDX 图形超分辨率策略，以符合带宽或合规性要求。

监控和故障排除

HDX 图形超分辨率依赖于客户端 GPU 处理来重建以降低分辨率传输的视频区域。因此，当超分辨率处于活动状态时，客户端 GPU 利用率增加是预期行为。

> **注意：**

> 请注意，当笔记本电脑使用电池供电时，启用超分辨率可能会对电池续航时间产生不利影响。

> GPU 利用率的水平取决于：

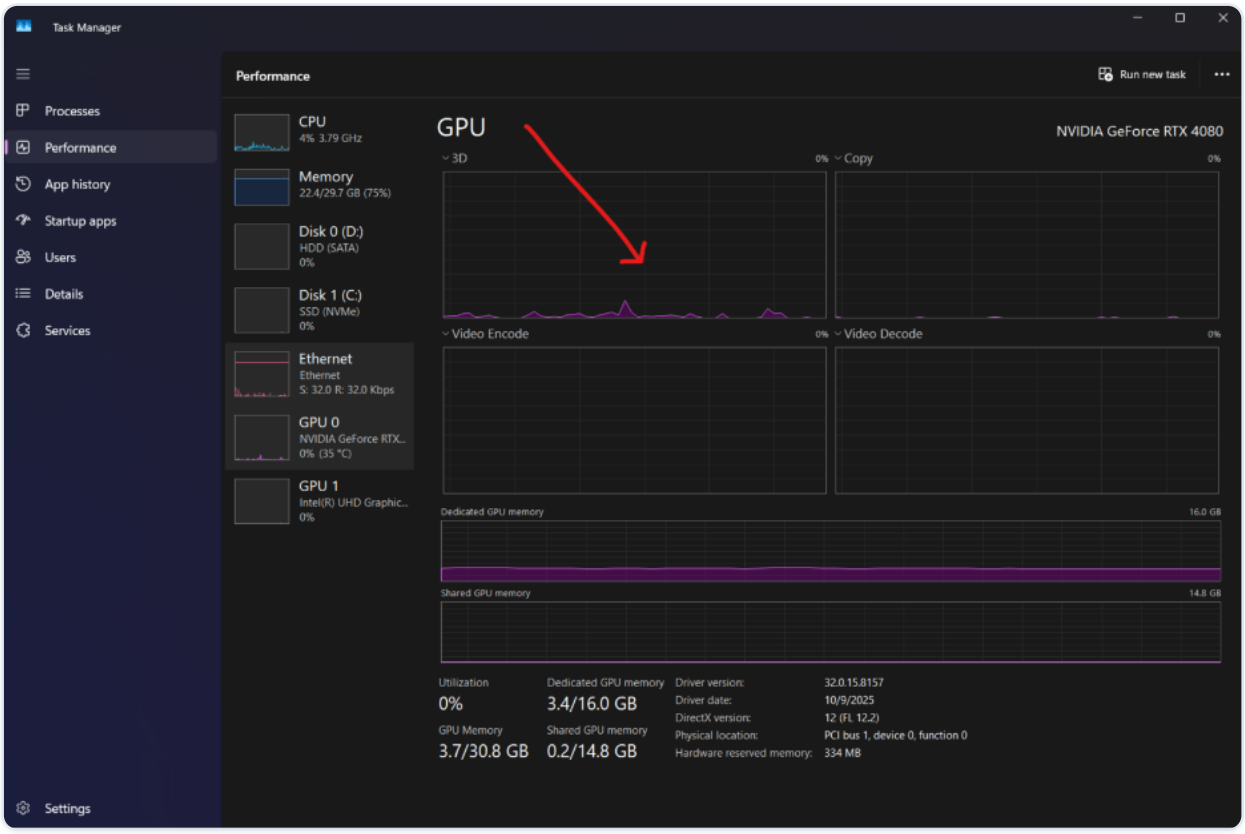
- 视频区域的大小
- 内容的帧率
- 连接显示器的数量和分辨率
- 客户端 GPU 的能力

本节介绍管理员和最终用户在使用 HDX 图形超分辨率时如何监视、验证和排查客户端活动。

监视客户端 GPU 利用率 (Windows)

管理员和最终用户可以使用 Windows 任务管理器监视客户端 GPU 使用情况。

1. 打开任务管理器
2. 选择“性能”选项卡
3. 从左侧菜单中选择“GPU”
4. 观察：
    - 视频或高动态内容播放期间的 GPU 利用率百分比



当 HDX 图形超分辨率处于活动状态时，视频播放或高动态工作负载期间的 GPU 活动增加是预期行为。

验证超分辨率是否处于活动状态

管理员可以通过以下组合确认 HDX 图形超分辨率处于活动状态：

- 客户端 GPU 利用率增加
- 与策略设置为“关”时相比，会话带宽使用量减少
- 可见的升频指示器（如果已启用）

如果在视频播放期间 GPU 利用率没有增加：

- 验证客户端 GPU 是否受支持
- 确认 HDX 图形超分辨率策略未设置为“关”
- 确保未启用冲突的图形模式

常见故障排除方案

客户端 GPU 使用率未增加

可能的原因：

- HDX 图形超分辨率策略设置为“关”
- 网络状况良好（自动模式未激活）
- 不支持或不兼容的客户端 GPU
- GPU 驱动程序已过时

客户端上的 GPU 利用率在很大程度上取决于视频区域的大小和 GPU 的功能；更强大的 GPU 对利用率的影响较小。

视频卡顿或帧速率低于预期

可能的原因：

- GPU 驱动程序已过时
- GPU 性能不佳
- 视频区域的大小过大

请监控客户端的 GPU 使用情况。如果 GPU 利用率显著高于预期，则客户端的 GPU 可能无法对所使用的分辨率进行超分辨率升采样。

客户端性能问题

如果用户遇到响应速度降低或性能下降的情况：

- 监控端点上的总 GPU 利用率
- 尽可能降低视频播放分辨率或帧速率
- 考虑使用策略模式“自动”而不是“开”
- 验证端点硬件是否符合建议的多显示器或高分辨率工作负载规范

支持数据收集建议

在排查超分辨率的客户端行为问题时，Citrix 建议收集并查看以下信息：

- Citrix Workspace 应用程序版本
- 客户端 GPU 型号和驱动程序版本
- 连接的显示器数量和分辨率
- HDX 图形超分辨率策略设置
- 重现期间的客户端 GPU 利用率

此信息有助于确定观察到的行为是预期行为还是与硬件相关。

Thinwire 简介

由 Thinwire 提供支持的 HDX™ Graphics 是 Citrix 的高级显示技术，可提供高性能、自适应且高效的远程桌面和应用程序体验。

Thinwire 通过智能分析、缓存和压缩图形数据，确保在各种网络条件和端点设备上实现最佳性能。

HDX™ 3D 专业版

HDX 3D Pro（现称为 HDX Graphics）为要求严苛的图形工作负载提供高性能用户体验。默认情况下，它利用 GPU 为 DirectX 和 OpenGL 应用程序提供硬件加速。此功能以前与 HDX 3D Pro 相关联，现在所有用户都可以直接使用，无需任何额外的策略或配置。

使用硬件加速，您可以为用户提供无缝且响应迅速的体验，即使对于图形密集型应用程序也是如此，包括设计、工程和多媒体制作等领域中使用的应用程序。

Citrix Virtual Apps and Desktops™ 的 HDX 3D Pro 功能使您能够交付使用图形处理单元 (GPU) 进行硬件加速时性能最佳的桌面和应用程序。这些应用程序包括基于 OpenGL 和 DirectX 的 3D 专业图形应用程序。标准 VDA 仅支持 DirectX 的 GPU 加速。

有关 HDX 3D Pro 策略设置，请参阅 优化 3D 图形工作负载。

所有受支持的 Citrix Workspace 应用程序都可以与 3D 图形配合使用。为了在复杂的 3D 工作负载、高分辨率显示器、多显示器配置和高帧率应用程序中获得最佳性能，我们建议使用最新版本的适用于 Windows 的 Citrix Workspace 应用程序和适用于 Linux 的 Citrix Workspace 应用程序。有关受支持的 Citrix Workspace 应用程序版本的更多信息，请参阅 Citrix Workspace 应用程序的生命周期里程碑。

3D 专业应用程序的示例包括：

- 计算机辅助设计、制造和工程 (CAD/CAM/CAE) 应用程序
- 地理信息系统 (GIS) 软件
- 用于医学成像的图片归档和通信系统 (PACS)
- 使用最新 OpenGL、DirectX、NVIDIA CUDA、OpenCL 和 WebGL 版本的应用程序
- 使用 NVIDIA 计算统一设备架构 (CUDA) GPU 进行并行计算的计算密集型非图形应用程序

HDX 3D Pro 在任何带宽下都能提供最佳用户体验：

- 在 WAN 连接上：在带宽低至 1.5 Mbps 的 WAN 连接上提供交互式用户体验。
- 在 LAN 连接上：在 LAN 连接上提供与本地桌面相当的用户体验。

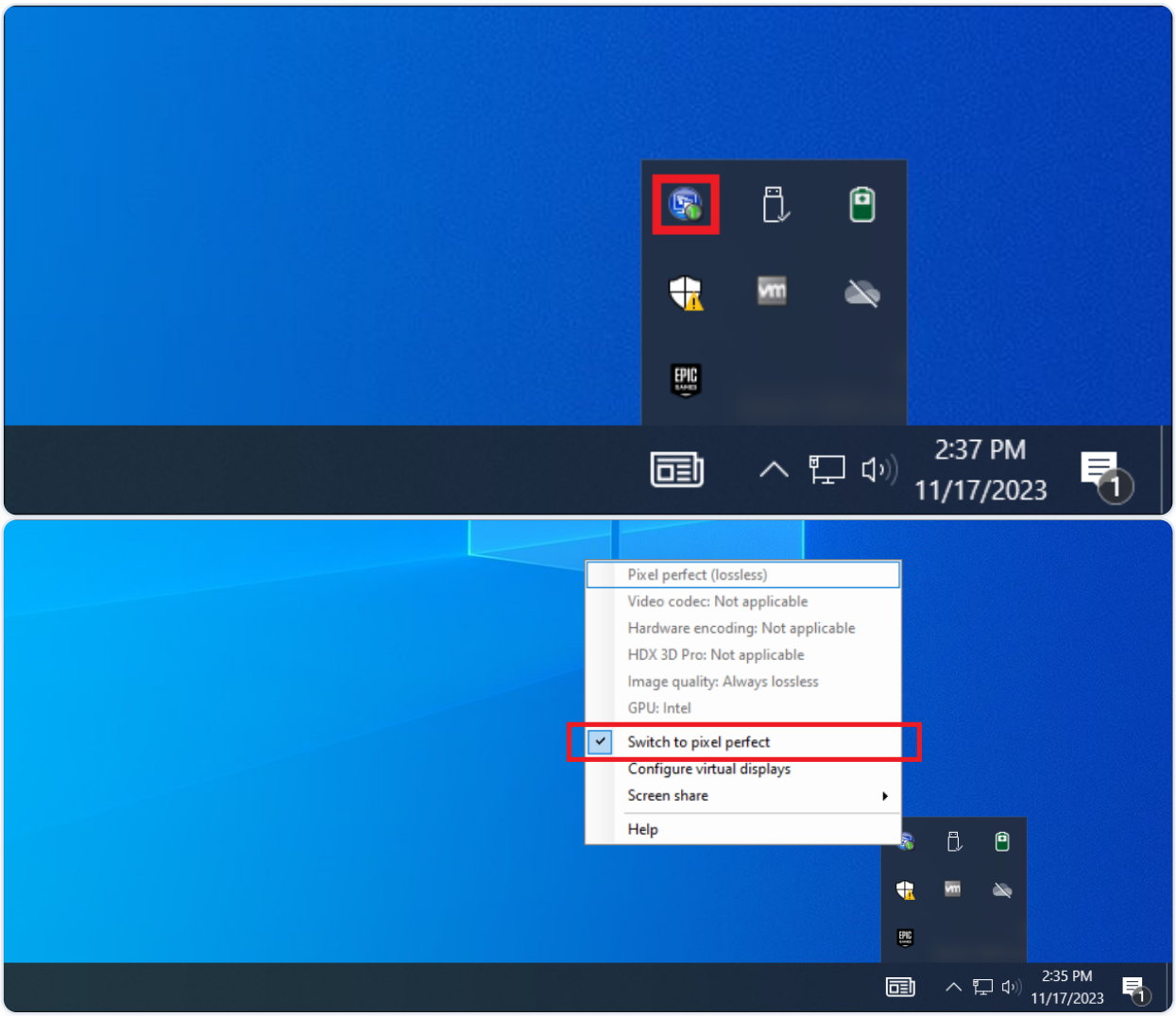
您可以通过将图形处理移至数据中心进行集中管理，用更简单的用户设备取代复杂且昂贵的工作站。

无损压缩选项，适用于特殊用例

HDX 3D Pro 还提供基于 CPU 的无损编解码器，以支持需要像素级完美图形的应用程序，例如医学成像。仅建议在特殊用例中使用真正的无损压缩，因为它会消耗更多的网络和处理资源。

使用无损压缩时：

- 图形状态指示器（通知区域图标）中的无损指示器会通知用户当前显示的屏幕是损耗帧还是无损帧。当**视觉质量**策略设置指定为**构建为无损**时，此图标会提供帮助。当发送的帧是无损帧时，无损指示器会变为绿色。



- 无损开关使用户可以在会话中的任何时候切换到**始终无损**模式。要在会话中选择或清除**无损**，请右键单击该图标，然后单击**切换到像素完美**或使用快捷方式 ALT+SHIFT+1。
    - 对于无损压缩：无论通过策略选择何种编解码器，HDX 3D Pro 都使用无损编解码器进行压缩。

- 对于有损压缩：HDX 3D Pro 使用原始编解码器，可以是默认编解码器，也可以是通过策略选择的编解码器。 无损开关设置不会保留到后续会话。要为每个连接使用无损编解码器，请在**视觉质量策略**设置中选择**始终无损**。

您可以覆盖默认快捷方式 ALT+SHIFT+1，以在会话内选择或取消选择无损。在 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator` 配置新的注册表设置。

- 名称: HKEY_LOCAL_MACHINE_HotKey, 类型: String
- 配置快捷方式组合的格式为 C=0|1, A=0|1, S=0|1, W=0|1, K=val。键必须用逗号“,”分隔。键的顺序无关紧要。
- A、C、S、W 和 K 是键，其中 C=Control，A=ALT，S=SHIFT，W=Win，K=有效键。K 的允许值为 0–9、a–z 和任何虚拟键代码。
- 例如： 对于 F10，设置 K=0x79 对于 Ctrl + F10，设置 C=1, K=0x79 对于 Alt + A，设置 A=1, K=a 或 A=1, K=A 或 K=A, A=1 对于 Ctrl + Alt + 5，设置 C=1, A=1, K=5 或 A=1, K=5, C=1 对于 Ctrl + Shift + F5，设置 A=1, S=1, K=0x74

优化 HDX 3D Pro 用户体验

当多个用户共享带宽有限的连接（例如，在分支机构）时，建议您使用“总体会话带宽限制”策略设置来限制每个用户可用的带宽。使用此设置可确保可用带宽不会随着用户的登录和注销而大幅波动。由于 HDX 3D Pro 会自动调整以使用所有可用带宽，因此用户会话期间可用带宽的巨大变化可能会对性能产生负面影响。 例如，如果 20 个用户共享一个 60 Mbps 的连接，则每个用户可用的带宽可能在 3 Mbps 到 60 Mbps 之间变化，具体取决于并发用户的数量。为了在此场景中优化用户体验，请确定高峰期每个用户所需的带宽，并始终将用户限制在此数量。 对于 3D 鼠标用户，建议您将通用 USB 重定向虚拟通道的优先级提高到 0。有关更改虚拟通道优先级的信息，请参阅知识中心文章 CTX128190。 使用 HDX Monitor 工具验证 HDX 可视化技术的运行和配置，并诊断和解决 HDX 问题。该工具位于 Citrix Virtual Apps and Desktops™ 安装介质的 **Support** 文件夹中。

GPU 加速

HDX™ Graphics 可在虚拟投递代理 (VDA) 和端点设备上无缝利用 GPU 硬件。

这种开箱即用的硬件加速（以前称为 HDX 3D Pro）默认启用，可显著提升图形密集型 DirectX 和 OpenGL 应用程序的性能，无论是在单会话还是多会话操作系统中。

Citrix Virtual Apps and Desktops™ 支持在 Windows 多会话操作系统会话中运行的图形密集型应用程序在服务器的图形处理单元 (GPU) 上进行渲染。通过将 OpenGL、DirectX、Direct3D 和 Windows Presentation Foundation (WPF) 渲染转移到服务器的 GPU，可以更高效地使用服务器的 CPU。

由于 Windows Server 是一个多用户操作系统，因此多个用户可以共享由 Citrix Virtual Apps™ 访问的 GPU，而无需 GPU 虚拟化 (vGPU)。

对于涉及编辑注册表的操作，请谨慎行事：不正确地编辑注册表可能会导致严重问题，可能需要您重新安装操作系统。Citrix® 无法保证可以解决因不正确使用注册表编辑器而导致的问题。使用注册表编辑器风险自负。在编辑注册表之前，请务必备份注册表。

GPU 共享

GPU 共享支持在远程桌面会话中对 OpenGL 和 DirectX 应用程序进行 GPU 硬件渲染。它具有以下特点：

- 可用于裸机或虚拟机，以提高应用程序的可伸缩性和性能。
- 支持多个并发会话共享 GPU 资源（大多数用户不需要专用 GPU 的渲染性能）。
- 无需特殊设置。

可根据管理程序和 GPU 供应商的要求，以完全直通或虚拟 GPU (vGPU) 模式将 GPU 分配给 Windows Server 虚拟机。还支持在物理 Windows Server 计算机上进行裸机部署。

GPU 共享不依赖于任何特定的显卡。

- 对于虚拟机，请选择与正在使用的管理程序兼容的显卡。有关 XenServer 硬件兼容性列表，请参阅 Hypervisor Hardware Compatibility List。
- 在裸机上运行时，建议操作系统仅启用一个显示适配器。如果硬件上安装了多个 GPU，请使用设备管理器禁用除一个之外的所有 GPU。

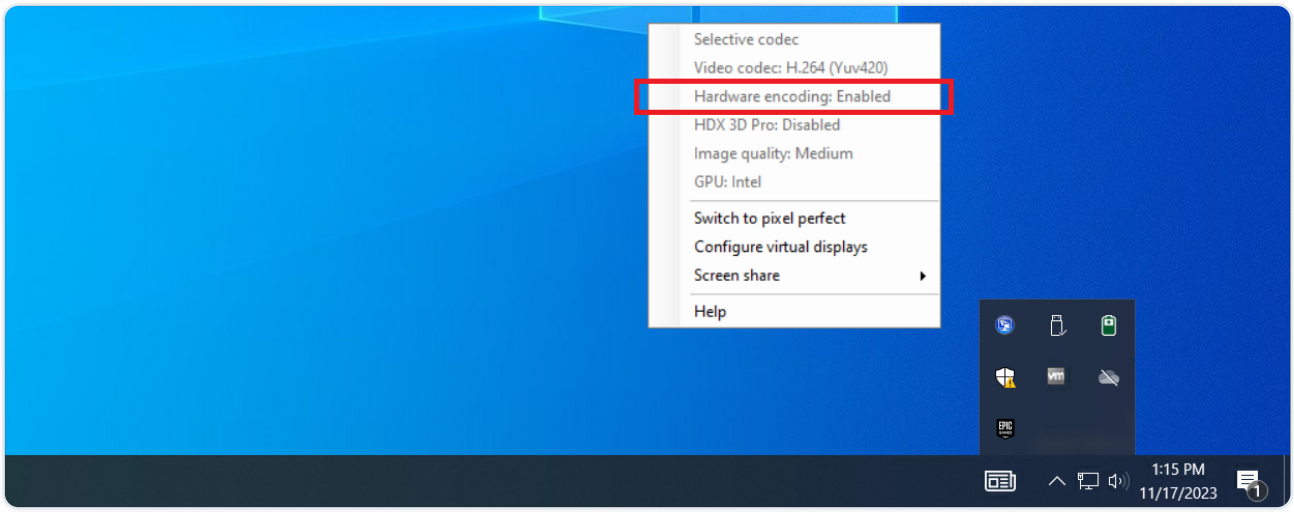
使用 GPU 共享的可伸缩性取决于以下几个因素：

- 正在运行的应用程序
- 它们消耗的视频 RAM 量
- 显卡的图形处理能力

有些应用程序比其他应用程序更能有效地处理视频 RAM 短缺。如果硬件过载，可能会导致显卡驱动程序不稳定或崩溃。限制并发用户数以避免此类问题。

- 访问 NVIDIA GPU 和 Intel Iris Pro 图形处理器的高性能视频编码器。一项策略设置（默认启用）控制此功能，并允许对 H.264 编码使用硬件编码（如果可用）。如果此类硬件不可用，VDA 将回退到使用软件视频编解码器的基于 CPU 的编码。有关详细信息，请参阅图形策略设置。

要确认 GPU 加速正在进行，可以使用图形状态指示器：



DirectX、Direct3D 和 WPF 渲染

DirectX、Direct3D 和 WPF 渲染仅适用于支持显示驱动程序接口 (DDI) 版本 9ex、10 或 11 的 GPU 服务器。

- 在 Windows Server 2016 及更高版本中，RD 会话主机服务器上的远程桌面服务 (RDS) 会话使用 Microsoft 基本渲染驱动程序作为默认适配器。要在 Windows Server 2016 及更高版本上的 RDS 会话中使用 GPU，请在组策略 **本地计算机策略** \> **计算机配置** \> **管理模板** \> **Windows 组件** \> **远程桌面服务** \> **远程桌面会话主机** \> **远程会话环境** 中启用“**为所有远程桌面服务会话使用硬件默认图形适配器**”设置。
- 要使 WPF 应用程序使用服务器的 GPU 进行渲染，请在运行 Windows 多会话操作系统会话的服务器注册表中创建设置。有关注册表设置的信息，请参阅注册表管理的功能列表中的Windows Presentation Foundation (WPF) 渲染。

适用于 CUDA 或 OpenCL 应用程序的 GPU 加速

在用户会话中运行的 CUDA 和 OpenCL 应用程序的 GPU 加速默认情况下处于禁用状态。

要使用 CUDA 加速功能，请启用注册表设置。有关信息，请参阅注册表管理的功能列表中的CUDA 或 OpenCL 应用程序的 GPU 加速。

10 位高动态范围 (HDR)

借助 10 位高动态范围 (HDR) 虚拟桌面会话，您可以使用增强的编码和解码功能来渲染具有扩展色彩范围、更高对比度和亮度的优质图像和视频。

系统要求

端点：

- 适用于 Windows 2209 或更高版本（适用于 NVIDIA GPU）的 Citrix Workspace™ 应用程序
- 端点上支持 10 位 HEVC (H.265) 444 解码的 NVIDIA GPU
- 支持 10 位 HDR 的显示器，必须使用显示设置在所有显示器上启用 10 位 HDR。

服务器：

- 适用于 NVIDIA GPU 的 Windows 单会话操作系统 VDA 2209 或更高版本，以及适用于 Intel GPU 的 VDA 2308 或更高版本
- VDA 上支持 10 位 HEVC 444 编码的 NVIDIA GPU

所需策略

端点：

- 启用图形的 H.265 解码

服务器：

- 优化 3D 图形工作负载
- 图形状态指示器（可选）

服务器配置

在支持 10 位 HDR 的端点显示器上启动 Citrix® 会话时，默认启用 HDR 会话。在多显示器 HDR 会话中，所有端点显示器都必须启用 10 位 HDR。HDR 会话支持窗口模式和全屏模式。

参考白电平

此设置通过尼特值定义白色亮度级别。它控制会话中相对的 HDR 屏幕亮度。默认值为 80 尼特。设置以下注册表项以定义不同的尼特值：

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 类型：REG_DWORD
- 名称: RefWhiteLevel

要激活此设置，您必须调整会话大小，或者断开连接并重新启动会话。

EDID 覆盖

您可以将 VDA 配置为对 HDR 会话使用端点显示器 EDID。这使您可以通过匹配色域和亮度范围来充分利用显示器的显示功能。默认情况下，HDR 会话假定显示器支持 HDR1000。 您可以使用 NVIDIA 或其他工具导出端点显示器 EDID。使用以下注册表项将其应用于 VDA：

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 类型: REG_BINARY
- 名称为: EDIDOverride

将 EDID 存储在注册表中时，它不得包含逗号、空格或特殊字符。要激活覆盖 EDID，请注销并启动新会话。

视觉无损体验

启用以下策略以获得视觉无损体验：

- 允许视觉无损压缩
- 视觉质量：始终无损或构建到无损

设置策略后，您可以使用图形状态指示器通过图像质量滑块或切换到像素完美模式来控制 HDR 会话质量。

允许 Windows 屏幕锁定

您可以使用此策略允许所有 Windows 显示超时（包括屏幕锁定）应用于工作站操作系统上的 Citrix Virtual Desktop 会话。此设置可以使用 Citrix Studio 中的 Citrix 组策略对象进行配置。

默认情况下，如果未启用此设置，则在活动会话期间，Citrix Virtual Desktop 不会响应会话锁定、屏幕保护程序或显示关闭的超时。

当工作站 VDA 上配置了受密码保护的屏幕保护程序时，必须启用此设置，以允许 Citrix Virtual Desktop 会话在达到屏幕保护程序超时时自动锁定。

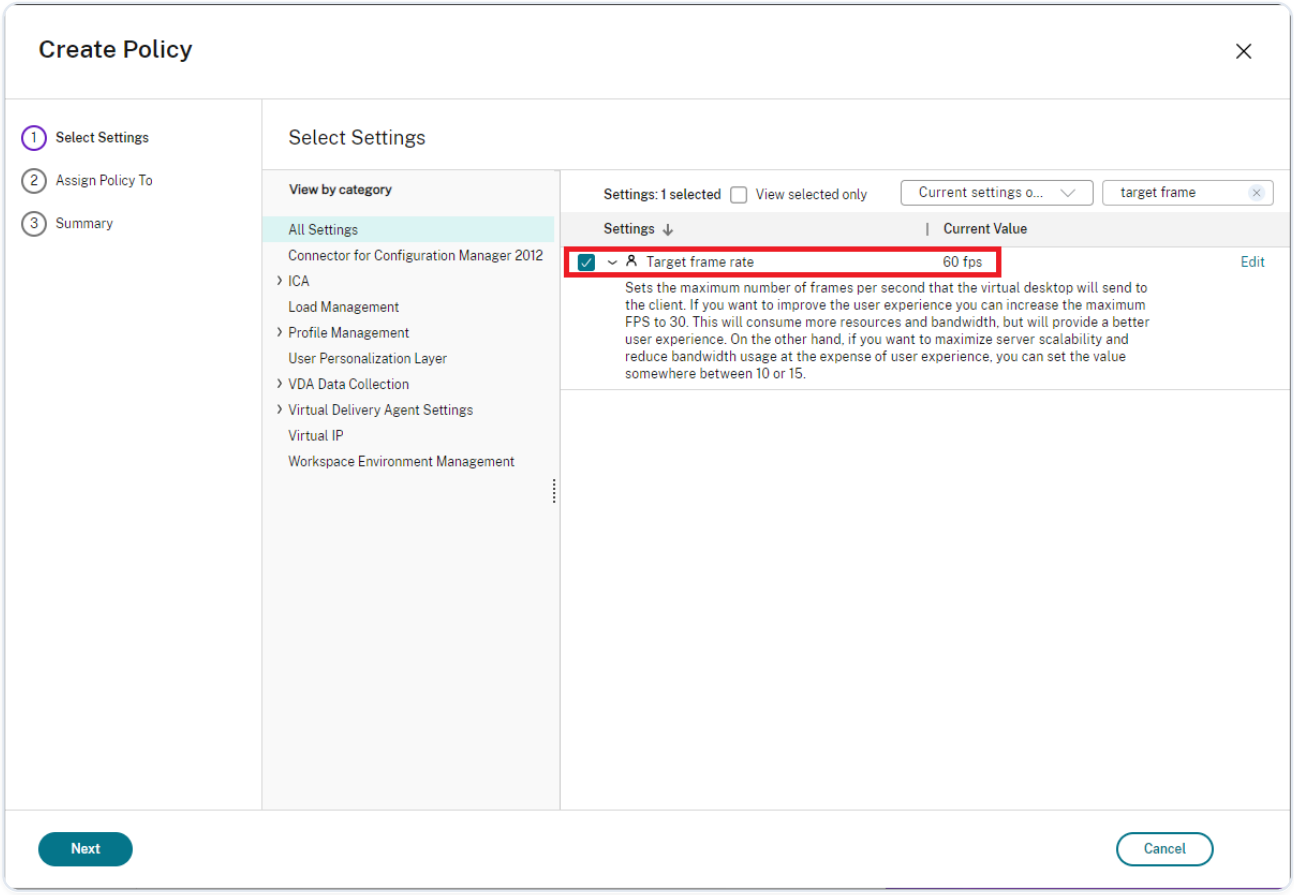
在 VDA 上配置显示关闭超时时启用此设置，会导致该超时到期后，会话在用户恢复与会话的交互之前不会更新。例如，显示的任何时间都不会更新，并且不会显示新通知。

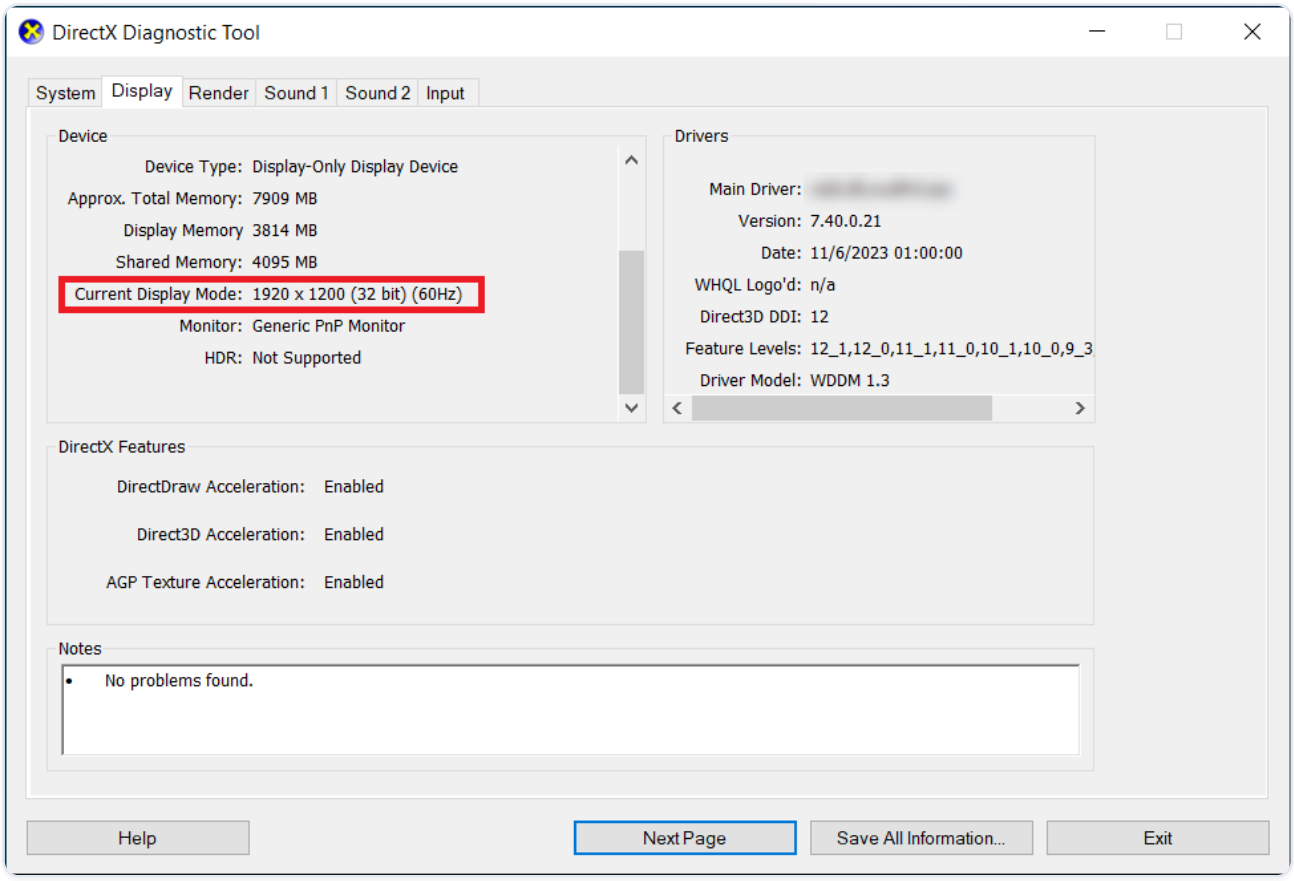
其他注意事项

- 您可以在虚拟 GPU 上最多四个显示器上启动 10 位 HDR 会话。
- 在以下情况下，Citrix 会话将恢复为 8 位非 HDR 模式：
    - 如果任何端点显示器未启用 10 位 HDR
    - 启用屏幕共享。
    - 在 VDA 上设置虚拟显示布局。
    - 在未设置“**允许视觉无损压缩**”策略的情况下切换到像素完美模式。

自适应刷新率

通过自适应刷新率，HDX™ 将虚拟显示器的刷新率与设置的目标 FPS 策略相匹配。自适应刷新率可为单会话和多会话 VDA 提供更好的性能和可扩展性。





注意

仅当使用 Citrix Indirect Display 或 IDD（根据 Citrix Virtual Apps and Desktops™ 默认设置）时，自适应刷新率才可用，而使用供应商提供的显示适配器时不可用。

图形容错模式

容错模式可确保在不可靠的网络上获得最佳性能和交互性。

当网络状况恶化，超出预定义的带宽、延迟和数据包丢失阈值时，Citrix® 图形编码器会自动切换到更激进的数据包传输模式，以克服数据包丢失的影响。

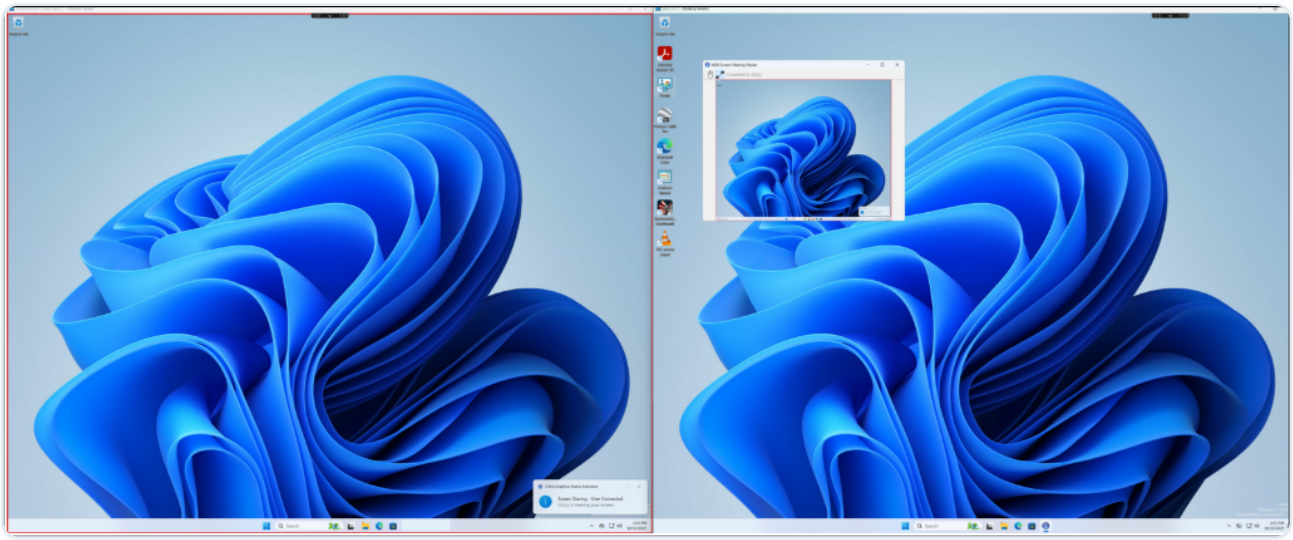
图形容错模式经过彻底改造，以确保在检测到数据包丢失时会话仍保持交互性。当网络状况恶化，超出预定义的带宽、延迟和数据包丢失阈值时，Citrix 图形编码器会自动切换到更激进的数据包传输模式，以克服数据包丢失的影响。因此，带宽使用量会按与数据包丢失量成比例的量增加。如果之后情况有所改善，Citrix 图形编码器会无缝切换回来。阈值可以通过策略进行配置，默认值为 300 毫秒延迟和 5% 数据包丢失。

目前支持适用于 Windows 2311 的 Citrix Workspace™ 应用程序。对其他平台的支持将在后续的 Citrix Workspace 应用程序版本中添加。与此功能的先前版本一样，必须启用 HDX™ 自适应传输

(EDT) 才能使此功能正常工作。此外，如果通过 Citrix Gateway Service 连接，则还必须在 Gateway 上启用图形容错模式。

HDX 屏幕共享

HDX 屏幕共享是 Citrix Virtual Apps and Desktops 中一项内置的、原生的、高性能功能，它使用户能够实时与他人共享其虚拟会话屏幕。它旨在提供低延迟和高质量，为协作、支持和培训场景提供无缝体验，而无需实施第三方软件解决方案。



HDX 屏幕共享功能直接集成到 HDX 协议中，这确保了共享会话既安全又高效，同时对会话性能的影响最小。

借助 HDX 屏幕共享，用户可以与一个或多个参与者共享其整个 Citrix 会话内容，包括键盘和鼠标控制。

此功能支持高分辨率显示器，最多可支持八台显示器。

HDX 屏幕共享可在所有 VDA 平台（包括 Windows、Linux 和 macOS）上使用，并提供跨平台兼容性。这意味着 Windows VDA 上的用户可以与 Linux 和 macOS VDA 上的用户共享其屏幕，反之亦然。

此外，HDX 屏幕共享不依赖任何客户端组件，因此可在所有客户端平台（包括移动设备）上访问。

关键概念

- **共享者：** 从其虚拟桌面会话发起屏幕共享并向他人展示其虚拟会话桌面的用户
- **查看者：** 连接到共享者会话以查看其屏幕的用户（或多个用户），也称为屏幕共享参与者
- **连接代码：** 共享者提供给查看者以访问共享会话的唯一系统生成安全代码。

- **图形状态指示器：** 位于通知区域的用户界面元素，提供用于启动、停止和管理屏幕共享会话的控件。
- **屏幕共享播放器：** 查看者用于查看共享者会话的会话内工具。

用例和示例使用场景

正确配置和利用 HDX 屏幕共享可以满足各种组织需求，从 IT 支持到协作开发和培训。

场景 1：IT 帮助台和远程支持

IT 管理员需要排查用户在其虚拟桌面中遇到的问题。IT 管理员无需尝试重现问题，即可通过 Citrix Director 中的 HDX 屏幕共享启动远程协助。 管理员可以实时查看用户的确切屏幕，从而更快地识别和解决问题。请求键盘和鼠标控制的功能允许管理员直接采取行动。 从 CVAD 2511 及更高版本开始，HDX 屏幕共享也已集成到 Citrix Director 中。有关通过 Citrix Director 使用 HDX 屏幕共享的更多信息，请参阅 Citrix Director 文档

场景 2：最终用户协作

一个工程师团队正在其虚拟桌面中，使用图形密集型应用程序处理复杂的 3D 模型。他们需要共同审查设计并进行实时调整。

一名工程师可以共享其会话，整个团队可以查看模型、提出更改建议，甚至轮流控制应用程序进行编辑。这避免了导出文件或使用第三方屏幕共享工具的需要。

场景 3：员工入职和培训

新员工正在学习如何使用专有的业务线应用程序。培训师可以直接在新员工的虚拟会话中演示应用程序的功能。

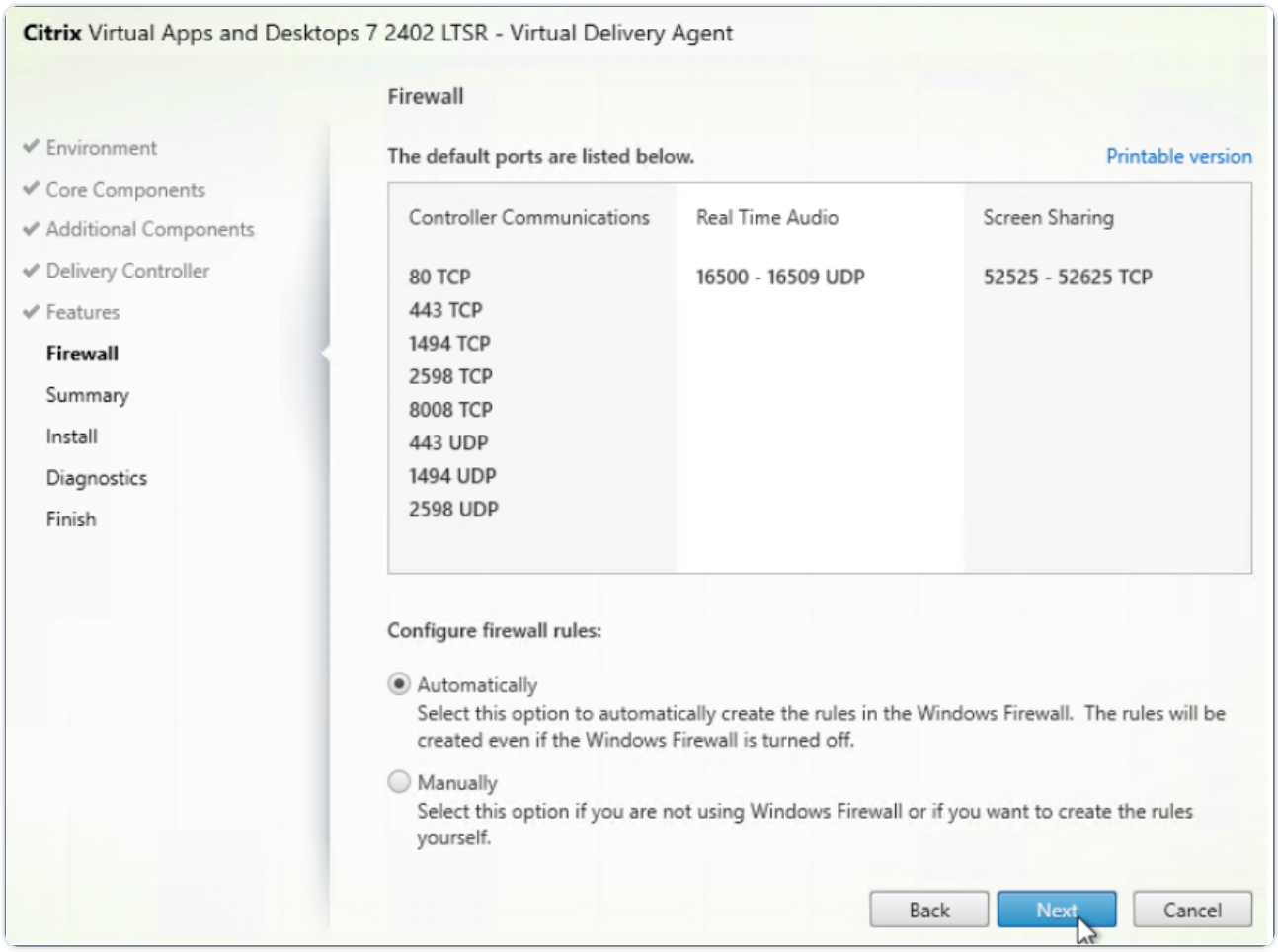
培训师可以一步一步地指导新员工。彩色边框指示器（红色或黄色）清晰地显示会话何时正在共享，为学习环境提供视觉提示。

系统要求

所有 VDA 平台都支持 HDX 屏幕共享，但某些平台可能存在额外要求。有关详细信息，请参阅下文。

HDX 屏幕共享默认使用 52525 到 52625 范围内的 TCP 端口。

安装 VDA 2112 及更高版本时，可以将 VDA 安装程序配置为自动打开 HDX 屏幕共享的默认防火墙端口。



如果在 VDA 安装期间未执行此操作，或者配置了自定义端口范围，请在 VDA 上手动打开这些端口。

> **注意：**

> 托管会话的 VDA 与连接到共享会话的计算机之间必须存在网络连接。

> 单个屏幕共享会话最多可连接 64 个查看器。端口范围控制多会话环境中可以开始屏幕共享的最大用户数。每个用户需要一个端口。

> **注意：**

> 连接到会话的所有显示器都将共享。您无法选择单个显示器。

> 不支持 AV1 和 H.265 视频编解码器以及 10 位颜色模式。在活动屏幕共享期间，会话将自动回退到 H.264 视频编码。屏幕共享会话结束后，AV1 和 H.265 将再次可用。

Windows 虚拟交付代理

- Windows：单会话或多会话操作系统 VDA
- 必须启用图形状态指示器。

> **注意：**
>
> 只能共享桌面会话。

Linux 虚拟交付代理

- 如果多个 Linux VDA 之间发生会话共享，建议升级到相同的 VDA 版本，以避免键盘输入问题。
- 建议将 Citrix Workspace™ 应用程序配置为使用扫描码模式
- 必须启用系统托盘图标

有关 Linux VDA 的 HDX 屏幕共享的更多信息，请参阅 Linux VDA HDX 屏幕共享文档

MacOS VDA

- Qt 5，修订版 5.15.13 或更高版本。

为了使所有 VDA 上的 HDX 屏幕共享具有统一的用户体验，您需要安装 Qt 框架，最低兼容版本为 Qt 5（修订版 5.15.13 或更高版本）。

在 VDA 上安装 Qt 5 可以通过例如 homebrew 来执行，运行以下 命令：

```
brew install qt@5
```

有关适用于 macOS VDA 的 HDX 屏幕共享的更多信息，请参阅适用于 HDX 屏幕共享的 macOS VDA 文档

配置

HDX 屏幕共享默认处于禁用状态，可以通过 Citrix® 策略启用和配置此功能。

这些策略将对 HDX 屏幕共享配置提供精细控制。

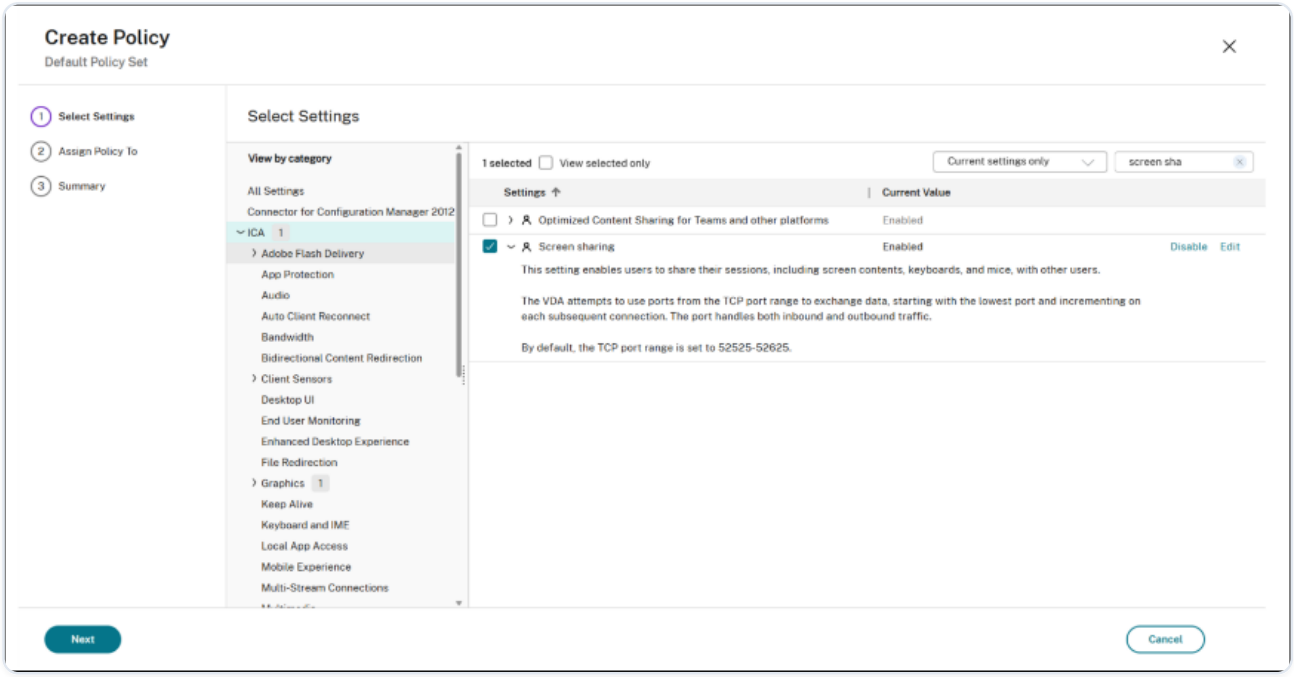
为最终用户启用 HDX 屏幕共享

HDX 屏幕共享默认处于禁用状态。要使最终用户能够通过 HDX 屏幕共享其屏幕，需要按如下方式启用和配置这些功能：

- 启用 HDX 屏幕共享策略
- 启用图形状态指示器
- **可选：** 在 VDA 防火墙中配置并打开自定义端口

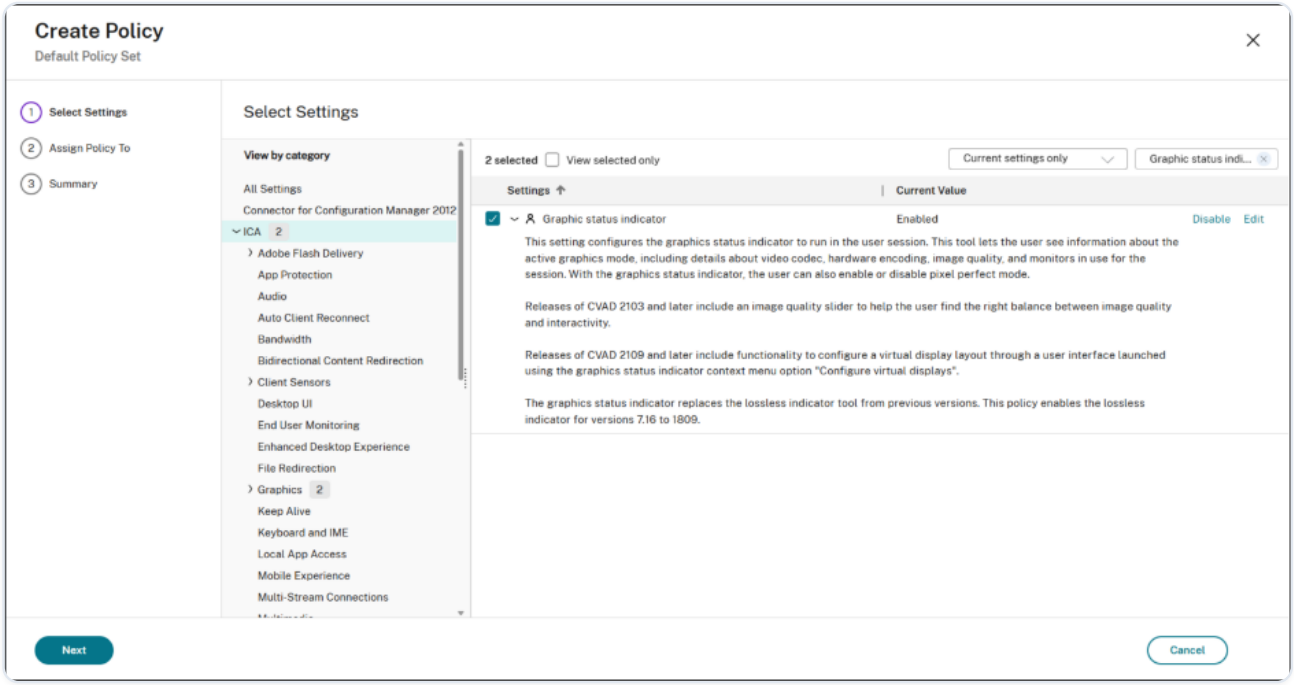
步骤 1：启用 HDX 屏幕共享

要启用 HDX 屏幕共享，请浏览到“**屏幕共享**”策略并将策略设置为“**已启用**”



步骤 2：启用图形状态指示器

浏览到“**图形状态指示器**”并将策略设置为“**已启用**”



额外的 HDX 屏幕共享配置

默认情况下，HDX 屏幕共享使用以下 TCP 端口进行通信：

- TCP 起始端口：52525
- TCP 结束端口：52625

默认 TCP 端口范围可以通过“HDX 屏幕共享端口”策略进行调整：

要调整 TCP 端口范围，请浏览到“HDX 屏幕共享端口”策略并将端口范围设置为所需的端口范围。

端口配置可用于限制在多会话 VDA 中同时共享屏幕的用户数量。

> **注意：**
>
> 端口配置不应与 Director 的 HDX 屏幕共享重叠。

> HDX 屏幕共享连接代码默认情况下永不失效，并且可以在屏幕共享会话期间无限期地用于加入该会话。

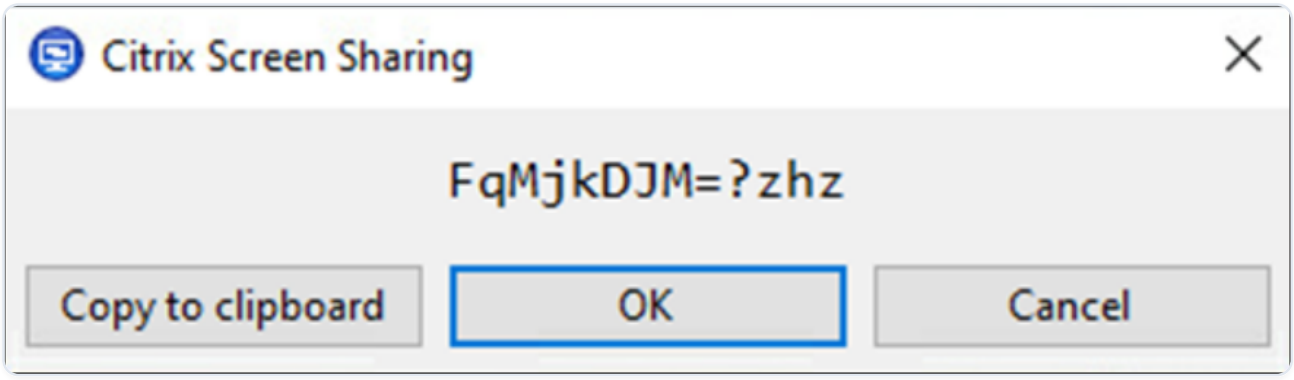
为了增强安全性，可以配置超时设置，在此之后连接代码将过期。一旦指定的超时期限过去，之前生成的连接代码将失效，新用户将无法使用此代码加入屏幕共享会话。共享者需要重新生成新的会话连接代码。

此外，当屏幕共享会话已启动且在配置的超时期限内没有观众连接时，屏幕共享将自动停止。要恢复屏幕共享，共享者需要重新启动 HDX 屏幕共享并共享连接代码。

要为 HDX 屏幕共享会话配置超时，请浏览到“HDX 屏幕共享超时”策略并将所需的超时值设置为分钟。

连接代码配置（预览）

默认情况下，HDX 屏幕共享使用 40 个字符的连接代码。从 CVAD 2411 开始，管理员可以配置 HDX 屏幕共享使用新的、更短的连接代码。新的连接代码更短，为 13 个字符，并且不包含模糊字符，以便共享者更容易地向潜在观众口头传达连接代码。



目前，配置作为 VDA 的注册表设置提供。请注意，新的、较短的连接代码不提供对旧版 VDA 的向后 兼容性。

> **注意：**
>
> 新的、较短的连接代码不提供对旧版 VDA 的向后兼容性。

先决条件

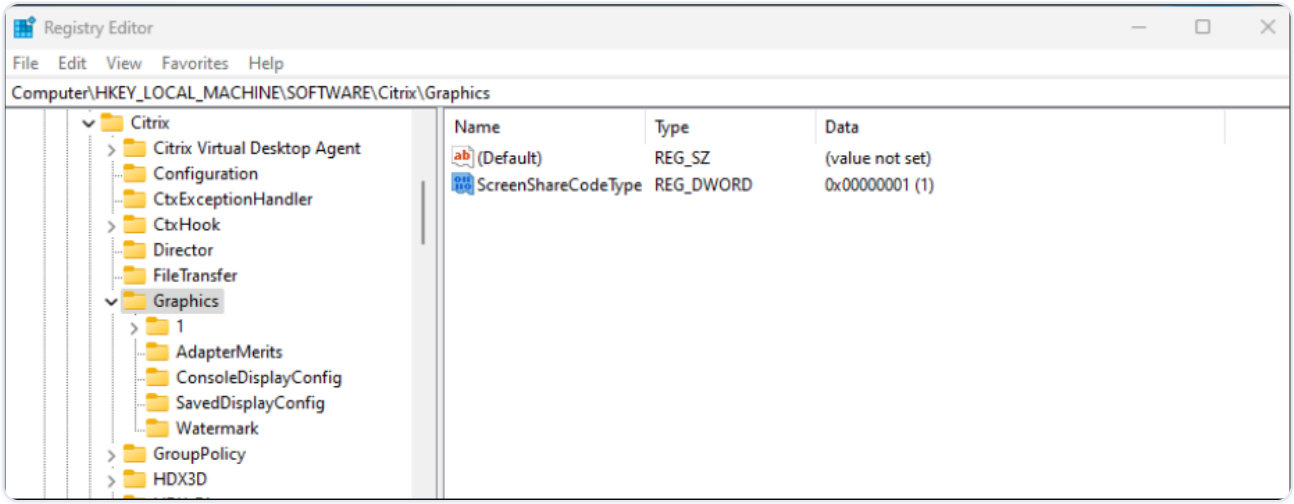
VDA - CVAD 2411 及更高版本

连接配置

要启用新的较短连接代码：

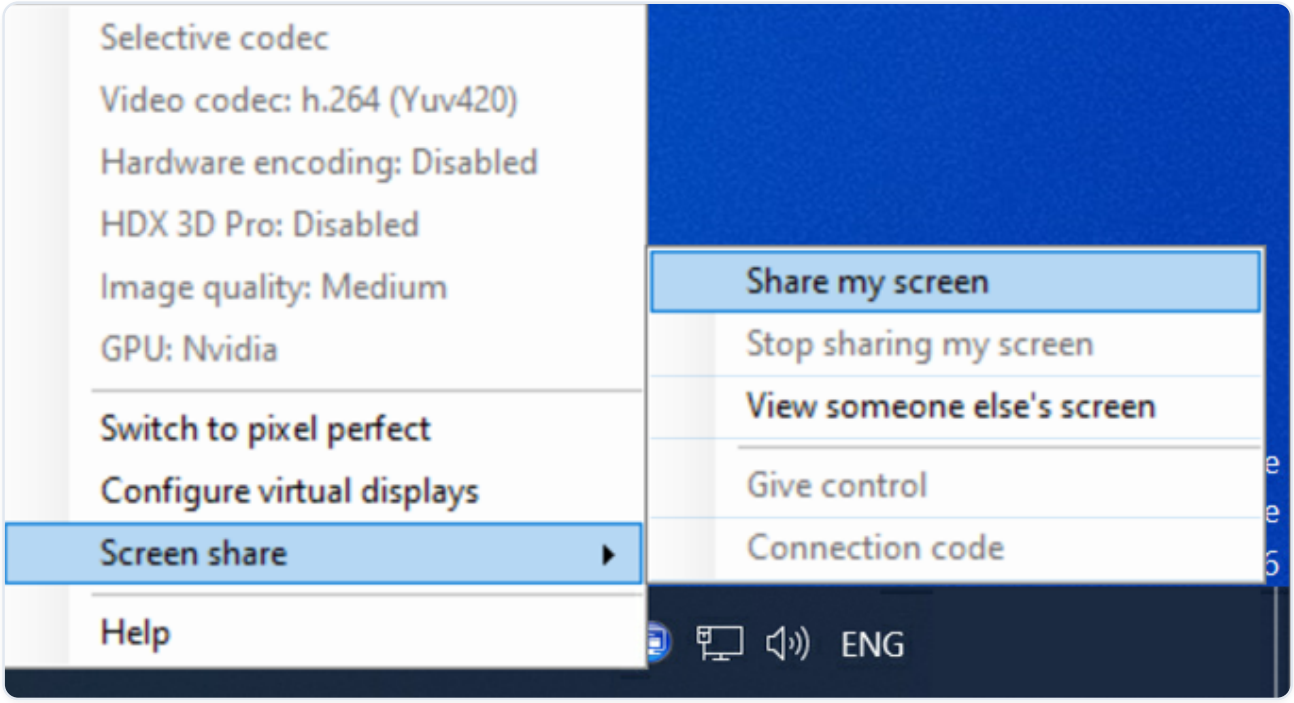
1. 使用 regedit.exe 打开 Windows 注册表编辑器。
2. 导航到 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\ScreenShare`
3. 创建一个名为 **CodeType** 的 **DWORD** 值，并将其设置为 1。

此键控制要使用的连接代码，0 表示旧版较长连接代码，1 表示新版较短代码。



启动屏幕共享会话

作为共享者，要共享会话，请在 Windows 通知区域中查找 HDX 图形状态指示器图标。右键单击它以显示菜单并选择“屏幕共享”>“共享我的屏幕”。



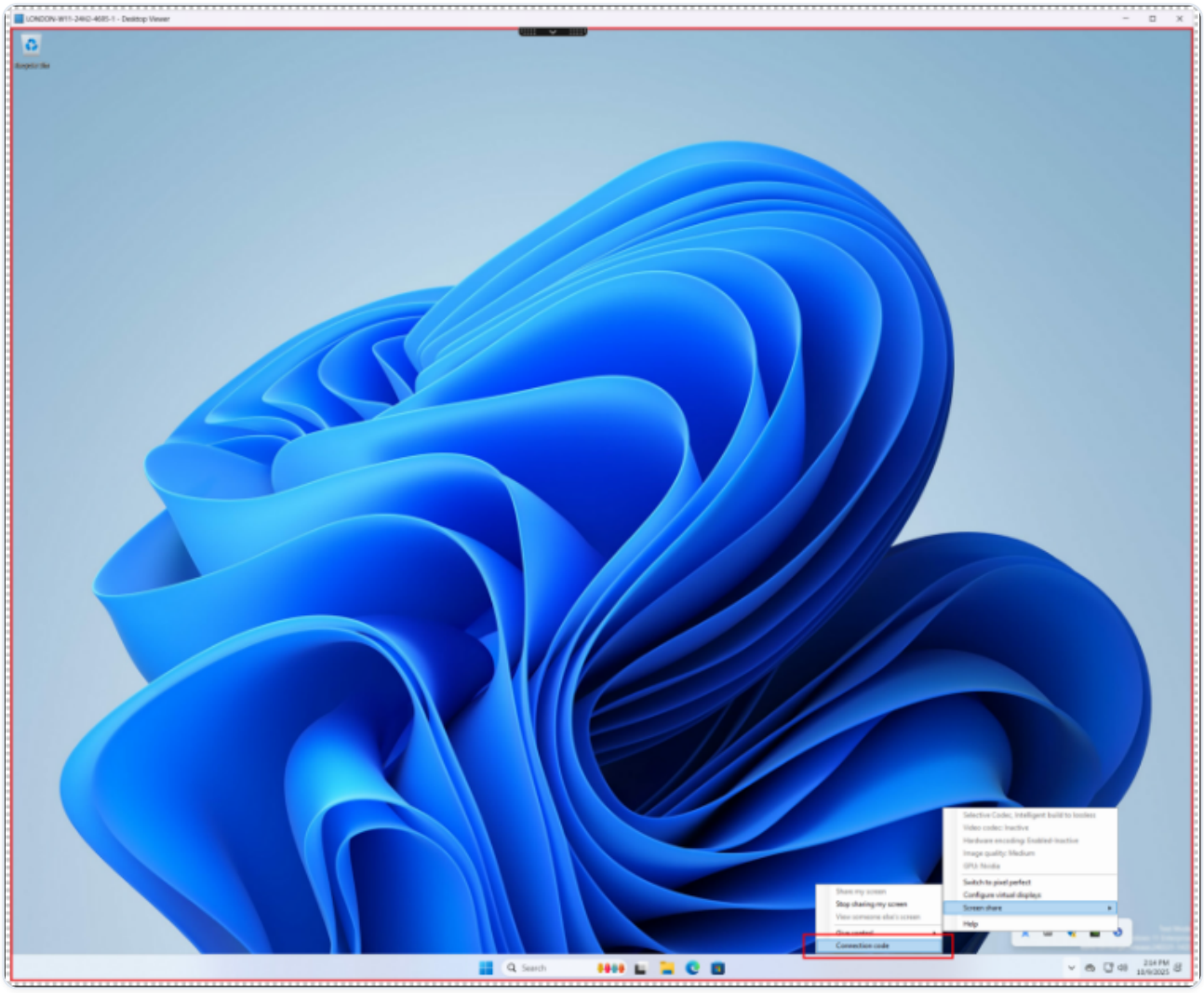
启动屏幕共享后，将出现一个对话框，其中包含可用于加入屏幕共享会话的连接代码。一个或多个查看者可以使用此代码连接到您的屏幕共享会话。

单击“复制到剪贴板”或手动选择并复制对话框中显示的连接代码。

连接代码可以粘贴到所选应用程序中，例如电子邮件应用程序或 Microsoft Teams，以便分发给其他用户。

复制连接代码后，可以通过单击“确定”或右上角的“x”来关闭对话框。

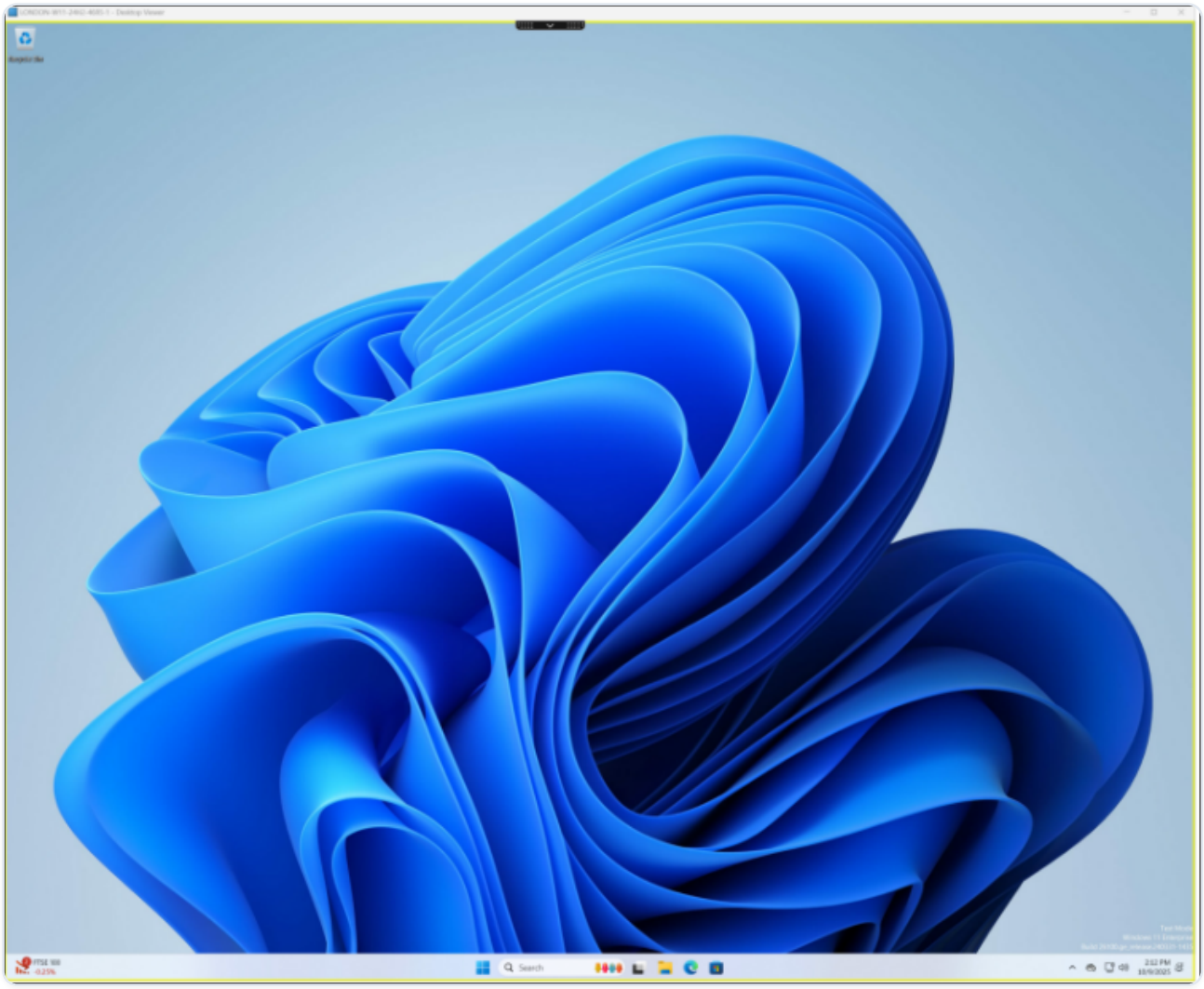
在会话共享期间，可以随时从“屏幕共享”>“连接代码”菜单选项中检索当前活动的连接代码。



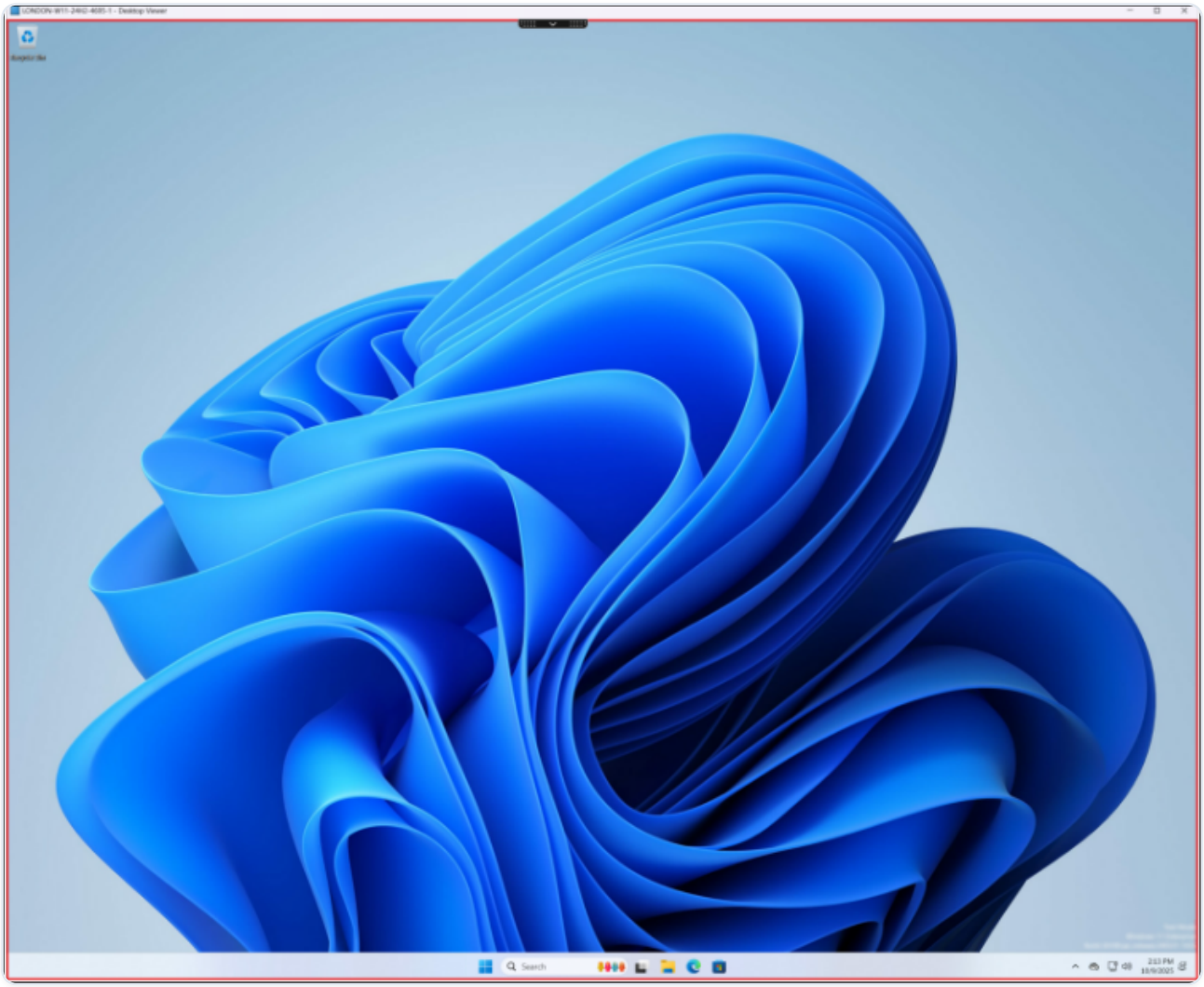
注意：

请谨慎选择共享连接代码的对象；所有与您共享连接代码的用户都可能连接到您正在进行的屏幕共享会话。

屏幕共享会话启动后，Citrix 会话周围将出现黄色边框，表示 HDX 屏幕共享处于活动状态，但尚未有观众加入。



当观众连接到屏幕共享会话时，边框将变为红色，表示屏幕共享会话处于活动状态且有观众连接。



请注意，如果您的 Citrix 会话中有多个活动屏幕，所有屏幕都将通过屏幕共享进行共享，并且观众将能够看到会话中所有连接的屏幕。

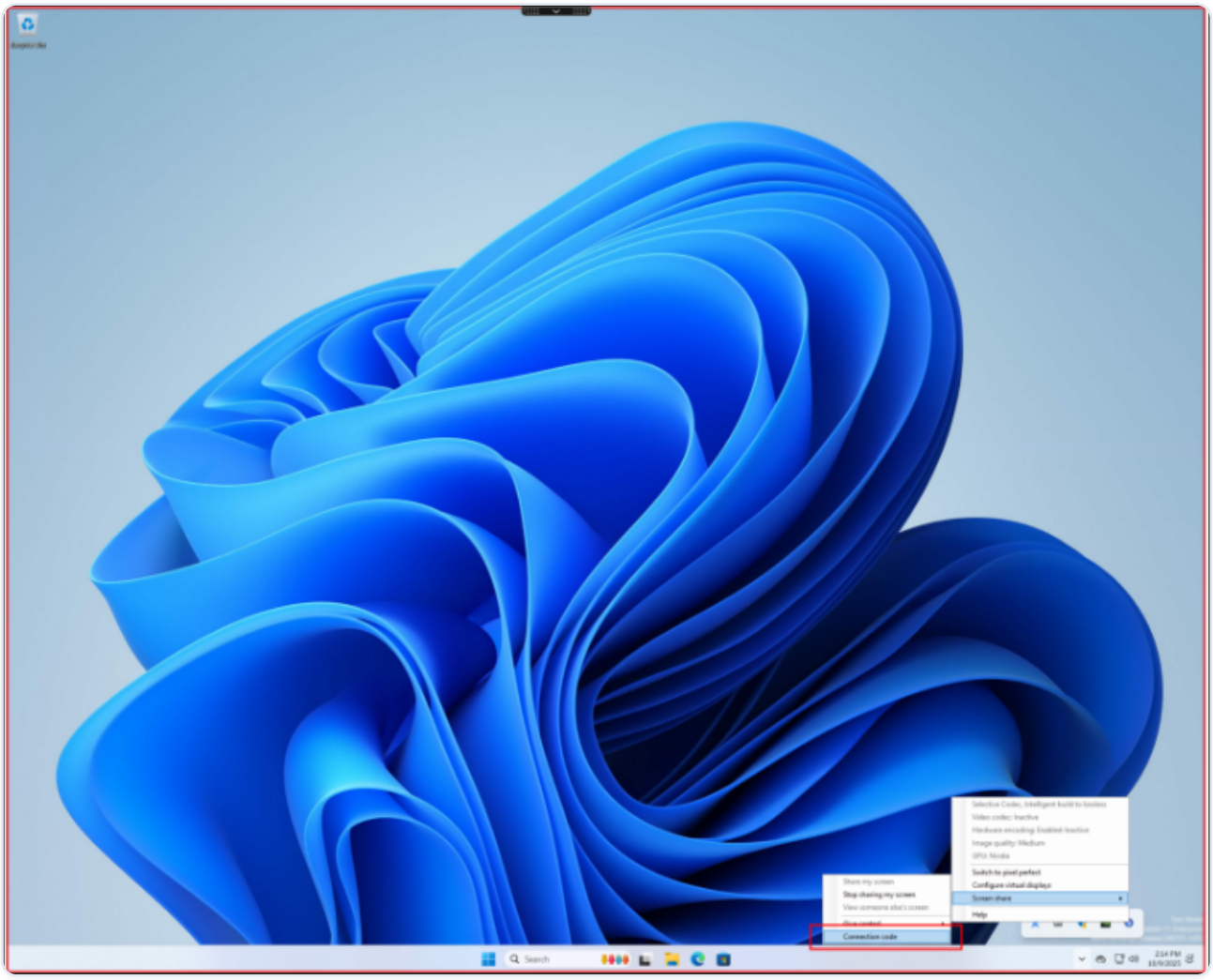
目前不支持在您的会话中仅共享单个显示器或连接显示器的一个子集。

默认情况下，最多 100 名观众可以连接到单个屏幕共享会话，尽管此限制可能会受到您的 Citrix 管理员的限制。

重新生成新的连接代码

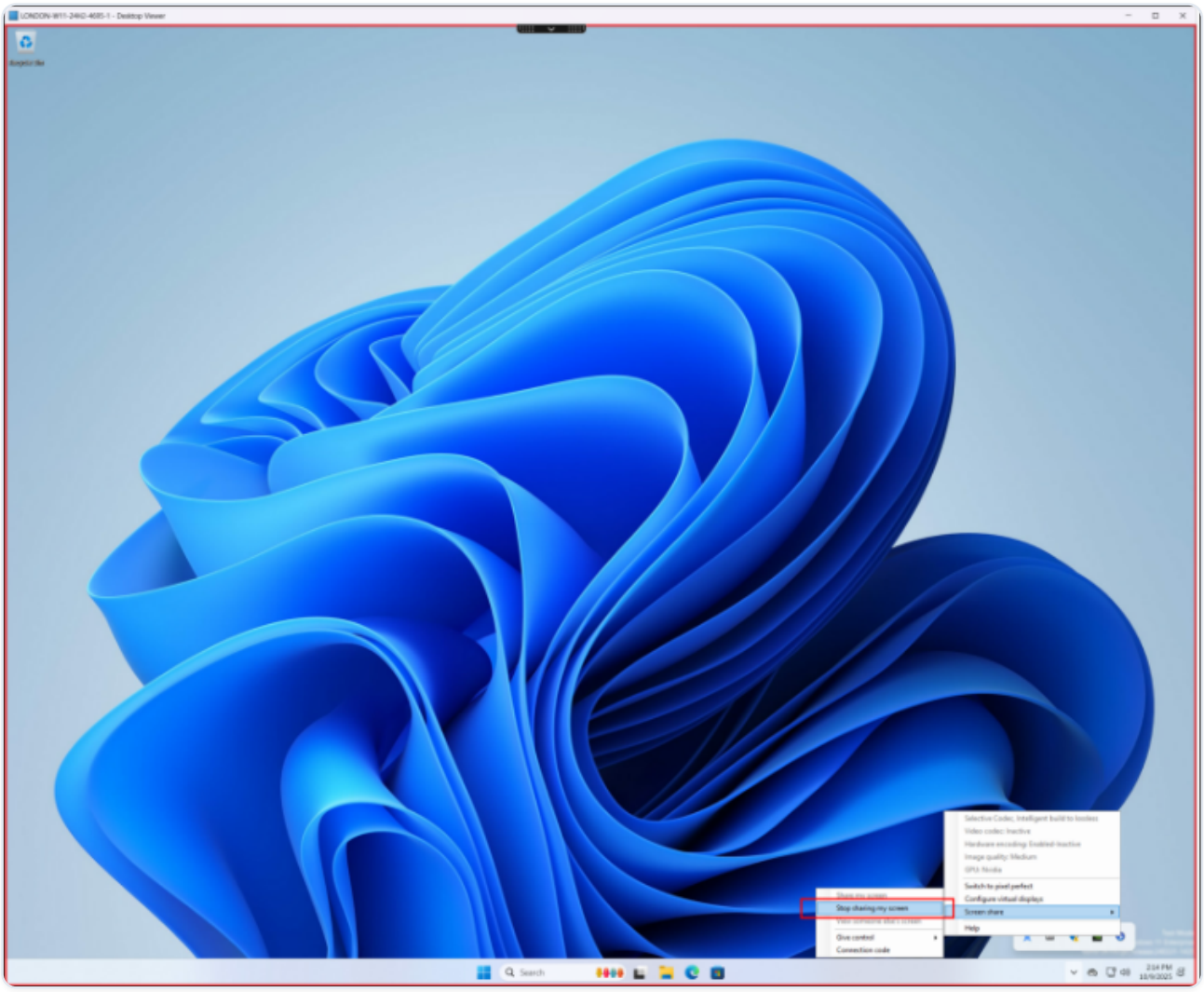
只要连接代码处于活动状态，新用户就可以使用该连接代码加入您的屏幕共享会话。如果代码已过期，现有观众将保持连接，但新用户将无法连接到您的屏幕共享会话。要允许新用户连接到您的会话，您需要重新生成一个新的连接代码。

在会话共享期间，可以随时从“屏幕共享”>“连接代码”菜单选项中检索新的连接代码。



停止屏幕共享

要停止屏幕共享，请在 Windows 通知区域中查找 HDX 图形状态指示器图标。右键单击它以显示菜单，然后选择“屏幕共享”>“停止共享我的屏幕”。屏幕共享将立即停止，所有当前查看者都将从您的会话中断开连接。红色边框将消失，表示屏幕共享已停止。

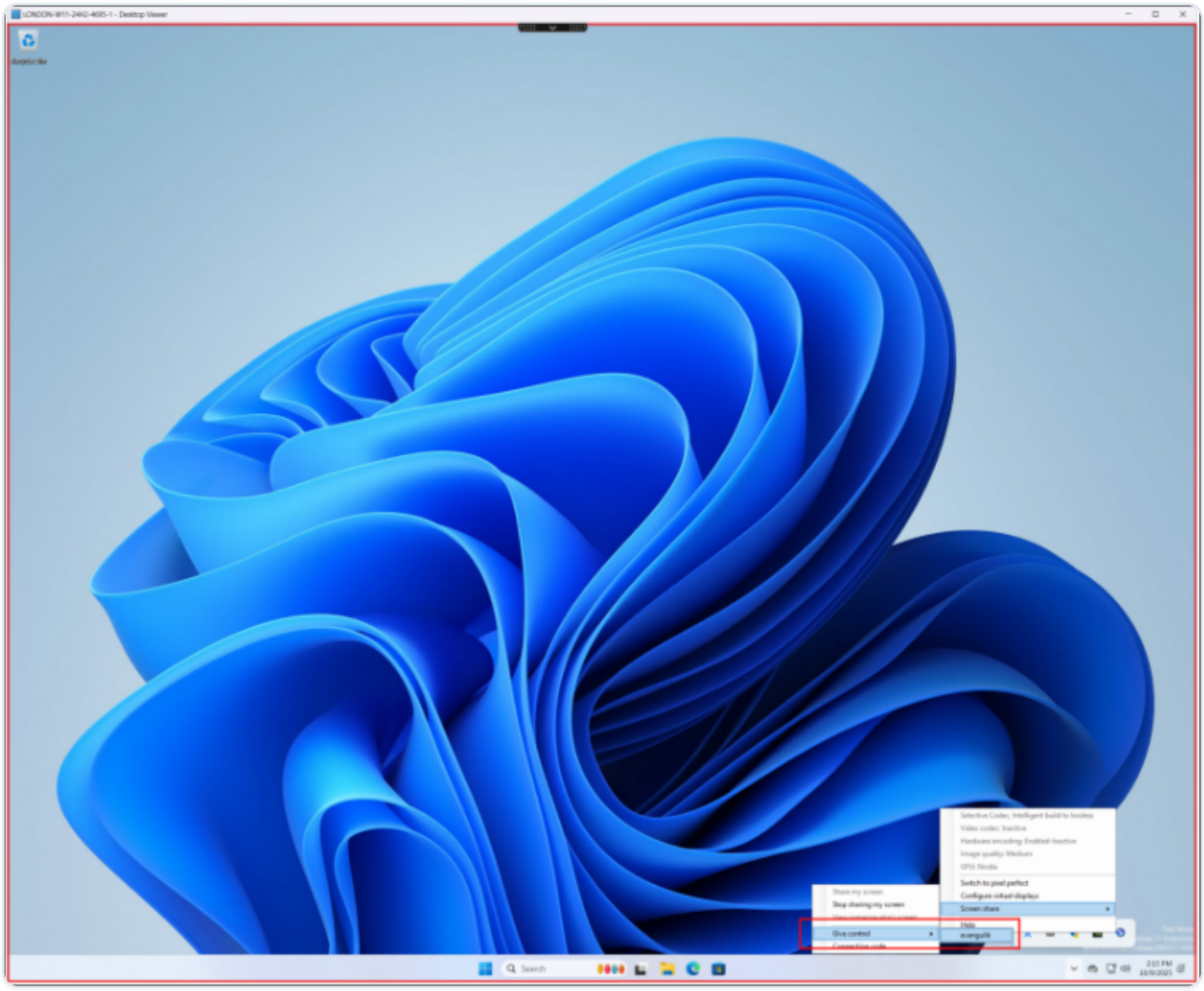


授予鼠标和键盘控制权

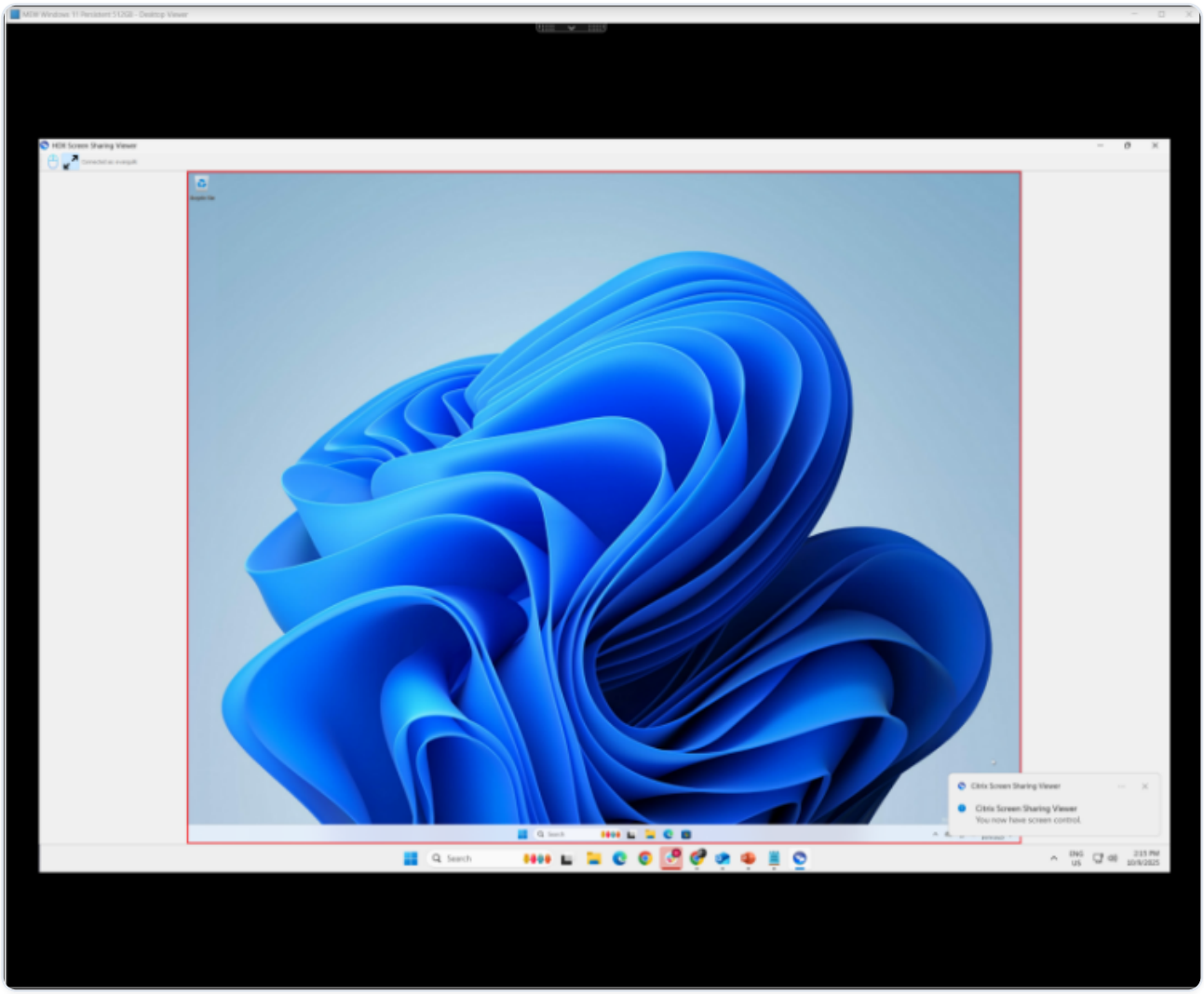
在屏幕共享会话的任何时候，作为共享者，您都可以将鼠标和键盘控制权移交给特定查看者。

移交后，该查看者将在您的 Citrix 会话中与您共享对您的鼠标和键盘的完全控制权。

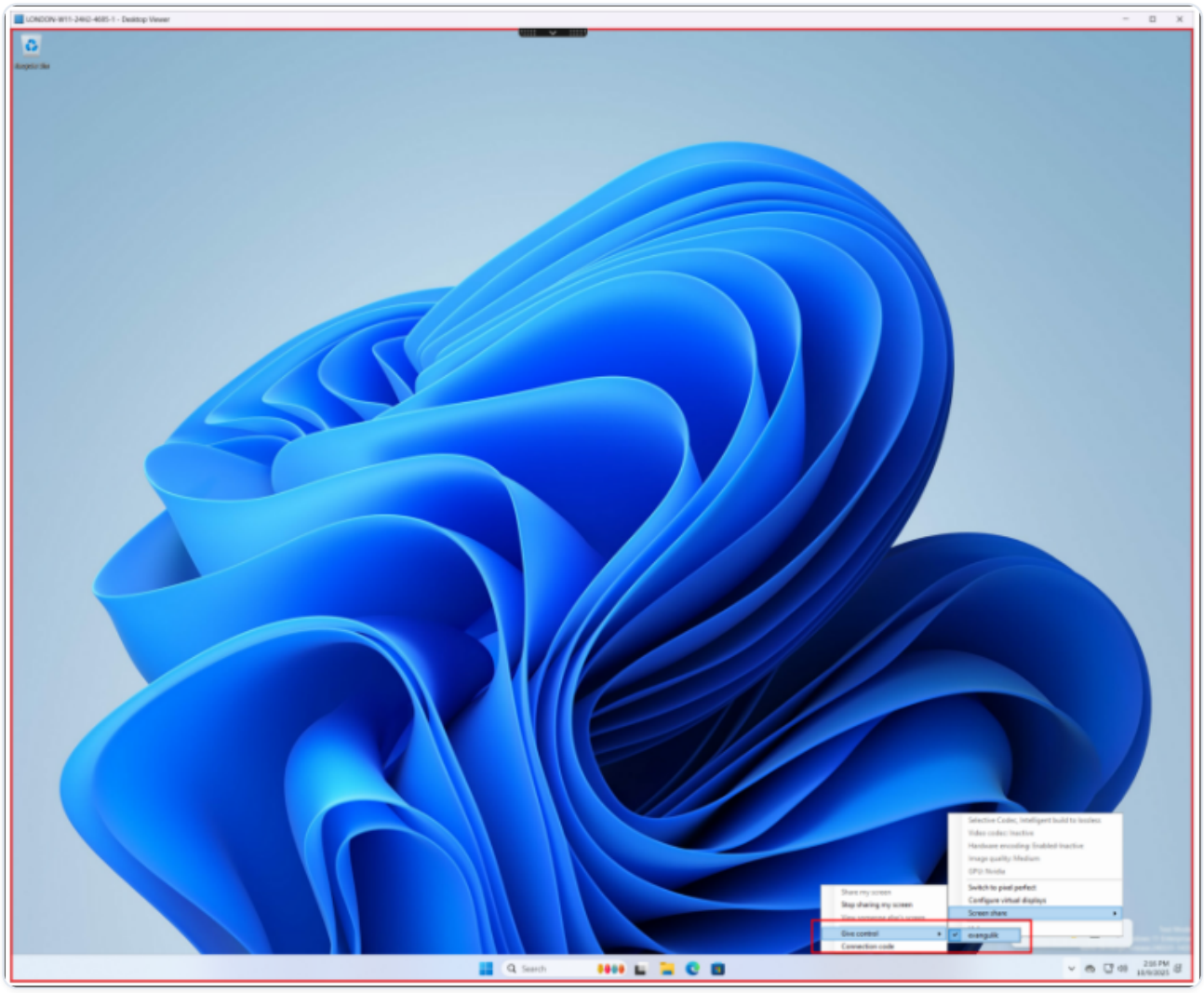
要共享鼠标和键盘控制权，请打开 Windows 通知区域中的图形状态指示器图标。右键单击它以显示菜单，然后选择“屏幕共享”>“授予控制权”，并选择一个活动查看者来移交控制权。



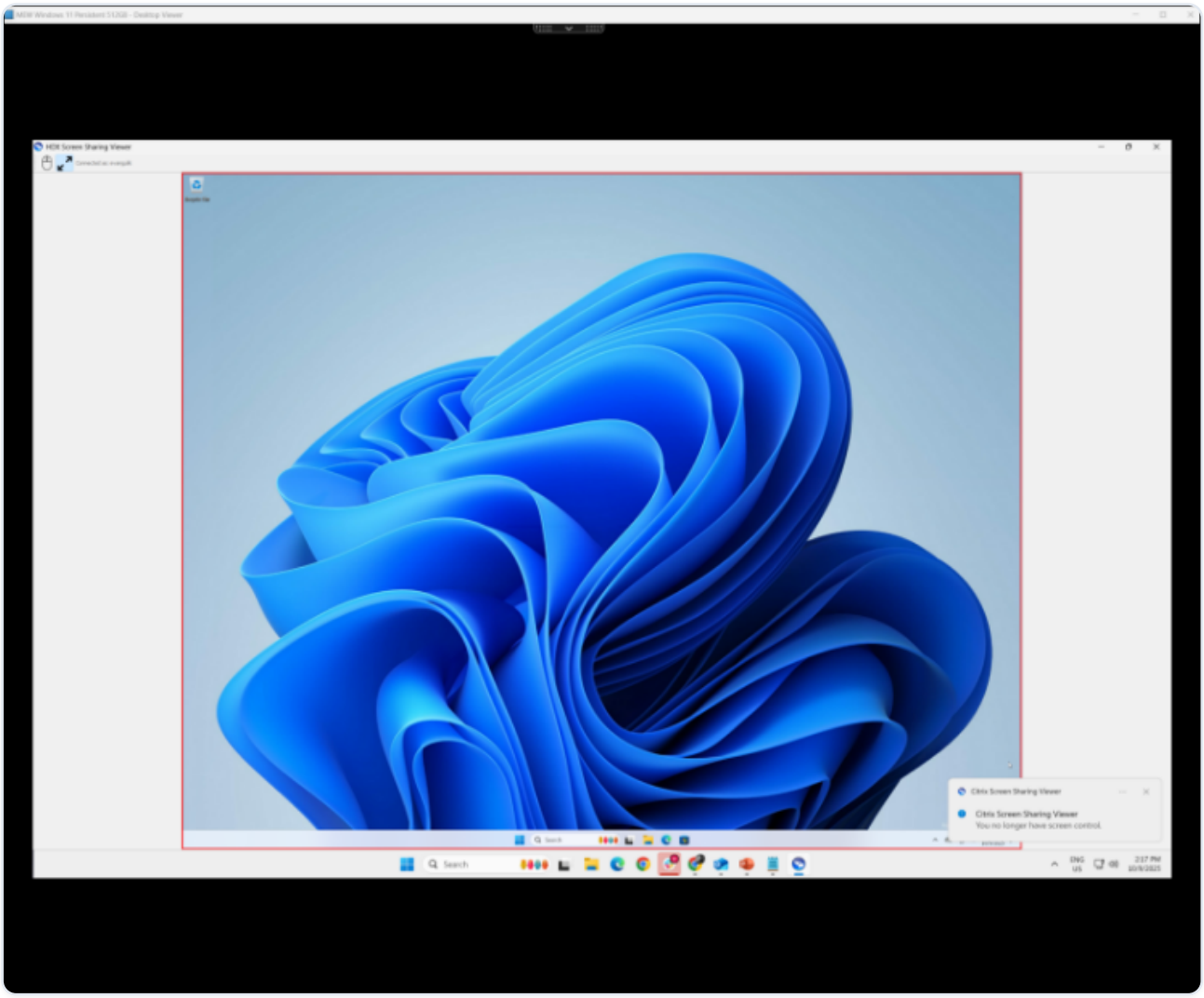
选定的查看者将收到通知，指示他已获得鼠标和键盘控制权。



要停止鼠标和键盘共享并收回控制权，请打开 Windows 通知区域中的图形状态指示器图标。右键单击它以显示菜单，然后选择“屏幕共享”>“授予控制权”，并取消选择活动查看者。

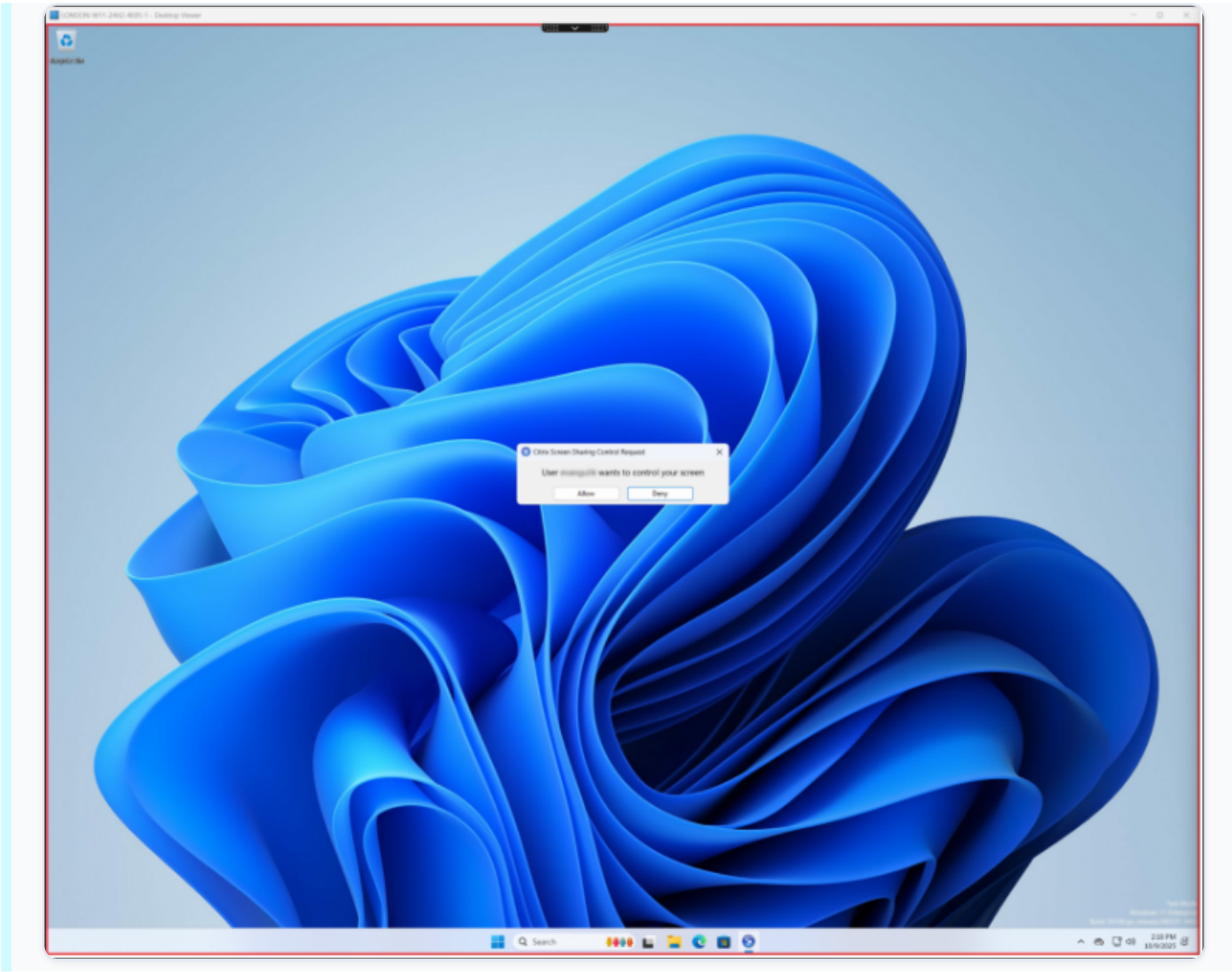


查看者将收到通知，告知他已失去鼠标和键盘控制权。



注意：

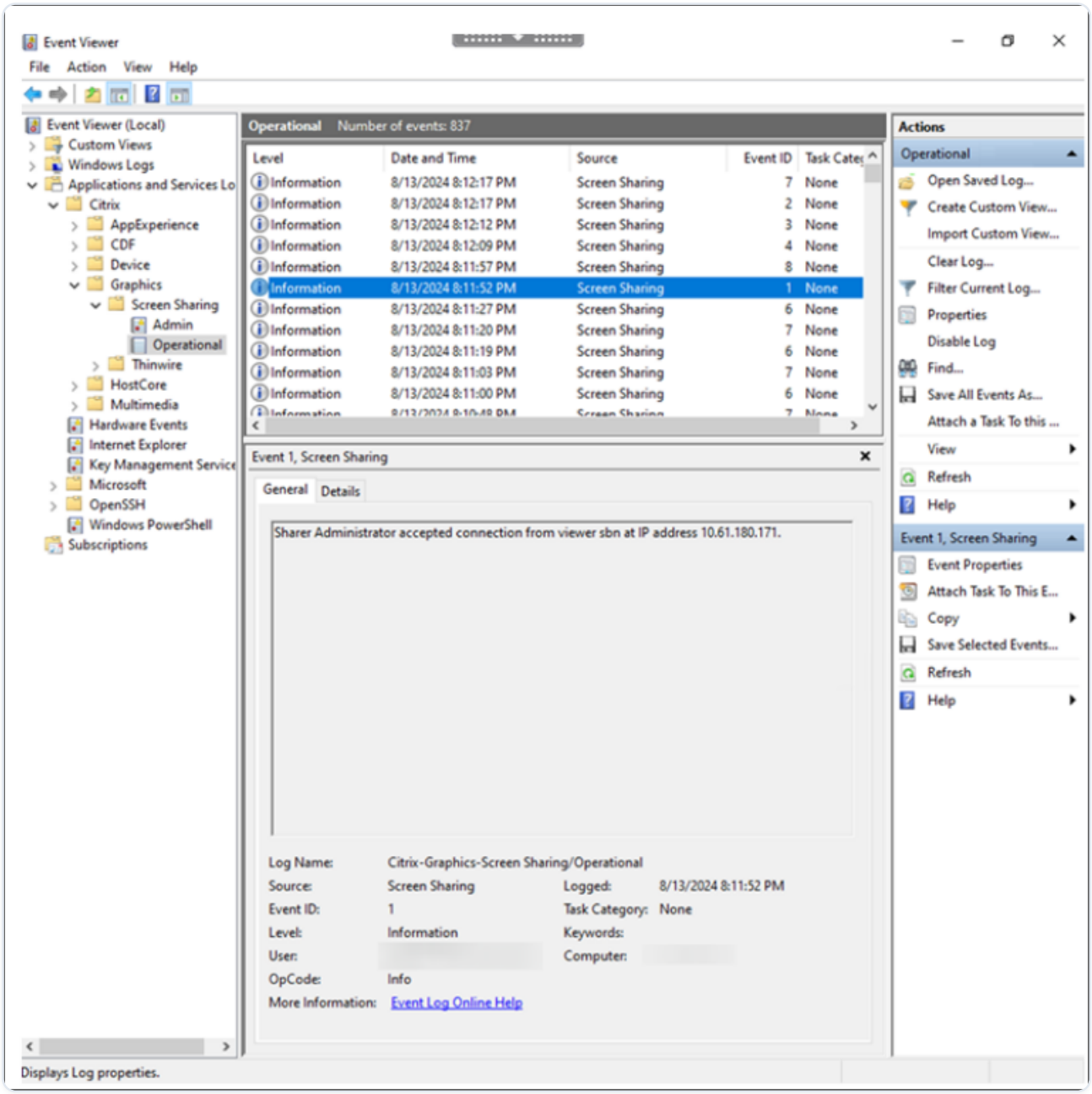
您一次只能与一位查看者共享鼠标和键盘控制权。查看者也可以请求控制鼠标和键盘。发生这种情况时，您将收到请求通知，并且可以选择允许或拒绝其请求。



事件日志记录

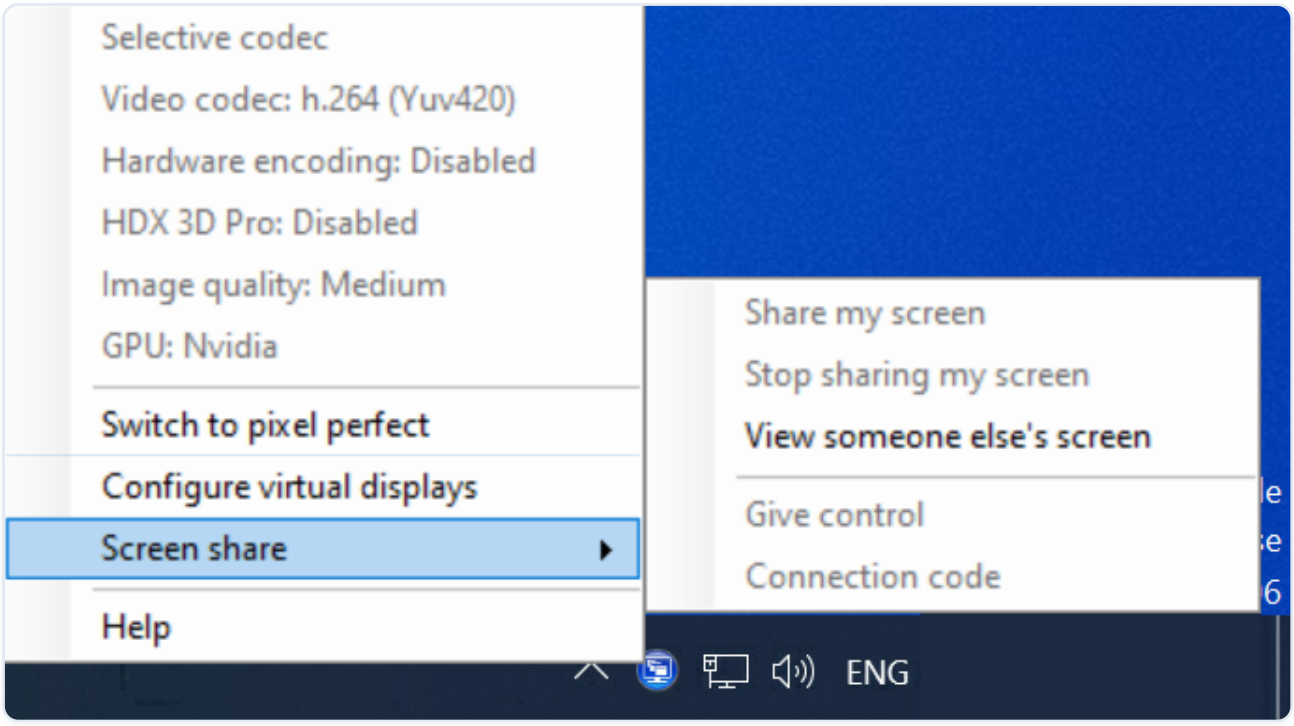
出于安全和审计目的，共享者 VDA 上的屏幕共享事件现在已收集并记录，这将允许管理员跟踪共享者 VDA 上的屏幕共享活动。在屏幕共享 会话期间，将记录以下信息和事件：

- 共享开始/停止 – 表示屏幕共享会话开始和停止的事件
- 连接请求 – 请求连接的查看者的 IP 和用户名，以及所使用的连接代码和连接决定（允许/拒绝连接，原因可能是身份验证失败或共享者决定）
- 屏幕控制请求 – 请求屏幕控制的查看者 IP 和用户名，以及决定（允许/拒绝）
- 查看者操作 - 断开屏幕共享会话连接或释放共享者屏幕控制权的查看者 IP 和用户名。



查看屏幕共享会话

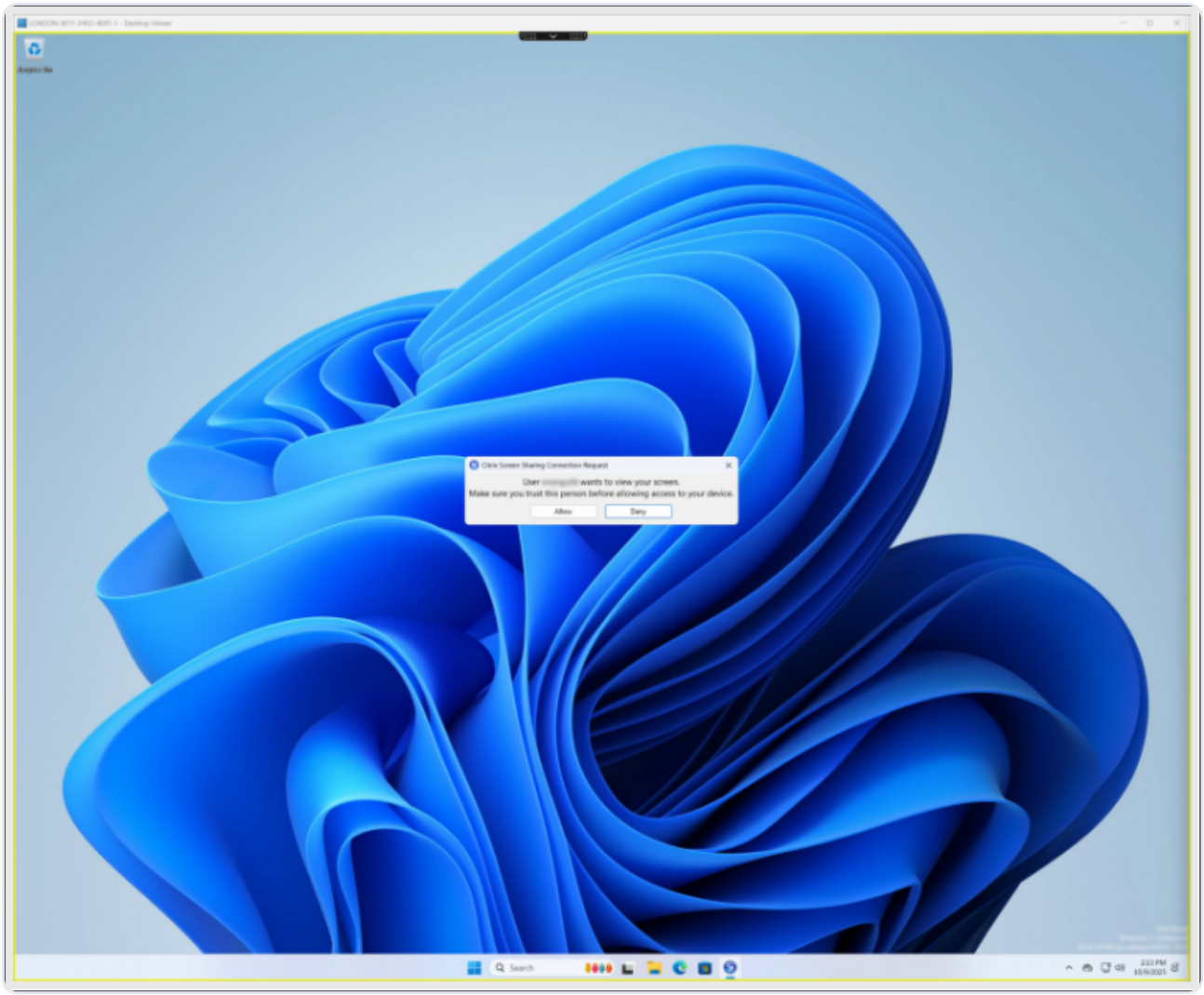
要连接到其他人的会话，请在 Windows 通知区域中查找 HDX 图形状态指示器图标。右键单击它以显示菜单，然后选择“屏幕共享”>“查看其他人的屏幕”。



系统将提示您输入连接代码。HDX 屏幕共享者将向您提供此代码。在文本框中输入或粘贴会话的连接字符串，该字符串由共享会话的用户提供。

当您单击“连接”时，连接代码将进行验证，如果验证成功，将建立与共享者会话的屏幕共享连接，并且屏幕共享查看器将自动打开并显示共享者的屏幕（或多个屏幕）。

当您连接到会话时，共享者将收到您参与其屏幕共享会话的通知。



调整显示缩放

如果共享者使用的显示器分辨率高于您的分辨率，或者他们在会话期间使用多个显示器，屏幕共享播放器将自动调整分辨率。要禁用缩放并查看共享者显示器的原始分辨率，请选择屏幕共享播放器左上角的对角箭头。

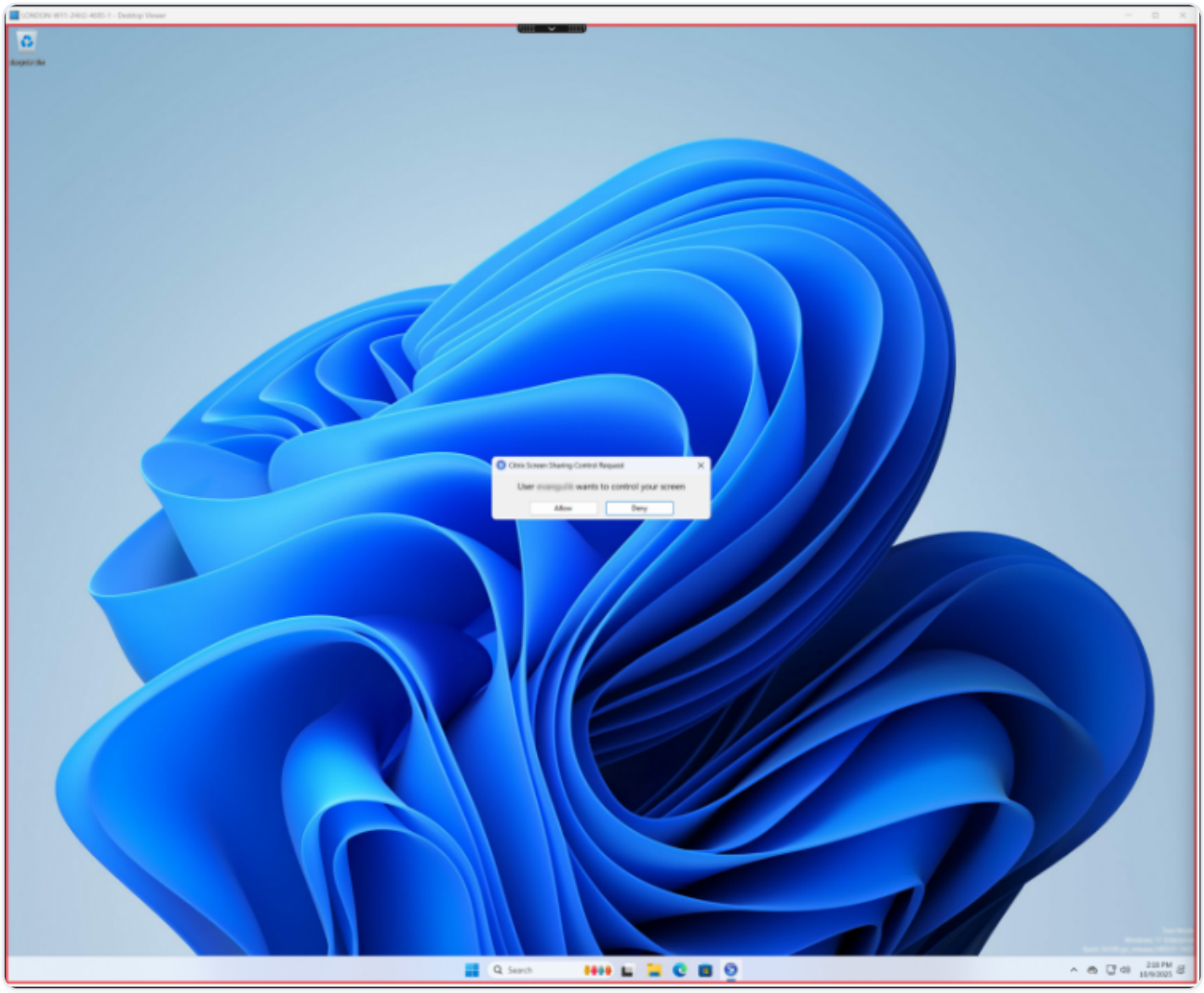
断开屏幕共享会话

要断开屏幕共享会话，请随时关闭屏幕共享播放器。要重新连接，如果连接代码尚未过期，您可以使用相同的代码与共享者重新加入屏幕共享会话。如果连接代码已过期，共享者需要为您重新生成一个新代码。连接代码的过期由连接超时屏幕共享策略控制，该策略可由管理员设置。

请求鼠标和键盘控制

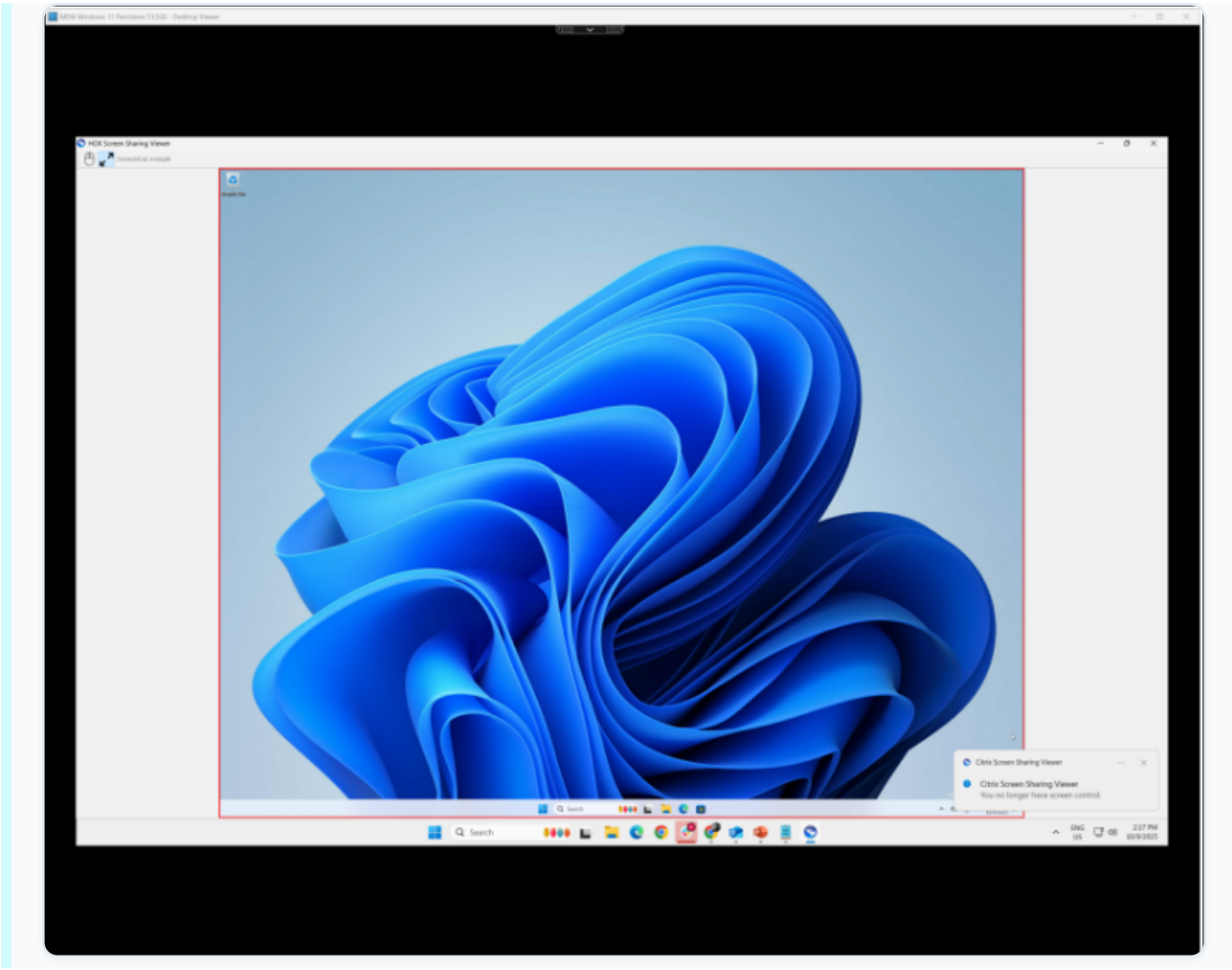
默认情况下，共享者在屏幕共享会话中拥有鼠标和键盘的完全控制权。作为查看者，您可以向共享者请求鼠标和键盘控制权。

要请求鼠标和键盘控制，请点击屏幕共享查看器左上角的“鼠标图标”。共享者将收到您的请求通知，并可以允许或拒绝。一旦共享者批准了鼠标和键盘控制请求，您作为查看者和屏幕共享者都将在会话中共享鼠标和键盘控制权。



注意：

共享者可以随时收回鼠标和键盘的独占控制权。



虚拟显示布局

虚拟显示配置允许您在 VDA 上的实时会话中为每个会话监视器定义虚拟显示布局。此功能允许您将每个会话监视器独立拆分为多个虚拟监视器。

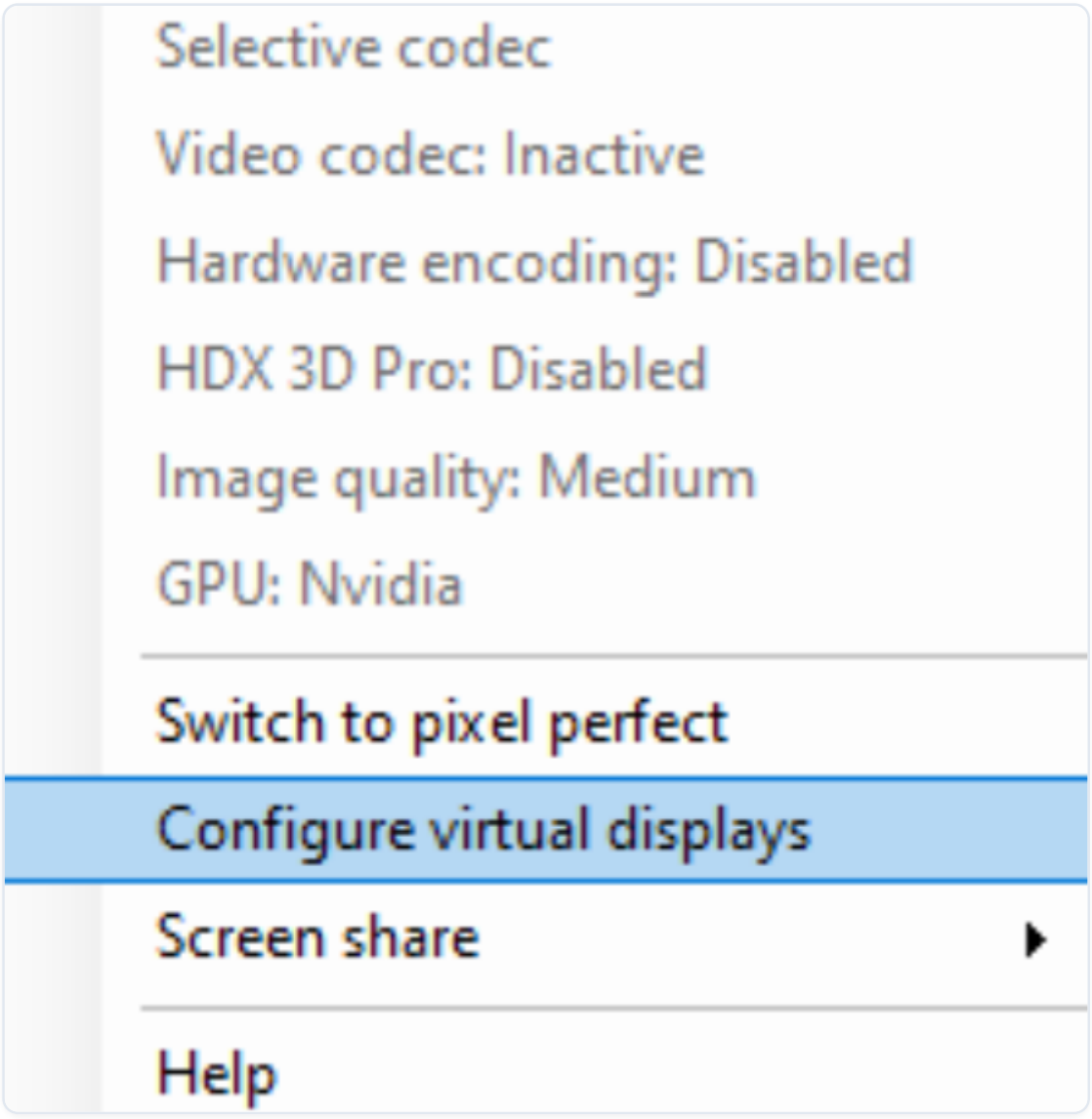
虚拟显示配置 UI 允许您在 VDA 上的实时会话中为每个会话监视器定义虚拟显示布局。此功能允许您将每个会话监视器独立拆分为多个虚拟监视器。您可以在远程桌面上总共拆分为 8 个虚拟监视器。此外，您还可以更新显示器的会话主监视器和 DPI 设置。

系统要求

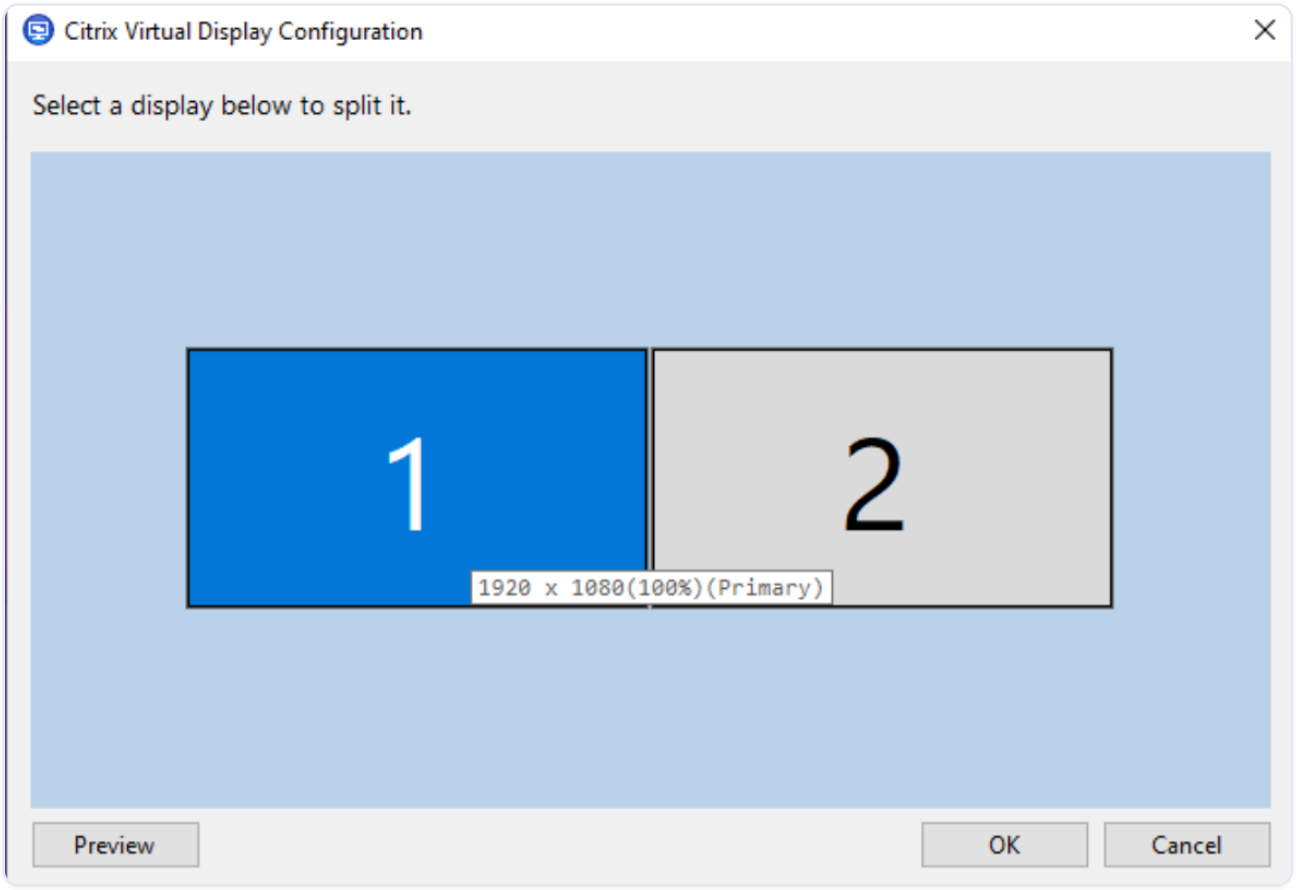
- Windows：单会话或多会话操作系统 VDA
- 图形状态指示器 策略必须启用
- 只能配置桌面会话。

配置

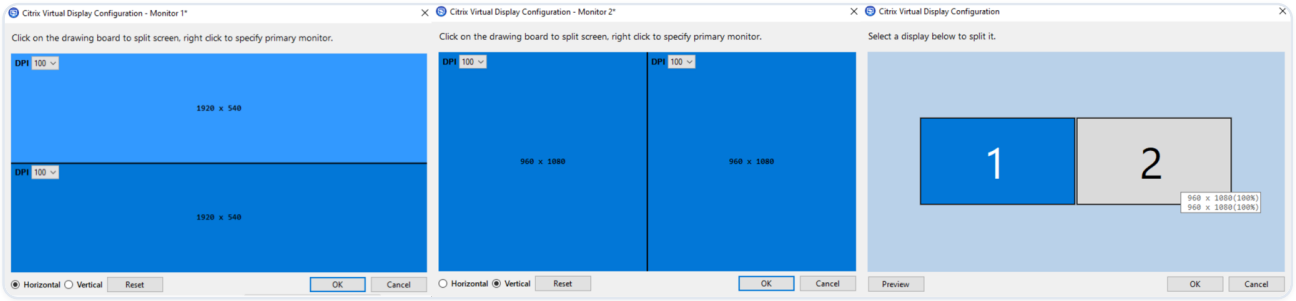
要配置虚拟显示布局，请右键单击图形状态指示器图标并选择“配置虚拟显示器”选项。虚拟显示配置 UI 将启动。



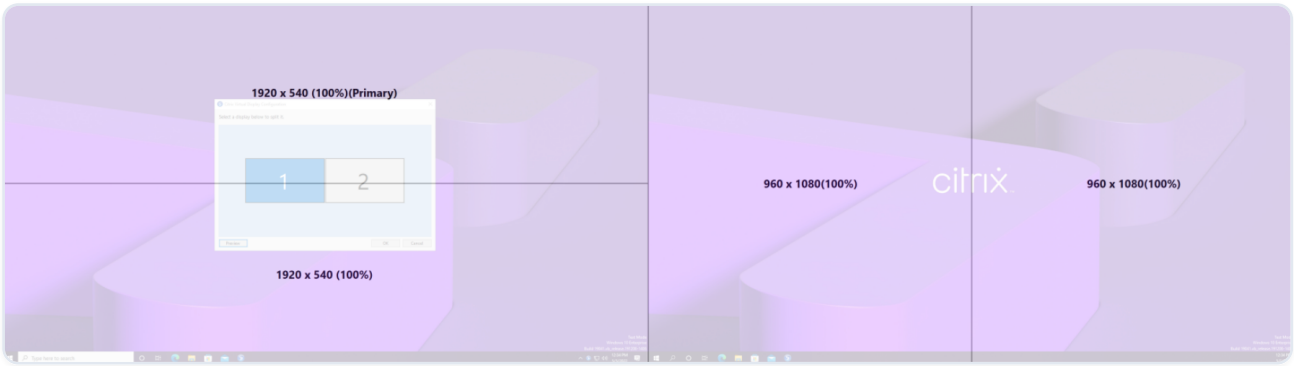
UI 显示当前会话显示布局，蓝色表示会话的主监视器。将鼠标悬停在显示器上时，您可以看到“显示设置”工具提示。该工具提示提供有关在给定会话监视器上定义的当前虚拟显示布局的信息。



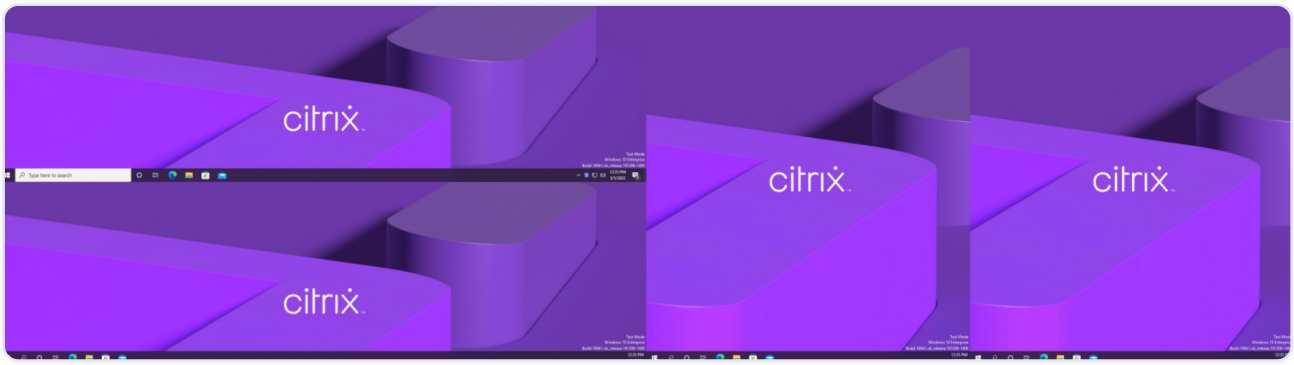
选择一个显示器以切换到交互式 UI，该 UI 允许您为选定的会话监视器配置虚拟显示器。您可以绘制水平或垂直线将屏幕分成虚拟监视器。屏幕根据会话监视器分辨率的指定百分比进行拆分。右键单击虚拟显示器以将其标记为主监视器，并使用 DPI 下拉列表为虚拟显示器设置首选缩放因子。定义虚拟显示布局后，单击 **OK** 暂时保存布局，或单击 **Cancel** 放弃任何更改。您可以使用 **Reset** 撤消配置并恢复会话监视器的原始布局。



要预览当前配置的虚拟显示布局，请单击 **Preview** 按钮。将出现一个窗口，突出显示会话中虚拟显示器的预期位置和分辨率。



单击 **OK** 立即应用并保存虚拟显示布局。单击 **Cancel** 关闭 UI 并放弃所有更改。



其他注意事项

- 所需的最低虚拟显示分辨率为 640 x 480。
- 通过 UI 定义的虚拟显示 DPI 取决于操作系统对给定显示分辨率的缩放支持。
- 请勿将此功能与 Citrix Workspace™ 应用程序中现有的虚拟显示功能同时使用。
- Server 2016 不支持预览功能。

基于文本的水印

基于文本的会话水印有助于阻止和跟踪数据窃取。此可追溯信息以威慑那些使用照片和屏幕截图窃取数据的人，显示在会话桌面上。您可以指定一个文本层水印。

水印可以显示在整个会话屏幕上，而不会改变原始文档的内容。基于文本的会话水印需要 VDA 支持。

> **重要提示：**

> 基于文本的会话水印不是一项安全功能。此解决方案不能完全阻止数据窃取，但它提供了一定程度的威慑和可追溯性。尽管我们不保证在使用此功能时信息完全可追溯，但我们建议您在适用情况下将此功能与其他安全解决方案结合使用。

> 会话水印是文本，并应用于交付给用户的会话。会话水印包含用于跟踪数据窃取的信息。最重要的数据是截取屏幕图像的当前会话的登录用户身份。为了更有效地跟踪数据泄露，请包含其他信息，例如服务器或客户端互联网协议地址以及连接时间。

要调整用户体验，请使用会话水印策略设置 来配置水印在屏幕上的位置和外观。

要求：

虚拟投递代理 (VDA)：

多会话操作系统 7.17 单会话操作系统 7.17

限制：

- 在使用本地应用程序访问、Windows 媒体重定向、MediaStream、浏览器内容重定向和 HTML5 视频重定向的会话中不支持会话水印。要使用会话水印，请确保禁用这些功能。
- 如果会话在全屏硬件加速模式（全屏 H.264 或 H.265 编码）下运行，则不支持会话水印，也不会显示。
- 如果设置了这些 HDX™ 策略，水印设置将不生效，并且会话显示中不会显示水印。

对视频编解码器使用硬件编码设置为**已启用 对压缩使用视频编解码器**设置为**针对整个屏幕**

- 如果设置了这些 HDX 策略，则行为不确定，并且可能不会显示水印。

  对视频编解码器使用硬件编码设置为**已启用 对压缩使用视频编解码器**设置为**在首选时使用视频编解码器**

  为确保显示水印，请将**对视频编解码器使用硬件编码**设置为**已禁用**，或将**对压缩使用视频编解码器**设置为**针对活动更改区域**或**不使用视频编解码器**。
- 会话水印仅支持 Thinwire 图形模式。
- 如果您使用会话录制，则录制的会话不包含水印。
- 如果您使用 Windows 远程协助，则不显示水印。
- 如果用户按下 **Print Screen** 键捕获屏幕，则 VDA 端捕获的屏幕不包含水印。我们建议您采取措施，避免捕获的图像被复制。

Citrix 截图工具在 Assistant 中的集成

概述

Citrix 截图工具允许用户在其 Citrix Virtual Apps and Desktops 会话中无缝捕获覆盖内容和重定向内容的屏幕截图。

传统上，本机会话内屏幕截图工具无法捕获已优化或卸载到客户端端点的内容。由于此媒体是在本地而不是在服务器 (VDA) 上呈现的，因此优化元素（例如 Microsoft Teams 视频或浏览器内容重定向 (BCR) 窗口）在标准屏幕截图中通常显示为纯黑色框或占位符图形。

Citrix 截图工具通过启用所有重定向内容的会话内屏幕截图来弥补这一差距。这可确保为文档、故障排除和协作提供完整准确的捕获，精确捕获用户所看到的会话。

支持的内容

Citrix 截图工具可成功捕获由以下功能优化的内容：

- **浏览器内容重定向 (BCR)：** 捕获卸载的 Web 渲染。有关此功能的详细信息，请参阅浏览器内容重定向文档。
- **HTML5 多媒体重定向：** 捕获优化的 HTML5 视频元素。有关此功能的详细信息，请参阅 HTML5 多媒体重定向文档。
- **Windows 媒体重定向：** 捕获重定向的 Windows 媒体播放。有关此功能的详细信息，请参阅 Windows 媒体重定向文档。
- **统一通信 (UC) 优化：** 捕获 HDX WebRTC / UCSDK 优化应用程序（例如 Microsoft Teams VDI 1.0、Amazon Connect、Five9、Ring Central）和第三方优化应用程序（例如 Microsoft Teams VDI 2.0 (SlimCore)、Zoom 和 Webex）的覆盖视频和 UI 元素。

系统要求

- **虚拟投递代理 (VDA)：** 版本 2607 LTSR 或更高版本。
- **Citrix Workspace 应用程序：** 适用于 Windows 的 Citrix Workspace 应用程序版本 2607 LTSR 或更高版本。
- **支持的端点操作系统：** 仅限 Windows。（注意：目前不支持 macOS、Linux 和 ChromeOS）。

配置

Citrix 截图工具通过 Citrix 策略进行控制。默认情况下，捕获重定向内容的功能处于启用状态。

要配置策略：

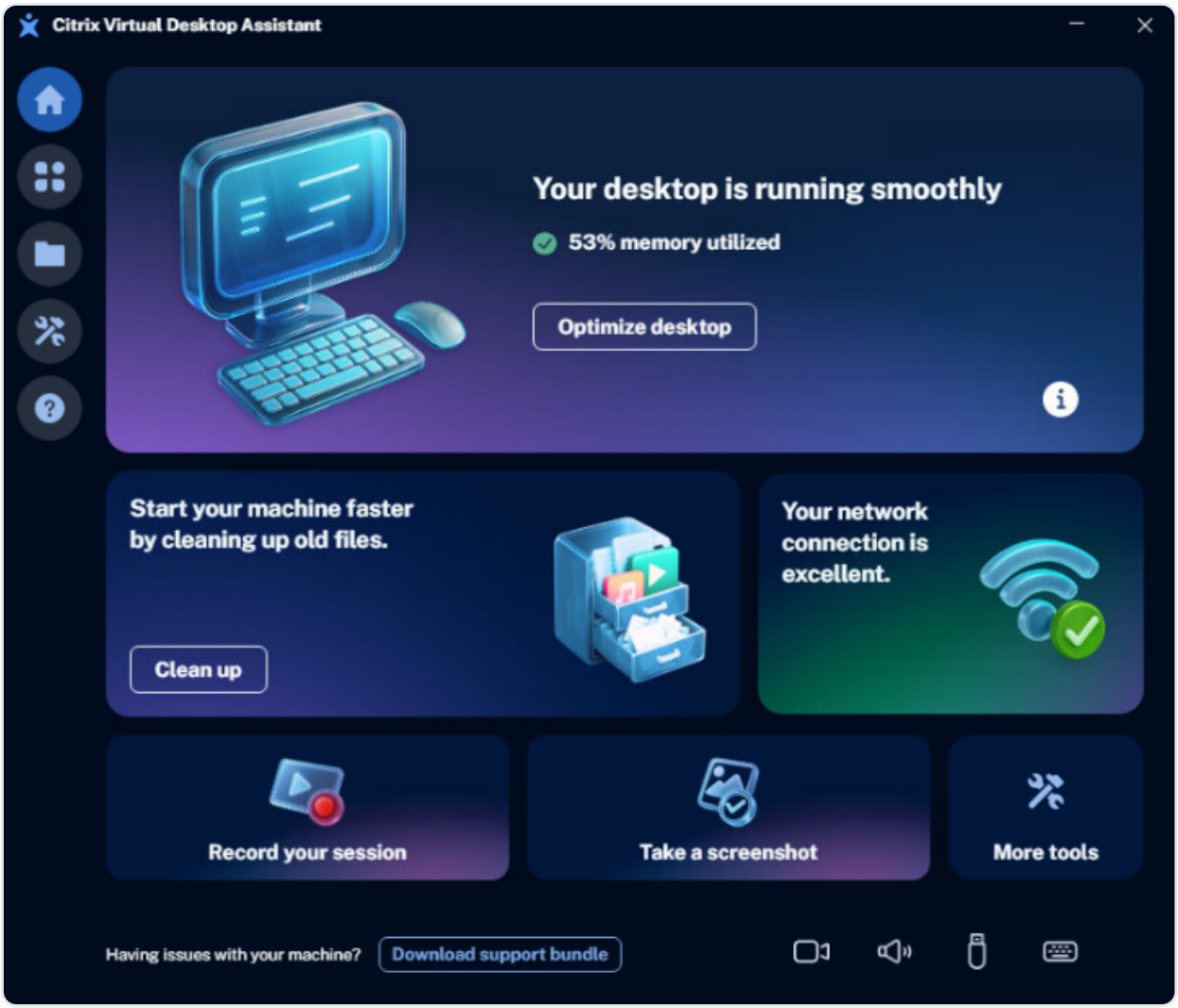
1. 打开 **Citrix Studio（或 Web Studio）** 并导航到策略。
2. 找到 **屏幕截图重定向内容** 策略设置。
3. 选择 **已启用** 以允许用户捕获叠加内容，如果您的环境具有禁止屏幕捕获的严格安全要求，则选择禁用。

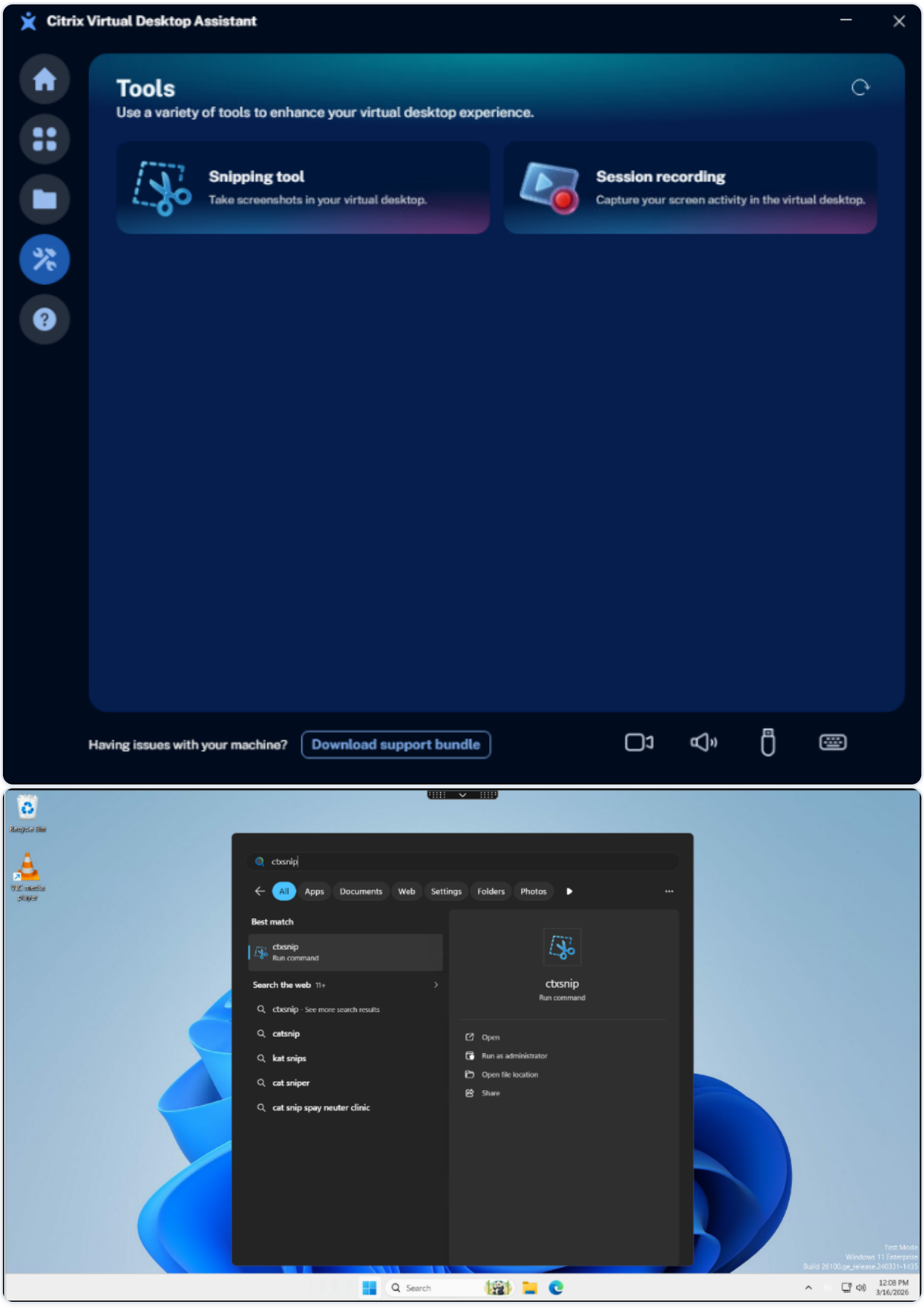
> **注意：**
>
> Citrix 截图工具遵循现有的安全边界。如果 Citrix App Protection 处于活动状态，该工具将自动禁用重定向内容的捕获，以防止数据泄露。有关详细信息，请参阅 App Protection 文档。

用法

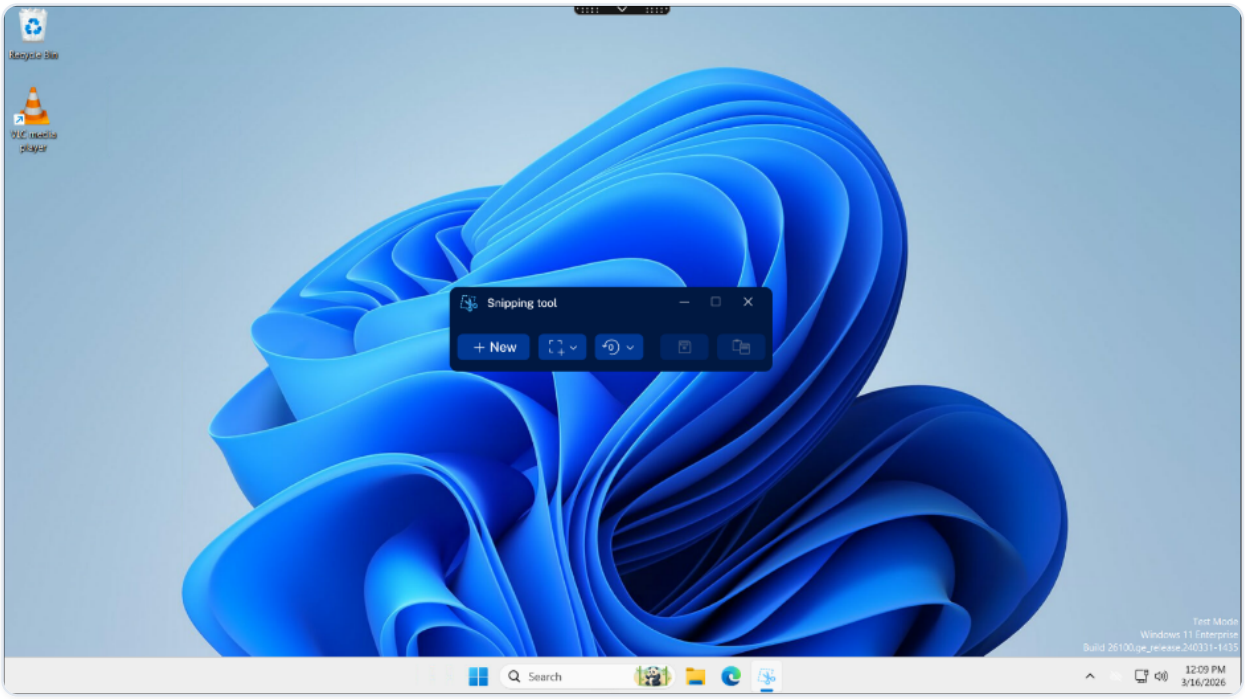
要捕获包含优化或重定向叠加内容的会话内屏幕截图，请按照以下步骤操作：

1. Citrix 建议直接从 Citrix Assistant（主页中的“更多工具”）启动 Citrix 截图工具。有关该应用程序的更多信息，请参阅Citrix Assistant 文档。（或者，您可以在虚拟桌面会话中打开 Windows“开始”菜单以启动 Citrix 截图工具）

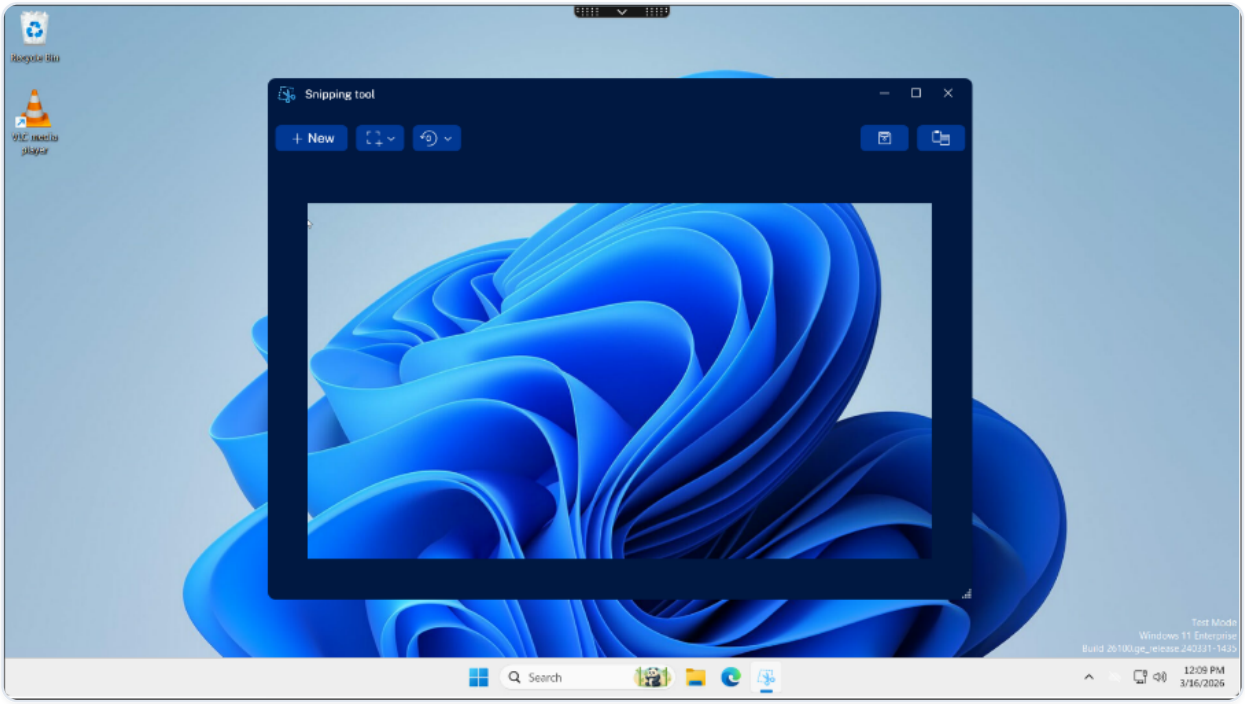

Citrix Virtual Desktop Assistant
Your desktop is running smoothly
53% memory utilized
Optimize desktop
Start your machine faster by cleaning up old files.
Clean up
Your network connection is excellent.
Record your session
Take a screenshot
More tools
Having issues with your machine?
Download support bundle



2. 单击“新建”按钮开始捕获。



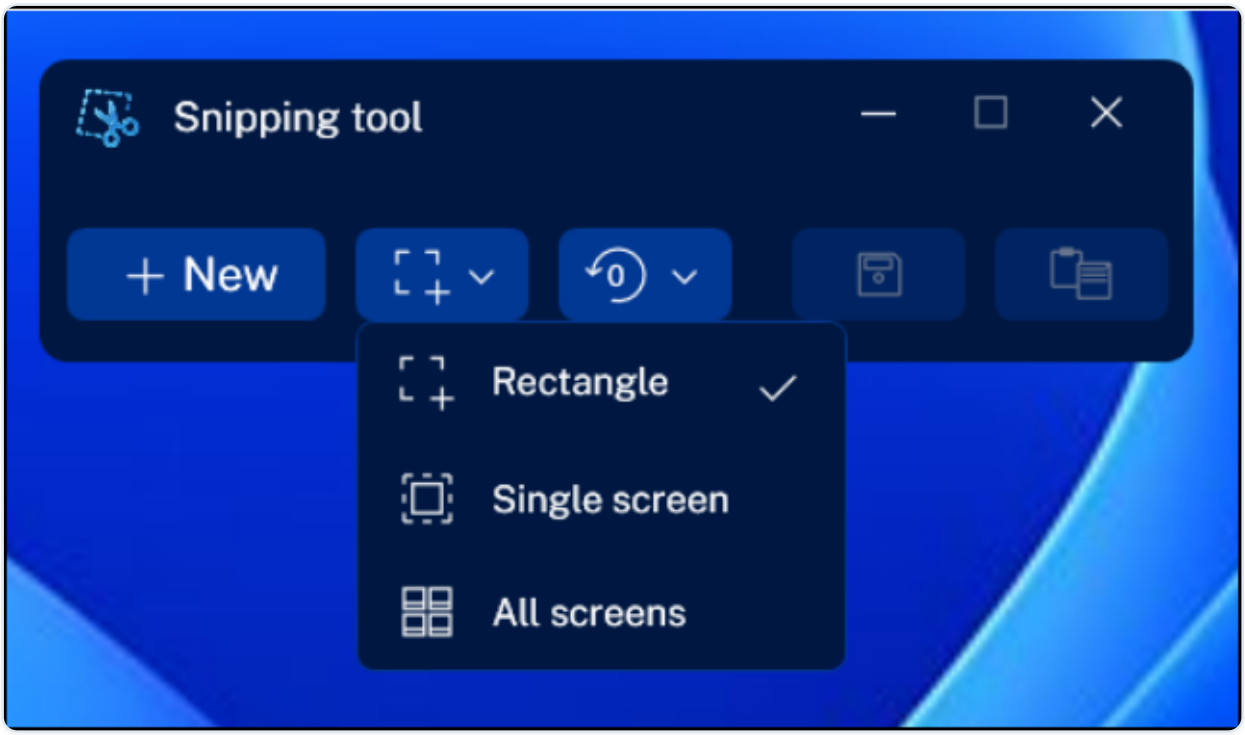
3. 单击并拖动光标以选择要捕获的屏幕特定区域。捕获屏幕截图后，您可以将图像直接复制到剪贴板，或将其保存为 .PNG 或 .BMP 文件。



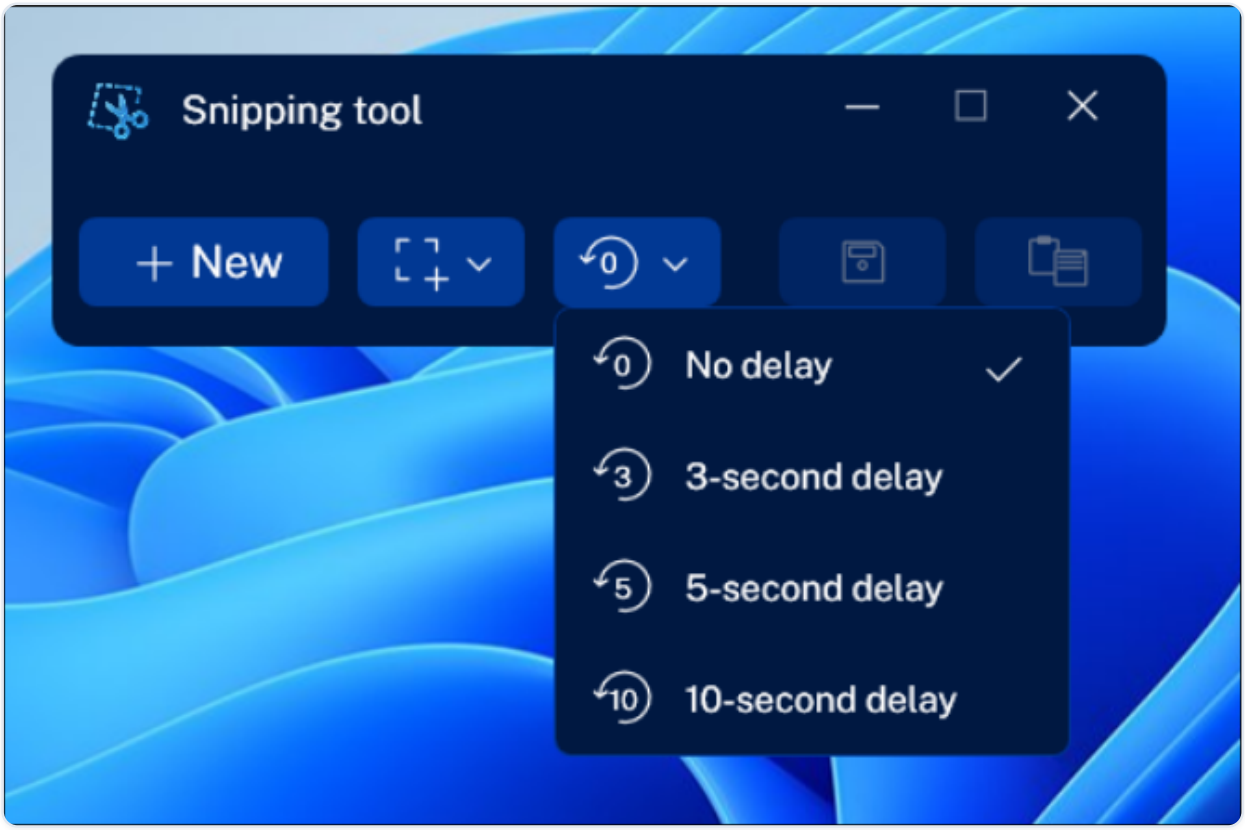
其他选项

Citrix 截图工具包含用于自定义屏幕截图的其他设置：

- **截图区域：** 默认情况下，该工具会捕获屏幕的自定义用户定义区域。您可以更改此模式以捕获整个会话的全屏截图。如果您使用多显示器设置，全屏模式将捕获所有活动屏幕。



- 延迟计时器：为了捕获临时的屏幕元素（例如下拉菜单或悬停状态），请使用“延迟”按钮选择一个倒计时器。该工具将等待指定的时间，然后冻结屏幕并捕获截图。



故障排除

叠加内容未被捕获

- 验证 Citrix Studio 中的“屏幕截图重定向内容”策略已设置为“已启用”。
- 确保您的虚拟投递代理 (VDA) 和 Citrix Workspace 应用程序都满足最低版本要求（2607 LTSR 或更高版本）。
- 检查应用程序保护或其他防屏幕捕获安全策略是否处于活动状态。如果这些安全边界已启用，它们将有意阻止该工具的功能以防止数据泄露。

屏幕截图中持续存在黑条或占位符消息

- 验证您正在主动使用 Citrix 截图工具来捕获屏幕。本机操作系统截图实用程序（例如默认的 Windows 截图工具）和第三方捕获应用程序无法拦截优化的叠加内容，并且仍然会导致黑框。

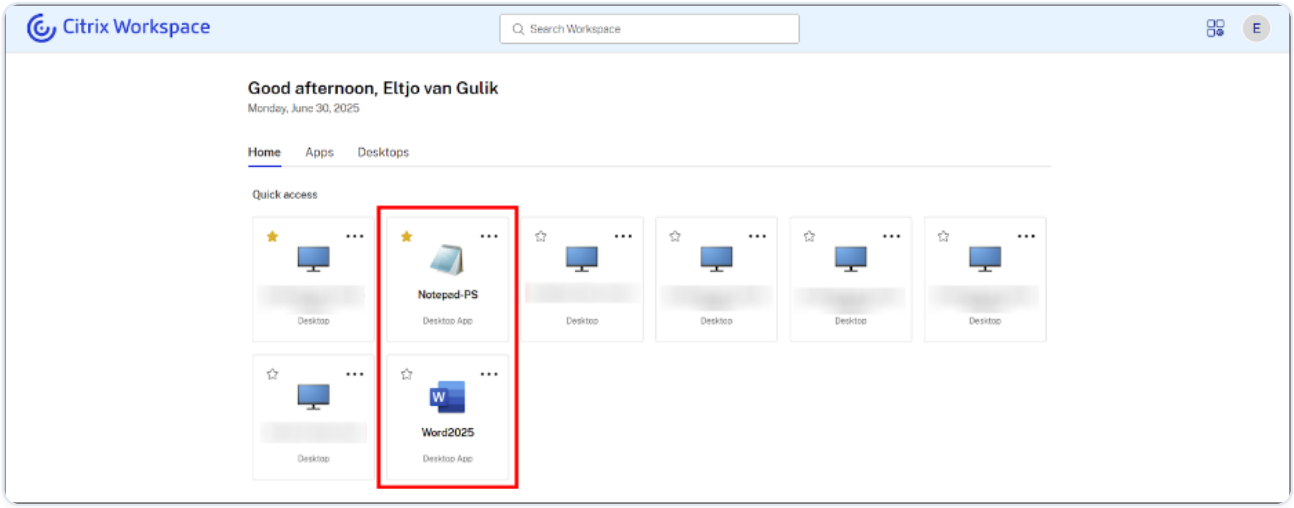
Citrix 截图工具不可用或缺失

- 确保您的虚拟投递代理 (VDA) 已更新到版本 2607 LTSR 或更高版本。该应用程序将不会出现在较旧的 VDA 版本上，也不受其支持。

无缝

Citrix 发布应用程序是 Citrix Virtual Apps and Desktops 的核心功能。它们使客户能够直接向用户交付单个 Windows 或 Linux 应用程序，而无需完整的桌面。

这消除了用户在本地安装和管理应用程序的需要，简化了他们的工作流程，并减轻了 IT 部门的负担。用户无需与完整的远程桌面环境交互，而是直接与应用程序窗口交互，从而创造了无缝且简化的体验。



发布应用程序（也称为无缝应用程序）背后的技术使应用程序能够交付给用户，使其看起来像直接在用户的本地设备上运行，即使它们实际上是在远程服务器上运行。这是通过隐藏托管应用程序的 Windows Server 桌面并将应用程序无缝地呈现给用户来实现的。

无缝应用程序可用于 Windows VDA 和 Linux VDA。对于 Windows VDA，无缝应用程序支持运行 Microsoft Windows Server 操作系统的 TSVDA，以及运行 Microsoft Windows 10 或 Windows 11 的 WSVDA。

无缝应用程序具有诸多优势，包括：

- **改善用户体验：** 用户可以从任何设备访问其应用程序，而无需担心底层操作系统。
- **提高安全性：** 应用程序在远程服务器上运行，这有助于保护它们免受恶意软件和其他威胁。
- **降低 IT 成本：** 无缝应用程序通过简化应用程序管理和部署来帮助降低 IT 成本。
- **集中管理：** 应用程序可以在中央位置进行管理和更新，简化了 IT 管理并确保了整个组织的一致性。这减少了部署补丁、更新和新应用程序所需的时间和精力。

- **应用程序兼容性：** 通过在标准化的服务器环境中运行应用程序，可以缓解因不同客户端操作系统或硬件配置而可能出现的兼容性问题。
- **简化的应用程序交付：** Citrix 利用 HDX™ 等先进技术，即使在带宽有限的连接上，也能为用户提供丰富、交互式的体验，无论是发布桌面还是发布应用程序。
- **异构应用程序支持：** 管理员可以发布 Linux 应用程序和 Windows 应用程序，从而实现从这两个平台无缝访问应用程序。

应用程序

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 唯一的管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

简介

如果您的部署仅使用交付组（而不使用应用程序组），则将应用程序添加到交付组。如果您还有应用程序组，通常会将应用程序添加到应用程序组中。此指导原则可简化管理。应用程序必须始终属于至少一个交付组或应用程序组。

在“添加应用程序”向导中，您可以选择一个或多个交付组，或一个或多个应用程序组，但不能同时选择两者。尽管您以后可以更改应用程序的组关联（例如，将应用程序从应用程序组移动到交付组），但最佳实践不鼓励增加这种复杂性。将您的应用程序保留在一种类型的组中。

当您将应用程序与多个组关联时，如果您没有足够的权限在所有这些组中查看该应用程序，则可能会出现可见性问题。在这种情况下，请咨询具有更高权限的管理员，或者扩展您的范围以包括与该应用程序关联的所有组。

如果您向同一用户发布两个同名应用程序（可能来自不同的组），请在 Web Studio 中更改 `Application name (for user)` 属性。否则，用户将在 Citrix Workspace™ 应用程序中看到重复的名称。

您可以在添加应用程序时或之后更改其属性（设置）。您还可以在添加应用程序时或之后更改应用程序所在的应用程序文件夹。

有关详细信息，请参阅：

- 创建交付组
- 创建应用程序组
- 标签

添加应用程序

您可以在创建交付组或应用程序组时添加应用程序。这些过程在 创建交付组 和 创建应用程序组 中有详细说明。以下过程描述了在创建组后如何添加应用程序。

须知：

- 您无法将应用程序添加到远程 PC 访问交付组。
- 您不能使用“添加应用程序”向导从交付组或应用程序组中删除应用程序。那是一个单独的操作。

要添加一个或多个应用程序：

1. 在左侧窗格中选择 **应用程序**，然后在操作栏中选择 **添加应用程序**。
2. “添加应用程序”向导启动并显示“**简介**”页面，您可以从该向导的未来启动中删除此页面。
3. 该向导将引导您完成“**组**”、“**应用程序**”和“**摘要**”页面。完成每个页面后，单击“**下一步**”，直到到达“**摘要**”页面。

如果您想将应用程序添加到单个交付组或应用程序组，可采用以下步骤 1 的替代方法：

- **仅向一个交付组添加应用程序：** 在步骤 1 中，在 Web Studio 左侧窗格中选择 **交付组**，在中间窗格中选择一个交付组，然后在操作栏中选择 **添加应用程序**。该向导不显示“**组**”页面。
- **仅向一个应用程序组添加应用程序：** 在步骤 1 中，在 Web Studio 左侧窗格中选择 **应用程序**，在中间窗格中选择一个应用程序组，然后在操作栏中应用程序组名称下选择 **添加应用程序** 条目。该向导不显示“**组**”页面。

组页面

此页面列出了站点中的所有交付组。如果您还创建了应用程序组，则此页面会列出应用程序组和交付组。您可以从任一组中选择，但不能同时从两个组中选择。换句话说，您不能同时将应用程序添加到应用程序组和交付组。通常，如果您正在使用应用程序组，请将应用程序添加到应用程序组，而不是交付组。

添加应用程序时，选中至少一个交付组（如果可用，则为应用程序组）旁边的复选框。每个应用程序都必须始终与至少一个组关联。

应用程序页面

单击“**添加**”以显示应用程序源。

- **从“开始”菜单：** 在所选交付组中的计算机上发现的应用程序。当您选择此源时，将启动一个新页面，其中包含发现的应用程序列表。选中要添加的应用程序的复选框，然后单击“**确定**”。

  如果您出现以下情况，则无法选择此源：(1) 选择了没有关联交付组的应用程序组，(2) 选择了具有关联交付组但这些交付组不包含任何计算机的应用程序组，或者 (3) 选择了不包含任何计算机的交付组。

- **手动：** 位于交付组中的 VDA 上或网络中其他位置的应用程序。选择此源将打开一个新页面，您可以在其中通过以下方式指定要添加的应用程序：

  - 键入可执行文件的路径、工作目录、可选命令行参数以及供管理员和用户使用的显示名称。
  - 从交付组中的 VDA 选择一个应用程序。为此，请单击“**浏览**”，输入用于访问 VDA 的凭据，等待连接到 VDA，然后从 VDA 中选择一个应用程序。所选应用程序的属性会自动填充页面上的字段。

- **现有：** 以前添加到站点的应用程序。选择此源时，将启动一个新页面，其中包含发现的应用程序列表。选中要添加的应用程序的复选框，然后单击“**确定**”。

  如果站点没有应用程序，则无法选择此源。

- **应用程序包：** App-V、MSIX、MSIX app attach 或 FlexApp 应用程序包中的应用程序。选择此源时，将启动“**从包中添加应用程序**”页面。选择一个应用程序包源，从结果显示中选择要添加的应用程序，然后选择“**确定**”。有关详细信息，请参阅部署和交付应用程序包。

- **应用程序组**：应用程序组。选择此源时，将启动一个新页面，其中包含应用程序组列表。（尽管显示内容也列出了每个组中的应用程序，但您只能选择组，而不能选择单个应用程序。）所选组中的所有当前和未来应用程序都将添加。选中要添加的应用程序组的复选框，然后单击“**确定**”。

  如果 (1) 没有应用程序组，或者 (2) 所选交付组不支持应用程序组（例如，具有静态分配计算机的交付组），则无法选择此源。

如表中所示，如果不存在该类型的有效源，则无法选择“**添加**”列表中的某些源。不兼容的源（例如，不能将应用程序组添加到应用程序组）不包括在列表中。已添加到您所选组的应用程序无法选择。

您可以从此页面或以后更改应用程序的属性（设置）。

默认情况下，添加的应用程序放置在名为 `Applications` 的应用程序文件夹中。您可以从此页面或以后更改应用程序。如果您尝试添加一个应用程序，并且同一文件夹中已存在同名应用程序，系统会提示您重命名要添加的应用程序。您可以接受提供的新名称，也可以拒绝，然后重命名应用程序或选择其他文件夹。例如，如果 `app` 已存在于“**应用程序**”文件夹中，并且您尝试将另一个名为 `app` 的应用程序添加到该文件夹，则会提供新名称 `app_1`。

摘要页面

如果您要添加 10 个或更少的应用程序，其名称将列在“**要添加的应用程序**”中。如果您要添加 10 个以上的应用程序，则会指定总数。

查看摘要信息，然后单击**完成**。

更改应用程序的组关联

添加应用程序后，您可以更改应用程序所关联的交付组和应用程序组。

您可以将应用程序拖动到其他组。这是使用操作栏中命令的替代方法。

如果应用程序与多个交付组关联（无论是使用应用程序组还是直接关联），则可以使用组优先级来指定评估多个组的顺序。可以根据访问策略、用户列表或智能访问标签等因素将组排除在考虑范围之外，并且从组中选择的特定计算机可能会受到区域首选项、启动就绪状态以及任何标签限制等因素的影响。默认情况下，所有组的优先级均为 0（最高）。如果交付组具有相同的优先级，则选择负载最低的交付组来启动应用程序。在这种情况下不考虑垂直负载平衡。

应用程序可以与包含可交付应用程序的共享（非专用）计算机的交付组关联。如果 (1) 交付组包含共享计算机且是使用早于 7.9 的 XenDesktop 7.x 版本创建的，并且 (2) 您具有 `Edit delivery group` 权限，则您还可以选择包含仅交付桌面的共享计算机的交付组。提交属性对话框时，交付组类型会自动转换为 `desktops and applications`。

1. 登录 Web Studio，在左侧窗格中选择“**应用程序**”，然后选择该应用程序。
2. 在操作栏中选择**属性**。
3. 选择**组**页面。
    - 要添加组，请单击**添加**，然后选择**应用程序组**或**交付组**。（如果您尚未创建任何应用程序组，则唯一条目是**交付组**。）然后选择一个或多个可用组。与应用程序不兼容或已与应用程序关联的组无法选择。
    - 要删除组，请选择一个或多个组，然后单击**删除**。如果删除组关联将导致应用程序不再与任何组关联，则会收到应用程序将被删除的警报。
    - 要更改组的优先级，请选择该组，然后单击**编辑优先级**。选择一个优先级值，然后单击**确定**。
4. 完成后，单击**应用**以应用更改并保持窗口打开，或单击**确定**以应用更改并关闭窗口。

复制、启用或禁用、重命名或删除应用程序

可执行以下操作：

- **复制：** 您可能希望复制应用程序以创建具有不同参数或属性的不同版本。复制应用程序时，它会自动使用唯一的后缀重命名并放置在原始应用程序旁边。您可能还希望复制应用程序，然后将其添加到不同的组。（复制后，移动应用程序最简单的方法是拖动它。）
- **启用或禁用：** 启用和禁用应用程序与启用和禁用交付组或应用程序组是不同的操作。
- **重命名：** 您一次只能重命名一个应用程序。如果您尝试重命名应用程序，并且同一文件夹或组中存在同名应用程序，系统会提示您指定其他名称。
- **删除：** 删除应用程序会将其从与之关联的交付组和应用程序组中删除，但不会从最初用于添加应用程序的源中删除。删除应用程序与从交付组或应用程序组中删除应用程序是不同的操作。

要复制、启用、禁用、重命名或删除应用程序：

1. 在左窗格中选择**应用程序**。
2. 在中间窗格中选择一个或多个应用程序，然后在操作栏中选择相应的任务。
3. 出现提示时，确认操作。

从交付组中删除应用程序

应用程序必须至少与一个交付组或应用程序组关联（属于）。如果您尝试从交付组中删除某个应用程序，而此操作将移除该应用程序与任何交付组或应用程序组的关联，系统会通知您如果继续，该应用程序将被删除。发生这种情况时，如果您想交付该应用程序，则必须从有效源再次添加它。

1. 在左窗格中选择**交付组**。
2. 选择一个交付组。在中间下部窗格的**应用程序**选项卡上，选择要删除的应用程序。
3. 从操作栏中选择**删除应用程序**。
4. 确认删除。

从应用程序组中删除应用程序

应用程序必须至少属于一个交付组或应用程序组。如果您尝试从应用程序组中删除某个应用程序，而此操作将导致该应用程序不再属于任何组，系统会通知您如果继续，该应用程序将被删除。发生这种情况时，如果您想交付该应用程序，则必须从有效源再次添加它。

1. 在左窗格中选择**应用程序**。
2. 在中间窗格中选择应用程序组，然后选择一个或多个应用程序。
3. 在操作栏中选择**从应用程序组中删除**。
4. 确认删除。

更改应用程序属性

您一次只能更改一个应用程序的属性。

要更改应用程序的属性：

1. 在左侧窗格中选择“**应用程序**”。
2. 选择一个应用程序，然后在操作栏中选择“**编辑应用程序属性**”。
3. 选择包含要更改的属性的页面。
4. 完成后，单击“**应用**”以应用所做的任何更改并保持窗口打开，或者单击“**确定**”以应用更改并关闭窗口。

在以下列表中，页面显示在括号中。

属性	页面
应用程序在 Citrix Workspace 应用程序中显示的类别/文件夹	交付
命令行参数；请参阅向已发布的应用程序传递参数	位置
应用程序可用的交付组和应用程序组	组
描述	标识
文件名扩展名和文件类型关联：应用程序自动打开哪些扩展名	文件类型关联
图标	交付
StoreFront™ 关键字	标识
限制；请参阅 配置应用程序限制	交付
名称：用户和管理员看到的名称	标识
可执行文件路径；请参阅 向已发布的应用程序传递参数	位置
用户桌面上的快捷方式：启用或禁用	交付

属性	页面
可见性：限制哪些用户可以在 Citrix Workspace 应用程序中看到该应用程序。不可见的应用程序仍然可以启动。要使其不可用且不可见，请将其添加到其他组。	限制可见性
工作目录	位置

应用程序更改可能不会对当前应用程序用户生效，直到他们从会话中注销。

配置应用程序限制

配置应用程序限制以帮助管理应用程序使用。例如，您可以使用应用程序限制来管理同时访问应用程序的用户数量。同样，应用程序限制可用于管理资源密集型应用程序的并发实例数量。该限制有助于维持服务器性能并防止服务质量下降。

此功能限制由 Controller 代理的应用程序启动次数（例如，从 Citrix Workspace 应用程序和 StoreFront 启动），而不是通过其他方法启动的正在运行的应用程序的数量。这意味着应用程序限制有助于管理员管理并发使用，但不能在所有场景中提供强制执行。例如，当 Controller 处于中断模式时，无法应用应用程序限制。

默认情况下，同时运行的应用程序实例数量没有限制。有多种应用程序限制设置。您可以配置其中任何一个或所有设置。

- 交付组中所有用户可同时运行的应用程序最大实例数。
- 交付组中每个用户一个应用程序实例。
- 每台计算机可同时运行的应用程序最大实例数（仅限 PowerShell）。

如果配置了限制，当用户尝试启动的应用程序实例将超出配置的限制时，会生成错误消息。如果配置了多个限制，则在达到第一个限制时报告错误。

使用应用程序限制的示例：

- **最大并发实例数限制：** 在交付组中，您将应用程序 `Alpha` 的最大并发实例数配置为 15。之后，该交付组中的用户同时运行 15 个该应用程序的实例。如果该交付组中的任何用户现在尝试启动 `Alpha`，则会生成错误消息。`Alpha` 未启动，因为它将超出配置的并发应用程序实例限制 (15)。
- **每个用户一个实例的应用程序限制：** 在另一个交付组中，您为应用程序 `Beta` 启用了每个用户一个实例的选项。用户 Tony 成功启动了应用程序 `Beta`。当天晚些时候，当该应用程序仍在

Tony 的会话中运行时，他尝试启动 `Beta` 的另一个实例。生成错误消息，并且 `Beta` 未启动，因为它将超出每个用户一个实例的限制。

- **最大并发实例数和每个用户一个实例的限制：** 在另一个交付组中，您将最大并发实例数配置为 10，并为应用程序 `Delta` 启用了每个用户一个实例的选项。之后，当该交付组中的 10 个用户各自运行一个 `Delta` 实例时，该交付组中任何其他尝试启动 `Delta` 的用户都将收到错误消息。`Delta` 未启动。如果当前 10 个 `Delta` 用户中的任何一个尝试启动该应用程序的第二个实例，他们将收到错误消息，并且第二个实例将不会启动。
- **每台计算机的最大并发实例数以及使用标记限制：** 应用程序 `Charlie` 具有许可和性能要求，这些要求决定了特定服务器上可以同时运行多少个实例。这些要求还决定了站点中所有服务器上可以同时运行多少个实例。

  应用程序每台计算机实例数限制会影响站点中的任何服务器（不仅仅是特定交付组中的计算机）。假设您的站点有三台服务器。对于应用程序 `Charlie`，您将每台计算机的应用程序实例数限制配置为 2。因此，站点范围内最多允许启动六个应用程序 `Charlie` 实例。（这是三台服务器上每台服务器两个 Charlie 实例的限制。）

  要将应用程序的使用限制为交付组中的特定计算机（除了限制站点中所有计算机上的实例之外）：

  - 为这些计算机使用标记功能。
  - 为该应用程序配置每台计算机的最大实例数限制。

如果应用程序通过控制器代理以外的方法启动（例如，当控制器处于中断模式时），并且超出了配置的限制，则用户无法启动更多实例，直到他们关闭足够的实例以不再超出限制。超出限制的实例不会被强制关闭。它们将被允许继续运行，直到其用户将其关闭。

如果禁用会话漫游，则禁用每个用户一个实例的应用程序限制。如果启用每个用户一个实例的应用程序限制，请勿配置允许在新设备上创建新会话的两个值中的任何一个。有关漫游的信息，请参阅会话。

要配置每个交付组的最大实例数限制以及每个用户一个实例的限制，请执行以下操作：

1. 在左侧窗格中选择 **应用程序**，然后选择一个应用程序。
2. 在操作栏中选择 **编辑应用程序属性**。
3. 在 **交付** 页面上，选择以下选项之一。

   - **允许无限制使用应用程序**。同时运行的实例数量没有限制。这是默认设置。
   - **设置应用程序限制**。有两种限制类型；请指定其中一种或两种。

     - 指定每台计算机可同时运行的最大实例数

- 将每个用户限制为一个应用程序实例

4. 单击 **确定** 以应用更改并关闭对话框，或单击 **应用** 以应用更改并保持对话框打开。

要配置每台计算机的最大实例数限制（仅限 PowerShell）：

- 在 PowerShell 中（对于 Citrix Cloud™ 部署，使用远程 PowerShell SDK；对于本地部署，使用 PowerShell SDK），输入相应的 `BrokerApplication` cmdlet 并附带 `MaxPerMachineInstances` 参数。
- 有关指导，请使用 `Get-Help` cmdlet。例如：

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

将参数传递给已发布的应用程序

使用应用程序属性的**位置**页面输入命令行并将参数传递给已发布的应用程序。

当您将已发布的应用程序与文件类型关联时，符号 `"%*"`（用双引号括起来的百分号和星号）将附加到应用程序命令行的末尾。这些符号用作传递给用户设备的参数的占位符。

如果已发布的应用程序未按预期启动，请验证其命令行是否包含正确的符号。默认情况下，当附加符号 `"%*"` 时，将验证用户设备提供的参数。对于使用用户设备提供的自定义参数的已发布的应用程序，符号 `"%**"` 将附加到命令行以绕过命令行验证。如果应用程序的命令行中没有这些符号，请手动添加它们。

如果可执行文件的路径包含带空格的目录名称（例如 `"C:\Program Files"`），请用双引号将应用程序的命令行括起来，以指示空格属于命令行。为此，请在路径周围添加双引号，并在 `%*` 符号周围添加另一组双引号。请务必在路径的结束引号和 `%*` 符号的开始引号之间包含一个空格。

例如，已发布的应用程序 Windows Media Player 的命令行是：

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **注意：**
>
> 用于启动已发布的应用程序的命令行中的最大字符数（包括参数）为 203。

排查已发布的应用程序的会话注销问题

发布应用程序时，仅指定已发布的应用程序的主可执行文件。但是，某些应用程序可能会生成在后台运行的额外（子）进程，并且当主已发布的应用程序关闭时，这些进程不会被相应的主可执行文件关闭。额外进程也可能由执行的脚本或特定的注册表项（例如 `Run` 和 `RunOnceKey`）创建。这些应用程序可能会阻止正常注销，导致会话残留或挂起，并可能导致会话无法关闭且用户无法注销。

在这种情况下，您需要使用 Citrix Director 重置或退出这些会话。

为了帮助识别和排查会话未正确注销的问题，Citrix 提供了三个注册表项。识别和排查由于这些问题导致会话未正确注销是一个三步过程：

1. 识别哪些会话的已发布的应用程序正在阻止正常注销
2. 识别这些已发布的应用程序是否生成任何额外（子）进程
3. 将这些进程添加到指定的注册表项以防止它们阻止注销

步骤 2：识别这些已发布的应用程序是否会生成任何额外的（子）进程

一旦确定某个已发布的应用程序会阻止正常注销，下一步就是确定该应用程序在运行时是否会生成额外的进程。

您可以阅读 `HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` 以确定当已发布的应用程序关闭时，是否有任何进程正在阻止正常注销。

在以下示例中，密钥 `LogoffCheckerBlockingProcess` 包含以下条目：

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

这些进程阻止了正常注销。

> **注意：**

> 将 替换为您要检查的会话的正确会话 ID。

步骤 3：将这些进程添加到指定的注册表项中，以防止它们阻止注销

您可以将这些进程添加到以下注册表项中，以防止它们在未来的会话中阻止注销：

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules

Type:REG_SZ

String:MyAppName.exe
```

有关 `LogoffCheckSysModules` 的更多信息，请参阅 从已发布的应用程序正常注销使会话处于活动状态。

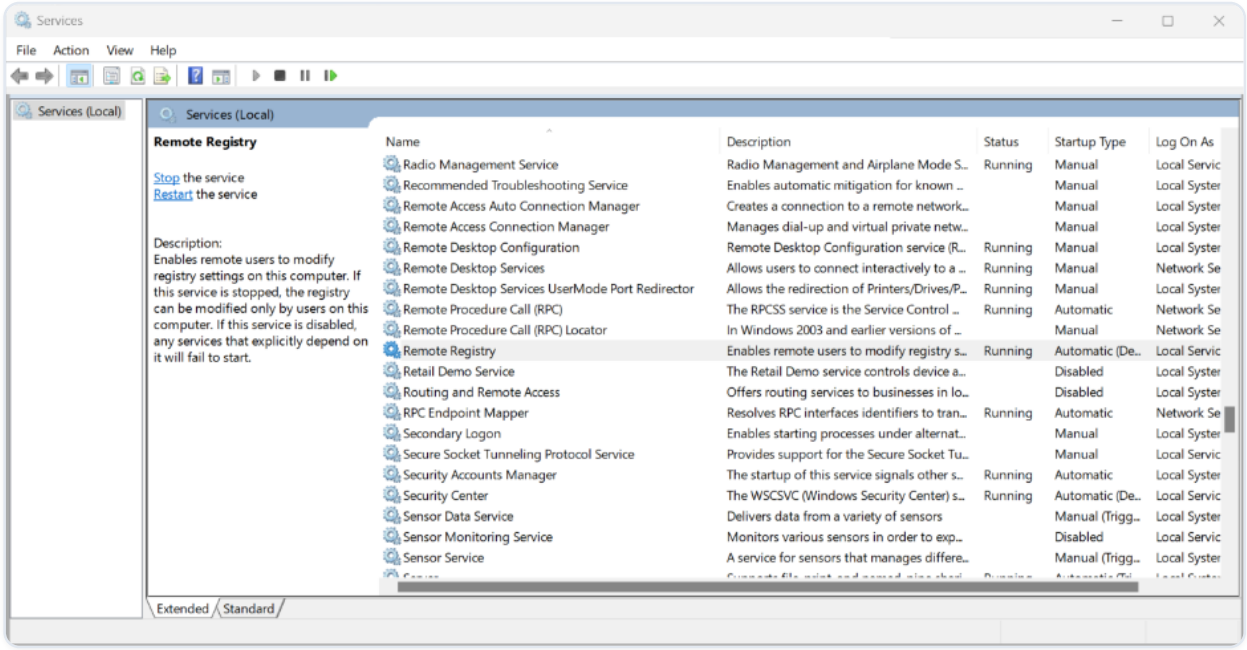
分步故障排除指南

1. 在测试中的 VDA 下启动远程注册表服务：

   a. 在“控制面板”中，选择 **“管理工具”>“服务”**。

   b. 右键单击 **“远程注册表服务”**，然后选择 **“属性”**。

   c. 在 **“启动类型”** 下，从下拉菜单中选择 **“自动”**。



2. 在测试 VDA 上关闭 Windows 防火墙，或者创建入站防火墙规则以启用端口 455：

   a. 在“控制面板”中，选择 **Windows Defender 防火墙 > 高级设置**。

   b. 右键单击**入站规则**，然后选择**新建规则**。

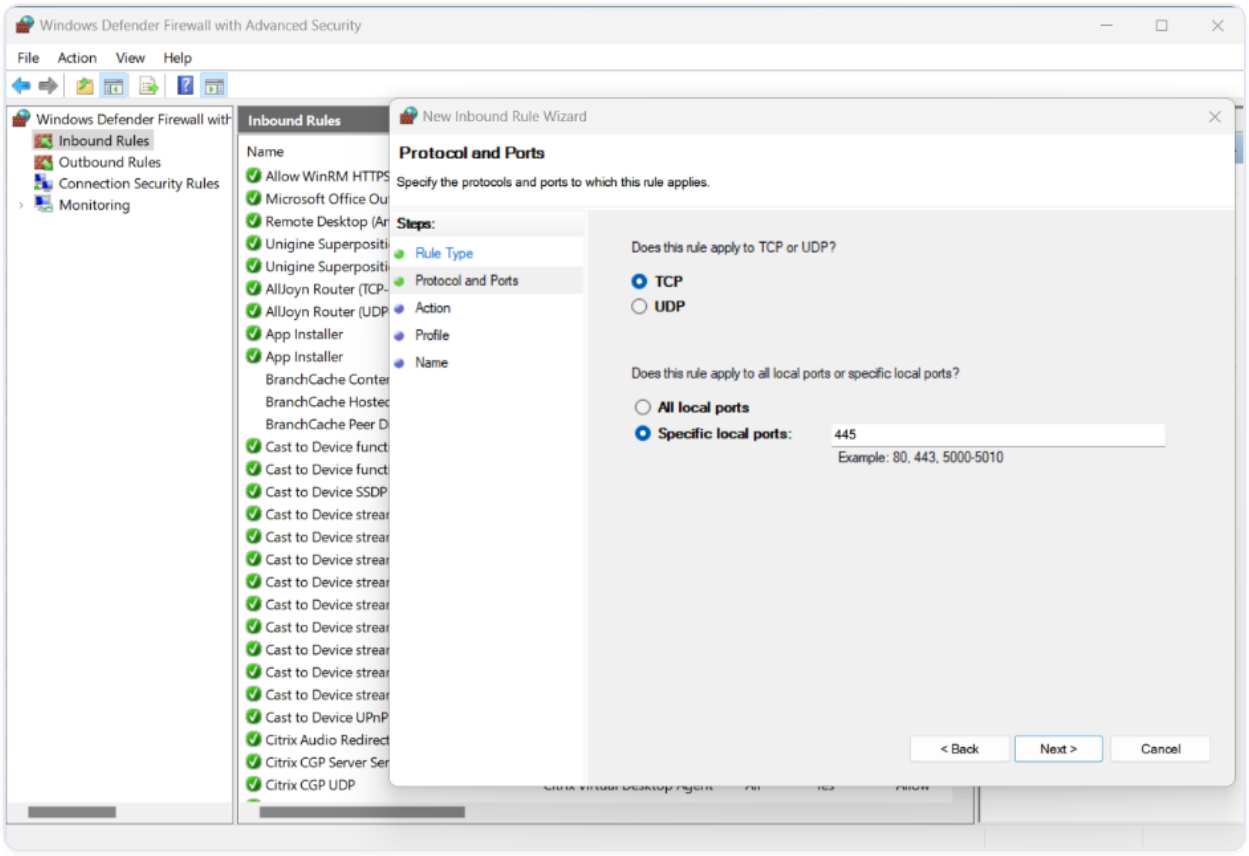
   c. 在**新建入站规则向导**中，选择**端口**。

   d. 在**协议和端口**页面上，选择 **TCP 和特定本地端口**。输入 `445` 作为本地端口。

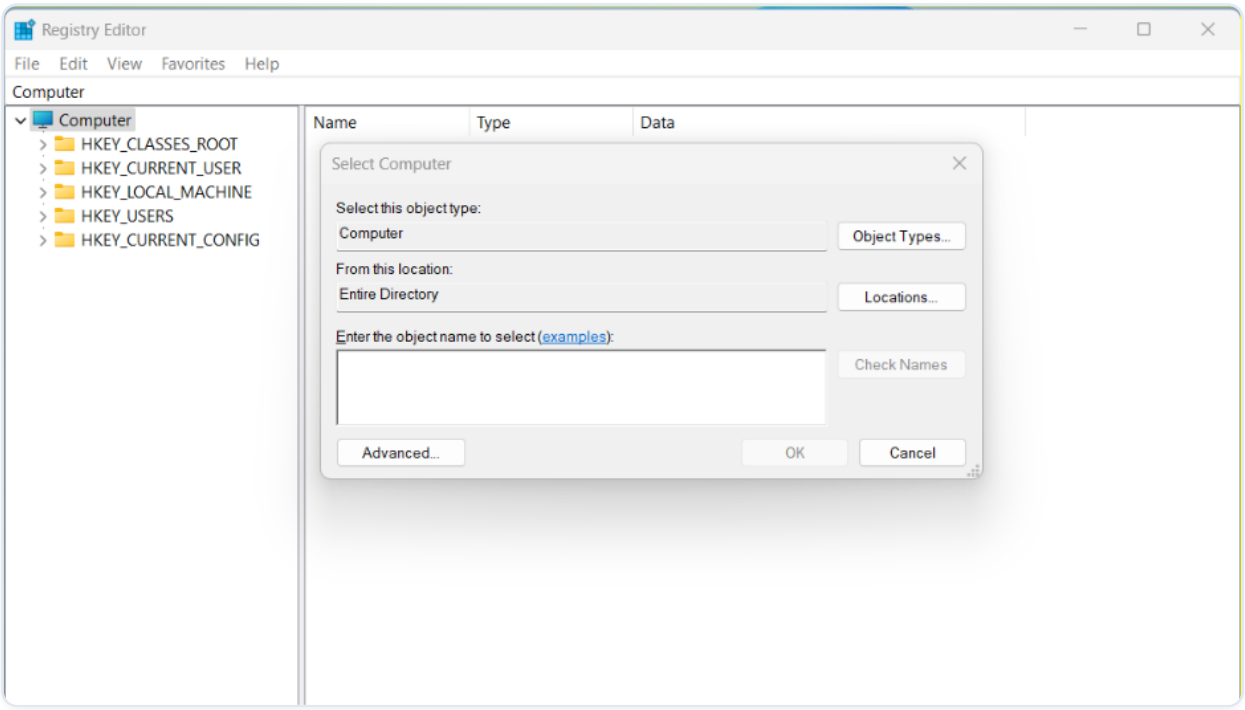
   e. 在**操作**页面上，选择**允许连接**。

   f. 选择要应用新入站规则的防火墙配置文件。

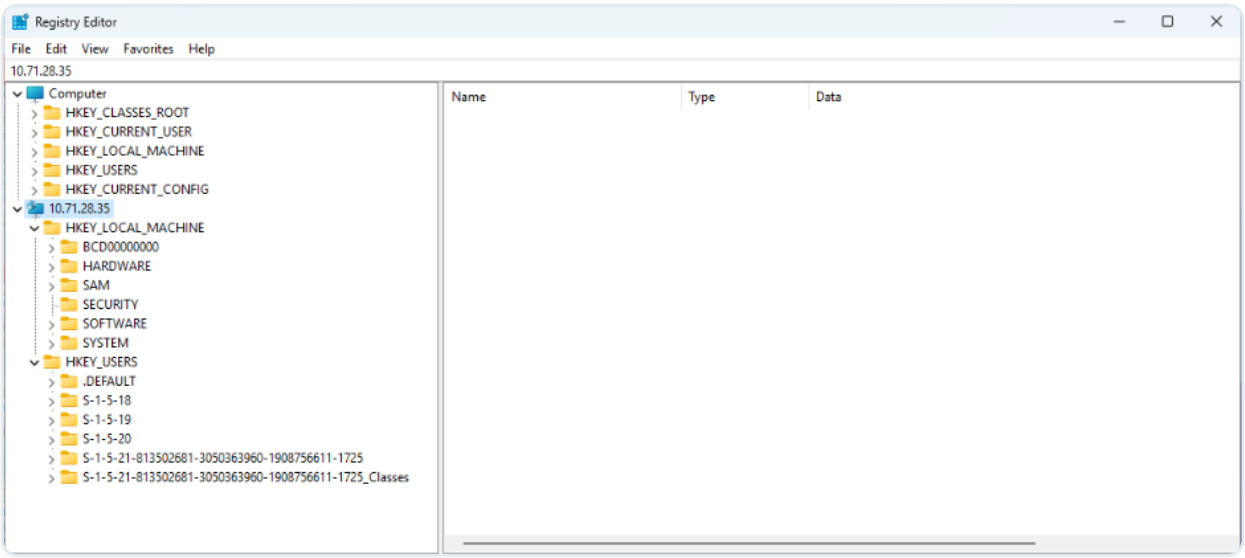
   g. 命名防火墙规则，然后选择**完成**以退出**新建入站规则向导**。



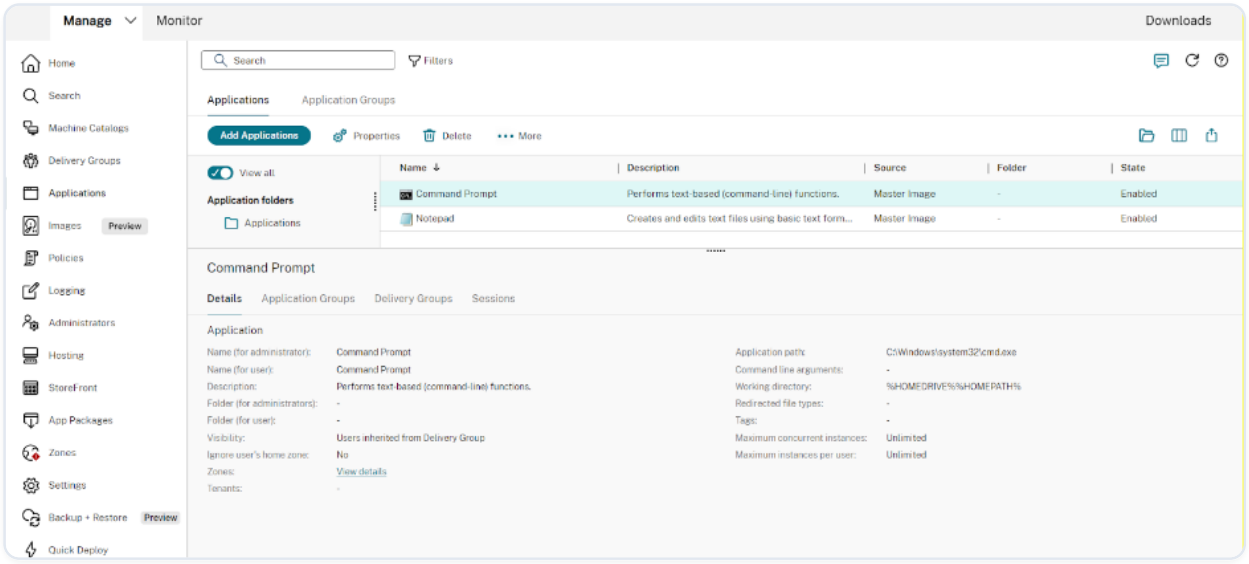
3. 从同一域中的另一台 VM（可以是 DC、DDC 或其他 VDA）运行 `Regedit` 并连接到远程注册表。



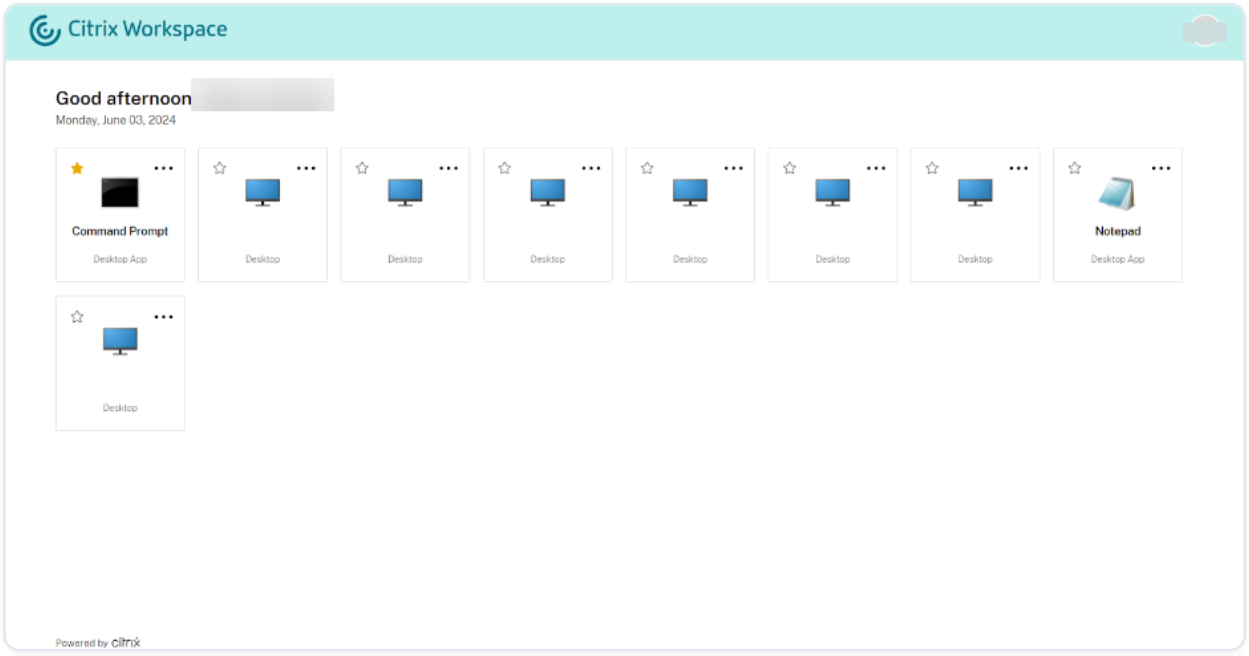
4. 输入测试 VDA 的 IP 地址，然后单击**确定**。`regedit` 树必须显示测试 VDA 的分支。



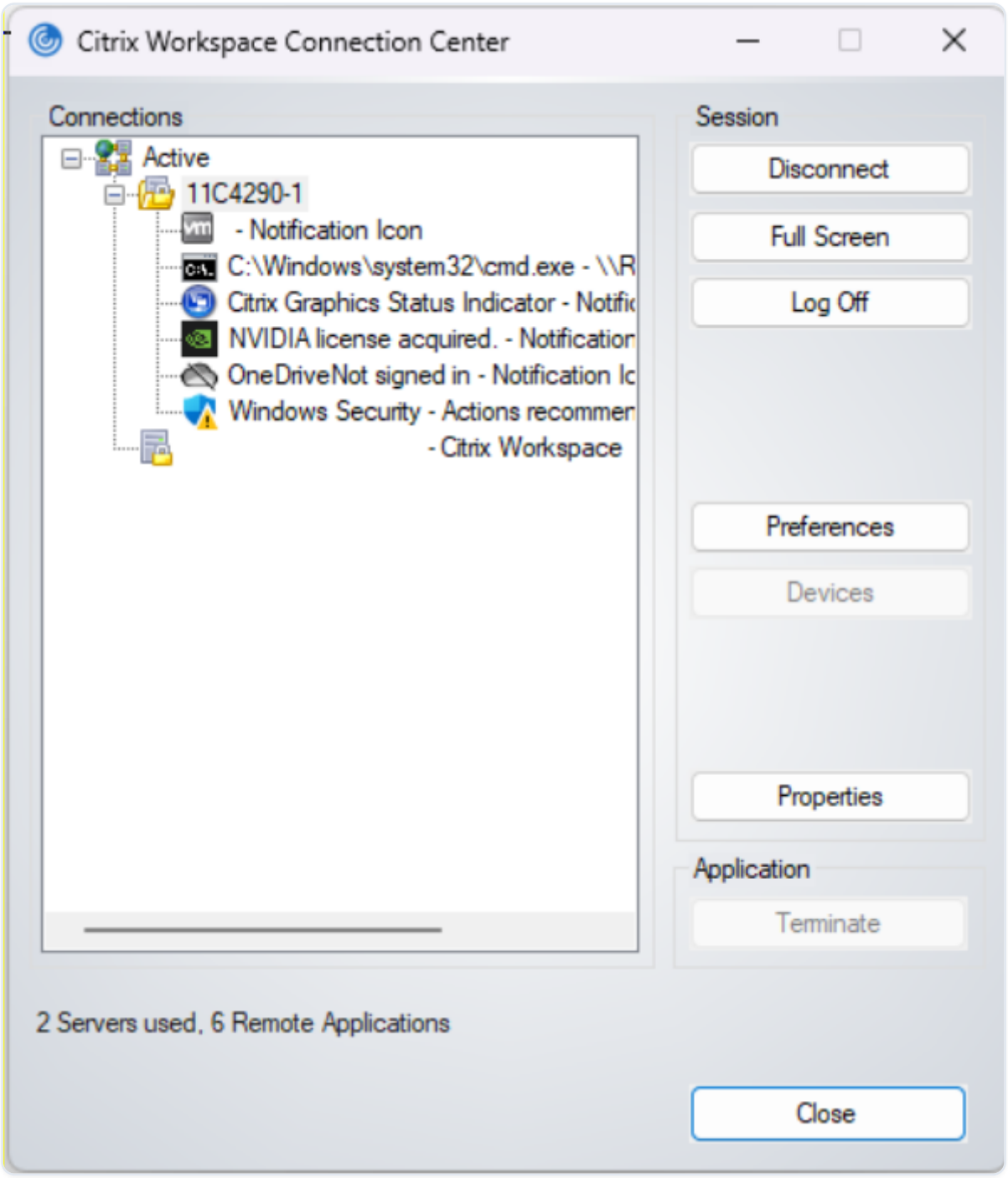
5. 打开**命令提示符**已发布的应用程序。



Citrix Workspace 上显示了**命令提示符**应用程序。



6. 在客户端上打开**连接中心**。这用于在关闭已打开的无缝应用程序后，监控会话何时注销。我们可以从下图中看到，命令提示符进程 `c:\Windows\system32\cmd.exe` 在远程 VDI 上处于活动状态。

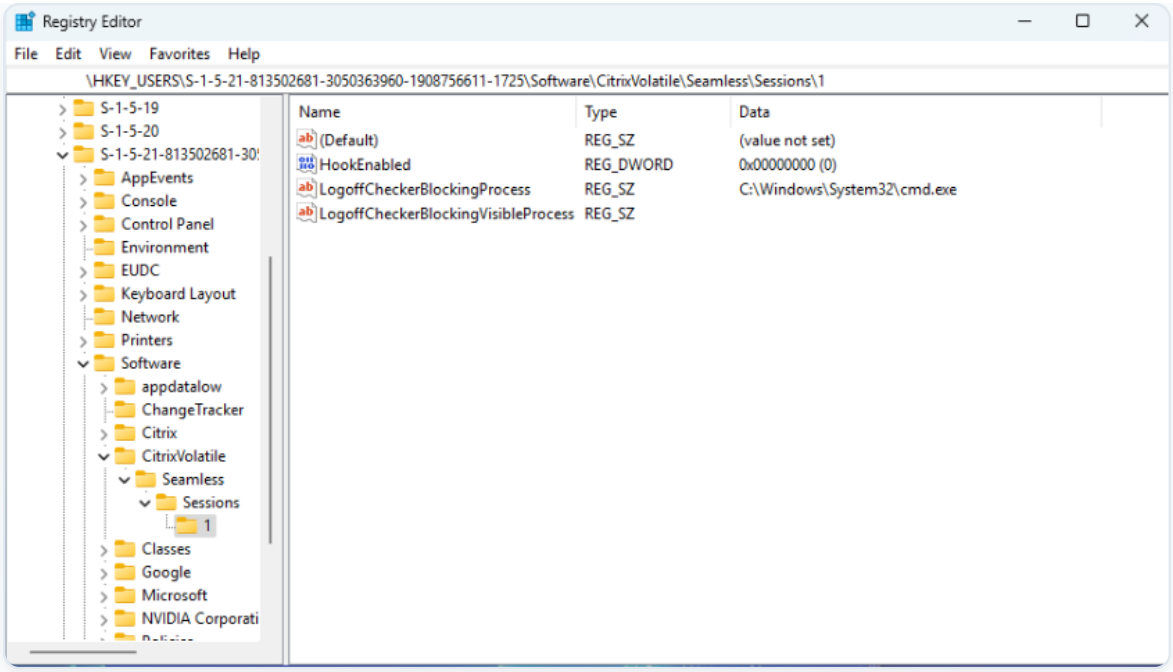


7. 从运行 **regedit** 的 VDA，转到以下远程 IP 位置： `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

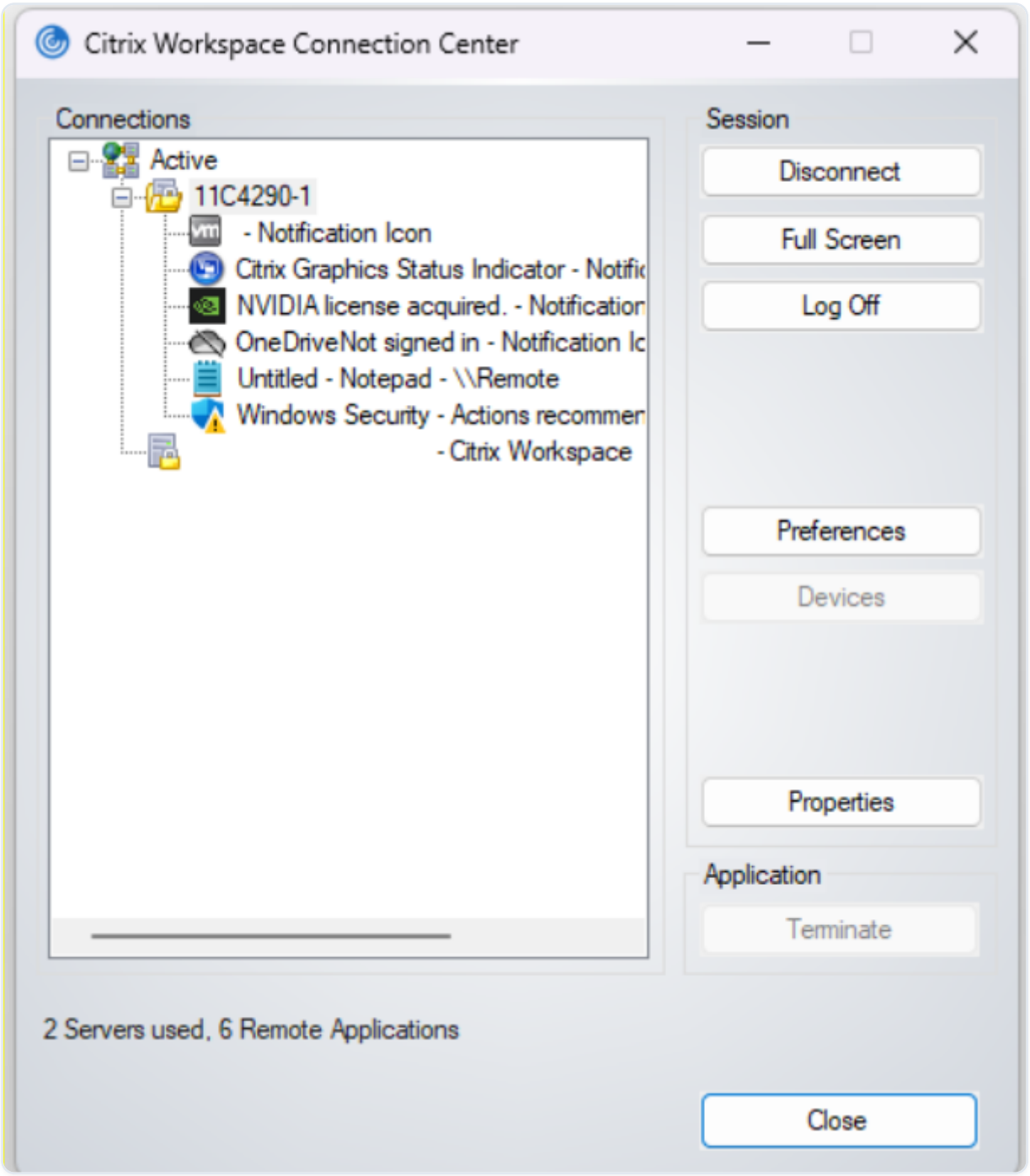
> **注意：**
>
> 每次打开新会话时，此路径都会更改。

8. 这里有两个要读取的键（不要在此处更改它们）：**LogoffCheckBlockingProcess** 和 **LogoffCheckerBlockingVisibleProcess**。这些键显示任何阻止注销的程序。第一个必须显示 `C:\Windows\System32\cmd.exe`，因为它已打开且尚未关闭。

> **注意：**
>
> **LogoffCheckBlockingProcess** 和 **LogoffCheckerBlockingVisibleProcess** 不得手动编辑。手动编辑这些注册表值可能会导致会话不稳定。

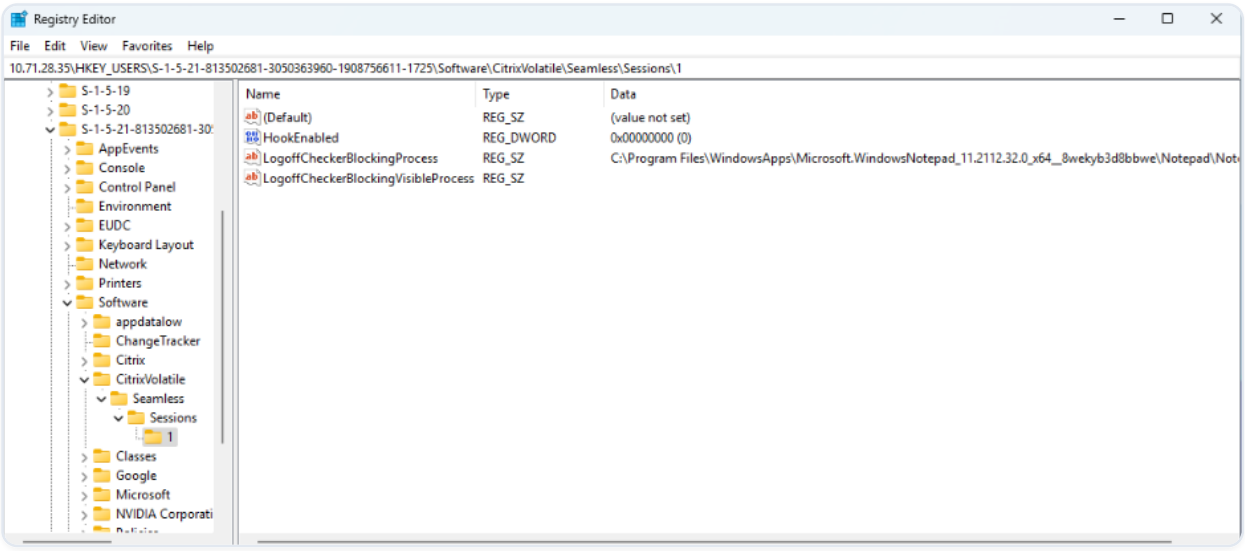


9. 单击右上角的 **X** 以退出 **Seamless CMD**。
10. 检查连接中心以查看会话是否关闭。关闭可能需要长达 30 秒。如果关闭，则没有应用程序或进程阻止正常注销。



11. 如果会话未关闭，请按 F5 刷新 **regedit** 输出。
12. 再次检查 **LogoffCheckBlockingProcess** 和 **LogoffCheckerBlockingVisibleProcess** 的内容。CMD 应该不再存在，但应该有另一个列出的进程。当前阻止会话注销的任何进程都必须显示在此处。

    在这种情况下，在命令提示符关闭之前，**Notepad.exe** 是从已发布的命令提示符打开的，并且此远程记事本进程正在阻止正常注销。



13. 记下此可执行文件的路径及其所在的键，然后将其输入到远程树下的以下注册表项中：

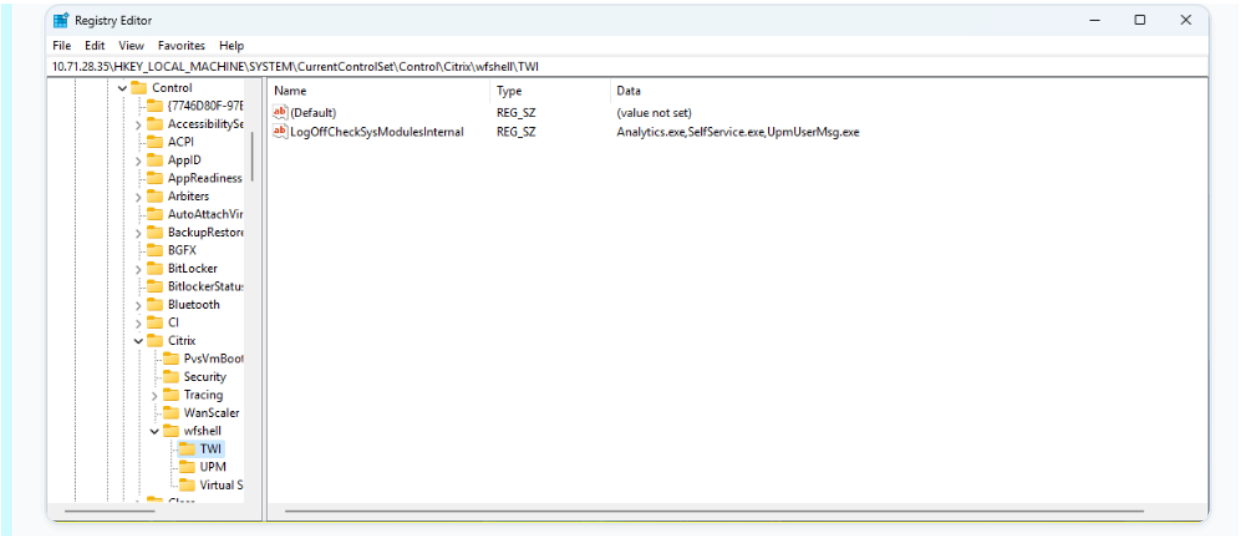
    - 如果它出现在 **LogoffCheckBlockingProcess** 中：

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - 如果它出现在 **LogoffCheckerBlockingVisibleProcess** 中：

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **注意：**
>
> 如果该键中已有一个或多个条目，请在末尾添加一个逗号，然后将新条目放在逗号后面。



14. 从客户端的连接中心注销会话，然后重新打开远程应用程序。

15. 重复步骤 9-16，直到会话在关闭远程应用程序后 30 秒内自动注销。

> **注意：**

故障排除后，如有需要，请恢复临时防火墙更改以允许远程注册表访问。

如何修改 LogonUI 以在打开已发布的应用程序时全尺寸查看 Windows 免责声明消息

在不发生身份验证直通的情况下，**LogonUI** 窗口的缩放功能得到了改进。**LogonUI** 窗口根据所使用的显示器分辨率和 DPI 设置进行缩放，这确保了完整的 **LogonUI** 窗口可见，而不会出现任何裁剪。

窗口大小（以像素为单位）也可以在注册表中手动设置。

1. 在“**运行**”命令中使用 `regedit` 打开“**注册表编辑器**”。
2. 转到 `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`。
3. 创建两个新的 DWORD 键：**LogonUIWidth** 和 **LogonUIHeight**。
4. 将这些键的值设置为 **LogonUI** 窗口所需的像素宽度和高度。

   手动设置 **LogonUI** 窗口大小时，自动缩放将被禁用。

注意：

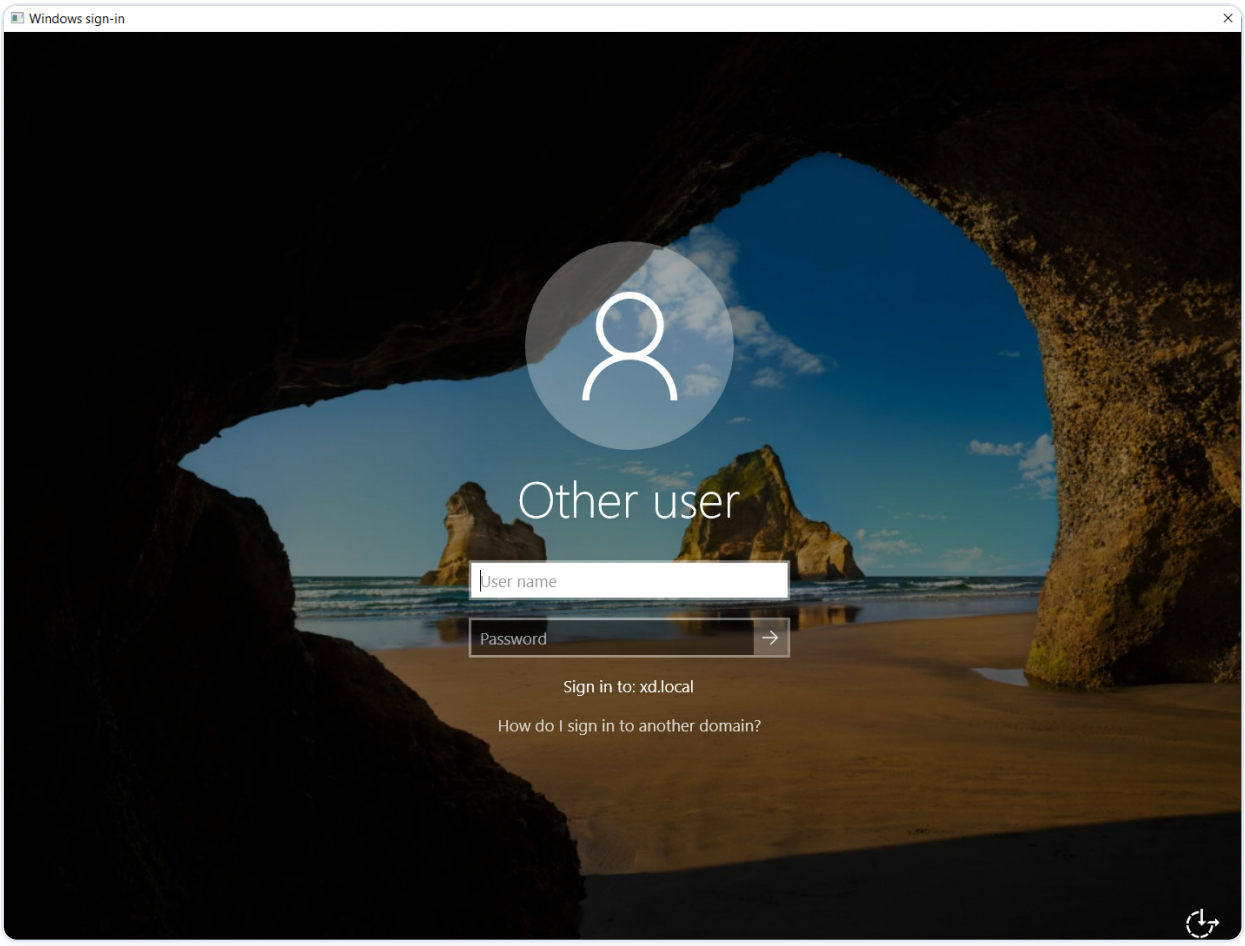
这些注册表路径已从 2407 及更高版本开始更改。旧的注册表值将被忽略并已弃用。

默认情况下，**LogonUI** 窗口包含一个带有关闭按钮的标题栏，最终用户可以在需要时断开会话。

禁用标题栏

您可以使用以下注册表项禁用 **LogonUI** 窗口中的标题栏：

1. 使用 **运行** 命令上的 `regedit` 打开注册表编辑器。
2. 转到 `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`。
3. 创建新的 DWORD 键：**LogonUICaption**，并将该键的值设置为 `0`。



管理应用程序文件夹

默认情况下，您添加到交付组的新应用程序会放置在名为 **Applications** 的文件夹中。您可以在创建交付组、添加应用程序或之后指定不同的文件夹。

须知：

- 您无法重命名或删除 Applications 文件夹，但可以将其包含的所有应用程序移动到您创建的其他文件夹中。
- 文件夹名称可以包含 1–64 个字符。允许使用空格。
- 文件夹最多可以嵌套五层。
- 文件夹不必包含应用程序。允许使用空文件夹。
- 除非您移动文件夹或在创建时指定不同的位置，否则文件夹在 Web Studio 中按字母顺序排列。
- 您可以拥有多个同名文件夹，只要每个文件夹都有不同的父文件夹。同样，您可以拥有多个同名应用程序，只要每个应用程序位于不同的文件夹中。
- 您必须拥有 `View Applications` 权限才能查看文件夹中的应用程序，并且您必须拥有该文件夹中所有应用程序的 `Edit Application Properties` 权限才能移除、重命名或删除包含应用程序的文件夹。

- 以下大多数过程都要求使用 Web Studio 中的操作栏执行操作。此外，您可以使用右键单击菜单或拖动项目。例如，如果您在不希望的位置创建或移动了文件夹，可以将其拖放到正确的位置。
- Web Studio 中的所有节点（例如，**计算机目录**、**交付组**、**应用程序**和**应用程序组**）在后端共享相同的文件夹树。为避免在重命名或移动文件夹时发生名称冲突，请对不同节点中的一级文件夹使用唯一名称。

  如果您使用 `New-BrokerAdminFolder` SDK cmdlet 创建文件夹并希望它显示在**应用程序**节点下，您必须使用 `Set-BrokerAdminFolderMetadata` cmdlet 添加 `ContainsApplications` 元数据。

  示例：

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplications -Value true
  ```

要管理应用程序文件夹，请在左侧窗格中选择**应用程序**。请使用以下列表作为指导。

- **要查看所有文件夹（不包括嵌套文件夹）：** 单击文件夹列表上方的**显示所有**。
- **要在最高级别（非嵌套）创建文件夹：** 选择**应用程序**文件夹。要将新文件夹放置在**应用程序**以外的现有文件夹下，请选择该文件夹。然后，在操作栏中选择**创建文件夹**。输入名称。
- **要移动文件夹：** 选择文件夹，然后在操作栏中选择**移动文件夹**。您一次只能移动一个文件夹，除非该文件夹包含嵌套文件夹。（移动文件夹最简单的方法是拖动它。）
- **要重命名文件夹：** 选择文件夹，然后在操作栏中选择**重命名文件夹**。输入名称。
- **要删除文件夹：** 选择文件夹，然后在操作栏中选择**删除文件夹**。当您删除包含应用程序和其他文件夹的文件夹时，这些对象也会被删除。删除应用程序会从交付组中移除应用程序分配。它不会将其从计算机中移除。
- **要将应用程序移动到文件夹中：** 选择一个或多个应用程序。然后，在操作栏中选择**移动应用程序**。选择文件夹。

在创建交付组或应用程序组时，您还可以在**应用程序**页面上将要添加的应用程序放置在文件夹中。默认情况下，添加的应用程序会进入**应用程序**文件夹。单击**更改**以选择或创建文件夹。

控制已发布的桌面上的应用程序本地启动

当用户从已发布的桌面中启动已发布的应用程序时，您可以控制该应用程序是在该桌面会话中启动还是作为已发布的应用程序启动。Citrix Workspace 应用程序会在 VDA 上的 Windows 注册表中搜索应用程序的安装路径，如果存在，则启动应用程序的本地实例。否则，将启动应用程序的托管实

例。如果您启动未安装在 VDA 上的应用程序，则会启动托管应用程序。有关详细信息，请参阅 vPrefer 启动。

在 PowerShell 中（在 Citrix Cloud 部署中使用远程 PowerShell SDK，或在本地部署中使用 PowerShell SDK），您可以更改此操作。

在 `New-Broker` Application 或 `Set-BrokerApplication` cmdlet 中，使用 `LocalLaunchDisabled` 选项。例如：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

默认情况下，此选项的值为 false (`-LocalLaunchDisabled $false`)。从已发布的桌面中启动已发布的应用程序时，该应用程序将在该桌面会话中启动。

如果将此选项的值设置为 true (`-LocalLaunchDisabled $true`)，则会启动已发布的应用程序。这会从已发布的桌面（使用适用于 Windows 的 Citrix Workspace 应用程序）为已发布的应用程序创建一个单独的附加会话。

要求和限制：

- 应用程序的 `ApplicationType` 值必须为 `HostedOnDesktop`。
- 此选项仅通过相应的 PowerShell SDK 提供。目前在 Web Studio 图形界面中不可用。
- 此选项最低要求：StoreFront 3.14、适用于 Windows 的 Citrix Receiver 4.11 和 Delivery Controller 7.17。

创建应用程序组

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

简介

应用程序组允许您管理应用程序集合。为跨不同交付组共享的应用程序或交付组中由部分用户使用的应用程序创建应用程序组。应用程序组是可选的；它们提供了一种替代方法，无需将相同的应用

程序添加到多个交付组。可以将交付组与多个应用程序组关联，也可以将应用程序组与多个交付组关联。

与使用更多交付组相比，使用应用程序组可以在应用程序管理和资源控制方面提供优势：

- 应用程序及其设置的逻辑分组允许您将这些应用程序作为一个单元进行管理。例如，您不必一次一个地将相同的应用程序添加到（发布到）各个交付组。
- 应用程序组之间的会话共享可以节省资源消耗。在其他情况下，禁用应用程序组之间的会话共享可能是有益的。
- 您可以使用标记限制功能从应用程序组发布应用程序，仅考虑所选交付组中的一部分计算机。通过标记限制，您可以将现有计算机用于多个发布任务，从而节省部署和管理额外计算机的成本。标记限制可以看作是将交付组中的计算机细分（或分区）。在隔离和排查交付组中一部分计算机的问题时，使用带有标记限制的应用程序组或桌面会很有帮助。

示例配置

示例 1：

下图显示了包含应用程序组的 Citrix Virtual Apps and Desktops™ 部署：

应用程序组(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/application-groups-50.png)

在此配置中，应用程序被添加到应用程序组，而不是交付组。交付组指定使用哪些计算机。（尽管未显示，但计算机位于计算机目录中。）

应用程序组 1 与交付组 1 关联。应用程序组 1 中指定的用户可以访问应用程序组 1 中的应用程序。这些组仅在它们也位于交付组 1 的用户列表中时才显示。此配置遵循应用程序组的用户列表是关联交付组的用户列表的子集（限制）的指导。应用程序组 1 中的设置（例如应用程序组之间的应用程序会话共享、关联的交付组）适用于该组中的应用程序和用户。交付组 1 中的设置适用于应用程序组 1 和 2 中的用户，因为这些应用程序组已与该交付组关联。

应用程序组 2 与两个交付组关联：1 和 2。每个交付组在应用程序组 2 中都被分配了一个优先级，指示在启动应用程序时检查交付组的顺序。优先级相同的交付组会进行负载平衡。应用程序组 2 中指定的用户可以访问应用程序组 2 中的应用程序。但是，他们也必须出现在交付组 1 和交付组 2 的用户列表中。

示例 2：

此简单布局使用标记限制来限制哪些计算机可用于某些桌面和应用程序启动。该站点有一个共享交付组、一个已发布的桌面和一个配置了两个应用程序的应用程序组。

标记示例(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/tags-example.png)

已向三台计算机（VDA 101–103）中的每台计算机添加了标记。

应用程序组是使用“Orange”标记限制创建的。它的每个应用程序都只在该交付组中具有“Orange”标记的计算机（VDA 102 和 103）上启动。

有关在应用程序组（以及桌面）中使用标签限制的更全面的示例和指导，请参阅标签。

指导和注意事项

Citrix 建议将应用程序添加到应用程序组或交付组，但不能同时添加到两者。否则，在两种组类型中都包含应用程序会增加复杂性，从而使其更难以管理。

默认情况下，应用程序组处于启用状态。创建应用程序组后，您可以编辑该组以更改此设置。请参阅管理应用程序组。

默认情况下，应用程序组之间的应用程序会话共享处于启用状态。请参阅应用程序组之间的会话共享。

Citrix 建议将交付组升级到当前版本。此过程需要：

1. 升级交付组中使用的计算机上的 VDA。
2. 升级包含这些计算机的计算机目录。
3. 升级交付组。

有关详细信息，请参阅管理交付组。

要使用应用程序组，您的核心组件最低版本必须为 7.9。

创建应用程序组需要交付组管理员内置角色的委派管理权限。有关详细信息，请参阅委派管理。

本文指的是将应用程序“关联”到多个应用程序组。它将此操作与从可用源添加该应用程序的实例区分开来。同样，交付组与应用程序组关联，而不是彼此的附加项或组件。

与应用程序组的会话共享

启用应用程序会话共享后，所有应用程序都在同一应用程序会话中启动。这节省了启动更多应用程序会话的成本，并允许使用涉及剪贴板的应用程序功能，例如复制粘贴操作。但是，在某些情况下，您可以清除会话共享。

使用应用程序组时，您可以通过以下三种方式配置应用程序会话共享，这些方式扩展了仅使用交付组时可用的标准会话共享行为：

- 应用程序组之间启用会话共享。

- 仅在同一应用程序组中的应用程序之间启用会话共享。
- 会话共享已禁用。

应用程序组之间的会话共享

您可以在应用程序组之间启用应用程序会话共享，也可以禁用它，将应用程序会话共享仅限于同一应用程序组中的应用程序。

- **启用应用程序组之间会话共享的有用示例：**

  应用程序组 1 包含 Microsoft Office 应用程序，例如 Word 和 Excel。应用程序组 2 包含其他应用程序，例如记事本和计算器，并且两个应用程序组都连接到同一个交付组。有权访问这两个应用程序组的用户通过启动 Word 来启动应用程序会话，然后启动记事本。如果控制器发现用户运行 Word 的现有会话适合运行记事本，则记事本将在现有会话中启动。如果记事本无法从现有会话中运行（例如，如果标记限制排除了会话正在运行的计算机），则会在合适的计算机上创建新会话，而不是使用会话共享。

- **禁用应用程序组之间会话共享的有用示例：**

  一种配置，其中包含一组与安装在同一台计算机上的其他应用程序不兼容的应用程序。例如，同一软件套件的两个不同版本或同一 Web 浏览器的两个不同版本。您不希望允许用户在同一会话中启动这两个版本。

  为软件套件的每个版本创建一个应用程序组，并将软件套件每个版本的应用程序添加到相应的应用程序组。如果这些应用程序组之间禁用了会话共享，则这些组中指定的用户可以在同一会话中运行相同版本的应用程序。用户仍然可以同时运行其他应用程序，但不能在同一会话中运行。当启动其中一个不同版本的应用程序，或任何不包含在应用程序组中的应用程序时，该应用程序将在新会话中启动。

此应用程序组之间的会话共享功能不是安全沙盒功能。它并非万无一失，也无法阻止用户通过其他方式（例如，通过 Windows 资源管理器）在其会话中启动应用程序。

如果计算机已满负荷，则不会在其上启动新会话。新应用程序将根据需要使用会话共享在该计算机上的现有会话中启动。

您只能将预启动会话提供给允许应用程序会话共享的应用程序组。（使用会话延迟功能的会话可用于所有应用程序组。）这些功能必须在与应用程序组关联的每个交付组中启用和配置。您无法在应用程序组中配置它们。

默认情况下，在创建应用程序组时，应用程序组之间的应用程序会话共享处于启用状态。创建组时无法更改此设置。创建应用程序组后，您可以编辑该组以更改此设置。请参阅管理应用程序组。

禁用应用程序组内的会话共享

您可以阻止同一应用程序组中的应用程序之间进行应用程序会话共享。

- **禁用应用程序组内的会话共享有帮助的示例：**

  您希望用户在单独的显示器上访问应用程序的多个同时全屏会话。

  您创建一个应用程序组并将应用程序添加到其中。

默认情况下，创建应用程序组时会启用应用程序会话共享。创建组时无法更改此设置。创建应用程序组后，您可以编辑该组以更改此设置。请参阅管理应用程序组。

创建应用程序组

要创建应用程序组，请执行以下操作：

1. 登录 Web Studio。
2. 在左侧窗格中选择**应用程序**，然后选择**应用程序组**选项卡。
3. 要使用文件夹组织应用程序组，请在**应用程序组**根文件夹下创建文件夹。有关详细信息，请参阅使用文件夹组织应用程序组。
4. 选择要创建组的文件夹，然后单击“**创建应用程序组**”。组创建向导将启动并显示“**简介**”页面。您可以从该向导的未来启动中删除此页面。
5. 按照向导在以下页面上配置设置。完成每个页面后，选择“**下一步**”，直到到达“**摘要**”页面。

步骤 1. 交付组

“**交付组**”页面列出了所有交付组，以及每个组包含的计算机数量。

- “**兼容的交付组**”列表包含您可以选择的交付组。兼容的交付组包含随机（非永久或静态分配）多会话或单会话操作系统计算机。
- “**不兼容的交付组**”列表包含您无法选择的交付组。每个条目都解释了其不兼容的原因，例如包含静态分配的计算机。

应用程序组可以与包含可交付应用程序的共享（非专用）计算机的交付组关联。

如果满足以下两个条件，您还可以选择包含仅交付桌面的共享计算机的交付组：

- 交付组包含共享计算机，并且是使用早于 7.9 版本的 XenDesktop 创建的。
- 您具有“编辑交付组”权限。

提交应用程序组创建向导时，交付组类型会自动转换为“桌面和应用程序”。

尽管您可以创建一个没有关联交付组的应用程序组（可能用于组织应用程序或作为当前未使用的应用程序的存储），但该应用程序组在指定至少一个交付组之前无法用于交付应用程序。此外，如果未指定任何交付组，则无法从“**从‘开始’菜单**”源向应用程序组添加应用程序。

您选择的交付组指定用于交付应用程序的计算机。选中要与应用程序组关联的交付组旁边的复选框。

要添加标记限制，请选择“**将启动限制到具有该标记的计算机**”，然后从下拉列表中选择该标记。

步骤 2. 用户

在应用程序组中指定应用程序用户。可以允许上一页中选择的交付组中的所有用户和用户组，也可以从这些交付组中选择特定的用户和用户组。如果将使用限制为指定用户，则只有交付组中指定的用户（即应用程序组）才能访问此组中的应用程序。本质上，应用程序组中的用户列表提供了对交付组中用户列表的筛选。

启用或禁用未经身份验证的用户使用应用程序仅在交付组中可用，而不在应用程序组中可用。

有关部署中指定用户列表的位置的信息，请参阅 指定用户列表的位置。

步骤 3. 应用程序

须知：

- 默认情况下，您添加的新应用程序将放置在名为“**应用程序**”的文件夹中。您可以指定其他文件夹。如果您尝试添加应用程序，并且该文件夹中已存在同名应用程序，系统将提示您重命名要添加的应用程序。如果您同意建议的唯一名称，则应用程序将以该新名称添加。否则，您必须自行重命名才能添加。有关详细信息，请参阅管理应用程序文件夹。
- 您可以在添加应用程序时或之后更改其属性（设置）。请参阅更改应用程序属性。如果您向同一用户发布两个同名应用程序，请在 Web Studio 中更改“**应用程序名称（面向用户）**”属性。否则，用户将在 Citrix Workspace 应用程序中看到重复的名称。
- 当您将应用程序添加到多个应用程序组时，如果您没有足够的权限在所有这些组中查看该应用程序，则可能会出现可见性问题。在这种情况下，请咨询具有更高权限的管理员，或者扩展您的范围以包括添加了该应用程序的所有组。

单击下拉菜单中的“**添加**”以显示应用程序源。

- **从“开始”菜单：** 在所选交付组中的计算机上发现的应用程序。选择此源时，将启动一个新页面，其中包含发现的应用程序列表。选中要添加的应用程序的复选框，然后单击“**确定**”。

  如果选择了以下任何一项，则无法选择此源：

  - 没有关联交付组的应用程序组。

- 关联交付组中不包含任何计算机的应用程序组。
- 不包含任何计算机的交付组。

- **手动定义：** 位于站点或网络中其他位置的应用程序。选择此源时，将启动一个新页面，您可以在其中键入可执行文件的路径、工作目录、可选命令行参数以及管理员和用户的显示名称。输入此信息后，单击“**确定**”。
- **现有：** 以前添加到站点的应用程序。选择此源时，将启动一个新页面，其中包含发现的应用程序列表。选中要添加的应用程序的复选框，然后单击“**确定**”。如果站点没有应用程序，则无法选择此源。
- **App-V：** App-V 软件包中的应用程序。选择此源时，将启动一个新页面，您可以在其中选择“**App-V 服务器**”或“**应用程序库**”。从结果显示中，选中要添加的应用程序的复选框，然后单击“**确定**”。有关详细信息，请参阅部署和交付 App-V 应用程序。如果未为站点配置 App-V，则无法选择此源（或可能不显示）。

如前所述，如果不存在该类型的有效源，则“**添加**”下拉菜单中的某些条目将不可选。不兼容的源根本不会列出（例如，您不能将应用程序组添加到应用程序组，因此在创建应用程序组时不会列出该源）。

步骤 4. 作用域

此页面仅在您之前创建了自定义作用域时显示。默认情况下，将选择**所有**作用域。有关详细信息，请参阅委派管理。

步骤 5. 摘要

输入应用程序组的名称。您还可以（可选）输入描述。

查看摘要信息，然后单击**完成**。

发布内容

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

> 您可以发布一个应用程序，该应用程序只是指向资源的 URL 或 UNC 路径，例如 Microsoft Word 文档或 Web 链接。此功能称为发布内容。发布内容的能力增加了向用户交付内容的灵活性。您可以受益于现有的应用程序访问控制和管理。您还可以指定是使用本地应用程序还是已发布的应用程序来打开内容。

发布的内容在 StoreFront™ 和 Citrix Workspace™ 应用程序中与其他应用程序一样显示。用户访问它的方式与访问应用程序的方式相同。在客户端上，资源照常打开。

- 如果本地安装的应用程序合适，则会启动它来打开资源。
- 如果已定义文件类型关联，则会启动已发布的应用程序来打开资源。

您可以使用 PowerShell SDK 发布内容。您不能使用 Web Studio 发布内容。但是，您可以在发布后使用 Web Studio 编辑应用程序属性。

配置概述和准备

发布内容使用 `New-BrokerApplication` cmdlet，并具有以下关键属性。（有关所有 cmdlet 属性的说明，请参阅 cmdlet 帮助。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType` 属性必须为 `PublishedContent`。

`CommandLineExecutable` 属性指定发布内容的位置。支持以下格式，限制为 255 个字符。

- HTML 网站地址（例如，`<http://www.citrix.com>`）
- Web 服务器上的文档文件（例如，`https://www.citrix.com/press/pressrelease.doc`）
- FTP 服务器上的目录（例如，`ftp://ftp.citrix.com/code`）
- FTP 服务器上的文档文件（例如，`ftp://ftp.citrix.com/code/Readme.txt` >）
- UNC 目录路径（例如，`file://myServer/myShare or \\\\myServer\\myShare`）
- UNC 文件路径（例如，`file://myServer/myShare/myFile.asf` 或 `\\myServer\myShare\myFile.asf`）

确保您拥有正确的 SDK。

- 对于 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）部署，下载 并安装 Citrix Virtual Apps and Desktops 远程 PowerShell SDK。

- 对于本地 Citrix Virtual Apps and Desktops 部署，请使用随 Delivery Controller 安装的 PowerShell SDK。添加已发布的内容应用程序需要最低版本为 7.11 的 Delivery Controller。

以下过程使用示例。在示例中：

- 已创建计算机目录。
- 已创建名为 `PublishedContentApps` 的交付组。该组使用目录中的多会话操作系统计算机。WordPad 应用程序已添加到该组。
- 已为交付组名称、`CommandLineExecutable` 位置和应用程序名称进行分配。

入门

在包含 PowerShell SDK 的计算机上，打开 PowerShell。

以下 cmdlet 添加相应的 PowerShell SDK 管理单元，并分配返回的交付组记录。

`Add-PsSnapin Citrix* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

如果您使用的是 Citrix DaaS，请通过输入您的 Citrix Cloud™ 凭据进行身份验证。如果存在多个客户，请选择一个。

发布 URL

分配位置和应用程序名称后，以下 cmdlet 将 Citrix 主页发布为应用程序。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"



New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

验证成功：

- 打开 StoreFront 并以可以访问 PublishedContentApps 交付组中应用程序的用户身份登录。显示屏包含新创建的带有默认图标的应用程序。要了解如何自定义图标，请参阅 `<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`。
- 单击 **Citrix 主页**应用程序。URL 将在本地运行的默认浏览器实例的新选项卡中启动。

发布位于 UNC 路径的资源

在此示例中，管理员已创建了一个名为 `PublishedResources` 的共享。分配位置和应用程序名称后，以下 cmdlet 将该共享中的 RTF 和 DOCX 文件发布为资源。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

验证成功：

- 刷新 StoreFront 窗口以查看新发布的文档。
- 单击 **PublishedRTF** 和 **PublishedDOCX** 应用程序。每个文档都会在本地运行的写字板中打开。

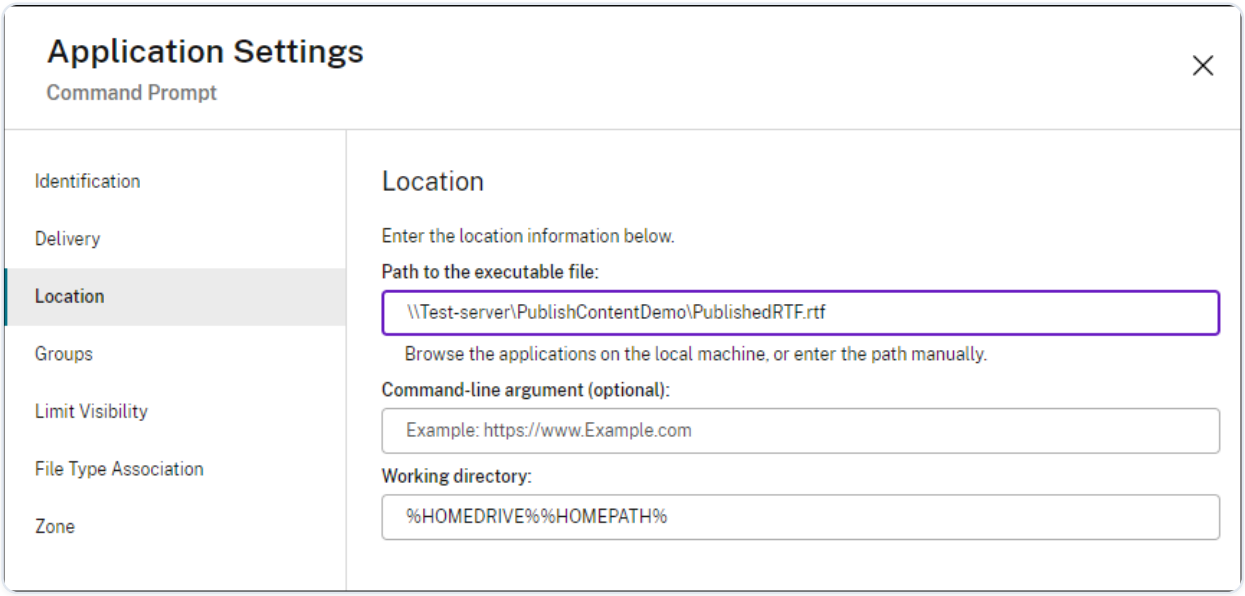
查看和编辑 PublishedContent 应用程序

您可以使用管理其他应用程序类型的方法来管理已发布的内容。

要查看和编辑 `PublishedContent` 应用程序，请执行以下步骤：

1. 登录 Web Studio 并在左侧窗格中选择**应用程序**。
2. 在**应用程序**选项卡上，选择一个 PublishedContent 应用程序，然后选择**属性**。

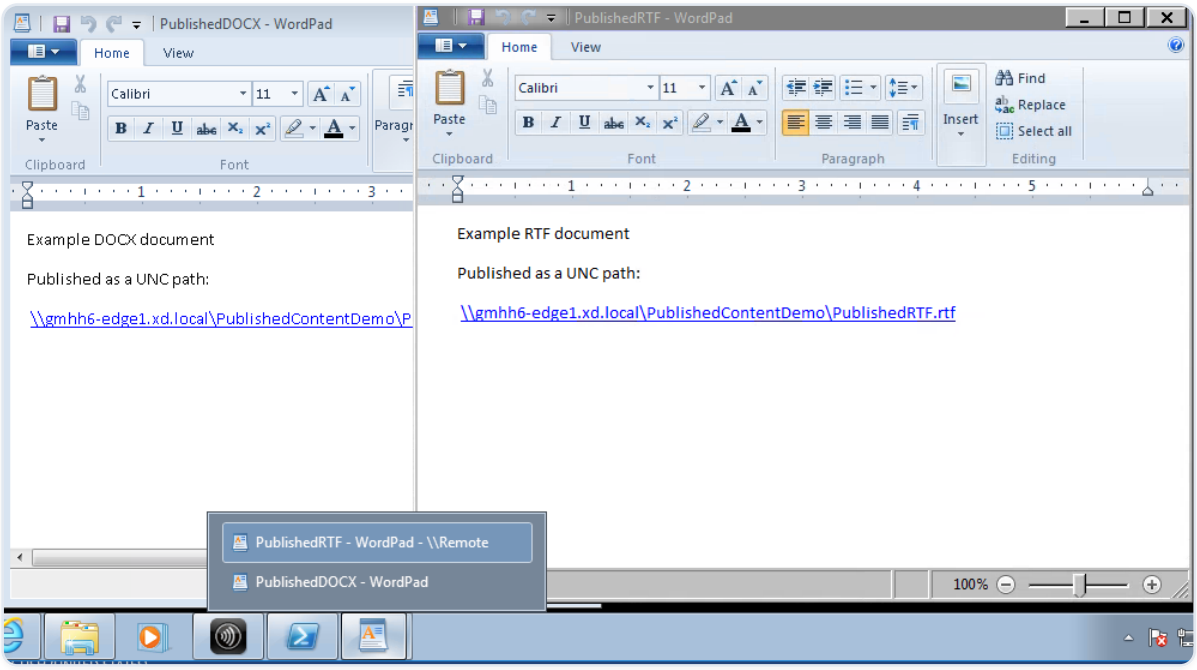
   应用程序属性（例如用户可见性、组关联和快捷方式）适用于已发布的内容。但是，您无法在**位置**页面上更改命令行参数或工作目录属性。
3. 要更改资源，请修改该页面上的**可执行文件路径**字段。



4. 要使用已发布的应用程序打开 `PublishedContent` 应用程序（而不是本地应用程序），请执行以下步骤：

   在此示例中，编辑已发布的写字板应用程序以创建 .rtf 文件的文件类型关联。

   a. 为交付组启用维护模式。
   b. 编辑“**文件类型关联**”属性。
   c. 完成后，禁用维护模式。
   d. 刷新 StoreFront 以加载文件类型关联更改，然后单击“**PublishedRTF**”和“**PublishedDOCX**”应用程序。请注意区别。“**PublishedDOCX**”仍将在本地写字板中打开。但是，由于文件类型关联，“**PublishedRTF**”现在将在已发布的写字板中打开。



更多信息

- 创建计算机目录
- 创建交付组
- 更改应用程序属性

应用程序包

应用程序包是 Citrix® 管理的预配置应用程序部署。它们允许应用程序虚拟化，这意味着应用程序独立于用户设备的操作系统和界面运行。

应用程序包简化了应用程序管理，减少了 IT 开销，并确保应用程序在其整个生命周期中安全且功能正常。

Citrix 支持以下打包技术，用于向用户交付应用程序：

- App-V 应用程序
- MSIX 和 MSIX app attach 应用程序
- FlexApp 应用程序
- Elastic App 应用程序
- Cloudpaging 应用程序

本文将引导您了解如何在 Citrix Virtual Apps and Desktops™ 环境中部署和交付这些打包的应用程序。

注意：

- 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。
- 我们不建议交替使用 Web Studio 和 Citrix Studio 来部署和交付应用程序包。它们各自使用不同的机制，这可能导致差异，例如 App-V 服务器信息在一个中显示正确而在另一个中不显示。此外，请注意 Citrix Studio 仅支持 App-V。

App-V 应用程序

应用程序虚拟化 (App-V) 是一种 Microsoft 技术，允许流式传输和访问应用程序，而无需在最终用户设备上安装。Citrix Virtual Apps and Desktops 可以使用 App-V 交付应用程序，提供一种集中高效的方式来管理各种客户端计算机上的应用程序。

有关交付 App-V 打包应用程序时所涉及的组件和概念的更多信息，请参阅 Microsoft 文档：适用于 Windows 客户端的应用程序虚拟化 (App-V) 概述。

重要术语

- **管理服务器**：提供一个集中式控制台来管理 App-V 基础结构，并将虚拟应用程序交付给 App-V 桌面客户端和远程桌面服务客户端。App-V 管理服务器负责身份验证、请求以及提供管理员所需的安全、计量、监控和数据收集功能。该服务器使用 Active Directory 和支持工具来管理用户和应用程序。
- **发布服务器**：为 App-V 客户端提供特定用户的应用程序，并托管用于流式传输的虚拟应用程序包。它从管理服务器获取包。
- **动态配置文件**：App-V 包可以使用动态配置文件进行自定义，这些文件应用于包后，可用于更改其特性。例如，您可以使用它们来定义额外的应用程序快捷方式和行为。有关详细信息，请参阅动态配置文件

动态配置文件

Citrix App-V 支持两种类型的动态配置文件。文件设置在应用程序启动时应用：

- **部署配置文件**为所有用户提供机器范围的配置。这些文件应命名为 `<packageFileName>_DeploymentConfig.xml` 并与它们所应用的 App-V 包位于同一文件夹中。单管理员和双管理员管理都支持这些文件。

- **用户配置文件**提供用户特定的配置，支持对包进行按用户自定义。单管理员支持以下列格式命名的用户配置文件：`<packageFileName>_[UserSID | Username | GroupSID | GroupName_]UserConfig.xml`，并位于它们所应用的 App-V 包的同一文件夹中。

  当特定包存在多个用户配置文件时，它们按以下优先级应用：

  a. 用户 SID

  b. 用户名

  c. AD 组 SID（第一个找到的获胜）

  d. AD 组名称（第一个找到的获胜）

  e. 默认值

  例如：

  ```
  MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml

  MyAppVPackage_joeblogs_UserConfig.xml

  MyAppVPackage_S-1-5-32-547_UserConfig.xml

  MyAppVPackage_Power Users_UserConfig.xml

  MyAppVPackage_UserConfig.xml
  ```

  注意：

  文件名的用户特定部分也可以选择出现在末尾（例如 `MyAppVPackage_UserConfig_joeblogs.xml`）。

重要提示：

当存在打开了包中应用程序的用户会话时，您无法应用对动态部署配置的更改。如果其他用户（但不是当前用户）打开了包中的应用程序，则可以应用对动态用户配置文件进行的更改。

动态配置文件位置

在单一管理员管理中，Citrix App-V 组件仅处理动态配置文件，这些文件与其 App-V 包位于同一文件夹中。

当启动包中的应用程序时，对相应动态配置文件的任何更改都将重新应用。如果您的动态配置文件与其包位于不同的位置，请使用映射文件将包映射到其部署配置文件。

要创建映射文件：

1. 打开一个新文本文件。
2. 对于每个动态配置文件，添加一行，使用 `<PackageGuid> : path` 格式指定包的路径。

   例如：

   ```
   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
   ```

3. 将文件另存为 `ctxAppVDynamicConfigurations.cfg`，并将其放在与包相同的文件夹中。

每次启动包中的应用程序时，都会在与 App-V 包相同的 UNC 共享上向上递归搜索整个目录层次结构以查找此文件。

方法

您可以使用以下方法交付和管理 App-V 包：

- **双管理员**：在此方法中，Citrix Virtual Apps and Desktops 和 App-V 服务器协同工作以交付和管理软件包。此方法要求 Citrix Virtual Apps and Desktops 定期刷新 App-V 服务器状态的快照视图。它会产生硬件、基础架构和管理开销。Citrix Virtual Apps and Desktops 和 App-V 服务器必须保持同步，尤其是用户权限。

  此方法最适用于紧密耦合的 App-V 和 Citrix 部署。在此方法中：

  - **App-V 管理服务器**处理动态配置文件
  - **应用程序包交付组件**安装在 VDA 计算机上：管理应用程序启动所需的相应发布服务器的注册。

  这可确保发布服务器在适当的时间为用户同步。发布服务器使用其配置的设置来维护应用程序包生命周期的其他方面（例如登录时刷新和连接组）。
- **单一管理员**：应用程序包存储在网络共享上。Citrix Virtual Apps and Desktops 独立交付和管理软件包。

此方法可减少开销，因为部署中不需要 App-V 服务器和数据库基础结构。

在此方法中，您将 App-V 包存储在网络共享上，并将其元数据从该位置上传到您的环境。然后，安装在 VDA 计算机上的应用程序包交付组件按如下方式管理和交付应用程序：

- 当应用程序启动时，处理部署配置文件和用户配置文件。
- 管理主机上包生命周期的所有方面。

注意：

- 您可以同时使用一种或两种管理方法。换句话说，当您将应用程序添加到交付组时，这些应用程序可以来自 App-V 服务器或网络共享上的 App-V 包。
- 如果您同时使用两种管理方法，并且 App-V 包在两个位置都有动态配置文件，则将使用 App-V 服务器中的文件（双重管理）。
- 在 Web Studio 导航窗格中选择“应用程序包”时，显示屏会显示包名称和类型。“**包类型**”列指示用于交付包的技术以及它们在“**应用程序库**”中的引用位置。选择包时，详细信息窗格会列出包中的应用程序和快捷方式。

MSIX 和 MSIX 应用附加应用程序

MSIX 是一种 Windows 应用程序包格式，可为所有 Windows 应用程序提供现代打包体验。MSIX 适用于各种 Windows 应用程序类型，包括 Win32、.NET 和 UWP 应用程序。

MSIX 应用附加利用预先扩展到虚拟硬盘上的 MSIX 包，这些包可以根据需要挂载到目标计算机，而不是流式传输包内容。它可以缩短部署时间、减少网络流量并降低目标计算机上的 IOPS，但需要额外的工作来创建和维护应用附加磁盘。

Citrix Virtual Apps and Desktops 通过安装在 VDA 计算机上的“**应用程序包交付组件**”向用户交付 MSIX 和 MSIX app attach 应用程序。此组件管理主机上包生命周期的所有方面。

有关 MSIX 和 MSIX app attach 的更多信息，请参阅 Microsoft 文档：MSIX documentation 和 App Attach in Azure Virtual Desktop。

注意：

- 我们支持桌面和服务器 VDA 上的本机 MSIX 包，以及仅在桌面 VDA 上支持 `.vhd`、`.vhdx` 和 `.cim` 磁盘映像格式的 MSIX app attach。
- Microsoft 不为 Server 2019 提供 AppAttach 实现。虽然 AppAttach 存在于 Server 2022 和 2025 中，但 Microsoft 不支持这些版本上的 AppAttach。因此，我们也不支持 Server 2022 和 2025 上的 AppAttach。
- 在 Windows Server 2019 上启用旁加载。
- 确保 VDA 信任用于签署软件包的证书。

FlexApp 应用程序

FlexApp 是 Liquidware 开发的一种应用程序分层解决方案，它可以在不通过传统应用程序安装过程修改底层基础映像的情况下，将任何应用程序附加到 Windows 会话。

FlexApp One 应用程序封装在一个可共享的单个文件中，使其无需在 Windows 会话上额外添加应用程序层即可运行。用户可以通过单击容器文件启动应用程序，这会快速将一个或多个应用程序集成到他们的 Windows 工作区中。

Citrix 通过安装在 VDA 计算机上的 App Packages Delivery Component 和 FlexApp 交付代理向用户交付 FlexApp 应用程序。这两个组件管理主机上软件包生命周期的所有方面。

Elastic App 应用程序

Elastic App 技术是 Citrix App Layering 的一项功能，它允许您在登录时动态地将应用程序层分配给用户，而不是将其安装到基础映像中。借助 Elastic App 技术，应用程序会跟随用户在不同的虚拟机之间移动，确保用户始终可以访问所需的应用程序，而不会使主映像变得臃肿。

Citrix Virtual Apps and Desktops 通过 Citrix Personalization 组件和 Application Layering Enterprise Layer Manager (ELM) 向用户交付 Elastic App 应用程序。这两个组件管理主机上包生命周期的所有方面。有关 Application Layering Enterprise Layer Manager 的更多信息，请参阅Citrix App Layering™ 文档。

Cloudpaging 应用程序

Cloudpaging 是 Numecent 的应用程序流技术，它将应用程序交付到 Windows 会话，而无需更改基础映像。

借助 Cloudpaging，应用程序几乎可以即时启动，因为最初只流式传输一小部分代码（通常不到 10%）。当用户访问其余组件时，它们会在后台流式传输，从而提供无缝体验。

对于 Citrix 环境，VDA 上的应用程序包交付组件与 Numecent Cloudpaging Player 协同工作，以管理应用程序生命周期。Citrix 组件协调交付，而 Cloudpaging Player 则处理会话内的按需流式传输和执行。

配置要求

请考虑以下配置详细信息：

云分页播放器和注销检查系统模块

将虚拟发布的应用程序与 Cloudpaging 容器结合使用时，请配置以下设置以允许会话注销：

设置	值
注册表项	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`
值名称	`LogoffCheckSysModules`
值类型	`REG_SZ`
值数据	`CoreHelper.exe`

允许列表中的 URL

除了标准的 URL 允许列表要求外，VDA 还需要访问以下端点：

参数	值
URL	`external-api.cloudpager.net`
端口	443
客户端	Cloudpager PoSh 模块
基于 Web 的正向代理配置	• 允许出站访问 • 需进行身份验证绕过
描述	Cloudpager PowerShell 模块

（可选）您可以创建一个专用交付组，其中包含一个仅用于执行 Cloudpager 发现的 VDA，以限制所需的白名单 URL。我们建议创建一个交付组，其中包含安装了 **VDA 版本 2511 或更高版本**和**应用程序包交付组件**的计算机。

有关 Cloudpager Client 网络和防火墙要求的更多信息，请参阅 Numecent 知识库文章。

部署和交付应用程序包

先决条件

为了支持交付 App-V、MSIX、MSIX app attach、FlexApp 包、Elastic App 应用程序和 Cloudpaging 包，您必须首先在 VDA 计算机上安装“**应用程序包交付组件**”。有关详细信息，请参阅在 VDA 计算机上安装应用程序包交付组件。

在 VDA 计算机上安装应用程序包交付组件

应用程序包交付组件管理 App-V、MSIX、MSIX app attach、FlexApp、Elastic App 和 Cloudpaging 格式的应用程序包的发布过程。默认情况下，在安装 VDA 时不会安装此组件。您可以在 VDA 安装期间或之后安装此组件。

要在 VDA 安装期间安装此组件，请使用以下任一方法：

- 在安装向导中，转到“**附加组件**”页面，然后选择“**应用程序包交付组件**”复选框。
- 在命令行界面中，使用 `/includeadditional "Citrix Personalization for App-V – VDA"` 选项。

要在 VDA 安装后安装此组件，请执行以下步骤：

1. 在 VDA 计算机上，转到“**控制面板 > 程序 > 程序和功能**”，右键单击“**Citrix Virtual Delivery Agent**”，然后选择“**更改**”。
2. 在出现的向导中，转到“**附加组件**”页面，然后启用“**应用程序包交付组件**”复选框。

> **注意：**
>
> - Microsoft App-V 桌面客户端是用于在用户设备上运行 App-V 包中的虚拟应用程序的组件。Windows 10（1607 或更高版本）以及 Windows Server 2019 及更高版本已包含此 App-V 客户端软件。您只需在 VDA 计算机上启用它。有关详细信息，请参阅此 Microsoft 文档文章：启用 App-V 内置客户端。
> - 对于 FlexApp 应用程序，请在 VDA 上安装 FlexApp One 代理以及应用程序包交付组件。

- 对于 Elastic App 应用程序，请在 VDA 上安装启用 App Layering 的映像以及应用程序包交付组件。
- 对于 Cloudpaging 应用程序，请在 VDA 上安装Cloudpaging Player以及应用程序包交付组件。

安装 FlexApp One 代理

1. 在 VDA 上启动管理员命令提示符。
2. 找到任何 FlexApp One 包的网络路径。
3. 输入以下命令：

```
\\path\to\any\FlexAppOnePackage.exe --install
```

4. 接受出现的任何提示。

安装启用 App Layering 的映像

1. 设置应用程序分层。 请按照 Citrix App Layering 文档中的说明进行操作。该过程包括：
   a. 设置企业层管理器 (ELM)。
   b. 导入黄金 OS 映像。
   c. 创建一个平台层。
   d. 创建应用程序层。
   e. 在 ELM 中，选中要交付的每个应用程序层的“**为 Studio 应用程序包启用此应用程序层**”复选框。
2. 在 VDA 计算机上安装包含 Elastic Layering 组件的映像。您可以使用以下方法之一：
   a. 从 ELM 部署已启用 Elastic Layering 的映像。
   b. 在计算机上手动安装 VDA 并在设置过程中选择 Elastic Layering 组件。

安装 Cloudpaging 播放器

1. 在 VDA 上打开管理员命令提示符。
2. 转到包含 Cloudpaging Player 安装程序的文件夹。
3. 运行以下命令以静默安装播放器并配置 SaaS 控制台 URL。根据需要替换占位符值：

```
cloudpaging-player-setup-x64-release.exe /S /v"/qn ADDLOCAL=ALL
REG_BASTOKENPATHORURL=https://your-tenant-url/api/token"
```

4. （可选）安装后通过检查以下注册表值来验证配置：
   - **路径：** `HKEY_LOCAL_MACHINE\SOFTWARE\Numecent\StreamingCore\Settings\Launcher`
   - **名称：** `BaseTokenPathOrURL`
   - **数据：** 该值必须与您在安装期间指定的 URL 匹配。

交付打包的应用程序

完成安装 (#prerequisites) 后，请执行以下操作以向用户交付打包的应用程序：

1. (#store-application-packages-on-network-shares) 在网络共享上存储应用程序包。
2. (#upload-application-packages-into-your-environment) 将应用程序包上传到您的环境。
3. (#add-applications-to-delivery-groups) 将应用程序添加到交付组。
4. 要启用相互依赖的 App-V 包的自动交付，请 (#optional-create-isolation-groups-for-app-v-packages) 创建隔离组。

在网络共享上存储应用程序包

设置基础结构后，生成应用程序包并将其存储在网络位置，例如 UNC 或 SMB 网络共享或 Azure 文件共享。

详细步骤如下：

1. 生成应用程序包。有关详细信息，请参阅 Microsoft 文档：创建和管理 App-V 虚拟化应用程序。
2. 在网络位置存储应用程序包：
   - 对于 **App-V Single Admin**：将包和相应的动态配置文件 (App-V) 存储在 UNC 或 SMB 网络共享或 Azure 文件共享上。
   - 对于 **App-V Dual Admin**：从 UNC 路径将包发布到 App-V 管理服务器。（不支持从 HTTP URL 发布。）
   - 对于 **MSIX 或 MSIX app attach**：将包存储在 UNC 或 SMB 网络共享或 Azure 文件共享上。
   - 对于 **FlexApp**：将包存储在 UNC 或 SMB 网络共享或 Azure 文件共享上。
   - 对于 **Elastic App**：将包存储在 UNC 或 SMB 网络共享或 Azure 文件共享上。
   - 对于 **Cloudpaging**：将软件包存储在 UNC 或 SMB 网络共享或 Azure 文件共享上。

3. 确保 VDA 对软件包存储路径具有读取权限：

   - 如果您将软件包存储在 AD 域中的 UNC 或 SMB 网络共享上，请授予 VDA 计算机对存储路径的读取权限。为此，您可以明确授予计算机的 AD 帐户对共享的读取权限，或者将该帐户包含在具有该权限的 AD 组中。
   - 如果您将软件包存储在 Azure 文件共享上，请首先授予用户帐户对 Azure 中存储路径的读取权限。接下来，配置在 VDA 计算机上运行的 `ctxAppVService` 以使用该用户帐户访问软件包存储路径。有关详细步骤，请参阅更改用户登录帐户。

更改用户登录帐户

在以下两种情况下更改用户登录帐户：

- 要使用链接的 AD 帐户访问 Azure 文件共享上的软件包：
  - 连接实体必须是用户帐户，而不是计算机帐户，因为 Microsoft Entra ID 不会向文件共享上的计算机帐户授予读取权限。
- 如果 MSIX 和 MSIX AppAttach 软件包包含服务：
  - 软件包必须使用在本地计算机上具有管理权限的用户帐户发布，然后才能发布给任何非管理用户。这是安装打包服务所必需的，并且软件包只能发布给用户，而不能发布给计算机，这使得默认的 LocalService 帐户不适用。

VDA 调用 `ctxAppVService` 来访问软件包存储路径并执行需要管理权限的操作。默认情况下，`ctxAppVService` 在计算机的 LocalService 帐户的上下文中运行，该帐户使用计算机的身份向 AD 进行身份验证，不适用于上述场景。

在任何一种情况下，都必须重新配置服务以使用具有本地管理权限并已授予对软件包存储位置（无论是 SMB 共享还是 Azure 文件共享）读取访问权限的 AD 用户帐户，具体如下：

1. 启动“**服务**”，右键单击“**ctxAppVService**”，然后选择“**属性**”。
2. 在“**登录**”选项卡上，选择“**此帐户**”：
   a. 输入一个具有本地管理权限和对软件包存储路径的读取权限的用户帐户。
   b. 输入用户密码两次。
3. 单击 **确定**。

将应用程序包上传到您的环境

根据需要将应用程序包存储到网络位置后，将其上传到您的环境以进行交付。根据需要使用以下任一方法：

- 批量上传
- 逐个上传

准备工作

Citrix Virtual Apps and Desktops 使用 VDA 计算机设置与网络位置的连接以进行包发现。因此，请事先创建交付组，并确保组中至少有一个 VDA 满足以下要求：

- VDA 版本：
  - 要发现 App-V 包：2203 或更高版本
  - 要发现 MSIX 和 MSIX app attach 包：2209 或更高版本
  - 要发现 FlexApp 包：2311 或更高版本以及 FlexApp Agent 软件
  - 要发现 ElasticApp 包：2511 或更高版本以及启用 App Layering 的映像
  - 要从 Cloudpager 控制台发现 Cloudpaging 包：2511 或更高版本
  - 要从网络共享发现 Cloudpaging 包：2607 LTSR 或更高版本
- 应用程序包交付组件：已安装
- 包位置权限：读取（有关详细信息，请参阅 在网络共享上存储应用程序包。）
- 电源：开
- 状态：已注册

批量上传应用程序包

将网络位置中的包上传到您的环境。上传前，请确保您已准备好以下各项：

- 满足 准备工作 要求的交付组
- 网络位置路径

要批量上传包，请执行以下步骤：

1. 在左侧窗格中，选择 **应用程序包**。
2. 在“**包发现**”选项卡上，单击“**创建发现配置文件**”按钮。“**创建发现配置文件**”页面随即出现。
3. 在 **名称** 字段中，输入配置文件的描述性名称。
4. 在 **交付组** 字段中，单击 **选择交付组**。接下来，选择一个满足 准备工作 中所述要求的交付组，然后单击 **确定**。
5. 在 **位置类型** 字段中，根据存储包的位置选择 **Microsoft App-V 服务器**、**网络共享** 或 **Numecent Cloudpager**，然后完成相应的设置：
   - 如果您选择了 **Microsoft App-V 服务器**，请输入以下信息：

- 管理服务器的 URL。示例：`http://appv-server.example.com`
- 管理服务器管理员的登录凭据。
- 发布服务器的 URL 和端口号。示例：`http://appv-server.example.com:3330`

- 如果您选择了 **Network share**，请指定以下信息：
  - 输入网络共享的 UNC 路径（示例：`\\Package-Server\apps\`）。对于 *Elastic App packages*，请输入 ELM 中 **System's Network File Share SMB path** 的 UNC 路径。
  - 选择要上传的包类型。选项包括 **App-V**、**MSIX**、**MSIX app attach**、**FlexApp**、**Elastic App** 和 **Cloudpaging**。
  - 指定是否在子文件夹中搜索包。

> **注意：**
>
> 如果您在包含 `cim` 映像的文件夹结构中搜索 MSIX app attach 包，请确保选择**搜索**子文件夹。否则，磁盘将无法正确发现。

- 如果选择了 **Numecent Cloudpager**（这意味着 Cloudpaging 应用程序存储在 Cloud Pager Console 上），请输入以下信息：
  - Cloudpager 控制台 URL。示例：`https://cloudpagerconsole.my.org`
  - PowerShell API 密钥。
  - AppLauncher MSID。

6. 单击“**创建发现配置文件**”。

“**创建发现配置文件**”页面关闭，新添加的配置文件将显示在配置文件列表中。Citrix Virtual Apps and Desktops 使用交付组中的 VDA 将软件包上传到您的环境。上传完成后，“状态”字段显示 *导入成功*。相应的软件包将显示在“**软件包**”选项卡上。

> **注意：**
>
> 要在源位置检查软件包更新并将其导入到您的环境，请在配置文件列表中选择该位置，然后单击“**检查更新**”。

逐个上传应用程序包

将应用程序包从网络共享上传到您的环境。上传之前，请确保已准备好以下各项：

- 满足准备工作中规定的要求的交付组
- 网络位置路径。

要将软件包上传到您的环境，请执行以下步骤：

1. 在左侧窗格中，选择“**应用程序包**”。
2. 在“**软件包**”选项卡上，单击“**添加软件包**”按钮。此时将显示“**添加软件包**”页面。
3. 在“**交付组**”字段中，单击“**选择交付组**”。接下来，选择一个符合准备工作中规定的要求的交付组，然后单击“**确定**”。
4. 在“**程序包完整路径**”字段中，根据需要输入路径：
   - 要一次上传多个程序包，请输入它们的完整路径，用分号分隔 (`;`)。示例：`\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - 要上传网络共享上存在的所有程序包，请输入存储路径。示例：`\\package-Server\apps\`
5. 单击“**添加程序包**”。

   应用程序程序包将显示在“**程序包**”选项卡上。

将应用程序添加到交付组

将应用程序程序包完全上传到您的环境后，根据需要将其应用程序添加到一个或多个交付组。这样，与这些交付组关联的用户就可以访问这些应用程序。

> **注意：**
>
> - 您可以通过交付组将打包的应用程序交付给单会话 VDA 和多会话 VDA。
> - 默认情况下，最终用户可以访问分配给与其*单会话*（或称为*桌面*）VDA 关联的交付组的所有打包应用程序。要将打包应用程序在*桌面* VDA 上的可见性限制为特定用户或组，请转到“**应用程序**”节点，选择该应用程序，然后选择“**编辑应用程序属性 > 限制可见性**”进行更改。请参阅限制应用程序的可见性

> 要将程序包中的一个或多个应用程序添加到多个交付组，请执行以下步骤：

1. 在左侧窗格中，选择 **App Packages**。
2. 在 **Packages** 选项卡上，根据需要选择一个包。
3. 在操作栏中，单击 **Add Delivery Groups**。将显示 **Assign Applications to Delivery Groups** 页面。
4. 根据需要选择软件包中的一个或多个应用程序，然后单击“**下一步**”。
5. 在交付组列表中，选择要分配应用程序的组，然后单击 **Next**。

> **注意：**
>
> - 如果您选择了 MSIX 或 MSIX app attach 包，则列表中仅显示 VDA 版本为 2106 或更高版本的交付组。
> - 如果您选择了 *FlexApp* 包，则列表中仅显示 VDA 版本为 2402 或更高版本的交付组。
> - 如果选择了 *Elastic App* 软件包，则列表中仅显示 VDA 版本为 2511 或更高版本的交付组。
> - 如果您选择了 *Cloudpaging* 包，则列表中仅显示 VDA 版本为 2511 或更高版本的交付组。

6. 单击“**完成**”。

要将各种包中的应用程序添加到多个交付组，请执行以下步骤：

1. 在左侧窗格中，选择 **App Packages**。
2. 在 **Applications** 选项卡上，选择 **Add Applications**。
3. 在 **Groups** 页面上，根据需要选择一个或多个交付组。
4. 在 **Applications** 页面上，按如下方式选择一个或多个应用程序包：
    a. 单击 **Add**，然后选择 **Application packages**。
    b. 选择所需的软件包配置文件类型（例如，App-V 单管理员）。此类型的所有软件包都会显示。
    c. 根据需要选择一个或多个包。
    d. 单击 **OK**，然后单击 **Next**。
    e. 要添加不同包类型的更多应用程序，请重复步骤 a 到 d。
5. 单击“**完成**”。

您还可以在以下情况下将打包的应用程序添加到交付组：

- 创建交付组。有关详细信息，请参阅 创建交付组。
- 编辑现有交付组或应用程序组。有关详细信息，请参阅 添加应用程序。

（可选）为 App-V 包创建隔离组

您可以创建隔离组，以实现相互依赖的 App-V 软件包的自动交付。

> **注意：**
>
> 隔离组支持 App-V 单管理员方法。如果您使用的是 App-V 双管理员方法，则可以通过在 Microsoft App-V 基础结构中创建*连接组*来实现相同的目标。有关详细信息，请参阅此 Microsoft 文档文章：关于连接组文件。

关于隔离组

隔离组是相互依赖的应用程序包的集合，这些包必须在同一个 Windows 沙盒中运行才能创建虚拟环境。Citrix App-V 隔离组与 App-V 连接组相似但不完全相同。隔离组包括两种类型的软件包：

- **显式应用程序包**：具有特定许可要求的应用程序。您可以通过将这些应用程序添加到交付组来将其限制为特定范围的用户。
- **自动应用程序包**：无论是否添加到交付组，始终对所有用户可用的应用程序。

例如，应用程序 `app-a` 需要 JRE 1.7 才能运行。您可以创建一个隔离组，其中包含 app-a（标记为*显式*）和 JRE 1.7（标记为*自动*）。接下来，将 `app-a` 的 App-V 软件包添加到一个或多个交付组。当用户启动 app-a 时，JRE 1.7 会随之自动部署。

当用户在隔离组中启动标记为 *显式* 的 App-V 应用程序时，Citrix Virtual Apps and Desktops 会检查用户在交付组中对该应用程序的访问权限。如果用户有权访问该应用程序，则同一隔离组中的任何 *自动* 应用程序包都将对用户可用。

您无需将*自动*软件包添加到任何交付组。如果隔离组中还有另一个*显式*应用程序包，则只有当该包位于同一交付组中时，该包才对用户可用。

创建 APP-V 隔离组

创建隔离组并将相互依赖的应用程序包添加到其中。详细步骤如下：

1. 在**隔离组**选项卡上，单击**添加隔离组**。
2. 输入隔离组的名称和描述。环境中的所有 App-V 单管理员软件包都会显示在**可用软件包**列表中。

3. 从**可用软件包**列表中，根据需要选择一个应用程序，然后单击向右箭头。所选应用程序将显示在**隔离组中的软件包**列表中。
4. 在“**部署**”字段中，为应用程序选择“**显式**”或“**自动**”。
5. 重复步骤 2-3 以添加更多程序包。
6. 要调整列表中程序包的顺序，请单击向上或向下箭头。
7. 单击 **保存**。

> **注意：**
>
> 隔离组配置会导致在 VDA 上创建 App-V 连接组。部署方案可能变得复杂，并且 App-V 客户端支持一次只在一个活动连接组中的程序包。建议您避免将同一个程序包添加到属于同一个交付组的两个不同隔离组中。

最佳实践

- 要部署 App-V 程序包，请使用 PowerShell 命令 `Enable-AppV` 在 VDA 上启用 App-V 子系统。
- 要部署 MSIX（和 AppAttach）程序包，VDA 必须信任用于签署这些程序包的证书。
- 在 Windows Server 2019 上，启用旁加载以部署 MSIX 程序包。Windows 10、11、Windows Server 2022 和 2025 不需要旁加载。
- App Attach 在 Windows Server 2019 上根本没有实现，并且目前 Microsoft（或 Citrix 扩展）在 Windows Server 2022 或 2025 上不支持它。

高级

以下高级主题提供了额外的配置选项和控件，用于在 Citrix Virtual Apps and Desktops 中微调打包应用程序的发现、更新和交付方式，超越了基本的应用程序包工作流程。

自动化打包应用程序发布

您可以使用 PowerShell 命令自动化打包应用程序发布：

在 Delivery Controller™ 上，运行以下 PowerShell 命令:

1. 加载包发现模块中存在的命令:

```
Import-Module "D:
\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```

> **注意:**
>
> 软件包发现模块的版本可以在 Citrix Virtual Apps and Desktops ISO 上找到，路径如步骤 1 中所述。

2. 软件包发现模块必须来自支持您正在发布的软件包类型的 Citrix Virtual Apps and Desktops 版本的 ISO，即 FlexAppOne 应用程序需要 2311 或更高版本。我们建议使用最新版本。
3. 检索相关的交付组 ID 和打包应用程序 ID:

```
Get-BrokerDesktopGroup | Format-Table Uid, Name

Get-AppLibAppVApplication | Format-Table Uid, Name
```

4. 发布包并创建相应的 BrokerMachineConfigurations:

```
Publish-PackagedApplication -AppLibararyApplicationUid
<AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
```

5. 同步 Broker 配置，这些配置稍后会发送到 VDA 上的 Broker 代理:

```
Update-DesktopGroupMachineConfigurations -DesktopGroupUid
<DesktopGroup.Uid>
```

> **注意:**
>
> 请务必在通过 PowerShell 命令行发布或从交付组中删除打包应用程序后运行 PowerShell 命令 `Update-DesktopGroupMachineConfigurations`。否则，有关已发布应用程序的信息将无法正确发送到 VDA，并且启动会失败。

限制应用程序可见性

在 Citrix Virtual Apps and Desktops 环境中，当软件包中的应用程序发布到桌面时，系统会遵循这些应用程序的 Active Directory (AD) 用户和组可见性设置。但是，即使用户只能看到软件包中的一个应用程序，也必须将整个软件包部署到虚拟桌面（或无缝应用程序）会话，因为单个软件包组件无法在 VDA 上细分。此外，在 VDA 2503 版本之前，初始发布后降低应用程序可见性的更改不会导致在

后续桌面启动时清理以前发布的软件包。此外，其他可见性层（例如桌面与工作区可见性）在这些 AD 可见性分配之上运行。

您可以控制打包应用程序是必须显示在 Workspace 中，还是部署到用户的 VDI 桌面会话。打包应用程序发布后，您可以使用 PowerShell 命令 `Set-BrokerApplication -Name "MyApp" -PackagedApplicationVisibility "Workspace|Desktop|WorkspaceAndDesktop"` 更新 `BrokerApplictaion` 上的 `PackagedApplicationVisibility` 属性。

`PackagedApplicationVisibility` 的默认值为 `WorkspaceAndDesktop`。

值 `Workspace`: 应用程序仅显示在 WorkspaceApp 中，可用于无缝 AppLaunch，但应用程序不会自动发布到用户启动的任何桌面会话。

值 `Desktop`：从 WorkspaceApp 隐藏应用程序图标，使其无法进行无缝 AppLaunch，但如果用户通过其 AD 组设置也可以访问该应用程序，则该应用程序仍可部署到用户的桌面会话。

> **注意：**
>
> 发布到单会话静态桌面的打包应用程序在 Workspace App 中永远不可用，无论此设置中配置的值如何。

从 App-V 完整基础架构迁移到单一管理员工作流

Microsoft App-V 完整基础架构（双管理员）即将终止支持。要继续交付 App-V 软件包和其他受支持的容器格式，请迁移到 Citrix 单一管理员模型。

单一管理员模型消除了对 App-V 管理和发布服务器的依赖，并将软件包管理集中到 Studio 中。

单一管理员模型的优势

转向单一管理员工作流可简化您的架构并优化软件包管理。

简化的架构

在单一管理员模型中，VDA 直接从文件共享检索软件包。Citrix 管理元数据、发布和隔离逻辑。

功能	完整基础架构（双管理员）	单一管理员（CITRIX 管理）
管理	App-V 管理控制台	Citrix 工作室 或 Web 工作室
数据库	必需 (SQL Server)	无（元数据存储在 Citrix 站点数据库中）

功能	完整基础架构（双管理员）	单一管理员（CITRIX 管理）
发布	App-V 发布服务器	思杰 VDA（`ctxAppVService`）
程序包源	UNC 共享（与管理服务器同步）	UNC 共享、SMB 共享或 Azure 文件
逻辑	连接组	Citrix 隔离组

战略优势

通过迁移到单一管理员，您还可以消除**同步延迟**。

- 在双管理员模型中，您必须同步 App-V 管理服务器，然后同步 Studio。
- 在单管理员模型中，当您在文件共享上更新包并在 Studio 中选择**刷新**时，更新后的包将在下次用户登录时可用。

迁移工作流

请按照以下步骤将您现有的 App-V 完整基础结构迁移到 Citrix 单管理员工作流：

1. 步骤 1：准备目标环境
2. 步骤 2：将包导入 Citrix 库

步骤 1：准备目标环境

在导入包之前，请确保您的基础结构和 VDA 已准备好支持单管理员模型。

1. **共享存储库**
   a. 确定托管您的 `.appv` 包的 UNC 共享。
   b. 确保 VDA 计算机帐户（例如，域计算机）对共享和 NTFS 权限都具有**读取**访问权限。
2. **VDA**

   确保所有 VDA 都已安装 **App Packages Delivery Component**。要在安装后添加此组件，请执行以下操作：

   a. 运行 VDA 安装程序。
   b. 在**程序和功能**中选择**更改**。
   c. 添加 **应用程序包交付组件**。
3. **XML 配置文件**

将 `_DeploymentConfig.xml` 和 `_UserConfig.xml` 文件移动到与相应 `.appv` 文件*相同*的文件夹中。

在单一管理员模型中，VDA 从文件共享上的程序包文件夹而不是从中央 App-V 数据库读取配置文件。

步骤 2：将程序包导入 Citrix 库

准备好环境后，将现有 App-V 程序包导入 Citrix 应用程序库。

1. 在 Citrix Studio 中，转到**配置** > **应用程序包**。
2. 如果您正在完全迁移，请删除与 App-V 管理服务器的任何现有连接。
3. 选择**添加程序包**并将其指向程序包的 UNC 路径。
4. Citrix 会扫描该文件夹并将程序包名称、版本和应用程序 ID 导入 Citrix 应用程序库。

导入后，您可以根据需要将应用程序分配给交付组。

> **注意：**

> **vPrefer 策略（可选）**：如果您希望应用程序在本地 VDA 上启动而不是重定向到远程服务器，请在您的 VDA 上启用 **vPrefer** GPO。

排除 App-V 应用程序故障（单一管理员模型）

如果 App-V 程序包（在单一管理员模型中）无法启动或未显示在用户会话中，请使用以下指南来识别和解决常见问题。

问题	描述	解决方案
包发现和“编目失败”错误	在 Studio 中添加包时，出现错误提示文件无法访问或元数据无效。	1. 验证权限。确保 Delivery Controller 计算机帐户（例如，`DOMAIN\DDC01$`）对托管包的 UNC 路径的共享和 NTFS 级别

问题	描述	解决方案	
		都具有**读取**权限。 2. 检查 XML 完整性。 确保 `.appv` 文件和 `_DeploymentConfig.xml` 文件具有相同的文件名开头，并且位于同一文件夹中。	
应用程序启动失败 (错误代码： 0x80070005 或 0x80040154)	用户点击应用程序图标后，出现 **Citrix 启动**屏幕，但应用程序未打开。	1. 验证 VDA 组件。 确保 VDA 上安装了 **App Packages Delivery Component**。 确认存在以下文件：`C:\Program Files\Citrix\AppV\ctxAppVService.exe`。 2. 检查 VDA 权限。 由于 VDA 从文件共享中拉取程序包，因此 VDA 计算机帐户（例如 `DOMAIN\VDA-`	

问题	描述	解决方案	
		`HR01$`）必须对 UNC 路径具有**读取**访问权限。 3. 验证 App-V 客户端配置。 • 在 VDA 上运行以下 PowerShell 命令：`Get-AppvClientConfiguration`。 • 如果您的程序包需要脚本，请确保 `EnablePackageScripts` 设置为 `$True`。	
隔离组冲突	插件（例如 Excel 加载项）无法看到其父应用程序。	1. 在 Studio 中，转到 **应用程序包** > **隔离组**。 2. 确保两个程序包都已添加到同一隔离组。 在单一管理员模型中，VDA 上的 App-V 客户端根据 Delivery Controller 提供的配置管理这些应用程序的虚拟连接。	

问题	描述	解决方案	
首次启动缓慢（缓冲）	首次启动大型 App-V 软件包（例如 AutoCAD 或 ArcGIS）需要几分钟。	1. 在 VDA 上，检查以下注册表项：`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AppV\Client\Streaming` 2. 将 `Autoload` 设置为 `2`（自动加载所有以前使用的软件包）以提高后续启动性能。 3. 检查网络性能。确保网络共享上的 SMB 签名或防病毒扫描没有限制传输速度。	

有用的 PowerShell 命令（在 VDA 上运行）

要验证 Citrix 是否已成功将软件包交付到 VDA，请在 PowerShell 窗口中运行以下命令：

命令	目的
`Get-AppvClientPackage`	显示当前缓存到 VDA 或发布到 VDA 的所有 App-V 软件包。
`Get-CtxAppvPackage`	显示由 Citrix 代理管理的软件包。
`Start-Service ctxAppVService`	重新启动 Citrix App-V 编排服务。

通用 Windows 平台应用

有关通用 Windows 平台 (UWP) 应用的信息，请参阅以下 Microsoft 文档：

- 什么是通用 Windows 平台 (UWP) 应用？
- Windows 程序包管理器

要求和限制

Citrix Virtual Apps and Desktops™ 支持在以下 Windows 计算机上将 UWP 应用与 VDA 结合使用：

- Windows 10 及更高版本
- Windows Server 2016 及更高版本

VDA 最低版本必须为 7.11。

以下 Citrix Virtual Apps and Desktops™ 功能在使用 UWP 应用程序时不受支持或受限：

- 不支持文件类型关联。
- 不支持本地应用访问。
- 动态预览：如果会话中运行的应用重叠，预览将显示默认图标。UWP 应用不支持用于动态预览的 Win32 API。
- 操作中心远程处理：UWP 应用可以使用操作中心在会话中显示消息。这些消息目前不会重定向到端点以显示给用户。

不支持从同一服务器启动 UWP 应用和非 UWP 应用。请将 UWP 应用和非 UWP 应用放置在单独的交付组或应用程序组中。

由于机器上安装的所有 UWP 应用程序都会被枚举，Citrix® 建议禁用用户对 Windows 应用商店的访问。这可以防止一个用户安装的 UWP 应用程序被其他用户访问。

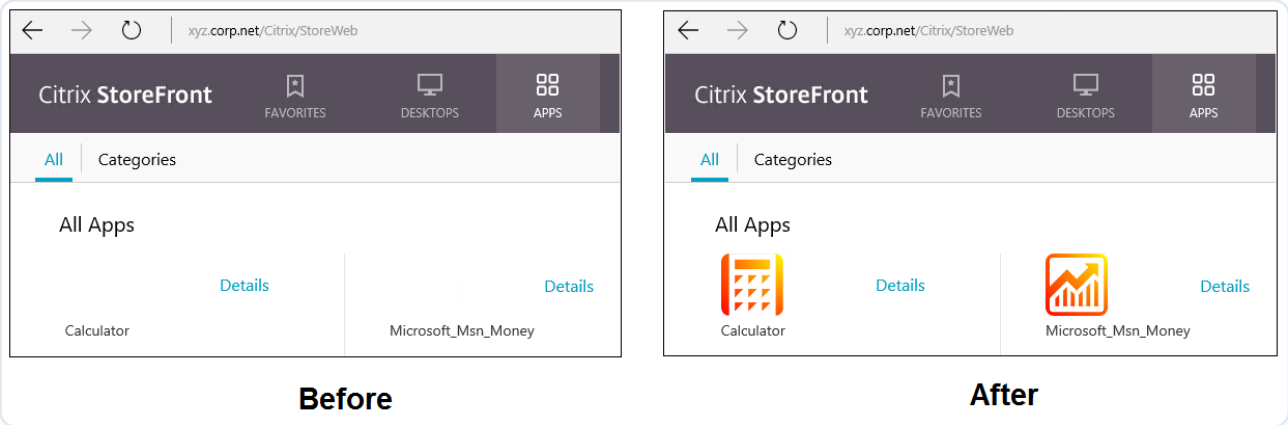
在旁加载期间，UWP 应用程序会安装在计算机上，并可供其他用户使用。当其他用户启动该应用程序时，它会被安装，并且操作系统会更新其 AppX 数据库以指示该用户“已安装”。

从在固定或无缝窗口中启动的已发布的 UWP 应用程序开始的正常注销可能会阻止 VDA 会话关闭并强制注销用户。发生这种情况时，VDA 会话中剩余的几个进程会阻止其正常关闭。要解决此问题，请确定是哪个进程阻止 VDA 会话关闭，然后按照 CTX891671 中的指导将其添加到“LogoffCheckSysModules”注册表项值中。

UWP 应用程序的应用程序显示名称和描述可能不正确。在将应用程序添加到交付组时，请编辑并更正这些属性。

请查看 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/whats-new/known-issues.html) 以了解任何其他问题。

目前，一些 UWP 应用程序具有启用透明度的白色图标，这导致图标在 StoreFront 显示的白色背景下不可见。为避免此问题，您可以更改背景。例如，在 StoreFront 计算机上，编辑文件 `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`。在文件末尾，添加 `.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`。下图说明了此示例的更改前后对比。



在 Windows Server 2016 及更高版本上，启动 UWP 应用程序时也可能会启动服务器管理器。为防止这种情况发生，您可以使用 `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon` 注册表项禁用服务器管理器在登录时自动启动。有关详细信息，请参阅 `<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`。

安装和发布 UWP 应用程序

默认情况下启用对 UWP 应用程序的支持。

要在 VDA（或主映像）上安装一个或多个 UWP 应用程序，请使用以下方法之一：

- 使用部署映像服务和管理 (DISM) 等工具，从适用于企业的 Windows 应用商店完成脱机安装，以将应用程序部署到桌面映像。有关详细信息，请参阅 Windows 程序包管理器。
- 旁加载应用程序。有关详细信息，请参阅 在 Windows 客户端设备中旁加载业务线 (LOB) 应用。
- 直接从适用于企业的 Windows 应用商店为每个目标用户安装 UWP 应用程序。

要在 Citrix Virtual Apps 或 Citrix Virtual Desktops™ 中添加（发布）一个或多个 UWP 应用程序，请执行以下操作：

1. UWP 应用安装到计算机后，将 UWP 应用添加到交付组或应用程序组。您可以在创建组时或之后执行此操作。在“**应用程序**”页面上，在“**添加**”菜单中，选择“**从‘开始’菜单**”。

2. 应用程序列表出现时，选择要发布的 UWP 应用。
3. 继续向导或关闭编辑对话框。

要禁用在 VDA 上使用通用应用，请在 `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` 中添加注册表设置 **EnableUWASeamlessSupport** 并将其设置为 **0**。

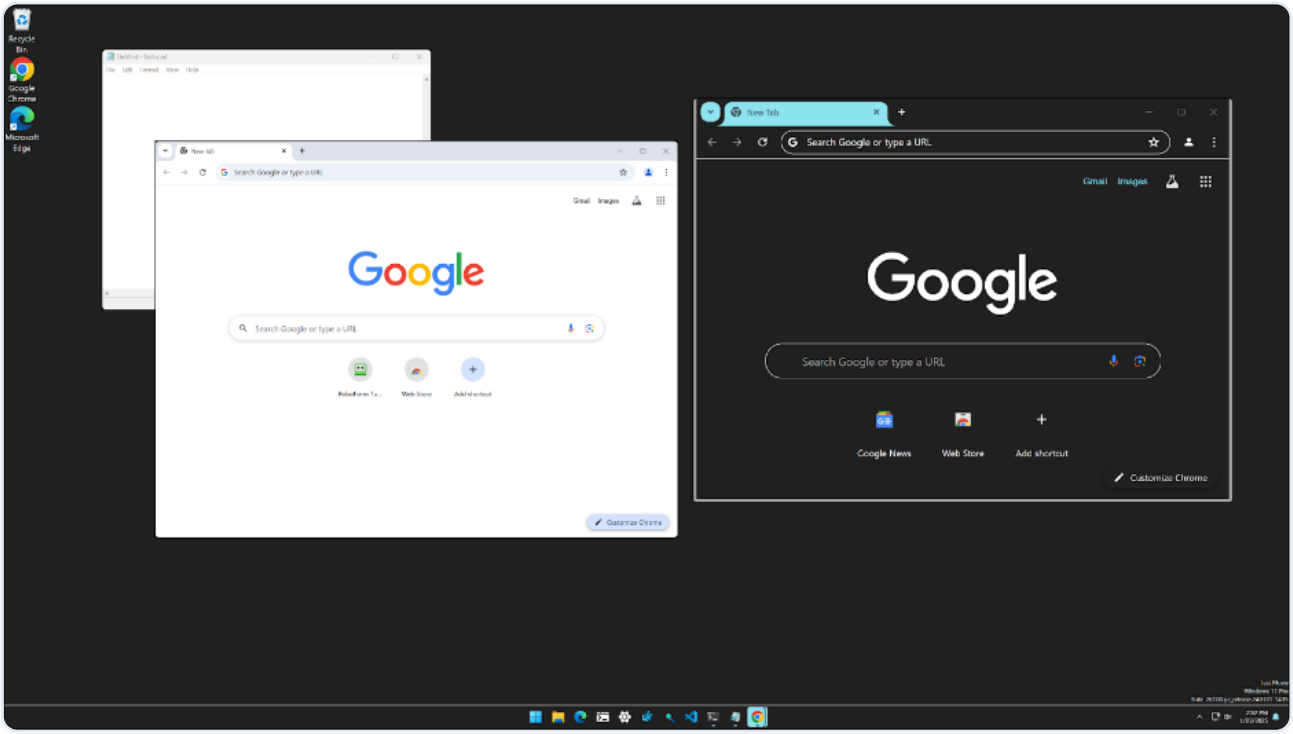
卸载 UWP 应用

当您使用 `Remove-AppXPackage` 等命令卸载 UWP 应用时，该项目仅针对管理员卸载。要从可能已启动和使用该应用的用户计算机中删除该应用，请在每台计算机上运行删除命令。您无法通过一个命令从所有用户的计算机中卸载 AppX 包。

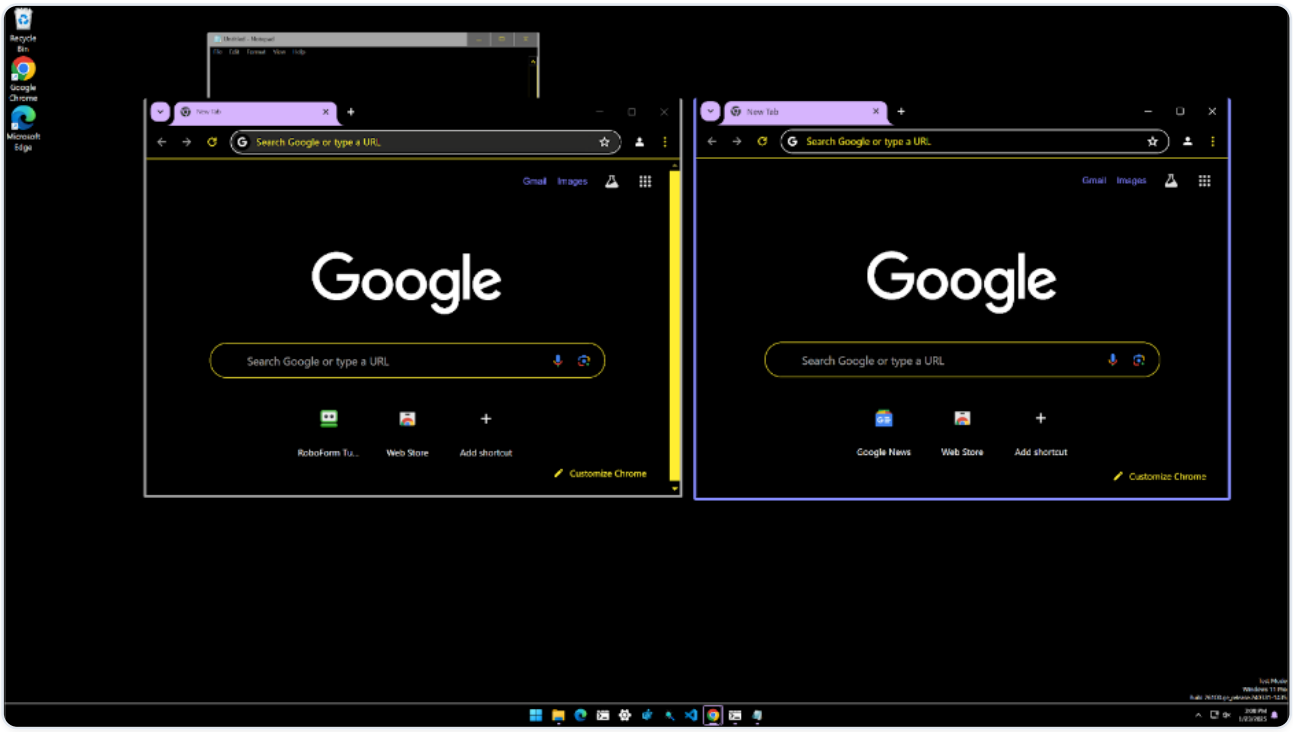
Windows 辅助功能设置

无缝应用程序的 Windows 辅助功能设置将在启动时自动将用户本地端点的一部分辅助功能设置镜像到已发布的应用程序会话。在会话期间，对本地端点辅助功能设置的更改将在可能的情况下自动应用于远程会话。

未启用无缝应用程序的 Windows 辅助功能设置时：



启用无缝应用程序的 Windows 辅助功能设置时：



无缝应用程序的 Windows 辅助功能设置将在会话期间自动且动态地将这些设置应用于远程应用程序：

辅助功能镜像将自动把用户的本地端点中的以下本地辅助功能设置镜像到 VDA。目前，支持以下辅助功能设置：

- 高对比度主题
- 深色模式
- 鼠标光标大小
- 文本大小

先决条件

Seamless Applications 的辅助功能设置的先决条件如下：

- 运行 CWA for Windows 2503 或更高版本的 Windows 端点
- 运行 VDA 2503 或更高版本的 Windows VDA

辅助功能镜像在以下 VDA 操作系统上可用：

- Windows 服务器 2022
- Windows 服务器 2025
- Windows 10 多会话
- Windows 11 单会话和多会话

以及在以下客户端操作系统上：

- Windows 10 系统
- Windows 十一

如何启用

从 Citrix Virtual Apps and Desktops 2511 和适用于 Windows 的 CWA 2511 开始，Seamless 应用程序的可访问性设置传播默认启用。

此功能无需管理员或最终用户配置。

适用于管理员

您可以通过注册表显式禁用运行 CVAD 2511 或更高版本的 VDA 的可访问性设置镜像。

1. 使用 regedit.exe 打开 **Windows 注册表编辑器**。
2. 导航到 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\`
3. 创建一个名为 AccessibilityMirroring 的 **DWORD** 值，并将其值设置为 0 以禁用。

访问在该 VDA 上托管的 Seamless 应用程序的所有用户，其客户端可访问性设置将不会传播到他们的 Seamless 应用程序。

适用于最终用户

如果您不想将可访问性设置从端点镜像到 Seamless 应用程序，可以通过在端点上显式禁用可访问性镜像来更改默认行为。

1. 使用 regedit.exe 打开 Windows 注册表编辑器。
2. 导航到 HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TWI
3. 创建一个名为 AccessibilityMirroring 的 DWORD 值，并将其值设置为 0 以禁用。

这将阻止在端点上设置的 Windows 可访问性设置传播到从该端点启动的所有 Seamless 应用程序。

适用于早期 VDA 和客户端的配置

对于较旧的 VDA（2503 及更高版本）和端点（适用于 Windows 的 CWA 2503.10 及更高版本），Seamless 应用程序的 Windows 可访问性设置传播默认禁用。

在 VDA 上，可以通过以下注册表设置启用 Seamless 应用程序的可访问性设置：

1. 使用 `regedit.exe` 打开 **Windows 注册表编辑器**。
2. 导航到 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\`
3. 创建一个名为 `AccessibilityMirroring` 的 **DWORD** 值，并将其值设置为 **1** 以启用。

使用 CWA 2503，无缝应用程序的辅助功能设置在客户端也将默认禁用，可以通过以下注册表设置启用：

1. 使用 `regedit.exe` 打开 **Windows 注册表编辑器**。
2. 导航到 `HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TWI`
3. 创建一个名为 `AccessibilityMirroring` 的 **DWORD** 值，并将其值设置为 **1** 以启用。

> **注意：**
>
> 要使无缝应用程序的辅助功能设置正常运行，注册表项必须同时存在于 VDA 和客户端上。
>
> 无需额外的用户干预或配置即可为无缝应用程序启用新的辅助功能设置。

窗口拖动

在与无缝应用程序交互时（例如窗口拖动），我们区分客户端拖动和服务器端拖动。在大多数用例中，客户端拖动优于服务器拖动。客户端拖动将带来更流畅的体验，并且窗口拖动操作是在本地而不是在服务器上执行的。

在大多数情况下，HDX™ 会自动执行客户端拖动，但是，某些应用程序可能只允许服务器拖动。服务器拖动可以通过在拖动窗口时应用程序“后面”显示的黑条来识别。选择标题栏的不同部分通常会导致客户端拖动。

请参阅下文了解客户端拖动和服务器拖动之间的区别。

Google Chrome 等应用程序允许通过拖动其选项卡来重新排列它们。

在某些情况下，这可能也会导致服务器拖动。这是预期行为。

无缝应用程序的透明窗口

概述

从 Citrix Virtual Apps and Desktops 2511 开始，无缝应用程序现在支持透明窗口。 窗口透明度是一种视觉效果，它使窗口边框或整个应用程序窗口半透明而不是不透明，从而允许用户看到它们后面的内容，无论是桌面背景还是其他窗口。

{包含无缝透明应用程序的图像}

> **注意：**
>
> 在无缝应用程序中使用透明度可能会影响服务器可扩展性和带宽使用。为了获得最佳性能，如果可能，请禁用应用程序中的任何透明效果。

先决条件

无缝应用程序透明窗口支持的先决条件如下：

- 运行 CWA for Windows 2511 或更高版本的 Windows 端点
- 运行 VDA 2511 或更高版本的 Windows VDA

无缝应用程序的透明窗口支持可在以下 VDA 操作系统上使用：

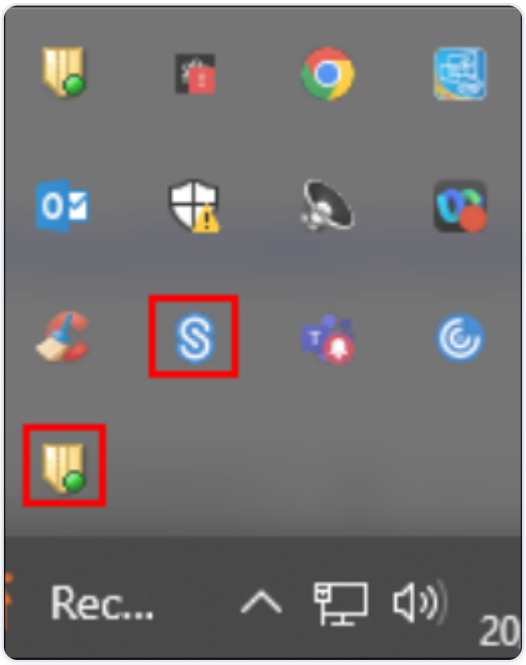
- Windows 服务器 2025
- Windows 11 单会话和多会话

> **注意：**
>
> - 请注意，对于发布在 Windows 10 或 Server 2022 及更早版本上的无缝应用程序，不支持透明窗口。
> - 无需额外配置，并且支持是开箱即用的。

系统托盘图标重定向

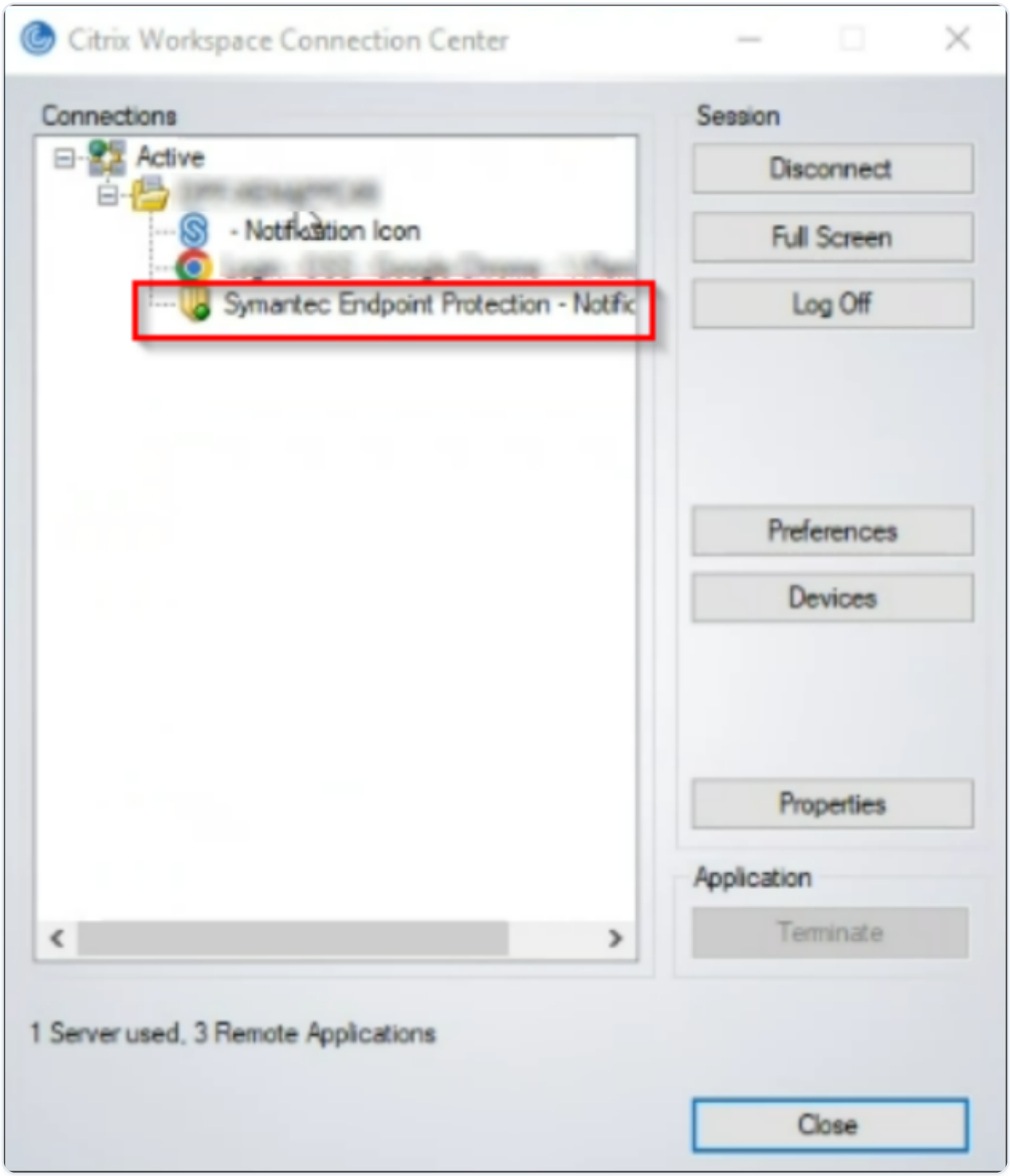
从 Citrix Virtual Apps and Desktops™ 2212 版本开始，VDA 上存在的远程系统托盘图标在使用无缝应用程序时将自动重定向到客户端。

托管无缝应用程序的 VDA 上的所有系统托盘图标都将重定向到端点。



在上面的示例中，Sharefile 和 Symantec 的标记系统托盘图标从 VDA 重定向到客户端。

这些图标也将出现在 Citrix Workspace™ 连接中心。



最终用户可以与这些重定向的系统托盘图标以与本地系统托盘图标相同的方式进行交互。

当使用托管在不同 VDA 上的无缝应用程序时，如果 VDA 具有相同的系统托盘图标，这可能会导致重复的系统托盘图标出现在端点上。

此行为默认启用，并且目前不可配置。

会话管理配置

默认情况下，当发布的应用程序关闭时，用户将从会话主机注销，并且会话将终止。如果用户使用在同一主机上运行的多个已发布的应用程序，则只有当所有应用程序都关闭时，会话才会终止。

在用户频繁漫游或预计全天频繁从同一主机访问打开的应用程序的场景中，可以通过更改会话管理行为来优化应用程序启动时间，以便在关闭已发布的应用程序时断开会话而不是注销。因此，允许用户重新连接到现有会话，而不是每次都启动新会话。

系统要求

- 控制平面
  - 思杰 DaaS 云
  - Citrix Virtual Apps and Desktops 2607 LTSR 或更高版本
- 虚拟投递代理
  - Windows：版本 2607 或更高版本

配置

会话管理

您可以通过在 Citrix 策略中配置以下设置来配置此行为：

- **关闭最后一个应用程序后断开已发布的应用程序会话**：此设置默认禁用。设置为“已启用”可将应用程序关闭行为从注销更改为断开连接。

自动重新打开应用程序

或者，可以在断开连接的会话中重新打开应用程序，通过减少重新连接会话时等待应用程序打开的时间，进一步优化应用程序启动时间。

要配置应用程序自动重新打开，请执行以下操作：

1. 创建名为 CTX-DSMRELAUNCH 的标记
2. 将该标记应用于您希望在断开连接的会话中自动重新打开的已发布应用程序。

有关标记的更多信息，请参阅标记文档。

注意事项

断开会话计时器

将应用程序关闭行为更改为断开连接可能会导致会话主机上保留的断开连接会话数量增加。因此，强烈建议配置断开连接计时器，以确保会话不会无限期地保持断开连接状态。 您可以通过以下选项之一配置断开连接超时：

1. 利用 Citrix 策略中的 断开连接会话计时器 – 多会话 和 断开连接会话计时器间隔 – 多会话 设置。
2. 使用组策略配置“**为断开连接的会话设置时间限制**”设置，该设置位于“**计算机配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 会话时间限制**”下。

WEM 多会话优化

强烈建议启用 WEM 多会话优化。此功能会在一分钟后自动降低断开连接会话的 CPU 和内存消耗，确保资源分配给活动用户并提高整体服务器性能。用户重新连接后，资源优先级和限制将相应恢复。

有关详细信息，请参阅 Workspace Environment Management (WEM) 文档。

发布应用程序

借助 Linux VDA 7.13 版，Citrix 将无缝应用程序功能添加到了所有受支持的 Linux 平台。使用此功能无需特定的安装过程。

> **提示：**
>
> 借助 Linux VDA 1.4 版，Citrix 添加了对非无缝已发布应用程序和会话共享的支持。

使用 Citrix Studio 发布应用程序

创建交付组或向现有交付组添加应用程序时，可以发布安装在 Linux VDA 上的应用程序。此过程与发布安装在 Windows VDA 上的应用程序类似。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 文档（基于所使用的 Citrix Virtual Apps and Desktops 版本）。

> **注意：**
>
> - 配置交付组时，请确保交付类型设置为 **Desktop and applications** 或 **Applications**。

- 建议您为应用程序和桌面交付创建单独的 VDA 和交付组。
- 要使用无缝应用程序，请勿在 StoreFront 上禁用无缝模式。无缝模式默认处于启用状态。如果您已通过设置“TWIMode=Off”将其禁用，请删除此设置，而不要将其更改为“TWIMode=On”。否则，您可能无法启动已发布的桌面。

限制

Linux VDA 不支持单个用户启动同一应用程序的多个并发实例。

在应用程序会话中，只有特定于应用程序的快捷方式才能按预期工作。

已知问题

发布应用程序时会遇到以下已知问题：

- 不支持非矩形窗口。窗口的角可能显示服务器端背景。
- 不支持预览已发布应用程序的窗口内容。
- 当您运行多个 LibreOffice 应用程序时，只有第一个启动的应用程序会显示在 Citrix Studio 上，因为这些应用程序共享进程。
- 已发布的基于 Qt5 的应用程序（例如“Dolphin”）可能不显示图标。要解决此问题，请参阅 `<https://wiki.archlinux.org/title/Qt>` 处的文章。
- Linux 应用程序通常有一个“关于”窗口，其中包含有关正在使用的应用程序的信息，并且这些窗口中通常包含用于获取更多信息的网页链接。单击“关于”窗口中的网页链接可以从已发布的应用程序（例如 **calc**、**gedit**、**calendar** 和 **LibreOffice Suite**）中启动 Web 浏览器。意外启动 Web 浏览器会绕过应用程序隔离并可能损害安全性。要解决此问题，请通过完成以下步骤更改默认 Web 浏览器：

  a. 在自定义位置创建 none.sh 文件，例如：

```
sudo mkdir /home/none


sudo touch /home/none/none.sh


sudo chmod +x /home/none/none.sh
```

b. 将以下行添加到 none.sh 文件中：

```
#!/bin/bash


echo "NONE"
```

c. 使用 sudo 创建 /etc/xdg/mimeapps.list 文件，然后将以下行添加到 mimeapps.list 文件中：

```
[Default Applications]


text/html=none.desktop


x-scheme-handler/http=none.desktop


x-scheme-handler/https=none.desktop


x-scheme-handler/about=none.desktop


x-scheme-handler/unknown=none.desktop
```

d. 使用 sudo 创建 /usr/share/applications/none.desktop 文件，然后将以下行添加到 none.desktop 文件中：

```
[Desktop Entry]


Encoding=UTF-8
```

```
Version=1.0

Type=Application

Terminal=false

Exec=/home/none/none.sh

Name=None

Icon=/home/none/none.sh
```

由于可以将 none.sh 文件放在自定义位置，请确保 none.desktop 可以正确引用 none.sh 文件。

故障排除

排查已发布的应用程序的会话注销问题

发布应用程序时，仅指定已发布的应用程序的主可执行文件。但是，某些应用程序可能会生成在后台运行的额外（子）进程，并且当主已发布的应用程序关闭时，这些进程不会被相应的主可执行文件关闭。额外进程也可能由执行的脚本或特定的注册表项（例如 `Run` 和 `RunOnceKey`）创建。这些应用程序可能会阻止正常注销，导致会话残留或挂起，并可能导致会话不关闭且用户无法注销。

在这种情况下，您需要使用 Citrix Director 重置或退出这些会话。

为了帮助识别和排查会话未正确注销的问题，Citrix 提供了三个注册表项。识别和排查由于这些问题导致会话未正确注销是一个三步过程：

1. 识别哪些会话的已发布应用程序正在阻止正常注销

2. 识别这些已发布的应用程序是否生成任何额外（子）进程
3. 将这些进程添加到指定的注册表项以防止它们阻止注销

步骤 2：识别这些已发布的应用程序是否生成任何额外的（子）进程

一旦确定某个已发布的应用程序会阻止正常注销，下一步是确定此应用程序在运行时是否会生成额外的进程。

您可以阅读 `HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` 以确定在关闭已发布的应用程序时是否有任何进程阻止正常注销。

在以下示例中，键 `LogoffCheckerBlockingProcess` 包含以下条目：

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

这些进程阻止了正常注销。

> **注意：**
>
> 将 替换为您要检查的会话的正确会话 ID。

步骤 3：将这些进程添加到指定的注册表项中，以防止它们阻止注销

您可以将这些进程添加到以下注册表项中，以防止它们在未来的会话中阻止注销：

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using
the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules

Type:REG_SZ
```

```
String:MyAppName.exe
```

有关 `LogoffCheckSysModules` 的更多信息，请参阅 从已发布的应用程序正常注销使会话处于活动状态。

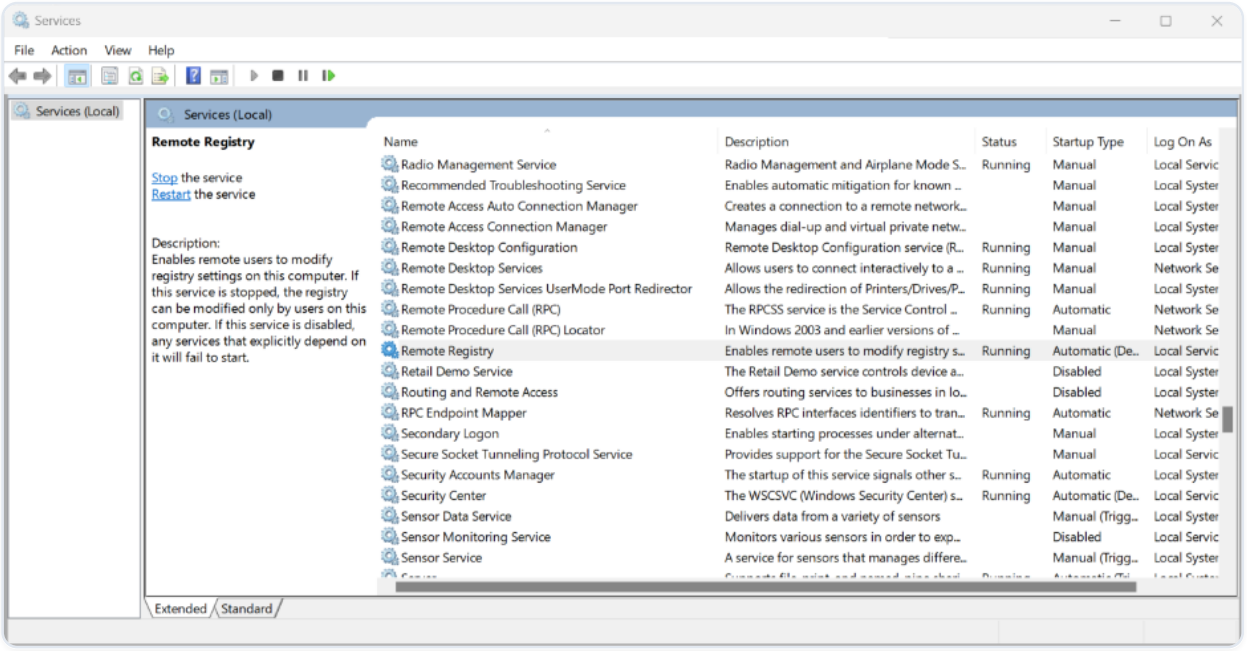
分步故障排除指南

1. 在测试中的 VDA 下启动远程注册表服务：

   a. 在“控制面板”中，选择 **“管理工具”>“服务”**。

   b. 右键单击 **“远程注册表服务”**，然后选择 **“属性”**。

   c. 在 **“启动类型”** 下，从下拉菜单中选择 **“自动”**。



2. 在测试 VDA 上关闭 Windows 防火墙，或者创建入站防火墙规则以启用端口 455：

   a. 在“控制面板”中，选择 **Windows Defender 防火墙 > 高级设置**。

   b. 右键单击**入站规则**，然后选择**新建规则**。

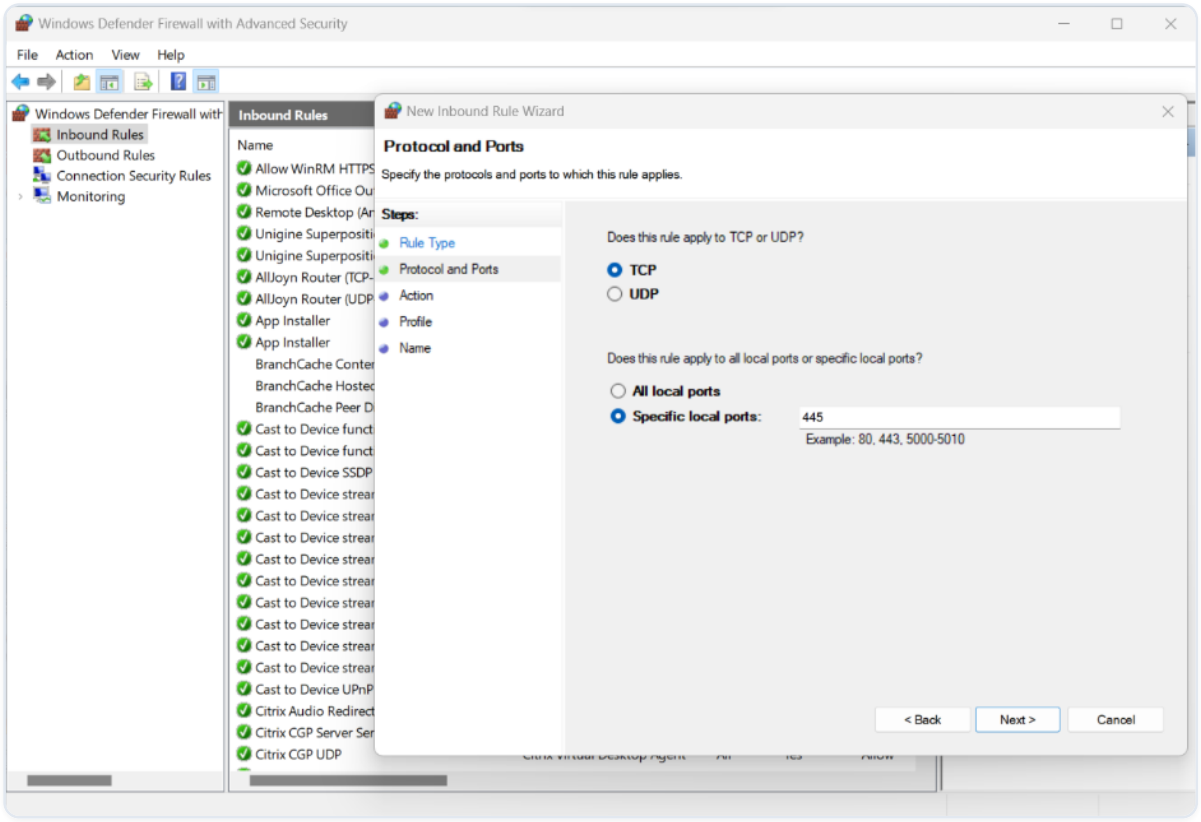
   c. 在**新建入站规则向导**中，选择**端口**。

   d. 在**协议和端口**页面上，选择 **TCP 和特定本地端口**。输入 `445` 作为本地端口。

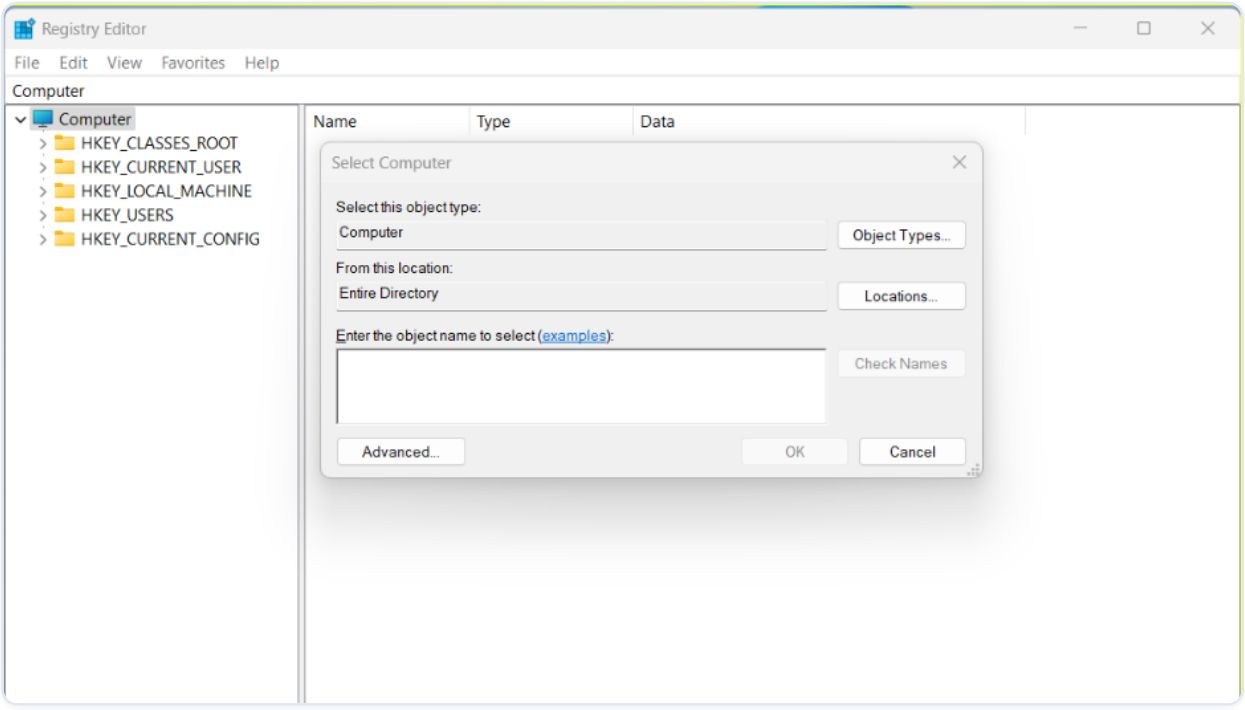
   e. 在**操作**页面上，选择**允许连接**。

   f. 选择要应用新入站规则的防火墙配置文件。

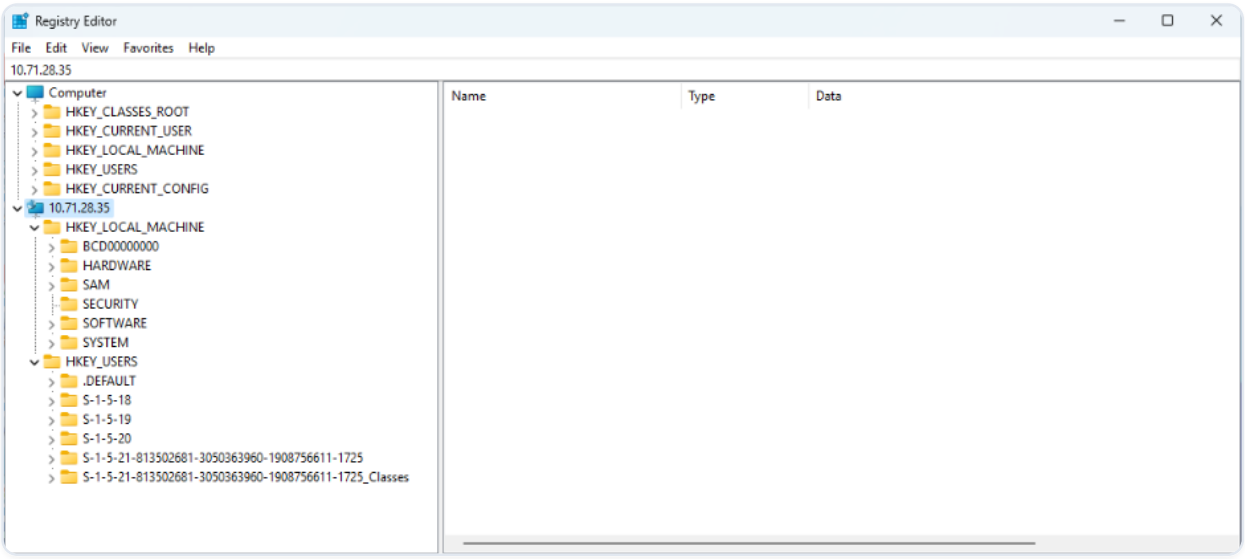
   g. 命名防火墙规则，然后选择**完成**以退出**新建入站规则向导**。



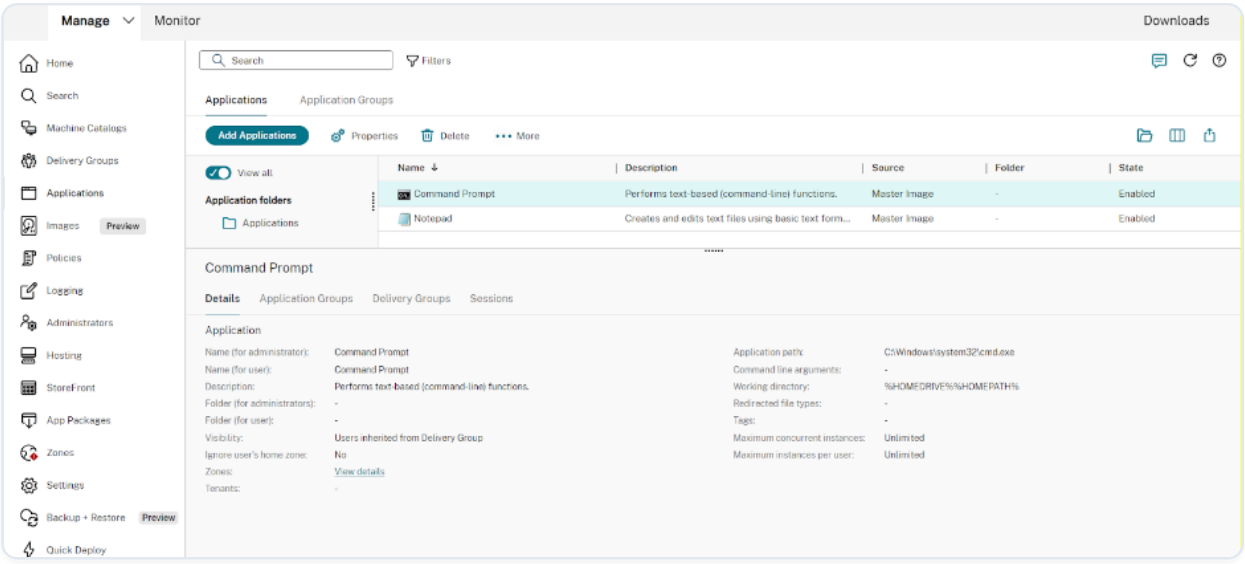
3. 从同一域中的另一台 VM（可以是 DC、DDC 或其他 VDA）运行 `Regedit` 并连接到远程注册表。



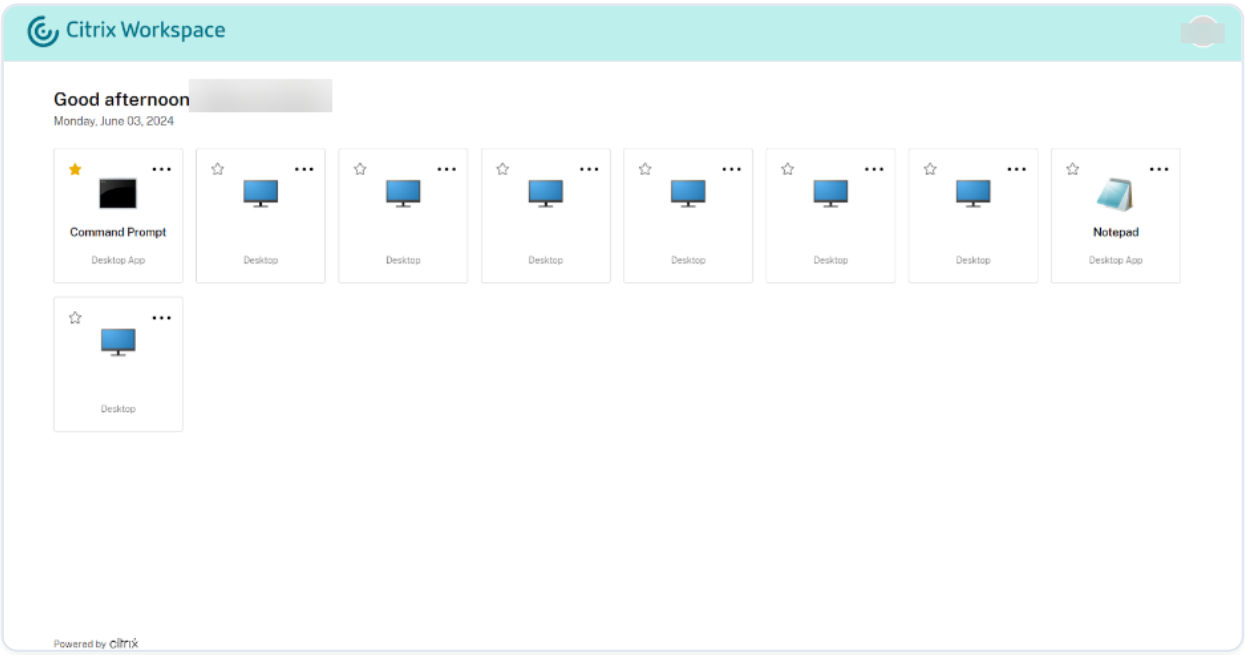
4. 输入测试 VDA 的 IP 地址，然后单击**确定**。`regedit` 树必须显示测试 VDA 的分支。



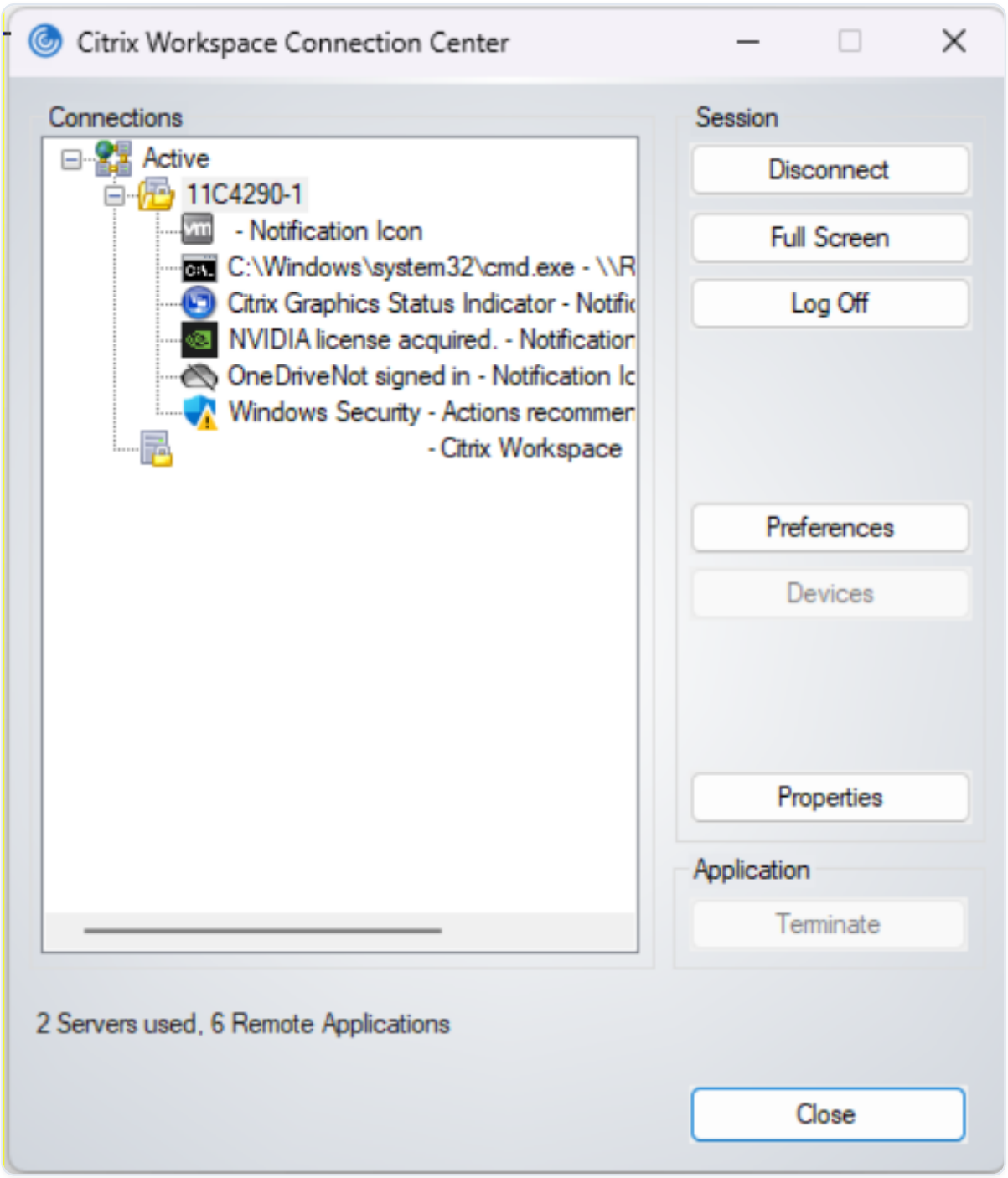
5. 打开**命令提示符**已发布的应用程序。



Citrix Workspace 上显示**命令提示符**应用程序。



6. 在客户端上打开**连接中心**。这用于在关闭已打开的无缝应用程序后，监控会话何时注销。我们可以在下图中看到命令提示符进程 `c:\Windows\system32\cmd.exe` 在远程 VDI 上处于活动状态。



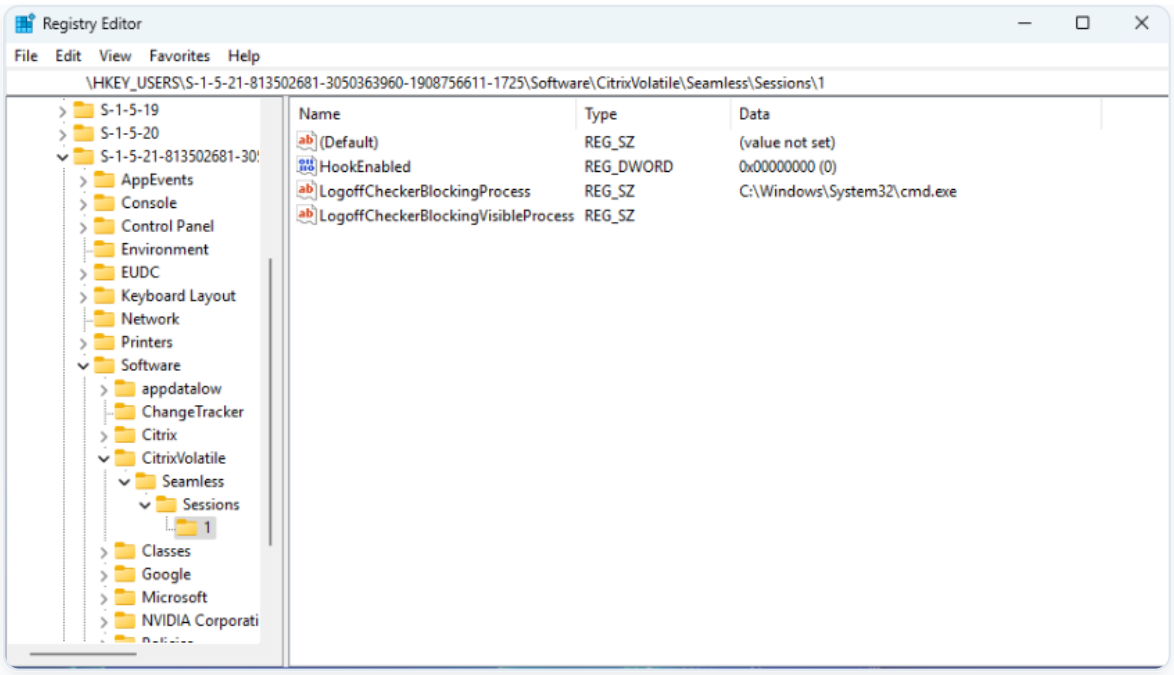
7. 从运行 **regedit** 的 VDA，转到以下远程 IP 位置： `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

> **注意：**

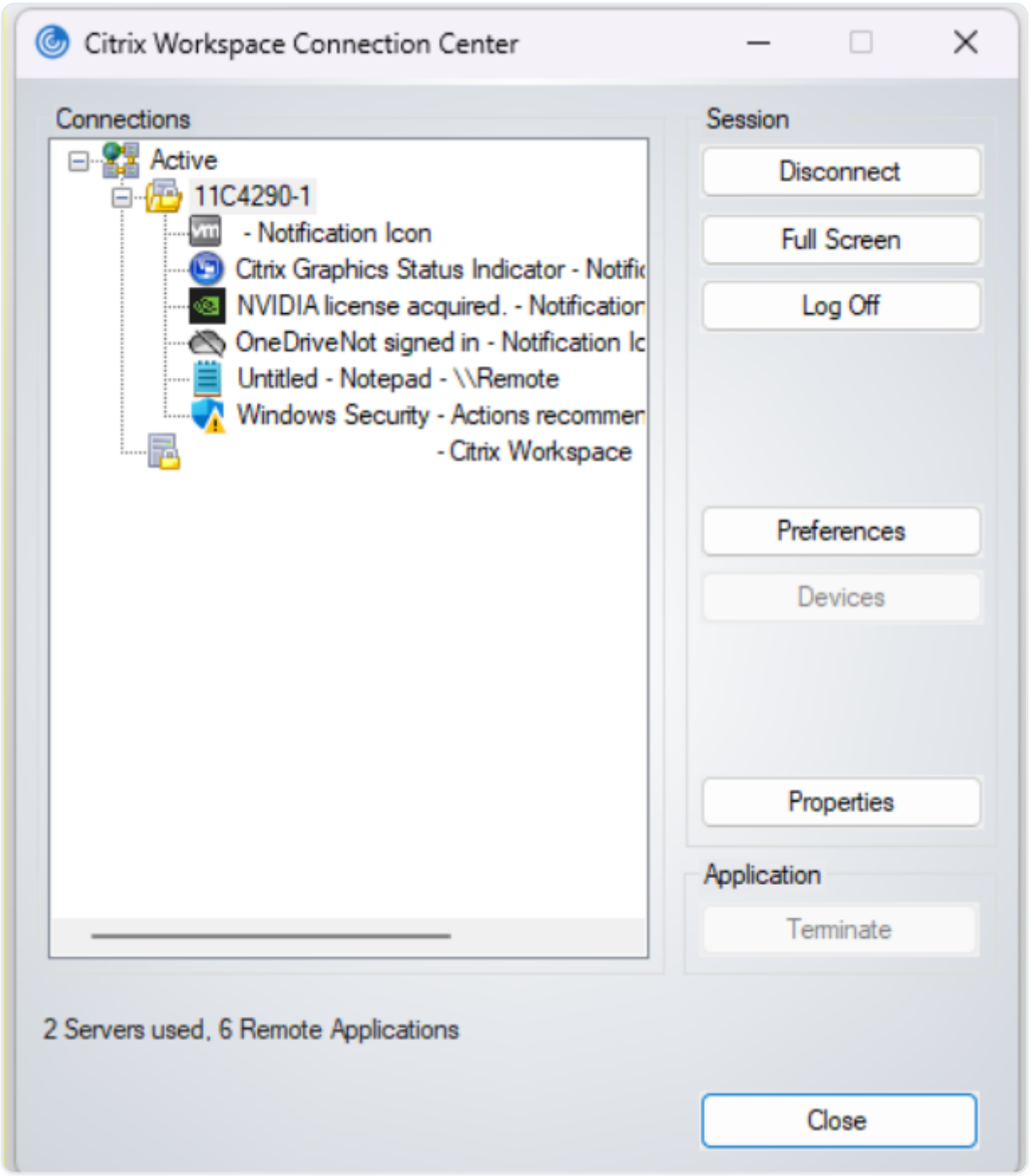
> 每次打开新会话时，此路径都会更改。

8. 这里有两个要读取的键（不要在此处更改它们）：**LogoffCheckBlockingProcess** 和 **LogoffCheckerBlockingVisibleProcess**。这些键显示任何阻止注销的程序。第一个必须显示 `C:\Windows\System32\cmd.exe`，因为它已打开且尚未关闭。

> **注意：**
>
> **LogoffCheckBlockingProcess** 和 **LogoffCheckerBlockingVisibleProcess** 不得手动编辑。手动编辑这些注册表值可能会导致会话不稳定。

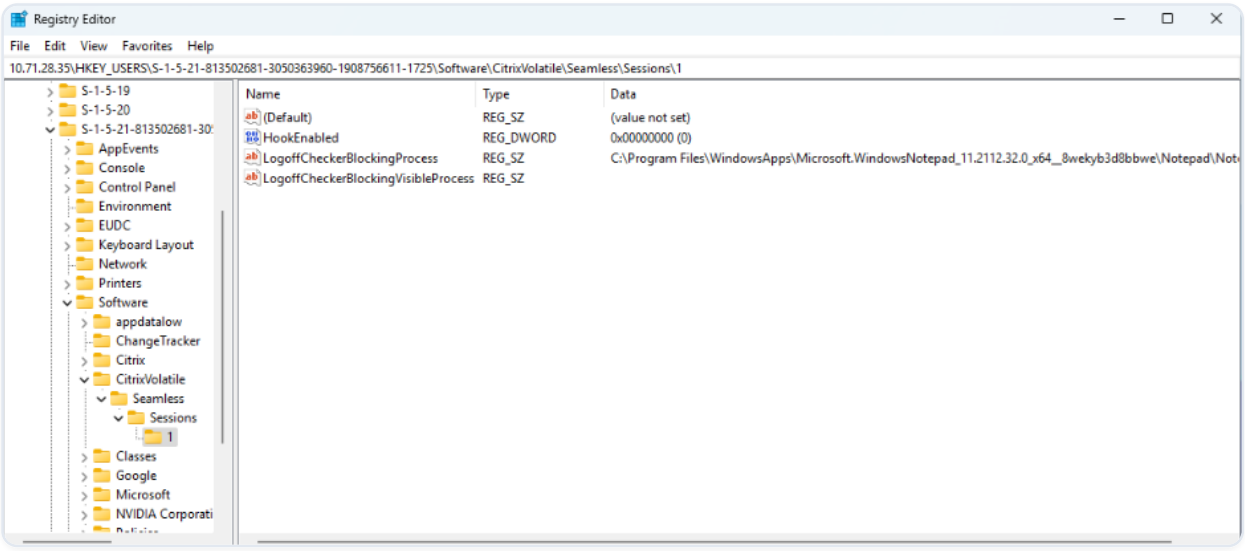


9. 单击右上角的 **X** 以退出 **Seamless CMD**。
10. 检查连接中心以查看会话是否关闭。可能需要长达 30 秒才能关闭。如果关闭，则没有应用程序或进程阻止正常注销。



11. 如果会话未关闭，请按 F5 刷新 **regedit** 输出。
12. 再次检查 **LogoffCheckBlockingProcess** 和 **LogoffCheckerBlockingVisibleProcess** 的内容。CMD 不应再存在，但应该有另一个列出的进程。当前阻止会话注销的任何进程都必须在此处显示。

    在这种情况下，在命令提示符关闭之前，**Notepad.exe** 是从已发布的命令提示符打开的，并且此远程记事本进程正在阻止正常注销。



13. 记下此可执行文件的路径以及它出现在哪个键中，并在远程树下的以下注册表项中输入它：

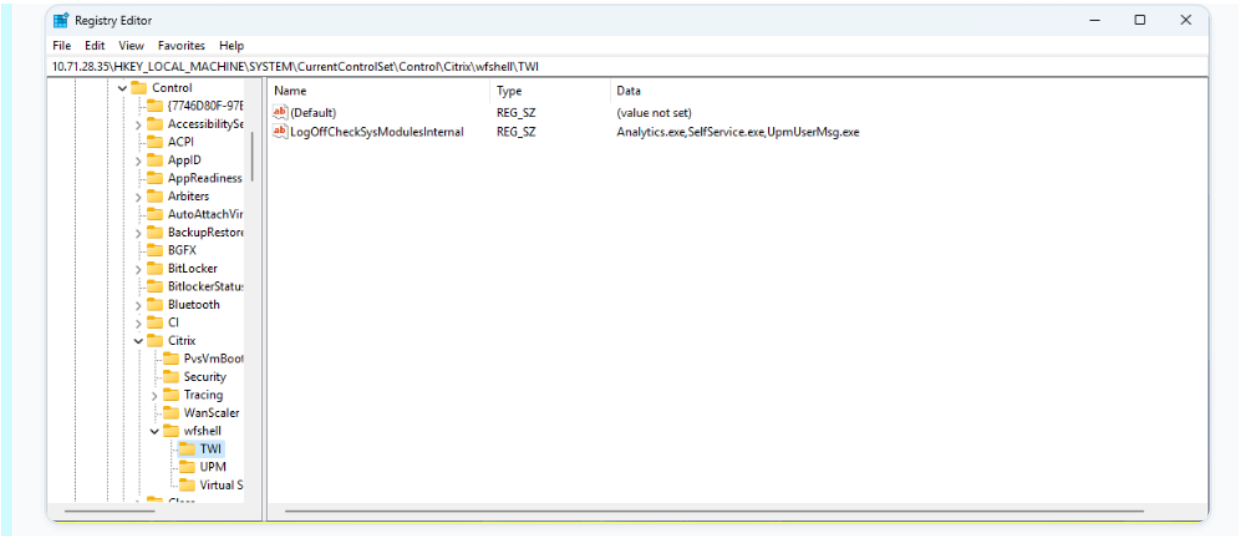
    - 如果它出现在 **LogoffCheckBlockingProcess** 中：

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - 如果它出现在 **LogoffCheckerBlockingVisibleProcess** 中：

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **注意：**
>
> 如果该键中已有一个或多个条目，请在末尾添加逗号，并将新条目放在逗号之后。



14. 从客户端的连接中心注销会话，然后重新打开远程应用程序。
15. 重复步骤 9-16，直到在关闭远程应用程序后 30 秒内自动注销会话。

> **注意：**

故障排除后，如有需要，请还原临时防火墙更改以允许远程注册表访问。

如何修改 LogonUI 以在打开已发布的应用程序时全尺寸查看 Windows 免责声明消息

在不发生身份验证直通的情况下，**LogonUI** 窗口的缩放功能得到了改进。**LogonUI** 窗口根据所使用的显示器分辨率和 DPI 设置进行缩放，这确保了完整的 **LogonUI** 窗口可见，而不会出现任何剪裁。

窗口大小（以像素为单位）也可以在注册表中手动设置。

1. 使用 **Run** 命令上的 `regedit` 打开 **Registry Editor**。
2. 转到 `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`。
3. 创建两个新的 DWORD 键：**LogonUIWidth** 和 **LogonUIHeight**。
4. 将这些键的值设置为 **LogonUI** 窗口所需的像素宽度和高度。

   手动设置 **LogonUI** 窗口大小时，自动缩放将被禁用。

注意：

这些注册表路径已从 2407 及更高版本开始更改。旧的注册表值将被忽略并已弃用。

默认情况下，**LogonUI** 窗口包含一个带有关闭按钮的标题栏，如果需要，最终用户可以使用该按钮断开会话连接。

禁用标题栏

您可以使用以下注册表项禁用 **LogonUI** 窗口中的标题栏：

1. 使用 `regedit` 在 **运行** 命令上打开注册表编辑器。
2. 转到 `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`。
3. 创建新的 DWORD 键：**LogonUICaption**，并将该键的值设置为 `0`。

   带有标题栏的 LogonUI 窗口 (/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/logonui-window-with-tilebar.png)

已发布的应用程序未显示

请参阅支持文章，以解决 已发布的应用程序无法启动或在启动期间消失 或 无法显示 的情况。

排查实例

其他无缝配置设置

在大多数情况下，默认服务器设置足以满足大多数应用程序的需求，并且已发布的应用程序不需要额外设置。

在某些情况下，需要额外配置，包括控制指定应用程序窗口的交互和显示，以及已发布的应用程序环境本身的设置。

> **注意：**
>
> 除非 Citrix 支持明确指示，否则 Citrix 不建议更改这些配置设置
>
> 这些设置在 无缝配置设置知识库文章 中有详细说明。

多媒体

HDX™ 技术栈通过两种互补的方法支持多媒体应用程序的交付：

- 服务器端渲染多媒体交付
- 客户端渲染多媒体重定向

此策略可确保您能够交付全范围的多媒体格式，提供出色的用户体验，同时最大限度地提高服务器可伸缩性以降低每用户成本。

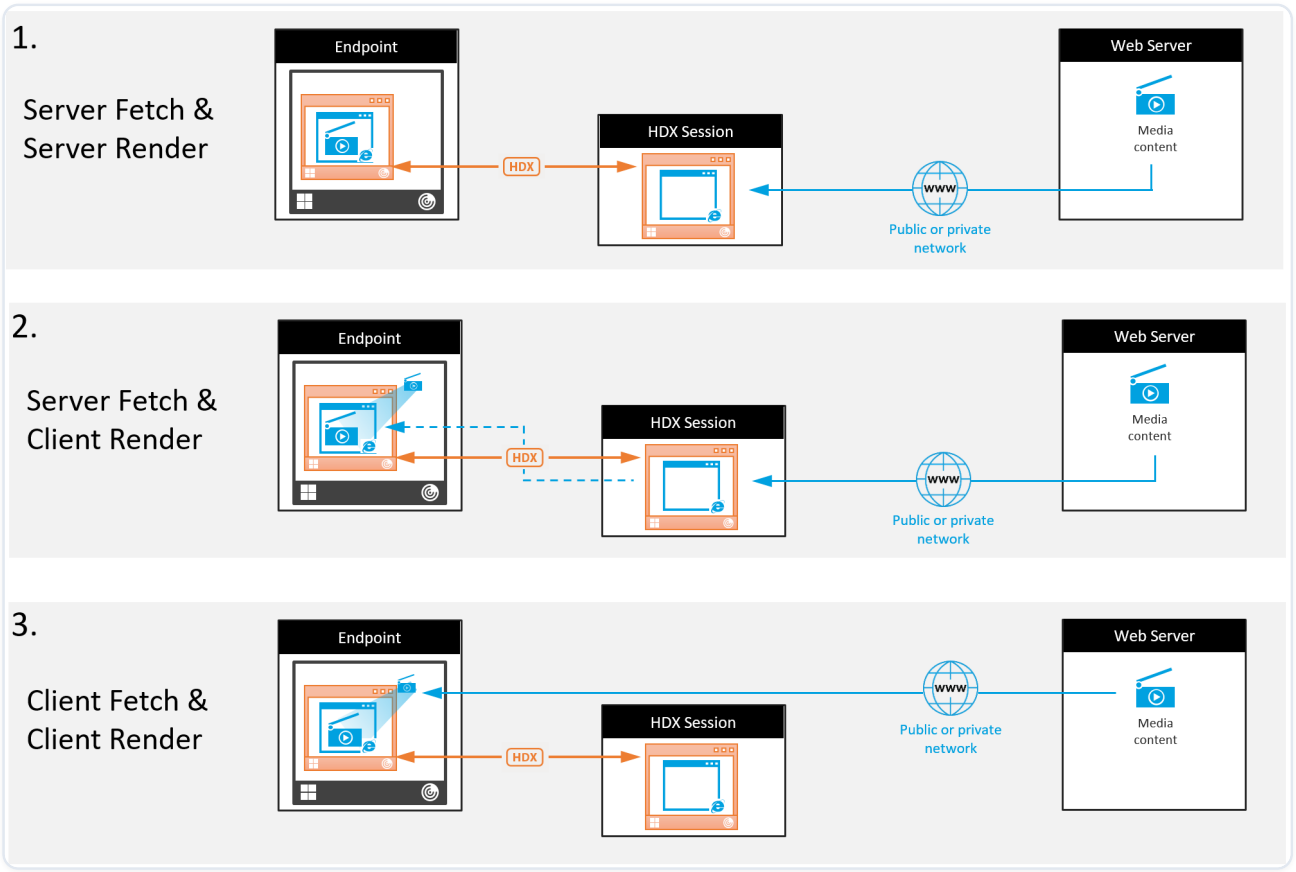
通过服务器渲染的多媒体交付，音频和视频内容由应用程序在 Citrix Virtual Apps and Desktops 服务器上解码和渲染。然后，内容使用 ICA 协议压缩并交付到用户设备上的 Citrix Workspace 应用程序。此方法提供了与各种应用程序和媒体格式的最高兼容性。由于视频处理是计算密集型的，因此服务器渲染的多媒体交付极大地受益于板载硬件加速。例如，对 DirectX 视频加速 (DXVA) 的支持通过在单独的硬件中执行 H.264 解码来分担 CPU 负载。Intel Quick Sync、AMD RapidFire 和 NVIDIA NVENC 技术提供硬件加速的 H.264 编码。

由于大多数服务器不提供任何用于视频压缩的硬件加速，如果所有视频处理都在服务器 CPU 上完成，服务器可伸缩性会受到负面影响。通过将许多多媒体格式重定向到用户设备进行本地渲染，可以保持较高的服务器可伸缩性。

- Windows Media 重定向可为通常与 Windows Media Player 关联的各种媒体格式分担服务器负载。
- HTML5 视频已变得流行，Citrix® 引入了一种针对此类内容的重定向技术。我们建议对使用 HTML5、HLS、DASH 或 WebRTC 的网站使用浏览器内容重定向。
- 您可以将通用联系重定向技术（主机到客户端重定向和本地应用程序访问）应用于多媒体内容。

综合这些技术，如果您不配置重定向，HDX 将执行服务器端渲染。 如果您配置重定向，HDX 将使用服务器获取和客户端渲染或客户端获取和客户端渲染。如果这些方法失败，HDX 将根据需要回退到服务器端渲染，并受回退预防策略的约束。

示例场景



场景 1.（服务器获取和服务器渲染）：

1. 服务器从其源获取媒体文件，解码，然后将内容呈现给音频设备或显示设备。
2. 服务器分别从显示设备或音频设备中提取呈现的图像或声音。
3. 服务器可以选择性地压缩它，然后将其传输到客户端。

这种方法会带来高 CPU 成本、高带宽成本（如果提取的图像/声音未有效压缩），并且服务器可伸缩性较低。

Thinwire 和音频虚拟通道处理此方法。这种方法的优点是它降低了客户端的硬件和软件要求。使用这种方法，解码在服务器上进行，并且适用于更广泛的设备和格式。

场景 2.（服务器获取和客户端渲染）：

这种方法依赖于能够在媒体内容解码并呈现给音频或显示设备之前对其进行拦截。压缩的音频/视频内容会发送到客户端，并在客户端进行解码和本地呈现。这种方法的优点是，这些被卸载到客户端设备，从而节省了服务器上的 CPU 周期。

但是，它也为客户端引入了一些额外的硬件和软件要求。客户端必须能够解码它可能接收的每种格式。

场景 3.（客户端获取和客户端渲染）：

这种方法依赖于能够在媒体内容 URL 从源获取之前对其进行拦截。URL 会发送到客户端，并在客户端获取、解码和本地呈现媒体内容。这种方法在概念上很简单。它的优点是既节省了服务器上的 CPU 周期，又节省了带宽，因为服务器只发送控制命令。但是，媒体内容并非总是可供客户端访问。

框架和平台：

单会话操作系统（Windows、Mac OS X 和 Linux）提供多媒体框架，可加快多媒体应用程序的开发。此表列出了一些更流行的多媒体框架。每个框架将媒体处理分为多个阶段，并使用基于管道的架构。

框架	平台
DirectShow	Windows (98 及更高版本)
媒体基础	Windows (Vista 及更高版本)
吉斯特里默	林纳克斯
快克时间	Mac 操作系统 X

支持媒体重定向技术的双跳

音频重定向	否
浏览器内容重定向	否
HDX 网络摄像头重定向	是
HTML5 视频重定向	是
Windows Media 重定向	是

音频功能

您可以配置以下 Citrix 策略设置并将其添加到优化 HDX 音频功能的策略中。有关用法详细信息以及与其他策略设置的关系和依赖项，请参阅音频策略设置、带宽策略设置和多流连接策略设置。

自适应音频

借助自适应音频，您无需手动配置 VDA 上的音频质量策略。自适应音频可优化您的环境设置，并替换过时的音频压缩格式，以提供卓越的用户体验。

自适应音频默认启用。要禁用自适应音频，请参阅音频策略设置。

重要提示：

当需要实时音频应用程序时，Citrix® 建议使用用户数据报协议 (UDP) 而非 TCP 传输音频。以下音频传输选项可通过 UDP 使用：

- 通过 UDP 传输音频
- HDX™ 自适应传输（Enlightened Data Transport）

使用 DTLS 的 UDP 音频加密仅在 Citrix Gateway 和 Citrix Workspace™ app 之间可用。因此，有时可能更倾向于使用 TCP 传输。TCP 支持从 VDA 到 Citrix Workspace app 的端到端 TLS 加密。

有关自适应音频和 UDP 音频的更多信息，请参阅通过 UDP 实时传输音频和音频 UDP 端口范围。

音频容错模式

从 2308 版本开始，容错模式支持音频。当用户通过存在延迟和数据包丢失的网络连接时，此功能可增强实时流媒体的用户体验，并提高通过 EDT 传输的音频质量。

有关容错模式和 EDT 的更多信息，请参阅 Citrix Virtual Apps and Desktops 文档中的其他信息。

音频容错模式默认启用。如果已禁用或要重新启用，请完成以下步骤：

1. 启用HDX 自适应传输 (EDT)。
2. 启用音频容错模式。

客户端要求和设置

以下是支持容错模式的最低 Citrix Workspace 应用程序版本：

- 适用于 Windows 的 Citrix Workspace 应用程序 2309

- 适用于 Linux 的 Citrix Workspace 应用程序 2311
- 适用于 Mac 的 Citrix Workspace 应用程序 2311

此外，请注意以下事项：

- (可选) 对于 Citrix Workspace 应用程序和 VDA 之间的直接连接，需要在 VDA 上启用 DTLS。
- (可选) 对于远程连接，Citrix Gateway Service 或 NetScaler Gateway 也必须支持容错模式。

音频质量

通常，通过向用户设备发送更多音频数据，更高的音质会消耗更多的带宽和服务器 CPU 利用率。声音压缩允许您平衡音质与整体会话性能；使用 Citrix 策略设置来配置应用于声音文件的压缩级别。

默认情况下，当使用 TCP 传输时，**音频质量策略**设置设为“高 - 高清音频”。当使用 UDP 传输（推荐）时，该策略设为“中 - 针对语音优化”。**高清音频**设置提供高保真立体声，但比其他质量设置消耗更多带宽。请勿将此音频质量用于非优化的语音聊天或视频聊天应用程序（例如软电话）。原因是它可能会在音频路径中引入不适合实时通信的延迟。无论选择何种传输协议，我们都建议将“针对语音优化”策略设置用于实时音频。

当带宽受限时（例如卫星或拨号连接），将音频质量降低到**低**会消耗最少的带宽。在这种情况下，请为低带宽连接上的用户创建单独的策略，以免对高带宽连接上的用户产生不利影响。

有关设置详细信息，请参阅音频策略设置。请记住在用户设备上启用客户端音频设置。

音频播放和录制带宽指南：

- 自适应音频（默认；推荐用于 VoIP 和所有用例）
  - 比特率：可变自适应
  - 通道数：播放为 2（立体声），麦克风捕获为 1（单声道）
  - 频率：48000 Hz
  - 位深度: 16 位
- 高质量
  - 比特率：播放时约 100 kbps（最小 75，最大 175 kbps）/ 麦克风捕获时约 70 kbps
  - 通道数：播放时 2（立体声），麦克风捕获时 1（单声道）
  - 频率：44100 Hz
  - 位深度: 16 位
- 中等质量

  - 比特率: 播放时约为 16 kbps (最小 20 kbps，最大 40 kbps)，麦克风捕获时约为 16 kbps
  - 通道数: 播放和捕获均为 1 (单声道)
  - 频率: 16000 Hz (宽带)
  - 位深度: 16 位
- 低质量
  - 比特率: 播放时约为 11 kbps (最小 10 kbps；最大 25 kbps)，麦克风捕获时约为 11 kbps
  - 通道数: 播放和捕获均为 1 (单声道)
  - 频率: 8000 Hz (窄带)
  - 位深度: 16 位

EDT 容错模式的音频质量增强器

从 2507 版本开始，EDT 自适应音频的音频质量增强器默认启用 音频容错模式。

音频质量增强器可在短暂的网络中断期间保持清晰的音频。此功能可适应网络条件，以确保在播放和录制期间提供一致的音频性能。

> **注意：**
>
> 自适应音频 必须启用此功能才能工作。

客户端音频重定向

要允许用户通过用户设备上的扬声器或其他声音设备接收来自服务器上应用程序的音频，请将**客户端音频重定向**设置保留为**允许**。这是默认设置。

客户端音频映射会给服务器和网络带来额外负载。但是，禁止客户端音频重定向会禁用所有 HDX 音频功能。

有关设置详细信息，请参阅音频策略设置。请记住在用户设备上启用客户端音频设置。

客户端麦克风重定向

要允许用户使用用户设备上的麦克风等输入设备录制音频，请将“**客户端麦克风重定向**”设置保留为默认值（允许）。

为安全起见，当用户不信任的服务器尝试访问麦克风时，用户设备会提醒其用户。用户可以在使用麦克风之前选择接受或拒绝访问。用户可以在 Citrix Workspace 应用程序上禁用此警报。

有关设置详细信息，请参阅音频策略设置。请记住在用户设备上启用客户端音频设置。

音频即插即用

“音频即插即用”策略设置允许或阻止使用多个音频设备录制和播放声音。此设置默认情况下处于“**已启用**”状态。音频即插即用功能使音频设备能够被识别。即使设备在用户会话启动后才插入，也能被识别。

此设置仅适用于 Windows 多会话操作系统计算机。

有关设置详细信息，请参阅音频策略设置。

音频重定向带宽限制和音频重定向带宽限制百分比

“音频重定向带宽限制”策略设置指定了会话中播放和录制音频的最大带宽（以千比特每秒为单位）。

“音频重定向带宽限制百分比”设置指定了音频重定向的最大带宽，该带宽是总可用带宽的百分比。

默认情况下，这两个设置都指定为零（无最大值）。如果同时配置了这两个设置，则使用带宽限制较低的那个。

有关设置详细信息，请参阅带宽策略设置。请记住在用户设备上启用客户端音频设置。

通过 UDP 实时传输的音频和音频 UDP 端口范围

默认情况下，允许通过用户数据报协议 (UDP) 实时传输音频（在安装时选择）。它在服务器上打开一个 UDP 端口，用于使用通过 UDP 实时传输的音频的连接。如果存在网络拥塞或数据包丢失，我们建议为音频配置 UDP/RTP，以确保最佳的用户体验。对于任何实时音频（例如软电话应用程序），UDP 音频优于 EDT。UDP 允许数据包丢失而无需重新传输，从而确保在高数据包丢失的连接上不会增加延迟。

> **重要提示：**
>
> 当 Citrix Gateway 不在路径中时，通过 UDP 传输的音频数据不会加密。如果 Citrix Gateway 配置为访问 Citrix Virtual Apps and Desktops™ 资源，则端点设备与 Citrix Gateway 之间的音频流量将使用 DTLS 协议进行保护。

> 音频 UDP 端口范围指定了 Windows VDA 用于与用户设备交换音频数据包的端口号范围。

默认情况下，范围是 16500 到 16509。

> **注意：**
>
> 如果自适应音频不需要通过 UDP 实时传输音频，Citrix 建议将策略设置配置为“已禁用”。这有助于避免 Citrix Workspace 应用程序客户端请求打开 UDP 连接或触发不必要的 Citrix Workspace 应用程序客户端防火墙配置对话框窗口出现。

> 有关通过 UDP 实时传输音频的设置详细信息，请参阅音频策略设置。有关音频 UDP 端口范围的详细信息，请参阅多流连接策略设置。请记住在用户设备上启用客户端音频设置。

通过 UDP 传输音频需要 Windows VDA。有关 Linux VDA 上支持的策略，请参阅策略支持列表。

用户设备的音频设置策略

1. 按照配置组策略对象管理模板中的说明加载组策略模板。
2. 在组策略编辑器中，展开**管理模板 > Citrix 组件 > Citrix Workspace > 用户体验**。
3. 对于**客户端音频设置**，选择**未配置**、**已启用**或**已禁用**。
   - **未配置**。默认情况下，音频重定向使用高质量音频或以前配置的自定义音频设置启用。
   - **已启用**。使用选定的选项启用音频重定向。
   - **已禁用**。禁用音频重定向。
4. 如果选择**已启用**，请选择一种音质。对于 UDP 音频，请使用**中等**（默认）。
5. 仅对于 UDP 音频，选择**启用实时传输**，然后设置要在本地 Windows 防火墙中打开的传入端口范围。
6. 要将 UDP 音频与 Citrix Gateway 结合使用，请选择 **允许通过网关进行实时传输**。使用 DTLS 配置 Citrix Gateway。有关详细信息，请参阅这篇文章。

作为管理员，如果您无法控制端点设备进行这些更改，请使用 StoreFront 中的 default.ica 属性来启用 UDP 音频。例如，对于自带设备或家用计算机。

1. 在 StoreFront 计算机上，使用记事本等编辑器打开 C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica。
2. 在 部分下进行以下条目。

   ; 此文本启用实时传输

EnableRtpAudio=真

; 此文本允许通过网关进行实时传输

EnableUDPThroughGateway=真

; 此文本将音频质量设置为中等

AudioBandwidthLimit=1

; UDP 端口范围

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509

如果您通过编辑 default.ica 启用用户数据报协议 (UDP) 音频，则该存储的所有用户都将启用 UDP 音频。

避免多媒体会议期间的回声

音频或视频会议中的用户可能会听到回声。回声通常发生在扬声器和麦克风距离过近时。因此，我们建议在音频和视频会议中使用耳机。

HDX 提供回声消除选项（默认启用），可最大程度地减少任何回声。回声消除的有效性对扬声器和麦克风之间的距离很敏感。请确保设备不要靠得太近或太远。

您可以更改注册表设置以禁用回声消除。有关信息，请参阅注册表管理的功能列表中的避免多媒体会议期间的回声。

软电话

软电话是充当电话界面的软件。您可以使用软电话通过互联网从计算机或其他智能设备拨打电话。通过使用软电话，您可以使用屏幕拨打电话号码并执行其他与电话相关的功能。

Citrix Virtual Apps and Desktops™ 支持多种交付软电话的替代方案。

- **控制模式**。托管软电话控制物理电话机。在此模式下，没有音频流量通过 Citrix Virtual Apps and Desktops 服务器。
- **HDX RealTime 优化软电话支持（推荐）**。媒体引擎在用户设备上运行，并且互联网协议语音流量以对等方式流动。例如，请参阅：
  - 适用于 Microsoft Teams 的 HDX 优化(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/multimedia/opt-ms-teams.html)

    - HDX RealTime Optimization Pack，它能够优化 Microsoft Skype for Business 的交付
    - Cisco Jabber Softphone for VDI（以前被称作 VXME）
    - 思科 Webex 会议 for VDI
    - Avaya VDI 至臻（以前称为 VDI Communicator）
    - Zoom VDI 插件
    - 捷信纯粹互动云
    - Nuance Dragon PowerMic 听写设备

- **本地应用程序访问**。Citrix Virtual Apps and Desktops 功能，允许软电话等应用程序在 Windows 用户设备上本地运行，但仍能与虚拟/已发布的桌面无缝集成。此功能将所有音频处理卸载到用户设备。有关详细信息，请参阅本地应用程序访问和 URL 重定向。
- **HDX RealTime 通用软电话支持**。基于 ICA 的互联网协议语音。

通用软电话支持

通用软电话支持使您能够在数据中心的 XenApp 或 XenDesktop 上托管未经修改的软电话。音频流量通过 Citrix ICA 协议（最好使用 UDP/RTP）传输到运行 Citrix Workspace 应用程序的用户设备。

通用软电话支持是 HDX RealTime 的一项功能。这种软电话交付方法在以下情况下特别有用：

- 没有可用的优化软电话交付解决方案，并且用户不在可以使用本地应用访问的 Windows 设备上。
- 优化交付软电话所需的媒体引擎未安装在用户设备上，或者不适用于用户设备上运行的操作系统版本。在这种情况下，通用 HDX RealTime 提供了一个有价值的备用解决方案。

使用 Citrix Virtual Apps and Desktops 交付软电话时，需要考虑以下两点：

- 软电话应用程序如何交付到虚拟/已发布的桌面。
- 音频如何传输到用户耳机、麦克风和扬声器，或 USB 电话机，以及如何从这些设备传输音频。

Citrix Virtual Apps and Desktops 包含多种技术来支持通用软电话交付：

- 针对语音优化的编解码器，用于实时音频的快速编码和带宽效率。
- 低延迟音频堆栈。
- 服务器端抖动缓冲区，用于在网络延迟波动时平滑音频。
- 服务质量 (Quality of Service) 的数据包标记 (DSCP 和 WMM)。
    - 用于 RTP 数据包 (第 3 层) 的 DSCP 标记

- 用于 Wi-Fi 的 WMM 标记

适用于 Windows、Linux、Chrome 和 Mac 的 Citrix Workspace 应用程序版本也支持语音通过 Internet 协议 (Voice over Internet Protocol)。适用于 Windows 的 Citrix Workspace 应用程序提供以下功能：

- 客户端抖动缓冲区 - 即使网络延迟波动，也能确保音频流畅。
- 回声消除 - 对于不使用耳机的员工，允许麦克风和扬声器之间的距离有更大的变化。
- 音频即插即用 - 音频设备无需在会话开始前插入。它们可以随时插入。
- 音频设备路由 - 用户可以将铃声定向到扬声器，但将语音路径定向到其耳机。
- 多流 ICA - 支持基于服务质量 (Quality of Service) 的灵活网络路由。
- ICA 支持四个 TCP 流和两个 UDP 流。其中一个 UDP 流支持通过 RTP 进行实时音频传输。

有关 Citrix Workspace 应用程序功能的摘要，请参阅 Citrix Receiver 功能矩阵。

系统配置建议

客户端硬件和软件：为了获得最佳音频质量，我们建议使用最新版本的 Citrix Workspace 应用程序和具有声学回声消除 (AEC) 功能的优质耳机。适用于 Windows、Linux 和 Mac 的 Citrix Workspace 应用程序版本支持语音通过 Internet 协议 (Voice over Internet Protocol)。此外，Dell Wyse 还为 ThinOS (WTOS) 提供语音通过 Internet 协议 (Voice over Internet Protocol) 支持。

CPU 考量：监视 VDA 上的 CPU 使用率，以确定是否需要为每个虚拟机分配两个虚拟 CPU。实时语音和视频是数据密集型的。配置两个虚拟 CPU 可减少线程切换延迟。因此，我们建议您在 Citrix Virtual Desktops™ VDI 环境中配置两个 vCPU。

拥有两个虚拟 CPU 并不一定意味着物理 CPU 数量翻倍，因为物理 CPU 可以在会话之间共享。

Citrix Gateway Protocol (CGP) 用于会话可靠性功能，也会增加 CPU 消耗。在高质量网络连接上，您可以禁用此功能以降低 VDA 上的 CPU 消耗。在功能强大的服务器上，上述任何步骤可能都不必要。

UDP 音频: 通过 UDP 传输的音频对网络拥塞和数据包丢失具有出色的容忍度。如果可用，我们建议使用它而不是 TCP。

LAN/WAN 配置: 正确的网络配置对于良好的实时音频质量至关重要。通常，您必须配置虚拟 LAN (VLAN)，因为过多的广播数据包可能会引入抖动。启用 IPv6 的设备可能会生成许多广播数据包。如果不需要 IPv6 支持，您可以在这些设备上禁用 IPv6。配置以支持服务质量。

WAN 连接使用设置: 您可以通过 LAN 和 WAN 连接使用语音聊天。在 WAN 连接上，音频质量取决于连接的延迟、数据包丢失和抖动。如果通过 WAN 连接向用户交付软电话，我们建议在数据中心和远程办公室之间使用 NetScaler® SD-WAN。这样做可以保持高服务质量。NetScaler SD-WAN 支持多流 ICA，包括 UDP。此外，对于单个 TCP 流，可以区分各种 ICA 虚拟通道的优先级，以确保高优先级实时音频数据获得优先处理。

使用 Director 或 HDX Monitor 验证您的 HDX 配置。

远程用户连接: Citrix Gateway 支持 DTLS 以本机方式（不封装在 TCP 中）交付 UDP/RTP 流量。为通过端口 443 的 UDP 流量双向打开防火墙。

编解码器选择和带宽消耗: 在用户设备和数据中心 VDA 之间，我们建议使用 **Optimized-for-Speech** 编解码器设置，也称为中等质量音频。在 VDA 平台和 IP-PBX 之间，软电话使用配置或协商的任何编解码器。例如：

- G711 提供良好的语音质量，但每个呼叫的带宽要求为 80 到 100 千比特每秒（取决于网络第 2 层开销）。
- G729 提供良好的语音质量，并且每个呼叫的带宽要求较低，为 30 到 40 千比特每秒（取决于网络第 2 层开销）。

将软电话应用程序交付到虚拟桌面

您可以通过两种方法将软电话交付到 XenDesktop® 虚拟桌面：

- 应用程序可以安装在虚拟桌面映像中。
- 应用程序可以使用 Microsoft App-V 流式传输到虚拟桌面。这种方法具有可管理性优势，因为虚拟桌面映像保持整洁。流式传输到虚拟桌面后，应用程序在该环境中运行，就像以常规方式安装一样。并非所有应用程序都与 App-V 兼容。

向用户设备交付音频以及从用户设备接收音频

通用 HDX RealTime 支持两种向用户设备交付音频以及从用户设备接收音频的方法：

- **Citrix 音频虚拟通道**。我们通常推荐使用 Citrix 音频虚拟通道，因为它专为音频传输而设计。
- **通用 USB 重定向**。如果用户设备通过 LAN 或类似 LAN 的连接回连到 Citrix Virtual Apps and Desktops 服务器，则支持带有按钮或显示屏（或两者兼有）的音频设备、人机接口设备 (HID)。

Citrix 音频虚拟通道

双向 Citrix 音频虚拟通道 (CTXCAM) 能够高效地通过网络传输音频。通用 HDX RealTime 从用户耳机或麦克风获取音频并进行压缩。然后，通过 ICA 将其发送到虚拟桌面上的软电话应用程序。同样，软电话的音频输出也会被压缩并沿另一个方向发送到用户耳机或扬声器。此压缩独立于软电话

本身使用的压缩（例如 G.729 或 G.711）。它使用 Optimized-for-Speech 编解码器（中等质量）完成。其特性非常适合 IP 语音。它具有快速编码时间，并且仅消耗大约每秒 56 千比特的网络带宽（每个方向 28 Kbps），峰值。此编解码器必须在 Studio 控制台中明确选择，因为它不是默认音频编解码器。默认是 HD 音频编解码器（高质量）。此编解码器非常适合高保真立体声配乐，但与 Optimized-for-Speech 编解码器相比，编码速度较慢。

通用 USB 重定向

Citrix 通用 USB 重定向技术（CTXGUSB 虚拟通道）提供了一种通用的远程连接 USB 设备的方法，包括复合设备（音频加 HID）和同步 USB 设备。此方法仅限于 LAN 连接的用户。原因是 USB 协议往往对网络延迟敏感，并且需要大量的网络带宽。同步 USB 重定向在使用某些软电话时效果很好。这种重定向提供了出色的语音质量和低延迟。但是，Citrix 音频虚拟通道是首选，因为它针对音频流量进行了优化。主要例外情况是当您使用带有按钮的音频设备时。例如，连接到用户设备并与数据中心进行 LAN 连接的 USB 电话。在这种情况下，通用 USB 重定向支持电话机或耳机上的按钮，这些按钮通过向软电话发送信号来控制功能。对于在设备本地工作的按钮没有问题。

音频诊断命令行工具

VDA 上的音频诊断命令行工具可用于查询与音频策略、配置和数据传输相关的会话数据。

用法

打开命令提示符，然后从 `C:\Program Files\Citrix\HDX\bin` 文件夹运行 `CtxAudio.exe`。

- 以管理员身份运行该工具会显示所有活动 ICA 会话的音频信息。
- 以非管理员身份运行该工具会显示当前用户的 ICA 会话音频信息。

输出

该工具会输出各种配置设置，这些设置有助于诊断会话中与音频相关的问题。

部分	描述
策略信息	应用于当前会话的音频策略。
设置信息	存储在注册表中的音频相关配置设置。
状态信息	应用于当前会话的音频状态、版本、编解码器和传输。
设备信息	会话中使用的设备名称、角色和状态。

> **注意：**
>
> 输出因您是在多会话 (TS) VDA 还是单会话 VDA (WSVDA) 上运行该工具而异。

限制

您在客户端上安装音频设备，启用音频重定向，然后启动 RDS 会话。音频文件可能无法播放，并显示错误消息。

作为一种解决方法，请在 RDS 计算机上添加注册表项，然后重新启动计算机。有关信息，请参阅注册表管理的功能列表中的音频限制。

浏览器内容重定向

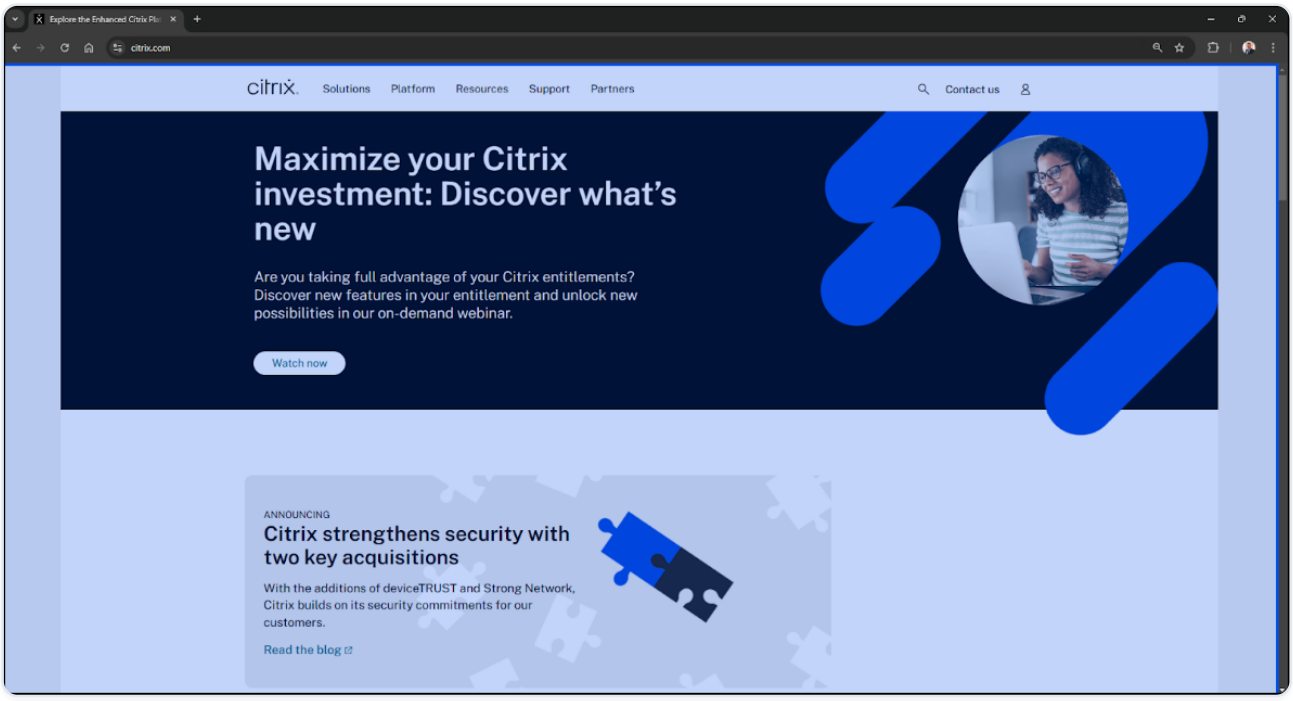
简介

浏览器内容重定向 (BCR) 提升了在 Citrix Virtual Apps and Desktops™ 环境中网页浏览的用户体验。通过将网页渲染卸载到用户的本地计算机，BCR 减少了服务器负载并提高了性能，尤其对于复杂或资源密集型网站。

工作原理

BCR 利用 Citrix Workspace™ 应用程序在用户设备上创建安全的浏览环境。当用户访问允许的网页时，浏览器窗口的视口会重定向到客户端。客户端浏览器引擎随后利用本地计算机的资源来渲染页面，从而实现更快的加载时间和更流畅的交互。

请注意，只有浏览器视口被重定向。视口是浏览器中显示内容的矩形区域。视口不包括地址栏、收藏夹工具栏或状态栏等内容。这些项目位于用户界面中，该界面仍在 VDA 中的浏览器上运行。



主要优势

浏览器内容重定向智能地管理网络流量，为您的用户提供卓越的体验，同时减轻您的基础设施的压力。

以下是它们如何使您的组织受益：

- **成本节约：** 将资源密集型网页卸载到用户设备，释放宝贵的服务器资源并减少带宽消耗。这意味着更低的硬件和网络成本。
- **增强用户体验：** 为您的用户提供更流畅、响应更快的浏览体验，即使是图形密集型网站。提供类似本机的性能，消除延迟并提高生产力。
- **提高安全性：** 维护安全环境，同时允许访问内部和外部资源。
- **提高灵活性：** 支持广泛的用例，从基本的网页浏览到需要代理遍历或 SSO 身份验证的复杂 Web 应用程序。使用 Citrix Web Studio™ 中的精细策略控制轻松管理重定向设置。

系统要求

服务器端组件

Citrix 虚拟应用和桌面

- 长期服务版本
  - 最低要求 - 任何非生命周期终止的 LTSR Citrix Virtual Apps and Desktops 版本
  - 推荐 - Citrix Virtual Apps and Desktops 2402 或更高版本

- 当前版本
  - 最低要求 - 任何非生命周期终止的 CR Citrix Virtual Apps and Desktops 版本
  - 推荐 - 最新版 Citrix Virtual Apps and Desktops

浏览器组件

- 浏览器
  - 微软 Edge
  - 谷歌浏览器
- 浏览器重定向扩展
  - Google Chrome 网上应用店
  - Microsoft Edge 附加组件
- 建议使用最新版本的浏览器以获得最佳体验

> **注意：**

> 要启用浏览器内容重定向或双向内容重定向，如果您打算使用 Microsoft Edge 附加组件商店中的浏览器重定向扩展，请确保您拥有 Virtual Delivery Agent (VDA) 2503 版本。对于较旧的 VDA 版本，您可以通过在 Microsoft Edge 浏览器中从 Chrome 网上应用店安装扩展来实现相同的功能。

> 上面提供的扩展链接是正式发布 (GA) 版本，适用于生产级部署。除了 GA 扩展之外，Citrix 还在 Google Chrome 网上应用店 上专门发布了一个 Beta (GA + 1) 扩展。

> Citrix 建议客户让测试用户使用 Beta 版本，以便对即将推出的更新进行测试并及早报告任何问题。这可确保在 GA 扩展正式发布时流程顺畅。

> 扩展版本通常与 Citrix Workspace App 版本匹配。

客户端组件

视窗

- Windows 10 或 11 版本

- Citrix Workspace 应用程序
  - 最低要求 - 任何未终止支持的 Citrix Workspace App
  - 推荐
    - 长期服务版本 - 适用于 Windows 的 Citrix Workspace App 2402 CU4 或更高版本，适用于 Windows 的 Citrix Workspace App 2507
    - 当前版本 - Citrix Workspace App 2405 或更高版本

> **注意：**
>
> - Citrix Workspace App Windows LTSR 1912 和 2203.1 版本不支持浏览器内容重定向。
> - 浏览器内容重定向所需的客户端浏览器引擎默认安装在 Citrix Workspace App 当前版本中
> - 浏览器内容重定向所需的客户端浏览器引擎默认不安装在 Citrix Workspace App 2402 LTSR 版本中。管理员可以利用 ADDLOCAL 开关在 Citrix Workspace App 之上安装 BCR 浏览器组件。
> - 从适用于 Windows 的 Citrix Workspace app 2507 开始，浏览器内容重定向 (BCR) 作为模块化组件进行管理，但仍与 Citrix Workspace App 打包在一起。BCR 组件现在也默认安装在 LTSR 版本上，确保 CR 和 LTSR 之间的一致性。此外，还将发布独立的 BCR 软件包，以应对在常规 Citrix Workspace app 发布周期之外需要独立更新或临时修补程序的情况。有关更多详细信息，请参阅 Citrix Workspace App Windows documentation。

林纳克斯

- Citrix Workspace 应用程序
  - 最低要求 - 任何未终止支持的 Citrix Workspace App
  - 推荐 - Citrix Workspace App 2408 或更高版本 有关更多详细信息，请参阅 适用于 Linux 的 Citrix Workspace App 文档。

> **注意：**

从适用于 Linux 的 Citrix Workspace app 2601 开始，浏览器内容重定向 (BCR) 作为模块化组件进行管理。BCR 组件将继续与适用于 Linux 的 Citrix Workspace app 默认打包并安装，确保一致的用户体验。此外，还将发布独立的 BCR 软件包，以应对在常规 Citrix Workspace app 发布周期之外需要独立更新或临时修补程序的情况。有关更多详细信息，请参阅 Citrix Workspace App Linux documentation

ChromeOS

- Citrix Workspace 应用程序
  - 来自 Chrome 网上应用店的最新版本

MacOS

- Citrix Workspace 应用程序
  - 最低要求 - 适用于 Mac 的 Citrix Workspace App 2411 或更高版本

注意：

- 对于 macOS，浏览器内容重定向包独立于 Citrix Workspace 应用程序，并且始终是最新版本。因此，该包将与高于指定最低版本的多个 CWA 版本兼容。
- 由于不依赖于适用于 Mac 的 Citrix Workspace 应用程序，浏览器内容重定向的版本号将与适用于 Mac 的 Citrix Workspace 应用程序版本不匹配。
- 客户端浏览器引擎未与适用于 Mac 的 Citrix Workspace 应用程序打包在一起。请在 Citrix 下载 上下载并安装适用于 Mac 的客户端。
- Intel 和 ARM 软件包是独立的。因此，您需要安装适合 macOS 端点的相应版本。
- 从适用于 Mac 的 Citrix Workspace 应用程序 2511.1 开始，模块化 BCR 组件默认安装，但未与 Citrix Workspace 应用程序打包在一起，从而无需从 Citrix 下载手动下载和安装该组件。独立的 BCR 软件包将发布，以应对在常规 Citrix Workspace 应用程序发布周期之外需要独立更新或临时修补程序的情况。有关更多详细信息，请参阅 适用于 Mac 的 Citrix Workspace 应用程序文档。

配置步骤

1. 根据系统要求安装客户端和服务器端组件
   - 有关扩展部署的详细信息，请参阅“扩展部署”部分

2. 配置 Studio 策略

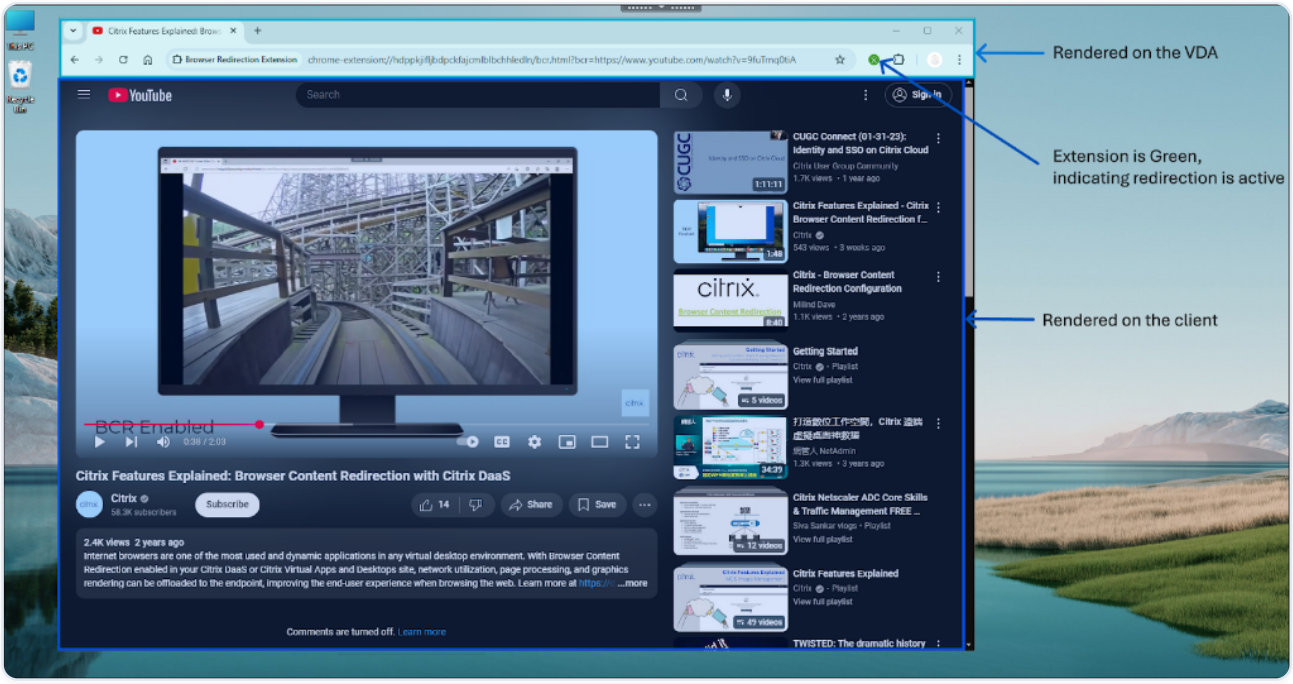
   - Web Studio 策略提供了一种精细的方式来配置浏览器内容重定向，以适应各种用例。
   - 基本策略允许管理员配置需要通过浏览器内容重定向允许/不允许的 URL。
   - URL 可以使用通配符进行配置。

3. 打开受支持的 Web 浏览器并导航到允许的 URL。

   - 如果在允许列表中找到匹配项，则网站将被重定向到客户端。
   - Citrix Workspace 应用程序将视口融合到 VDA 端浏览器上，以提供无缝体验。

4. 扩展程序图标的颜色指示内容重定向的状态

   - 绿色：活动且已连接
   - 灰色：在当前选项卡上不活动/空闲
   - 红色：损坏/不工作



注意：

- HTML5 视频重定向和浏览器内容重定向是独立的功能。此功能不需要 HTML5 视频重定向策略即可工作。但是，Citrix HDX™ HTML5 视频重定向服务用于浏览器内容重定向。
- 我们建议通过 Web Studio 而不是注册表项进行所有配置。

功能和配置选项

浏览器内容重定向提供了多种配置方式，以适应各种客户环境的使用场景。有关策略设置的详细信息，请参阅浏览器内容重定向策略设置。

重定向机制

客户端获取客户端渲染

默认情况下，浏览器内容重定向在此模式下运行，即客户端浏览器引擎直接访问网页。这需要客户端网络对网页的必要访问。客户端获取客户端渲染场景将所有网络、CPU 和 RAM 使用量从 Citrix VDA 卸载到客户端，是配置浏览器内容重定向的最优方式。

策略配置选项

- 浏览器内容重定向：允许
- 浏览器内容重定向 ACL 配置
  - 指定需要重定向的 URL。默认情况下，YouTube 是唯一配置为重定向的网站
- 浏览器内容重定向阻止列表配置
  - 可选配置选项，用于阻止任何特定的 URL/子 URL 进行重定向。结合上述选项使用此选项可实现最大程度的自定义。

服务器获取客户端渲染

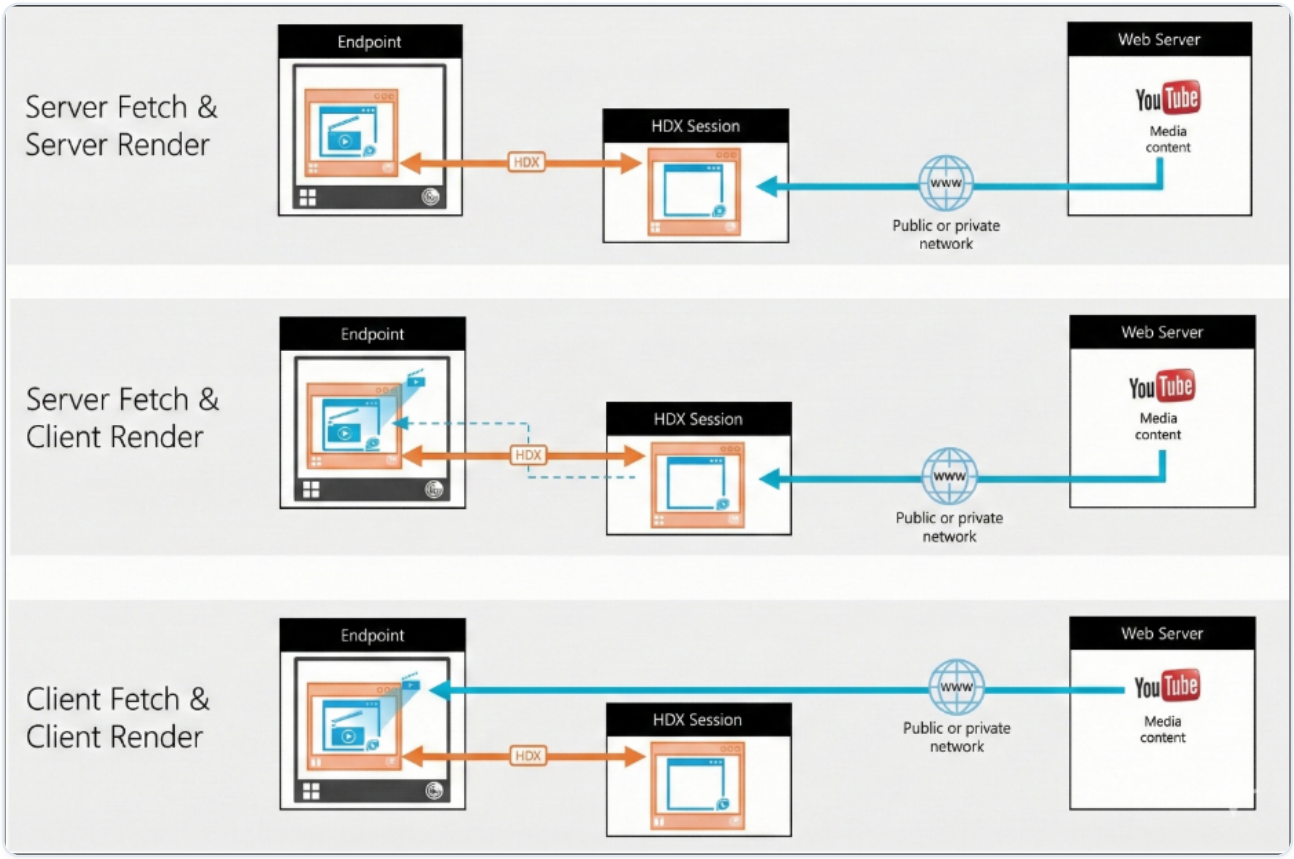
在这种情况下，客户端浏览器引擎通过 VDA 使用虚拟通道联系 Web 服务器并从中获取内容。当客户端没有 Internet 访问权限时（例如，瘦客户端），此选项非常有用。VDA 上的 CPU 和 RAM 消耗较低，但 ICA® 虚拟通道会消耗带宽。

在此场景中有三种操作模式。“代理”一词是指 VDA 访问以获取 Internet 访问权限的代理设备。

策略配置选项

- 除了“客户端获取客户端渲染”部分中指定的策略外，还请配置以下内容
- 浏览器内容重定向代理配置
  - **直接或透明：** 如果要利用服务器获取客户端渲染，并且可以从 VDA 直接访问或通过透明代理访问网页，请配置此选项。策略中应配置关键字“DIRECT”。
  - **显式代理：** 如果要利用服务器获取客户端渲染，并且可以从 VDA 显式代理访问网页，请配置此选项。
  - **PAC 文件：** 如果您依赖 PAC 文件，请配置此选项，VDA 中的浏览器可以自动选择合适的代理服务器来获取指定的 URL。

回退模式



有时客户端重定向可能会失败。例如，如果客户端计算机没有直接 Internet 访问权限，则错误响应可能会返回到 VDA。在这种情况下，VDA 上的浏览器可以重新加载并在服务器上渲染页面。

身份验证处理

身份验证站点

在浏览器内容重定向的当前实现中，无论重定向机制如何，都需要配置身份验证站点，以便浏览器内容重定向能够处理网站登录。

示例：

1. 当浏览器内容重定向 ACL 配置中仅配置了 `<https://www.youtube.com/*/>` 且未配置身份验证站点时，BCR 将在登录网站时回退到服务器端渲染，并将在那里继续。
2. 在这种情况下，为了让 BCR 处理身份验证站点，请根据需要配置 `<https://www.accounts.google.com/*/>` 和任何其他身份验证站点，例如 IdP 网站。每个网站的登录方式都不同，因此请务必列出
3. 配置后，BCR 将处理身份验证。例如，通过客户端获取客户端渲染，身份验证也将从客户端浏览器引擎进行，以实现无缝登录体验。

策略配置选项

除了重定向机制部分中提到的策略之外，还要配置浏览器内容重定向身份验证站点策略

注意：

- BCR 客户端浏览器在重定向窗口关闭后不会保留 Cookie（包括身份验证）。这表现为在 BCR 窗口完全关闭并重新打开时需要重新登录网站。
- BCR 客户端浏览器不读取 VDA 端浏览器的 Cookie。因此，用户个性化设置和偏好设置不会与 VDA 浏览器同步。

集成 Windows 身份验证

当在与 VDA 相同的域中配置了集成 Windows 身份验证 (IWA) 时，浏览器内容重定向可以提供一种无缝的方式来对网站进行身份验证。

策略配置选项

- 配置浏览器内容重定向集成 Windows 身份验证支持策略

在启用单点登录之前，请完成以下操作：

- 配置 Kerberos 基础结构，以颁发由主机名构建的服务主体名称 (SPN) 的票证。例如，HTTP/serverhostname.com。
- 对于服务器获取客户端渲染：当您在服务器获取模式下使用浏览器内容重定向时，请确保在 VDA 上正确配置了 DNS。
- 对于客户端获取客户端渲染：当您在客户端获取模式下使用浏览器内容重定向时，请确保在客户端设备上正确配置了 DNS，并允许从覆盖层到 Web 服务器 IP 地址的 TCP 连接。

代理身份验证

浏览器内容重定向可以提供一种无缝的方式，以便在从服务器获取内容时向您的 Web 代理进行身份验证。启用后，浏览器内容重定向将自动获取并使用 Kerberos 服务票证向代理进行身份验证。

策略配置选项

- 配置浏览器内容重定向服务器获取代理身份验证策略

在启用服务器获取代理身份验证策略之前，请完成以下操作：

- 您需要配置 PAC 文件以通过下游 Web 代理路由流量，并设置代理以使用 Kerberos 身份验证。

服务器端证书验证

浏览器内容重定向通过证书验证支持得到进一步增强。当从客户端访问重定向的网站时，客户端覆盖浏览器可能不信任来自服务器或 MitM 代理的证书。在这种情况下，BCR 现在可以根据 VDA 的证书存储验证主机或代理证书。

最低要求

此功能默认启用，满足以下要求后无需进行任何配置：

- 思杰虚拟应用和桌面 2507
- 适用于 Windows 的 Citrix Workspace 应用程序 2511
- 适用于 Linux 的 Citrix Workspace 应用程序 2604
- 浏览器重定向扩展（Chrome 或 Edge）25.11 或更高版本。

单点登录支持

浏览器内容重定向现在通过单点登录支持提供简化的用户体验，从而实现 VDA 侧身份验证和 Cookie 共享。此增强功能消除了冗余登录，通过在 BCR 会话中（即使在 BCR 窗口关闭后）保持身份验证和 Cookie 持久性来提高工作效率。这种无缝体验通过确保身份验证源自 VDA 而非客户端，进一步增强了安全性。

有关此功能的详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/multimedia/single-sign-on-support.html) 部分中的。

在屏幕截图中捕获重定向内容

浏览器内容重定向在端点上呈现网页，因此标准的会话内屏幕截图工具会将重定向的内容捕获为空白区域。使用 Citrix 截图工具将此内容包含在您的屏幕截图中。Citrix 建议从 Citrix Virtual Desktop Assistant 启动它，以便于查找。有关更多信息，请参阅 Citrix Virtual Desktop Assistant 文档。

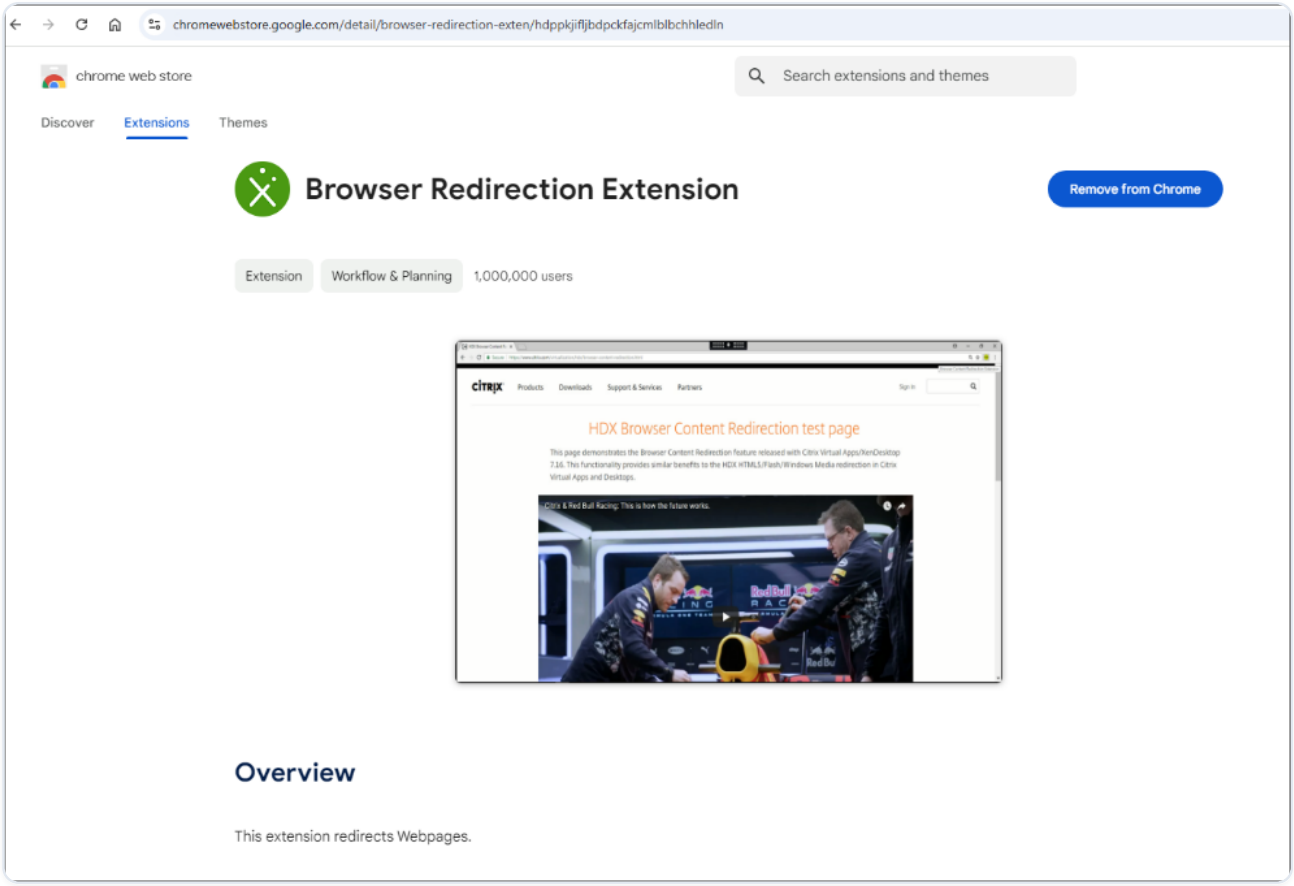
用例

浏览器内容重定向 (BCR) 可用于各种网站，特别是那些资源密集型且企业频繁访问的网站。这包括 YouTube 等视频流平台，它们可以从将渲染卸载到端点设备中显著受益，从而减少服务器负载并节省成本。此外，BCR 非常适合统一通信应用程序，例如视频会议和协作工具（Google Meet、Teams Web、Zoom Web）以及联络中心应用程序（Genesys Cloud），可确保流畅的性能和增强的用户体验。通过利用 BCR，企业可以优化其资源并提高各种基于 Web 的应用程序的效率。有关如何配置特定网站的信息，请参阅 CTX238236。

扩展部署

手动部署

浏览器重定向扩展已在 Chrome 和 Edge 网上应用店发布。该扩展仅在 VDA 上的浏览器中需要，而不在客户端。要安装该扩展，请导航到 Chrome / Edge 网上应用店，搜索浏览器重定向扩展并添加到相应的浏览器。此方法适用于单个用户。要将扩展部署到大量用户，请使用组策略部署扩展。



使用组策略部署

先决条件

- **访问权限：** 您需要对将配置组策略的计算机或 Active Directory 环境拥有管理员权限。
- **ADMX 文件：** 下载适用于您的 Chrome 版本的 Google Chrome ADMX 文件（管理模板）。您可以在 Google Chrome Enterprise 帮助 页面上找到这些文件。
- **Edge 模板：** 从 Microsoft Edge Enterprise 登陆 页面下载 Microsoft Edge 管理模板 (ADMX 文件)。
- **扩展 ID 和更新 URL：** Citrix 浏览器内容重定向扩展的扩展 ID 和更新 URL。

GOOGLE CHROME 的步骤

1. 导入 ADMX 文件：

- 将 Chrome ADMX 文件复制到您的管理模板中央存储。这通常是域控制器上的 %SystemRoot%\PolicyDefinitions。

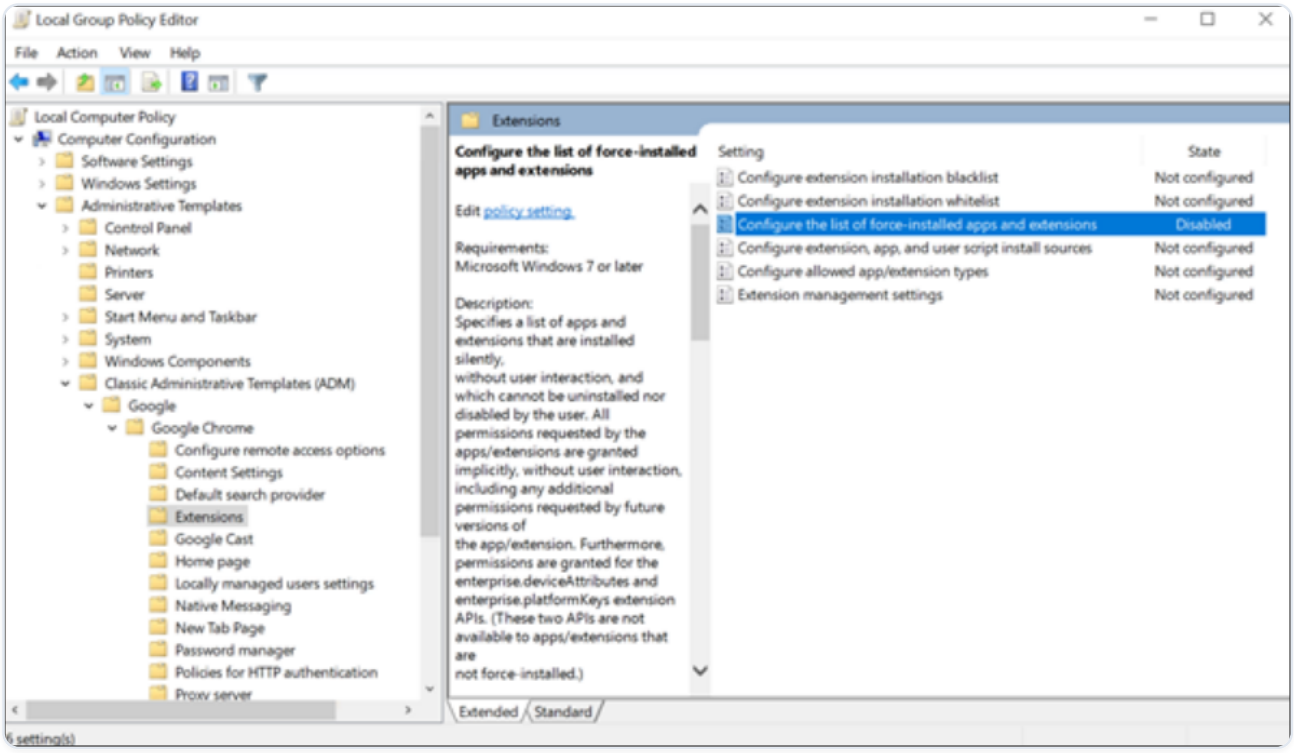
2. 打开组策略管理：
   - 启动组策略管理控制台 (gpmc.msc)。
3. 创建或编辑 GPO：
   - 创建新的组策略对象 (GPO) 或编辑适用于要部署扩展的用户的现有组策略对象。
4. 导航到扩展设置：
   - 在 GPO 编辑器中，转到：
     - 用户配置 > 管理模板 > 经典管理模板 (ADM) > Google > Google Chrome > 扩展程序
5. 启用“配置强制安装的应用和扩展程序列表”：
   - 双击此策略设置并选择“已启用”。
   - 如果“配置强制安装的应用和扩展程序列表”设置设为“已禁用”，则扩展程序将自动从所有用户的 Chrome 中删除。
6. 添加扩展程序 ID 和更新 URL：
   - 单击“显示”按钮。
   - 以以下格式输入扩展程序 ID 和更新 URL：<extension_id>;<update_url>
   - 值: hdppkjifljbdpckfajcmlblbchhledln; `<https://clients2.google.com/service/update2/crx/>` (更新统一资源定位符)
7. 应用 GPO：
   - 将 GPO 链接到 Active Directory 结构中相应的组织单位 (OU)。
8. 更新组策略:
   - 在目标计算机上，运行 gpupdate /force 立即应用策略，或等待策略自动更新。

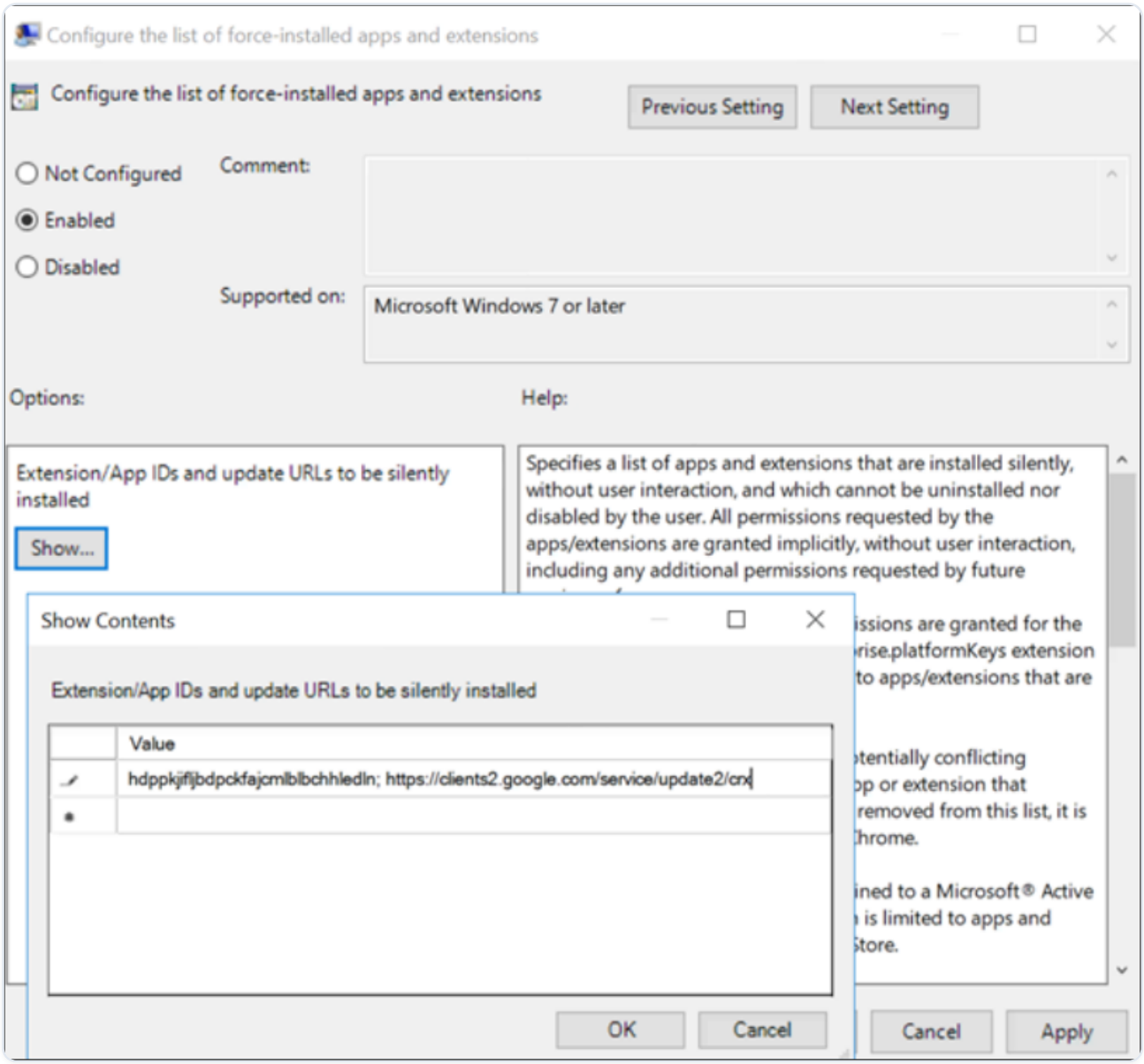
MICROSOFT EDGE 的步骤

1. 导入 ADMX 文件:
   - 将 Edge ADMX 文件复制到您的管理模板中央存储 (%SystemRoot%\PolicyDefinitions)。
2. 打开组策略管理:

- 启动组策略管理控制台 (gpmc.msc)。

3. 创建或编辑 GPO:
   - 创建新的 GPO 或编辑现有 GPO。
4. 导航到扩展设置:
   - 在 GPO 编辑器中，转到:
     - 计算机配置 > 策略 > 管理模板 > Microsoft Edge > 扩展
5. 启用“控制静默安装的扩展”:
   - 双击此策略设置并选择“已启用”。
6. 添加扩展 ID 和更新 URL:
   - 点击“显示”按钮。
   - 以 <extension_id>;<update_url> 格式输入扩展 ID 和更新 URL。
   - 值: hdppkjifljbdpckfajcmlblbchhledln; `<https://clients2.google.com/service/update2/crx/>` (更新统一资源定位符)
7. 应用 GPO：
   - 将 GPO 链接到 Active Directory 结构中相应的组织单位 (OU)。
8. 更新组策略：
   - 在目标计算机上，运行 gpupdate /force 或等待自动更新。


Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Printers
Server
Start Menu and Taskbar
System
Windows Components
Classic Administrative Templates (ADM)
Google
Google Chrome
Configure remote access options
Content Settings
Default search provider
Extensions
Google Cast
Home page
Locally managed users settings
Native Messaging
New Tab Page
Password manager
Policies for HTTP authentication
Proxy server
Extensions
Configure the list of force-installed apps and extensions
Edit policy setting
Requirements:
Microsoft Windows 7 or later
Description:
Specifies a list of apps and extensions that are installed silently,
without user interaction, and which cannot be uninstalled nor disabled by the user. All permissions requested by the apps/extensions are granted implicitly, without user interaction, including any additional permissions requested by future versions of
the app/extension. Furthermore, permissions are granted for the enterprise.deviceAttributes and enterprise.platformKeys extension APIs. (These two APIs are not available to apps/extensions that are
not force-installed.)
Setting
State
Configure extension installation blacklist
Not configured
Configure extension installation whitelist
Not configured
Configure the list of force-installed apps and extensions
Disabled
Configure extension, app, and user script install sources
Not configured
Configure allowed app/extension types
Not configured
Extension management settings
Not configured
Extended
Standard
6 setting(s)



故障排除

有关故障排除信息，请参阅知识中心文章 如何对浏览器内容重定向进行故障排除。

浏览器内容重定向限制

服务器端限制 (VDA)

浏览器内容重定向不支持以下用例。如果需要对任何提及的场景或新场景进行增强，请联系 Citrix 产品团队。

- 浏览器内容重定向不支持弹出窗口。
- 使用浏览器内容重定向时，必须禁用 HTML5 视频重定向策略。
- 在会话断开/重新连接的情况下，需要刷新 VDA 浏览器窗口，BCR 才能再次生效。

- 不支持从 BCR 重定向的窗口进行打印和文件下载。
- 将浏览器内容重定向与浏览器配置文件共享结合使用时，不支持多配置文件 SSO 持久性。
- 浏览器内容重定向不支持隐身模式或隐私浏览模式。

客户端限制 (CWA)

- ARMhf 框架不支持浏览器内容重定向。
- BCR 在一个浏览器上最多支持 25 个重定向选项卡，在两个浏览器中总共支持 30 个重定向选项卡。

单点登录支持

简介

浏览器内容重定向现在提供简化的用户体验，支持单点登录，实现VDA端身份验证和Cookie共享。

此增强功能消除了重复登录，通过在BCR会话中保持身份验证和Cookie持久性（即使在BCR窗口关闭后），从而提高了生产力。

这种无缝体验通过确保身份验证源自VDA而非客户端，进一步增强了安全性。

无单点登录

- 在BCR中打开已验证页面时，要求用户每次重新输入其凭据，从而破坏了SSO持久性。
- SSO仅在BCR窗口保持打开状态时才得以维持；关闭并重新打开窗口会强制用户重复登录过程。
- 身份验证流程发生在客户端，迫使管理员从客户端设备提供对安全身份验证站点的网络访问权限。

使用单点登录

- 用户不再需要输入凭据（当已在VDA上进行身份验证时），因为SSO会从VDA浏览器无缝保留。
- 身份验证发生在VDA端，这通过限制客户端网络要求和暴露来提高安全态势，从而提供显著改进且不间断的体验。

最低要求

- 思杰虚拟应用和桌面 2507
- 思杰工作区应用程序适用于 Windows 2511
- 思杰工作区应用程序适用于 Linux 2601

- 浏览器重定向扩展 (Chrome 或 Edge) 25.11 或更高版本

支持的身份验证序列

目前有两种类型的身份验证序列支持 BCR 单点登录。

基于重定向的身份验证

在这种标准方法中，应用程序使用 HTTP 重定向强制用户跳转到专门的身份验证页面。

例如，如果用户尝试在没有必要的会话 cookie 的情况下访问 `<https://my.intranet.app>`，Web 应用程序将以 HTTP 302 重定向响应到身份验证端点，例如 `<https://my.intranet.app/auth>`。

一旦用户在该页面成功进行身份验证，浏览器将重定向回原始应用程序 URL，现在包含所需的身份验证 Cookie。

页面内基于表单的身份验证

此方法将用户保留在预期的应用程序 URL 上，同时动态呈现登录界面。

例如，如果用户导航到受保护的页面（例如 `<https://my.intranet.app>`），页面会直接加载身份验证表单而不会触发重定向，因为缺少必要的 cookie。此过程可能涉及页面界面和身份提供程序 (IDP) 之间的多次内部交换。这些交换会一直持续，直到提供并使用最终的有效 cookie，从而授予用户访问原始页面内容的权限。

> **注意：**
>
> 如果您的场景不属于上述机制涵盖的范围，并且无法设置您的 Web 应用程序以使用上述机制，请联系 Citrix 产品团队。

配置

步骤 0：简介

有两种方法可以配置 BCR 单点登录。选择配置方法取决于所需 BCR 网站的身份验证机制以及您为单点登录支持配置多个 Web 应用程序所需的灵活性。

方法 1：此方法使用 Web Studio 中现有的 BCR 策略并利用它们实现单点登录支持。

在引入单点登录支持之前，浏览器内容重定向身份验证站点策略用于指定用于身份验证（或中间页面）的 URL，以重定向到客户端，确保流程不中断。

引入单点登录支持后，BCR 将利用 VDA 侧浏览器上的身份验证 Cookie，因此，身份验证站点策略中的 URL 现在需要配置在浏览器内容重定向阻止列表策略中。这可确保身份验证通过 VDA 进行。

方法 2： 此方法的操作逻辑与方法 1 类似，但 URL 是通过 JSON (`bcrconfig.json`) 配置的，并且托管的 JSON URL 在 BCR ACL 策略中调用。JSON 配置提供了额外的灵活性。

1. 企业在其环境中使用了多种 Web 应用程序，每个应用程序可能根据其实现方式使用不同的身份验证机制。新的 JSON 方法使配置更加直观、健壮和可扩展。
2. 在处理**基于页面内表单的身份验证**时，方法 1 无法设置特定的身份验证 Cookie，因为没有现有策略支持此类配置。因此，如果您的网站需要**基于页面内表单的身份验证**，JSON 是唯一的实现方式。

展望未来，JSON 提供了一种可扩展的方式来引入更强大的功能，Citrix 建议尝试基于 JSON 的配置。

步骤 1：确定身份验证机制

要确定您的配置应使用哪种方法，第一步是确定您的应用程序正在使用哪种身份验证机制。要准确确定 Web 应用程序的身份验证方法，最佳方法是联系 Web 应用程序管理员。

如果无法做到这一点，您必须在**未**安装 BCR 扩展的情况下执行身份验证流程时，检查浏览器开发人员工具“网络”选项卡中的请求/响应交互。以下结果可以帮助您确定身份验证类型：

对于基于重定向的身份验证： 在“状态”列下查找一个或多个 302（重定向）响应。302 响应应包含指向身份验证页面的位置标头。如果您使用方法 1，则必须在浏览器内容重定向阻止列表策略中设置此页面 URL；如果您使用方法 2，则必须在 `bcrconfig.json` 文件中的应用程序配置的 `denyList` 部分中设置此页面 URL。

对于基于页面内表单的身份验证： 在“方法”列下查找多个 POST 请求。POST 请求的后续响应之一应返回一个 set-cookie 标头，其中包含特定于 Web 应用程序的身份验证 Cookie。此 Cookie 应在 `bcrconfig.json` 文件中应用程序配置的 Cookie 部分中设置。由于方法 1 不支持基于页面内表单的身份验证，因此方法 2 是此场景的唯一配置选项。

示例： 以下是 github.com 的示例。此方法可用于您希望通过 BCR 重定向并确保配置正确的任何网站

1. 打开 **Chrome**，然后按 **CTRL+SHIFT+I** 调出其开发人员工具。
2. 单击“**网络**”选项卡。
3. 选中“**保留日志**”设置。
4. 单击“**文档**”筛选器以简化网络日志。
5. 在 **名称** 旁边右键单击并添加 **URL** 列。

6. 在开发者工具仍处于打开状态时，浏览到 **github.com**。
7. 登录到 **github.com**
8. 记下 github.com 初始页面与登录后目标页面之间的所有中间跳转。
9. 分析请求/响应标头以确定如上所述的身份验证类型。

步骤 2：选择配置方法

1. 如果您只处理基于重定向的身份验证，并且不需要重定向具有不同需求的多个 Web 应用程序（例如，一个 Web 应用程序使用基于重定向的身份验证，另一个 Web 应用程序使用基于页面内表单的身份验证），则可以选择方法 1 来配置单点登录。
2. 如果您正在处理基于页面内表单的身份验证，或者正在处理具有不同身份验证机制的多个 Web 应用程序，或者即使您只有基于重定向的身份验证也只是想要更大的灵活性，则可以选择方法 2。

步骤 3：配置

方法 1：使用现有策略配置 BCR 单点登录

1. 通过在 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXMediaStream key: Dword BrowserProfileSharing value 1` 中创建以下注册表值来在 VDA 中启用此功能。
2. 使用要重定向的网站配置浏览器内容重定向 ACL 配置策略。这方面无需更改配置。
3. 如果您已在身份验证站点策略中配置了 URL，请将其复制到浏览器内容重定向阻止列表策略中，并禁用身份验证站点策略。
4. 如果您之前未配置身份验证/中间站点，请识别中间 URL（在浏览器开发者工具的“网络”选项卡下，在**未**安装 BCR 扩展的情况下执行身份验证流程时，从请求/响应交互中获取），并将其配置到阻止列表中。

方法 2：使用 JSON 配置 BCR 单点登录

创建 bcrconfig.json

`bcrconfig.json` 可以包含多个 Web 应用程序配置。BCR 扩展将尝试把请求的 URL 与 apps 数组中某个应用程序指定的 `allowList` 之一进行匹配，并动态应用其相关规则，以决定如何处理页面重定向和单点登录处理。以下键可用于控制 BCR 扩展如何处理 Web 应用程序（请注意，根据 JSON 规范，*布尔*值必须为小写 - 只能是 **true** 或 **false**）：

- **appName** ：这主要由扩展在内部使用，并用于日志记录目的。
- **allowList** ：应用程序在 `allowList` 中必须至少包含一个 URL，该 URL 旨在被重定向，以便客户端而不是 VDA 呈现页面。可以定义多个 URL，并且接受通配符。通配符规则与 浏览器内容

重定向 ACL 配置 完全相同。例如，要配置所有 Google 应用程序进行重定向，请使用以下数组：

- **denyList** ：定义当需要身份验证时，Web 应用程序将用户重定向到的 URL。此配置主要对于基于重定向的身份验证至关重要，但它也可用于防止某些基于表单的身份验证流中的特定重定向。此键中列出的 URL 将不会被重定向，以便进行服务器端身份验证。当不需要配置文件共享时，您也可以使用此功能来限制域的特定子 URL 不被重定向到客户端。
- **profileSharing** ：这是需要设置的键值，以确保共享单点登录身份验证 Cookie 和存储用户偏好的其他 Cookie，从而确保服务器端和客户端呈现页面之间的一致行为。
- **cookies** ：定义 Web 应用程序加载时无需提示用户所需的一个或多个身份验证 Cookie。然后，扩展将阻止客户端重定向，直到检测到此处列出的所有 Cookie 都已为给定的 Web 应用程序 URL 设置。此设置主要用于页面内基于表单的身份验证，但在某些情况下，除了指定 denyList 之外，它还可以用于基于重定向的身份验证。
- **deleteClientCache**：如果使用 `bcrconfig.json` 配置机制，则 BCR 客户端默认会删除其浏览器缓存以增强安全性。此过程发生在用户关闭所有重定向的选项卡或在会话中首次启动重定向页面时。将此键的值设置为 **false** 以防止此行为。如果客户端设备受信任，则将此键设置为 **false** 可以增强用户体验。如果客户端设备不受信任，则不设置此键（或）将此键设置为 **true** 可以增强安全态势。
- **schemaVersion** ：这主要由扩展在内部使用，并用于日志记录目的。在撰写本文时，其值应设置为 **2511**。

示例配置

```
{

  "apps": [

    {

      "appName": "myWebApp1",

      "allowList": [

        "https://myWebApp1.com/*"

      ],

      "denyList": [],

      "requires": {
```

```
      "profileSharing": false,
      "cookies": []
    }
  },
  {
    "appName": "myWebApp2",
    "allowList": [
      "https://myWebApp2.com/*"
    ],
    "denyList": [
      "https://myWebApp2.com/authPortal/*"
    ],
    "requires": {
      "profileSharing": true,
      "cookies": []
    }
  },
  {
    "appName": "myWebApp3",
    "allowList": [
      "https://*.myWebApp3.com/"
    ],
```

```
      "denyList": [
        "https://myWebApp3.com/authPortal/*"
      ],
      "requires": {
        "profileSharing": true,
        "cookies": [
          "requiredAuthCookie1",
          "requiredAuthCookie2"
        ]
      }
    }
  ],
  "preferences": {
    "deleteClientCache": true
  },
  "schemaVersion": "2511"
}
```

这是一个示例 `bcrconfig.json` 文件。其元素在下面详细解释：

上述 JSON 结构包含 3 个具有不同配置的应用程序：

myWebApp1 场景，无 SSO：

- `allowList` 键的字符串数组值指定 `<https://myWebApp1.com>` 中的所有路径都应重定向到客户端，除非 `denyList` 键中列出了值（如果有）。

- `denyList` 键的字符串数组值为空，因此不会阻止任何身份验证站点进行重定向。因此，身份验证将不会严格保留在服务器端。
- The `profileSharing` 键的布尔值设置为 **false**，因此与 `allowList` 条目相关的 cookie 不会与客户端共享。
- cookies 键的字符串数组为空，但由于 `profileSharing` 共享键设置为 **false**，它无论如何都会被忽略。

myWebApp2，基于重定向的身份验证场景：

- `allowList` 键的字符串数组值指定 `<https://myWebApp2.com>` 中的所有路径都应重定向到客户端，除非 `denyList` 键中列出了值（如果有）。
- The `denyList` 键的字符串数组值指定 **myWebApp2.com** 域下以 `/authPortal/` 开头的路径将阻止客户端重定向，以便执行服务器端身份验证。
- The `profileSharing` 键的布尔值设置为 **true**，因此与 allowList 条目相关的 cookie 将与客户端共享，并且单点登录将通过。
- cookies 键的字符串数组为空，因此扩展程序不会等待在服务器端身份验证后设置特定 cookie，然后才将其与客户端共享。

myWebApp3，基于表单的身份验证场景：

- `allowList` 键的字符串数组值指定 `<https://myWebApp3.com>` 中的所有路径都应重定向到客户端，除非 `denyList` 键中列出了值（如果有）。
- The `denyList` 键的字符串数组值指定 **myWebApp3.com** 域下以 `/authPortal/` 开头的路径将阻止客户端重定向，以便执行服务器端身份验证。
- The `profileSharing` 键的布尔值设置为 **true**，因此与 `allowList` 条目相关的 cookie 将与客户端共享。
- cookies 键的字符串数组包含一个 cookie 名称，因此扩展程序将等待在服务器端身份验证后设置此 cookie。`allowList` 中相关 URL 的 cookie 将与客户端共享，并发生客户端重定向。

首选项

- The `deleteClientCache` 键设置为 **true**，因此 BCR 客户端默认删除其浏览器缓存以增强安全性。即使未设置此键，这也是默认行为。

配置 BCR 策略

创建 `bcrconfig.json` 后，请按照以下步骤配置 浏览器内容重定向 ACL 配置 以使用 JSON 文件中的内容。

- 将文件命名为 `.bcrconfig.json` 扩展名，例如 `myrules.bcrconfig.json`

- 将 JSON 文件托管在 VDA 可访问的 Web 服务器上，并记下 URL。

  注意：

  服务器必须允许文件下载；Microsoft IIS 站点默认允许 JSON 文件下载。

- 在 Citrix Studio 中，在“策略”下，将上一步中的 URL 添加到“浏览器内容重定向 ACL 配置”设置中：

  注意：

  浏览器内容重定向 ACL 配置设置中的其他条目可以保留。如果发生冲突，BCR 扩展会优先处理 `bcrconfig.json` 设置。Citrix 建议将整个配置转移到 JSON，以便于管理、应用程序级配置和可伸缩性。

- 保存策略并启动会话以测试策略配置。

  注意：

  设置策略后，您可以随时编辑托管的 `bcrconfig.json` 文件进行调整。文件仅在运行 BCR 扩展的主浏览器进程启动或重新启动时重新加载并应用更改。

注意：

- 本质上，从策略角度来看，您只需启用浏览器内容重定向策略（默认已启用），并使用指向 JSON 文件的 URL 配置浏览器内容重定向 ACL 配置策略。
- JSON 配置目前适用于以下策略并使其更灵活，但其余策略仍执行与以前相同的操作。
  - **浏览器内容重定向 ACL 配置：** ACL 中的 URL 现在可以通过 `allowList` 键通过 JSON 进行配置。
  - **浏览器内容重定向阻止列表配置：** 阻止列表现在可以通过 `denyList` 键通过 JSON 进行配置。

- **浏览器内容重定向身份验证站点：** 身份验证站点也可以通过 `denyList` 键通过 JSON 进行配置。

网络摄像头重定向和视频压缩

警告：

不正确地编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix® 无法保证可以解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。在编辑注册表之前，请务必备份注册表。

虚拟会话中运行的应用程序可以通过使用 HDX 网络摄像头视频压缩或 HDX 即插即用通用 USB 重定向来使用网络摄像头。使用 **Citrix Workspace™ app > 首选项 > 设备** 在模式之间切换。如果可能，Citrix 建议您始终使用 HDX 网络摄像头视频压缩。仅当 HDX 视频压缩存在应用程序兼容性问题或需要网络摄像头的高级本机功能时，才建议使用 HDX 通用 USB 重定向。为了获得更好的性能，Citrix 建议虚拟投递代理 (VDA) 至少具有两个虚拟 CPU。

为防止用户从 HDX 网络摄像头视频压缩切换，请使用 **ICA® 策略设置 > USB 设备策略** 设置下的策略设置禁用 USB 设备重定向。Citrix Workspace 应用程序用户可以通过选择 Desktop Viewer 麦克风和网络摄像头设置 **不使用我的麦克风或网络摄像头** 来覆盖默认行为。

HDX 网络摄像头视频压缩

HDX 网络摄像头视频压缩也称为**优化**网络摄像头模式。这种类型的网络摄像头视频压缩将 H.264 视频直接发送到虚拟会话中运行的视频会议应用程序。为了优化 VDA 资源，HDX 网络摄像头压缩不会对网络摄像头视频进行编码、转码和解码。此功能默认启用。

要禁用从服务器到视频会议应用程序的直接视频流，请将 VDA 上的注册表项设置为 0。有关信息，请参阅注册表管理的特性列表中的 网络摄像头视频压缩。

如果禁用视频资源流的默认功能，HDX 网络摄像头视频压缩将使用客户端操作系统中的多媒体框架技术来拦截来自捕获设备的视频，并对其进行转码和压缩。捕获设备制造商提供插入操作系统内核流式处理架构的驱动程序。

客户端处理与网络摄像头的通信。然后，客户端仅将视频发送到可以正确显示它的服务器。服务器不直接处理网络摄像头，但其集成可在您的桌面上提供相同的体验。Workspace 应用程序会压缩视频以节省带宽，并在 WAN 场景中提供更好的弹性。

网络摄像头压缩(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/webcam-compression.png)

必须为 HDX 网络摄像头视频压缩启用**多媒体会议**策略。此策略默认启用。

如果网络摄像头支持硬件编码，HDX 视频压缩默认使用硬件编码。硬件编码可能比软件编码消耗更多带宽。要强制进行软件压缩，请编辑客户端上的注册表项。有关信息，请参阅注册表管理的特性列表中的 网络摄像头软件压缩。

HDX 网络摄像头视频压缩要求

HDX 网络摄像头视频压缩支持以下版本的 Citrix Workspace 应用程序：

平台	处理器
适用于 Windows 的 Citrix Workspace 应用程序	适用于 Windows 的 Citrix Workspace 应用程序支持 XenApp 和 XenDesktop 7.17 及更高版本上的 32 位和 64 位应用程序的网络摄像头视频压缩。在早期版本中，适用于 Windows 的 Citrix Workspace 应用程序仅支持 32 位应用程序。
适用于 Mac 的 Citrix Workspace 应用程序	适用于 Mac 的 Citrix Workspace 应用程序 2006 或更高版本支持 XenApp 和 XenDesktop 7.17 及更高版本上的 64 位应用程序的网络摄像头视频压缩。在早期版本中，适用于 Mac 的 Citrix Workspace 应用程序仅支持 32 位应用程序。
适用于 Linux 的 Citrix Workspace 应用程序	适用于 Linux 的 Citrix Workspace 应用程序支持虚拟桌面上的 32 位和 64 位应用程序。
适用于 Chrome 的 Citrix Workspace 应用程序	由于某些 ARM Chromebook 不支持 H.264 编码，因此只有 32 位应用程序才能使用优化的 HDX 网络摄像头视频压缩。

基于媒体基础的视频应用程序支持在 Windows 10 或更高版本以及 Windows Server 2019 或更高版本上使用 HDX 网络摄像头视频压缩。有关详细信息，请参阅知识中心文章 CTX132764。

其他用户设备要求：

- 产生声音的适当硬件。
- DirectShow 兼容网络摄像头（使用网络摄像头默认设置）。支持硬件编码的网络摄像头可降低客户端 CPU 使用率。

- 对于 HDX 网络摄像头视频压缩，如果可能，请在客户端上安装从摄像头制造商处获取的网络摄像头驱动程序。服务器上不需要安装设备驱动程序。

不同的网络摄像头提供不同的帧速率，并具有不同的亮度和对比度级别。调整网络摄像头的对比度可以显著减少上行流量。Citrix 使用以下网络摄像头进行初始功能验证：

- Microsoft LifeCam VX 型号（2000、3000、5000、7000）
- 创新 Live! 摄像头 Optia Pro
- 罗技 QuickCam Messenger
- 罗技 C600, C920
- HP Deluxe 网络摄像头

要调整首选视频帧速率，请编辑客户端上的注册表项。有关信息，请参阅注册表管理的功能列表中的 网络摄像头视频压缩帧速率。

高清网络摄像头流式传输

服务器上的视频会议应用程序根据支持的格式类型选择网络摄像头格式和分辨率。会话开始时，客户端将网络摄像头信息发送到服务器。从应用程序中选择一个网络摄像头。当网络摄像头和视频会议应用程序支持高清渲染时，应用程序将使用高清分辨率。我们支持所有网络摄像头分辨率。

此功能需要适用于 Windows 的 Citrix Workspace 应用程序（最低版本 1808）或适用于 Windows 的 Citrix Receiver（最低版本 4.10）。

您可以使用注册表项禁用和启用此功能。有关信息，请参阅注册表管理的功能列表中的 高清网络摄像头流式传输。

如果媒体类型协商失败，HDX 将回退到默认的 VGA 分辨率（640 x 480 像素）。您可以使用客户端上的注册表项配置默认分辨率。确保摄像头支持指定的分辨率。有关信息，请参阅注册表管理的功能列表中的 高清网络摄像头分辨率。

HDX 网络摄像头视频压缩与即插即用通用 USB 重定向相比，使用的带宽显著减少，并且在 WAN 连接上运行良好。要调整带宽，请在客户端上设置注册表项。有关信息，请参阅注册表管理的特性列表中的 高清网络摄像头带宽。

输入每秒位数的值。如果未指定带宽，视频会议应用程序默认使用 350000 bps。

HDX 即插即用通用 USB 重定向

HDX 即插即用通用 USB 重定向（同步）也称为**通用**网络摄像头模式。HDX 即插即用通用 USB 重定向的优点是您无需在瘦客户端/端点上安装驱动程序。USB 堆栈是虚拟化的，因此您插入本地客户

端的任何设备都会发送到远程 VM。远程桌面表现得就像您本地插入了设备一样。Windows 桌面处理与硬件的所有交互，并通过即插即用逻辑查找正确的驱动程序。如果服务器上存在驱动程序，大多数网络摄像头都可以工作，并且可以通过 ICA 工作。通用网络摄像头模式使用显著更多的带宽（每秒数兆比特），因为您通过网络使用 USB 协议发送未压缩的视频。

支持带网络摄像头重定向的 Microsoft 虚拟摄像头

从 2607 LTSR 开始，Windows VDA（Windows 11 和 Windows Server 2025）利用 Microsoft 内置的虚拟摄像头功能，升级了网络摄像头重定向和摄像头体验。优点包括扩展了与更多应用程序的兼容性、提高了安全性和隐私性，并提供了更接近本地和原生摄像头的使用体验。此功能默认启用。

> **注意：**
>
> 此功能要求在系统设置中启用**摄像头访问**；在 Windows Server 2025 上，此设置默认禁用。

HTML5 多媒体重定向

> **注意：**
>
> HTML5 多媒体重定向计划在未来版本中弃用。建议客户过渡到浏览器内容重定向 (BCR)（推荐的替代技术），以确保功能持续可用。

> HTML5 多媒体重定向扩展了 HDX™ MediaStream 的多媒体重定向功能，以包括 HTML5 音频和视频。由于多媒体内容在线分发的增长，尤其是针对移动设备，浏览器行业开发了更高效的音频和视频呈现方式。

Flash 曾是标准，但它需要插件，并非在所有设备上都可用，并且在移动设备上电池使用量更高。像 YouTube、Netflix 以及 Mozilla、Google 和 Microsoft 的新版浏览器等公司正在转向 HTML5，使其成为新标准。

基于 HTML5 的多媒体相对于专有插件具有许多优势，包括：

- 独立于公司的标准 (W3C)
- 简化的数字版权管理 (DRM) 工作流程
- 更好的性能，没有插件带来的安全问题

HTTP 渐进式下载

HTTP 渐进式下载是一种基于 HTTP 的伪流式传输方法，支持 HTML5。在渐进式下载中，浏览器在从 HTTP Web 服务器下载单个文件（以单一质量编码）时播放该文件。视频在接收时存储到驱动器中，并从驱动器播放。如果您重新观看视频，浏览器可以从缓存加载视频。

有关渐进式下载的示例，请参阅 HTML5 视频重定向测试页面。要检查网页中的视频元素并在 HTML5 视频标签中查找源（mp4 容器格式），请使用浏览器中的开发人员工具：

比较 HTML5 和 Flash

功能	HTML5	闪存
需要专有播放器	否	是
在移动设备上运行	是	部分
在不同平台上的运行速度	高	慢
iOS 支持	是	否
资源使用情况	较少	较多
加载更快	是	否

要求

我们仅支持 mp4 格式的渐进式下载重定向。我们不支持 WebM 和 DASH/HLS 等自适应比特率流技术。

我们支持以下功能，并使用策略来控制它们。有关详细信息，请参阅多媒体策略设置。

- 服务器端渲染
- 服务器获取客户端渲染
- 客户端获取和渲染

Citrix Workspace™ 应用程序和 Citrix Receiver™ 的最低版本：

- 适用于 Windows 的 Citrix Workspace 应用程序 1808
- 适用于 Windows 的 Citrix Receiver 4.5
- 适用于 Linux 的 Citrix Workspace 应用程序 1808
- 适用于 Linux 的 Citrix Receiver 13.5

最低 VDA 浏览器版本	WINDOWS 操作系统版本/内部版本/服务包
Internet Explorer 浏览器 11.0	Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1)；Windows 7 x86 和 x64；Windows Server 2016 RTM 14393 (1607)；Windows Server 2012 R2
Firefox 47 手动将证书添加到 Firefox 证书存储，或将 Firefox 配置为从 Windows 信任的证书存储中搜索证书。有关详细信息，请参阅 `https://wiki.mozilla.org/CA:AddRootToFirefox`	Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1); Windows 7 x86 和 x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
谷歌浏览器 51	Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1); Windows 7 x86 和 x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2

HTML5 视频重定向解决方案的组件

- **HdxVideo.js** - 拦截网站上视频命令的 JavaScript 挂钩。HdxVideo.js 使用安全 WebSocket (SSL/TLS) 与 WebSocketService 通信。
- **WebSocket SSL 证书**
  - 对于 CA（根）：**Citrix XenApp/XenDesktop HDX 产品内 CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA) 位置：**证书 (本地计算机) > 受信任的根证书颁发机构 > 证书**。
  - 对于最终实体（叶）：**Citrix XenApp/XenDesktop HDX 服务** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service) 位置：**证书 (本地计算机) > 个人 > 证书**。
- **WebSocketService.exe** - 在本地系统上运行，执行 SSL 终止和用户会话映射。TLS 安全 WebSocket 侦听 127.0.0.1 端口 9001。
- **WebSocketAgent.exe** - 在用户会话上运行，并根据 WebSocketService 命令的指示呈现视频。

如何启用 HTML5 视频重定向?

在此版本中，此功能仅适用于受控网页。它要求将 HdxVideo.js JavaScript（包含在 Citrix Virtual Apps and Desktops 安装介质中）添加到提供 HTML5 多媒体内容的网页中。例如，内部培训站点上的视频。

不支持基于自适应比特率技术（例如，HTTP Live Streaming (HLS) 和 Dynamic Adaptive Streaming over HTTP (DASH)）的网站，例如 youtube.com。

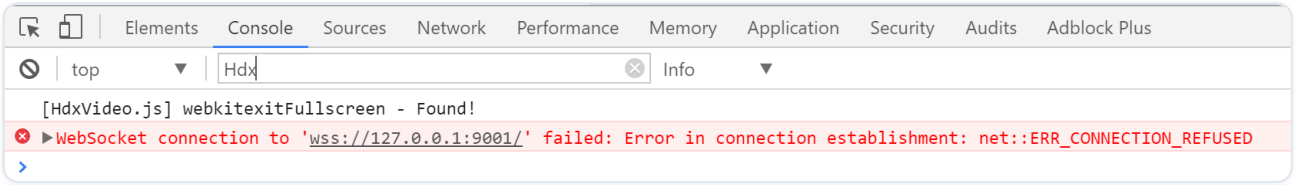
有关详细信息，请参阅 *多媒体策略设置*。

在屏幕截图中捕获重定向内容

HTML5 多媒体重定向在端点上呈现视频，因此标准会话内屏幕截图工具会将重定向的视频捕获为空白区域。使用 Citrix 截图工具将此内容包含在您的屏幕截图中。Citrix 建议从 Citrix Virtual Desktop Assistant 启动它，以便于查找。有关详细信息，请参阅 Citrix Virtual Desktop Assistant 文档。

故障排除提示

当网页尝试运行 HdxVideo.js 时，可能会发生错误。如果 JavaScript 加载失败，HTML5 重定向机制也会失败。通过检查浏览器开发人员工具窗口中的控制台，确保没有与 HdxVideo.js 相关的错误。例如：



Microsoft Teams 优化（新）

Citrix® 支持两种方式在 VDI 环境中优化 Microsoft Teams 音频和视频：Citrix HDX™ 优化和 Microsoft 的 Teams 新 VDI 解决方案。经典版 Teams 已达到生命周期终止，因此本页描述的优化方法适用于当前的 Microsoft Teams 客户端。

> **注意：**
>
> Microsoft 已宣布弃用基于 WebRTC 的适用于 Windows 端点的 Microsoft Teams Citrix HDX 优化。以下是两个里程碑：
>
> - October 1, 2026 - 支持终止：不再由 Microsoft 或 Citrix 正式支持。
> - April 1, 2027 - 可用性终止：基于 WebRTC 的优化停止运行。旧版优化的 Citrix Studio 策略不再生效。

建议客户迁移到 Teams 新 VDI 解决方案。此更改仅影响 Windows 端点。macOS、Linux、ChromeOS 和 HTML5 端点不受影响。有关更多详细信息，请参阅 Microsoft 博客。

优化方法

- **Citrix HDX 优化 (MTOP)**：Citrix 和 Microsoft 的组合解决方案，使用 Citrix 拥有的虚拟通道 (CTXMTOP)。媒体卸载由 Citrix Workspace™ 应用程序中的 `HdxRtcEngine` 处理。此解决方案传统上称为 MTOP。
- **Teams 新 VDI 解决方案**：一种由 Microsoft 拥有和管理的新型优化，使用 Microsoft 拥有的虚拟通道 (MSTEAMS、MSTEAM1 和 MSTEAM2)。它适用于 Windows 和 Mac 端点。有关完整详细信息，请参阅 Microsoft 文档中的 Teams 新 VDI 解决方案。

注意：

无论您使用哪种优化方法，Microsoft Teams 视频和屏幕共享都会在端点上呈现。因此，标准会话内屏幕截图工具会将此内容捕获为空白区域。使用 Citrix 截图工具将其包含在您的屏幕截图中。Citrix 建议从 Citrix Virtual Desktop Assistant 启动它，以便于查找。有关更多信息，请参阅 Citrix Virtual Desktop Assistant 文档。

主要区别

CITRIX HDX 优化	TEAMS 新 VDI 解决方案
此优化是 Citrix 和 Microsoft 的组合解决方案，使用 Citrix 拥有的虚拟通道 (CTXMTOP)。	此优化解决方案由 Microsoft 拥有和管理，使用 Microsoft 拥有的虚拟通道 (MSTEAMS、MSTEAM1 和 MSTEAM2)。
媒体卸载由 `HdxRtcEngine` 处理，它位于 Citrix Workspace 应用程序中。	媒体卸载由 Windows 和 Mac 端点上的 SlimCore 媒体引擎处理。
端点上不需要额外组件，只需安装 Citrix Workspace 应用程序。	附加组件 - **Teams VDI 插件**需要通过各种方式部署到端点上。此插件管理 SlimCore 媒体引擎的下载和更新。
适用于端点平台 - Windows、macOS、Linux 和 ChromeOS。	适用于端点平台 - Windows 和 Mac。
新功能由 Citrix 和 Microsoft 联合管理。	新功能由 Microsoft 管理。用户可以访问一些 新功能，这些功能在 Citrix HDX 优化中不可用。

CITRIX HDX 优化	TEAMS 新 VDI 解决方案
由 Citrix 和 Microsoft 双方支持，具体取决于所涉及的组件。客户可以向 Citrix 或 Microsoft 提交案例，并根据需要被重定向到相应的团队。	由 Microsoft 拥有和支持。Citrix 支持所涉及的 Citrix 组件，例如 Citrix Workspace 应用程序、虚拟通道允许列表和插件部署机制。

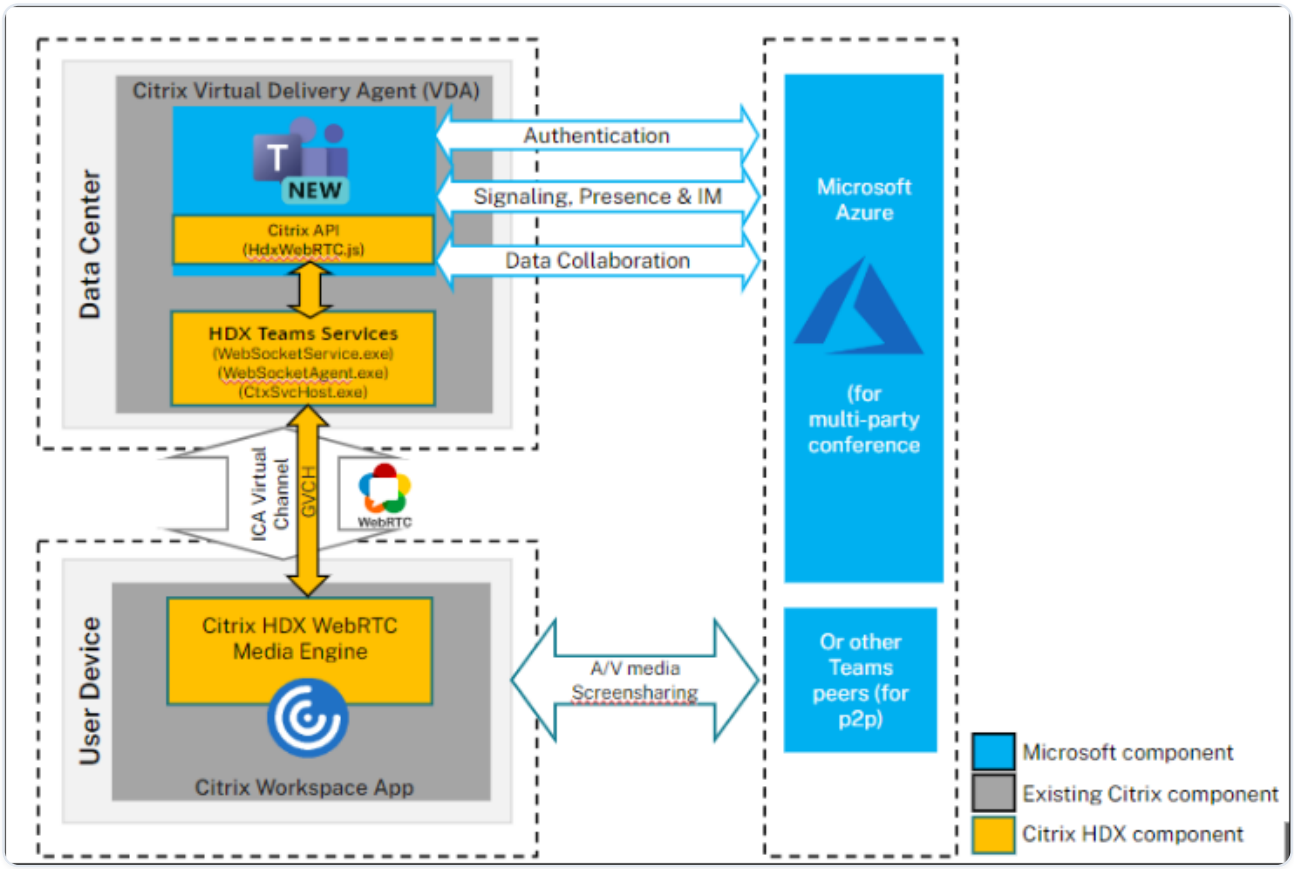
互操作性和漫游

Citrix HDX 优化和适用于 Teams 的新 VDI 解决方案可以并行存在，但 Teams 客户端一次只使用其中一个。

- 当 Teams 应用程序启动时，优化按以下顺序选择：适用于 Teams 的新 VDI 解决方案，然后是 Citrix HDX 优化 (WebRTC)，然后是标准音频/视频重定向。
- 如果适用于 Teams 的新 VDI 解决方案失败，Teams 将直接回退到标准音频/视频重定向，而不是 WebRTC。需要重新启动 Teams 应用程序才能重新运行选择并选择适合的优化。
- 端点之间的漫游是无缝的，不需要重新启动 Teams 应用程序，包括用户在支持和不支持适用于 Teams 的新 VDI 解决方案的端点之间漫游时。

Citrix HDX™ 优化

在 Citrix HDX (WebRTC 优化) 中，负责处理卸载媒体的端点上的媒体引擎 (HdxRtcEngine) 嵌入在 Citrix Workspace™ 应用程序中，安装 Citrix Workspace 应用程序也会自动安装该引擎。



系统要求

本节描述了支持新 Teams 客户端所需的最低和推荐版本。请注意，在最低版本中，某些关键错误修复或最新功能可能不可用。部署推荐版本以获得最佳体验，包括最新的修复和功能。

VDI 操作系统

有关详细信息，请参阅 Microsoft 文档中提供的建议。

注意：

- 不支持 Windows Server 2016。Citrix 建议您相应地规划升级。
- 由于版本更新频繁，此处提及的版本可能会达到生命周期结束。因此，请参阅 Citrix Workspace app 和 Citrix Virtual Apps and Desktops 的产品生命周期页面，以确保您正在使用不同组件的受支持版本。
- 如果您使用的是 Citrix Virtual Apps and Desktops™ 1912 LTSR，Citrix 建议规划升级，因为它将于 2024 年 12 月达到生命周期结束。

虚拟投递代理 (VDA)

最低版本	推荐版本
1912 LTSR CU8 及更高版本；2203 LTSR（任何 CU 版本）；2212 CR	2203 LTSR CU5 及更高版本（或）2402 LTSR 以及任何更高版本的 CR

Citrix Workspace 应用程序

最低版本	推荐版本
Windows 2203 LTSR (最新累积更新); Windows 2302 CR; Linux 2207; Mac 2302; Chrome/ HTML5 2301	Windows 操作系统 2402 LTSR；Windows 操作系统 2405 CR；Linux 操作系统 2405；Mac 操作系统 2405；ChromeOS/HTML5 操作系统 2405

部署

1. 在 VDI 上安装新的 Teams 客户端。有关详细信息，请参阅 为 VDI 部署新的 Teams。
2. 在 VDA 上配置以下注册表项以优化新的 Teams。
   - **位置：** `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
   - **密钥 (REG_Multi_SZ)**: `ProcessWhitelist`
   - **值：** `msedgewebview2.exe`

   > **注意：**
   >
   > 从 Citrix Virtual Apps and Desktops 2402 LTSR（或）Citrix Virtual Apps and Desktops 2203 LTSR CU5+ 开始，您无需手动配置 `msedgewebview2.exe` 注册表项，因为它默认已列入允许列表。
3. 确保已启用 Microsoft Teams 重定向 策略。此策略默认处于启用状态。
4. 客户端无需进行额外配置。按照向导说明安装 Citrix Workspace 应用程序。

应用程序分层

新版 Microsoft Teams 已更改其安装方法，现在安装在 C:\Program Files\WindowsApps 下。为支持此更改，您必须运行 App Layering 2403.2 或更高版本。您可以在 App Layering 下载 页面下载包含此修复的升级磁盘。

有关详细信息，请参阅 App Layering 文档。

Citrix 配置文件管理

有关如何为新版 Microsoft Teams 启用漫游的信息，请参阅 Citrix Profile Management 文档。Citrix Profile Management 的当前最低版本指南为 2402 LTSR（或）2203 LTSR CU5+。

网络注意事项

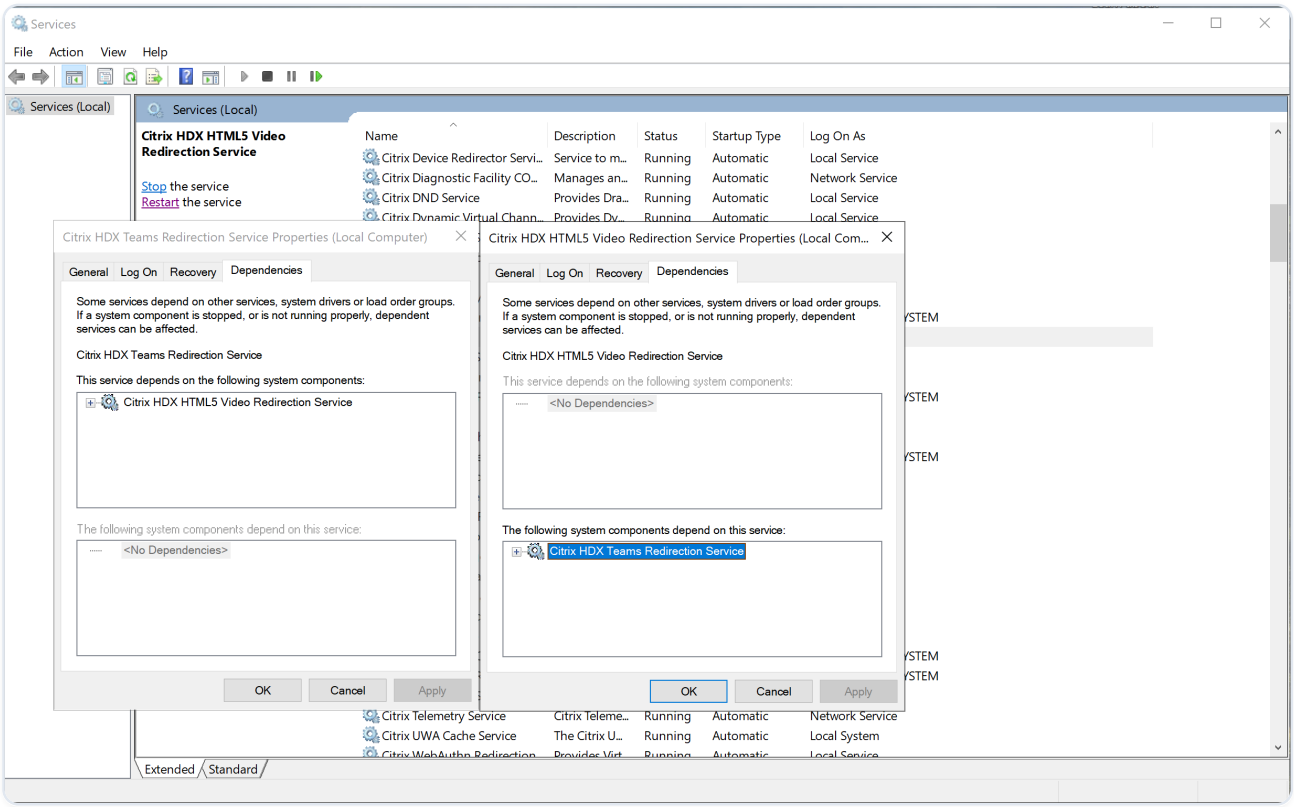
新版 Teams 的网络要求与经典版 Teams 没有区别。因此，请参阅经典版 Teams 文档中的 网络要求 部分。

功能参考

Microsoft Teams 优化显式服务依赖项

从 Citrix Virtual Apps / Desktops 2607 LTSR 开始，**Citrix HDX Teams 重定向服务**（由 HDX 优化型 Microsoft Teams 和 UCSDK 优化型应用程序使用）现在明确声明依赖于 **Citrix HDX HTML5 视频重定向服务 (WebSocketService)**。

此更新可确保在 Teams 服务启动时自动验证并启动 HTML5 服务，从而防止在服务严格管理的环境中 Microsoft Teams 和 UCSDK 集成应用程序出现优化失败。



优化叠加剪裁以增强性能和用户体验

从 CVAD 2511 开始，用于处理 HDX Microsoft Teams 优化和 UCSDK 优化等功能中重定向视频叠加的机制已重新设计，以改善用户体验和服务器性能。

主要优势

- **改进的视觉准确性：** 此增强功能解决了视觉故障，即应用程序元素（例如弹出菜单或通知）会错误地出现在视频内容后面。新逻辑可确保所有组件按正确顺序渲染，从而提供更流畅、更可预测的体验。
- **增强的性能：** 此优化显著降低了虚拟投递代理上的 CPU 利用率。通过用更高效的基于图形的方法取代旧的、资源密集型轮询方法，此更改提高了服务器可伸缩性并允许更高的用户密度。

> **注意：**
>
> 此功能取决于未来版本的 Microsoft Teams（或其他 UCSDK 合作伙伴应用程序），并且需要 Citrix Workspace App for Windows 2511。

功能矩阵和版本支持

由于版本更新频繁，此处提到的一些旧版本可能已达到生命周期结束。因此，请参阅 Citrix Workspace App 和 Citrix Virtual Apps and Desktops 的产品生命周期页面，以确保您使用的是受支持的不同组件版本。

> **注意：**
>
> - 此处提到的版本是支持特定功能的最低版本（或）支持新版 Teams 的最低版本，以较高者为准。
> - 最低版本部分中提到的 Citrix Virtual Apps and Desktops™ 1912 LTSR CU8+ 未在下表中提及，因为它将于 2024 年 12 月达到生命周期结束。但是，在此之前它仍然是受支持的版本。
> - 最低 Citrix Virtual Apps and Desktops 版本为 `N/A` 的功能仅表示该功能不涉及 VDA 方面的任何更改。

功能	VDA（最低版本）	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 MAC 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 LINUX 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序（最低版本）
音频/视频（点对点和会议）	2203 LTSR（任何 CU）、2212 CR	2203 LTSR 最新 CU, 2302 CR	2302	2207	2301
屏幕共享	2203 LTSR（任何 CU）、2212 CR	2203 LTSR 最新 CU, 2302 CR	2302	2207	2301
i. 屏幕指示器红色边框	2203 LTSR（任何 CU）、2212 CR	2203 LTSR 最新 CU, 2302 CR	2302	2207	否
ii. 将捕获限制为 Desktop Viewer	2203 LTSR（任何 CU）、2212 CR	2203 LTSR 最新 CU, 2302 CR	2302	2207	否
三、多显示器	2203 LTSR（任何 CU）、2212 CR	2203 LTSR 最新 CU, 2302 CR	2302	2207	否
DTMF	N/A	2203 LTSR 最新 CU, 2302 CR	2302	2207	2301
代理服务器支持	N/A	2203 LTSR 最新 CU, 2302 CR	2302	2207	2305

功能	VDA（最低版本）	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 MAC 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 LINUX 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序（最低版本）
应用程序共享	2203 LTSR（任何 CU）、2212 CR	2203 LTSR 最新 CU, 2302 CR	2302	2209	否
实时字幕	N/A	2203 LTSR 最新 CU, 2302 CR	2302	2207	2303
动态 e911	N/A	2203 LTSR 最新 CU, 2302 CR	2302	2207	2301
授予控制权	N/A	2203 LTSR 最新 CU, 2302 CR	2302	2207	否
请求控制权	N/A	2203 LTSR 最新 CU, 2302 CR	2302	2207	2303
多窗口	2203 LTSR（任何 CU）、2212 CR	2203 LTSR 最新 CU, 2302 CR	2302	2207	2303
会议转录	2203 LTSR（任何 CU）、2212 CR	2203 LTSR 最新 CU, 2302 CR	2302	2207	2303
背景模糊	2203 LTSR（任何	2203 LTSR 最新 CU, 2302 CR	2302	2212	2303

功能	VDA（最低版本）	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 MAC 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 LINUX 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序（最低版本）
	CU）、2212 CR				
屏幕共享（带应用程序保护）	2203 LTSR（任何 CU）、2212 CR	2402 LTSR, 2309.1 CR	2308	2311	否
同播	2203 LTSR（任何 CU）、2212 CR	2402 LTSR, 2305 CR	2305	2305	2312
辅助铃声	2203 LTSR（任何 CU）、2212 CR	2402 LTSR, 2307.1 CR	2308	2308	2312
共享系统音频	2203 LTSR（任何 CU）、2212 CR	2402 LTSR、2403 CR	2405	2402	否

故障排除及其他注意事项

有关新版 Teams，请参阅 CTX253754、Microsoft Teams 故障排除。有关新版 Teams 的任何最新更新，请参阅 CTX585013。

已知限制

Citrix Workspace 应用程序的限制

- HID 支持 - 不支持接听和结束呼叫。支持调高和调低音量。

- 用户在使用 VDA 上的截图工具时无法截取 Microsoft Teams 内容的屏幕截图。但是，如果在客户端使用截图工具，则可以捕获内容。
- 共享系统音频的限制
  - 当与 RAVE 和 BCR 重定向的应用程序或选项卡共享屏幕时，无法使用此功能共享音频。
  - 此功能仅在已发布的桌面上受支持

VDA 上的限制

- 不支持将新版 Teams 作为已发布的（无缝）应用程序
  - 在 CVAD 2402 LTSR、2203 LTSR CU5 及更高版本中已修复
- 当您将 Citrix Workspace 应用程序的高 DPI 设置配置为“是”时，重定向的视频窗口会显示在不正确的位置。当显示器的 DPI 缩放因子设置为 100% 以上时，会出现此限制。
- Microsoft Teams 2.1 一次只支持重定向一个网络摄像头。但是，它不支持在单会话 VDA 上进行多个网络摄像头重定向或即插即用 (PnP) 网络摄像头重定向。

对 Citrix Workspace 应用程序和 VDA 的限制

- 您只能使用客户端计算机上的音量条来控制优化通话的音量，而不能在 VDA 上控制。

有关 Microsoft 限制的更多详细信息，请参阅 VDI 中不支持的功能。

Teams 的新 VDI 解决方案

> **注意：**

> Teams 的新 VDI 解决方案目前已在 Citrix® 上面向 Windows 和 Mac 端点普遍可用。此解决方案需要最低版本的 Microsoft Teams。请参阅系统要求。

> 在 Teams 的新 VDI 解决方案中，Microsoft 使用 Citrix 虚拟通道 SDK 构建自定义虚拟通道。在端点上，媒体被卸载到 Microsoft 媒体引擎 (SlimCore)，而不是 `HdxRtcEngine`。自定义虚拟通道负责 VDA 上的 Teams 与端点上的媒体引擎之间的通信。

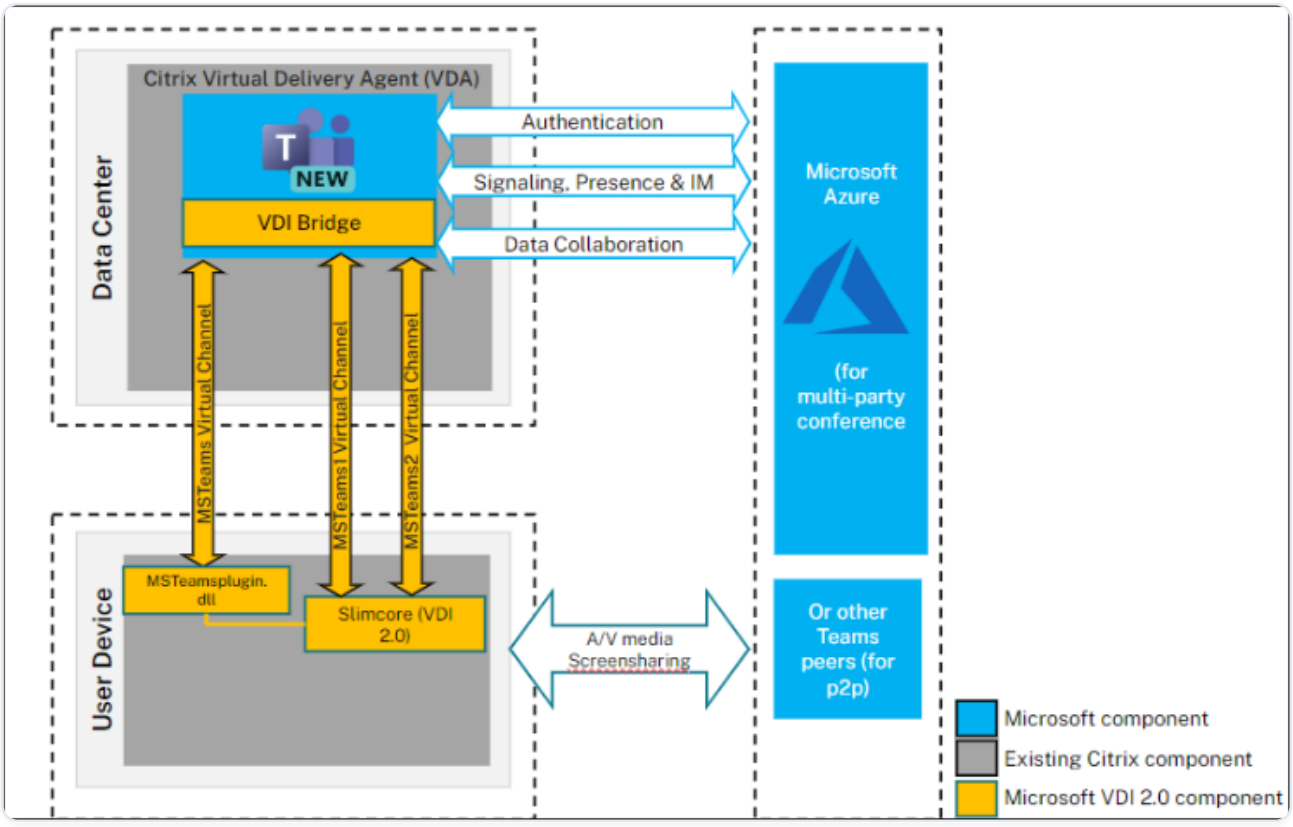
> **注意：**

Microsoft 已宣布弃用基于 WebRTC 的 Citrix HDX™ Microsoft Teams 优化（适用于 Windows 端点）。以下是两个里程碑：

- October 1, 2026 - 支持终止：Microsoft 或 Citrix 不再正式支持。
- April 1, 2027 - 可用性终止：基于 WebRTC 的优化停止运行。Citrix Studio 中针对旧版优化的策略不再生效。

建议客户迁移到 Teams 的新 VDI 解决方案。此更改仅影响 Windows 端点。macOS、Linux、ChromeOS 和 HTML5 端点不受影响。有关更多详细信息，请参阅Microsoft 博客。

此解决方案由 Microsoft 拥有和管理。Citrix 支持所涉及的 Citrix 组件：Citrix Workspace™ 应用程序、虚拟通道允许列表以及本页描述的插件部署机制。有关 Microsoft 拥有的架构和完整详细信息，请参阅 Microsoft 文档中的Teams 的新 VDI 解决方案。



系统要求

本节列出了支持 Teams 的新 VDI 解决方案所需的最低和推荐版本。在最低版本上，某些关键错误修复或最新功能可能不可用。部署推荐版本以获得最佳体验。

虚拟投递代理 (VDA)

> **注意：**
>
> 如果您使用的是 2203 LTSR CU2 或更低版本，或者 2303 CR 或更低版本，请参阅 CTX682593 以了解这些版本中的限制并规划您的升级。

最低版本	推荐版本
2203 LTSR CU3；2305 CR	2203 LTSR CU5+；2402 LTSR 和任何更高版本的 CR

适用于 Windows 的 Citrix Workspace 应用程序

最低版本	推荐版本
2203 LTSR（最新 CU）；2302 CR	2402 LTSR；2405 CR 或更高版本

适用于 Mac 的 Citrix Workspace 应用程序

最低版本	推荐版本
2508.10	2607 或更高版本

Mac 端点需要 macOS 14、15 或 26。macOS 26 需要 Citrix Workspace 应用程序 2511 或更高版本。在适用于 Mac 的 Citrix Workspace 应用程序 2508.10 上，必须手动安装插件。通过 Citrix Workspace 应用程序、客户端应用程序管理或虚拟通道插件管理器安装插件的选项从适用于 Mac 的 Citrix Workspace 应用程序 2603 开始提供。

有关最低 Microsoft Teams 版本、端点操作系统要求和硬件要求，请参阅 Microsoft 文档。

组件

- 新 Teams `vdiBridge`：与 Teams 捆绑的服务器端虚拟通道模块。
- 自定义虚拟通道 (VC)：Microsoft Teams 拥有的自定义 VC。
- 插件：客户端 VC dll。负责媒体引擎的下载和清理。
- 媒体引擎 (SlimCore)：由 Microsoft 以 MSIX 包形式提供的特定于操作系统的媒体引擎。

部署

1. 确保您拥有 先决条件 中列出的 Microsoft Teams 版本。
2. 配置**虚拟通道允许列表**策略以允许 Microsoft Teams 虚拟通道。这些通道允许 Teams 客户端连接到客户端插件。有关详细信息，请参阅 虚拟通道安全性。

   此解决方案需要三个自定义虚拟通道。使用通配符允许 `ms-teams.exe` 可执行文件和自定义虚拟通道：

   ```
   MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

   MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

   MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
   ```

   注意：

   - VDA 2603 及更高版本默认允许这三个虚拟通道。这些版本不需要 Studio 策略配置。
   - 虚拟通道允许列表策略的通配符在 CVAD 2203 LTSR CU2 及更高版本，或 Citrix Virtual Apps and Desktops™ 2206 CR 及更高版本中可用。
   - VDA 计算机必须重新启动才能使策略生效。
   - MSTeams 安装路径会更改，因为它是一个 MSIX 应用程序，因此需要通配符。允许上面显示的精确行。

3. 此解决方案由 Microsoft Teams 端的策略控制，而不是由 Citrix 策略控制。它默认启用。要为特定用户组启用或禁用它，请参阅 Microsoft 文档。
4. 在您的端点上部署 Teams 插件。请参阅安装 Teams 插件的选项。
5. 有关媒体引擎暂存和注册以及可能阻止 MSIX 安装的组策略，请参阅 Microsoft 文档。

安装 Teams 插件的选项

无论采用何种安装方法，插件都将放置在端点上的 Citrix Workspace 应用程序位置：

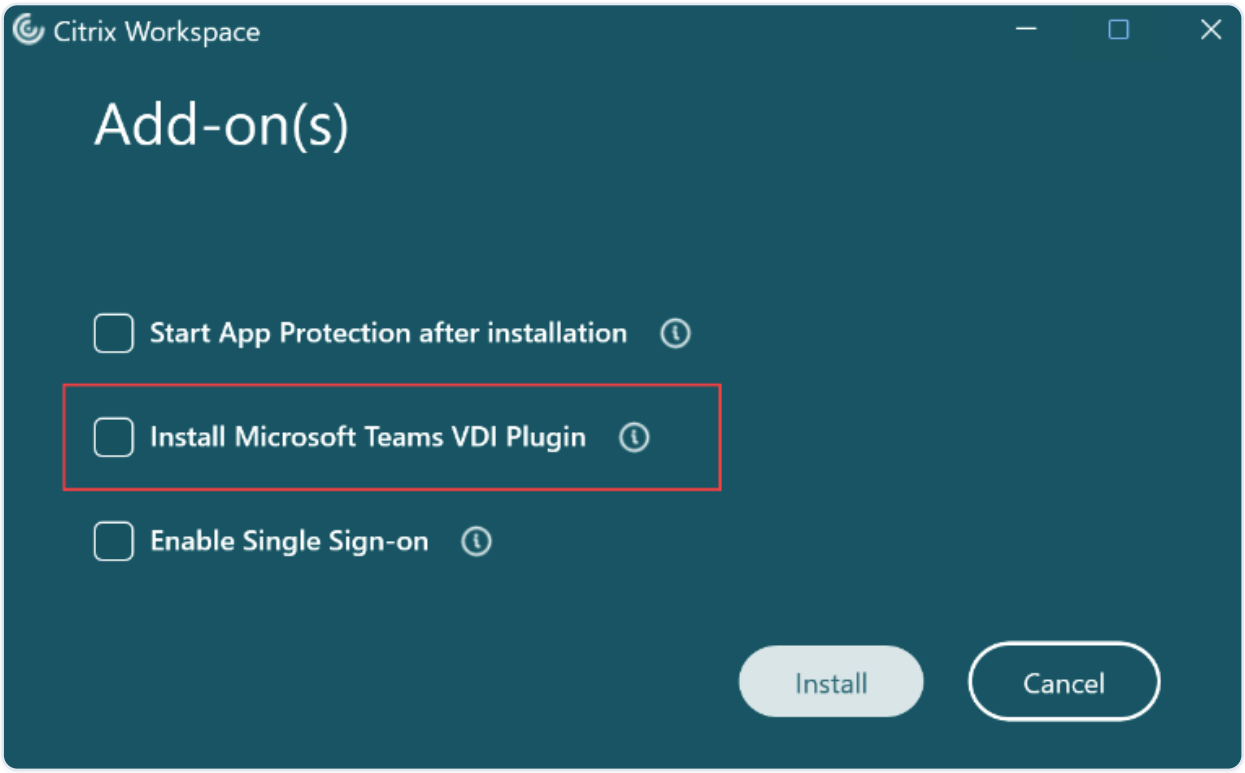
- Windows (`MsTeamsPluginCitrix.dll`)：64 位 `C:\Program Files (x86)\Citrix\ICA Client`；32 位 `C:\Program Files\Citrix\ICA Client`
- Mac: `/Applications/Utilities/MsTeamsVdi.Plugin.app`

注意：

- 在 Windows 上，以管理员模式安装 Citrix Workspace 应用程序，以便虚拟通道正确打开。不支持按用户安装 Citrix Workspace 应用程序。
- 从 Microsoft Store 安装 Citrix Workspace 应用程序时，不支持 Microsoft Teams VDI 插件。
- 如果在端点上未找到 Citrix Workspace 应用程序，则插件安装将停止。
- 在 Windows 上，插件和 Citrix Workspace 应用程序必须具有相同的体系结构。32 位 Citrix Workspace 应用程序无法加载 64 位插件。
- 插件可以升级或修复，但不能降级，并且只能在没有活动会话时进行。

选项 1：通过 Citrix Workspace 应用程序安装

- **Windows：** 在全新安装或手动升级期间，在**附加组件**页面上选择**安装 Microsoft Teams VDI 插件**。从适用于 Windows 2508 的 Citrix Workspace 应用程序开始，此选项默认处于选中状态。清除此选项可跳过安装。升级会记住您之前的选择。



您还可以使用 `/InstallMSTeamsPlugin` 开关从命令行安装。例如，`CitrixWorkspaceApp.exe /InstallMSTeamsPlugin=Y` 安装插件，而 `/InstallMSTeamsPlugin=N` 阻止安装。

对于全新安装，最低要求是适用于 Windows 2402 LTSR 的 Citrix Workspace 应用程序。对于就地升级，最低要求是适用于 Windows 2405 CR 的 Citrix Workspace 应用程序。有关最新详细信息，请参阅 安装第三方插件。

- **Mac：** 在 Citrix Workspace 应用程序安装期间安装插件的选项从适用于 Mac 2603 的 Citrix Workspace 应用程序开始提供，并且需要用户操作。适用于 Mac 2607 的 Citrix Workspace 应用程序默认自动安装插件。在适用于 Mac 2508.10 的 Citrix Workspace 应用程序上，请手动安装插件。请参阅 选项 2：直接下载插件。

选项 2：直接下载插件

- **Windows：** 下载 MSI 并使用 SCCM 或 Intune 等工具将其部署到任何受支持的 Citrix Workspace 应用程序版本上：
  - 32 位 思杰工作区应用程序：aka.ms/plugin
  - 64 位 思杰工作区应用程序：aka.ms/plugin_x64
  - 适用于 Arm 架构的 Citrix Workspace 应用程序：aka.ms/plugin_arm64
- **Mac：** 从 aka.ms/macplugin 下载插件并使用 JAMF 等工具进行部署。

选项 3：客户端应用程序管理（以前称为全局应用程序配置服务）

客户端应用程序管理（以前称为全局应用程序配置服务，或 GACS）管理托管和非托管端点的应用程序设置，并且可以在您的端点上部署 Teams 插件。在 Mac 上，这需要适用于 Mac 2603 或更高版本的 Citrix Workspace 应用程序。请参阅 Microsoft Teams VDI 插件管理。

选项 4：虚拟通道插件管理器

虚拟通道插件管理器为需要端点组件的应用程序（包括适用于 Teams 的新 VDI 解决方案）在客户端端点上部署插件。它检测在 VDA 上运行的应用程序，并提示用户在端点上安装插件。管理员可以在 BYOD 场景中使用它。在 Mac 上，这需要适用于 Mac 2603 或更高版本的 Citrix Workspace 应用程序。请参阅 虚拟通道插件管理器。

插件更新场景

当通过选项 1、3 或 4 安装插件时，Citrix 会无缝处理 Teams 插件更新。如果插件是手动安装的（选项 2），Citrix 不会处理更新。

- 确保 Citrix Workspace 应用程序自动更新已开启，以便进行插件自动更新。
- 确保 Windows 版 Citrix Workspace 应用程序最低版本为 2405。Windows 版 Citrix Workspace 应用程序 2508 或更高版本在 Citrix Workspace 应用程序自动更新时会自动安装插件。
- Citrix 不负责插件的卸载。如有需要，请单独卸载插件。

> **注意：**
>
> Citrix 负责 Teams 插件的更新，而不负责媒体引擎的更新。媒体引擎由 Microsoft 提供和更新。

作为 Citrix 发布应用程序的 Teams

当所有必需组件都满足最低版本要求时，作为 Citrix Virtual Apps 应用程序发布的 Teams 可以通过此解决方案进行优化。有关所需版本和已知限制，请参阅 Microsoft 文档。

互操作性和漫游

有关 Teams 新 VDI 解决方案和 Citrix HDX 优化如何协同工作以及漫游行为的信息，请参阅 Optimization for Microsoft Teams。

网络注意事项

请参阅 Microsoft 文档中的 Networking considerations。

功能支持

功能集和实现由 Microsoft 拥有。请参阅 Microsoft 文档中的 feature list。

故障排除

Microsoft Teams 客户端会报告优化状态，并在优化失败时报告错误代码。这些状态指示器和错误代码由 Microsoft 定义。有关完整列表和端到端故障排除，请参阅 Microsoft 文档中的 Troubleshooting the New VDI solution for Teams。

Citrix Monitor 提供此解决方案优化状态的可视性。在会话详细信息中，“会话拓扑”视图显示应用程序是否已优化，并标记任何缺失的组件，例如插件管理器、插件及其版本、虚拟通道状态以及虚拟通道允许列表状态。有关更多信息，请参阅 Real-time communications optimization visibility。

某些 Microsoft 错误代码指向 Citrix 端的配置。常见的 Citrix 检查：

- 如果 Teams 客户端报告自定义虚拟通道被阻止 (Microsoft 错误 2003)，请确认虚拟通道允许列表包含 MSTEAMS、MSTEAM1 和 MSTEAM2。
- 如果 Teams 客户端报告未检测到插件 (Microsoft 错误 2000)，请确认插件已安装并加载。在 Process Explorer 中，选择 `wfica32.exe`，显示下部窗格，并在 DLL 选项卡中检查 `MsTeamsPluginCitrix.dll`。
- 如果 Teams 客户端报告了不受支持的 Citrix Workspace 应用程序版本（Microsoft 错误 2004），请升级到受支持的版本。请参阅系统要求。

已知限制

这些功能和实现由 Microsoft 拥有。请参阅 Microsoft 文档中的已知问题。

Microsoft Teams（经典版）优化

> **注意：**
>
> 新的 Microsoft Teams 2.1 现已面向 VDA 正式发布。此 Microsoft Teams 版本与使用 WebRTC (VDI 1.0) 的 Citrix Microsoft Teams 优化兼容。
>
> 从 Citrix Virtual Apps and Desktops 2402 开始，您无需手动配置 `msedgewebview2.exe` 注册表项，因为它默认已列入允许列表。
>
> 新的 Microsoft Teams 现已支持已发布的应用程序。
>
> Citrix 使用 Citrix Virtual Apps and Desktops™ 和 Citrix Workspace™ 应用程序为基于桌面的 Microsoft Teams 提供优化。默认情况下，我们将所有必需的组件捆绑到 Citrix Workspace 应用程序和虚拟投递代理 (VDA) 中。

我们对 Microsoft Teams 的优化包括 VDA 端的 HDX™ 服务以及一个用于与 Microsoft Teams 托管应用程序接口以接收命令的 API。这些组件会打开一个控制虚拟通道 (CTXMTOP) 到 Citrix Workspace 应用程序端的媒体引擎。端点在本地解码并提供多媒体，将 Citrix Workspace 应用程序窗口移回托管的 Microsoft Teams 应用程序中。

身份验证和信令在 Microsoft Teams 托管应用程序上本地发生，就像其他 Microsoft Teams 服务（例如聊天或协作）一样。音频/视频重定向不会影响它们。

`CTXMTOP` 是一个命令和控制虚拟通道。这意味着媒体不会在 Citrix Workspace 应用程序和 VDA 之间交换。

仅支持客户端获取/客户端渲染。

此视频演示将向您介绍 Microsoft Teams 在 Citrix 虚拟环境中的工作方式。



微软团队安装

Citrix 和 Microsoft 建议使用最新版本的 Microsoft Teams 并保持其更新。 发布日期比当前版本发布日期早 90 天以上的 Microsoft Teams 桌面应用程序版本不受支持。 不受支持的 Microsoft Teams 桌面应用程序版本会向用户显示阻止页面，并要求更新应用程序。

有关最新可用版本的信息，请参阅 Microsoft Teams 应用（桌面版和 Mac 版）的更新历史记录。

建议您遵循 Microsoft Teams 全机安装指南。避免使用将 Microsoft Teams 安装到 `AppData` 的 .exe 安装程序。相反，请使用命令行中的 `ALLUSER=1` 标志将其安装到 `C:\Program Files (x86)\Microsoft\Teams`。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

此示例还使用 `ALLUSERS=1` 参数。设置此参数后，Microsoft Teams 全局安装程序将显示在**控制面板**中的**程序和功能**中。此外，它还会显示在计算机所有用户的 Windows 设置中的**应用和功能**中。如果所有用户都具有管理员凭据，则可以卸载 Microsoft Teams。

了解 `ALLUSERS=1` 和 `ALLUSER=1` 之间的区别非常重要。您可以在非 VDI 和 VDI 环境中使用 `ALLUSERS=1` 参数。仅在 VDI 环境中使用 `ALLUSER=1` 参数来指定每计算机安装。

在 `ALLUSER=1` 模式下，Microsoft Teams 应用程序在新版本发布时不会自动更新。我们建议将此模式用于非持久性环境，例如 Windows Server 或 Windows 10 随机/池化目录中的托管共享应用程序或桌面。有关详细信息，请参阅 使用 MSI 安装 Microsoft Teams（VDI 安装部分）。

假设您有一个 Windows 10 专用持久性 VDI 环境。您希望 Microsoft Teams 应用程序自动更新，并希望 Microsoft Teams 以每用户方式安装在 `Appdata/Local` 下。在这种情况下，请使用 `.exe` 安装程序或不带 `ALLUSER=1` 的 MSI。

> **注意：**
>
> Citrix 建议在黄金映像中安装 Microsoft Teams 之前安装 VDA。此安装顺序是使 `ALLUSER=1` 标志生效所必需的。如果您在安装 VDA 之前已在虚拟机中安装 Microsoft Teams，请卸载并重新安装 Microsoft Teams。

适用于远程电脑访问

Citrix 建议在安装 VDA 后安装 Microsoft Teams 版本 1.4.00.22472 或更高版本。否则，您需要注销并重新登录，Microsoft Teams 才能按预期检测到 VDA。版本 1.4.00.22472 及更高版本包含在 Microsoft Teams 启动时和登录时运行的增强逻辑，用于 VDA 检测。这些版本还包括活动会话类型

识别（HDX、RDP 或本地连接到客户端计算机）。如果您是本地连接，以前版本的 Microsoft Teams 可能无法检测并禁用某些功能或 UI 元素。例如，分组讨论室、会议和聊天弹出窗口或会议反应。

> **重要提示：**
>
> 当您从本地会话漫游到 HDX 会话，并且 Microsoft Teams 在后台保持打开和运行状态时，您必须退出并重新启动 Microsoft Teams 才能正确地与 HDX 进行优化。 相反，如果您通过优化的 HDX 会话远程使用 Microsoft Teams，请断开 HDX 会话，并在设备上本地重新连接到相同的 Windows 会话。在办公室工作时，您必须重新启动 Microsoft Teams，以便它能够正确检测远程 PC 访问状态（HDX 或本地）。因为 Microsoft Teams 只能在应用程序启动时评估 VDI 模式，而不能在它已经在后台运行时评估。如果不重新启动，Microsoft Teams 可能无法加载弹出窗口、分组讨论室或会议反应等功能。

对于应用程序分层

如果使用 Citrix App Layering 在不同层中管理 VDA 和 Microsoft Teams 安装，则必须在从命令行使用 `ALLUSER=1` 标志安装 Microsoft Teams 之前，在 Windows VDA 上创建注册表项。有关更多信息，请参阅 多媒体 下的 *使用 Citrix App Layering 优化 Microsoft Teams* 部分。

配置文件管理建议

我们建议将计算机范围安装程序用于 Windows Server 和池化 VDI Windows 10 环境。

当从命令行将 **ALLUSER=1** 标志传递给 MSI（全机安装程序）时，Microsoft Teams 应用程序将安装在 `C:\Program Files (x86)` (~300 MB) 下。该应用程序使用 `AppData\Local\Microsoft\TeamsMeetingAddin` 存储日志，使用 `AppData\Roaming\Microsoft\Teams` (~600–700 MB) 存储用户特定配置、用户界面元素缓存等。

> **重要提示：**
>
> 如果您不传递 **ALLUSER=1** 标志，MSI 会将 Teams.exe 安装程序和 `setup.json` 放置在 `C:\Program Files (x86)\Teams Installer` 下。注册表项 (TeamsMachineInstaller) 将添加到：`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`

> 随后的用户登录将改为触发 **AppData** 中的最终安装。

计算机范围安装程序

以下是在任何 Windows Server 64 位 VM 上安装 Microsoft Teams 全机安装程序所创建的文件夹、桌面快捷方式和注册表示例：

文件夹：

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

桌面快捷方式:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

注册表:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- 名称: `Teams`
- 类型: `REG_SZ`
- 值: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **注意：**
>
> 注册表位置因底层操作系统和位数而异。

建议

- 我们建议通过删除 Microsoft Teams 注册表项来禁用自动启动。这样做可以防止许多同时发生的登录（例如，在工作日开始时）导致 VM 的 CPU 飙升。
- 如果虚拟桌面没有 GPU/vGPU，我们建议在 Microsoft Teams **设置**中设置**禁用 GPU 硬件加速**以提高性能。此设置 (`"disableGpu":true`) 存储在 `desktop-config.json` 中的 `%Appdata%\Microsoft\Teams` 。您可以使用登录脚本编辑该文件并将值设置为 `true` 。

- 如果使用 Citrix Workspace Environment Management™ (WEM)，请启用**CPU 峰值保护**以管理 Microsoft Teams 的处理器消耗。

每用户安装程序

使用 `.exe` 安装程序时，安装过程有所不同。所有文件都放置在 AppData 中。

文件夹:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

桌面快捷方式:

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

注册表:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

最佳实践

最佳实践建议基于用例场景。 在非持久性设置中使用 Microsoft Teams 需要配置文件缓存管理器，以实现高效的 Microsoft Teams 运行时数据同步。使用配置文件缓存管理器，在用户会话期间会缓存适当的用户特定信息。例如，用户特定信息包括用户数据、配置文件和设置。同步这两个文件夹中的数据：

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Microsoft Teams 缓存内容排除列表，适用于非持久性设置

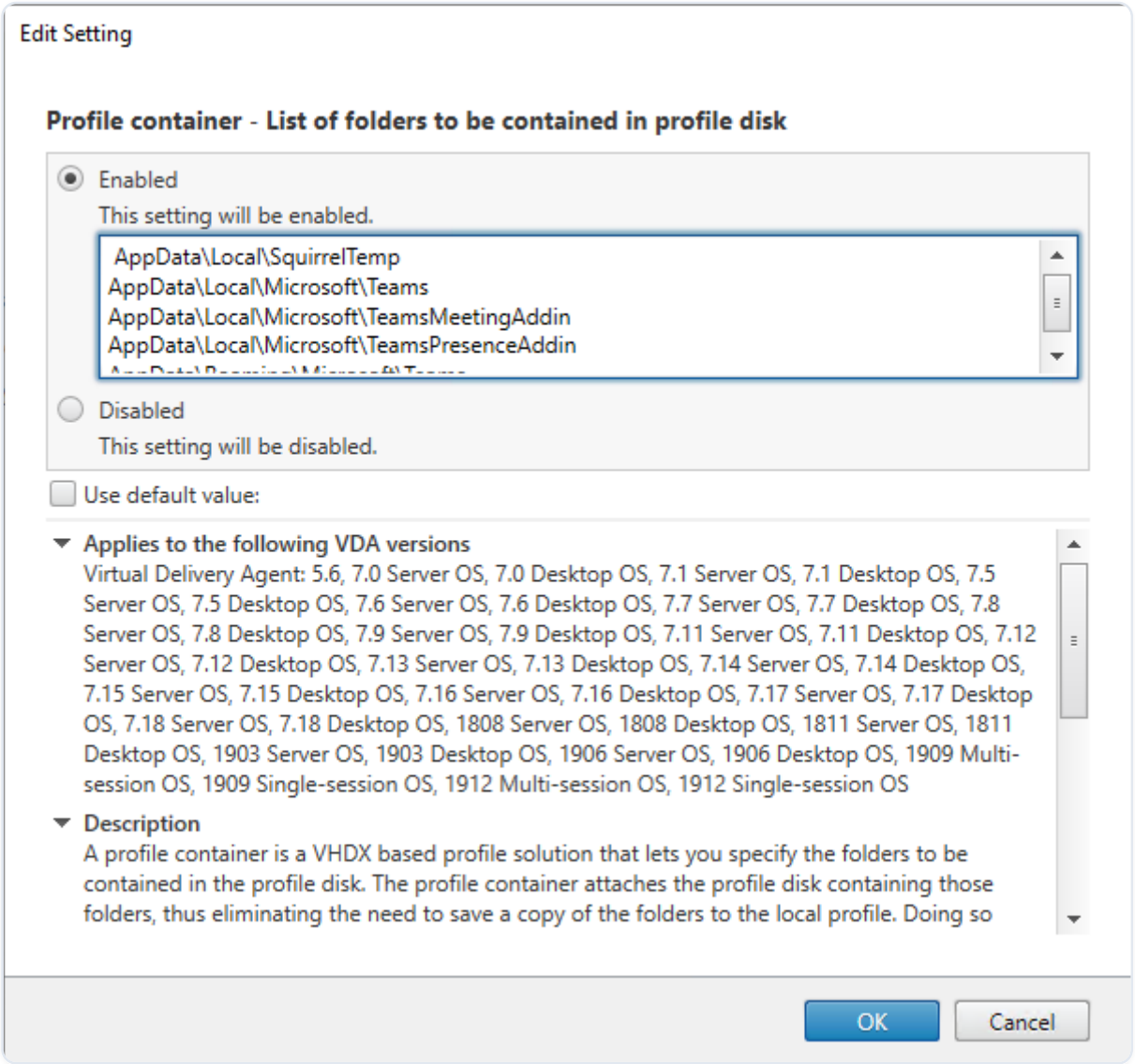
按照 Microsoft 文档中的说明，从 Microsoft Teams 缓存文件夹中排除文件和目录。此操作有助于减小用户缓存大小，从而进一步优化您的非持久性设置。

用例：单会话场景

在此场景中，最终用户一次在一个位置使用 Microsoft Teams。他们不需要同时在两个 Windows 会话中运行 Microsoft Teams。在常见的虚拟桌面部署中，每个用户分配到一个桌面，Microsoft Teams

作为单个应用程序部署在虚拟桌面中。 我们建议启用 Citrix Profile 容器，并将 Per-user installer 中列出的每个用户目录重定向到该容器中。

1. 在黄金映像中部署 Microsoft Teams 机器范围安装程序 (**ALLUSER=1**)。
2. 启用 Citrix Profile Management 并设置具有适当权限的用户配置文件存储。
3. 启用以下 Profile Management 策略设置：**文件系统 > 同步 > 配置文件容器 – 配置文件磁盘中包含的文件夹列表**。



列出此配置中的所有每用户目录。您还可以使用 Citrix Workspace Environment Management (WEM) 服务配置这些设置。

4. 将设置应用于正确的交付组。
5. 登录以验证部署。

系统要求

最低推荐版本 - Delivery Controller (DDCs) 1906.2

如果您使用的是早期版本，请参阅 启用 Microsoft Teams 优化：

支持的操作系统：

- Windows Server 2022、2019、2016、2012R2 Standard 和数据中心版，以及带 Server Core 选项的版本

最低版本 - 虚拟交付代理 (VDA) 1906.2

支持的操作系统：

- Windows 十一
- Windows 10 64 位，版本 1607 及更高版本。Citrix Workspace 应用程序 for Windows 2109.1 及更高版本支持 VM 托管应用程序。
- Windows Server 2022、2019、2016 和 2012 R2（标准版和数据中心版）

要求：

- BCR_x64.msi - 包含 Microsoft Teams 优化代码并从 GUI 自动启动的 MSI。如果您使用命令行界面进行 VDA 安装，请勿将其排除。

推荐版本 – 适用于 Windows 的 Citrix Workspace 应用程序最新 CR 和最低版本 - 适用于 Windows 的 Citrix Workspace 应用程序 1907

- 视窗 11。
- Windows 10（32 位和 64 位版本，包括嵌入式版本）（对 Windows 7 的支持已在版本 2006 停止）（对 Windows 8.1 的支持已在版本 2204.1 停止）。
- Windows 10 物联网企业版 2016 LTSB (v1607) 和 2019 LTSC (v1809)。
- 支持的处理器 (CPU) 架构：x86 和 x64（不支持 ARM）。
- 端点要求：大约 2.2–2.4 GHz 双核 CPU，可在点对点视频会议通话期间支持 720p 高清分辨率。
- 双核或四核CPU，基础速度较低（约1.5 GHz），配备Intel Turbo Boost或AMD Turbo Core，可提升至至少2.4 GHz。
- 经验证的HP瘦客户端：t630/t640、t730/t740、mt44/mt45。
- 经验证的Dell瘦客户端：5070、5470移动TC和一体机。
- 经验证的10ZiG瘦客户端：4510和5810q。

- 有关经验证的端点的完整列表，请参阅瘦客户端。
- Citrix Workspace app 至少需要 600 MB 可用磁盘空间和 1 GB RAM。
- Microsoft .NET Framework 的最低要求是版本 4.8。如果系统中不存在 .NET Framework，Citrix Workspace app 会自动下载并安装它。

管理员可以通过更改Microsoft Teams 优化策略来启用/禁用以优化模式启动 Microsoft Teams。在 Citrix Workspace app 中以优化模式启动的用户无法禁用 Microsoft Teams。

最低版本 - 适用于 Linux 的 Citrix Workspace 应用程序 2006

有关详细信息，请参阅适用于 Linux 的 Citrix Workspace app 文档中的Microsoft Teams 优化。

软件：

- `GStreamer` 1.0 或更高版本，或 Cairo 2
- `libc++-9.0` 或更高版本
- `libgdk` 3.22 或更高版本
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04 或更高版本

身份验证增强功能：

- Libsecret 程序库
- libunwind-12 库。有关详细信息，请参阅为 llvm-12 添加 libunwind-12 库依赖项。

硬件：

- 最低 1.8 GHz 双核 CPU，能够在点对点视频会议通话期间支持 720p 高清分辨率
- 双核或四核 CPU，基本速度为 1.8 GHz，Intel Turbo Boost 高速至少为 2.9 GHz

有关已验证端点的完整列表，请参阅瘦客户端。

有关详细信息，请参阅安装 Citrix Workspace 应用程序的必备条件。

您可以通过将 `/opt/Citrix/ICAClient/config/module.ini` 文件中 **VDWEBRTC** 字段的值更新为 Off 来禁用 Microsoft Teams 优化。默认值为 VDWEBRTC=On。更新完成后，重新启动会话。（需要 Root 权限）。

最低版本 - 适用于 Mac 的 Citrix Workspace 应用程序 2012

支持的操作系统：

- macOS Catalina (10.15) 版本。
- macOS Big Sur 11.0.1 及更高版本。
- macOS Monterey 版本。

支持的功能：

- 音频
- 视频
- 屏幕共享优化（传入和传出）

> **注意：**
>
> Citrix Viewer 应用程序需要访问 macOS 安全与隐私偏好设置才能使屏幕共享正常工作。用户可以在 **Apple 菜单 > 系统偏好设置 > 安全与隐私 > 隐私选项卡 > 屏幕录制** 中配置此偏好设置，然后选择 **Citrix Viewer**。

> Microsoft Teams 优化默认情况下适用于 Citrix Workspace 应用程序 2012 及更高版本以及 macOS 10.15。

如果要禁用 Microsoft Teams 优化，请在终端中运行此命令并重新启动 Citrix Workspace 应用程序：

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

最低版本 - 适用于 ChromeOS 的最新版 Citrix Workspace 应用程序，运行于最新版 ChromeOS 上

硬件：

- 性能与 Intel i3 四核 2.4 GHz 处理器相当或更优的处理器。

支持的功能：

- 音频
- 视频
- 屏幕共享优化（传入和传出）- 默认禁用。有关如何启用此功能的说明，请参阅这些设置。

单服务器可扩展性

本节提供建议和指导，以估算单个物理主机可支持的用户或虚拟机 (VM) 数量。这通常被称为 Citrix Virtual Apps and Desktops™ 单服务器可伸缩性 (SSS)。在 Citrix Virtual Apps (CVA) 或会话虚拟化环境中，它也常被称为用户密度。其目的是找出在运行主要虚拟机管理程序的单个硬件上可以运行多少用户或虚拟机。

> **注意：**
>
> 本节包含估算 SSS 的指导。此指导是高级别的，可能不一定适用于您的独特情况或环境。真正了解 Citrix Virtual Apps and Desktops SSS 的唯一方法是使用可伸缩性或负载测试工具，例如 Login VSI。Citrix 建议仅使用此指导和这些简单规则来快速估算 SSS。但是，Citrix 建议使用 Login VSI 或您选择的负载测试工具来验证结果，尤其是在购买硬件或做出任何财务决策之前。

硬件（被测系统）

- 戴尔 PowerEdge R740
- Intel Xeon (Gold) 6126 @ 2.60 GHz (最大睿频 3.70 GHz)，每个插槽 12 个核心，双插槽，启用超线程
- 382 GB 内存
- 本地 SSD RAID 0 存储（11 块磁盘）6 TB

软件

单个虚拟机（40 个逻辑处理器），运行 Windows 2019 (TSVDA) 和 Citrix Virtual Apps and Desktops 2106 VMware ESXi 6.7

术语

- 知识工作者工作负载：包括 Acrobat Reader、Freemind/Java、照片查看器、Edge 以及 MS Office 应用程序，例如 Excel、Outlook、PowerPoint 和 Word。
- 基准：运行知识工作者工作负载（不含 Microsoft Teams）的服务器可伸缩性测试。
- Microsoft Teams 工作负载：知识工作者典型工作负载 + Microsoft Teams。

Microsoft Teams 如何进行压力测试

- Microsoft Teams 已通过 HDX 优化。因此，所有多媒体处理都卸载到端点或客户端，不属于测量范围。

- 在工作负载启动之前，所有 Microsoft Teams 进程都已停止或终止。
- 打开 Microsoft Teams（冷启动）。
- 测量 Microsoft Teams 加载并获取 Microsoft Teams 主窗口焦点所需的时间。
- 使用键盘快捷方式切换到聊天窗口。
- 使用键盘快捷方式切换到日历窗口。
- 使用键盘快捷方式向特定用户发送聊天消息。
- 使用键盘快捷方式切换到 Microsoft Teams 窗口。

结果

- 与基线（137 个用户）相比，Microsoft Teams 工作负载（81 个用户）的可伸缩性影响为 40%。
- 将服务器容量（CPU）增加约 40% 可使用户数量恢复到基线工作负载时的水平。
- 与基线相比，Microsoft Teams 工作负载需要额外 20% 的内存。
- 将每个用户的存储大小增加 512-1024 MB。
- IOPS 写入增加约 50%，IOPS 读取增加约 100%。Microsoft Teams 在存储速度较慢的环境中可能会产生显著影响。

功能矩阵和版本支持

功能	MICROSOFT TEAMS（最低版本）	VDA（最低版本）	适用于 WINDOWS CR 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 MAC 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 LINUX 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 CHROME OS 的 CITRIX WORKSPACE 应用程序（最低版本）
音频/视频（P2P 和会议）	当前版本减 90 天	1906	1907	2009	2004	2105.5
屏幕共享	当前版本减去 90 天	1906	1907	2012	2006	2105.5
i. 屏幕指示器红色边框	当前版本减去 90 天	1906	2002	2012	2006	否

功能	MICROSOFT TEAMS（最低版本）	VDA（最低版本）	适用于 WINDOWS CR 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 MAC 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 LINUX 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 CHROME OS 的 CITRIX WORKSPACE 应用程序（最低版本）
ii. 将捕获限制为 Desktop Viewer	当前版本减去 90 天	1906	2009.5	2012	2006	否
三、多显示器	当前版本减去 90 天	1912 CU6+	2106 (1)	2106	2106	否
DTMF	当前版本减去 90 天	N/A	2102	2101	2101	2111.1
代理服务器支持	当前版本减去 90 天	N/A	2012 (2)	2104 (3)	2101 (3)	2305
应用程序共享	当前版本减去 90 天	2109	2109.1	2203.1	2209	否
实时字幕	当前版本减去 90 天	不适用 (4)	2109.1	2109	2109	2303
动态 e911	当前版本减去 90 天	N/A	2112.1	2112	2112	2112
授予控制权	当前版本减去 90 天	N/A	2112.1	2203.1	否	否

功能	MICROSOFT TEAMS（最低版本）	VDA（最低版本）	适用于 WINDOWS CR 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 MAC 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 LINUX 的 CITRIX WORKSPACE 应用程序（最低版本）	适用于 CHROME OS 的 CITRIX WORKSPACE 应用程序（最低版本）
请求控制权	当前版本减去 90 天	N/A	2112.1	2203.1	2203	2303
多窗口	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
会议转录	当前版本减去 90 天	2112.1, 1912 CU6+	2112	2203.1	2203	2303
背景模糊	当前版本减去 90 天	2112, 1912 CU6+	2207	2301	2212	2303

1. CD Viewer 仅支持全屏模式。不支持 SHIFT+F2。
2. Negotiate/Kerberos、NTLM、Basic 和 Digest。也支持 `Pac` 文件。
3. 仅匿名。
4. 如果 VDA 版本为 2112 或更高，则实时字幕仅在 Citrix Workspace 应用程序版本为 Mac 2203.1、Linux 2203 或 Windows 2112 时才有效。这是因为如果 Microsoft Teams 处于单窗口 UI 模式或多窗口模式，实时字幕的行为会有所不同。
5. MultiWindow 在 2112 VDA 中引入，但已向后移植到 VDA 1912 LTSR CU6 版本。

注意：

- 在 **适用于 Windows 1912 CU6（或更高版本）的 Citrix Workspace 应用程序** 中列出的所有功能均适用于适用于 Windows 2203.1 LTSR CU1 的 Citrix Workspace 应用程序。

- Microsoft 已弃用对 Microsoft Teams 中单窗口模式的支持。为符合要求，您必须将 VDA 升级到 1912 CU6+ LTSR，并将 Citrix Workspace 应用程序升级到 2203 CU2+ 或更高版本，这些版本支持多窗口模式。

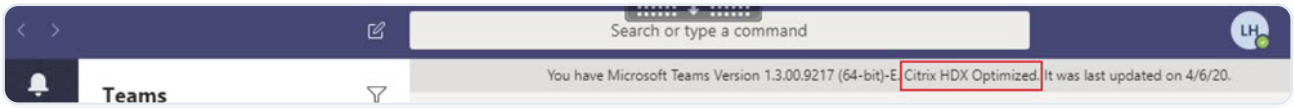
启用 Microsoft Teams 优化

要启用 Microsoft Teams 优化，请使用 Microsoft Teams 重定向 策略中描述的“管理”策略。此策略默认处于**启用**状态。除了启用此策略外，HDX 还会检查以验证 Citrix Workspace 应用程序的版本是否至少达到最低要求版本。如果启用了该策略且 Citrix Workspace 应用程序版本受支持，则 VDA 上的 **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** 将自动设置为 **1**。Microsoft Teams 读取此项以在 VDI 模式下加载。

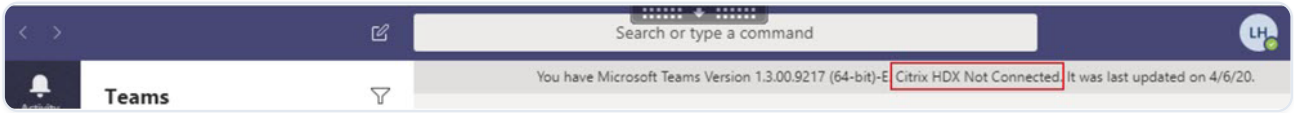
注意：

如果您使用的是 1906.2 或更高版本的 VDA，或者使用的是在“管理”控制台 (Studio) 中没有可用策略的旧控制器版本（例如，版本 7.15），您的 VDA 仍然可以进行优化。VDA 中默认启用 Microsoft Teams 的 HDX 优化。

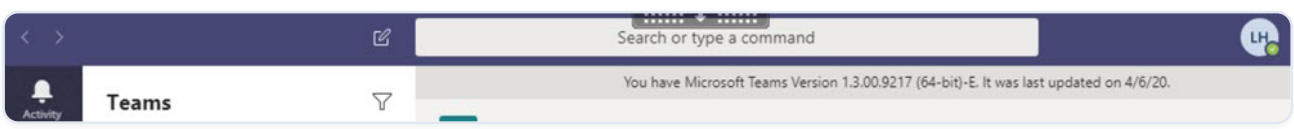
如果单击“**关于 > 版本**”，则会显示“**Citrix HDX 已优化**”图例：



如果看到“**Citrix HDX 未连接**”，则表示 Citrix API 已加载到 Microsoft Teams 中。加载 API 是重定向的第一步。但堆栈的后续部分存在错误。该错误很可能出现在 VDA 服务或 Citrix Workspace 应用程序中。



如果您没有看到任何图例，则表示 Microsoft Teams 未能加载 Citrix API。右键单击通知区域图标并重新启动以退出 Microsoft Teams。确保“管理”策略未设置为**禁止**，并且 Citrix Workspace 应用程序版本受支持。



重要：会话重新连接

- 当连接性发生变化时，您可能需要重新启动 Microsoft Teams 才能获得 HDX 优化会话。例如，如果您从不受支持的端点（适用于 iOS、Android 或旧版 Windows/Linux/Mac 的 Workspace 应用程序）漫游到受支持的端点（适用于 Windows/Linux/Mac/ChromeOS/HTML5 的 Workspace 应用程序），反之亦然。
- 如果您已在 VDA 中使用 Microsoft Teams .exe 安装程序安装了该应用程序，则还需要重新启动 Microsoft Teams。.exe 安装程序推荐用于持久性 VDI 部署。在这种情况下，当 HDX 会话处于断开连接状态时，Microsoft Teams 可以自动更新。因此，重新连接到 HDX 会话的用户会发现 Microsoft Teams 未优化运行。
- 当您从本地会话漫游到 HDX 会话时，必须重新启动 Microsoft Teams 以使用 HDX 进行优化。在远程电脑访问方案中需要此操作。

网络要求

Microsoft Teams 依赖 Microsoft 365 中的媒体处理器服务器进行会议或多方通话。此外，Microsoft Teams 依赖 Microsoft 365 传输中继来处理以下场景：

- 点对点呼叫中的两个对等方没有直接连接
- 参与者与媒体处理器没有直接连接。

因此，对等方与 Microsoft 365 云之间的网络状况决定了通话性能。有关网络规划的详细指南，请参阅 Microsoft 365 网络连接原则。

我们建议评估您的环境，以识别可能影响您的整体云语音和视频部署的任何风险和要求。 使用 Skype for Business 网络评估工具 测试您的网络是否已为 Microsoft Teams 做好准备。有关支持信息，请参阅 支持。

实时传输协议 (RTP) 流量的关键网络建议摘要

- 从分支机构尽可能直接连接到 Microsoft 365 网络。
- 规划并提供分支机构的充足带宽。
- 检查每个分支机构的网络连接和质量。
- 如果您必须在分支机构使用以下任何一项，请确保 RTP/UDP 流量（由 Citrix Workspace 应用程序中的 HdxRtcEngine.exe 处理）畅通无阻。
    - 绕过代理服务器
    - 网络 SSL 拦截
    - 深度包检测设备

- VPN 回环（如果可能，请使用拆分隧道）

重要提示：VPN 拆分隧道配置

HdxRtcEngine.exe 流量必须从 VPN 隧道中分流，并允许使用用户的本地 Internet 连接直接连接到服务。实现此目的的方式取决于所使用的 VPN 产品和机器平台，但大多数 VPN 解决方案都允许通过一些简单的策略配置来应用此逻辑。有关 VPN 平台特定分流隧道指南的更多信息，请参阅 这篇 Microsoft 文章。

Workspace 应用程序中的 WebRTC 媒体引擎 (HdxRtcEngine.exe) 使用安全实时传输协议 (SRTP) 处理卸载到客户端的多媒体流。SRTP 为 RTP 提供机密性和身份验证。对于此功能，对称密钥（通过 DTLS 协商）用于使用 AES 加密算法加密媒体和控制消息。

建议使用以下指标以获得积极的用户体验：

指标	端点到 MICROSOFT 365
延迟（单向）	< 50 毫秒
延迟 (RTT)	< 100 毫秒
丢包率	在任意 15 秒间隔内 <1%
数据包到达间隔抖动	在任意 15 秒间隔内 <30 毫秒

有关更多信息，请参阅 为 Microsoft Teams 准备组织网络。

对于带宽要求，Microsoft Teams 优化可以使用各种音频编解码器 (OPUS/G.722/PCM G711) 和视频编解码器 (H264)。

对等方在呼叫建立过程中使用会话描述协议 (SDP) Offer/Answer 协商这些编解码器。 Citrix 对每个用户的最低建议是：

类型	带宽	编解码器
音频（每个方向）	约 90 kbps	G.722
音频（每个方向）	约 60 kbps	奥普斯*
视频（每个方向）	约 700 kbps	H264 360p @ 30 帧/秒 16:9

类型	带宽	编解码器
屏幕共享	约 300 kbps	H264 1080p @ 15 帧/秒

* Opus 支持从 6 kbps 到 510 kbps 的恒定和可变比特率编码。

Opus 和 H264 是点对点和电话会议的首选编解码器。

> **重要提示：**
>
> 关于性能，在客户端计算机上，编码比解码更消耗 CPU 资源。您可以在适用于 Linux 和 Windows 的 Citrix Workspace 应用程序中硬编码最大编码分辨率。请参阅 编码器性能估算器 和 Microsoft Teams 优化。

代理服务器

根据代理的位置，请考虑以下事项：

- VDA 上的代理配置：

  如果您在 VDA 中配置了显式代理服务器并通过代理路由到 localhost 的连接，则重定向会失败。要正确配置代理，您必须在 **Internet 选项 > 连接 > LAN 设置 > 代理服务器**中选择**“对于本地地址不使用代理服务器”**设置，并绕过 `127.0.0.1:9002`。

  如果您使用 PAC 文件，则 PAC 文件中的 VDA 代理配置脚本必须为 `wss://127.0.0.1:9002` 返回 **DIRECT**。否则，优化将失败。为确保脚本返回 **DIRECT**，请使用 `shExpMatch(url, "wss://127.0.0.1:9002/*")`。

- Citrix Workspace 应用程序上的代理配置：

  如果分支机构配置为通过代理访问 Internet，则以下版本支持代理服务器：

  - 适用于 Windows 的 Citrix Workspace 应用程序版本 2012（支持协商/Kerberos、NTLM、Basic 和 Digest。还支持 `Pac` 文件）
  - 适用于 Windows 的 Citrix Workspace 应用程序版本 1912 CU5（支持协商/Kerberos、NTLM、Basic 和 Digest。还支持 `Pac` 文件）
  - 适用于 Linux 的 Citrix Workspace 应用程序版本 2101（匿名身份验证）
  - 适用于 Mac 的 Citrix Workspace 应用程序版本 2104（匿名身份验证）

运行早期版本 Citrix Workspace 应用程序的客户端设备无法读取代理配置。这些设备直接将流量发送到 Microsoft 365 TURN 服务器。

重要提示：

- 验证客户端设备是否可以连接到 DNS 服务器以执行 DNS 解析。客户端设备必须能够解析以下 Microsoft Teams 中继服务器的 FQDN：
  - `worldaz.relay.teams.microsoft.com`
  - `inaz.relay.teams.microsoft.com`
  - `uaeaz.relay.teams.microsoft.com`
  - `euaz.relay.teams.microsoft.com`
  - `usaz.relay.teams.microsoft.com`
  - `turn.dod.teams.microsoft.us`
  - `turn.gov.teams.microsoft.us`

如果 DNS 请求不成功，则与外部用户的 P2P 通话以及媒体建立失败的电话会议将失败。

- 会议服务器的位置是根据第一个参与者的虚拟桌面位置（而不是客户端）选择的。

呼叫建立和媒体流路径

在可能的情况下，Citrix Workspace 应用程序中的 HDX WebRTC 媒体引擎 (HdxRtcEngine.exe) 尝试通过用户数据报协议 (UDP) 在点对点呼叫中建立直接网络安全实时传输协议 (SRTP) 连接。如果 UDP 高端口被阻止，媒体引擎将回退到 TCP/TLS 443。

HDX 媒体引擎支持 ICE、NAT 会话遍历实用程序 (STUN) 和使用 NAT 中继遍历 (TURN)，用于候选发现和建立连接。此支持意味着端点必须能够执行 DNS 解析。

设想这样一种情况：两个对等点之间或对等点与会议服务器之间没有直接路径，并且您正在加入多方呼叫或会议。HdxRtcEngine.exe 使用 Microsoft 365 中的 Microsoft Teams 传输中继服务器来连接其他对等点或媒体处理器（会议在此处托管）。您的客户端计算机必须能够访问三个 Microsoft 365 子网 IP 地址范围和四个 UDP 端口（如果 UDP 被阻止，则回退到 TCP/TLS 443）。有关详细信息，请参阅 呼叫设置 和 Office 365 URL 和 IP 地址范围 ID 11 中的体系结构图。

ID	类别	地址	目标端口
11	需要优化	13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15	**UDP：** 3478、3479、3480、3481，**TCP：** 443（回退）

这些范围包括传输中继和媒体处理器，由 Azure 负载均衡器前端。 Microsoft Teams 传输中继提供 STUN 和 TURN 功能，但它们不是 ICE 端点。此外，Microsoft Teams 传输中继不终止媒体、TLS 或执行任何转码。当它们将流量转发到其他对等方或媒体处理器时，它们可以将 TCP（如果 HdxRtcEngine.exe 使用 TCP）桥接到 UDP。

Workspace 应用程序 WebRTC 媒体引擎联系 Microsoft 365 云中最近的 Microsoft Teams 传输中继。媒体引擎使用任播 IP 和端口 3478–3481 UDP（每个工作负载使用不同的 UDP 端口，尽管可能发生多路复用）或 443 TCP/TLS 进行回退。呼叫质量取决于底层网络协议。由于 UDP 始终优于 TCP，因此我们建议您设计网络以适应分支机构中的 UDP 流量。

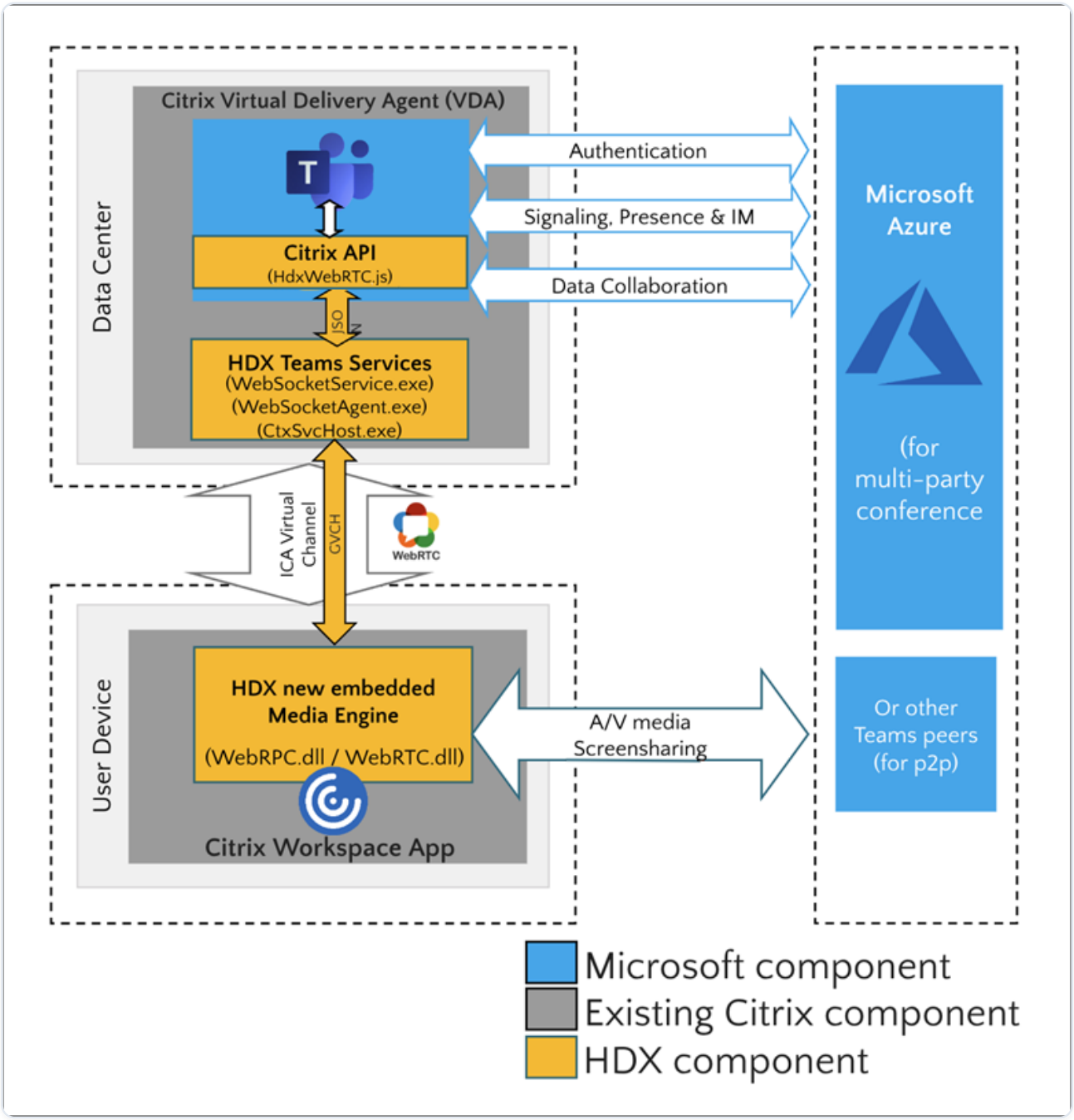
如果 Microsoft Teams 以优化模式加载且 HdxRtcEngine.exe 在端点上运行，则 ICE 故障可能会导致呼叫设置失败或仅单向音频/视频。如果呼叫无法完成或媒体流不是全双工，请首先检查端点上的 **Wireshark 跟踪**。有关 ICE 候选收集过程的更多信息，请参阅 支持 部分中的“收集日志”。

> **注意：**
>
> 如果端点没有互联网访问权限，则如果用户都在同一 LAN 上，他们仍然可以进行点对点呼叫。会议将失败。在这种情况下，呼叫设置开始前会有 30 秒的超时。

呼叫设置

使用此架构图作为呼叫流序列的视觉参考。图中指示了相应的步骤。

架构



1. 启动 微软团队。
2. Microsoft Teams 向 O365 进行身份验证。租户策略被下发到 Microsoft Teams 客户端，相关的 TURN 和信令通道信息被中继到应用程序。
3. Microsoft Teams 检测到它正在 VDA 中运行，并向 Citrix JavaScript API 发出 API 调用。
4. Microsoft Teams 中的 Citrix JavaScript 打开一个安全的 WebSocket 连接到在 VDA 上运行的 WebSocketService.exe，它在用户会话中生成 WebSocketAgent.exe。
5. WebSocketAgent.exe 通过调用 Citrix HDX Microsoft Teams 重定向服务 (CtxSvcHost.exe) 实例化一个通用虚拟通道。

6. Citrix Workspace 应用程序的 wfica32.exe (HDX 引擎) 生成一个名为 HdxRtcEngine.exe 的新进程，这是用于 Microsoft Teams 优化的新 WebRTC 引擎。
7. Citrix 媒体引擎和 Teams.exe 具有双向虚拟通道路径，可以开始处理多媒体请求。

   -----用户呼叫------

8. **对等方 A** 单击“**呼叫**”按钮。Teams.exe 与 Microsoft 365 中的 Microsoft Teams 服务通信，与**对等方 B** 建立端到端信令路径。Microsoft Teams 向 HdxRtcEngine 请求一系列支持的呼叫参数（编解码器、分辨率等，这被称为会话描述协议 (SDP) 提议）。然后，这些呼叫参数通过信令路径中继到 Microsoft 365 中的 Microsoft Teams 服务，并从那里中继到另一个对等方。
9. SDP 要约/应答（单次协商）通过信令通道进行，并且 ICE 连接检查（使用 STUN 绑定请求进行 NAT 和防火墙遍历）完成。然后，安全实时传输协议 (SRTP) 媒体直接在 HdxRtcEngine.exe 和其他对等方之间（如果是会议，则在 HdxRtcEngine.exe 和 Microsoft 365 会议服务器之间）流动。

Microsoft 电话系统

Phone System 是 Microsoft 的技术，可在 Microsoft 365 云中通过 Microsoft Teams 实现呼叫控制和 PBX。Microsoft Teams 优化支持 Phone System，使用 Microsoft 365 呼叫计划或直接路由。通过直接路由，您可以将自己支持的会话边界控制器直接连接到 Microsoft Phone System，而无需任何额外的本地软件。 支持呼叫队列、转接、呼叫转移、保持、静音和恢复呼叫。

DTMF

以下版本的 Citrix Workspace 应用程序（及更高版本）支持双音多频 (DTMF) 功能：

- 适用于 Windows 版本 2102 的 Citrix Workspace 应用程序
- 适用于 Windows LTSR 1912 CU5 的 Citrix Workspace 应用程序（仅限 Windows 10 操作系统）
- 适用于 Linux 的 Citrix Workspace 应用程序版本 2101
- 适用于 Mac 的 Citrix Workspace 应用程序版本 2101
- 适用于 ChromeOS 的 Citrix Workspace 应用程序版本 2111.1

支持动态 e911

从版本 2112 开始，Citrix Workspace 应用程序支持动态紧急呼叫。在 Microsoft Calling Plans、Operator Connect 和 Direct Routing 中使用时，它允许您执行以下操作：

- 配置和路由紧急呼叫。
- 通知安全人员。

通知是根据在端点上运行的 Citrix Workspace 应用程序的当前位置提供的，而不是根据在 VDA 上运行的 Microsoft Teams 客户端的位置提供的。

Ray Baum 法案要求将 911 呼叫者的可调度位置传输到相应的公共安全应答点 (PSAP)。当与以下版本的 Citrix Workspace 应用程序一起使用时，通过 HDX 优化的 Microsoft Teams 符合 Ray Baum 法案：

- 适用于 Windows 的 Citrix Workspace 应用程序版本 2112.1 及更高版本
- 适用于 Linux 的 Citrix Workspace 应用程序版本 2112 及更高版本
- 适用于 Mac 的 Citrix Workspace 应用程序版本 2112 及更高版本
- 适用于 ChromeOS 的 Citrix Workspace 应用程序版本 2112 及更高版本

要启用动态紧急呼叫，管理员必须使用 Microsoft Teams 管理中心并配置以下内容以创建网络或紧急位置映射：

- 网络设置
- 位置信息服务 (LIS)

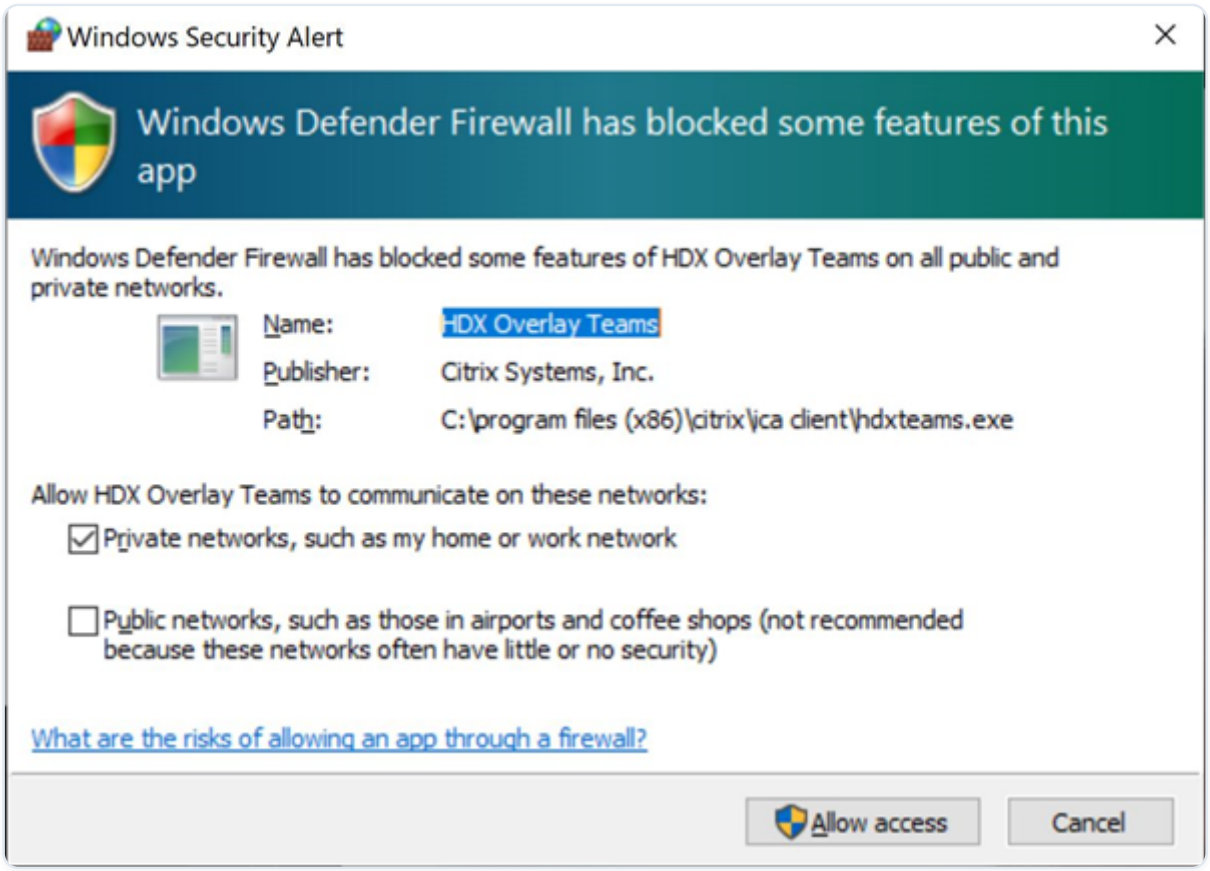
有关动态紧急呼叫的更多信息，请参阅 Microsoft 文档。

Citrix Workspace 应用程序中继到 Microsoft Teams 的可调度位置信息包括：

- 使用链路层发现协议 (LLDP) 的以太网/交换机连接的机箱 ID/端口 ID。以太网/交换机 (LLDP) 支持以下平台：
  - Windows 8.1 和 10 版本
  - macOS，需要 LLDP 启用软件。要下载 LLDP 启用软件，请转至 `www.microsoft.com` 并搜索 LLDP 启用软件。
  - Linux，需要将 LLDP 库包含在瘦客户端的操作系统 (OS) 分发中。
- 安装了 Citrix Workspace 应用程序的端点的 WLAN BBSID 和 {IPv4-IPv6；子网；MAC 地址}。
  - Workspace 应用程序（适用于 Windows、Linux 和 Mac）支持基于子网和 WiFi 的位置。
- 纬度和经度，如果用户在安装 Citrix Workspace 应用程序的操作系统级别授予了权限（权限设置为 HDX RTC Engine）
  - 所有 Workspace 应用程序平台均支持。但是，对于适用于 Linux 的 Citrix Workspace，您必须在瘦客户端的操作系统分发版中包含 `libgps` 库（>sudo apt-get install libgps23 gpsd lldpd）。

防火墙注意事项

当用户首次使用 Microsoft Teams 客户端启动优化呼叫时，他们可能会注意到 **Windows 防火墙**设置的警告。该警告要求用户允许 HdxTeams.exe 或 HdxRtcEngine.exe（HDX Overlay Microsoft Teams）进行通信。



以下四个条目已添加到 **Windows Defender 防火墙 > 高级安全** 控制台的 **入站规则** 下。如果需要，您可以应用更严格的规则。

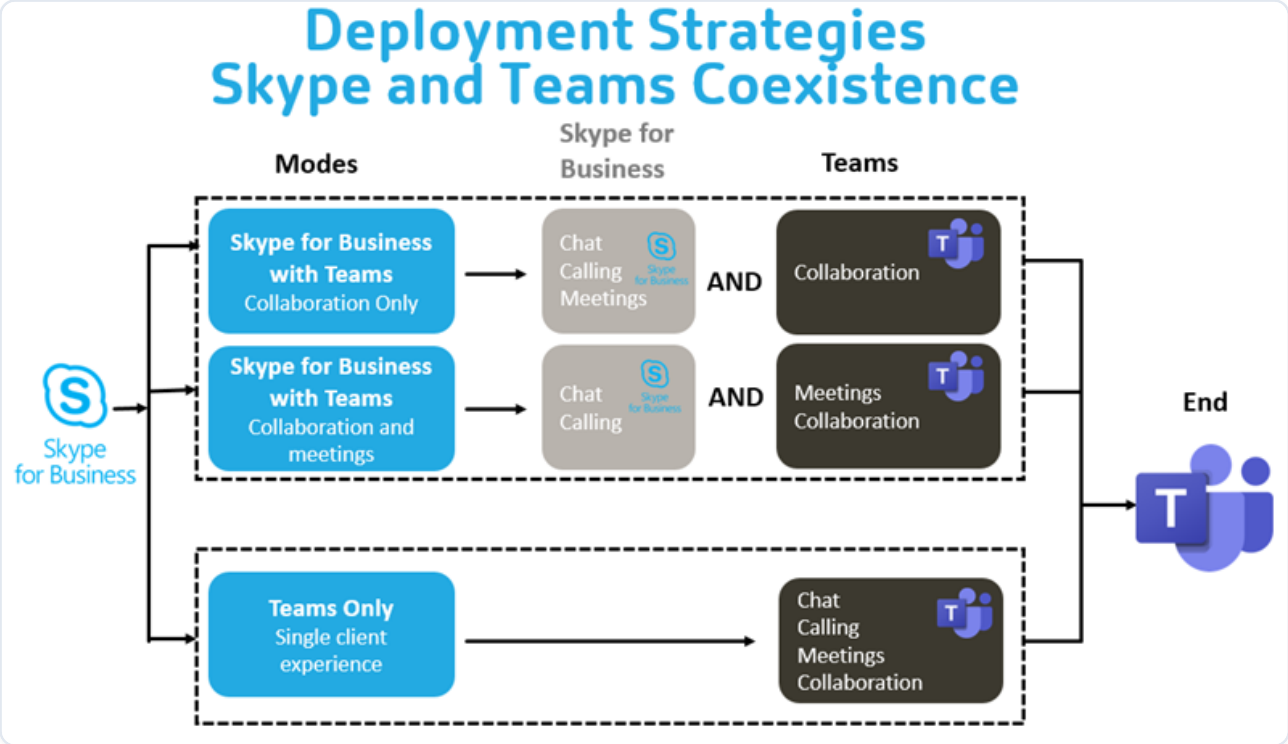
防火墙入站规则](/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/firewall2.png)

微软团队 和 商务版 Skype 共存

您可以将 Microsoft Teams 和 Skype for Business 作为两个具有重叠功能的独立解决方案并排部署。 有关详细信息，请参阅了解 Microsoft Teams 和 Skype for Business 共存和互操作性。

Citrix RealTime Optimization Pack 和适用于 Microsoft Teams 多媒体引擎的 HDX 优化将遵循您环境中设置的配置。示例包括孤岛模式以及 Skype for Business 与 Microsoft Teams 协作。此外，还包括 Skype for Business 与 Microsoft Teams 协作和会议。

外设访问一次只能授予单个应用程序。例如，RealTime Media Engine 在通话期间访问网络摄像头会锁定成像设备。当设备释放后，它将可用于 Microsoft Teams。



Citrix SD-WAN™：针对 Microsoft Teams 优化的网络连接

最佳的音频和视频质量需要连接到 Microsoft 365 云的网络，该网络应具有低延迟、低抖动和低数据包丢失。将来自分支机构的 Citrix Workspace 应用程序用户的 Microsoft Teams 音视频 RTP 流量回传到数据中心，然后再传输到互联网，可能会增加过多的延迟。这还可能导致 WAN 链路拥塞。Citrix SD-WAN 遵循 Microsoft 365 网络连接原则，优化了 Microsoft Teams 的连接。Citrix SD-WAN 使用基于 Microsoft REST 的 Microsoft 365 IP 地址和 Web 服务以及近端 DNS。此用途旨在识别、分类和引导 Microsoft Teams 流量。

许多地区的商业宽带互联网连接都存在间歇性数据包丢失、过度抖动和中断的问题。

当网络状况不稳定或降级时，Citrix SD-WAN 提供两种解决方案来保持 Microsoft Teams 音视频质量。

- 如果您使用 Microsoft Azure，部署在 Azure VNET 中的 Citrix SD-WAN 虚拟设备 (VPX) 可提供高级连接优化。这些优化包括无缝链路故障转移和音频数据包竞速。
- Citrix SD-WAN 客户可以通过 Citrix Cloud™ Direct 服务连接到 Microsoft 365。此服务为所有互联网流量提供可靠且安全的传输。

如果分支机构互联网连接质量不是问题，那么最小化延迟可能就足够了。将 Microsoft Teams 流量直接从 Citrix SD-WAN 分支设备引导到最近的 Microsoft 365 前端，以最大程度地减少延迟。有关详细信息，请参阅Citrix SD-WAN Office 365 优化。

思杰 SD-WAN](/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/sd-wan.png)

多窗口会议和聊天

您可以在 Windows 中为 Microsoft Teams 使用多个会议或聊天窗口。有关弹出功能的详细信息，请参阅 Microsoft 365 网站上的Microsoft Teams 聊天和会议弹出窗口。

> **注意：**
>
> 此功能支持适用于 Windows 2112.1、Mac 2203、Linux 2203、ChromeOS 2303 的 Citrix Workspace 应用程序。它需要 VDA 2112 或更高版本，并已向后移植到 1912 CU6+ LTSR。

背景模糊和背景效果

适用于 Windows、Mac、Linux 和 ChromeOS/HTML5 的 Citrix Workspace 应用程序支持通过 HDX 优化在 Microsoft Teams 中实现背景模糊和背景效果。

您可以模糊背景或将其替换为默认图像，并通过帮助对话保持专注于轮廓（身体和面部）来避免意外干扰。您可以在 P2P 或电话会议中使用此功能。

> **注意：**
>
> 此功能与 Microsoft Teams UI/按钮集成。多窗口支持是先决条件，需要将 VDA 更新到 2112 或更高版本。有关详细信息，请参阅多窗口会议和聊天。

> Microsoft Teams UI 对背景模糊和效果的控制需要以下最低版本：

- 适用于 Windows 2207 的 Citrix Workspace 应用程序
- 适用于 Mac 2301 的 Citrix Workspace 应用程序
- 适用于 Linux 的 Citrix Workspace 应用程序 2307
- 适用于 ChromeOS 2303 的 Citrix Workspace 应用程序

限制：

- 客户端在用 Microsoft Teams 默认图像替换背景图像时必须连接到互联网。
- Microsoft Teams UI 不支持管理员和用户定义的背景图像替换。如果图像也存储在客户端上，则可以使用客户端上的配置设置来配置自定义背景图像。

设置自定义背景图像

仅当您不打算使用 Microsoft Teams UI 来控制此功能，或者管理员想要覆盖默认行为时，才需要以下注册表项。例如，由于端点性能不足而禁用背景模糊。

在 Windows 上

要设置自定义背景图像，管理员或最终用户必须在客户端或端点上配置以下注册表项：

位置：`HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- 名称：VideoBackgroundEffect
- 类型: DWORD
- 值：0（已禁用），1（已启用），2（背景图像替换）

将值设置为 1 会模糊背景。最终用户或管理员可以设置此值。

值设置为 2 还需要存在 **VideoBackgroundImage** 键。只有管理员可以设置此值。仅当您要替换背景图像而不是模糊背景时，才需要以下键：

- 名称：VideoBackgroundImage
- 类型: REG_SZ
- 值：my_image_name.jpeg

视频背景图像必须存在于 `C:\Program Files (x86)\Citrix\ICA Client` 目录中。

此注册表配置还可用于在 Citrix Workspace 应用程序 2206 中启用背景模糊或图像替换，而无需 Microsoft Teams UI 选择器。换句话说，如果您的环境或 VDA 不支持多窗口，您仍然可以使用 Citrix Workspace 应用程序 2206 或更高版本应用 HKCU 注册表变通方法以实现类似结果，尽管用户无法在 HDX 会话或 Microsoft Teams 通话期间控制此功能。

注册表项更改仅在 HDX 会话连接时生效。

在 Mac 上

用户下载的图片位置：*/Users/username/Downloads/any_image.png*

运行以下命令将自定义图像设置为默认图像：

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"
```

在 Linux 上

用户下载的图片位置：*/home/username/Downloads/any_image.jpg*

创建文件 */var/.config/citrix/hdx_rtc_engine/config.json* 并以 JSON 格式添加以下配置键。例如，

```
{


"VideoBackgroundEffect":2,


"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"


}
```

在 HTML5 上

1. 导航到 **HTML5Client** 文件夹中的 **configuration.js** 文件。
2. 添加 **backgroundEffects** 属性并将该属性设置为 **true**。例如，

```
'features' : {

    'msTeamsOptimization' :

    {

        'backgroundEffects' : true

    }

}
```

3. 保存更改。

客户端 CPU 消耗注意事项

虽然模糊功能对 CPU 的消耗不大，但您仍可预期消耗会增加。例如，在具有 4 核、1.5 GHz Intel® Pentium® Silver 芯片（TurboBoost 可达 2.8 GHz）的瘦客户端上，背景模糊会使 CPU 使用率增加约 2%。平均 CPU 使用率低于 20%。

Microsoft Teams 中的图库视图和活动发言人

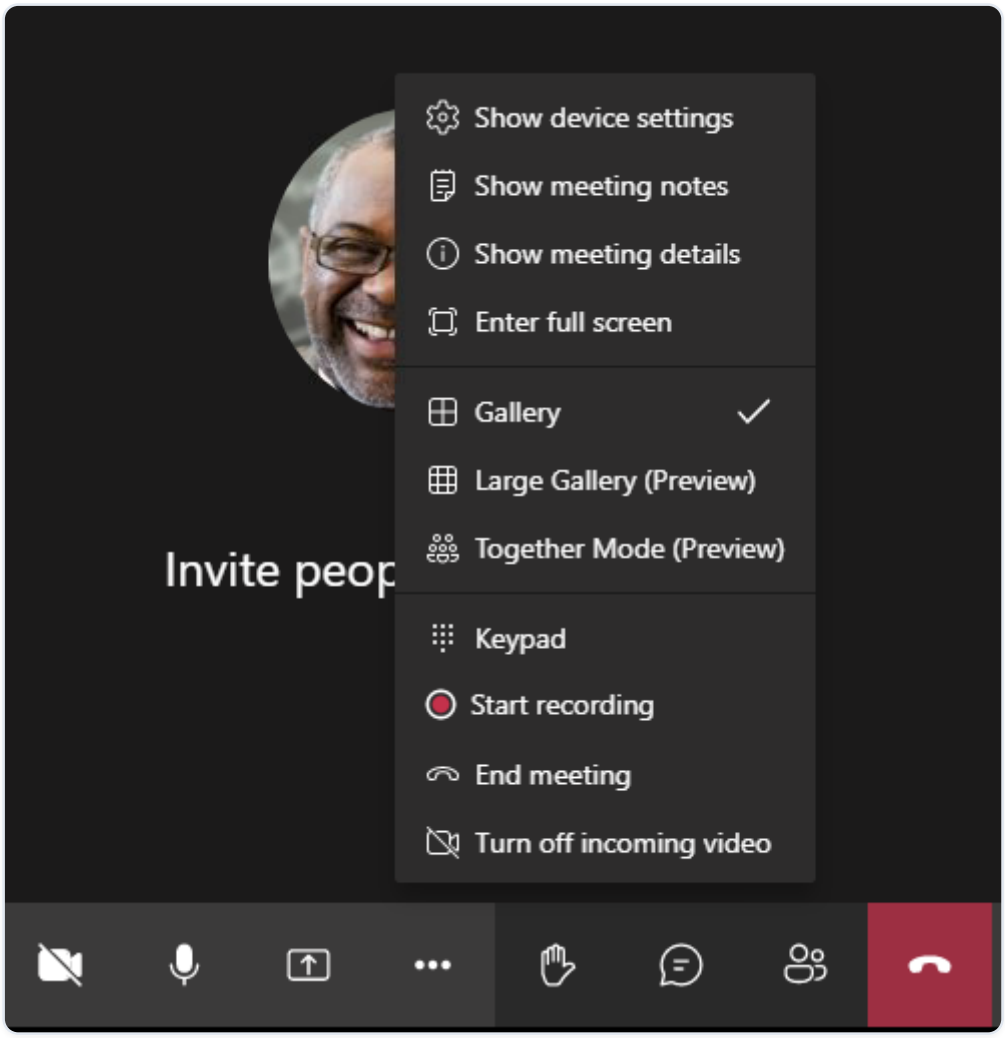
Microsoft Teams 支持 **Gallery**（图库）、**Large gallery**（大型图库）和 **Together mode**（同框模式）布局。

Microsoft Teams 显示一个 2x2 网格，其中包含四名参与者的视频流（称为 **Gallery**）。在这种情况下，Microsoft Teams 会向客户端设备发送四个视频流进行解码。当超过四名参与者共享视频时，屏幕上只会显示最后四名最活跃的发言者。

Microsoft Teams 还提供大型图库视图，网格最大可达 7x7。因此，Microsoft Teams 会议服务器会合成一个视频源并将其发送到客户端设备进行解码，从而降低 CPU 消耗。这种单一的矩阵式视频源也可能包含用户的自预览视频。

最后，Microsoft Teams 支持 **Together mode**（同框模式），这是新会议体验的一部分。Microsoft Teams 使用 AI 分割技术将参与者数字地放置在共享背景中，从而将所有参与者置于同一礼堂中。

用户可以在电话会议期间通过在省略号菜单中选择 **Gallery**（图库）、**Large gallery**（大型图库）或 **Together mode**（同框模式）布局来控制这些模式。



支持视频宽高比限制（适用于 Windows 2102 的 Citrix Workspace 应用程序、适用于 Linux 2106 的 Citrix Workspace 应用程序、适用于 MAC 2106 及更高版本的 Citrix Workspace 应用程序）：

- 在图库/大型图库视图中，可以使用 **Fill to frame**（填充到帧）选项。此选项会裁剪视频大小以使其适合子窗口。另一方面，**Fit to frame**（适应帧）会在视频两侧显示黑边（信箱模式），因此不会进行裁剪。

下表提供了图库和大型图库布局的比较：

	图库视图 2X2（默认）	大型图库视图
布局/网格	显示一个 2x2 网格，其中包含四名参与者的视频流。屏幕上仅显示最后四位最活跃的发言者，其他参与者不会显示在网格中。	显示一个 7x7 网格，其中包含 49 名参与者的视频流。
混合技术	媒体路由器将每个参与者的单个流转发给每个用户。	中央会议服务器混合并转码所有音频或视频，为每个参与者

	图库视图 2X2（默认）	大型图库视图
		创建定制的复合布局。此操作会引入一些额外的延迟。
活跃发言者	新的活跃发言者会替换网格中最不活跃的发言者。	显示所有参与者，无论他们是活跃还是不活跃。
端点编码	如果启用了 Simulcast，一个或多个视频流可能会在端点进行编码。有关 Simulcast 支持的详细信息，请参阅 Simulcast。	如果启用了 Simulcast，一个或多个视频流可能会在端点进行编码。有关 Simulcast 支持的详细信息，请参阅 Simulcast。
端点解码	每个参与者最多可获得四个独立的媒体流。这会增加端点上 HdxRtcEngine.exe 的 CPU 消耗（用于解码/渲染）。	每个参与者只获得一个音频和视频流。此设置可降低端点的 CPU 消耗。
最大分辨率	720p。当四名参与者共享视频时，每个视频源的最大分辨率为 360p。如果共享视频的参与者少于四名，每个视频源的分辨率可能会更高。	复合布局或混音为 720p。在复合布局中，每个参与者不需要高质量视频流。由于此条件，每个发送方都会降低分辨率或上传比特率。
“慢速用户”问题	发送方将每种模式（音频/视频/屏幕共享）的质量调整为参与者中最低的通用网络质量。然后，此多媒体流会转发给所有其他参与者。因此，网络状况不佳的参与者会影响通话中其他所有人的质量。	不易受最低通用网络质量场景的影响。会议服务器根据单个参与者的网络状况提供不同的质量。
自预览	实时以小缩略图显示自己。	以缩略图显示自己，并与其余视频源混合。因此，您可能会看到自己被包含在主视频布局中，并带有一些额外的延迟。

Microsoft Teams 中的屏幕共享

Microsoft Teams 依赖于基于视频的屏幕共享 (VBSS)，它使用 H264 等视频编解码器有效地编码共享桌面并创建高清流。通过 HDX 优化，传入的屏幕共享被视为视频流。

从适用于 Windows、Linux、Mac 的 Citrix Workspace 应用程序 2109 或更高版本以及适用于 ChromeOS 的 Citrix Workspace 应用程序 2303 开始，用户可以同时共享其屏幕和视频摄像头。

在早期版本中，如果您正在进行视频通话，而另一位对等方开始共享桌面，则原始摄像头视频源会暂停。取而代之的是显示屏幕共享视频源。然后，对等方必须手动恢复摄像头共享。

PowerPoint Live 注意事项

如果您正在从 PowerPoint Live 共享内容，则不存在此限制。在这种情况下，其他对等方仍然可以看到您的网络摄像头和内容，并可以来回导航以查看其他幻灯片。在此场景中，幻灯片在 VDA 上呈现。要访问 PowerPoint Live 幻灯片组，请单击“共享托盘”按钮并选择建议的 PowerPoint 幻灯片之一，或者单击“浏览”并在您的计算机或 OneDrive 中查找 PowerPoint 文件。

出站屏幕共享也经过优化并卸载到 Citrix Workspace 应用程序。在这种情况下，媒体引擎仅捕获并传输 Citrix Desktop Viewer (CDViewer.exe) 窗口，该窗口周围会绘制红色边框。任何与 Desktop Viewer 重叠的本地应用程序都不会被捕获。

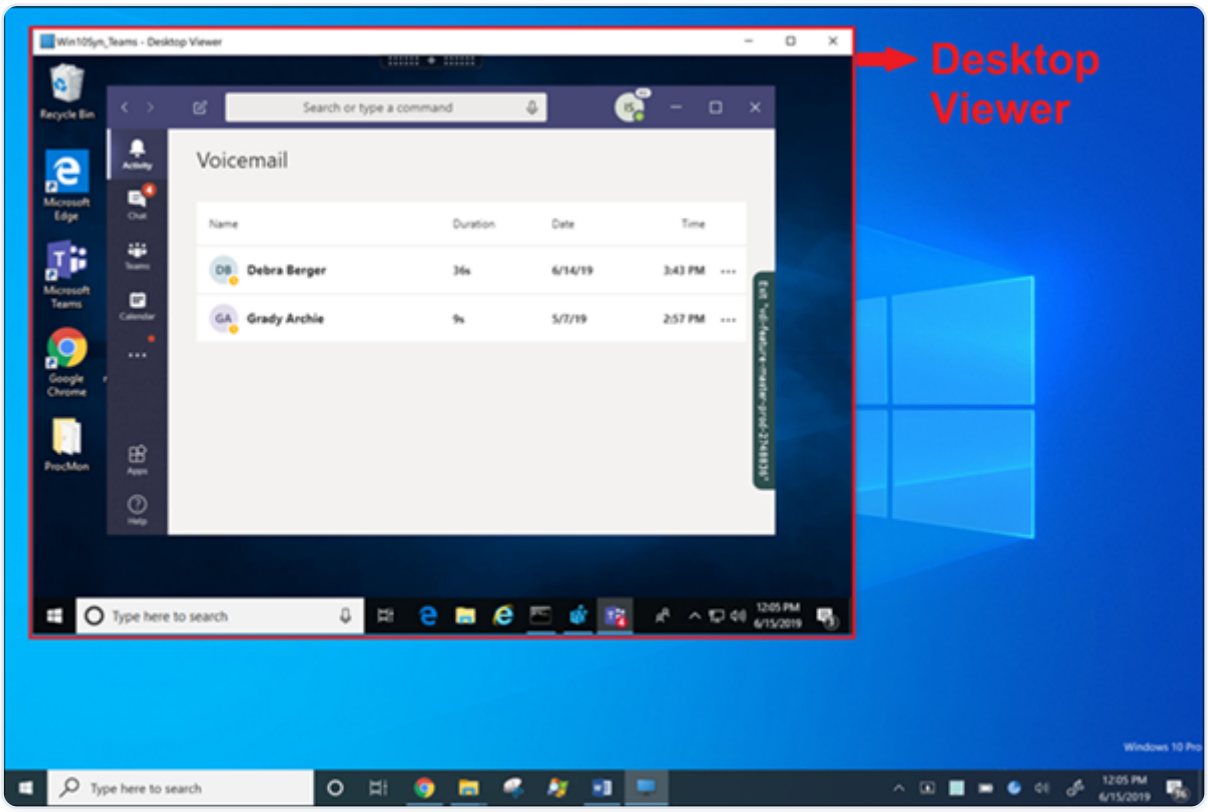
注意

在适用于 Mac 的 Citrix Workspace 应用程序中设置特定权限以启用屏幕共享。有关详细信息，请参阅系统要求。

已知限制：

- 如果 Desktop Viewer 被禁用或正在使用 Desktop Lock，则 Microsoft Teams 屏幕选择器中无法进行多显示器选择。可以通过编辑 `.ICA` 文件模板或 `StoreFront web.config` 来禁用 Desktop Viewer。SHIFT+F2 热键与多显示器屏幕共享不兼容。
- 在 2106 之前的 Workspace 应用程序版本中，仅共享主显示器。将虚拟桌面中的应用程序拖到主显示器上，以便通话中的其他对等方可以看到它。
- 如果您使用虚拟显示器布局功能（单个物理显示器的逻辑分区）配置 Citrix Workspace 应用程序，则多显示器屏幕共享可能无法工作。在这种情况下，所有虚拟显示器都将作为复合图像共享。

- 旧版本的适用于 Windows 的 Citrix Workspace 应用程序（1907 至 2008）还会共享在客户端计算机中运行的本地应用程序。仅当本地应用程序叠加在 Desktop Viewer 之上时，才可能进行此共享。此行为已在 2009.6 或更高版本以及 1912 CU5 或更高版本中移除。
- 在屏幕共享期间，如果您从窗口模式切换到全屏模式，屏幕共享将停止。您必须停止并重新共享才能使屏幕共享正常工作。
- 无法将共享控件固定到 Optimized Microsoft Teams 中的特定位置。
- 共享最小化应用程序时，应用程序的标题栏也可能被共享。



从无缝应用程序进行屏幕共享：

如果您将 Microsoft Teams 发布为独立的无缝应用程序，屏幕共享将捕获物理端点的本地桌面。需要 Citrix Workspace 应用程序最低版本 1909。

应用共享

从适用于 Windows 的 Citrix Workspace 应用程序 2112.1 和 VDA 2112 开始，Microsoft Teams 支持应用程序共享。

从适用于 Windows 的 Citrix Workspace 应用程序 2109、Mac 2203、Linux 2209 和 VDA 2109 开始，Microsoft Teams 支持共享在虚拟会话中运行的特定应用程序的屏幕。您还可以使用优化的 Microsoft Teams 共享自定义内部应用程序，例如 Java。要共享特定应用程序，请执行以下操作：

1. 在远程会话中导航到 Microsoft Teams 应用程序。

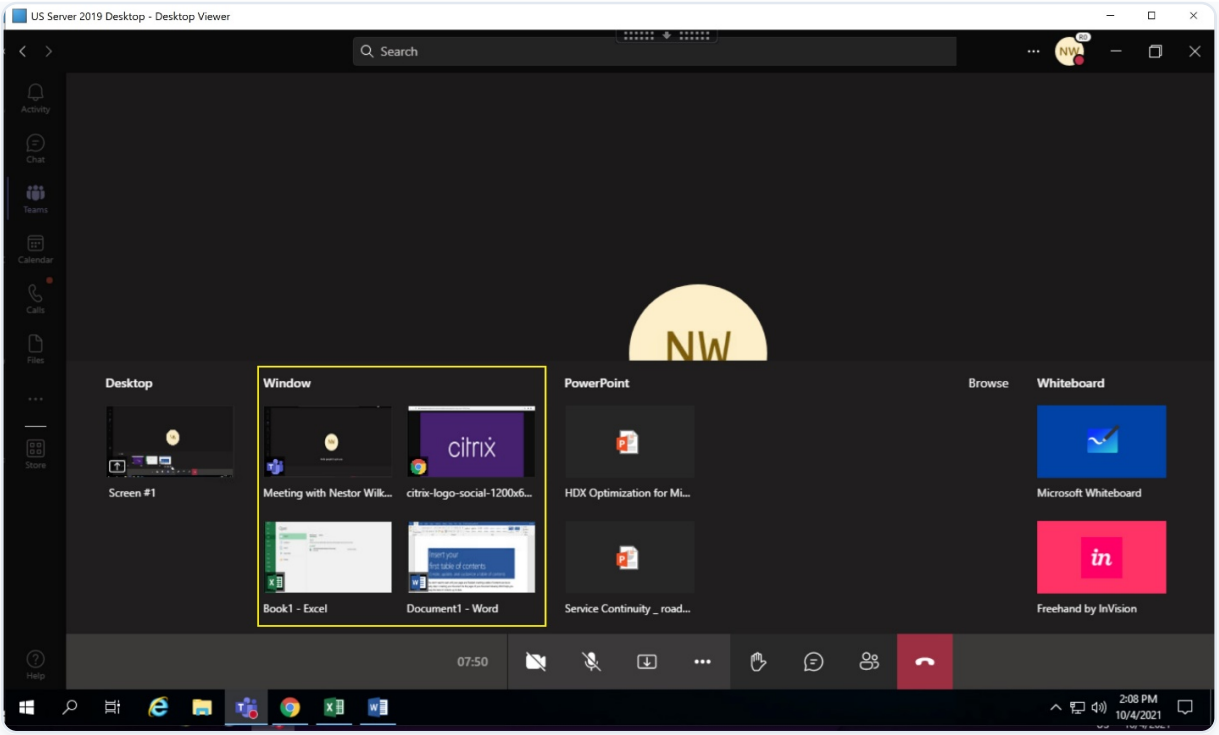
2. 在 Microsoft Teams UI 中单击**共享内容**。
3. 选择要在会议中共享的应用程序。您选择的应用程序周围会出现红色边框，通话中的对等方可以看到共享的应用程序。

要共享其他应用程序，请再次单击**共享内容**并选择一个新应用程序。

如果要禁用应用程序共享，请在 VDA 上的 `HKLM\SOFTWARE\Citrix\Graphics` 处创建以下注册表项：名称：`UseWsProvider` 类型：`DWORD` 值：0

注意：

- 如果最小化应用程序，Microsoft Teams 将显示共享应用程序的最后一张图像。您可以最大化窗口以恢复屏幕共享。
- 屏幕共享取决于 VDA 端的窗口捕获。然后，内容以最大速率中继到 Citrix Workspace 应用程序。最大速率为每秒 30 帧。Citrix Workspace 应用程序将内容转发给对等方或会议服务器。



特定应用程序屏幕共享的已知限制：

- 屏幕共享应用程序时，鼠标指针不可见。
- 如果您在共享应用程序时将其最小化，则屏幕选择器中只会显示应用程序图标。屏幕选择器中不会预览应用程序的缩略图。您无法共享内容，并且直到您最大化应用程序后才会出现红色边框。

- LAA 应用程序会显示一个列表，其中包含可在 VDA 中通过优化的 Microsoft Teams 与桌面应用程序共享的应用程序。但是，当您从列表中选择应用程序时，结果可能不符合预期。

与应用程序保护的兼容性 特定应用程序的屏幕共享与 HDX 优化版 Microsoft Teams 中的应用程序保护功能兼容。如果您从启用了应用程序保护的交付组启动应用程序或桌面，则可以屏幕共享特定应用程序。

当您在 Microsoft Teams UI 中单击“**共享内容**”时，屏幕选择器会移除“**桌面**”选项。您只能选择“**窗口**”选项来共享任何打开的应用程序。

> **注意：**
>
> 当您从启用了应用程序保护的交付组启动应用程序或桌面时，如果您使用的是适用于 Windows 2202 或更早版本的 Citrix Workspace 应用程序，则无法看到传入的视频或屏幕共享。

在 Microsoft Teams 中授予和请求控制权

此功能在以下版本的 Citrix Workspace 应用程序中受支持（不依赖于 VDA 版本或操作系统、单会话或多会话）：

- 适用于 Windows 的 Citrix Workspace 应用程序版本 2112.1 或更高版本
- 适用于 Mac 的 Citrix Workspace 应用程序版本 2203.1 或更高版本
- 适用于 Linux 的 Citrix Workspace 应用程序版本 2203 或更高版本
- 适用于 ChromeOS 的 Citrix Workspace 应用程序版本 2303 或更高版本

在 Microsoft Teams 通话期间，当参与者共享屏幕时，您可以请求控制权。获得控制权后，您可以对共享屏幕进行选择、编辑或其他键盘和鼠标操作。

要在共享屏幕时取得控制权，请单击 Microsoft Teams UI 中的“**请求控制**”按钮。共享屏幕的会议参与者可以允许或拒绝您的请求。

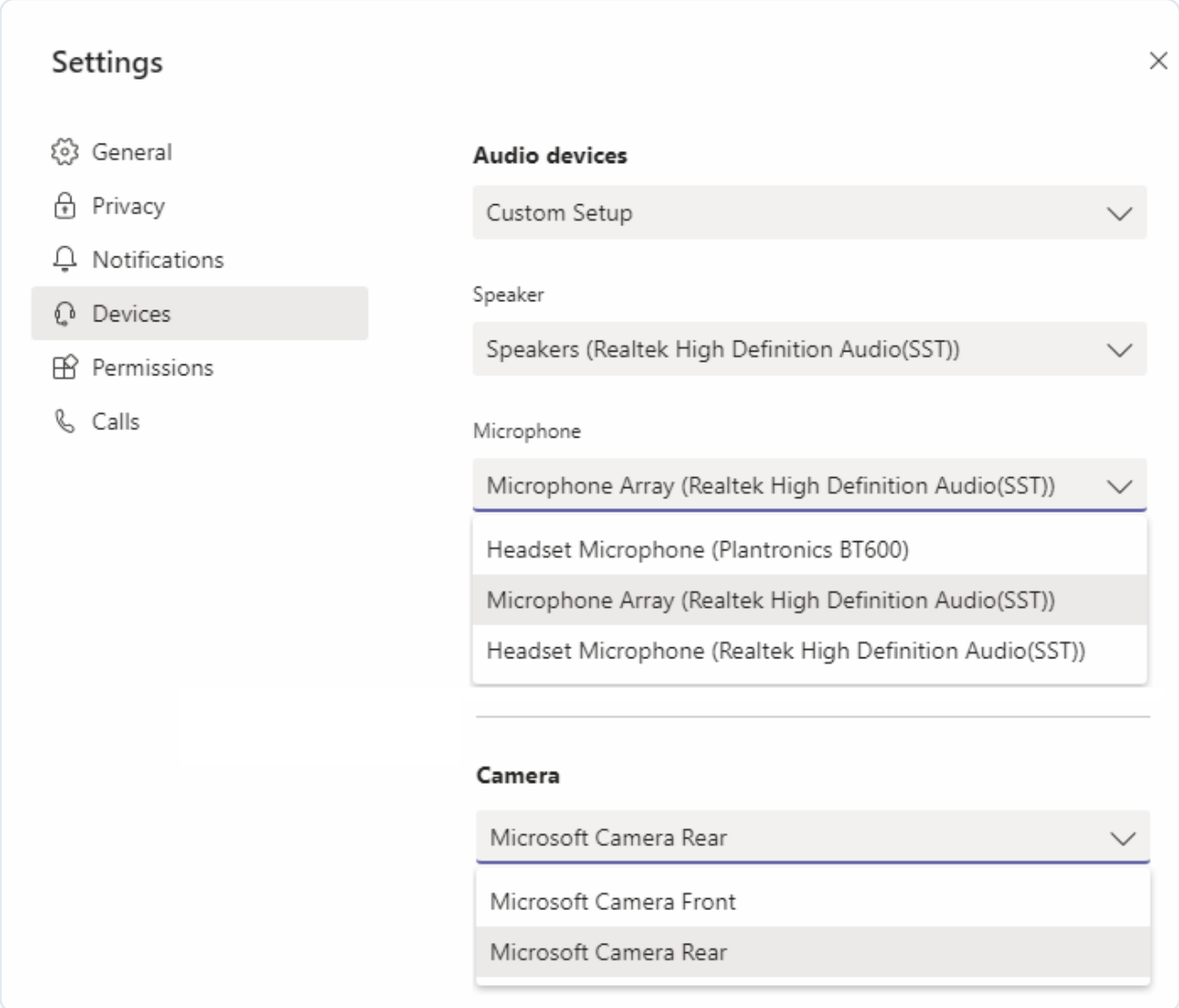
在您拥有控制权时，可以对共享屏幕进行选择、编辑和其他修改。对于这些操作，您可以使用键盘和鼠标。完成后，单击“**请求控制**”。

> **限制：**

- 如果用户正在共享单个应用程序（也称为应用程序共享），则“授予”和“请求”控制不可用。必须共享整个桌面或显示器。
- 将控制栏固定到特定位置的功能不可用。

Microsoft Teams 中的外设

当 Microsoft Teams 优化处于活动状态时，Citrix Workspace 应用程序会访问外设（耳机、麦克风、摄像头、扬声器等）。然后，外设会在 Microsoft Teams UI (**设置 > 设备**) 中正确列出。



Microsoft Teams 不直接访问设备。相反，它依赖于 Workspace 应用程序 WebRTC 媒体引擎来获取、捕获和处理媒体。Microsoft Teams 列出设备供用户选择。

在 Microsoft Teams 处于活动状态时插入的外设默认情况下不会被选中。您必须从 Microsoft Teams UI 的“**设置**”>“**设备**”屏幕手动选择外设。选择外设后，Microsoft Teams 会缓存外设信息。因此，当您从同一端点重新连接到会话时，外设会自动选中。

建议：

- 带有内置回声消除功能的 Microsoft Teams 认证耳机。在具有额外外设的设置中，如果麦克风和扬声器位于单独的设备上，则可能会出现回声。例如，带有内置麦克风的网络摄像头和带有扬声器的显示器。使用外部扬声器时，请将其尽可能远离麦克风。此外，请将它们放置在远离任何可能将声音折射到麦克风中的表面。有关详细信息，请访问 `www.microsoft.com` 并搜索 Microsoft Teams 认证耳机。
- Microsoft Teams 认证摄像头，尽管 Skype for Business 认证外设与 Microsoft Teams 兼容。有关详细信息，请访问 <www.microsoft.com> 并搜索 Microsoft Teams 认证摄像头和 Skype for Business 认证外设。
- Citrix Workspace 应用程序媒体引擎无法利用执行板载 H.264 编码的网络摄像头（UVC 1.1 和 1.5）进行 CPU 卸载。

> **注意：**
>
> 适用于 Windows 的 Workspace 应用程序 2009.6 现在可以获取支持 24 位音频格式或高于 96 kHz 频率的外设。
>
> HdxTeams.exe（在适用于 Windows 的 Citrix Workspace 应用程序 2009 或更早版本中）仅支持以下特定的音频设备格式（通道、位深度和采样率）：
>
> - 播放设备：最多2通道，16位，频率高达96,000 Hz
> - 录音设备：最多4通道，16位，频率高达96,000 Hz
>
> 即使一个扬声器或麦克风与预期设置不匹配，Microsoft Teams 中的设备枚举也会失败，并且在 **设置 > 设备** 下显示 **无**。
>
> **HdxTeams.exe** 中的 **Webrpc** 日志显示此类信息：
>
> `Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.
>
> `Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!`!

作为一种变通方法，请禁用特定设备或：

1. 打开 **声音控制面板** (mmsys.cpl)。
2. 选择播放或录音设备。
3. 转到 **属性 > 高级** 并将设置更改为受支持的模式。

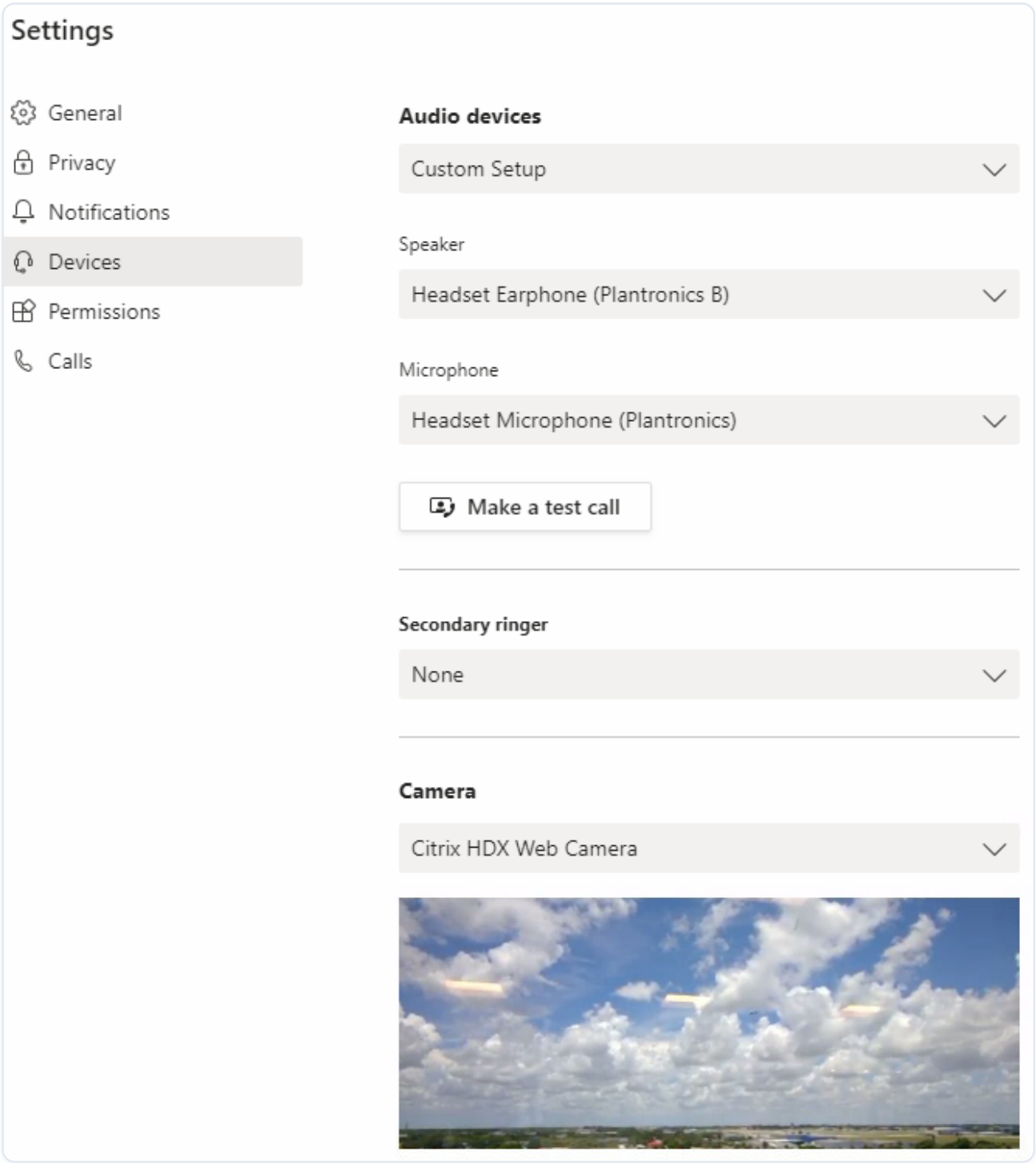
回退模式

如果 Microsoft Teams 未能在优化 VDI 模式下加载（在 Microsoft Teams/关于/版本中显示“Citrix HDX 未连接”），VDA 将回退到旧版 HDX 技术。旧版 HDX 技术可能是网络摄像头重定向以及客户端音频和麦克风重定向。如果您使用的 Workspace 应用程序版本/平台操作系统不支持 Microsoft Teams 优化，则回退注册表项不适用。 在回退模式下，外设会映射到 VDA。外设在 Microsoft Teams 应用程序中显示，就像它们本地连接到虚拟桌面一样。

您现在可以通过在 VDA 中设置注册表项来精细控制回退机制。有关详细信息，请参阅注册表管理的功能列表中的Microsoft Teams 回退模式。

此功能需要 Microsoft Teams 1.3.0.13565 或更高版本。

在 Microsoft Teams 应用程序中查看“**设置 > 设备**”选项卡时，要确定您处于优化模式还是未优化模式，主要区别在于摄像头名称。如果 Microsoft Teams 以未优化模式加载，则会启动旧版 HDX 技术。网络摄像头名称带有 **Citrix HDX** 后缀，如以下图形所示。与优化模式相比，扬声器和麦克风设备名称可能略有不同（或被截断）。



使用旧版 HDX 技术时，Microsoft Teams 不会将音频、视频和屏幕共享处理卸载到端点的 Citrix Workspace 应用程序 WebRTC 媒体引擎。相反，HDX 技术使用服务器端渲染。打开视频时，预计 VDA 上的 CPU 消耗会很高。实时音频性能可能不理想。

已知限制

Citrix 限制

Citrix Workspace 应用程序的限制：

- HID 按钮 - 不支持接听和结束通话。支持音量增大和减小。

- Microsoft Teams 管理中心中的 QoS 设置不适用于 VDI 用户。
- 用户无法在使用 VDA 上的截图工具时截取 Microsoft Teams 内容的屏幕截图。但是，如果在客户端使用截图工具，则可以捕获内容。

VDA 上的限制：

- 当您将 **Citrix Workspace app High DPI** 设置配置为 `Yes` 时，重定向的视频窗口会显示错位。当显示器的 DPI 缩放因子设置为 100% 以上时，会出现此限制。

Citrix Workspace 应用程序和 VDA 上的限制：

- 您只能使用客户端计算机上的音量条控制优化通话的音量，而不能在 VDA 上控制。

同播

Windows 和 Mac 上的优化 Microsoft Teams 视频会议通话已启用 Simulcast 支持。对于 Linux，请咨询您的瘦客户端供应商。 借助 Simulcast，通过适应适当的分辨率，可以改善不同端点上的视频会议通话质量和体验，从而为所有呼叫者提供最佳通话体验。

借助这种改进的体验，每个用户可以根据端点功能、网络条件等多种因素，以不同的分辨率（例如 720p、360p 等）传输多个视频流。接收端点随后会请求其能够处理的最高质量分辨率，从而为所有用户提供最佳视频体验。

> **注意：**
>
> 此功能仅在 Microsoft Teams 推出更新后可用。有关预计到达时间 (ETA) 的信息，请访问 `<https://www.microsoft.com/>` 并搜索 Microsoft 365 路线图。当 Microsoft 推出更新后，您可以查看 CTX253754 以获取文档更新和公告。

Microsoft 限制

- 不支持 3x3 画廊视图。Microsoft Teams 依赖项 – 请联系 Microsoft 了解何时可以预期 3x3 网格。
- 与 Skype for Business 的互操作性仅限于音频通话，不支持视频模式。
- 传入和传出视频流的最大分辨率为 720p。
- 不支持 PSTN 呼叫回铃音。
- 不支持直接路由的媒体旁路。
- 不支持广播和直播活动的制作人及演示者角色。支持与会者角色，但未优化（而是在 VDA 上呈现）。

- 不支持 Microsoft Teams 中的放大和缩小功能。
- 不支持基于位置的路由和媒体旁路。
- 不支持呼叫合并（用户界面中不显示此选项）。

Citrix 和 Microsoft 限制

- 进行屏幕共享时，**包括系统音频**选项不可用。
- 同步广播在 ChromeOS 上不受支持。

即将终止支持的 Microsoft Teams 单窗口模式

在 January 31, 2024，Microsoft 将停止对使用 VDI Microsoft Teams 优化时的 Microsoft Teams 单窗口 UI 的支持，并仅支持多窗口体验。Microsoft 已于 9/8/2023 在 M365 管理中心（帖子 ID：MC674419）发布了此弃用通知。 有关多窗口功能的公开详细信息，请参阅技术社区文章：New Meeting and Calling Experience in Microsoft Teams。

> **注意：**

> Citrix 建议您将 VDA 和 Citrix Workspace 应用程序升级到受支持的版本，以继续在优化模式下使用 Microsoft Teams 进行视频和屏幕共享。如果您不升级您的基础架构和端点以支持多窗口，您的通话、视频通话和屏幕共享将变为非优化状态。这可能会导致通话质量问题、延迟增加以及服务器负载增加。

> 下表说明了在 Citrix VDI 上继续使用 Microsoft Teams 优化呼叫所需的 VDA 和 Citrix Workspace 应用程序的最低版本、LTSR 版本和推荐版本：

组件	最低版本 (1)	LTSR 支持的版本 (2)	推荐版本 (3)
微软 Teams	1.5.00.11865	不适用	最新
VDA	1912 CU6 LTSR, 2109 CR, 2203 LTSR	1912 CU8+, 2203 LTSR CU2+ (4)	2308 CR+
适用于 Windows 的 Citrix Workspace 应用程序	2112.1 CR	2203 CU2+ (4)	2309 CR+

组件	最低版本 (1)	LTSR 支持的版本 (2)	推荐版本 (3)
适用于 Mac 的 Citrix Workspace 应用程序	2203 CR	不适用	2308 CR+
适用于 Linux 的 Citrix Workspace 应用程序	2202 CR	不适用	2308 CR+
适用于 ChromeOS 或 HTML5 的 Citrix Workspace 应用程序	2303 CR	不适用	2309 CR+

注意：

1. 最低版本：这是首次引入多窗口功能的版本。此处列出的一些最低版本可能已终止支持。
2. LTSR 支持版本：这是 Citrix 为多窗口功能支持的 LTSR 版本。这些 LTSR 版本的旧版本可能仍可运行，但一旦发布新的 LTSR CU 版本，这些旧版本将不再获得支持。有关 LTSR 支持策略的更多信息，请参阅 `<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr>`。
3. 推荐版本：这是 Citrix 建议用户/客户升级其软件时使用的版本。这些都是 CR 版本。
4. 适用于 VDA 和 CWA 基础版本的 2203 LTSR 版本包含多窗口功能。这些版本已被最新的 CU 取代，后者是官方支持的版本。客户可自行决定继续使用这些不受支持的版本。Citrix 鼓励使用 LTSR 版本的客户升级到最新的 CU。

WebRTC 中 SDP 格式（方案 B）的弃用公告

Citrix 计划在未来的版本中弃用 WebRTC 对当前 SDP 格式（方案 B）的支持。您必须在 WebRTC 中使用统一计划 (Unified Plan) 来支持优化的 Microsoft Teams 功能。

受影响的产品

在 Citrix Workspace 应用程序的未来版本中，即将发布的 Citrix Workspace 应用程序的端点与 Citrix Workspace 应用程序 2108 或更早版本的端点之间的呼叫将不受支持。此呼叫不兼容性包括 1912 LTSR Citrix Workspace 应用程序客户端 (CWA)。以下 CWA 客户端受到影响：

- 适用于 Windows 的 Citrix Workspace 应用程序

- 适用于 Linux 的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序
- 适用于 Chrome 的 Citrix Workspace 应用程序

方案 B 的替代方案

如果您运行的 Citrix Workspace 应用程序版本低于 2109，则必须升级到受支持的版本（最好是最新的 CR 版本）。否则，与未来版本或更新端点的任何呼叫都将无法连接。如果联合通信合作伙伴尚未升级其 Citrix Workspace，则未来版本与您的联合通信合作伙伴之间的呼叫也可能无法完成。

Citrix Workspace 应用程序 2108 版本已于 2023 年 3 月结束支持，必须升级到更新版本。有关更多信息，请参阅 Workspace App，了解 Citrix Workspace 应用程序版本支持的详细信息。

有关方案 B 弃用的更多信息，请参阅 WebRTC 文档。

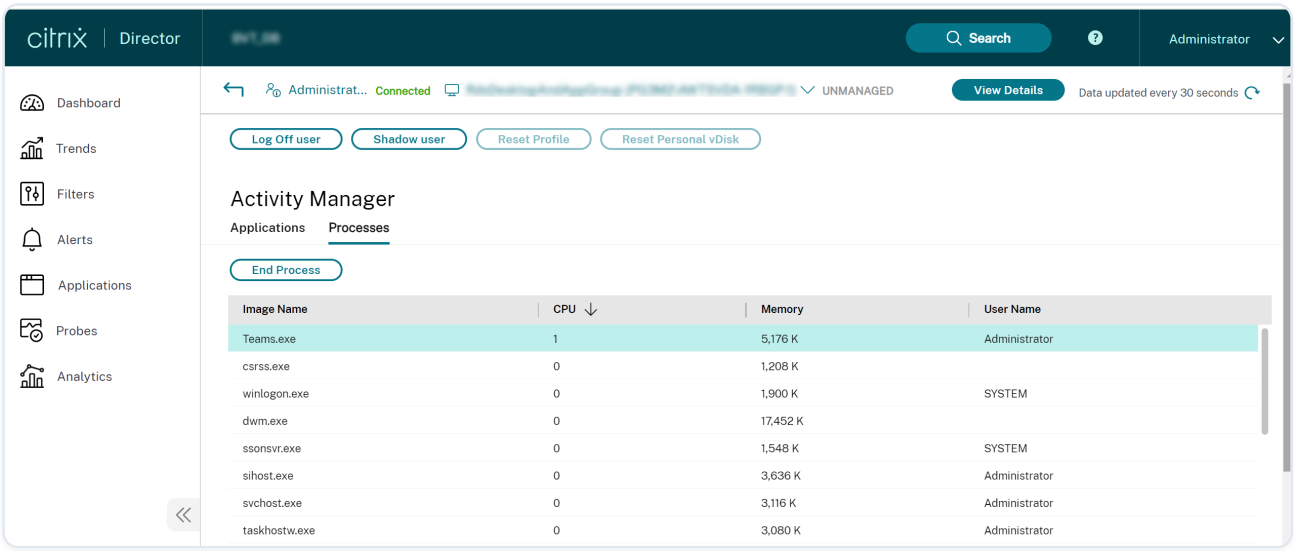
更多信息

- 监视、故障排除和支持 Microsoft Teams
- 将 Microsoft Teams 桌面应用程序部署到 VM
- 使用 MSI 安装 Microsoft Teams（VDI 安装部分）
- 瘦客户端
- Skype for Business 网络评估工具
- 了解 Microsoft Teams 和 Skype for Business 的共存和互操作性

监视、故障排除和支持 Microsoft Teams

监视 Teams

本节提供了使用 HDX 监视 Microsoft Teams 优化的指南。 如果您在优化模式下运行，并且 `HdxRtcEngine.exe` 正在客户端计算机上运行，则 VDA 上名为 `WebSocketAgent.exe` 的进程正在会话中运行。使用 Director 中的**活动管理器**查看应用程序。



可以在 Director > **用户详细信息**页面 > **会话详细信息**面板 > **MS Teams 优化**字段中查看 Microsoft Teams 优化状态。优化 Microsoft Teams 对于改善用户体验（例如清晰的音频和视频）至关重要。此功能适用于 VDA 2311 及更高版本。支持的 Citrix Workspace™ 应用程序版本列在 Microsoft Teams 优化中。仅当 Microsoft Teams 作为已发布的应用程序或在已发布的桌面中运行时，Director 才会显示 Microsoft Teams 优化状态。 有关详细信息，请参阅Microsoft Teams 优化状态。

使用 VDA 最低版本 1912，您可以使用 Citrix HDX Monitor（最低版本 3.11）监视活动的 Teams 呼叫。Citrix Virtual Apps and Desktops 产品 ISO 在文件夹 `layout\image-full\Support\HDX Monitor` 中包含最新的 `hdxmonitor.msi`。 使用 VDA 最低版本 1912，您可以使用 Citrix HDX Monitor（最低版本 3.11）监视活动的 Microsoft Teams 呼叫。Citrix Virtual Apps and Desktops 产品 ISO 在文件夹 `layout\image-full\Support\HDX Monitor` 中包含最新的 `hdxmonitor.msi`。

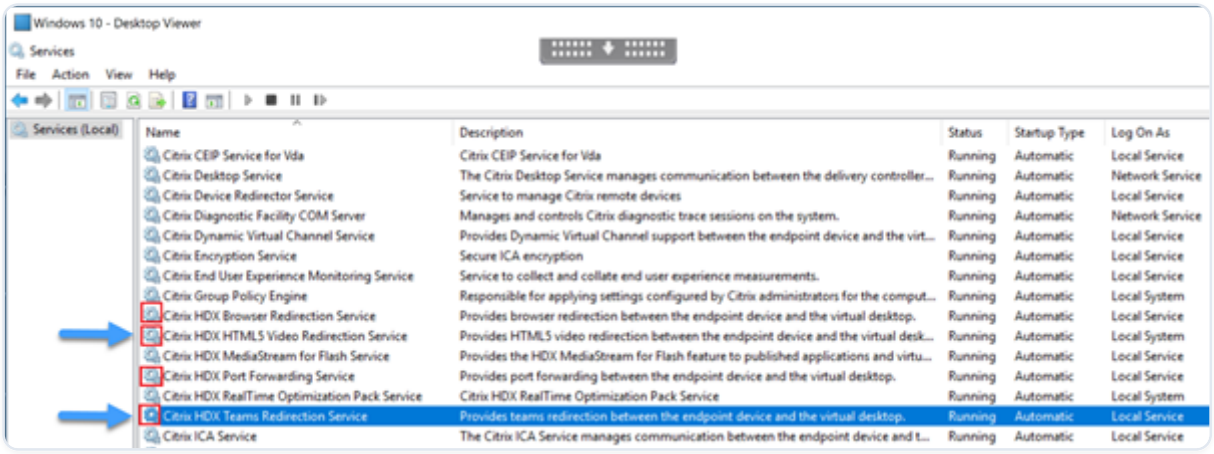
有关详细信息，请参阅知识中心文章 CTX253754 中的 “*监视*”。

故障排除

本节提供了在使用 Microsoft Teams 优化时可能遇到的问题的故障排除提示。有关详细信息，请参阅 CTX253754。

在虚拟交付代理上

BCR_x64.msi 安装了四个服务。只有两个服务负责 VDA 中的 Microsoft Teams 重定向。



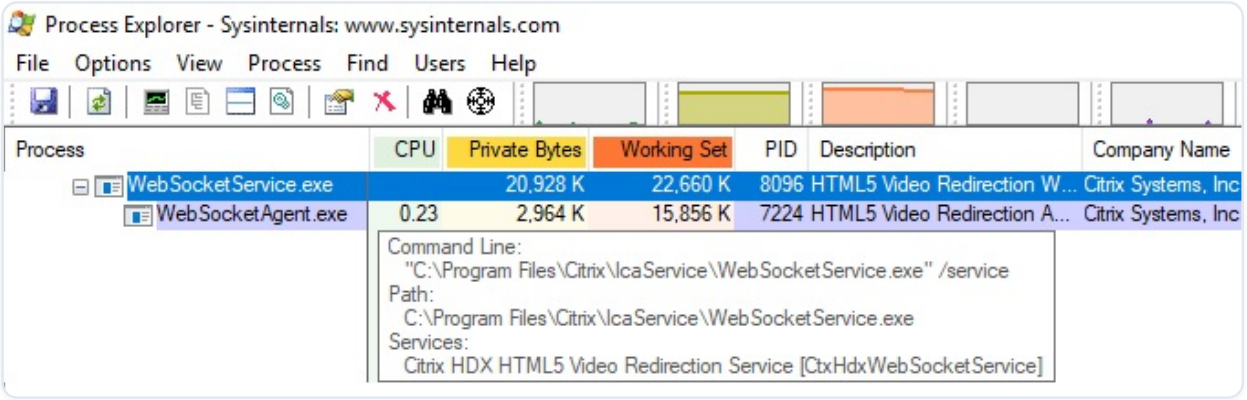
- **Citrix HDX Teams 重定向服务**建立 Microsoft Teams 中使用的虚拟通道。该服务依赖于 CtxSvcHost.exe。
- **Citrix HDX HTML5 视频重定向服务**作为 WebSocketService.exe 运行，侦听 127.0.0.1:9002 TCP。WebSocketService.exe 执行两个主要功能：

  i. **安全 WebSocket 的 TLS 终止**从 vdiCitrixPeerConnection.js 接收安全 WebSocket 连接，vdiCitrixPeerConnection.js 是 Microsoft Teams 应用程序中的一个组件。您可以使用 Process Monitor 跟踪它。有关证书的详细信息，请参阅 TLS 和 HTML5 视频重定向以及浏览器内容重定向部分。

  某些防病毒和桌面安全软件会干扰 `WebSocketService.exe` 及其证书的正常运行。尽管 Citrix HDX HTML5 视频重定向服务可能在 `services.msc` 控制台中运行，但 localhost `127.0.0.1:9002` TCP 套接字从未处于侦听模式（如 netstat 中所示）。尝试重新启动服务会导致其挂起（“正在停止...”）。确保为 `WebSocketService.exe` 进程应用适当的排除项。



ii. **用户会话映射。**当 Microsoft Teams 应用程序启动时，WebSocketService.exe 会在 VDA 中用户的会话中启动 WebSocketAgent.exe 进程。WebSocketService.exe 在会话 0 中以 LocalSystem 帐户运行。



您可以使用 `netstat` 检查 WebSocketService.exe 服务在 VDA 中是否处于活动侦听状态。

从提升的命令提示符窗口运行 `netstat -anob -p tcp`：

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

成功连接后，状态将变为 ESTABLISHED：

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

重要提示：

WebSocketService.exe 侦听两个 TCP 套接字：127.0.0.1:9001 和 127.0.0.1:9002。端口 9001 用于浏览器内容重定向和 HTML5 视频重定向。端口 9002 用于 Microsoft Teams 重定向。确保 VDA 的 Windows 操作系统中没有任何代理配置会阻止 Teams.exe 和 WebSocketService.exe 之间的直接通信。有时，当您在 Internet Explorer 11 中配置显式代理（**Internet 选项 > 连接 > 局域网设置 > 代理服务器**）时，连接可能会通过分配的代理服务器。使用手动和显式代理设置时，请验证是否已选中**对于本地地址不使用代理服务器**。

服务位置和说明

服务	WINDOWS SERVER 操作系统中可执行文件的路径	登录为	描述
Citrix HTML5 视频重定向服务	"C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service	本地系统帐户	为多个 HDX 多媒体服务提供执行虚拟桌面和端点设备之间媒体重定向所需的初始框架。
Citrix HDX 浏览器内容重定向服务	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	此帐户（本地服务）	提供端点设备和虚拟桌面之间的浏览器内容重定向。
Citrix 端口转发服务	"C:\Program Files (x86)\Citrix\System3	此帐户（本地服务）	为浏览器内容重定向提供端点设备和虚拟

服务	WINDOWS SERVER 操作系统中可执行文件的路径	登录为	描述
	2\CtxSvcHost.exe" -g PortFwdSvcs		桌面之间的端口转发。
Citrix HDX Teams 重定向服务	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	本地系统帐户	提供端点设备和虚拟桌面之间的 Microsoft Teams 重定向。

Citrix Workspace 应用程序

在用户的端点上，适用于 Windows 的 Citrix Workspace 应用程序会实例化一个名为 HdxTeams.exe 或 HdxRtcEngine.exe 的新服务。当 Microsoft Teams 在 VDA 中启动且用户尝试在自预览中呼叫或访问外设时，会发生这种情况。如果您没有看到此服务，请检查以下各项：

1. 确保您至少安装了适用于 Windows 的 Workspace App 1905 版本。您是否在 Workspace 应用程序安装路径中看到 HdxTeams.exe 或 HdxRtcEngine.exe 和 webrpc.dll 二进制文件？
2. 如果您已验证步骤 1，请执行以下操作以检查 HdxTeams.exe 或 HdxRtcEngine.exe 是否正在启动。
    a. 退出 VDA 上的 Microsoft Teams。
    b. 在 VDA 上启动 services.msc。
    c. 停止 Citrix HDX Teams 重定向服务。
    d. 断开 ICA® 会话。
    e. 连接 ICA 会话。
    f. 启动 Citrix HDX Teams 重定向服务。
    g. 重新启动 Citrix HDX HTML5 视频重定向服务。
    h. 在 VDA 上启动 Microsoft Teams。
3. 如果您仍然没有看到 HdxTeams.exe 或 HdxRtcEngine.exe 在客户端端点上启动，请执行以下操作：
    a. 重新启动 VDA。
    b. 重新启动客户端端点。

支持

Citrix 和 Microsoft 共同支持使用 Microsoft Teams 优化功能从 Citrix Virtual Apps and Desktops™ 交付 Microsoft Teams。这种联合支持是两家公司密切合作的结果。如果您拥有有效的支持合同，并且在使用此解决方案时遇到问题，请向您怀疑导致问题的供应商提交支持工单。也就是说，Teams 的问题找 Microsoft，优化组件的问题找 Citrix。 Citrix 或 Microsoft 收到工单后，会进行问题分类并酌情升级。您无需联系两家公司的支持团队。

当您遇到问题时，我们建议您在 Teams UI 中单击 **帮助 > 报告问题**。VDA 侧日志会在 Citrix 和 Microsoft 之间自动共享，以更快地解决技术问题。

收集日志

HDX 媒体引擎日志可在用户计算机上找到（不在 VDA 上）。如果出现任何问题，请务必将日志附加到您的支持案例中。

Windows 日志：

您可以在 **HDXTeams** 文件夹（AppData/Local/Temp/HDXTeams 或 AppData/Local/Temp/HdxRtcEngine）内的 %TEMP% 中找到 Windows 日志。查找名为 webrpc_Day_Month_timestamp_Year.txt 的 .txt 文件。如果您使用的是较新版本的 Citrix Workspace 应用程序（例如 Citrix Workspace 应用程序 2009.5 或更高版本），请将日志存储在 AppData\Local\Temp\HdxRtcEngine 中。

每个会话都会创建一个单独的日志文件夹。

Mac 日志：

1. VDWEBRTC 日志 - 记录虚拟通道的执行。

   位置：`/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. HdxRtcEngine 日志 - 记录 HdxRtcEngine 上进程的执行。

   位置：`$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

   HdxRtcEngine 日志默认启用。

3. Webrpc 日志 - 是最重要的日志，记录 webrtc 库的封装执行。

   位置：`/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Linux 日志：

您可以在 `/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/` 文件夹中找到 Linux 日志。 Webrtc 日志：`/tmp/webrpc/<current date>/webrtc.log` 内核日志：`/var/log/syslog`

ICE/STUN/TURN/ 日志：

建立呼叫时，需要以下四个 ICE 阶段：

- 候选收集
- 候选交换
- 连接性检查 (STUN 绑定请求)
- 候选提升

在 HdxRtcEngine.exe 日志中，以下条目是相关的交互式连接建立 (ICE) 条目。这些条目必须存在，呼叫设置才能成功。有关收集阶段的示例代码片段，请参见下文：

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering
```

```
[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

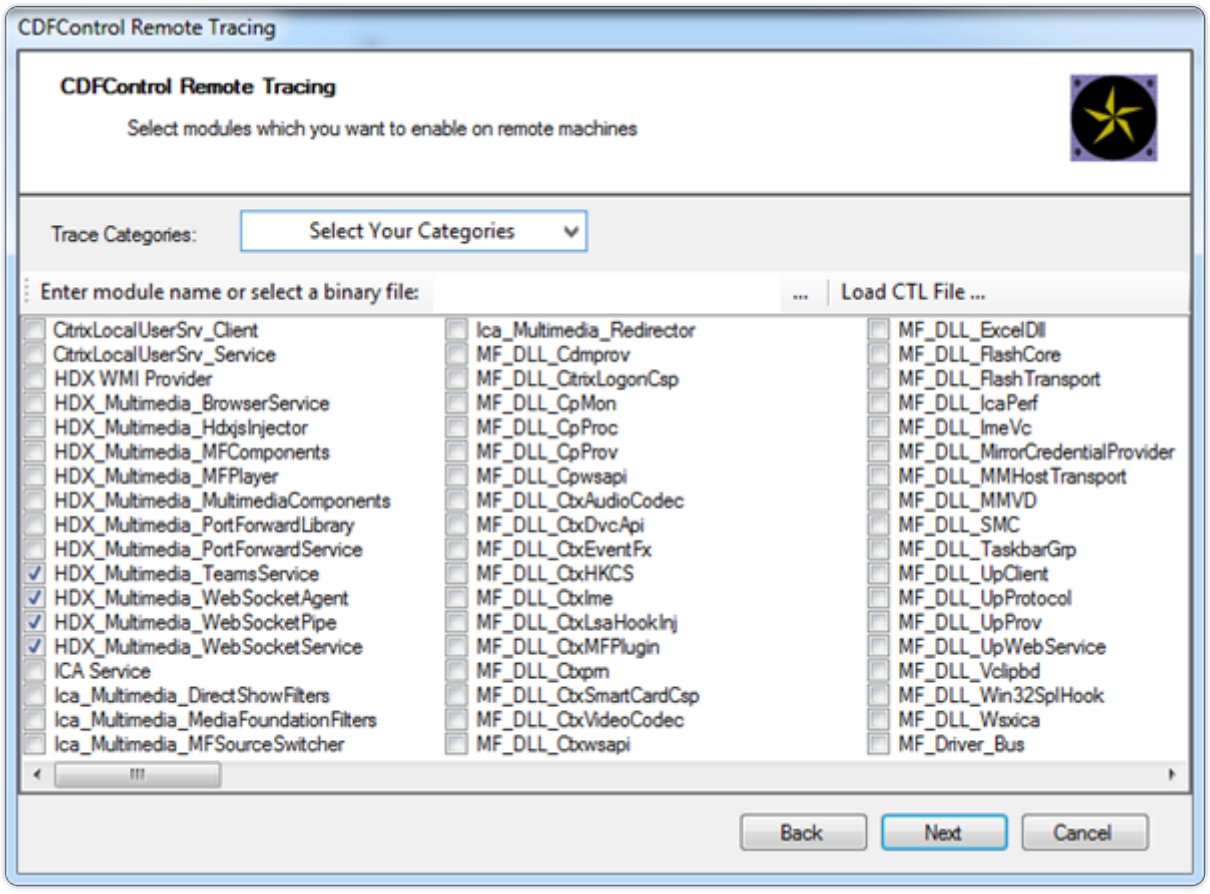
如果存在多个 ICE 候选，优先级顺序为：

1. 主机
2. 对等反射
3. 服务器反射
4. 传输中继

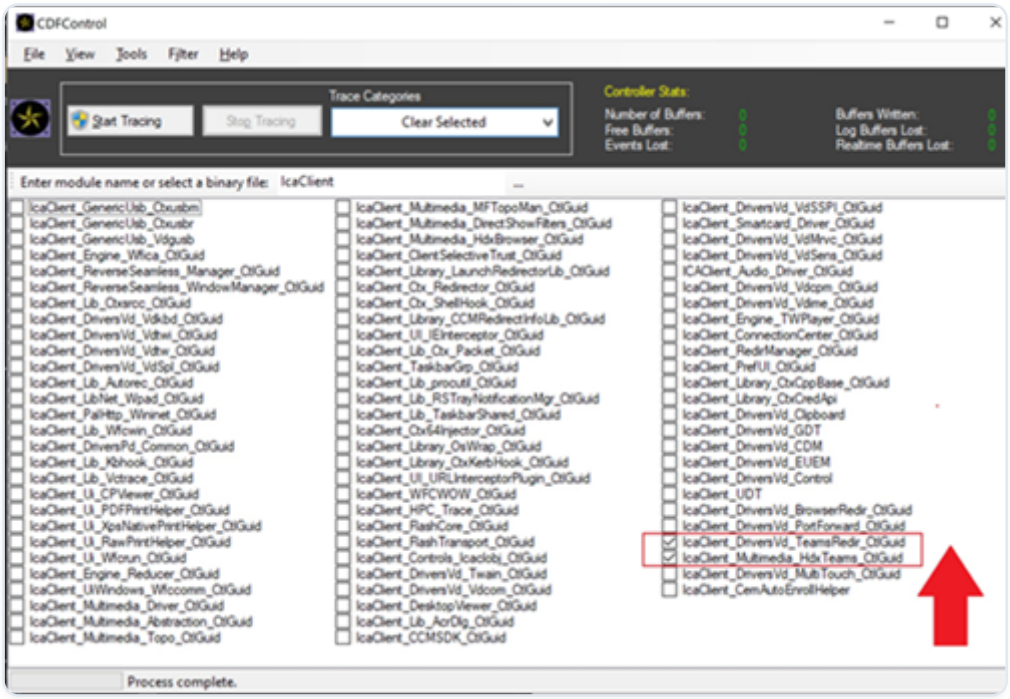
如果您遇到问题并能持续重现，我们建议您在 Microsoft Teams 中单击“**帮助 > 报告问题**”。如果您已向 Microsoft 提交案例，Citrix 和 Microsoft 之间会共享日志以解决技术问题。 在联系 Citrix 支持之前捕获 CDF 跟踪也很有益。有关详细信息，请参阅知识中心文章 CDFcontrol。

有关收集 CDF 跟踪的建议，请参阅知识中心文章 Recommendations for Collecting the CDF Traces 。

VDA 端 CDF 跟踪 - 启用以下 CDF 跟踪提供程序：



Workspace 应用程序端 CDF 跟踪 - 启用以下 CDF 跟踪提供程序：



- IcaClient_DriversVd_TeamsRedir（可选）
- IcaClient_Multimedia_HdxTeams（需要 Citrix Workspace 应用程序 2012 或更高版本）

Windows Media 重定向

Windows Media 重定向控制并优化服务器向用户交付流式音频和视频的方式。通过在客户端设备而非服务器上播放媒体运行时文件，Windows Media 重定向减少了播放多媒体文件所需的带宽。Windows Media 重定向提高了在虚拟 Windows 桌面上运行的 Windows Media Player 和兼容播放器的性能。

如果未满足 Windows Media 客户端内容获取的要求，媒体交付会自动使用服务器端获取。此方法对用户是透明的。您可以使用 Citrix Scout 从 HostMMTransport.dll 执行 Citrix 诊断工具 (CDF) 跟踪，以确定所使用的方法。有关详细信息，请参阅 Citrix Scout。

Windows Media 重定向在主机服务器上拦截媒体管道，捕获其本机压缩格式的媒体数据，并将内容重定向到客户端设备。然后，客户端设备会重新创建媒体管道，以解压缩并呈现从主机服务器接收的媒体数据。Windows Media 重定向在运行 Windows 操作系统的客户端设备上运行良好。这些设备具有重建主机服务器上存在的媒体管道所需的多媒体框架。Linux 客户端使用类似的开源媒体框架来重建媒体管道。

策略设置 **Windows Media 重定向** 控制此功能，并且默认情况下为 **允许**。通常，此设置会将从服务器呈现的音频和视频质量提高到与在客户端设备上本地播放的内容相当的水平。在极少数情况下，使用 Windows Media 重定向播放的媒体效果可能比使用基本 ICA® 压缩和常规音频呈现的媒体效果差。您可以通过将 **Windows Media 重定向** 设置添加到策略并将其值设置为 **禁用** 来禁用此功能。

有关策略设置的详细信息，请参阅 多媒体策略设置。

在屏幕截图中捕获重定向内容

Windows Media 重定向在端点上呈现媒体，因此，标准的会话内屏幕截图工具会将重定向的视频捕获为空白区域。使用 Citrix 截图工具将此内容包含在您的屏幕截图中。Citrix 建议从 Citrix Virtual Desktop Assistant 启动它，以便于查找。有关详细信息，请参阅 Citrix Virtual Desktop Assistant 文档。

限制

当您在会话中使用 Windows Media Player 并启用远程音频和视频扩展 (RAVE) 时，可能会出现黑屏。如果您右键单击视频内容并选择 **始终在顶部显示“正在播放”**，则可能会出现此黑屏。

虚拟通道插件管理器

简介

虚拟通道插件管理器旨在为指定应用程序在客户端端点上部署插件。插件管理器会检测在 VDA 上运行的特定应用程序，并提示用户在端点上安装插件，以在使用应用程序时获得最佳体验。

用户可以选择安装插件、跳过或拒绝安装。插件管理器提供了在所有端点（无论是否受管）上管理插件的灵活性。

例如：Microsoft Teams 采用了一种新的架构 (SlimCore Optimization)，需要将插件安装在端点上才能使优化生效。虚拟通道插件管理器可以在您的所有端点上部署这些插件。有关更多信息，请参阅 new VDI solution for Teams。

系统要求

以下是虚拟通道插件管理器的最低要求。

- 虚拟桌面代理 (VDA)
  - 2411 CR
- DDC
  - Cloud 121 版本
  - 2407 CR
- Citrix Workspace™ 应用程序 (Citrix Workspace 应用程序)

  - 适用于 Windows 的 Citrix Workspace 应用程序 2409
- 适用于 Mac 的 Citrix Workspace 应用程序 2508

> **注意：**
>
> 此功能目前适用于 Windows 端点。

支持的应用程序

- 目前支持的应用程序如下所示：
  - Microsoft Teams - 请参阅 适用于 Teams 的新 VDI 解决方案

虚拟通道插件管理器

了解此功能

Citrix® 了解客户环境可能很复杂，并且在托管和非托管端点上部署插件需要付出大量精力。此功能旨在简化此过程。

此功能包括两个组件：一个在 VDA 侧（检测器进程），另一个在 Citrix Workspace™ 应用程序侧（安装程序进程）。当管理员满足上述先决条件时，例如启用策略、进行注册表项并指定要监视的应用程序时：

- VDA 侧检测器进程监视最终用户登录虚拟桌面后启动应用程序的情况
- 检测器进程通知 Citrix Workspace 应用程序侧，提示用户安装优化指定应用程序所需的插件
- 用户会在屏幕上收到一个弹出窗口，其中包含有关插件的简要详细信息。用户可以选择安装插件、跳过或选择永不安装。
  - 如果用户跳过安装过程，则在该会话中不会再次看到弹出窗口。安装提示将在会话重新连接时出现。
  - 如果用户选择永不安装插件，此选择将记录在其用户配置文件中，供管理员查看。
- 如果用户选择安装插件，Citrix Workspace 应用程序侧将在端点上下载并安装插件。
  - 成功安装后，系统将向用户显示一条消息，提示他们重新连接会话以使插件生效。用户可以选择立即执行此操作，也可以关闭成功消息并稍后重新连接。
  - 如果安装失败，用户将看到错误消息，并且故障将记录下来，供管理员查看。

虚拟通道插件管理器

部署

1. 检查 Microsoft Teams 重定向策略是否已启用：有关更多详细信息，请参阅 Microsoft Teams 重定向策略。

   无论监视哪个应用程序，都必须启用此策略。将来，如果支持更多应用程序并且您希望监视这些应用程序而不是 Microsoft Teams，则仍必须启用此策略。请注意，此策略默认情况下处于启用状态。

2. 必须启用虚拟通道插件管理器策略：有关如何启用此策略的详细说明，请参阅 虚拟通道插件管理器策略设置。

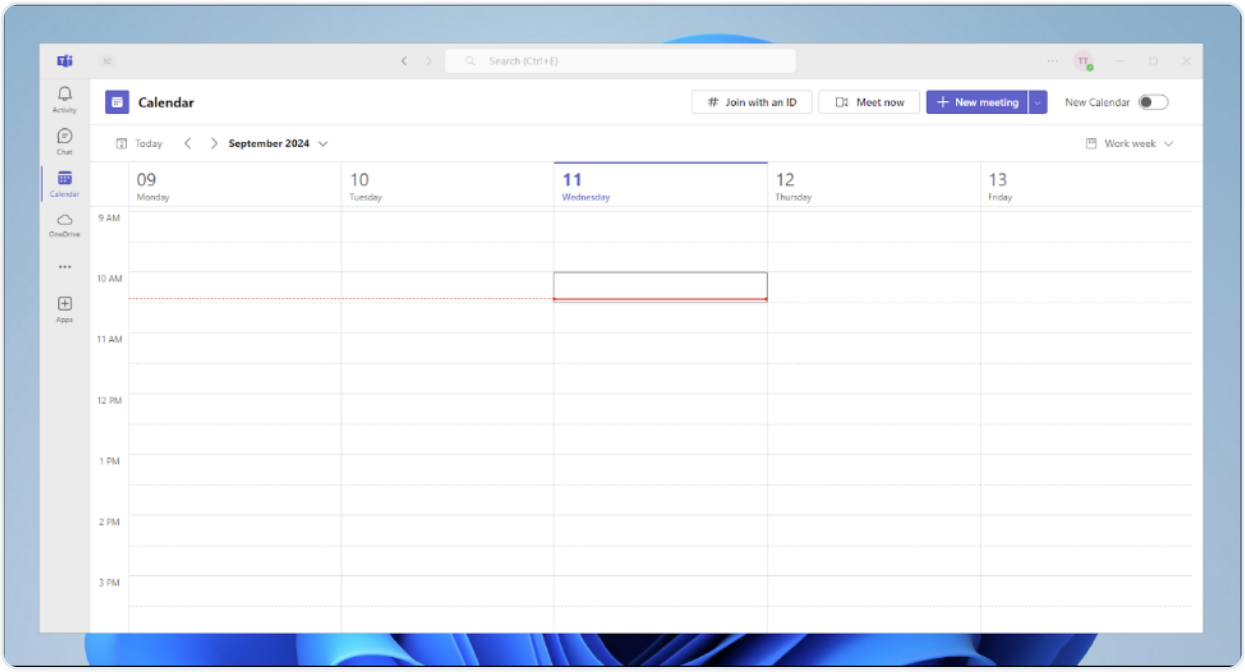
   此策略在 Citrix Studio 的多媒体策略设置中可用。启用此策略后，您可以指定要监视的应用程序名称，例如“Microsoft Teams”。此策略默认情况下处于禁用状态。

3. Citrix Workspace™ 应用程序必须以系统范围模式安装。

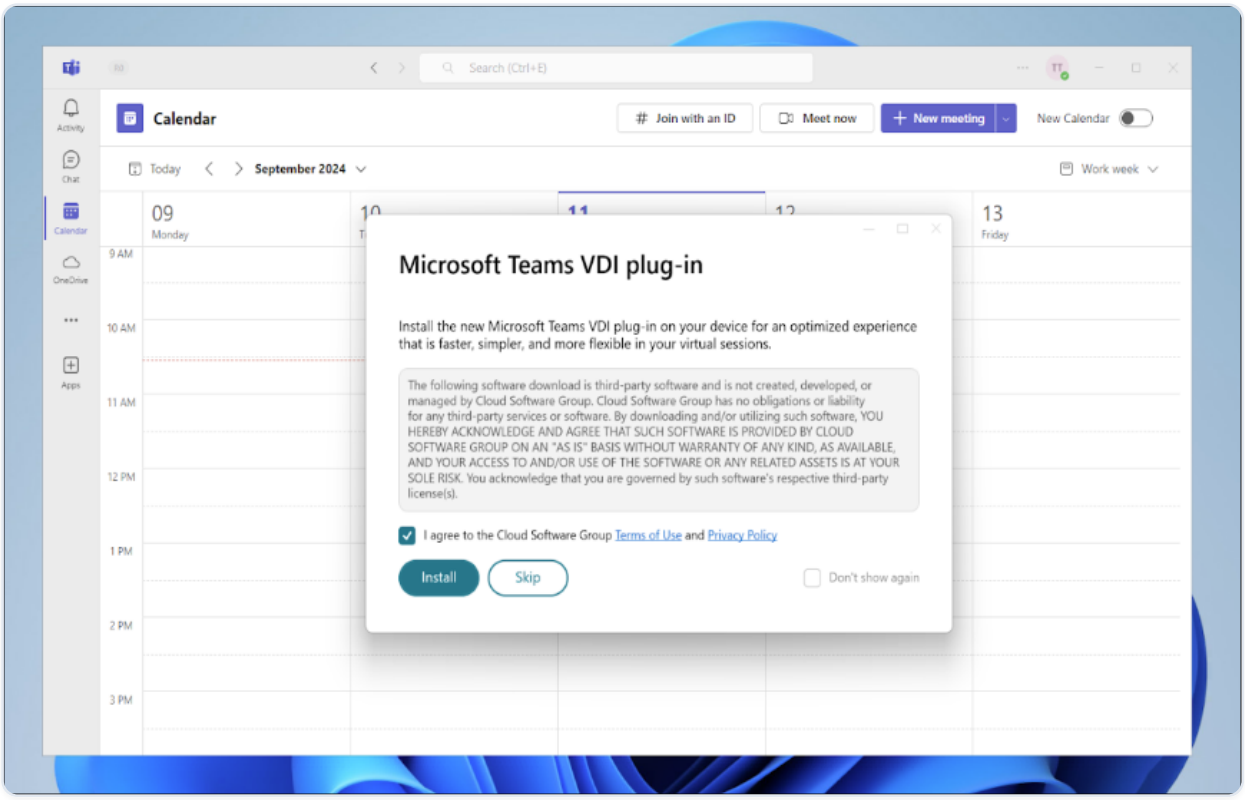
> **注意：**
>
> 插件从第三方 CDN 下载到端点。例如，如果您选择 Microsoft Teams，插件将从 Microsoft CDN 下载。因此，端点必须能够访问第三方 CDN。否则，插件安装将失败。

过程

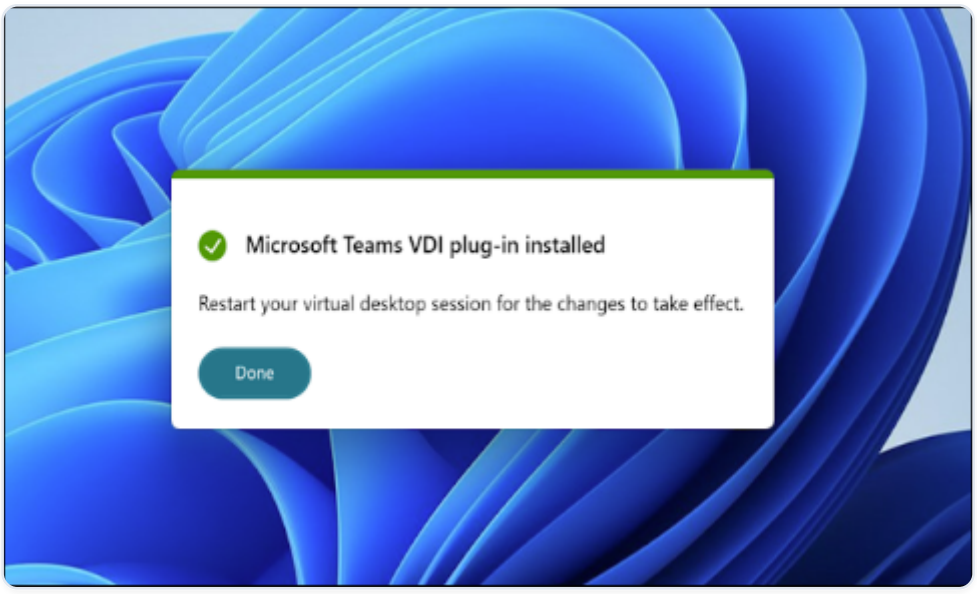
1. 用户在 Citrix 会话中启动应用程序。例如，Microsoft Teams。



2. 用户会收到一个弹出窗口，提示在端点上安装 Teams VDI 插件以获得更好的体验。弹出窗口位于会话上方而不是会话内部，因为插件将安装在端点上。



3. 用户单击安装按钮，插件随即安装。用户需要重新启动虚拟桌面会话才能使更改生效。



已知问题和限制

- 在 2407 VDA 中，除了策略之外，VDA 上还需要将以下注册表设置设为 1 才能激活此功能。此注册表设置是自动允许的，并且从 2411 VDA 开始无需配置。

  `HKLM\SOFTWARE\Citrix\HDXMediaStream

Name: EnableAppDetector Type: DWORD`

- 更多限制待添加

统一通信 SDK 优化

简介

Citrix Virtual Apps and Desktops 允许您将应用程序交付给各种终端设备上的用户。其中许多应用程序包含实时通信 (RTC) 功能，例如音频和视频会议。但是，在虚拟化环境中交付这些应用程序时可能会出现挑战。传统的交付方法会将媒体流（音频/视频）从客户端设备路由到数据中心内的 VDI 服务器，然后再将其发送回终端。这种“回传”会给服务器带来不必要的流量和处理开销，尤其是在带宽密集型音频和视频通话中。

Citrix 统一通信 SDK (UCSDK) 是一种技术，允许技术供应商优化这些 RTC 应用程序以在 Citrix 环境中使用。当应用程序经过优化后，它可以提供与在本地桌面上运行的应用程序相同甚至更好的用户体验。在当今世界，无缝的实时通信对于提高生产力和协作至关重要。在虚拟环境中使用应用程序时，音频和视频通话、屏幕共享和其他通信功能必须像在本地桌面上一样流畅运行。优化的应用程序可提供这种体验。

本产品文档详细介绍了 Citrix 客户学习和部署 UCSDK 优化应用程序所需的一切。

工作原理

Citrix 为 VDI 中的实时通信应用程序提供了一种优化的交付方法。此方法利用统一通信 SDK (UCSDK) 将虚拟化应用程序分为两部分：

- **用户界面 (UI)：** 用户界面保留在虚拟主机中，在虚拟桌面或应用程序窗口中无缝显示。
- **媒体引擎：** 媒体处理任务（音频和视频的编码/解码）被卸载到用户的本地设备。这最大限度地减少了服务器负载并优化了网络使用。

通常，Citrix 会向实时通信领域的技术供应商提供 UCSDK，并与他们合作将 UCSDK 集成到这些应用程序中。一旦集成，任何使用 UCSDK 优化应用程序的 Citrix 客户都将获得增强的体验。在构建自定义内部应用程序的情况下，Citrix 客户也可以使用 Citrix UCSDK。然而，在大多数情况下，客户不需要使用和开发 UCSDK – 他们只需要配置 Citrix 环境和应用程序即可获得优化的体验。

> **注意：**
>
> Citrix WebRTC SDK（或）HDX™ 优化应用程序的引用表示与 Citrix UCSDK 集成，并且可以互换使用。

主要优势

当您使用通过 Citrix UCSDK 优化的应用程序时，您可以期待：

- 通过将处理器密集型媒体编码/解码从 Citrix Virtual Delivery Agent (VDA) 卸载到客户端终端，增强媒体处理性能，从而提高最终用户的整体响应能力。
- 降低 Citrix VDA 上的 CPU 和带宽使用率，使 IT 部门能够支持每个主机更多的并发用户，并使企业能够经济高效地扩展 Citrix 虚拟桌面部署。
- 降低企业的总拥有成本，因为优化的终端延长了旧版虚拟桌面的使用寿命并减少了主机基础设施需求，从而随着时间的推移降低了资本支出和运营成本。
- 支持 Windows、Mac、Linux、ChromeOS 和 HTML5 终端平台。

用例

UCSDK 专为优化遵循 WebRTC 标准的实时通信应用程序而构建。以下是可以使用/已经使用 UCSDK 的关键场景和基于 WebRTC 的应用程序类型。

- **联络中心即服务 (CCaaS) / 云联络中心平台：** 主要管理跨多个渠道的客户交互，优化座席工作流程。
  - 示例：亚马逊连接、Twilio、Avaya 体验平台、Talkdesk、内容大师
- **统一通信即服务 (UCaaS) / 云业务通信：** 集成语音、视频、团队消息和状态，实现全面的业务通信。
  - 示例：Ring Central、8x8、Intermedia、阿尔卡特朗讯彩虹
- **通信平台即服务 (CPaaS)：** 提供 API，用于将实时通信功能直接嵌入到自定义应用程序中。
  - 示例：Twilio、Ribbon Communications 等公司
- **企业视频会议和协作：** 专为高质量视频会议、电话会议和高级协作功能而设计的平台。
  - 示例：Pexip
- **金融交易通信：** 专为满足金融市场独特、高性能和合规的通信需求而设计。
  - 示例：IPC Unigy
- **虚拟学习和培训平台：** 专为交互式、高质量的虚拟课堂和培训体验而设计。
  - 示例：Vitero

Citrix UCSDK 的底层 WebRTC 基础意味着其优化功能可以扩展到任何基于 WebRTC 的通信应用程序。这为优化利用 WebRTC 进行实时交互的各种应用程序打开了大门，即使它们目前尚未列为通过 UCSDK 优化的应用程序。我们鼓励客户就他们希望优化的任何用例或应用程序联系 Citrix。

UCSDK 架构

UCSDK 架构(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/ucsdk-architecture.png)

- 供应商应用程序：这可以是任何集成了 UCSDK 的第三方实时通信应用程序，可以是桌面版或基于浏览器的版本。
- UCSDK JS：UCSDK JS 提供 API，供供应商应用程序用于将音频/视频卸载到端点。
- HdxRtcEngine：这是 Citrix Workspace 应用程序中嵌入的 WebRTC 媒体引擎，用于处理和管理卸载的音频/视频通话。

SDK 加载并使用后，如果重定向成功，`HdxRtcEngine.exe` 进程将在客户端端点上启动。一旦 `HdxRtcEngine.exe` 在客户端端点上启动，任何信令和负载数据都会从 Citrix VDA 流向客户端端点，到达云端，再返回到客户端端点，然后转发到 VDA。例如，一个完整的往返流程可能是：

`Vendor App -> CitrxWebrtc.js SDK -> Citrix VDA components -> Citrix Client Endpoint components -> Cloud -> Citrix Client Endpoint components -> Citrix VDA components -> CitrxWebrtc.js SDK -> Vendor App`

系统要求

系统要求指出了与最新版 UCSDK - 5.0.0 配合使用的 Citrix 组件的各种版本。有关旧版 SDK 的兼容性详细信息和特定功能要求，请参阅下面的 版本和功能矩阵 表。

> **注意：**
>
> 客户若要使用添加到 UCSDK 的任何功能，请确保供应商应用程序已集成相应的 UCSDK 版本并启用了该功能，并在您的环境中使用相应的 VDA 和 CWA 版本。

完全兼容的版本

完全兼容的版本表示，通过将这些版本的 Citrix 组件与最新版 UCSDK 结合使用，客户可以利用所有可用功能。对于当前最新版 UCSDK – 5.0.0，完全兼容的 Citrix 组件版本如下：

- **Citrix 虚拟应用和桌面™：** 2607 LTSR
- **Citrix Workspace 应用程序 Windows：** 2607 LTSR

- **Citrix Workspace 应用程序 Mac：** 待发布
- **Citrix Workspace 应用程序 Linux：** 2607 LTSR
- **Citrix Workspace 应用程序 ChromeOS/HTML5：** 待发布

> **注意：**
>
> UCSDK 优化支持所有端点平台：Windows、Mac、Linux、ChromeOS 和 HTML5。如果上述列表显示某个特定端点平台“待发布”，则表示尚未发布与最新 UCSDK 功能完全兼容的版本。因此，即使使用较新的 UCSDK，客户仍然可以使用旧版本的 Citrix Workspace 应用程序来继续使用现有功能。

配置

UCSDK 功能取决于三个因素：供应商集成的 UCSDK 版本和供应商启用的功能、Citrix Virtual Apps and Desktops 以及正在使用的 Citrix Workspace 应用程序版本。

在 Citrix 端，请确保配置以下内容，以便允许优化应用程序：

1. 确保 Microsoft Teams 重定向策略已开启。有关详细信息，请参阅 多媒体策略设置。请注意，此策略默认处于开启状态。
2. 默认情况下，不支持使用 `CitrixWebrtc.js` SDK 的第三方 Electron 或基于浏览器的应用程序。`CtxHdxWebSocketService`（`WebSocketService.exe`）不允许来自不在允许列表中的应用程序的连接。必须将所需的应用程序二进制可执行文件名称添加到白名单注册表项。

> **注意：**
>
> 从 CVAD 2607 LTSR 开始，使用 Citrix 统一通信 SDK (UCSDK) 的应用程序的优化不再依赖于 **Microsoft Teams 重定向**策略。管理员现在可以禁用 Microsoft Teams 优化，而不会影响其他集成 UCSDK 的应用程序。要使用此分离，供应商应用程序必须与 CVAD 2607 LTSR 一起使用 Bootstrap 方法（首次在 UCSDK 4.0 中引入）。有关更多详细信息，请参阅 统一通信 SDK 文档。

在 VDA 上

- 创建密钥路径：`HKLM\Software\WOW6432Node\Citrix\WebSocketService`
- 密钥名称：`ProcessWhitelist`

- 类型: `MULTISZ`
- 密钥值：`Mytestapp.exe`

如果有多个应用程序，请在新行中键入每个应用程序。请勿从文本文件复制粘贴或插入逗号。确保提供的名称与应用程序的可执行文件名称匹配。此注册表值不区分大小写。

如果应用程序是通过浏览器而不是成熟的桌面应用程序访问的，则需要在注册表值中允许，例如 `chrome.exe`。

成功配置上述注册表后，重新启动 VDA 或重新启动 `CtxHdxWebSocketService` 以完成白名单设置。

在客户端上

无需配置。只需安装 Citrix Workspace 应用程序。

每个供应商可能都有一个非常具体的应用程序名称。因此，请参阅(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/policies/reference/ica-policy-settings/multimedia-policy-settings.html#microsoft-teams-redirection)部分中链接的供应商文档，以确定WebSocketService中必须允许哪个应用程序名称。

功能参考

在屏幕截图中捕获重定向内容

当经过UCSDK优化的应用程序涉及视频或共享屏幕叠加时，该内容会在端点上呈现，因此标准的会话内屏幕截图工具会将其捕获为空白区域。使用Citrix Snipping Tool将此内容包含在您的屏幕截图中。Citrix建议从Citrix Virtual Desktop Assistant启动它，以便于查找。有关更多信息，请参阅(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/manage-deployment/assistant-app.html#tools-page)。

通过智能同步缩短呼叫连接时间

Smart Sync 功能在 UCSDK 5.0.0 中引入，通过简化 VDA 和客户端端点之间的通信来缩短呼叫连接时间。此增强功能全面加快了呼叫设置速度，为高延迟网络环境提供了最显著的性能改进。

Citrix 建议客户联系其应用程序供应商，升级到 UCSDK 5.0.0 以利用此功能。

> **注意：**
>
> 此功能仅依赖于 UCSDK 5.0.0 和 Citrix Workspace 应用程序。有关确切的客户端版本，请参阅版本和功能矩阵。没有 VDA 版本依赖性，因此仍可使用较旧的支持的 VDA。

解耦 UCSDK 和 HDX Microsoft Teams 优化

此功能将统一通信 SDK (UCSDK) 的优化逻辑与 Microsoft Teams 优化策略分离。以前，“Microsoft Teams 重定向”策略充当主开关；为 Teams 禁用它会无意中强制所有其他基于 UCSDK 的应用程序回退到服务器端渲染。

通过此增强功能，无论 Teams 策略状态如何，WebRTC 重定向所需的虚拟通道都可用于第三方应用程序。

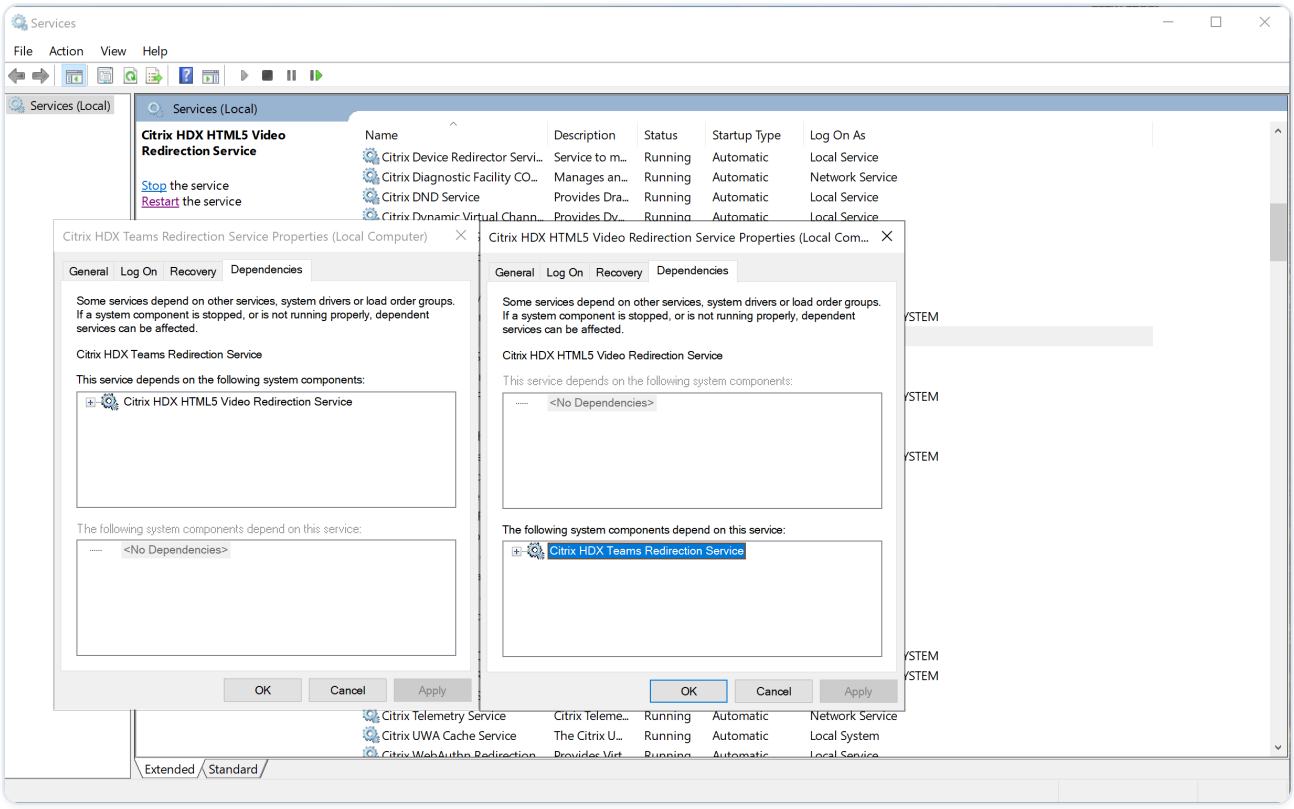
- **优势**
  - **精细控制：** 管理员可以有选择地管理 Microsoft Teams 优化策略，而不会影响 Amazon Connect、Five9、RingCentral 或其他 UCSDK 集成应用程序等关键业务应用程序的优化。
  - **操作稳定性：** 通过防止 UCSDK 优化应用程序中意外的性能下降来确保业务连续性。管理员可以禁用 HDX Teams 优化以进行故障排除或合规性原因，而不会破坏其主要业务工具的高清音频/视频体验。
- **要求**
  - **VDA 要求：** Citrix Virtual Apps/Desktops 2607 LTSR 或更高版本
  - **应用程序兼容性：** 第三方应用程序必须使用 UCSDK 引导初始化方法

> **注意：**
>
> - 此功能不影响 Microsoft Teams SlimCore 优化。SlimCore 优化使用 Microsoft 专有虚拟通道独立运行，不依赖于 Citrix CTXMTOP 虚拟通道。
> - 要利用此功能，第三方应用程序必须使用 UCSDK 4.0 或更高版本构建。客户应向应用程序供应商（例如 Amazon Connect、Five9、RingCentral）核实其特定版本是否使用引导初始化。

Microsoft Teams 优化的显式服务依赖项

从 Citrix Virtual Apps / Desktops 2607 LTSR 开始，**Citrix HDX Teams Redirection Service**（由 HDX 优化 Microsoft Teams 和 UCSDK 优化应用程序使用）现在明确声明依赖于 **Citrix HDX HTML5 Video Redirection Service (WebSocketService)**。

此更新可确保在 Teams 服务启动时自动验证并启动 HTML5 服务，从而防止在服务严格管理的环境中 Microsoft Teams 和 UCSDK 集成应用程序的优化失败。



优化叠加剪裁以增强性能和用户体验

从 CVAD 2511 开始，用于处理 HDX Microsoft Teams 优化和 UCSDK 优化等功能中重定向视频叠加的机制已重新设计，以改善用户体验和服务器性能。

主要优势

- **改进的视觉准确性：** 此增强功能解决了应用程序元素（例如弹出菜单或通知）错误地出现在视频内容后面的视觉故障。新逻辑确保所有组件都以正确的顺序呈现，从而提供更无缝和可预测的体验。
- **增强的性能：** 此优化显著降低了虚拟投递代理上的 CPU 利用率。通过用更高效的基于图形的方法取代旧的、资源密集型轮询方法，此更改提高了服务器可伸缩性并允许更高的用户密度。

> **注意：**
>
> 此功能取决于未来版本的 Microsoft Teams（或其他 UCSDK 合作伙伴应用程序），并且需要 Citrix Workspace App for Windows 2511。

版本和功能矩阵

由于版本更新频繁，请参阅 Citrix Virtual Apps and Desktops 和 Citrix Workspace app 产品生命周期页面，以确保特定版本受支持。对于许多旧功能，表中提及的版本是撰写本文档时最后受支持的当前版本 (CR)。

功能	UCSDK 版本	VDA	CWA WINDOWS 客户端	CWA MAC	CWA LINUX 版	CWA CHROME OS/ HTML5
音频/视频 (点对点和会议)	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
屏幕共享	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
DTMF	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
代理服务器支持	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
应用程序共享	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	N/A
动态 e911	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
多窗口	3.1.0	2203 LTSR 最	2402 LTSR 最	2311	2311	2312

功能	UCSDK 版本	VDA	CWA WINDOWS 客户端	CWA MAC	CWA LINUX 版	CWA CHROME OS/ HTML5
		新 CU / 2311 CR	新 CU / 2311 CR			
SDP 统一计划支持	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
流分辨率 / 同播	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
远程音频（带循环）	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2405
基于浏览器的 UCSDK（引导支持）	4.0.2	2407 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
Web HID API	4.0.2	2203 LTSR 最新 CU / 2311 CR	2409.10	2411	2411	2505
网络音频 API	4.0.2	2203 LTSR 最新 CU / 2311 CR	2405	2405	2405	N/A
重新启动 ICE	4.1.0	2203 LTSR 最新 CU / 2311 CR	2503.2	2503	2503	2502.10

功能	UCSDK 版本	VDA	CWA WINDOWS 客户端	CWA MAC	CWA LINUX 版	CWA CHROME OS/ HTML5
屏幕录制(预览)[1]	4.1.0	2503	2503.2	N/A	N/A	N/A
智能同步	5.0.0	2203 LTSR 最新 CU / 2311 CR	2607 LTSR	N/A	2604	N/A

注意：

我们为屏幕录制引入了一项新策略，因此您需要 2503 版本的 delivery controller™，它随附于 CVAD 2503。

当前供应商支持

许多第三方供应商已将统一通信 SDK 集成到其产品中。以下是当前供应商及其支持文档的列表：

供应商	文档
斯普林克勒	适用于语音呼叫的 Citrix 媒体卸载 - Sprinklr
微软 Dynamics 365	Dynamics 365 联络中心文档
亚马逊 Connect	为 Citrix 云桌面优化 Amazon Connect 音频
铃盛	在 Citrix VDI 环境中使用 RingCentral
福耐特	Citrix 环境中的 Five9 WebRTC
特威利奥	Citrix VDI 上的特威利奥 Flex
亚美亚	适用于 Citrix 的 Avaya Experience Platform 公有云 VDI 解决方案
8x8	Citrix VDI 与 8x8 Work 桌面版和 Web 版的集成

供应商	文档
康腾古鲁	康腾古鲁 Citrix 集成
瑞本通信	瑞本通信 Citrix WebRTC SDK
英特媒体	在 Citrix Virtual Apps and Desktops 上安装英特媒体 Unite
阿尔卡特朗讯彩虹	针对 Rainbow 桌面应用程序的 Citrix 优化
拓客	Talkdesk 座席工作区 VDI 连接
IPC	IPC Unigy 软客户端 Citrix VDI
维特罗	适用于 Citrix VDI 的 Vitero Inspire
佩克西普	在 Citrix Pexip Infinity Docs 中部署 Connect 桌面应用程序
Zoom Web 应用程序	为 Zoom Web 应用程序配置 WebRTC 重定向

故障排除

有关故障排除信息，请参阅 针对使用 Citrix 统一通信 SDK 优化的应用程序的故障排除指南。

已知问题和限制

本节将记录当前已识别的已知问题和限制。

通用内容重定向

内容重定向允许您控制用户是通过服务器上发布的应用程序访问信息，还是通过在用户设备本地运行的应用程序访问信息。

客户端文件夹重定向

客户端文件夹重定向改变了客户端文件在主机端会话中的访问方式。

- 当您仅在服务器上启用客户端驱动器映射时，客户端完整卷会自动作为通用命名约定 (UNC) 链接映射到会话。
- 当您在服务器上启用客户端文件夹重定向并且用户在 Windows 桌面设备上对其进行配置时，用户指定的本地卷部分将被重定向。

主机到客户端重定向

对于某些不常见的用例，请考虑使用主机到客户端重定向。通常，其他形式的内容重定向可能更好。我们仅在多会话操作系统 VDA 上支持此类型的重定向，而不支持在单会话操作系统 VDA 上。

本地应用访问和 URL 重定向

本地应用访问将本地安装的 Windows 应用程序无缝集成到托管桌面环境中。它无需在不同计算机之间切换即可实现此目的。

客户端文件夹重定向

客户端文件夹重定向改变了客户端文件在主机端会话中的访问方式。如果只在服务器上启用客户端驱动器映射，客户端的完整卷将自动映射为通用命名约定 (UNC) 链接到会话。当您在服务器上启用客户端文件夹重定向并且用户在用户设备上配置它时，用户指定的本地卷部分将被重定向。

只有用户指定的文件夹会作为 UNC 链接出现在会话中。也就是说，它不是用户设备上的完整文件系统。如果您通过注册表禁用 UNC 链接，客户端文件夹将作为映射驱动器出现在会话中。

客户端文件夹重定向仅在 Windows 单会话操作系统计算机上受支持。

外部 USB 驱动器的客户端文件夹重定向在设备分离和重新连接后不会保存。

在服务器上启用客户端文件夹重定向。然后，在客户端设备上，指定要重定向的文件夹。用于指定客户端文件夹选项的应用程序 (CtxCFRUI.exe) 随此版本提供的 Citrix Workspace 应用程序一起提供。

要求：

对于服务器：

- Windows 服务器 2022
- Windows Server 2019，标准版和数据中心版

对于客户端：

- Windows 10 系统
- Windows 十一

要在服务器上启用客户端文件夹重定向，请参阅通过注册表管理的特性列表中的客户端文件夹重定向。

在用户设备上，指定要重定向的文件夹：

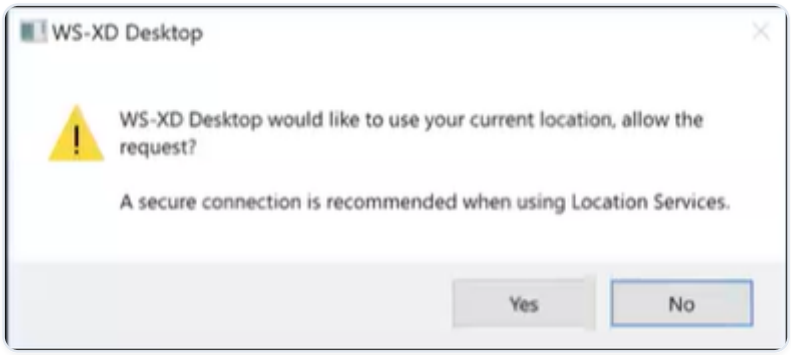
1. 确保已安装最新版本的 Citrix Workspace™ 应用程序。
2. 从 Citrix Workspace 应用程序安装目录中，启动 CtxCFRUI.exe **(..\Citrix\ICA Client\CtxCFRUI.exe)**。
3. 选择 **Custom** 单选按钮，然后添加、编辑或删除文件夹。
4. 断开并重新连接您的会话以使设置生效。

客户端位置重定向

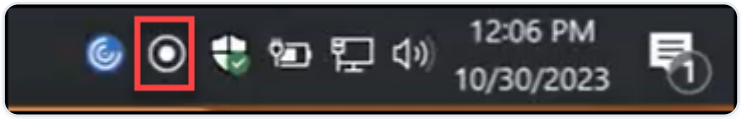
启用客户端位置重定向后，VDA 托管的应用程序和桌面会话可以无缝访问客户端的当前位置。在多会话操作系统（TS VDA 或多会话 WS VDA）上，每个会话都有其由连接的客户端提供的唯一位置。使用此功能，VDA 上依赖位置的应用程序可以获取客户端的准确位置。

有关详细信息，请参阅 Microsoft 文档。

在启用客户端位置重定向并允许服务器端和客户端访问位置后，当您启动访问位置的应用程序或桌面时，客户端会提示您通过以下对话框共享其当前位置：



启用客户端位置重定向后，如果 VDA 托管的应用程序或桌面查询当前位置信息，客户端任务栏中将显示以下图标。



系统要求

对于服务器：

- 单会话 (Win10/11) 或多会话 (Win 11 22H2 和 Server 2022 23H2 或更高版本) OS VDA
- 适用于 Windows、iOS 或 Android 的 Citrix Workspace™ 应用程序

配置

必须使用 Citrix® 策略启用客户端位置重定向，此功能才能正常工作。客户端位置重定向默认处于禁用状态。

要启用客户端位置重定向，请完成以下步骤：

在 Windows VDA 和客户端上：

1. 在“**设置 > 隐私 > 位置**”中，启用以下选项：
    - **允许此设备访问位置**
    - **允许应用访问您的位置**
    - **允许桌面应用程序访问您的位置**
2. 对于多会话操作系统，请启用**位置覆盖**设置。

在 Controller/DDC 端：

启用 **Studio > 策略 > 位置 > 设置 > 允许应用程序使用客户端设备的物理位置** 策略。 有关详细信息，请参阅客户端传感器策略设置。

双向内容重定向

双向内容重定向允许 Web 浏览器中的 HTTP 或 HTTPS URL，或嵌入到应用程序中的 URL，在 Citrix VDA 会话和客户端端点之间双向转发。在 Citrix 会话中运行的浏览器中输入的 URL 可以使用客户端的默认浏览器打开。相反，在客户端上运行的浏览器中输入的 URL 可以在 Citrix 会话中打开，无论是通过发布的应用程序还是桌面。双向内容重定向的一些常见用例包括：

- 在启动浏览器无法访问源的网络的情况下重定向 Web URL。
- 出于浏览器兼容性和安全原因重定向 Web URL。
- 当不希望在 Citrix 会话或客户端上运行 Web 浏览器时，重定向嵌入在应用程序中的 Web URL。

系统要求

- 单会话或多会话操作系统 VDA
- 适用于 Windows 的 Citrix Workspace™ 应用程序 2311 或更高版本
- 适用于 Linux 的 Citrix Workspace™ 应用程序 2503 或更高版本
- 适用于 Mac 的 Citrix Workspace™ 应用程序 2607 或更高版本

浏览器：

- 带有 Citrix 浏览器重定向扩展程序的 Google Chrome
  - Google Chrome 扩展程序
- 带有 Citrix 浏览器重定向扩展程序的 Microsoft Edge
  - Microsoft Edge 扩展程序

配置

从 Citrix Virtual Apps and Desktops™ 2311 版本开始，双向内容重定向仅通过 Citrix Studio 进行配置。以前的版本在客户端端点和 Studio 上都配置了策略设置。双向内容重定向默认处于禁用状态。

有关 VDA 配置，请参阅 **ICA 策略**设置中的双向内容重定向。

要使浏览器重定向正常工作，必须使用所示命令在原始浏览器（URL 重定向来源）上注册浏览器扩展程序。根据所使用的浏览器，在 VDA 和客户端上按需运行这些命令。

浏览器	VDA	客户端
谷歌浏览器	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regChrome
微软 Edge	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regEdge
所有可用浏览器	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regall	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regall

要注销浏览器扩展：

浏览器	VDA	客户端
谷歌浏览器	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregChrome
微软 Edge	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregEdge
所有可用浏览器	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /注销所有	"%ProgramFiles(x86)%\Citrix\ICA Client\重定向器.exe" /取消注册所有

注意：

- 在具有管理员权限的命令提示符 (CMD) 窗口中运行这些命令。
- 注册命令会使 Chrome 和 Edge 浏览器在首次启动时提示用户启用 Citrix 浏览器重定向扩展。

- 注册命令还会将浏览器重定向扩展链接到本机消息传递主机，这允许扩展与本机代码通信。如果没有此功能，浏览器将阻止通信。
- 您也可以从 Google Chrome 网上应用店手动安装浏览器扩展。要从 Microsoft Edge 附加组件商店使用浏览器重定向扩展，您需要 Virtual Delivery Agent (VDA) 2503 或更高版本。对于较旧的 VDA 版本，请在 Microsoft Edge 浏览器中从 Google Chrome 网上应用店安装该扩展（请参阅 从 Chrome 网上应用店向 Microsoft Edge 添加扩展）。
- 系统要求中列出的 Citrix Workspace 应用程序版本是支持双向内容重定向和 OAuth 重定向所需的最低版本。
- 对于 Mac：由于 macOS 对公证应用程序的安全要求，自定义 OAuth 回调 URL 方案必须预先在 Citrix 注册，并且不能在安装后动态更改。默认情况下仅支持 `citrix-oauth-redir`。请联系 Citrix 产品团队注册您的 URL 方案。

从 Citrix VDA 到客户端的通配符重定向

双向内容重定向支持在定义要重定向的 URL 时使用通配符。要配置双向内容重定向，请参阅配置说明。

从 VDA 到客户端的自定义协议重定向

双向内容重定向支持将自定义协议从 Citrix VDA 重定向到客户端。支持 HTTP 或 HTTPS 以外的协议。要配置双向内容重定向，请参阅配置说明。

在 Web Studio 中，在**双向内容重定向**中设置自定义协议。

注意：

- 您必须具有管理员权限才能运行这些命令。
- 客户端必须注册一个应用程序来处理该协议。否则，URL 将重定向到客户端并启动失败。
- 在 Chrome 和 Edge 浏览器中输入或启动的自定义协议 URL 不受支持，也不会被重定向。
- 不支持以下协议：`rtsp://, rtspu://, pnm://, mms://`。

其他注意事项

- 浏览器要求和配置仅适用于启动重定向的浏览器。重定向成功后 URL 打开的目标浏览器不属于支持范围。将 URL 从 VDA 重定向到客户端时，仅 VDA 上需要支持的浏览器配置。相反，将

URL 从客户端重定向到 VDA 时，仅客户端上需要支持的浏览器配置。重定向的 URL 将根据方向移交给目标计算机（客户端或 VDA）上配置的默认浏览器。不需要在 VDA 和客户端上使用相同的浏览器类型。

- 检查重定向规则是否会导致循环配置。例如，VDA 策略设置为重定向 `https://www.citrix.com`，而客户端策略设置为重定向相同的 URL，从而导致无限循环。
- 不支持 URL 缩短器。
- 客户端到 VDA 的重定向要求使用管理员权限安装 Windows 客户端。
- 如果目标浏览器已打开，则重定向的 URL 会在新选项卡中打开。否则，URL 会在新浏览器窗口中打开。
- 启用本地应用访问 (LAA) 时，双向内容重定向不起作用。

主机到客户端重定向

主机到客户端重定向允许在 Citrix® 会话中运行的应用程序中嵌入为超链接的 URL 使用用户端点设备上的相应应用程序打开。主机到客户端重定向的一些常见用例包括：

- 在 Citrix 服务器无法访问 Internet 或网络源的情况下重定向网站。
- 出于安全、性能、兼容性或可伸缩性原因，不希望在 Citrix 会话中运行 Web 浏览器时重定向网站。
- 在 Citrix 服务器上未安装打开 URL 所需的应用程序的情况下重定向特定 URL 类型。

主机到客户端重定向不适用于您在网页上访问或在 Citrix 会话中运行的 Web 浏览器的地址栏中键入的 URL。有关 Web 浏览器中 URL 的重定向，请参阅双向 URL 重定向或浏览器内容重定向。

系统要求

- 多会话操作系统 VDA
- 支持的客户端：
  - 适用于 Windows 的 Citrix Workspace™ 应用程序
  - 适用于 Mac 的 Citrix Workspace 应用程序
  - 适用于 Linux 的 Citrix Workspace 应用程序
  - 适用于 HTML5 的 Citrix Workspace 应用程序
  - 适用于 Chrome 的 Citrix Workspace 应用程序

客户端设备必须安装并配置一个应用程序，用于处理 URL 类型的重定向。

配置

使用 主机到客户端重定向 Citrix 策略启用此功能。**主机到客户端重定向**默认处于禁用状态。启用主机到客户端重定向策略后，Citrix Launcher 应用程序会向 Windows 服务器注册，以确保它可以拦截 URL 并将其发送到客户端设备。

然后，您必须配置 Windows 组策略，以使用 Citrix Launcher 作为所需 URL 类型的默认应用程序。在 Citrix 服务器 VDA 上，创建 ServerFTAdefaultPolicy.xml 文件并插入以下 XML 代码。

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

在组策略管理控制台中，转到 **计算机配置 > 管理模板 > Windows 组件 > 文件资源管理器 > 设置默认关联配置文件**， 并保存您的 ServerFTAdefaultPolicy.xml 文件。

> **注意：**

> 如果 Citrix 服务器没有组策略设置，Windows 会提示用户选择一个应用程序来打开 URL。

> 默认情况下，我们支持以下 URL 类型的重定向：

- HTTP
- HTTPS

- RTSP
- RTSPU
- PNM
- MMS

要将其他标准或自定义 URL 类型添加到重定向列表，请在前面引用的 ServerFTAdefaultPolicy.xml 文件中创建新的 **Association Identifier** 行。例如：

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

将 URL 类型添加到列表还需要客户端配置。在 Windows 客户端上创建以下注册表项和值。

> **注意：**
>
> 错误编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。编辑注册表之前，请务必备份注册表。

- 项：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 值名称：ExtraURLProtocols
- 值类型：REG_SZ
- 值数据：指定所需的 URL 类型，用分号分隔。包括 URL 权限部分之前的所有内容。例如：`ftp://;mailto:;customtype1://;custometype2://`

您只能为 Windows 客户端添加 URL 类型。缺少上述注册表设置的客户端会拒绝重定向回 Citrix 会话。客户端必须安装并配置一个应用程序来处理指定的 URL 类型。

要从默认重定向列表中删除 URL 类型，请在服务器 VDA 上创建以下注册表项和值。

- 项: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 值名称: DisableServerFTA
- 值类型: DWORD
- 值数据: 1
- 值名称: NoRedirectClasses
- 值类型: REG_MULTI_SZ
- 值数据: 指定以下值的任意组合：`http`、`https`、`rtsp`、`rtspu`、`pnm` 或 `mms`。在单独的行上键入多个值。例如：

`http`

`https`

`rtsp`

要针对特定网站集启用主机到客户端重定向，请在服务器 VDA 上创建注册表项和值。

- 项: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 值名称: ValidSites
- 值类型: REG_MULTI_SZ
- 值数据: 指定完全限定域名 (FQDN) 的任意组合。在单独的行上键入多个 FQDN。仅包含 FQDN，不带协议 (`http://` 或 `https://`)。FQDN 只能在最左侧位置包含星号 (`*`) 作为通配符。此通配符匹配单个域级别，这与 RFC 6125 中的规则一致。例如：

`www.exmaple.com`

`*.example.com`

> **注意：**
>
> 您不能将 **ValidSites** 键与 **DisableServerFTA** 和 **NoRedirectClasses** 键一起使用。

服务器 VDA 默认浏览器配置

本节中提及的启用主机到客户端重定向会覆盖服务器 VDA 上任何先前的默认浏览器配置。如果 Web URL 未重定向，Citrix Launcher 会将该 URL 传递给 `command_backup` 注册表项中配置的浏

览器。该注册表项默认指向 Internet Explorer，但您可以修改它以包含不同浏览器的路径。有关详细信息，请参阅注册表管理的功能列表中的 服务器 VDA 默认浏览器配置。

本地应用访问和 URL 重定向

简介

本地应用访问将本地安装的 Windows 应用程序无缝集成到托管桌面环境中，无需在不同桌面之间切换。通过本地应用访问，您可以：

- 直接从虚拟桌面访问安装在物理笔记本电脑、PC 或其他设备上的本地应用程序。
- 提供灵活的应用程序交付解决方案。如果用户拥有无法虚拟化或 IT 部门不维护的本地应用程序，这些应用程序仍会像安装在虚拟桌面上一样运行。
- 消除应用程序与虚拟桌面分开托管时产生的双跳延迟。为此，请在用户的 Windows 设备上放置已发布的应用程序的快捷方式。
- 使用以下应用程序：
    - 视频会议软件，例如 GoToMeeting。
    - 尚未虚拟化的专业或小众应用程序。
    - 否则会将大量数据从用户设备传输到服务器再传回用户设备的应用程序和外围设备。例如，DVD 刻录机和电视调谐器。

在 Citrix Virtual Apps and Desktops™ 中，托管桌面会话使用 URL 重定向来启动本地应用访问应用程序。URL 重定向使应用程序可以通过多个 URL 地址访问。它通过在桌面会话的浏览器中选择嵌入式链接来启动本地浏览器（基于浏览器的 URL 阻止列表）。如果您导航到阻止列表中不存在的 URL，该 URL 将在桌面会话中再次打开。

URL 重定向仅适用于桌面会话，不适用于应用程序会话。可用于应用程序会话的唯一重定向功能是主机到客户端的内容重定向，这是一种服务器 FTA（文件类型关联）重定向。此 FTA 将某些协议（例如 HTTP、HTTPS、RTSP 或 MMS）重定向到客户端。例如，如果您仅使用 HTTP 打开嵌入式链接，则这些链接将直接通过客户端应用程序打开。不支持 URL 阻止列表或允许列表。

启用本地应用访问后，以本地运行的应用程序、用户托管的应用程序中的链接或桌面快捷方式形式显示给用户的 URL 将通过以下方式之一进行重定向：

- 从用户计算机到托管桌面
- 从 Citrix Virtual Apps and Desktops™ 服务器到用户计算机
- 在它们启动的环境中呈现（未重定向）

要指定来自特定网站内容的重定向路径，请在虚拟投递代理上配置 URL 允许列表和 URL 阻止列表。这些列表包含指定 URL 重定向策略设置的多字符串注册表项。有关详细信息，请参阅本地应用程序访问策略设置。

URL 可以在 VDA 上呈现，但有以下例外情况：

- 地理/区域信息 — 需要区域信息的网站，例如 msn.com 或 news.google.com（根据地理位置打开特定国家/地区的页面）。例如，如果 VDA 是从英国的数据中心预配的，并且客户端从印度连接，则用户期望看到 in.msn.com。但用户看到的却是 uk.msn.com。
- 多媒体内容 — 包含富媒体内容的网站在客户端设备上呈现时，可为最终用户提供原生体验，即使在高延迟网络中也能节省带宽。此功能可重定向包含其他媒体类型（例如 Silverlight）的站点。此过程在安全环境中进行。也就是说，管理员批准的 URL 在客户端上运行，而其余 URL 则重定向到 VDA。

除了 URL 重定向之外，您还可以使用 FTA 重定向。当会话中遇到文件时，FTA 会启动本地应用程序。如果启动了本地应用程序，则该本地应用程序必须有权访问该文件才能将其打开。因此，您只能使用本地应用程序打开位于网络共享或客户端驱动器（使用客户端驱动器映射）上的文件。例如，当打开 PDF 文件时，如果 PDF 阅读器是本地应用程序，则文件将使用该 PDF 阅读器打开。由于本地应用程序可以直接访问文件，因此无需通过 ICA® 进行文件网络传输即可打开文件。

要求、注意事项和限制

我们支持在适用于 Windows 多会话操作系统 VDA 和适用于 Windows 单会话操作系统 VDA 的有效操作系统上使用本地应用程序访问。本地应用程序访问需要 Citrix Workspace app for Windows 4.1 版（最低版本）。支持以下浏览器：

- Edge，最新版本
- Firefox，最新版本和扩展支持版本
- Chrome，最新版本

使用本地应用程序访问和 URL 重定向时，请查看以下注意事项和限制。

- 本地应用程序访问专为跨所有显示器的全屏虚拟桌面而设计：
  - 如果您将本地应用程序访问与在窗口模式下运行或未覆盖所有显示器的虚拟桌面一起使用，用户体验可能会令人困惑。
  - 多显示器 — 当一个显示器最大化时，它将成为在该会话中启动的所有应用程序的默认桌面。即使后续应用程序通常在另一个显示器上启动，也会出现此默认设置。
  - 该功能支持一个 VDA。不支持与多个并发 VDA 集成。

- 某些应用程序可能会出现意外行为，从而影响用户：
  - 驱动器盘符可能会让用户感到困惑，例如本地 C: 盘而不是虚拟桌面 C: 盘。
  - 虚拟桌面中可用的打印机不适用于本地应用程序。
  - 需要提升权限的应用程序不能作为客户端托管应用程序启动。
  - 对于单实例应用程序（例如 Windows Media Player），没有特殊处理。
  - 本地应用程序显示本地计算机的 Windows 主题。
  - 不支持全屏应用程序。这些应用程序包括以全屏模式打开的应用程序，例如 PowerPoint 幻灯片演示或覆盖整个桌面的照片查看器。
  - 本地应用程序访问在 VDA 上复制本地应用程序的属性（例如客户端桌面和“开始”菜单上的快捷方式）。但是，它不复制其他属性，例如快捷键和只读属性。
  - 自定义重叠窗口顺序处理方式的应用程序可能会产生不可预测的结果。例如，某些窗口可能会被隐藏。
  - 不支持快捷方式，包括“我的电脑”、“回收站”、“控制面板”、“网络驱动器”快捷方式和文件夹快捷方式。
  - 不支持以下文件类型和文件：自定义文件类型、没有关联程序的文件、zip 文件和隐藏文件。
  - 对于混合的 32 位和 64 位客户端托管或 VDA 应用程序，不支持任务栏分组。也就是说，不支持将 32 位本地应用程序与 64 位 VDA 应用程序分组。
  - 无法使用 COM 启动应用程序。例如，如果您在 Office 应用程序中单击嵌入的 Office 文档，则无法检测到进程启动，并且本地应用程序集成会失败。
- 不支持双跳场景，即用户在另一个虚拟桌面会话中启动虚拟桌面。
- URL 重定向仅支持显式 URL（即，根据浏览器不同，显示在浏览器地址栏中或通过浏览器内导航找到的 URL）。
- URL 重定向仅适用于桌面会话，不适用于应用程序会话。
- VDA 会话中的本地桌面文件夹不允许用户创建文件。
- 本地运行的应用程序的多个实例的行为方式与为虚拟桌面建立的任务栏设置一致。但是，本地运行的应用程序的快捷方式不会与这些应用程序的运行实例分组。它们也不会与托管应用程序的运行实例或托管应用程序的固定快捷方式分组。用户只能从任务栏关闭本地运行的应用程序窗口。尽管用户可以将本地应用程序窗口固定到桌面任务栏和“开始”菜单，但使用这些快捷方式时，应用程序可能无法一致地启动。
- 如果将**允许本地应用访问**策略设置设为**已启用**，则不支持浏览器内容重定向。默认情况下，本地应用访问是禁止的。

与 Windows 的交互

本地应用程序访问与 Windows 的交互包括以下行为。

- Windows 8 和 Windows Server 2012 快捷方式行为
  - 客户端上安装的 Windows 应用商店应用程序不会作为本地应用程序访问快捷方式的一部分进行枚举。
  - 图像和视频文件默认使用 Windows 应用商店应用程序打开。但是，本地应用程序访问会枚举 Windows 应用商店应用程序并使用桌面应用程序打开快捷方式。
- 本地程序
  - 对于 Windows 7，该文件夹在“开始”菜单中可用。
  - 对于 Windows 8，“本地程序”仅在用户从“开始”屏幕中选择“**所有应用**”作为类别时才可用。“本地程序”中不会显示所有子文件夹。
- 适用于应用程序的 Windows 8 图形功能
  - 桌面应用程序仅限于桌面区域，并由“开始”屏幕和 Windows 8 样式应用程序覆盖。
  - 本地应用访问应用程序在多显示器模式下行为不像桌面应用程序。在多显示器模式下，开始屏幕和桌面显示在不同的显示器上。
- Windows 8 和本地应用访问 URL 重定向
  - 由于 Windows 8 Internet Explorer 未启用任何加载项，请使用桌面版 Internet Explorer 启用 URL 重定向。
  - 在 Windows Server 2012 中，Internet Explorer 默认禁用加载项。要实施 URL 重定向，请禁用 Internet Explorer 增强配置。然后重置 Internet Explorer 选项并重新启动，以确保为标准用户启用加载项。

配置本地应用访问和 URL 重定向

要将本地应用访问和 URL 重定向与 Citrix Workspace™ 应用程序结合使用：

- 在本地客户端计算机上安装 Citrix Workspace 应用程序。您可以在 Citrix Workspace 应用程序安装期间启用这两个功能，也可以使用组策略编辑器启用本地应用访问模板。
- 将**允许本地应用访问**策略设置设为**已启用**。您还可以为 URL 重定向配置 URL 允许列表和阻止列表策略设置。有关详细信息，请参阅本地应用访问策略设置。

启用本地应用访问和 URL 重定向

要针对所有本地应用程序启用本地应用访问，请执行以下步骤：

1. 登录 Web Studio，然后单击左侧窗格中的**策略**。
2. 在操作栏中，单击**创建策略**。
3. 在“创建策略”窗口中，在搜索框中键入“允许本地应用访问”，然后单击**选择**。
4. 在“编辑设置”窗口中，选择“**允许**”。默认情况下，“**允许本地应用访问**”策略是禁止的。当此设置被允许时，VDA 允许最终用户决定是否在会话中启用已发布的应用程序和本地应用访问快捷方式。（当此设置被禁止时，已发布的应用程序和本地应用访问快捷方式均不适用于 VDA。）此策略设置适用于整个计算机和 URL 重定向策略。
5. 在“创建策略”窗口中，在搜索框中键入“URL 重定向允许列表”，然后单击**选择**。URL 重定向允许列表指定要在远程会话的默认浏览器中打开的 URL。
6. 在“编辑设置”窗口中，单击“**添加**”以添加 URL，然后单击“**确定**”。
7. 在“创建策略”窗口中，在搜索框中键入“URL 重定向阻止列表”，然后单击**选择**。URL 重定向阻止列表指定重定向到在端点上运行的默认浏览器的 URL。
8. 在“编辑设置”窗口中，单击“**添加**”以添加 URL，然后单击“**确定**”。
9. 在“设置”页面上，单击“**下一步**”。
10. 在“用户和计算机”页面上，将策略分配给适用的交付组，然后单击“**下一步**”。
11. 在“摘要”页面上，查看设置，然后单击“**完成**”。

要在 Citrix Workspace 应用程序安装期间为所有本地应用程序启用 URL 重定向，请执行以下步骤：

1. 在计算机上为所有用户安装 Citrix Workspace 应用程序时启用 URL 重定向。这样做还会注册 URL 重定向所需的浏览器加载项。
2. 从命令提示符处，运行相应的命令以使用以下选项之一安装 Citrix Workspace 应用程序：
   - 对于 CitrixReceiver.exe，请使用 `/ALLOW_CLIENTHOSTEDAPPSURL=1`。
   - 对于 CitrixReceiverWeb.exe，请使用 `/ALLOW_CLIENTHOSTEDAPPSURL=1`。

使用组策略编辑器启用本地应用程序访问模板

> **注意：**

- 在使用组策略编辑器启用本地应用访问模板之前，请将 receiver.admx/adml 模板文件添加到本地 GPO。
- 仅当将 CitrixBase.admx/CitrixBase.adml 添加到 %systemroot%\policyDefinitions 文件夹时，Windows 版 Citrix Workspace 应用程序模板文件才可在本地 GPO 的**管理模板 > Citrix 组件 > Citrix Workspace** 文件夹中找到。

要使用组策略编辑器启用本地应用程序访问模板，请按照以下步骤操作：

1. 运行 **gpedit.msc**。
2. 转到 **计算机配置 > 管理模板 > 经典管理模板 (ADM) > Citrix 组件 > Citrix Workspace > 用户体验**。
3. 单击 **本地应用程序访问设置**。
4. 选择 **已启用**，然后选择 **允许 URL 重定向**。对于 URL 重定向，请使用本文档后面 *注册浏览器加载项* 部分中描述的命令行注册浏览器加载项。

仅提供对已发布应用程序的访问

您可以使用注册表编辑器或 PowerShell SDK 提供对已发布应用程序的访问。

对于注册表编辑器，请参阅注册表管理的功能列表中的 已发布应用程序的本地应用程序访问。

要使用 PowerShell SDK：

1. 在运行 Delivery Controller™ 的计算机上打开 PowerShell。
2. 输入以下命令：`set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

要在云服务部署中访问**添加本地应用访问应用程序**，请使用 Citrix DaaS 远程 PowerShell SDK。有关详细信息，请参阅 Citrix DaaS 远程 PowerShell SDK。

1. 下载安装程序：

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`

2. 运行以下命令：

   a. `asnp citrix.*`.

   b. `Get-XdAuthentication`

3. 输入以下命令：`set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

完成适用的上述步骤后，请按照以下步骤继续操作。

1. 登录 Web Studio 并在左侧窗格中选择**应用程序**。
2. 在中间上方窗格中，右键单击空白区域，然后从上下文菜单中选择**添加本地应用程序访问应用程序**。您也可以在操作栏中单击**添加本地应用程序访问应用程序**。要在操作栏中显示“添加本地应用程序访问应用程序”选项，请单击**刷新**。
3. 发布本地应用程序访问应用程序。

    - 本地应用程序访问向导将启动并显示“简介”页面，您可以选择在以后启动向导时不再显示此页面。
    - 该向导将引导您完成下面介绍的“组”、“位置”、“标识”、“交付”和“摘要”页面。完成每个页面后，单击“**下一步**”，直到到达“摘要”页面。
    - 在“组”页面上，选择一个或多个要添加新应用程序的交付组，然后单击“**下一步**”。
    - 在“位置”页面上，键入应用程序在用户本地计算机上的完整可执行文件路径，并键入应用程序所在文件夹的路径。Citrix 建议您使用系统环境变量路径；例如，%ProgramFiles(x86)%\Internet Explorer\iexplore.exe。
    - 在“标识”页面上，接受默认值或键入所需信息，然后单击“**下一步**”。
    - 在“交付”页面上，配置此应用程序如何交付给用户，然后单击**下一步**。您可以为所选应用程序指定图标。您还可以指定虚拟桌面上的本地应用程序快捷方式是在“开始”菜单、桌面还是两者上可见。
    - 在“摘要”页面上，查看设置，然后单击“**完成**”以退出本地应用程序访问向导。

注册浏览器加载项

> **注意：**
>
> 当您从命令行使用 /ALLOW_CLIENTHOSTEDAPPSURL=1 选项安装 Citrix Workspace 应用程序时，URL 重定向所需的浏览器加载项会自动注册。

> 您可以使用以下命令注册和注销一个或所有加载项：

- 要在客户端设备上注册加载项：\<*client-installation-folder*>\redirector.exe /reg\<*browser*>
- 要在客户端设备上注销加载项：\<*client-installation-folder*>\redirector.exe /unreg\<*browser*>

- 要在 VDA 上注册加载项：\<*VDAinstallation-folder*>\VDARedirector.exe /reg\<*browser*>
- 要在 VDA 上注销加载项：\<*VDAinstallation-folder*>\VDARedirector.exe /unreg\<*browser*>

其中 \<*browser*> 是 Internet Explorer、Firefox、Chrome 或所有。

例如，以下命令在运行 Citrix Workspace 应用程序的设备上注册 Internet Explorer 加载项。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

以下命令在 Windows 多会话操作系统 VDA 上注册所有加载项。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

跨浏览器 URL 拦截

- 默认情况下，Internet Explorer 会重定向指定的 URL。如果 URL 不在阻止列表中，但浏览器或网站将其重定向到另一个 URL，则最终 URL 不会被重定向。即使它在阻止列表中，也不会被重定向。

要使 URL 重定向正常工作，请在浏览器提示时启用加载项。如果使用 Internet 选项的加载项或提示中的加载项被禁用，则 URL 重定向将无法正常工作。

- Firefox 附加组件始终重定向 URL。

安装附加组件时，Firefox 会提示在新标签页上允许或阻止安装该附加组件。允许该附加组件才能使功能正常工作。

- Chrome 附加组件始终重定向导航到的最终 URL，而不是输入的 URL。

扩展程序已外部安装。禁用扩展程序后，URL 重定向功能在 Chrome 中不起作用。如果在无痕模式下需要 URL 重定向，请在浏览器设置中允许该扩展程序在该模式下运行。

配置注销和断开连接时的本地应用程序行为

> **注意：**
>
> 如果您不按照这些步骤配置设置，则默认情况下，当用户注销或断开与虚拟桌面的连接时，本地应用程序会继续运行。重新连接后，如果本地应用程序在虚拟桌面上可用，则会重新集成。

> 要配置注销和断开连接时的本地应用程序行为，请参阅注册表管理的功能列表中的注销和断开连接时的本地应用程序行为。

打印

有效的打印管理是 Citrix Virtual Apps and Desktops™ (CVAD) 环境中高效 IT 运营的基石。用户需要无缝且可靠地访问打印资源，而管理员则需要强大的工具来配置、管理、保护和排查打印基础架构。

本文档是一份全面的专家级指南，旨在更新现有知识库，并为 IT 管理员提供对 CVAD 打印各个方面的透彻理解。

打印仍然是许多业务工作流程的基本要求。在 Citrix Virtual Apps and Desktops™ (CVAD) 环境中，由于用户会话与物理打印机硬件之间的分离，高效管理从虚拟会话到物理设备的打印请求带来了独特的挑战。

CVAD 提供了一套全面的技术和策略，旨在弥合这一差距，提供灵活性以适应不同的打印机类型、网络条件和用户要求，同时力求实现最佳性能和管理简便性。

Citrix Universal™ 打印驱动程序 (UPD)

> **重要说明：**

> Citrix Virtual Apps and Desktops™ 的第四季度版本中，**通用驱动程序首选项**策略设置的默认顺序将发生更改。新的默认顺序将是：

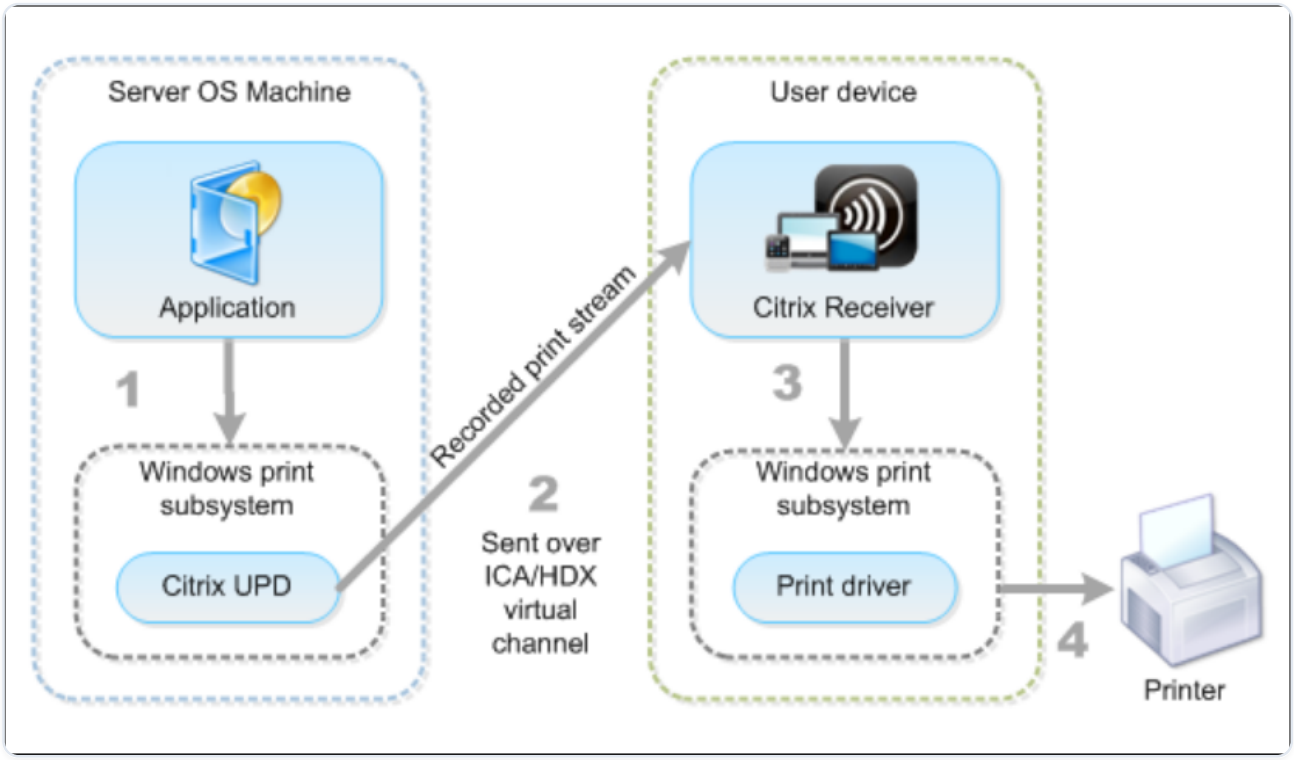
> - EMF
> - XPS
> - 打印机控制语言5c
> - PCL4
> - PDF
> - PS

> 有关更多详细信息，请参阅通用驱动程序首选项页面。

> Citrix Universal Print Driver (UPD) 不是单个驱动程序，而是一种技术，包含服务器 (VDA) 和客户端（带 Workspace 应用程序的端点）上的组件。

- **服务器组件：** 随 VDA 安装，这包括实际的通用打印驱动程序，例如“Citrix Universal Printer”（使用 EMF 格式）和“Citrix XPS Universal Printer”（使用 XPS 格式），以及对 PDF 和 PS 格式的支持。它的作用是以设备无关的格式捕获在 VDA 上运行的应用程序生成的打印输出。
- **客户端组件：** 包含在 Citrix Workspace™ 应用程序安装中，此组件接收从 VDA 发送的打印流。然后，它与端点设备上的本地 Windows 打印子系统交互，使用为目标打印机本地安装的相应设备专用驱动程序来呈现打印作业。

下图显示了通用打印驱动程序组件以及本地连接到设备的打印机的典型工作流程 -



UPD 的主要目标是简化 Citrix® 环境中的打印机驱动程序管理。通过在 VDA 上使用内置驱动程序，管理员可以避免安装和维护数百种不同的制造商专用驱动程序，这些驱动程序是导致不稳定和冲突的常见原因。UPD 旨在与各种打印机兼容，在虚拟会话和客户端的打印功能之间提供通用接口。

支持的格式

UPD 技术支持多种打印数据格式，从而在打印作业的处理和渲染方式上提供了灵活性：

- **EMF（增强型图元文件格式）：** “Citrix Universal Printer”驱动程序使用的默认格式。它是一种 32 位 Windows 原生矢量格式。使用 EMF 打印通常效率很高，但通常需要基于 Windows 的客户端端点进行渲染。

- **XPS（XML 纸张规范）：**“Citrix XPS Universal Printer”驱动程序使用。XPS 是 Microsoft 开发的一种基于 XML 的页面描述语言，概念上类似于 PDF，旨在实现平台独立性。
- **PS (PostScript)：** Adobe 开发的一种页面描述语言，以其处理复杂图形和排版的能力而闻名，常用于出版业以及各种打印机和多功能外设。Linux 客户端通常使用 UPD 进行 PostScript 打印。
- **PDF：** PDF 是一种广泛使用的文档交换开放标准。它封装了固定布局平面文档的完整描述，包括显示文档所需的文本、字体、图形和其他信息。它旨在实现平台独立性，是跨不同系统和应用程序保留文档保真度的理想选择。

使用 UPD 具有以下几个潜在优势：

- **减少驱动程序管理：** 显著减少 VDA 映像所需的驱动程序数量，从而简化映像创建和维护。
- **提高稳定性：** 驱动程序越少，潜在冲突就越少，与驱动程序相关的后台处理程序崩溃或系统不稳定的风险就越低。
- **优化打印作业：** 某些 UPD 格式，尤其是 EMF，有时可以使打印作业大小比原生驱动程序更小。
- **高级功能支持：** 如果客户端上的原生驱动程序通过 Microsoft 的标准打印功能技术公开了这些功能，EMF 和 XPS UPD 组件可以支持高级打印功能（例如装订、纸盘选择）。

PDF 打印

Citrix Virtual Apps and Desktops 通过 Citrix Universal Print Driver (UPD) 支持 PDF 作为自动创建的客户端打印机的页面描述语言 (PDL)。这提供了一个通用的 UPD 解决方案，适用于所有客户端平台（Windows、Mac 和 Linux），使用 PDF 作为 VDA 和客户端端点之间交换的打印格式。

以前，Citrix Universal PDF Printer 作为通用会话级端点运行，不与任何特定的客户端打印机关联。用户会在客户端收到一个 PDF 文件，在本地 PDF 查看器中打开它，并可选择从那里打印。通过增强的 PDF 打印，打印作业直接路由到自动创建的客户端打印机，并且在 VDA 打印对话框中选择的打印票证设置（例如双面打印、方向、颜色模式和装订）会传递到客户端打印机并得到遵守。

PDF 打印

要求

Citrix® 控制平面

- Citrix Virtual Apps and Desktops™ 2402 或更高版本
- 思杰 DaaS

会话主机

- 操作系统
  - Windows 十一
  - Windows Server 2019 或更高版本
- VDA
  - Windows: 2603 或更高版本

客户端

有关详细信息，请参阅通用驱动程序首选项 页面。

- 操作系统
  - Windows 十一
  - 林纳克斯
- Workspace 应用程序
  - Windows: 2603 或更高版本
  - Linux: 2511 或更高版本

配置

可以通过更新 Studio 控制台中**通用驱动程序首选项**策略设置的顺序来启用 PDF 打印，如下所述。

策略	所需值
通用驱动程序首选项	PDF:EMF:XPS:PS

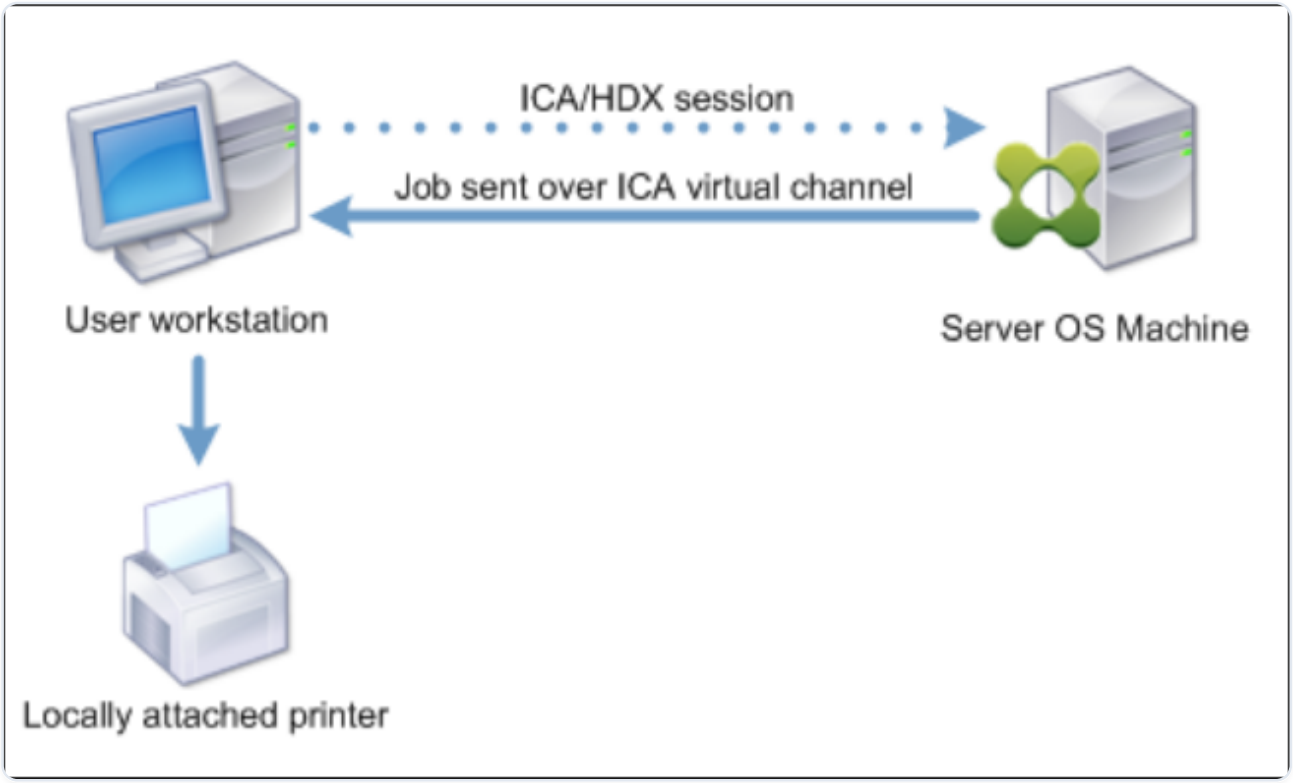
无需进行其他 VDA 侧注册表修改。

> **注意：**
>
> 将 PDF 设置在**通用驱动程序首选项**列表的开头，使其在自动创建的打印机中优先于 PS、EMF 和 XPS。 有关其他详细信息，请参阅通用驱动程序首选项 页面。

配置

客户端打印机重定向

这通常是默认机制，即当用户登录时，在用户端点设备上配置的打印机将自动映射到 Citrix® 会话中。这包括直接连接到客户端的打印机（USB、LPT 等）以及映射到客户端计算机上的网络打印机。最终用户通常无法手动选择要重定向的本地打印机；这由管理策略控制。



设置步骤

此功能默认启用。相关设置和配置可在“客户端打印机”模板中找到。此模板中的策略设置可用于进一步自定义和优化客户端打印重定向体验。

与客户端打印机重定向相关的策略可在客户端打印机策略设置中找到。

注意事项

主要挑战是，如果客户端端点上映射并重定向了大量打印机，可能会导致性能下降和不稳定。此外，由于驱动程序不兼容或客户端问题，可能会发生打印机映射失败。可靠性在很大程度上取决于客户端设备的配置和运行状况。一些管理员倾向于完全避免自动创建客户端打印机，因为这可能会带来潜在的负载和驱动程序管理复杂性。

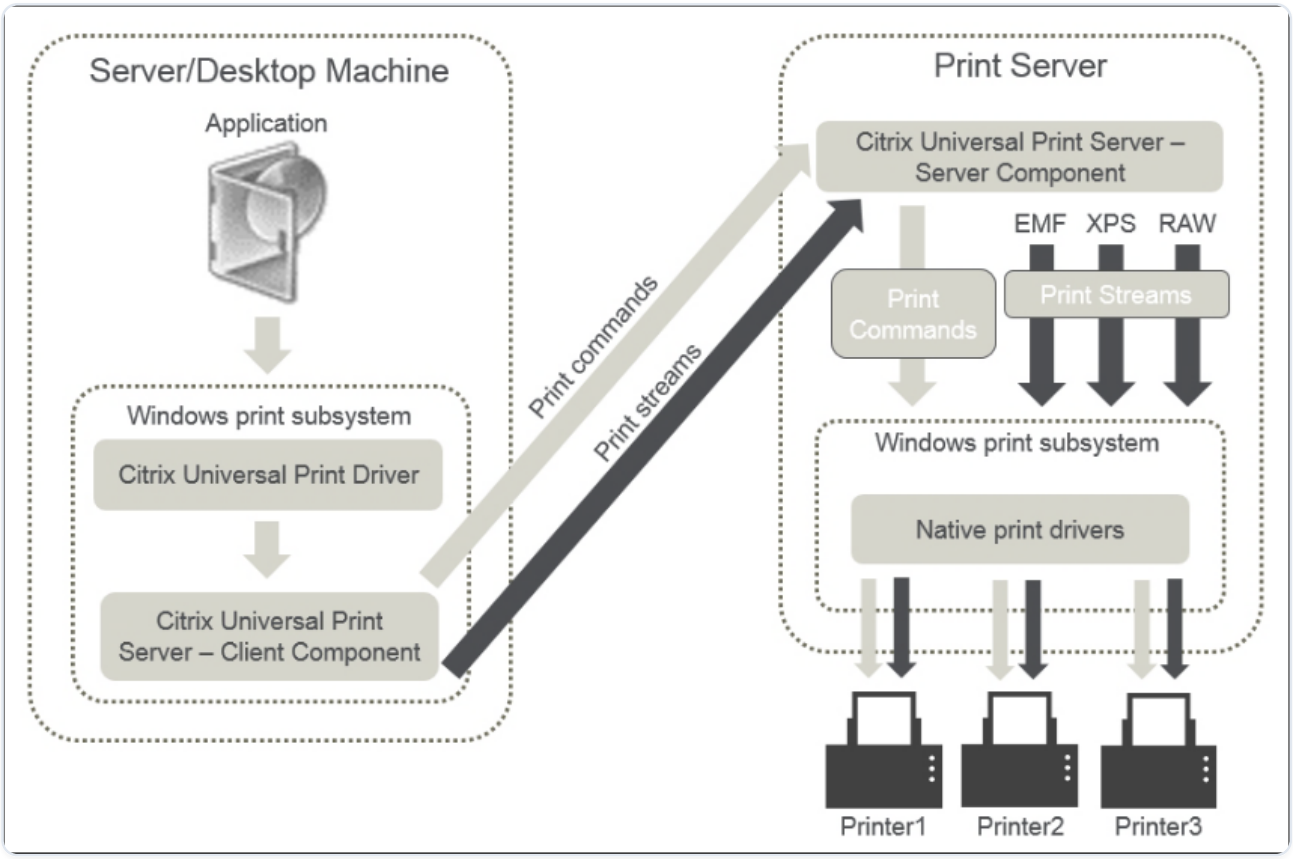
用例

需要访问直接连接到其本地计算机的打印机的用户（USB、LPT、COM、仅映射到客户端的网络打印机）。

Citrix Universal™ 打印服务器 (UPS)

UPS 是一个可选的 Citrix® 组件，旨在优化和管理网络打印。它由两部分组成：

- **UPServer** 组件安装在网络中的一个或多个 Windows 打印服务器上。
- **UPClient** 组件是 VDA 安装的一部分。通过策略启用后，VDA 会与 UPServer 通信以建立与网络打印机的连接，通常利用 Citrix Universal Print Driver (UPD)。



UPS 具有多项优势，尤其适用于跨 WAN 链接或大型环境中的网络打印：

- 网络优化：在 VDA 和 UPServer 之间发送的打印数据经过优化和压缩，减少了带宽消耗，这在 WAN 连接上尤为重要。
- 集中式驱动程序管理：允许将 Citrix UPD 用于网络打印机，从而减少了在 VDA 上安装和管理大量本机打印机驱动程序的需要。
- 高可用性：支持跨多个 UPServer 进行负载平衡，并在服务器不可用时自动进行故障转移。

要求

- Microsoft Visual C++ 2015–2022 可再发行组件
- Microsoft .NET Framework 4.8（至少需要此版本）
- UPServer 的操作系统要求
    - Windows 服务器 2025

- Windows 服务器 2022
- Windows 服务器 2019

配置/设置步骤

此功能默认禁用。相关设置和配置可在“Universal Print Server”模板中找到。此模板中的策略设置可用于进一步自定义和优化 Universal Print Server 体验。

除了启用设置之外，还有一些策略设置可以微调 UPS 行为：

- 通信端口配置（HTTP/SOAP、CGP 及其 SSL/TLS 等效项）。
- 打印流的输入带宽限制。
- 用于负载平衡的 UPS 服务器列表。 故障转移检测的服务中断阈值。
- Web 服务连接超时。
- 用于安全通信的 SSL/TLS 配置设置。

有关详细信息，请参阅Citrix UPS 策略设置。

最佳实践

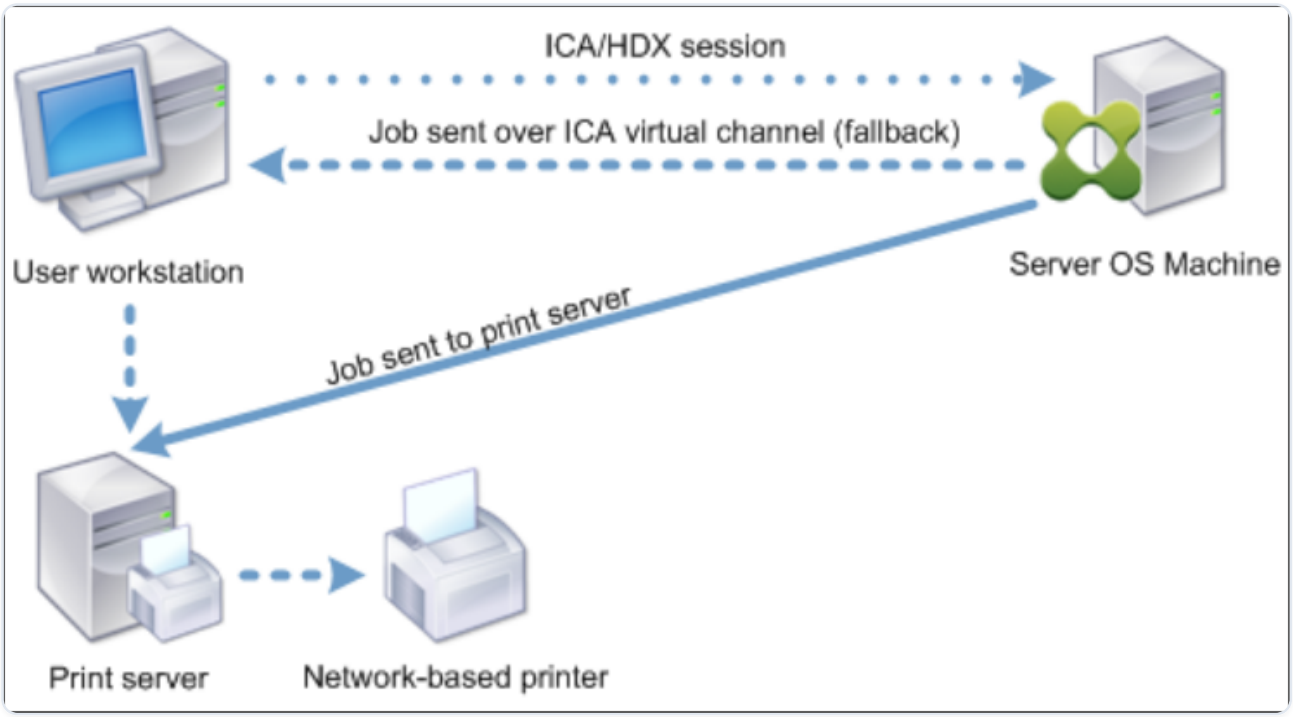
- 通过 WAN 链接使用 UPS 进行网络打印以优化性能。
- 利用 Citrix 通用打印驱动程序 (UPD) 减少 VDA 上的驱动程序管理。
- 配置多个 UPS 服务器之间的负载平衡以实现高可用性。

用例

Citrix 明确建议在涉及 WAN 链接的远程打印服务器场景中使用 UPS。它也适用于旨在最大限度地减少 VDA 驱动程序占用空间、提高网络打印性能、为网络打印提供高可用性或根据网络位置实施近距离打印的环境。无法直接连接到网络打印机的瘦客户端可以通过 VDA 利用 UPS。

网络打印机（在 VDA 上）

在此，打印作业直接从 VDA 经网络发送到网络打印服务器（可以是标准 Windows 打印服务器，也可以是 Citrix Universal™ Print Server）。对于与 VDA 位于同一局域网 (LAN) 中的打印机，此路径通常更快。当启用直接连接时，这是网络打印机的默认路径。如果已发布的应用程序或桌面无法访问打印服务器，或者多会话操作系统计算机上未安装本机打印机驱动程序，则打印作业将回退到通过 ICA 连接进行路由。



要求

- 所需的打印机驱动程序取决于托管网络打印机的打印服务器类型：
  - 如果打印机托管在标准 Windows 打印服务器上，则必须在 VDA 上安装相应的本机打印机驱动程序。
  - 如果打印机托管在 Citrix Universal Print Server (UPS) 上，则连接可以使用本机驱动程序或 Citrix UPD。
- 从 VDA 到打印服务器的网络连接。
- 适用于已登录用户的适当权限。

连接和配置网络打印机的指南（策略设置）

- 通过 UNC 路径连接打印机（例如，“\\PrintServer\PrinterName”）
- **会话打印机：** 这是此方法的主要策略。管理员可以通过键入 UNC 路径或浏览网络来添加打印机。可以将筛选器应用于策略，以定位特定用户、组、客户端 IP 等。
- **打印机分配：** 一种替代策略，可用于同时将大量打印机分配给多个用户或设备。它允许为这些分配设置会话打印机和默认打印机。

最佳实践（允许直接连接到网络打印机）

- 考虑“直接连接到网络打印机”策略用于路由（直接 VDA 到服务器或通过客户端/ICA）。
  - 启用时（默认设置），局域网上的打印性能将达到最佳。在此场景中，打印流量未压缩。

- 如果 VDA 和打印服务器不在同一网络中（WAN 场景），请禁用此策略设置。这将强制打印流量通过客户端端点并利用 ICA® 压缩，但会引入延迟。

启用直接连接有利于 LAN 性能，但会在 VDA 和打印服务器之间使用未压缩的网络流量。禁用它会强制流量通过客户端路径，利用 ICA 压缩，这对于 WAN 场景有利，但会增加延迟。

用例

直接从虚拟会话访问共享部门或办公室打印机。需要在 VDA 上安装本机驱动程序。

限制

在不利的网络条件（WAN）下，打印性能会很差。此外，驱动程序管理对 IT 管理员来说是一个巨大的开销。

故障排除

系统方法

在复杂的 Citrix Virtual Apps and Desktops™ (CVAD) 环境中排查打印问题需要系统的方法，而不是随意猜测。建议的流程包括：

1. **识别症状：** 明确定义问题（例如，打印机未显示、作业卡住、输出错误、打印缓慢）。
2. **隔离范围：** 确定受影响的人员（一个用户、多个用户、特定应用程序）、涉及的打印机以及问题发生的 VDA 或客户端设备。
3. **检查基本项：** 验证网络连接（VDA 到打印服务器，客户端到 VDA），确保打印机在线且在 Citrix® 外部正常工作，检查客户端的本地打印（针对重定向问题）。
4. **审查策略：** 使用 Citrix 组策略建模向导等工具或通过检查 VDA 上应用的策略设置，检查应用于受影响用户/会话的相关 Citrix 策略设置。确保策略设置按预期配置，并且没有明显的冲突。
5. **检查日志：** 检查 VDA、客户端设备和打印服务器（如果适用）上的 Windows 事件日志（应用程序和系统日志、PrintService 日志）。如果已启用，请检查 Citrix 特定日志。3
6. **测试组件：** 尝试将问题隔离到特定组件 – 尝试从不同的应用程序打印，尝试不同的打印机，使用通用驱动程序（如 UPD 或 Microsoft XPS Document Writer）进行测试，检查打印后台处理程序和 Citrix Print Manager 服务的状态。
7. **查阅资源：** 利用产品文档、支持文章和社区论坛查找已知问题和解决方案。

常见问题和解决方案

下面记录了一些现场报告的常见打印问题和建议的故障排除步骤：

- **无法自动创建打印机/打印机未在会话中显示：**
  - **潜在原因：** 客户端打印机重定向策略已禁用；自动创建客户端打印机策略设置为“无”或筛选不正确；客户端设备打印后台处理程序问题；Workspace 应用程序问题；客户端与 VDA 之间的网络连接问题；Citrix Print Manager Service (CpSvc.exe) 未运行或在 VDA 上崩溃；VDA 上缺少所需的打印机驱动程序（如果需要本机驱动程序）；Citrix 策略未正确应用于会话。
  - **故障排除步骤：**
    a. 验证客户端打印机重定向策略是否为“允许”，并且“自动创建客户端打印机”是否为用户/会话正确配置。
    b. 检查 VDA 上的 CpSvc.exe 服务状态；如有必要，请重新启动。
    c. 检查 VDA 和客户端上的 Windows 打印后台处理程序服务状态；如有必要，请重新启动。
    d. 验证基本网络连接。
    e. 在客户端设备上本地测试打印。
    f. 确保安装了兼容的 Workspace 应用程序版本。
    g. 检查 VDA 事件日志中与 CpSvc 或打印机创建相关的错误。
    h. 在 VDA 上强制更新策略 (gpupdate /force)。
    i. 检查 VDA 上应用的策略，确认存在预期设置。
    j. 如果预期使用本机驱动程序，请验证它们是否已安装在 VDA 上。
    k. 检查 VDA 上本地/组策略中的 RDS/终端服务器打印机重定向设置。
    l. 查找并清理 VDA 注册表中的孤立打印机条目。
- **打印后台处理程序崩溃/服务无响应（在 VDA 或打印服务器上）：**
  - **潜在原因：** 有缺陷或不兼容的打印机驱动程序（通常是第三方）；队列中损坏的打印作业；驱动程序冲突；系统资源不足。
  - **故障排除步骤：**
    a. 使用 Windows 事件日志（应用程序日志通常显示后台处理程序崩溃）识别故障进程/模块。
    b. 尝试重新启动打印后台处理程序服务。
    c. 如果重新启动失败或问题再次出现，尝试手动清除打印队列（停止后台处理程序服务，删除 C:\Windows\System32\spool\PRINTERS 中的文件，启动后台处理程序服务）。

d. 识别并删除有问题的打印机驱动程序。彻底删除可能需要编辑注册表。

e. 使用 Citrix UPD 或通用 Microsoft 驱动程序进行测试。

f. 检查并清理注册表中的孤立打印处理器。

- **策略冲突 / 设置被忽略：**
  - **潜在原因：**GPO 设置覆盖 Citrix 策略；Citrix 策略优先级或筛选器冲突；策略处理期间出错。
  - **故障排除步骤：**

    a. 使用 Citrix 组策略建模向导模拟针对受影响的用户/VDA 的策略应用。

    b. 验证策略筛选器（用户组、客户端 IP 等）是否正确。

    c. 检查 Studio/Web Studio 中的策略优先级。

    d. 暂时阻止 VDA 的 OU 上的 GPO 继承，以隔离 Citrix 策略问题。

    e. 检查 VDA 上的策略处理结果（例如，使用 gpresult /h report.html）。

    f. 简化应用于用户/VDA 的策略集，并逐步重新添加策略以找出冲突。

- **驱动程序问题（常规 - 兼容性、损坏、映射）：**
  - **潜在原因：** 驱动程序与 VDA 操作系统或 Citrix 版本不兼容；驱动程序安装损坏；VDA 上缺少策略要求的驱动程序；多个驱动程序之间存在冲突；打印机驱动程序映射策略配置不正确。
  - **故障排除步骤：**

    a. 尝试使用 Citrix UPD 打印（配置通用打印驱动程序使用策略）。

    b. 根据应用的策略验证是否选择了正确的驱动程序（本机或 UPD）。

    c. 确保所需的本机驱动程序已正确安装在 VDA 上（如果使用）。

    d. 查阅供应商文档，了解驱动程序与 CVAD 和 VDA 操作系统版本的兼容性。

    e. 对有问题的驱动程序执行干净的重新安装（卸载、重启、安装）。

    f. 仔细审查并测试打印机驱动程序映射策略规则。

    g. 最大限度地减少 VDA 上安装的驱动程序数量。

- **打印速度慢/性能问题：**
  - **潜在原因：** 网络拥堵或高延迟（尤其是广域网）；大型、复杂的打印作业（例如，高分辨率图形）；低效的打印机驱动程序；打印优化（压缩、缓存）被禁用或配置错误；低效的路由（例如，通过慢速广域网直接连接）。

- **故障排除步骤：**

  a. 分析 VDA、客户端和打印服务器之间的网络路径和性能。

  b. 配置 Citrix 打印带宽限制策略。

  c. 通过通用打印策略启用并配置 UPD 优化（图像压缩、字体/图像缓存）。

  d. 对于 WAN 链接，禁用“直接连接到打印服务器”策略，以强制流量通过压缩的 ICA® 通道。

  e. 如果使用 UPS，请确保其已针对网络进行优化配置。

  f. 分析打印作业本身 – 如果可能，降低分辨率或复杂性。

  g. 使用不同的驱动程序进行测试（例如，UPD 与本机驱动程序）。

- **输出不正确（字符缺失、格式错误、方向错误）：**

  - **潜在原因：** 文档/应用程序所需的 VDA 上缺少字体；字体替换不正确；打印机驱动程序不兼容；特定 UPD 格式问题（例如，EMF 与 XPS）；应用程序错误；与本地客户端打印机上启用的高级打印功能冲突。
  - **故障排除步骤：**

    a. 确保 VDA 上安装了所有必需的字体。

    b. 尝试更改通用驱动程序首选项策略顺序（例如，先尝试 XPS，再尝试 EMF）。

    c. 尝试从不同的应用程序打印同一文档。

    d. 尝试打印到不同的物理打印机或虚拟打印机（例如，Microsoft XPS Document Writer）。

    e. 尝试使用不同的打印机驱动程序（UPD 与本机驱动程序，或不同的本机版本）。

    f. 检查应用程序的打印设置和页面设置。

    g. 在客户端设备的本地打印机属性中禁用“高级打印功能”。

    h. 验证用户首选项和策略中的打印方向设置。

- **Citrix 打印管理器服务 (CpSvc.exe) 崩溃/挂起：**

  - **潜在原因：** 无响应的打印机驱动程序在注册表中留下孤立对象；与打印相关的 Citrix 策略数据损坏；系统资源争用。
  - **故障排除步骤：**

    a. 按照步骤清理 VDA 注册表中孤立的打印机和打印处理器条目。首先需要停止打印后台处理程序和 CpSvc 服务。

b. 识别并删除有问题的打印机驱动程序。

c. 考虑清理 VDA 上的 Citrix 策略缓存文件夹/注册表项并强制刷新策略。

d. 监控 VDA 资源使用情况（CPU、内存）。

e. 重新启动 CpSvc 和打印后台处理程序服务。

- **PDF 打印机问题：**
  - **潜在原因：** 自动创建 PDF 通用打印机策略已禁用；VDA 或 Workspace 应用程序版本不兼容；客户端端点上未安装 PDF 查看器；使用了不受支持的浏览器（例如 Edge）或 HTML5 配置错误（CSP 标头、config.js）。
  - **故障排除步骤：**

    a. 验证自动创建 PDF 通用打印机策略已启用并已应用。

    b. 确认 VDA 和 Workspace 应用程序满足最低版本要求。

    c. 确保客户端上安装了受支持的 PDF 查看器（例如 Adobe Reader、Chrome）并将其设置为默认值。

    d. 如果使用 HTML5 Workspace 应用程序，请验证浏览器兼容性并检查 configuration.js 和 CSP 标头设置。

    e. 在策略更改后重新启动 Citrix 会话。

基本最终用户故障排除

如果组织策略允许，遇到简单打印问题的用户有时可以通过基本步骤自行解决，然后再上报给 IT 部门 -

- 完全注销 HDX™ 会话并重新登录。
- 检查端点设备上本地打印机的状态（确保其在线、未暂停、无错误）。
- 重新启动本地端点设备。

最佳实践

- **利用通用打印服务器 (UPS)：** 建议使用，尤其适用于跨 WAN 的网络打印，因为它具有优化和集中管理优势。
- **采用通用打印驱动程序 (UPD)：** 使用 UPD 作为主要驱动程序策略，以最大程度地减少驱动程序数量和冲突。
- **选择性使用经过审查的本机驱动程序：** 如果特定打印机功能需要本机驱动程序，请确保对其进行彻底测试。

- **最小化驱动程序占用空间：** 在 VDA 映像上安装最少数量的打印机驱动程序。
- **利用驱动程序映射：** 使用打印机驱动程序映射和兼容性策略来替换有问题的驱动程序或强制使用 UPD。
- **严格测试：** 切勿将未经测试的驱动程序部署到生产环境。
- **谨慎管理驱动程序更新：** 避免就地更新；首选干净卸载、重新启动和重新安装过程。
- **清理未使用的驱动程序：** 定期删除不再需要的驱动程序。
- **优化路由：** 确保打印作业采用最有效的路径（例如，通过启用直接连接到打印服务器，在 LAN 上实现 VDA 到打印服务器的直接连接；通过禁用直接连接，通过 ICA/客户端在 WAN 上进行路由）。
- **考虑分布式打印服务器：** 对于没有 UPS 的大型、地理分散的组织，在每个物理位置放置打印服务器有助于管理和负载分配（尽管带有负载平衡的 UPS 提供了更集成的 Citrix® 解决方案）。
- **清除旧打印作业：** 定期从打印队列中清除卡住或旧的作业。

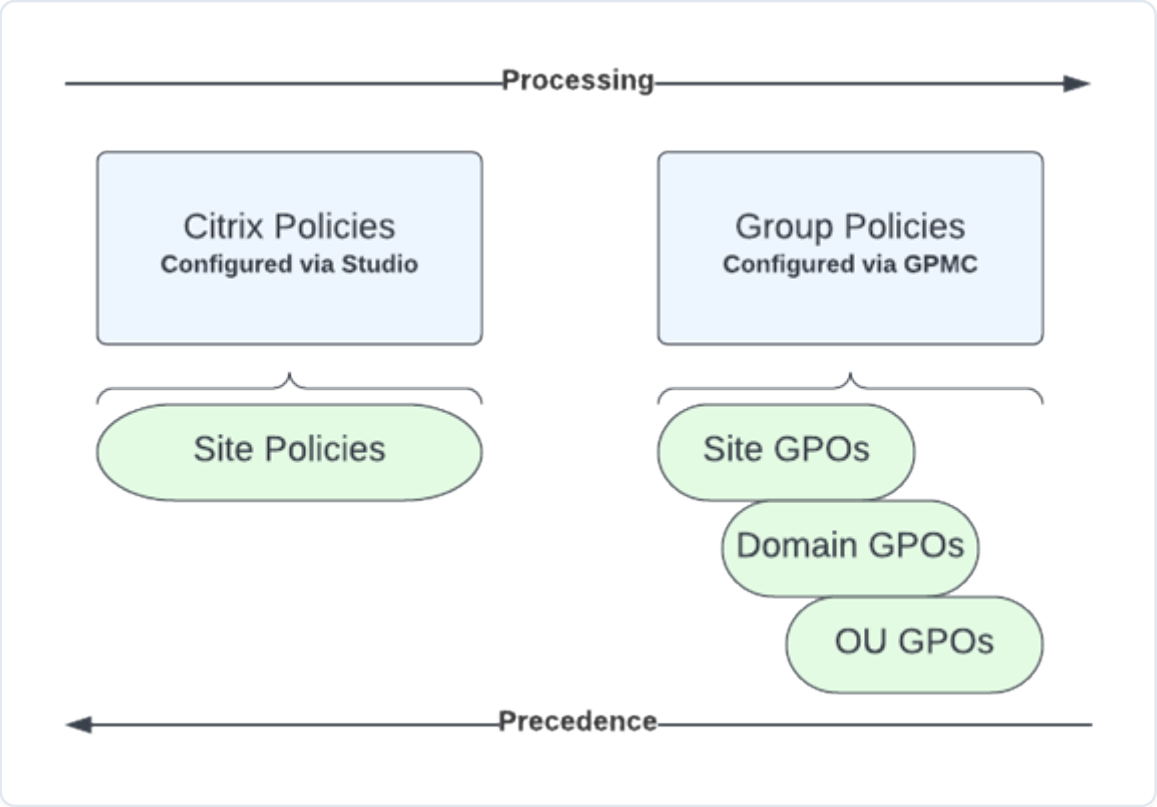
设计注意事项

- **定制预配：** 根据用户要求选择预配方法（自动创建、会话打印机、UPS、PDF 打印机）（例如，漫游用户受益于邻近打印或 PDF 打印；静态工作站可能使用会话打印机）。
- **规划路由：** 根据端点、VDA 和打印服务器的网络位置设计打印作业路由。
- **确保冗余：** 通过负载平衡策略实现打印服务器冗余，尤其是在使用 UPS 时。

策略

策略是设置的集合，用于定义如何管理一组用户、设备或连接类型的会话、带宽和安全性。

您可以将策略设置应用于物理机和虚拟机或用户。您可以在本地级别或 Active Directory 中的安全组中将设置应用于单个用户。这些配置定义了特定的条件和规则。如果您未明确分配策略，则这些设置将应用于所有连接。



您可以在网络的不同级别应用策略。放置在组织单位 GPO 级别的策略设置在网络上具有最高优先级。域 GPO 级别的策略会覆盖站点组策略对象级别的策略。站点组策略对象级别会覆盖 Microsoft 和 Citrix 本地策略级别上的任何冲突策略。

所有 Citrix 本地策略都在 Web Studio 控制台中创建和管理，并存储在站点数据库中。组策略使用 Microsoft 组策略管理控制台 (GPMC) 创建和管理，并存储在 Active Directory 中。Microsoft 本地策略在 Windows 操作系统中创建并存储在注册表中。

Studio 使用建模向导帮助管理员比较模板和策略中的配置设置，以帮助消除冲突和冗余设置。管理员可以使用 GPMC 设置 GPO 来配置设置。此外，还可以将它们应用于网络不同级别的目标用户集。

这些 GPO 存储在 Active Directory 中。出于安全考虑，大多数 IT 人员对这些设置的管理访问权限受到限制。

设置根据优先级及其条件进行合并。任何禁用的设置都会覆盖排名较低的已启用设置。未配置的策略设置将被忽略，并且不会覆盖排名较低的设置。

本地策略也可能与 Active Directory 中的组策略发生冲突，这些策略可能会根据情况相互覆盖。

所有策略按以下顺序处理：

1. 最终用户使用域凭据登录到计算机。
2. 凭据发送到域控制器。
3. Active Directory 应用所有策略（最终用户、端点、组织单位和域）。
4. 最终用户登录到 Citrix Workspace™ 应用程序并访问应用程序或桌面。
5. Citrix 和 Microsoft 策略针对最终用户和托管资源的计算机进行处理。
6. Active Directory 确定策略设置的优先级。然后，它将这些设置应用于端点设备的注册表和托管资源的计算机。
7. 最终用户从资源注销。最终用户和端点设备的 Citrix 策略不再处于活动状态。
8. 最终用户从用户设备注销，这将释放 GPO 用户策略。
9. 最终用户关闭设备，这将释放 GPO 计算机策略。

为用户、设备和计算机组创建策略时，某些成员可能具有不同的要求，并且需要对某些策略设置进行例外处理。例外情况通过 Studio 和 GPMC 中的筛选器进行设置，这些筛选器确定策略影响的对象。

> **注意：**
>
> 我们不支持在同一个 GPO 中混合使用 Windows 和 Citrix 策略。

概述

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio™（基于 Web）是 Citrix Virtual Apps and Desktops™ 唯一的管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web

> Studio。有关 Citrix® Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

> 策略是设置的集合，用于定义如何管理一组用户、设备或连接类型的会话、带宽和安全性。Citrix® 策略提供了一种集中管理这些方面的高效方式。每个策略都可以包含根据您的环境量身定制的多个设置和筛选器（对象分配）。

策略管理工具

- Web 工作室

  使用 Web Studio 创建的策略存储在站点数据库中，并在发生以下任一情况时将更新推送到 VDA：

  - 当该 VDA 向代理注册时
  - 当用户启动会话时

- 组策略管理控制台 (GPMC)

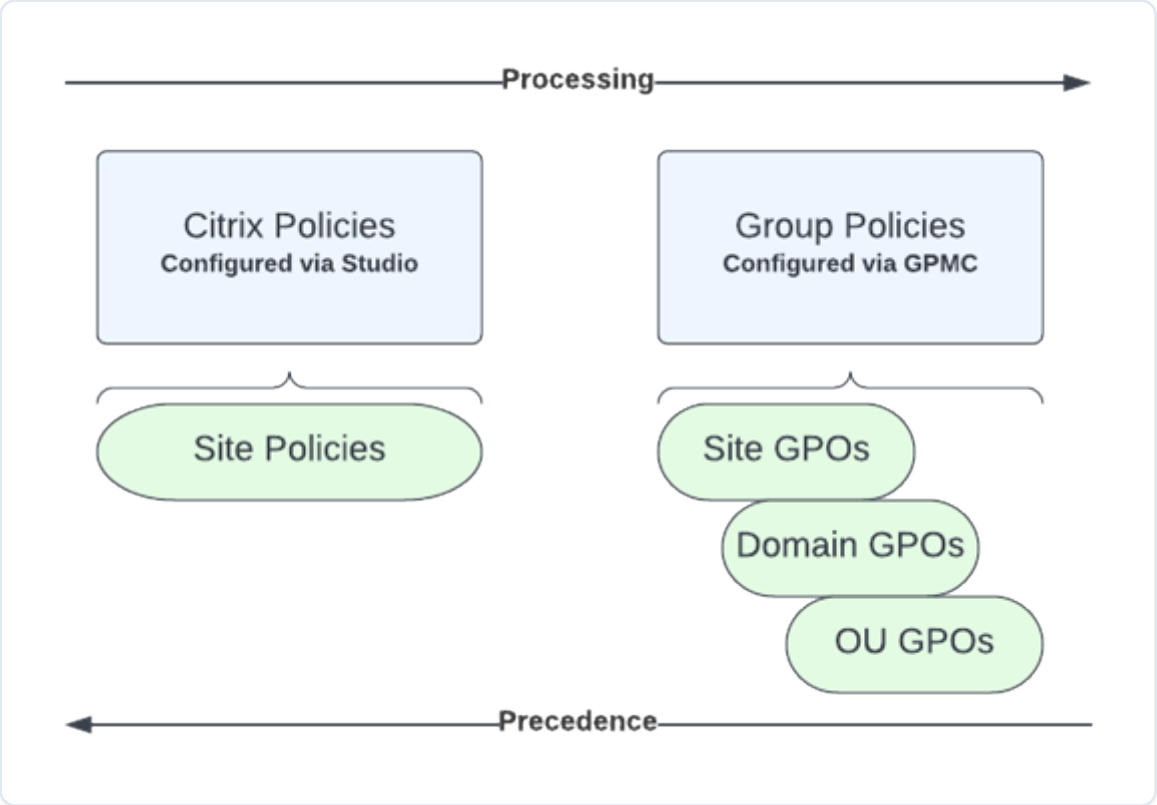
  如果您的网络环境使用 Active Directory 并且您有权管理组策略，您可以使用 GPMC 创建和编辑策略。

  在 GPMC 中，您可以使用所需的设置和筛选器配置组策略对象 (GPO)。这些策略优先于在 Web Studio 中配置的策略。有关详细信息，请参阅 CTX238166。

策略处理顺序

组策略设置按以下顺序处理：

1. 站点级 GPO（存储在站点数据库中）
2. 域级 GPO
3. 组织单位 (OU) GPO



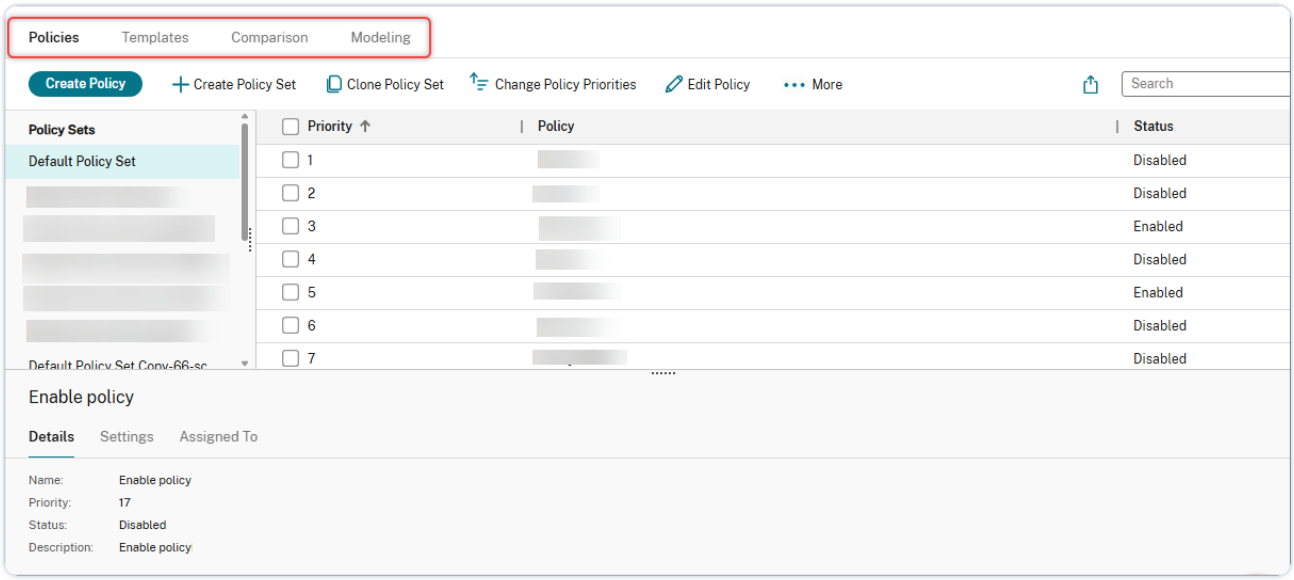
如果在两个 GPO 中为同一策略应用了不同的设置，则最后处理的策略设置会覆盖之前处理的设置。此配置意味着策略设置按以下顺序优先：

1. OU GPO（最高优先级）
2. 域级 GPO
3. 站点级 GPO（最低优先级）

如果您使用具有冲突设置的多个策略，可以通过分配策略优先级来控制优先级。有关详细信息，请参阅 管理策略分配例外。

了解 Web Studio > 策略界面

要访问策略、设置或模板，请登录 Web Studio 并在左侧窗格中选择“**策略**”。



- **策略**选项卡允许您创建和管理策略集和策略。从策略集中选择策略时，将显示以下选项卡：
  - **概述** – 显示策略名称、优先级、状态和描述。
  - **设置** – 列出所有已配置的设置。
  - **分配给** – 显示已分配的交付组。您可以编辑或删除分配。策略根据运行会话的桌面的交付组应用。有关详细信息，请参阅创建策略。
- **模板**选项卡允许您创建策略模板以及管理 Citrix 提供的模板和自定义模板。选择模板时，将显示以下选项卡：
  - **描述** – 解释模板的用途。
  - **设置** – 列出已配置的设置。有关详细信息，请参阅 创建模板。
- **比较**选项卡允许您将策略或模板中的设置与其他设置进行比较。使用此功能检查合规性或差异。有关详细信息，请参阅 比较策略和模板。
- **建模**选项卡允许您模拟连接场景并查看有效的策略结果。有关详细信息，请参阅 模拟和评估策略。

策略配置工作流

要使用 Web Studio 配置 Citrix 策略，请遵循以下工作流程：

1. 创建策略。
   a. 配置策略设置。

      添加和配置您的环境所需的设置。

   b. 分配策略。

将策略分配给相应的计算机和用户对象。

2. 设置策略优先级。

   按优先级顺序排列策略，以确定哪些设置优先。

3. 验证有效策略。

   使用策略建模向导确认已应用的设置。

创建模板

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio™（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

模板为创建策略提供了预定义起点。我们提供针对特定环境和网络条件优化的内置模板。您可以使用这些模板来：

- 创建您自己的策略和模板，以便在各个站点之间共享。
- 在跨部署比较时进行参考。例如，“...使用 Citrix 模板 X 或 Y 时...”.
- 通过导入或导出模板，与 Citrix 支持部门或受信任的第三方沟通策略配置。

内置模板

提供以下内置模板：

- **超高清用户体验**。此模板强制实施可最大程度提高用户体验的默认设置。在按优先级顺序处理多个策略的场景中使用此模板。
- **高服务器可扩展性**。应用此模板可节省服务器资源。此模板平衡了用户体验和服务器可扩展性。它在提供良好用户体验的同时，增加了可在单个服务器上托管的用户数量。此模板不使用视频编解码器进行图形压缩，并阻止服务器端多媒体呈现。
- **高服务器可扩展性 - 旧版操作系统**。此高服务器可扩展性模板仅适用于运行 Windows Server 2008 R2 或 Windows 7 及更早版本的 VDA。此模板依赖于旧版图形模式，该模式对于这些操作系统更高效。

- **针对 NetScaler SD-WAN 优化**。为使用 NetScaler SD-WAN 优化 Citrix Virtual Desktops 交付的分支机构用户应用此模板。（NetScaler SD-WAN 是 CloudBridge 的新名称）。
- **针对 WAN 优化**。此模板适用于分支机构中通过共享 WAN 或低带宽连接的远程位置工作的任务型员工。这些员工访问具有图形简单用户界面和少量多媒体内容的应用程序。此模板以牺牲视频播放体验和部分服务器可扩展性为代价，以优化带宽效率。
- **针对 WAN 优化 - 旧版操作系统**。此模板仅适用于运行 Windows Server 2008 R2 或 Windows 7 及更早版本的 VDA。此模板依赖于旧版图形模式，该模式对于这些操作系统更高效。
- **安全和控制**。在风险容忍度低的环境中使用此模板，以最大程度地减少 Citrix Virtual Apps and Desktops™ 中默认启用的功能。此模板包含禁用以下各项访问的设置：
  - 打印
  - 剪贴板
  - 外围设备
  - 驱动器映射
  - 端口重定向
  - 用户设备上的 Flash 加速

  应用此模板可能会占用更多带宽并降低每台服务器的用户密度。

尽管我们建议使用内置模板中的默认设置，但某些设置（例如 **WAN 模板**中的**会话总带宽限制**）未配置，以允许管理员进行特定于部署的调整。

模板默认设置图像(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/template-default-settings.png)

假设您正在使用早于 XenApp 和 XenDesktop 7.6 FP3 的部署（策略管理和 VDA）。此外，还需要高服务器可扩展性和针对 WAN 模板进行优化。在这种情况下，请在适用时使用这些模板的旧版操作系统版本。

> **注意：**
>
> 我们创建并更新内置模板。您无法修改或删除这些模板。

创建模板

要从模板创建模板：

1. 在 Web Studio 中，选择左侧窗格中的**策略**。
2. 选择“**模板**”选项卡，然后选择要从中创建模板的模板。
3. 选择“**创建模板**”选项卡。此时将显示“**选择设置**”屏幕。
4. 选择并配置要包含在模板中的策略设置。
5. 单击**下一步**。将显示**摘要**屏幕。
6. 输入模板名称。
7. 单击“**完成**”。新模板将显示在“**模板**”选项卡上

要基于策略创建模板：

1. 在 Web Studio 中，选择左侧窗格中的**策略**。
2. 在**策略**选项卡上，选择要从中创建模板的策略。
3. 单击**更多**选项卡。
4. 选择**另存为模板**。将显示**选择设置**屏幕。
5. 选择并配置要包含在模板中的任何新策略设置。
6. 单击**下一步**。将显示**摘要**屏幕。
7. 输入模板的名称和描述，然后单击**完成**。

创建策略

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio™（基于 Web）是 Citrix Virtual Apps and Desktops™ 唯一的管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

> 策略定义了两个部分：

- 一组设置，用于定义如何为一组用户、设备或连接类型管理会话、带宽和安全性。
- 要分配策略的用户和计算机。在创建策略之前，请确定它影响哪些用户组或设备。您可能希望根据工作职能、连接类型、设备平台或地理位置创建策略。

创建策略时，您可以基于策略模板中的设置并根据需要对其进行自定义。您也可以从头开始，手动添加必要的设置。本节涵盖以下主题：

- 策略的工作原理
- 从头开始创建策略
- 从模板创建策略

> **提示**
>
> 如果某个组已存在策略，请考虑编辑现有策略，而不是创建新策略。避免仅为了启用特定设置或排除特定用户而创建策略。

策略的工作原理

当用户登录时，将识别所有与连接分配匹配的策略。这些策略按优先级排序，并比较任何设置的多个实例。对于每个设置，将应用优先级最高的策略中的值。如果优先级较高的策略禁用某个设置，则该设置将覆盖任何已启用该设置的优先级较低的策略。未配置的设置将被忽略。

> **重要提示：**
>
> 如果您使用组策略管理控制台同时配置 Active Directory 和 Citrix 策略，则分配和设置可能无法按预期应用。有关详细信息，请参阅 CTX127461。

未筛选的策略

我们提供一个名为 **Unfiltered** 的默认策略。

- 在 Web Studio 中管理 Citrix® 策略时，Unfiltered 策略中的设置将应用于站点中的所有服务器、桌面和连接。
- 要使设置生效，站点和连接必须在包含该策略的 GPO 范围内。

  示例：名为 **Sales-US** 的 GPO 链接到 **Sales** OU，并包含所有美国销售团队成员。此 GPO 配置了一个包含多个用户设置的 **Unfiltered** 策略。当销售经理登录时，**Unfiltered** 策略设置将应用，因为该用户位于 **Sales-US** GPO 中。

分配模式

分配模式控制策略是否根据连接条件匹配情况应用。

- **允许**（默认）：仅当连接与分配条件匹配时才应用策略。
- **拒绝**：如果连接不符合条件，则应用策略。

示例 1：相同的分配类型，不同的模式

策略 1 包括：

- 分配 A：销售组，模式 = 允许
- 分配 B：销售经理帐户，模式 = 拒绝

尽管用户在销售组中，但拒绝分配优先。当销售经理登录时，策略不适用。

示例 2：不同的分配类型，相同的模式

策略 2 包括：

- 分配 C: 销售组 (用户), 模式 = 允许
- 分配 D: 公司 IP 范围 (客户端 IP), 模式 = 允许

仅当两个分配都满足时，策略才适用。如果销售经理从办公室登录，则两个条件都满足，策略将适用。

策略 3 包括：

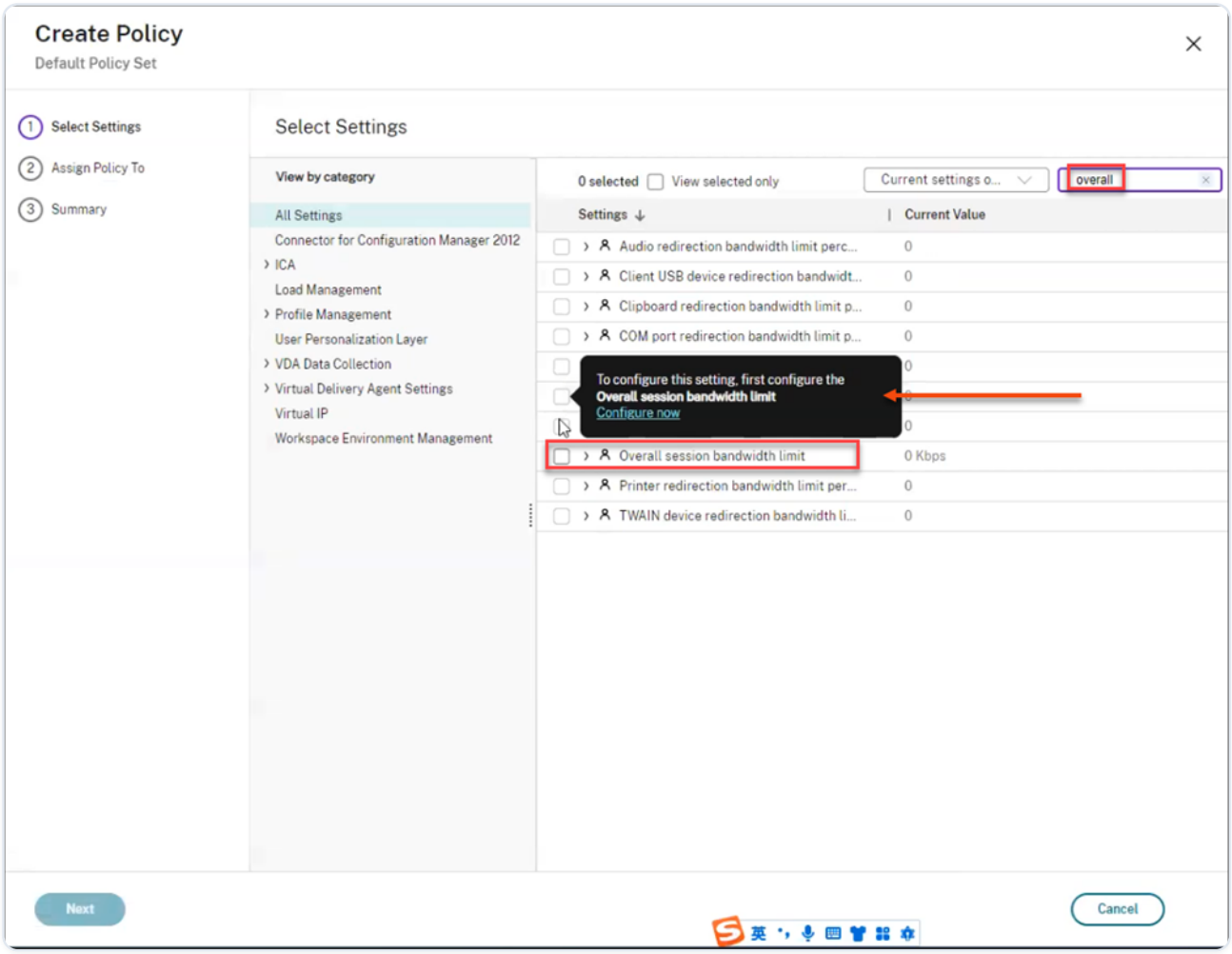
- 分配 E: 销售组 (用户), 模式 = 允许
- 分配 F: NetScaler Gateway 连接 (访问控制), 模式 = 允许

如果销售经理从办公室登录（而不是通过 NetScaler），则分配 F 不满足，因此策略不适用。

策略设置：父子关系

某些策略设置取决于父设置。例如，您必须先配置**总体会话带宽限制**，然后其子设置才能可用。

在 Web Studio 中配置策略时，将鼠标悬停在子设置上可查看必须首先配置哪个父设置。如果父设置被禁用，则相关的子设置将自动禁用。



下表列出了父设置及其对应的子设置：

父策略	依赖子策略
总体会话带宽限制	音频重定向带宽限制百分比
	剪贴板重定向带宽限制百分比
	COM 端口重定向带宽限制百分比
	文件重定向带宽限制百分比
	HDX™ MediaStream 多媒体加速带宽限制百分比
	LPT 端口重定向带宽限制百分比
	打印机重定向带宽限制百分比
	客户端 USB 设备重定向带宽限制百分比

父策略	依赖子策略
	TWAIN 设备重定向带宽限制百分比
允许双向内容重定向	允许重定向到客户端的 URL
	允许重定向到 VDA 的 URL
CPU 使用率	CPU 使用率排除进程优先级
旧版图形模式	渐进式压缩级别
启用会话水印	水印自定义文本
	会话水印样式
	水印透明度
HDX 自适应传输	音频的容错模式

策略设置状态

某些策略设置可以具有以下状态之一：

- **允许**或**禁止**：允许或阻止由设置控制的操作。有时，允许或阻止用户在会话中管理设置的操作。例如，如果菜单动画设置为“允许”，则用户可以在其会话中控制它。
- **已启用**或**已禁用**：打开或关闭设置。如果设置在优先级较高的策略中被禁用，则即使在优先级较低的策略中启用，也不会应用该设置。

安全默认设置

如果在 VDA 安装期间启用了安全默认设置，则策略设置的优先级如下：

1. 自定义设置
2. 安全默认设置
3. 默认设置

要查看安全默认值，请执行以下操作：

1. 在 Web Studio 中，单击左侧窗格中的**策略**。
2. 在**策略**选项卡上，单击**创建策略**。
3. 在**选择设置**表中，当您将鼠标悬停在当前值为**允许**的设置上时，会显示**安全默认值：禁止**。

安全默认设置(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/secure-default-setting.png)

策略设置的有效性

某些设置必须一起使用和启用。例如，要允许用户访问其本地设备上的网络驱动器：

- **客户端驱动器重定向**必须启用
- **客户端网络驱动器**也必须包含在内

如果**客户端驱动器重定向**被禁用，即使**客户端网络驱动器**已启用，用户也无法访问网络驱动器。

通常，与计算机相关的设置更改在 VDA 重启或用户登录时生效。与用户相关的设置更改在下次登录时应用。

将设置添加到策略时，您可以选择“使用默认值”以防止更改。此选项会禁用手动配置，并且仅应用默认值，无论之前输入的值是什么。

最佳实践

- 将策略分配给组而不是单个用户。如果您将策略分配给组，则在您从组中添加或删除用户时，分配会自动更新。
- 禁用未使用的策略。未添加任何设置的策略会产生不必要的处理开销。

从头开始创建策略

要创建策略：

1. 在 Web Studio 中，单击左侧窗格中的**策略**。
2. 在“**策略**”选项卡上，单击“**创建策略**”。
3. 在“**选择设置**”页面上，(#step-1-select-and-configure-policy-settings)，然后单击“**下一步**”。
4. 在“**将策略分配到**”页面上，选择此策略所在的策略集，然后(#step-2-specify-policy-assignments)。单击“**下一步**”。
5. 在“**摘要**”页面上，完成以下设置：
    a. 输入策略的名称和描述。
    b. 要启用策略，请选择“**启用策略**”。
6. 单击“**完成**”。

步骤 1：选择和配置策略设置

策略设置按功能分组。例如，与配置文件管理相关的设置位于“**配置文件管理**”类别下。

设置分为两种类型：

- **计算机设置**：应用于计算机并在虚拟桌面启动时生效（即使没有用户登录）。它们定义虚拟桌面行为。
- **用户设置**：在用户连接或重新连接时应用。它们定义用户体验。

要选择和配置设置：

1. 在“**选择设置**”页面上，要按 VDA 版本查看设置，请从右上角的下拉列表选项中选择以下选项之一：
   - **所有设置**：查看所有 VDA 版本的全部设置
   - **仅当前设置**：仅查看当前 VDA 版本的设置
   - **仅旧版设置**：仅查看已弃用 VDA 版本的设置
2. 要搜索设置，请在搜索框中输入设置的完整或部分名称。
3. 选择一个设置。单击**启用**以将其打开，或单击**编辑**以指定值。
4. 重复步骤 3 以选择和配置策略的更多设置。

> **注意：**
>
> 策略设置可以为“已启用”、“已禁用”或“未配置”。默认情况下，策略设置未配置，这意味着它们未添加到策略中。设置仅在添加到策略后才应用。

步骤 2：指定策略分配

策略分配定义策略适用于哪些用户和计算机。有关分配如何影响策略行为的信息，请参阅策略工作原理。

要指定策略分配：

1. 在**将策略分配给**页面上，选择**筛选的用户和计算机**。
2. 通过指定分配（也称为*筛选器*）来选择用户或计算机。有关可用分配类型，请参阅下表。

> **注意：**
>
> - 如果您未指定任何分配或将其禁用，则策略将应用于**所有**连接。

- 策略*分配*也称为策略*筛选器*。有关详细信息，请参阅创建、修改或删除策略的筛选器和筛选器如何应用？

分配类型	描述	
访问控制	客户端连接的访问控制条件： • **连接类型**：是否将策略应用于通过或不通过 NetScaler® Gateway 建立的连接。*NetScaler Gateway 场名称* - NetScaler Gateway 虚拟服务器的名称。*访问条件* - 要使用的端点分析策略或会话策略的名称。 • **NetScaler Gateway 场名称**：NetScaler Gateway 虚拟服务器的名称。*访问条件* - 要使用的端点分析策略或会话策略的名称。 • **访问条件**：要使用的端点分析策略或会话策略的名称。	
Citrix SD-WAN™	用户会话是否通过 Citrix SD-WAN 启动。**注意：** 您只能向策略添加一个 Citrix SD-WAN 分配。	

分配类型	描述
客户端 IP 地址	用于连接会话的用户设备的 IP 地址：IPv4 示例：12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24；IPv6 示例：2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
客户端名称	用户设备的名称。精确匹配：ClientABCName。使用通配符：Client*Name。
客户端平台	用于连接会话的用户设备的操作系统类型，例如 Windows、Linux、iOS、Android 或 HTML5。所需 VDA 版本：2503 或更高版本。
交付组	交付组成员身份。
交付组类型	桌面或应用程序的类型：专用桌面、共享桌面、专用应用程序或共享应用程序。
组织单位 (OU)	组织单位。
标签	标签。**注意：** 将此策略应用于所有已标记的计算机。不包括应用程序标签。
用户或组	用户或组名称。支持的用户和组身份类型包括 Active Directory、Microsoft Entra ID、Okta 和 Google Cloud。所需 VDA 版本：2507 或更高版本。

从模板创建策略

您可以基于 Citrix 提供的或自定义模板 创建策略。生成的策略独立于原始模板。

要从模板创建策略，请执行以下操作：

1. 在 Web Studio 中，选择左侧窗格中的**策略**。
2. 选择 **模板** 选项卡，然后选择要使用的模板。
3. 在操作栏中单击 **从模板创建策略**。将显示 **创建策略** 页面，其中显示所选模板中预配置的所有设置。
4. 根据需要修改设置并添加更多设置，然后单击 **下一步**。
5. 在 **将策略分配到** 页面上，选择此策略所在的策略集，然后选择要分配策略的对象。单击 **下一步**。
6. 在 **摘要** 页面上，输入策略的名称和描述。
7. 单击 **完成**。新策略将显示在 **策略** 选项卡上指定的策略集中。

下一步操作

- 确定策略优先级
- 模拟和评估策略

创建策略集

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio™（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

> 策略集是 Citrix Virtual Apps and Desktops™ 中的对象，它们聚合策略以实现简化的基于角色的访问和轻松管理。创建后，范围和交付组将分配给策略集，以便只有授权管理员才能管理适用于其相关用户和计算机的策略。

策略集通过将 Citrix® 策略组织成逻辑组来帮助您更有效地管理它们。当您将策略集分配给交付组时，交付组将仅使用该策略集中的策略。

本节介绍策略集的行为方式、如何创建和分配它们以及它们如何与范围和筛选器交互。

优势

策略集提供以下几个主要优势：

- 针对分布式管理员团队的基于角色的访问控制
- 简化的兼并、收购和整合
- 有限的故障域
- 对策略的多租户支持

下表比较了有无策略集时策略的工作方式：

无策略集	有策略集
所有策略、设置、筛选器（分配）和优先级都在一个中心位置进行管理。	每个策略集都有自己的设置、筛选器（分配）和优先级。
如果您管理一个策略，则必须管理所有策略。	完全管理员可以将管理特定策略集的能力单独委派给低级别管理员。
在大型和分布式环境中，策略变得复杂且难以管理。	在大型和分布式环境中，策略可以轻松地划分和管理。

工作原理

策略集分配给交付组并限定于特定管理员。集中的策略继续使用筛选器（分配）来确定它们适用于哪些用户或计算机。

主要行为：

- 策略集分配给交付组
  - 一个交付组一次只能使用一个策略集。
  - 一个策略集可以分配给多个交付组。
  - 如果交付组未分配策略集，它将使用**默认策略集**。
- 策略上的筛选器仍然适用，无论策略是否在集中。
- 一个策略集可以有一个或多个作用域。
  - 作用域表示管理员可以管理的对象集合（例如，连接、目录、交付组和应用程序组）。

  - 作为管理员，您可以定义策略集的作用域，以便只有授权管理员才能查看或编辑它。您可以在创建策略集时或稍后编辑该集时设置作用域。

- **默认策略集**默认情况下已选中**绕过此资源的作用域控制**。此设置可确保所有管理员都能看到该策略集。要应用作用域控制，请编辑策略集，清除**绕过此资源的作用域控制**复选框，然后选择所需的作用域。

策略筛选器和分配其工作方式与没有策略集时相同。有关详细信息，请参阅筛选器如何应用。

启用策略集

在 Web Studio 中，转到**设置 > 站点设置**，然后打开**策略集**设置。

> **注意：**
>
> - 在创建策略集之前，必须启用策略集。
> - 启用策略集后，所有现有策略都将分组到**默认策略集**中。除非您分配了不同的策略集，否则此策略集会自动分配给所有交付组。将新的策略集分配给交付组后，该组将停止使用默认策略集。

创建策略集

您可以创建策略集以反映管理员团队和公司中的逻辑划分。例如，您可以为每个地理区域、业务部门或特定用例创建策略集。

您可以通过两种方式创建策略集：

- 从头开始创建策略集
- 通过复制现有策略集来创建策略集

或者，您可以使用 Citrix Virtual Apps and Desktops PowerShell SDK 来创建和管理策略集。

从头开始创建策略集

1. 在 Web Studio 中，选择左侧窗格中的**策略**节点。
2. 单击**策略**选项卡。
3. 选择**创建策略集**。
4. 单击**名称和描述**选项卡，然后输入策略集的名称和描述。
5. 点击“**分配**”选项卡，并选择一个或多个交付组。

6. 点击“**作用域**”选项卡，并选择定义策略集可应用于的对象的范围。
7. 点击“**创建**”完成。

克隆策略集

1. 在 Web Studio 中，在左侧窗格中选择“**策略**”节点。
2. 点击“**策略**”选项卡。
3. 选择“**克隆策略集**”。
4. 更新策略集的名称。
5. 更新或创建策略集的分配，然后点击“**下一步**”。
6. 选择或清除要包含在克隆策略集中的策略。
7. 更新策略的作用域。
8. 单击**创建**。

优先处理策略

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio™（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

> 当多个策略应用于一个连接时，Citrix Virtual Apps and Desktops™ 会按优先级顺序评估它们。数字越小表示优先级越高（1 为最高）。当策略之间存在冲突设置时，最高优先级策略的设置将生效。

您可以使用 Web Studio 或 PowerShell 更改策略优先级。

使用 Web Studio 更改策略优先级

1. 在 **Web Studio** 中，选择左侧窗格中的**策略**。
2. 在**策略**选项卡上，从操作栏中选择**更改策略优先级**。
3. 在**更改策略优先级**页面上，使用以下任一方法重新排序策略：
   - 将策略拖动到所需位置。

- 单击**向上**或**向下**箭头图标将其移动一个位置。
- 单击**顶部**或**底部**箭头图标将其移动到第一个或最后一个位置。
- 单击**编辑**图标，输入优先级编号，然后单击**保存**。

4. 单击**保存**以应用更改。

使用 PowerShell 更改策略优先级

使用 `Set-GpoPolicyPriority.ps1` 脚本以编程方式重新排序策略优先级。该脚本接受策略名称和目标优先级编号，在内部解析策略 GUID，并使用 `Set-BrokerGpoPolicyPriorities` 应用更新后的顺序。当您通过自动化而不是 Web Studio 控制台管理策略优先级时，请使用此方法。

本机 `Set-BrokerGpoPolicyPriorities` cmdlet 需要策略 GUID 的完整有序列表。此脚本通过接受策略名称和所需优先级，然后自动处理 GUID 解析来消除这种复杂性。

开始之前

运行脚本前，请确保满足以下要求：

- 已安装 Broker SDK 的受支持版本的 Citrix Virtual Apps and Desktops
- 脚本必须在安装了 Citrix Broker SDK 的 Delivery Controller™ 上运行
- PowerShell 管理单元：`Citrix.Broker.Admin.V2`（由脚本自动加载）

运行脚本

1. 将 `Set-GpoPolicyPriority.ps1` 复制到 Delivery Controller。
2. 在 Delivery Controller 上打开 PowerShell 会话。
3. 使用所需参数运行脚本。

```
.\Set-GpoPolicyPriority.ps1 -PolicyName "<PolicyName>" -NewPriority
<Number>
```

将 `<PolicyName>` 替换为策略名称，将 `<Number>` 替换为目标优先级。

脚本会输出当前优先级和目标优先级，确认更改，并运行验证步骤。添加 `-Verbose` 可在脚本应用重新排序之前查看详细信息。

参数

参数	必需	描述
`-PolicyName`	是	要重新确定优先级的策略名称
`-NewPriority`	是	目标优先级（1 = 最高）。使用 0 或负数将策略移动到最高位置；使用超出策略计数的数字将其移动到最低位置
`-PolicySetGuid`	否	特定策略集的 GUID。省略以定位 `DefaultSitePolicies`

示例

将默认策略集中的策略设置为最高优先级：

```
.\Set-GpoPolicyPriority.ps1 -PolicyName "MyPolicy" -NewPriority 1
```

将策略设置为最低优先级：

```
.\Set-GpoPolicyPriority.ps1 -PolicyName "MyPolicy" -NewPriority 9999
```

将特定策略集中的策略设置为优先级 5：

```
.\Set-GpoPolicyPriority.ps1 -PolicyName "MyPolicy" -NewPriority 5
-PolicySetGuid "12345678-1234-1234-1234-123456789012"
```

管理策略分配例外

注意：

从版本 2511 开始，Citrix Web Studio™（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

> 当您使用筛选器将策略分配给用户组、用户设备或计算机时，组中的某些成员可能需要不同的设置。您无需为每个个体创建完全独立的策略即可处理这些情况。

您可以通过以下方式为组中的特定用户或计算机创建例外：

- 仅为这些组成员创建单独的策略并赋予其更高的优先级
- 对添加到策略的分配使用 *拒绝* 模式

对例外使用拒绝模式

将模式设置为 *拒绝* 的分配意味着该策略适用于不符合分配条件的连接。例如，策略包含以下分配：

- *分配 A*：客户端 IP 地址分配范围 `208.77.88.*`，模式 = *允许*。
- *分配 B*：特定用户帐户，模式 = *拒绝*。

此策略适用于从指定 IP 范围连接的用户，**除了** *分配 B* 中定义的用户。

> **注意：**

> 在“**分配策略**”步骤中，如果清除“**启用**”复选框，则分配将被禁用。如果策略没有启用的分配，则它将应用于站点中的所有对象。

相关内容

- 确定策略优先级
- 模拟和评估策略

模拟和评估策略

> **注意：**

> 从版本 2511 开始，Citrix Web Studio™（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

使用 Web Studio 中的比较和策略建模工具来验证配置、测试策略行为并评估在部署之前应用了哪些设置。

注意：

- “**建模**”选项卡仅在客户请求启用后才可用。
- 仅对启用了筛选器的策略进行建模。禁用的策略永不应用；未启用筛选器的策略始终应用。

比较策略和模板

使用 Web Studio 中的比较功能查看策略、模板或默认设置之间的差异。这有助于您验证配置一致性、保持符合最佳实践并排查意外行为。

您可以：

- 比较策略或模板的设置
- 将设置与默认值进行比较
- 识别策略之间冲突或缺失的配置

要比较策略和模板：

1. 在 Web Studio 中，选择左侧窗格中的**策略**。
2. 单击“**比较**”选项卡，然后单击“**选择**”。
3. 选择要比较的策略或模板。
4. （可选）选择“**与默认设置比较**”以包括默认值。
5. 单击“**比较**”。设置将显示在列中。
    - 要查看所有设置，请选择“**显示所有设置**”。
    - 要返回默认视图，请选择 **显示常用设置**。

运行策略建模向导

1. 在 Web Studio 中，选择 **策略**。
2. 选择 **建模** 选项卡。
3. 在操作栏中选择 **策略建模**。

4. 阅读 **简介** 页面，然后单击 **下一步**。
5. 选择用户或计算机。您还可以浏览容器或特定用户或计算机。单击 **下一步**。
6. 选择您的筛选证据。您可以选择通过指定详细信息（例如 **交付组**、**标记** 和 **客户端 IP 地址**）来优化模拟。单击 **下一步**。
7. 查看摘要，然后单击 **运行**。

查看和管理建模结果

向导运行后，它会生成一份报告，您可以查看、处理和导出该报告。

查看报告

- 使用下拉菜单查看 **所有设置**、**计算机设置** 或 **用户设置**。
- 搜索特定设置。
- 单击某个设置以查看其应用或未应用的原因。
- 以 JSON 或 HTML 格式导出结果。

管理报告

模拟运行后，操作栏中提供以下选项：

选项	描述
查看建模报告	查看或导出结果。
重新运行策略建模	使用相同条件再次运行。
删除建模报告	删除当前报告。

使用策略的结果集评估策略应用

如果连接未按预期运行，则可能是策略冲突所致。优先级较高的策略可以覆盖其他策略。使用策略的结果集 (RSoP) 评估哪些设置适用于给定连接。

有两种 RSoP 方法可用：

- **Citrix 组策略建模向导**

  通过指定用户和分配条件来模拟连接场景。

- **组策略结果**

生成应用于用户和虚拟投递代理 (VDA) 的 Citrix 策略报告。

> **注意：**
>
> 当您从组策略管理控制台 (GPMC) 运行 Citrix 组策略建模向导时，在 **Web Studio** 中创建的站点策略设置不包含在策略的结果集中。为了获得最全面的结果，请从 **Web Studio** 启动策略建模向导，除非您仅使用 GPMC 创建策略。

排查策略问题

用户、IP 地址和其他分配的对象可以同时应用多个策略，这可能导致意外行为。

如果您运行策略建模向导，但没有策略应用于用户连接，则可能是因为：

- 没有策略的分配与评估条件匹配。
- 与分配匹配的策略未配置任何设置。
- 与分配匹配的策略已禁用。

要解决这些问题，请执行以下操作：

- 启用相关策略。
- 为每个策略配置至少一个设置。

> **注意：**
>
> 在双跳场景中 (例如，单会话操作系统 VDA 连接到多会话操作系统 VDA)，Citrix 策略将单会话操作系统 VDA 视为用户设备。为第二跳缓存的映像应用于第一跳计算机。

在 Director 中查看已应用的策略

非管理员可以使用 **Director** 查看应用于用户会话的策略。这有助于验证哪些策略设置正在生效，而无需访问 Web Studio。

将旧版 MMC 组策略模板迁移到 Web Studio

> **注意：**

> 从版本 2511 开始，Citrix Web Studio™（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

> 旧版 MMC Studio 组策略模板存储在运行 MMC Studio 的本地计算机上的管理员用户配置文件中。Web Studio 模板存储在站点数据库中，所有管理员都可以从任何计算机访问。由于这两种格式之间不存在直接的导出或导入路径，因此请使用策略作为中介来迁移旧版模板。

开始之前

- 确保您可以访问存储旧版模板的 MMC Studio 安装。
- 确保 Web Studio 可以访问相同的 Citrix Virtual Apps and Desktops™ 站点。
- 记下旧版模板中的设置，以便在迁移后进行验证。

迁移模板

1. 在 MMC Studio 中，导航到要迁移的模板。
2. 在“**操作**”窗格中，选择“**从模板创建策略**”。
3. 按照向导创建策略。为方便起见，请使用与模板相同的名称。
4. 最多等待 5 分钟，策略才会显示在 Web Studio 中。此时间是站点服务将策略数据从 MMC 格式转换为 Web Studio 格式所需的。
5. 打开 Web Studio 并在左侧窗格中选择“**策略**”。
6. 确认策略在策略列表中可见。
7. 选择策略，然后在功能区中选择“**... 更多**”，然后单击“**另存为模板**”。
8. 按照向导创建 Web Studio 模板。

迁移后，模板将存储在站点数据库中，并且所有从任何计算机使用 Web Studio 的管理员都可以访问该模板。

验证迁移

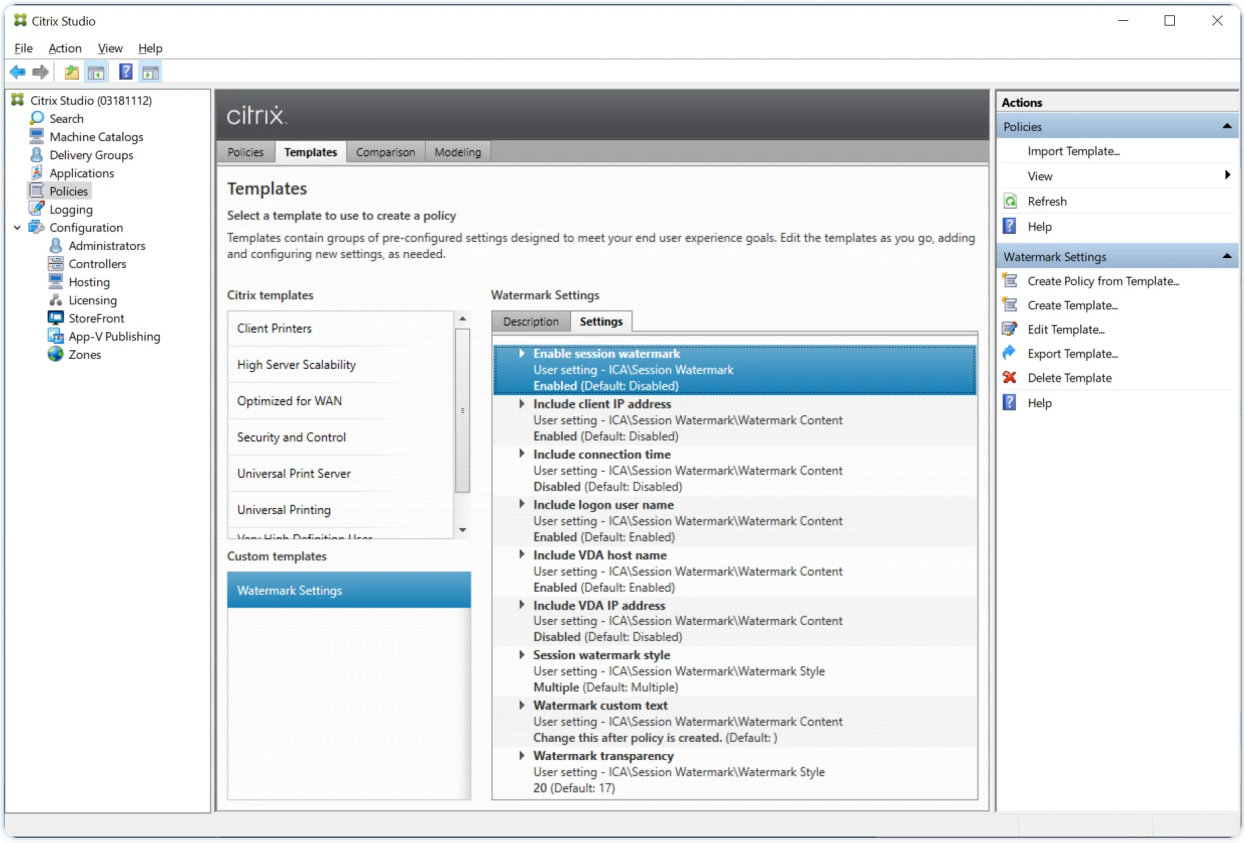
1. 在 Web Studio 中，选择“**策略**”节点中的“**模板**”选项卡。
2. 确认已迁移的模板可见。
3. 将设置与原始 MMC 模板进行比较，以确认它们匹配。

验证迁移后，可以停用原始 MMC 模板。MMC 模板仍保留在创建它的计算机本地。

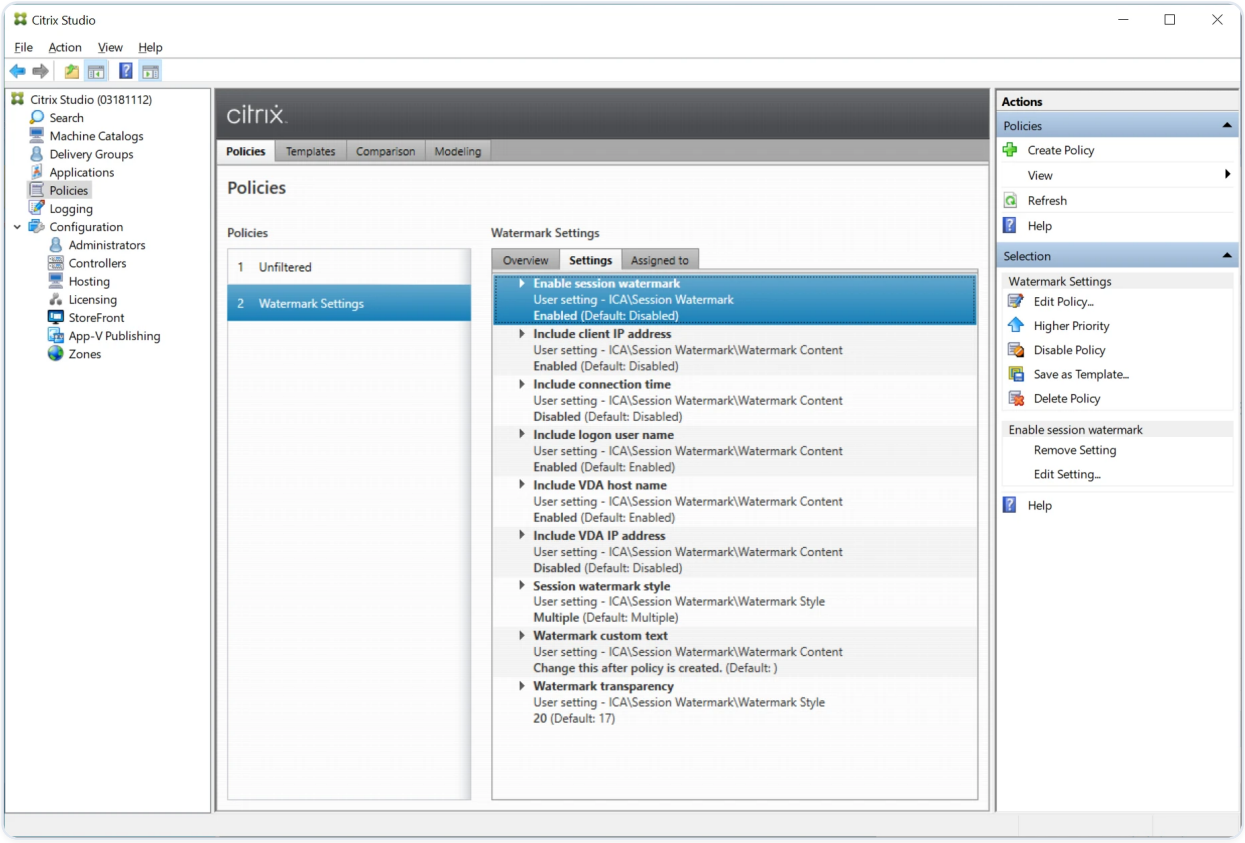
示例

以下示例演示如何迁移名为 *Watermark Settings* 的模板，该模板包含跨多个站点共享的水印配置。

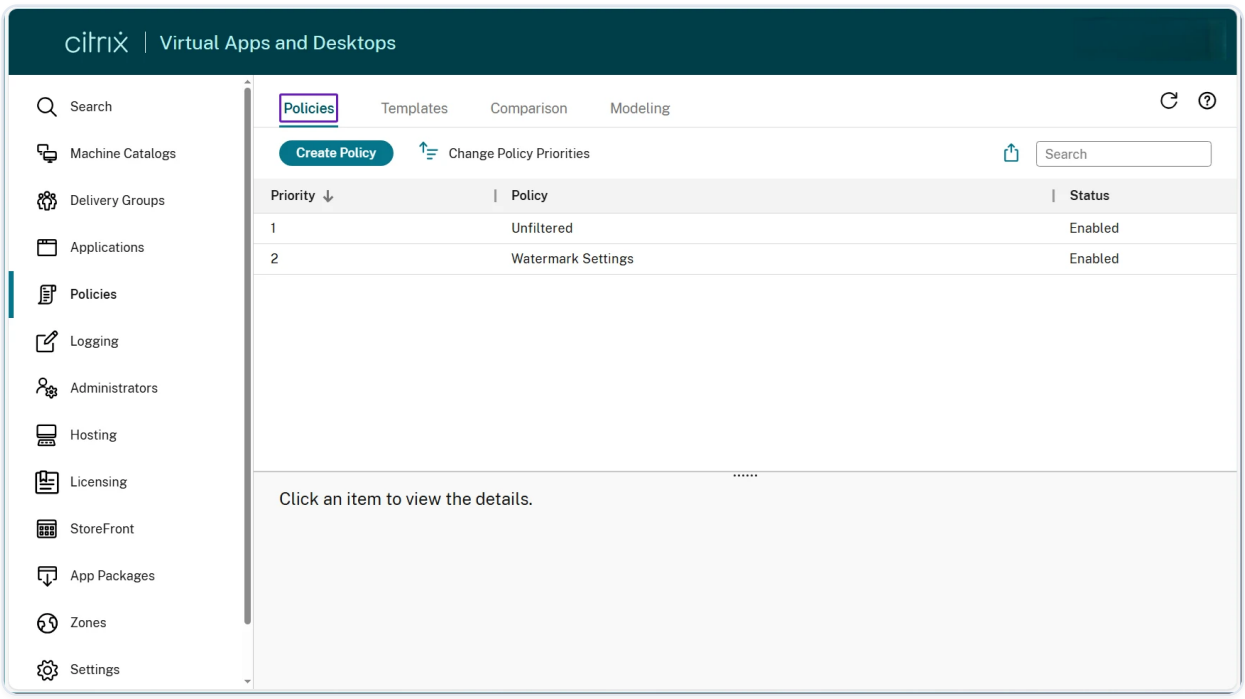
1. 在 MMC Studio 中，找到 *Watermark Settings* 模板。在“**操作**”窗格中，单击“**从模板创建策略**”。



2. 按照向导创建策略。为方便起见，将策略命名为 *Watermark Settings* 以与模板匹配。



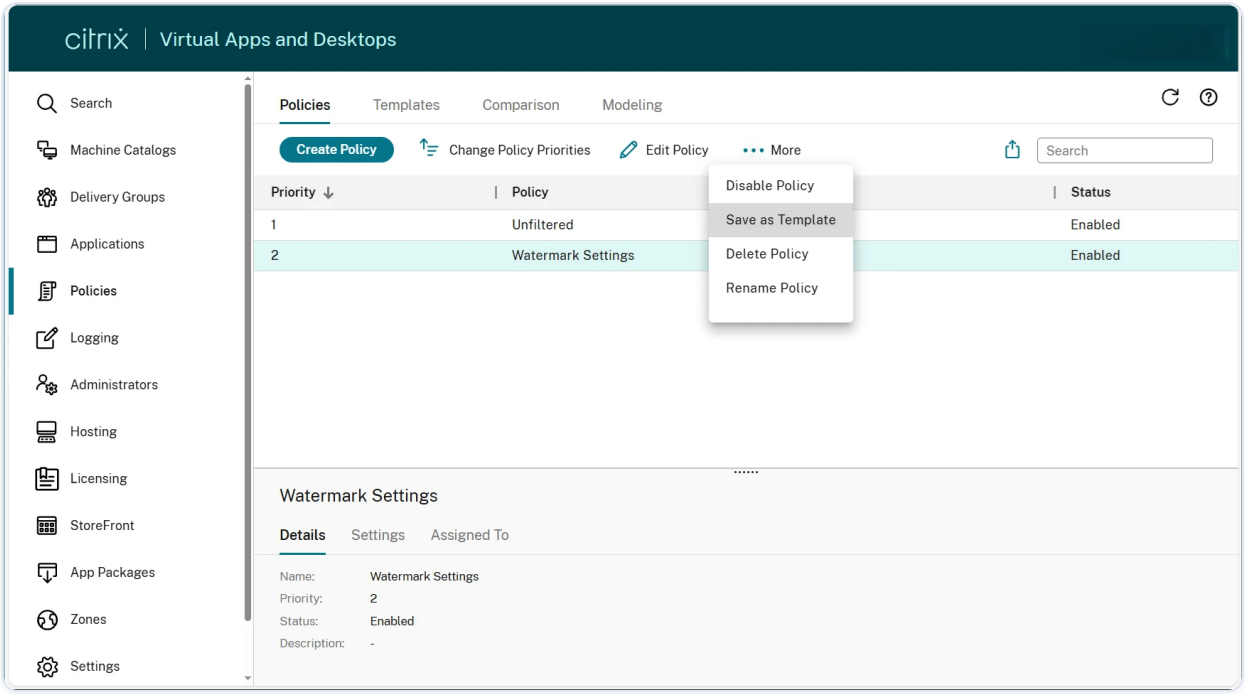
3. 等待最多 5 分钟，然后打开 Web Studio。验证策略 *Watermark Settings* 是否显示在策略列表中。



注意：

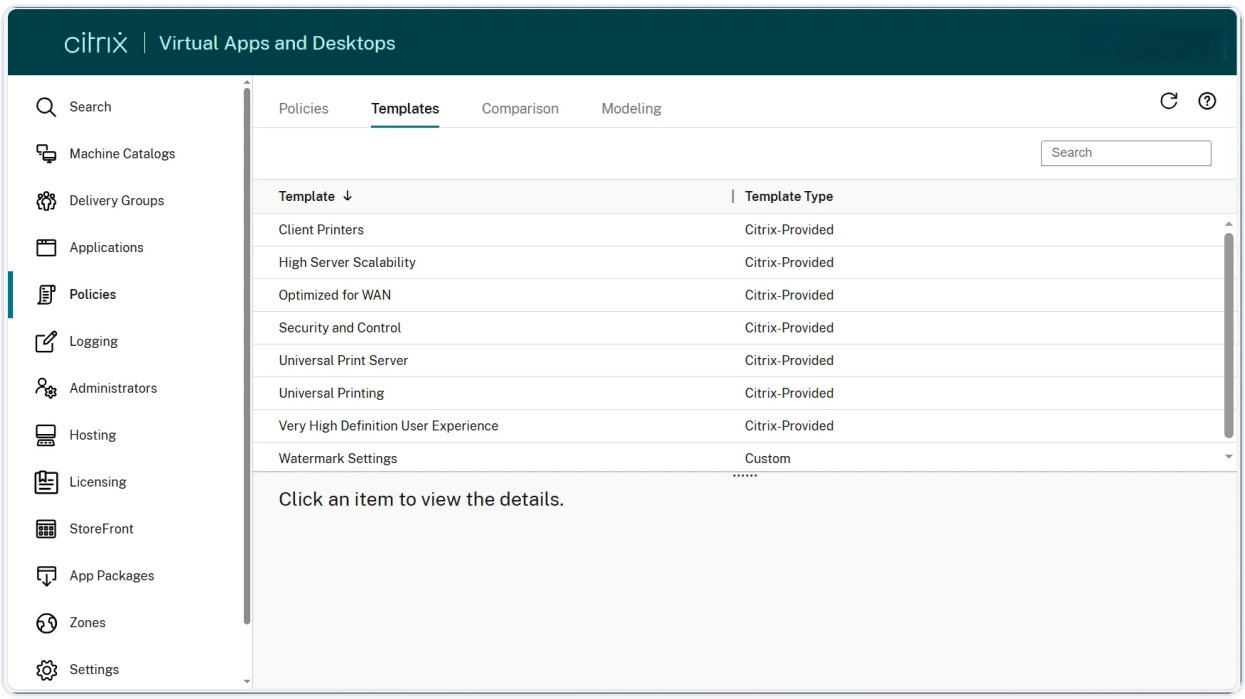
此时，模板尚未显示在“**模板**”选项卡上。策略是中间环节 — 您将在下一步中使用它来创建 Web Studio 模板。

4. 选择 *Watermark Settings* 策略，然后在功能区中选择“**... 更多**”，然后单击“**另存为模板**”。



5. 按照向导操作以创建 Web Studio 模板。

6. 选择“**模板**”选项卡。现在，*水印设置*模板对所有管理员可见，并且可从任何有权访问站点的计算机进行访问。



相关内容

有关在 Web Studio 中管理模板的详细信息，请参阅管理策略模板。

升级后移除已弃用的策略设置

当 Citrix® 弃用产品组件时，其关联的策略设置将失效。升级后，使用 `GpoClean.ps1` 从 Citrix Virtual Apps and Desktops™ 策略中识别并移除这些已弃用的设置，包括因此而变为空的任何策略。

开始之前

运行脚本前，请确保满足以下要求：

- 已安装 **Broker SDK** 和 **Group Policy Management** 的受支持的 Citrix Virtual Apps and Desktops 版本
- 在 Delivery Controller™ 上具有 **Citrix 策略管理**权限

> **注意：**
>
> 脚本会自动加载 `Citrix.Broker.Admin.V2` 和 `Citrix.Common.GroupPolicy` 管理单元。

移除已弃用的策略设置

运行 `GpoClean.ps1` 以移除已弃用的策略设置：

1. 将 `GpoClean.ps1` 复制到您具有 **Citrix 策略管理**权限的 Delivery Controller 上。
2. 在 Delivery Controller 上打开 PowerShell 会话。
3. 运行脚本。无需任何参数。

```
.\GpoClean.ps1
```

> **注意：**
>
> 添加 `-Verbose` 以获取详细的按设置日志记录：`.\GpoClean.ps1 -Verbose`。

脚本分两个阶段运行：

阶段	发生什么
阶段 1	运行 `Test-BrokerDesktopPolicy`，识别 `DeprecatedSetting` 错误，并将每个受影响的设置设为 `NotConfigured`
阶段 2	重新运行 `Test-BrokerDesktopPolicy`，识别没有配置设置的策略（`PolicyHasNoSettings`），并将其删除

所有更改都保存在单个写入操作中。摘要报告已删除的设置和策略的数量。如果未找到任何已弃用的设置，脚本将退出且不进行任何更改。

注意：

- `Unfiltered` 策略永远不会被删除，即使它不包含任何配置的设置。

脚本

将以下内容另存为 `GpoClean.ps1`，然后按照 删除已弃用的策略设置 中所述运行它：

```
<#

.Synopsis



    Cleans up deprecated settings from Citrix policies and removes
policies that no longer have any settings.



.Description



    This script runs Test-BrokerDesktopPolicy to identify deprecated
settings in policies. When a setting is
```

```
    deprecated (DeprecatedSetting error), the script removes the setting
from the policy using the Citrix Group Policy

    PowerShell Provider. After removing deprecated settings, if a policy
has no settings remaining

    (PolicyHasNoSettings error), the policy is removed automatically,
except for the 'Unfiltered' policy which is

    preserved.



    This script is useful for cleaning up policies after upgrading to a
newer version where some settings have been

    deprecated.



.Requirements



    Run this script on a DDC that has the Citrix Group Policy Management
and Citrix Broker SDK installed.

#>



[CmdletBinding()]

param()



Write-Host "Checking Citrix policies for deprecated settings..."



# Load the Citrix Broker PowerShell Snapin.
```

```
$BrokerSnapin = "Citrix.Broker.Admin.V2"
$loaded = Get-PSSnapin $BrokerSnapin -ErrorAction SilentlyContinue
if ($loaded -eq $null)
{
    Add-PSSnapin $BrokerSnapin
}


# First pass: Run Test-BrokerDesktopPolicy to check for errors.
Write-Host "Running policy validation..."
$testResults = Test-BrokerDesktopPolicy | Select-Object -Property *


if ($testResults -eq $null -or $testResults.Count -eq 0)
{
    Write-Host "No policy errors found. All policies are clean."
    exit 0
}


# Check if there are any DeprecatedSetting errors.
$hasDeprecatedSettings = $false
foreach ($result in $testResults)
{
    if ([string]$result.ErrorCode -eq 'DeprecatedSetting')
```

```
    {
        $hasDeprecatedSettings = $true
        break
    }
}

if (-not $hasDeprecatedSettings)
{
    Write-Host "No deprecated settings found. Policy errors exist but do not require cleaning."
    Write-Host "Run 'Test-BrokerDesktopPolicy' to see other policy issues."
    exit 0
}

# Load the Citrix Group Policy PowerShell Provider (only if we need to clean).
Write-Host "`nDeprecated settings found. Loading Group Policy provider for cleanup..."
$GpSnapin = "Citrix.Common.GroupPolicy"
$Provider = "CitrixGroupPolicy"
$SiteName = "CitrixGP"

$loaded = Get-PSSnapin $GpSnapin -ErrorAction SilentlyContinue
```

```
if ($loaded -eq $null)

{

    Add-PSSnapin $GpSnapin

}



# Mount the provider drive if it has not been mounted.

$GpDrive = Get-PSDrive $SiteName -ErrorAction SilentlyContinue

if ($GpDrive -eq $null)

{

    [void]($GpDrive = New-PSDrive -PSProvider $Provider -Name $SiteName
-Root \ -Controller localhost)

}



$uRoot = $SiteName + ":\User\"

$cRoot = $SiteName + ":\Computer\"



$GpDrive.AutoWriteBack = $false



$settingsRemoved = 0

$policiesRemoved = 0



$settingNameMappings = @{
```

```
    'PvsIntegrationEnabled' = 'ImageProviderIntegrationEnabled'

}



function Remove-SettingFromPolicy

{

    param(

        [string] $policyName,

        [string] $settingName

    )



    $targetSettingName = Split-Path -Path $settingName -Leaf



    if ($settingNameMappings.ContainsKey($targetSettingName))

    {

        $mappedSettingName = $settingNameMappings[$targetSettingName]

        Write-Verbose "Mapping deprecated setting name
'$targetSettingName' to '$mappedSettingName'"

        $targetSettingName = $mappedSettingName

    }



    $searchPattern = $SiteName + ":\" + "*\" + $policyName + "\Settings\*"

    Write-Verbose "Searching for settings matching '$targetSettingName' in
policy '$policyName'..."
```

```
    $allSettings = Get-ChildItem -Path $searchPattern -Recurse
-ErrorAction SilentlyContinue |

        Where-Object {

            ($_.PSObject.Properties['State'] -and $_.State -ne
'NotConfigured') -or

            ($_.Name -eq 'Values' -and $_.Values -ne $null -and $_.Values
-ne '')

        }



    $found = $false

    foreach ($setting in $allSettings)

    {

        $RootPath = "{0}\{1}::{2}:" -f $GpSnapin, $Provider, $SiteName

        $relativePath = $setting.PSPath.Substring($RootPath.Length)

        Write-Verbose "  Checking configured setting: $relativePath"

        $currentSettingName = Split-Path -Path $setting.PSPath -Leaf

        if ($currentSettingName -ne $targetSettingName) { continue }

        Write-Verbose "  Found matching setting: $relativePath"

        Set-ItemProperty -Path $setting.PSPath -Name State -Value
NotConfigured

        Write-Host "  Set setting '$relativePath' to NotConfigured"

        $Script:settingsRemoved++

        $found = $true

    }
```

```
    if (-not $found)
    {
        Write-Warning "Could not find setting '$targetSettingName' in
policy '$policyName'"
    }
}

function Remove-PolicyByName
{
    param(
        [string] $policyName
    )

    if ($policyName -eq 'Unfiltered')
    {
        Write-Host "  Skipping removal of 'Unfiltered' policy (reserved
policy)"
        return
    }

    $uPath = $uRoot + $policyName
    $cPath = $cRoot + $policyName
```

```
    if (Test-Path $uPath)

    {

        $uSettings = Get-ChildItem -Path ($uPath + "\Settings") -Recurse
-ErrorAction SilentlyContinue |

            Where-Object {

                ($_.PSObject.Properties['State'] -and $_.State -ne
'NotConfigured') -or

                ($_.Name -eq 'Values' -and $_.Values -ne $null -and
$_.Values -ne '')

            }

        if ($uSettings.Count -eq 0)

        {

            Remove-Item -Path $uPath -Force -Recurse

            Write-Host "  Removed policy: \User\$policyName"

            $Script:policiesRemoved++

        }

    }



    if (Test-Path $cPath)

    {

        $cSettings = Get-ChildItem -Path ($cPath + "\Settings") -Recurse
-ErrorAction SilentlyContinue |

            Where-Object {
```

```
                ($_.PSObject.Properties['State'] -and $_.State -ne
'NotConfigured') -or

                ($_.Name -eq 'Values' -and $_.Values -ne $null -and
$_.Values -ne '')

            }

        if ($cSettings.Count -eq 0)

        {

            Remove-Item -Path $cPath -Force -Recurse

            Write-Host "  Removed policy: \Computer\$policyName"

            $Script:policiesRemoved++

        }

    }

}



# Phase 1: Remove deprecated settings.

Write-Host "`nPhase 1: Removing deprecated settings (this may take some
time)..."

foreach ($result in $testResults)

{

    if ([string]$result.ErrorCode -eq 'DeprecatedSetting')

    {

        Write-Host "`nPolicy '$($result.PolicyName)' has deprecated
settings:"

        if ($result.Settings -ne $null)
```

```
        {

            foreach ($setting in $result.Settings)

            {

                Write-Host "  - Setting '$($setting.SettingName)' is
deprecated"

                Remove-SettingFromPolicy -policyName $result.PolicyName
-settingName $setting.SettingName

            }

        }

    }

}



# Phase 2: Remove empty policies.

Write-Host "`nPhase 2: Checking for policies with no settings..."

$testResults2 = Test-BrokerDesktopPolicy | Select-Object -Property *



if ($testResults2 -eq $null -or $testResults2.Count -eq 0)

{

    Write-Host "No policy errors found."

}

else

{

    foreach ($result in $testResults2)
```

```
    {
        if ([string]$result.ErrorCode -eq 'PolicyHasNoSettings')
        {
            Write-Host "`nPolicy '$($result.PolicyName)' has no settings
remaining:"
            Remove-PolicyByName -policyName $result.PolicyName
        }
    }
}


# Save all changes.
if ($settingsRemoved -gt 0 -or $policiesRemoved -gt 0)
{
    Write-Host "`nSaving changes..."
    $GpDrive.Save()
}


Remove-PSDrive $SiteName


Write-Host "`n========================================="
Write-Host "Policy Cleanup Summary:"
Write-Host "  Settings removed: $settingsRemoved"
```

```
Write-Host "  Policies removed: $policiesRemoved"

Write-Host "========================================="



if ($settingsRemoved -eq 0 -and $policiesRemoved -eq 0)

{

    Write-Host "`nNo issues found. All policies are clean."

}

else

{

    Write-Host "`nCleanup completed successfully."

}



exit 0
```

相关内容

有关每个版本中已弃用设置的更多信息，请参阅 策略更改。

策略设置参考

策略包含在策略强制执行时应用的设置。本节中的描述还指明了是否需要更多设置才能启用某个功能，或者这些设置是否与某个设置类似。

快速参考

下表列出了可在策略中配置的设置。在左列中找到要完成的任务，然后在右列中找到其对应的设置。

所有策略设置的完整列表均以 .CHM（编译的 HTML）格式和 .CSV 格式提供。这些文件位于安装了代理（交付控制器）的服务器上的 `\program files\citrix\grouppolicy` 文件夹中。您也可以单击此处下载最新版本的策略设置。

音频

对于此任务	使用此策略设置
控制是否允许多个音频设备的使用	音频即插即用
控制是否允许从用户设备上的麦克风输入音频	客户端麦克风重定向
控制用户设备上的音频质量	音频质量
控制用户设备上扬声器的音频映射	客户端音频重定向

用户设备的带宽

要限制用于以下目的的带宽	使用此策略设置
客户端音频映射	音频重定向带宽限制或音频重定向带宽限制百分比
使用本地剪贴板进行剪切和粘贴	剪贴板重定向带宽限制或剪贴板重定向带宽限制百分比
在会话中访问本地客户端驱动器	文件重定向带宽限制或文件重定向带宽限制百分比
HDX™ MediaStream 多媒体加速	HDX MediaStream 多媒体加速带宽限制或 HDX MediaStream 多媒体加速带宽限制百分比
客户端会话	总体会话带宽限制
打印	打印机重定向带宽限制或打印机重定向带宽限制百分比
TWAIN 设备（例如照相机或扫描仪）	TWAIN 设备重定向带宽限制或 TWAIN 设备重定向带宽限制百分比
USB 设备	客户端 USB 设备重定向带宽限制或客户端 USB 设备重定向带宽限制百分比

客户端驱动器和用户设备的重定向

对于此任务	使用此策略设置
控制用户登录服务器时是否连接用户设备上的驱动器	自动连接客户端驱动器
控制服务器与本地剪贴板之间的剪切和粘贴数据传输	客户端剪贴板重定向
控制驱动器如何从用户设备映射	客户端驱动器重定向
控制用户的本地硬盘驱动器在会话中是否可用	客户端固定驱动器和客户端驱动器重定向
控制用户的本地软盘驱动器在会话中是否可用	客户端软盘驱动器和客户端驱动器重定向
控制用户的网络驱动器在会话中是否可用	客户端网络驱动器和客户端驱动器重定向
控制用户的本地 CD、DVD 或蓝光驱动器在会话中是否可用	客户端光盘驱动器和客户端驱动器重定向
控制用户的本地可移动驱动器在会话中是否可用	客户端可移动驱动器和客户端驱动器重定向
控制用户的 TWAIN 设备（例如扫描仪和照相机）在会话中是否可用，并控制图像数据传输的压缩	客户端 TWAIN 设备重定向；TWAIN 压缩重定向
控制 USB 设备在会话中是否可用	客户端 USB 设备重定向和客户端 USB 设备重定向规则
提高通过 WAN 向客户端磁盘写入和复制文件的速度	使用异步写入

内容重定向

对于此任务	使用此策略设置
控制是否使用从服务器到用户设备的内容重定向	主机到客户端重定向

桌面 UI

对于此任务	使用此策略设置
控制是否在用户会话中使用桌面壁纸	桌面壁纸
在拖动窗口时查看窗口内容	拖动时查看窗口内容

图形和多媒体

重要提示：

Flash 策略保留仅是为了允许使用旧版 VDA 的客户使用较新的控制器（例如，版本 1912 控制器）并仍可使用 Flash。此 VDA 版本不支持 Flash。

对于此任务	使用此策略设置
控制从虚拟桌面发送到用户设备的最大每秒帧数	目标帧率
控制在用户设备上显示的图像的视觉质量	视觉质量
控制网站在会话中访问时是否可以显示 Flash 内容	Flash 服务器端内容获取 URL 列表；Flash URL 兼容性列表；Flash 视频回退阻止策略设置；Flash 视频回退阻止错误 *.swf
控制服务器渲染视频的压缩	使用视频编解码器进行压缩；对视频编解码器使用硬件编码
控制向用户交付 HTML5 多媒体 Web 内容	HTML5 视频重定向

优先处理多流网络流量

对于此任务	使用此策略设置
指定跨多个连接的 ICA® 流量端口并建立网络优先级	多端口策略
启用服务器和用户设备之间的多流连接支持	多流（计算机和用户设置）

打印

对于此任务	使用此策略设置
控制在用户设备上创建客户端打印机	自动创建客户端打印机和客户端打印机重定向
控制打印机属性的存储位置	打印机属性保留
控制客户端或服务器是否处理打印请求	直接连接到打印服务器
控制用户是否可以访问连接到其用户设备的打印机	客户端打印机重定向
控制在自动创建客户端和网络打印机时安装本机 Windows 驱动程序	自动安装内置打印机驱动程序
控制何时使用通用打印机驱动程序	通用打印机驱动程序使用情况
根据漫游用户会话信息选择打印机	默认打印机
为通用打印服务器配置负载平衡和故障转移阈值	用于负载平衡的通用打印服务器；通用打印服务器停用阈值

注意：

策略不能用于在桌面或应用程序会话中启用屏幕保护程序。对于需要屏幕保护程序的用户，可以在用户设备上实施屏幕保护程序。

ICA® 策略设置

注意：

本页提供 ICA 策略设置的说明和支持的配置值。有关使用策略的更多信息，请参阅 使用策略 部分。

自适应传输

自适应传输

此设置允许或阻止通过 EDT 作为主要方式以及通过 TCP 作为备用方式进行数据传输。

默认情况下，自适应传输处于启用状态（**首选**），并在可能时使用 EDT，回退到 TCP。您可以根据需要更改其设置：

- **首选**。在可能时使用通过 EDT 的自适应传输，回退到 TCP。
- **诊断模式**。EDT 被强制启用，并且回退到 TCP 被禁用。我们建议仅将此设置用于故障排除。
- **关闭**。TCP 被强制启用，并且 EDT 被禁用。

有关详细信息，请参阅 自适应传输。

MTU 重新发现

MTU 重新发现允许检测使用 EDT 作为传输协议的活动会话中的更改，并调整会话的 MTU 以防止性能问题。

此设置可按如下方式配置：

- 关闭：MTU 重新发现已禁用。
- 静态：当检测到 MTU 降低时，会话的 MTU 将在会话的剩余时间内设置为 1200。
- 动态：当在活动会话中检测到 MTU 降低时，将触发 MTU 发现以确定连接的最佳 MTU。

默认情况下，此设置处于禁用状态。

应用程序启动等待超时

此设置指定会话等待第一个应用程序启动的等待超时值（以毫秒为单位）。如果应用程序的启动时间超过此时间段，则会话将结束。

您可以选择默认时间（10,000 毫秒）或指定一个以毫秒为单位的数字。

客户端剪贴板重定向

此设置允许或阻止将用户设备上的剪贴板映射到服务器上的剪贴板。

默认情况下，允许剪贴板重定向。

要阻止会话与本地剪贴板之间的数据复制和粘贴，请选择 **禁止**。用户仍可以在会话中运行的应用程序之间复制和粘贴数据。

允许此设置后，配置剪贴板在客户端连接中可占用的最大允许带宽。使用**剪贴板重定向带宽限制**或**剪贴板重定向带宽限制百分比**设置。

客户端剪贴板写入允许的格式

当**限制客户端剪贴板写入**设置为**已启用**时，主机剪贴板数据无法与客户端端点共享。您可以使用此设置允许特定数据格式与客户端端点剪贴板共享。要使用此设置，请启用它并添加要允许的特定格式。

以下剪贴板格式是系统定义的：

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

以下自定义格式在 XenApp 和 XenDesktop 以及 Citrix Virtual Apps and Desktops™ 中预定义：

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML 格式默认禁用。要启用此功能：

- 验证 **客户端剪贴板重定向** 是否设置为 **允许**。
- 验证 **限制客户端剪贴板写入** 是否设置为 **已启用**。
- 在 **客户端剪贴板写入允许的格式** 中添加 **CF_HTML**（以及您希望支持的任何其他格式）的条目。

您可以添加更多自定义格式。自定义格式名称必须与要注册到系统的格式匹配。格式名称区分大小写。

如果**客户端剪贴板重定向**策略设置为**禁止**，或者**限制客户端剪贴板写入**策略设置为**禁用**，则此设置不适用。

> **注意：**
>
> 启用 HTML 格式剪贴板复制支持 (CF_HTML) 会将复制内容源中的任何脚本复制到目标。在继续复制之前，请检查您是否信任源。如果您复制了包含脚本的内容，则只有将目标文件保存为 HTML 文件并运行它时，这些脚本才会生效。

限制剪贴板客户端到会话的传输大小

此设置指定用户在单个复制粘贴操作期间可以从客户端端点传输到虚拟会话的剪贴板数据的最大大小。

要限制剪贴板传输大小，请启用**限制剪贴板客户端到会话的传输大小**设置。然后，在**大小限制**字段中，输入一个以千字节为单位的值，以定义本地剪贴板与会话之间的数据传输大小。

默认情况下，此设置处于禁用状态，并且对客户端到会话的传输没有限制。

限制剪贴板会话到客户端的传输大小

此设置指定用户在单个复制粘贴操作期间可以从虚拟会话传输到客户端端点的剪贴板数据的最大大小。

要限制剪贴板传输大小，请启用**限制剪贴板会话到客户端的传输大小**设置。然后，在**大小限制**字段中，输入一个以千字节为单位的值，以定义会话与本地剪贴板之间的数据传输大小。

默认情况下，此设置处于禁用状态，并且对会话到客户端的传输没有限制。

限制客户端剪贴板写入

如果此设置处于**启用**状态，则主机剪贴板数据无法与客户端端点共享。您可以通过启用**客户端剪贴板写入允许的格式**设置来允许特定格式。

默认情况下，此设置处于**禁用**状态。

限制会话剪贴板写入

当此设置为**已启用**时，客户端剪贴板数据无法与会话应用程序共享。您可以通过启用**会话剪贴板写入允许的格式**设置来允许特定格式。

默认情况下，此设置为**已禁用**。

会话剪贴板写入允许的格式

当**限制会话剪贴板写入**设置为**已启用**时，客户端剪贴板数据无法与会话应用程序共享。您可以使用此设置来允许特定数据格式与会话剪贴板共享。

以下剪贴板格式是系统定义的：

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE

- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

以下自定义格式已预定义在 XenApp 和 XenDesktop 以及 Citrix Virtual Apps and Desktops™ 中：

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML 格式默认禁用。要启用此功能，请执行以下操作：

- 验证**客户端剪贴板重定向**是否设置为**允许**。
- 验证**限制会话剪贴板写入**是否设置为**已启用**。
- 在**会话剪贴板写入允许的格式**中添加**CF_HTML**（以及您希望支持的任何其他格式）的条目。

您可以添加更多自定义格式。自定义格式名称必须与要注册到系统的格式匹配。格式名称区分大小写。

如果**客户端剪贴板重定向**策略设置为**已禁止**或**限制会话剪贴板写入**策略设置为**已禁用**，则此设置不适用。

> **注意：**
>
> 启用 HTML 格式剪贴板复制支持 (CF_HTML) 会将复制内容源中的任何脚本复制到目标。在继续复制之前，请检查您是否信任源。如果您复制了包含脚本的内容，则只有将目标文件另存为 HTML 文件并运行它，这些脚本才会生效。

桌面启动

此设置允许或阻止 VDA 直接访问用户组中的非管理用户使用 ICA 连接连接到该 VDA 上的会话。

默认情况下，非管理用户无法连接到这些会话。

此设置不影响使用 RDP 连接的 VDA 直接访问用户组中的非管理用户。当此设置启用或禁用时，这些用户可以连接到 VDA。此设置不影响不在 VDA 直接访问用户组中的非管理用户。当此设置启用或禁用时，这些用户无法连接到 VDA。

拖放设置

此设置允许或阻止在客户端与虚拟应用程序或桌面之间拖放文件。默认情况下，拖放策略处于禁用状态。如果需要，您可以启用此策略。

FIDO2

FIDO2 重定向

此设置启用或禁用 FIDO2 重定向。FIDO2 重定向允许用户利用虚拟机中的本地端点 FIDO2 组件。用户可以通过 FIDO2 安全密钥或在具有 TPM 2.0 和 Windows Hello 的设备上使用集成生物识别技术来验证虚拟会话。

当此设置为 **允许** 时，用户可以使用本地端点功能进行 FIDO2 身份验证。默认情况下，此设置为 **允许**。

FIDO2 允许的进程

此设置允许管理员指定哪些应用程序被允许在虚拟会话中使用 FIDO2 和 WebAuthn 重定向。

允许列表中的应用程序必须具有应用程序可执行文件的完整本地路径。不支持网络路径。

通配符(*) 可用于应用程序路径中以替换单个目录、目录名称的一部分、可执行文件基本名称或可执行文件基本名称的一部分。

HDX™ 直接

HDX™ 直接

当直接通信可用时，HDX Direct 允许客户端自动与会话主机建立直接连接。连接使用网络级加密安全建立。

HDX Direct 模式

HDX Direct 可用于为内部和外部客户端建立与会话主机的直接连接。此设置确定 HDX Direct 仅适用于内部客户端，还是同时适用于内部和外部客户端。

当设置为仅 **内部** 时，HDX Direct 仅尝试为内部网络中的客户端建立直接连接。

当设置为 **内部** 和 **外部** 时，HDX Direct 尝试为内部和外部客户端建立直接连接。

默认情况下，HDX Direct 仅为内部客户端设置。

HDX Direct 端口范围

HDX Direct 用于外部用户连接的端口范围。 默认情况下，HDX Direct 使用的端口范围是：55000–55250。

ICA 侦听器

ICA 侦听器连接超时

此设置指定使用 ICA 协议的连接完成所需的最长等待时间。

默认情况下，最长等待时间为 120,000 毫秒，即两分钟。

ICA 侦听器端口号

此设置指定服务器上 ICA 协议使用的 TCP/IP 端口号。

默认情况下，端口号设置为 1494。

有效端口号必须在 0-65535 范围内，并且不得与其他知名端口号冲突。如果更改端口号，请重新启动服务器以使新值生效。如果更改服务器上的端口号，则还必须在连接到服务器的每个 Citrix Workspace™ 应用程序或插件上更改它。

键盘和输入法编辑器 (IME)

此设置启用或禁用以下功能：

- 动态键盘布局同步
- 输入法编辑器 (IME)
- Unicode 键盘布局映射
- 隐藏或显示键盘布局切换通知对话框消息
- 触控设备最终用户的自动触控键盘显示

1. 在 Web Studio 中，选择 **键盘和 IME**。
2. 选择 **客户端键盘布局同步和 IME 改进** 以控制 VDA 中的动态键盘布局同步和通用客户端输入法编辑器 (IME) 功能。您可以配置：

   已禁用 - 动态键盘布局同步和通用客户端输入法编辑器 (IME)。

   支持动态客户端键盘布局同步 - 启用动态键盘布局同步。

支持动态客户端键盘布局同步和 IME 改进 - 同时启用动态键盘布局同步和通用客户端输入法编辑器 (IME)。

3. 选择 **启用 Unicode 键盘布局映射** 以启用或禁用 Unicode 键盘映射。
4. 选择 **隐藏键盘布局切换弹出消息框** 以控制当用户更改客户端键盘布局时是否显示一条消息，指示键盘布局正在同步。如果您阻止消息出现，用户必须等待片刻才能开始输入，以避免字符输入不正确。
5. 选择 **自动键盘显示** 以允许或禁止在您进入或离开输入字段时客户端软/触控键盘自动显示或隐藏。

默认设置：

- **客户端键盘布局同步和 IME 改进**
  - 在 Windows Server 2019/2022/2025 和多会话 Win 10/11 中已禁用
  - 在单会话 Win 10/11 中已启用
- **Unicode 键盘布局映射**
  - 禁止（表示 Unicode 键盘布局映射默认禁用，如果最终用户在 CWAs 上使用 Unicode 输入模式，则需要配置并允许它）
- **隐藏键盘布局切换弹出消息框**
  - 禁止（表示将显示弹出消息框）
- **自动键盘显示**
  - 禁止（表示当您进入或离开输入字段时，客户端软/触摸键盘不会自动显示或隐藏）

此策略将替换策略设置的“**描述**”部分中列出的注册表设置。

注销检查器启动延迟

此设置指定延迟注销检查器启动的持续时间。使用此策略可设置客户端会话在断开会话连接之前等待的时间（以秒为单位）。

此设置还会增加用户从服务器注销所需的时间。

容错模式

> **重要提示：**

- 此功能至少需要适用于 Windows 的 Citrix Workspace 应用程序 2002。此版本的 VDA 在可用时将支持此功能。
- Citrix Gateway 和 Citrix Gateway Service 支持图形容错模式。此模式仅适用于直接连接。

此设置启用或禁用图形容错模式。

默认情况下，图形容错模式为“**允许**”。

当允许时，当丢包和延迟超过阈值时，将进入该模式。您可以使用容忍丢包阈值策略设置这些阈值。

容忍丢包阈值

当容忍丢包模式可用时，此设置指定会话切换到图形容忍丢包模式的网络指标阈值。

默认阈值为：

- 丢包率：5%
- 延迟：300 毫秒 (RTT)

有关详细信息，请参阅容忍丢包模式。

音频容错模式

此设置启用或禁用音频的容忍丢包模式。

启用后，音频将通过容忍丢包模式发送。

默认情况下，音频的容忍丢包模式为**禁止**。

要启用此策略，请将音频容忍丢包模式策略的注册表编辑为**允许**。

启用音频的容忍丢包模式需要 EDT 传输。

Rendezvous（会合）

Rendezvous 协议

此设置更改使用 Citrix Gateway Service 时 HDX 会话的代理方式。启用后，HDX 流量不再通过 Citrix Cloud Connector。相反，VDA 直接与 Citrix Gateway Service 建立出站连接（从而增强 Cloud Connector 的可扩展性）。

重要提示：

> Citrix Cloud™ 中的功能切换和 HDX 策略设置控制此功能。Citrix Cloud 功能切换默认启用，而 HDX 设置默认禁用。HDX 设置仅影响通过 Citrix Gateway Service 建立的 HDX 会话。此设置不影响客户端与 VDA 之间直接建立的会话或通过本地 Citrix Gateway 建立的会话。

> 有关信息，请参阅 Rendezvous 协议。

Rendezvous 代理配置

此设置允许您配置一个显式代理，以便与 Rendezvous 协议一起使用。如果使用透明代理，则无需启用此设置。

默认情况下，此设置处于禁用状态。

禁用时，VDA 在尝试与网关服务建立 Rendezvous 连接时，不会通过任何非透明代理路由出站流量。

启用时，VDA 会尝试通过此设置中定义的代理与网关服务建立 Rendezvous 连接。

VDA 支持将 HTTP 和 SOCKS5 代理用于 Rendezvous 连接。要将 VDA 配置为对 Rendezvous 连接使用代理，必须启用此设置。此外，请指定代理地址或 PAC 文件的路径。例如：

- 代理地址：`http://<URL or IP>:<port>` 或 `socks5://<URL or IP>:<port>`
- PAC 文件：`http://<URL or IP>/<path>/<filename>.pac`

  VDA 版本 2103 是支持使用 PAC 文件进行代理配置的最低版本。有关 SOCKS5 代理的 PAC 文件架构的更多信息，请参阅 代理配置。

> **注意：**

> 只有 SOCKS5 代理支持通过 EDT 进行数据传输。对于 HTTP 代理，请使用 TCP 作为 ICA 的传输协议。

> 有关详细信息，请参阅 Rendezvous 协议。

安全 HDX

此设置启用或禁用 Secure HDX 的使用。

Secure HDX 使用应用程序级加密来保护 HDX 协议，从而为 HDX 会话提供真正的端到端加密。

启用后，将强制执行 Secure HDX，并且会阻止与不支持 Secure HDX 的客户端的连接。Secure HDX 默认处于禁用状态。

客户端连接期间启动未发布的程序

此设置指定是否允许通过 RDP 在服务器上启动初始应用程序。

默认情况下，不允许通过 RDP 在服务器上启动初始应用程序。

会话指标收集

此设置允许 Citrix 收集 VDA 和 Workspace 之间的用户和计算机会话指标，以改善用户体验。

Citrix 会收集操作系统、正常运行时间、计算机系统信息、视频控制器详细信息、VDA 版本、部署类型和域加入状态等数据。此外，您还可以收集一些会话配置以及性能和可靠性数据，以帮助改进产品。有关我们的客户体验改善计划的更多信息，请参阅：

- `<https://more.citrix.com/XD-CEIP>`
- `<https://docs.citrix.com/zh-cn/linux-virtual-delivery-agent/2607-ltsr/configure/administration/linux-vda-data-collection-program>`
- `<https://docs.citrix.com/zh-cn/mac-vda/configure/session/supportability-service>`

默认情况下，此设置为启用状态。

平板电脑模式切换策略设置

平板电脑模式切换可优化 VDA 上 Store 应用程序、Win32 应用程序和 Windows shell 的外观和行为。它通过在从小尺寸设备（如手机和平板电脑）或任何支持触摸的设备连接时，自动将虚拟桌面切换到平板电脑模式来实现此目的。

如果禁用此策略，VDA 将处于用户设置的模式，并且无论客户端类型如何，都将始终保持相同的模式。

身份验证策略设置

身份验证部分包含控制身份验证设置的策略设置。

Microsoft Entra 单点登录

此设置启用或禁用 VDA 中 Microsoft Entra 单点登录的使用。此设置默认启用。

自动客户端重新连接策略设置

“**自动客户端重新连接**”部分包含用于控制会话自动重新连接的策略设置。

自动客户端重新连接

此设置允许或阻止在连接中断后由同一客户端自动重新连接。

对于 Citrix Receiver for Windows 4.7 及更高版本以及 Citrix Workspace app 1808 及更高版本，自动客户端重新连接仅使用 Citrix Studio 中的策略设置。在 Studio 中更新这些策略会将自动客户端重新连接从服务器同步到客户端。对于旧版 Citrix Receiver for Windows，要配置自动客户端重新连接，请使用 Studio 策略并更改注册表或 default.ica 文件。

允许自动客户端重新连接使用户能够在连接中断后从中断处继续工作。自动重新连接会检测到中断的连接，然后将用户重新连接到其会话。

如果不使用包含会话 ID 和凭据密钥的 Citrix Workspace™ app cookie，自动重新连接可能会导致启动新会话。也就是说，不是重新连接到现有会话。如果 cookie 已过期，则不会使用该 cookie。例如，cookie 可能会因重新连接延迟或需要重新输入凭据而过期。如果用户有意断开连接，则不会触发自动客户端重新连接。

重新连接正在进行时，会话窗口会灰显。倒计时计时器显示会话重新连接前的剩余时间。会话超时后，它将断开连接。

对于应用程序会话，当允许自动重新连接时，通知区域中会显示一个倒计时计时器。此计时器指定会话重新连接前的剩余时间。Citrix Workspace app 会尝试重新连接到会话，直到成功重新连接或用户取消重新连接尝试。

对于用户会话，当允许自动重新连接时，Citrix Workspace app 会在指定时间内尝试重新连接到会话，除非成功重新连接或用户取消重新连接尝试。默认情况下，此期限为两分钟。要更改此期限，请编辑策略。

默认情况下，允许自动客户端重新连接。您可以通过将策略设置为**禁止**来禁用它。

自动客户端重新连接身份验证

此设置指定自动客户端重新连接是否需要身份验证。

用户首次登录时，凭据会被加密并存储在内存中，同时会创建一个包含加密密钥的 cookie。该 cookie 会发送到 Citrix Workspace app。配置此设置后，将不使用 cookie。相反，当 Citrix Workspace app 尝试自动重新连接时，会向用户显示一个对话框，要求输入凭据。

默认情况下，不需要身份验证。

自动客户端重新连接日志记录

此设置启用或禁用在事件日志中记录自动客户端重新连接。

启用日志记录后，服务器系统日志会捕获有关成功和失败的自动重新连接事件的信息。站点不提供所有服务器的重新连接事件的组合日志。

默认情况下，日志记录处于禁用状态。

自动客户端重新连接超时

默认情况下，客户端自动重新连接超时设置为 120 秒，客户端自动重新连接超时的最大可配置值为 300 秒。使用此策略设置超时值。

重新连接 UI 透明度级别

此设置允许您指定在会话可靠性重新连接期间应用于 XenApp 或 XenDesktop® 会话窗口的不透明度级别。

默认情况下，重新连接 UI 透明度设置为 80%。

音频策略设置

音频部分包含策略设置，这些设置允许用户设备在会话中发送和接收音频，而不会降低性能。

自适应音频

此设置启用或禁用自适应音频。启用此策略后，音频质量设置将动态调整，以提供最佳用户体验。此设置适用于使用 Citrix Virtual Apps and Desktops™ 2109 或更高版本的 VDA 的单会话操作系统和多会话操作系统会话。

禁止此设置时，将应用音频质量策略。有关详细信息，请参阅音频质量。

默认情况下，自适应音频策略处于启用状态。

通过 UDP 实时传输音频

此设置允许或阻止 VDA 和用户设备之间通过 RTP 使用用户数据报协议 (UDP) 传输和接收音频。禁用此设置时，音频将通过 TCP 发送和接收。

默认情况下，允许通过 UDP 传输音频。

音频即插即用

此设置允许或阻止使用多个音频设备录制和播放声音。

默认情况下，允许使用多个音频设备。

此设置仅适用于 Windows 多会话操作系统计算机。

音频质量

此设置指定用户会话中接收到的声音质量级别。

默认情况下，声音质量设置为“高 - 高清音频”。

要控制声音质量，请选择以下选项之一：

- 选择“低” - 适用于低带宽连接的低速连接。发送到用户设备的声音被压缩到 16 Kbps。这种压缩会导致声音质量显著下降。但也能为低带宽连接提供合理的性能。
- 选择中等 - 针对语音进行优化，以提供 IP 语音应用程序。此设置可在网络连接不佳（线路低于 512 Kbps，或存在严重拥塞和数据包丢失）的情况下提供媒体应用程序。此编解码器提供快速编码时间，使其非常适合在需要服务器端媒体处理时与软电话和统一通信应用程序配合使用。

  发送到用户设备的音频被压缩到 64 Kbps。这种压缩会导致用户设备上播放的音频质量适度降低，同时提供低延迟并消耗低带宽。如果 IP 语音质量不理想，请确保“通过 UDP 的音频实时传输”策略设置已设置为“允许”。

  现在，仅当选择此音频质量时，才支持通过 UDP 的实时传输 (RTP)。即使对于通过低速（低于 512 Kbps）线路等具有挑战性的网络连接传输媒体应用程序，也请使用此音频质量。此外，当网络中存在拥塞和数据包丢失时也适用。
- 选择高 - 适用于带宽充足且音质重要的连接的高清音频。客户端可以以其原始速率播放声音。声音以高质量级别压缩，可保持高达 CD 质量，并使用高达 112 Kbps 的带宽。传输此量的数据可能会导致 CPU 使用率增加和网络拥塞。

带宽仅在录制或播放音频时消耗。如果两者同时发生，带宽消耗将翻倍。

要指定最大带宽量，请配置“**音频重定向带宽限制**”或“**音频重定向带宽限制百分比**”设置。

客户端音频重定向

此设置指定服务器上托管的应用程序是否可以通过用户设备上安装的声音设备播放声音。此设置还指定用户是否可以录制音频输入。

默认情况下，允许音频重定向。

允许此设置后，您可以限制播放或录制音频所消耗的带宽。限制音频消耗的带宽量可以提高应用程序性能，但也可能会降低音频质量。带宽仅在录制或播放音频时消耗。如果两者同时发生，带宽消耗将翻倍。要指定最大带宽量，请配置“**音频重定向带宽限制**”或“**音频重定向带宽限制百分比**”设置。

在 Windows 多会话操作系统计算机上，请确保启用“**音频即插即用**”设置以支持多个音频设备。

重要提示：禁止客户端音频重定向会禁用所有 HDX™ 音频功能。

客户端麦克风重定向

此设置启用或禁用客户端麦克风重定向。启用后，用户可以使用麦克风在会话中录制音频输入。

默认情况下，允许麦克风重定向。

为了安全起见，当设备上的不受信任服务器尝试访问麦克风时，会向用户发出警报。用户可以选择接受或不接受访问。用户可以在 Citrix Workspace™ 应用程序上禁用此警报。

在 Windows 多会话操作系统计算机上，请确保启用“音频即插即用”设置以支持多个音频设备。

如果用户设备上禁用了**客户端音频重定向**设置，则此规则无效。

带宽策略设置

带宽部分包含用于避免与客户端会话带宽使用相关的性能问题的策略设置。

重要提示：将这些策略设置与**多流策略**设置一起使用可能会产生意外结果。如果您在策略中使用多流设置，请确保不包含这些带宽限制策略设置。

音频重定向带宽限制

此设置指定用户会话中播放或录制音频允许的最大带宽。允许的最大带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为**音频重定向带宽限制百分比**设置输入一个值，则应用限制性最强的设置（较低的值）。

音频重定向带宽限制百分比

此设置指定播放或录制音频允许的最大带宽限制，占总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为**音频重定向带宽限制**设置输入一个值，则应用限制性最强的设置（较低的值）。

如果您配置此设置，则还必须配置**会话总带宽限制**设置，该设置指定可用于客户端会话的带宽总量。

客户端 USB 设备重定向带宽限制

此设置指定将 USB 设备重定向到客户端和从客户端重定向允许的最大带宽。允许的最大带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为**客户端 USB 设备重定向带宽限制百分比**设置输入一个值，则应用限制性最强的设置（较低的值）。

客户端 USB 设备重定向带宽限制百分比

此设置指定将 USB 设备重定向到客户端和从客户端重定向允许的最大带宽，占总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为 **客户端 USB 设备重定向带宽限制** 设置输入一个值，则应用限制最严格的设置（较低的值）。

如果您配置此设置，则还必须配置 **会话总带宽限制** 设置，该设置指定了客户端会话可用的总带宽量。

剪贴板重定向带宽限制

此设置指定了会话与本地剪贴板之间数据传输的最大允许带宽。最大允许带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为 **剪贴板重定向带宽限制百分比** 设置输入一个值，则应用限制最严格的设置（较低的值）。

剪贴板重定向带宽限制百分比

此设置指定了会话与本地剪贴板之间数据传输的最大允许带宽，该带宽是会话总带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为 **剪贴板重定向带宽限制** 设置输入一个值，则应用限制最严格的设置（较低的值）。

如果您配置此设置，则还必须配置 **会话总带宽限制** 设置，该设置指定了客户端会话可用的总带宽量。

COM 端口重定向带宽限制

> **注意：**
>
> 对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置；请参阅 使用注册表配置 COM 端口和 LPT 端口重定向设置。

> 此设置指定了客户端连接中访问 COM 端口的最大允许带宽（以千比特每秒为单位）。如果您为此设置输入一个值，并为 **COM 端口重定向带宽限制百分比** 设置输入一个值，则应用限制最严格的设置（较低的值）。

COM 端口重定向带宽限制百分比

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置；请参阅 使用注册表配置 COM 端口和 LPT 端口重定向设置。

此设置指定了客户端连接中访问 COM 端口的最大允许带宽，该带宽是会话总带宽的百分比。

默认情况下，未指定最大值（零）

如果您为此设置输入一个值，并为 **COM 端口重定向带宽限制** 设置输入一个值，则应用限制最严格的设置（较低的值）。

如果您配置此设置，则还必须配置“**会话总带宽限制**”设置，该设置指定客户端会话可用的总带宽量。

文件重定向带宽限制

此设置指定用户会话中访问客户端驱动器的最大允许带宽。最大允许带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**文件重定向带宽限制百分比**”设置输入一个值，则最严格的设置（较低的值）将生效。

文件重定向带宽限制百分比

此设置指定访问客户端驱动器的最大允许带宽限制，该限制是总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**文件重定向带宽限制**”设置输入一个值，则最严格的设置（较低的值）将应用。

如果您配置此设置，则还必须配置“**会话总带宽限制**”设置，该设置指定客户端会话可用的总带宽量。

HDX™ MediaStream 多媒体加速带宽限制

此设置指定使用 HDX MediaStream 多媒体加速传输流式音频和视频的最大允许带宽限制。最大允许带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**HDX MediaStream 多媒体加速带宽限制百分比**”设置输入一个值，则最严格的设置（较低的值）将生效。

HDX MediaStream 多媒体加速带宽限制百分比

此设置指定使用 HDX MediaStream 多媒体加速传输流式音频和视频的最大允许带宽，该带宽是总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置和**HDX MediaStream 多媒体加速带宽限制**设置输入值，则最严格的设置（较低的值）将生效。

如果配置此设置，则还必须配置**会话总带宽限制**设置，该设置指定可用于客户端会话的总带宽量。

LPT 端口重定向带宽限制

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置；请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。

此设置指定单个用户会话中使用 LPT 端口的打印作业允许的最大带宽。允许的最大带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置和**LPT 端口重定向带宽限制百分比**设置输入值，则最严格的设置（较低的值）将应用。

LPT 端口重定向带宽限制百分比

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置；请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。

此设置指定单个客户端会话中使用 LPT 端口的打印作业的带宽限制，该限制占总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置和**LPT 端口重定向带宽限制**设置输入值，则最严格的设置（较低的值）将应用。

如果配置此设置，则还必须配置**会话总带宽限制**设置，该设置指定可用于客户端会话的总带宽量。

总体会话带宽限制

此设置指定用户会话可用的总带宽量，以千比特每秒为单位。

可强制执行的最大带宽上限为 20 Mbps (20,000 Kbps)。默认情况下，未指定最大值（零）。

当客户端连接之外的其他应用程序争用有限带宽时，限制客户端连接消耗的带宽量可以提高性能。

打印机重定向带宽限制

此设置指定用户会话中访问客户端打印机允许的最大带宽。允许的最大带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**打印机重定向带宽限制百分比**”设置输入一个值，则应用限制性最强的设置（较低的值）。

打印机重定向带宽限制百分比

此设置指定了访问客户端打印机的最大允许带宽，该带宽是总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**打印机重定向带宽限制**”设置输入一个值，则应用限制性最强的设置（值较低的设置）。

如果您配置此设置，则还必须配置“**总会话带宽限制**”设置，该设置指定了客户端会话可用的总带宽量。

TWAIN 设备重定向带宽限制

此设置指定了从已发布的应用程序控制 TWAIN 成像设备的最大允许带宽。最大允许带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**TWAIN 设备重定向带宽限制百分比**”设置输入一个值，则应用限制性最强的设置（较低的值）。

TWAIN 设备重定向带宽限制百分比

此设置指定了从已发布的应用程序控制 TWAIN 成像设备的最大允许带宽，该带宽是总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**TWAIN 设备重定向带宽限制**”设置输入一个值，则应用限制性最强的设置（值较低的设置）。

如果您配置此设置，则还必须配置“**总会话带宽限制**”设置，该设置指定了客户端会话可用的总带宽量。

双向内容重定向策略设置

“**双向内容重定向**”部分包含用于启用或禁用客户端到 VDA 和 VDA 到客户端 URL 重定向的策略设置。

服务器策略在 Web Studio 中设置。从 Citrix Workspace™ app 2311 版开始，此设置取代了 Web Studio 中以下三个已弃用的旧版设置：

- 允许双向内容重定向
- 允许重定向到 VDA 的 URL
- 允许重定向到客户端的 URL

它还取代了 Windows 客户端上的以下三个本地组策略对象 (GPO) 设置：

- 双向内容重定向
- 双向内容重定向覆盖
- OAuth 重定向

如果启用此设置，则在连接到已发布的应用程序或桌面时，客户端到 VDA 的设置将发送到客户端以配置双向内容重定向。

配置(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/bidirectional-content-redirection-configuration.png)

如果配置此设置，它将优先于 Web Studio 和客户端上的旧版设置。Citrix® 建议仅使用新的策略设置并删除任何旧版设置，以避免意外行为。

如果 VDA 和 DDC 运行的是 2311 或更高版本，则不得设置客户端策略。否则，客户端策略将从 Citrix Workspace app 组策略对象管理模板中设置。

Citrix 提供主机到客户端重定向和本地应用程序访问以实现客户端到 URL 重定向。但是，Citrix 建议您对已加入域的 Windows 客户端使用双向内容重定向。

Citrix 建议使用 Web Studio 中的新 UI 来配置此功能。

通配符重定向

双向内容重定向支持在定义要重定向的 URL 时使用通配符。有关更多详细信息以及如何配置双向内容重定向，请参阅配置说明。 在 Web Studio 中，通过编辑 JSON 字符串作为 `hostToClientUrls` 数组或 `clientToHostUrls` 数组中 `url` 键的值来设置通配符 URL。

> **注意：**

- 不要在 `hostToClientUrls` 和 `clientToHostUrls` 中设置相同的 URL，以避免无限循环。
- 不支持顶级域。例如，`<https://www.citrix.*>` 或 `<http://www.citrix.co*>` 不会被重定向。

双向内容重定向配置

将此策略设置为 `Enabled` 以开始配置此功能，然后单击 **管理 URL**。设置以下配置：

- **VDA 到客户端重定向**
- **客户端到 VDA 重定向**

VDA 到客户端重定向

要将 URL 从 VDA 重定向到客户端，请每行输入一个 URL。允许使用通配符。 OAuth 重定向使您能够使用客户端端点上的浏览器执行身份验证并将令牌发送回 VDA。

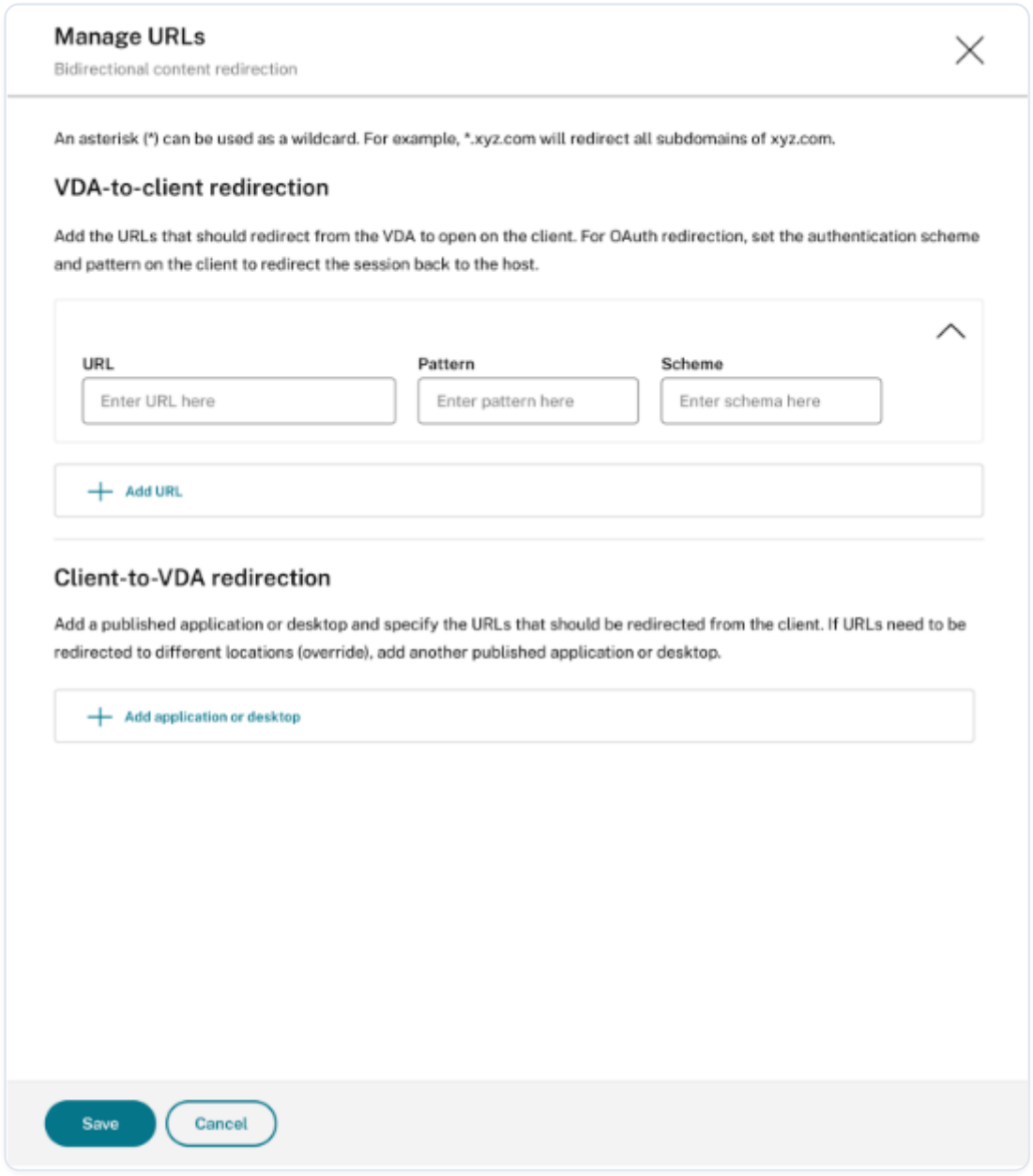
优点：

- 您可以避免将这些凭据存储在托管环境中。
- 您可以使用端点上而非 VDA 上可用的生物识别功能。

配置：

要为 URL 配置 VDA 到客户端重定向，请指定以下内容：

- **URL**（必填）添加必须从 VDA 重定向到客户端打开的 URL。对于 **OAuth 重定向**，请在客户端上设置身份验证方案和模式，以将会话重定向回主机。
- **模式**：（可选）URL 正则表达式，当通过 VDA 到客户端 URL 重定向到客户端时，该表达式将被跟踪，就像 OAuth 身份验证流已开始一样；当流完成时（通过打开结果方案或重定向 URL 模式检测到），该结果 URL 将重定向回启动该流的主机 VDA。
- **方案**：（可选）如果指定了 **方案**，则终止 URL 预期为以下形式：`<scheme>`:// `<something>`。假设未指定方案（为空）。在这种情况下，原始结果 URL 模式将通过正则表达式捕获组（必须在模式中指定）从模式中提取，并且原始 URL 将被重写以使用 `citrix-oauth-redir://` 重定向 URL。当流完成时，原始重定向 URL 将重定向回主机 (VDA)。在这种情况下，任何 OAuth 授权服务器都必须配置为允许 `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` 重定向 URL。



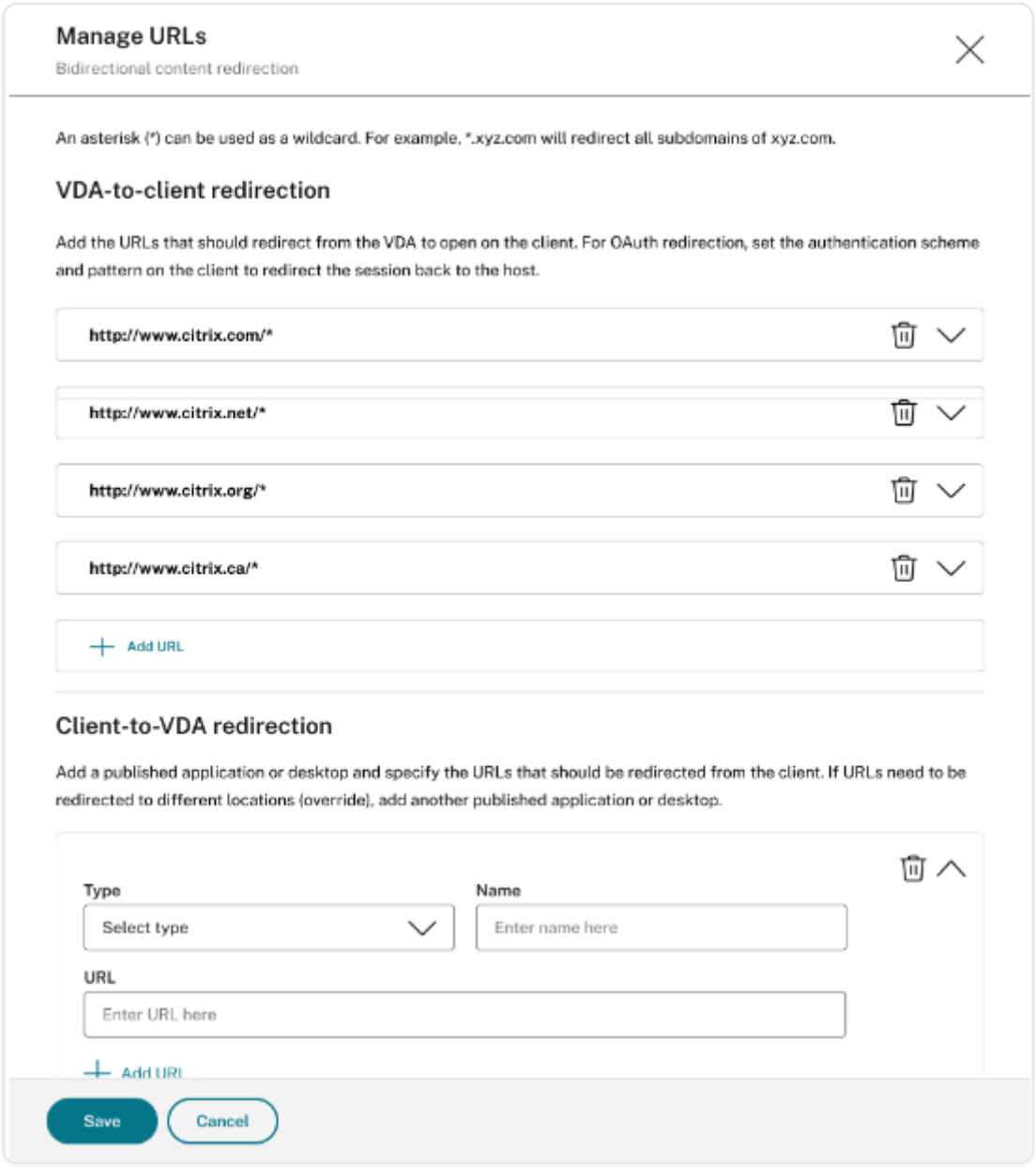
> **注意：**
>
> 尽管 **模式** 和 **方案** 都是可选的，但如果指定了 **模式**，则还必须指定 **方案**。

客户端到 VDA 重定向

要将 URL 从客户端重定向到 VDA，请完成以下步骤：

1. 配置客户端 URL 的目标。
2. 选择已发布的应用程序或已发布的桌面。
3. 指定该资源的名称。

4. 添加所有必须重定向到该资源的 URL。 您可以通过添加新的应用程序或桌面，然后指定要重定向到该资源的 URL 来覆盖此默认资源。



OAuth 重定向

OAuth 重定向使您能够使用客户端端点浏览器进行身份验证，并将令牌发送回 VDA。

优势：

- 您可以避免将这些凭据存储在托管环境中。
- 您可以使用端点上而非 VDA 上可用的生物识别功能。

要为 URL 配置 OAuth 重定向，请指定以下参数：

- **oAuthRedirectionPattern**：（可选）URL 正则表达式，当通过 VDA 到客户端 URL 重定向重定向到客户端时，该表达式会被跟踪，就像 OAuth 身份验证流程已开始一样；当流程完成（通过打开的结果方案或重定向 URL 模式检测到）时，该结果 URL 将重定向回启动该流程的主机 VDA。
- **oAuthScheme**：（可选）如果指定了方案 (Scheme)，则终止 URL 预期采用以下形式：`<scheme>`:// `<something>`。如果未指定方案（为空），则原始结果 URL 模式将通过正则表达式捕获组（必须在模式中指定）从模式中提取，并且原始 URL 将被重写以使用 `citrix-oauth-redir://` 重定向 URL。当流程完成时，原始重定向 URL 将重定向回主机 (VDA)。在这种情况下，任何 OAuth 授权服务器都必须配置为允许 `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` 重定向 URL。

对于客户端到 VDA 的重定向，为每个要重定向的资源创建 **clientToHostConfig**。 对于每个资源，请包含以下参数：

- **publishedAppOrDesktopNameType**：（必需）在 Web Studio 中配置的已发布桌面（“Desktop”）或已发布应用程序（“Application”）。如果资源无效，重定向将无法正常工作。
- **publishedAppOrDesktopName**：（必需）在 Web Studio 中配置的资源名称。
- **clientToHostUrls**：（必需）要从客户端重定向到主机 (VDA) 的 URL 列表。允许使用通配符。

已知限制

当您使用 PowerShell 启动带有自定义 URL 方案（非 HTTP 或 HTTPS）的浏览器时，自定义 URL 不会重定向到客户端。

浏览器内容重定向策略设置

浏览器内容重定向 (BCR) 增强了在 Citrix Virtual Apps and Desktops™ 环境中网页浏览的用户体验。通过将网页渲染卸载到用户的本地计算机，BCR 减少了服务器负载并提高了性能，尤其是对于复杂或资源密集型网站。 本文档详细介绍了浏览器内容重定向的每个可用策略设置选项。

浏览器内容重定向

此设置充当浏览器内容重定向的主开关。

- **作用：** 确定网页是在服务器上还是在本地设备上呈现。启用后，Citrix Workspace™ 应用程序会尝试在您的设备上获取并显示网页内容，以获得更流畅的体验。如果失败，它会回退到在服务器上呈现。
- **选项：**
  - **允许：** （默认）启用浏览器内容重定向。
  - **禁止：** 禁用浏览器内容重定向。

- **注意事项：** 如果允许，Citrix Workspace 应用程序会尝试客户端获取和客户端渲染。如果客户端获取和客户端渲染失败，浏览器内容重定向将回退到服务器端渲染。要启用服务器获取和客户端渲染，请启用“浏览器内容重定向代理配置”设置。

浏览器内容重定向 ACL 配置

此设置允许您创建允许或不允许使用浏览器内容重定向的网站（URL）列表。

- **作用：** 让您可以精细控制哪些网站通过浏览器内容重定向进行优化。您可以指定整个网站或特定页面。
- **工作原理：**
  - **允许的 URL：** 此列表中的网站内容将显示在您的设备上。您可以使用通配符 () *来包含多个页面或子域（例如，* `<https://www.example.com/>` 或 `<http://*.example.com/>`）。URL 的协议中不允许使用通配符。
- **默认：** `<https://www.youtube.com/*>`
- **示例：**
  - **允许的模式：** <http://www.xyz.com/index.html, `<https://www.xyz.com/*>` , `<http://www.xyz.com/*videos>` *> , `<http://*.xyz.com/<>` >
  - **不允许：** `<http://*.*.com/>`
  - 通过在 URL 中指定路径，可以实现更精细的控制。例如，如果您指定 `<https://www.xyz.com/sports/index.html>`，则只有 index.html 页面会被重定向

浏览器内容重定向阻止列表配置

此设置与“浏览器内容重定向 ACL 配置”设置结合使用。

- **作用：** 即使在 ACL 配置中允许，它也提供额外的控制层，允许您阻止特定的网站或页面。阻止列表具有优先权。
- **工作原理：** 您可以指定不希望重定向到设备的网站或页面，即使这些网站或页面通常由 ACL 配置允许。
- **默认值：** 未配置 URL
- **通配符：** 与 ACL 配置类似，您可以使用通配符 (*) 来阻止多个页面或子域。
- **示例：** 要仅阻止网站上的 index.html 页面，您将输入：`<https://www.example.com/sports/index.html>`

浏览器内容重定向身份验证站点

此设置允许您管理浏览器内容重定向如何与使用外部身份提供程序 (IdP) 进行登录的网站配合使用。

- **作用：** 确保浏览器内容重定向保持活动状态，即使您被重定向到不同的网站进行身份验证（例如当网站使用 Okta 或其他服务进行登录时）。
- **工作原理：** 您将身份验证网站的 URL 添加到此列表，以便在登录过程中不会中断重定向过程。
- **默认值：** 未配置 URL
- **示例：** 如果 www.example.com 使用 www.example.okta.com 进行身份验证，您将把 www.example.com/ 添加到浏览器内容重定向 ACL 配置中，并将身份验证网站 www.example.okta.com 添加到浏览器内容重定向身份验证站点中。
- **更多信息：** 有关详细信息，请参阅 Citrix 知识中心文章 CTX238236 和浏览器内容重定向中的多媒体部分。

浏览器内容重定向代理配置

此设置让您可以更好地控制浏览器内容重定向如何使用网络的代理服务器，并有助于在您的环境不允许客户端提取客户端渲染的情况下实现服务器提取客户端渲染。

- **作用：** 强制 Citrix Workspace 应用程序使用服务器提取方法来提取 Web 内容。启用后，它总是尝试从服务器提取内容并将其显示在您的设备上。
- **选项：**
  - 显式代理：使用特定的代理服务器。您需要提供代理服务器的地址和端口号（例如，`<http://proxy.example.com:80>`）
    - 允许的模式：
    - http://<hostname/ip address\>:\<port\> | 示例：`<http://proxy.example.citrix.com:80>` `<http://10.10.10.10:8080>`
  - PAC/WPAD：使用 PAC 文件或 WPAD 自动确定代理设置。您需要提供 PAC 文件的 URL（例如，`<http://wpad.myproxy.com:30/configuration/pac/Proxy.pac>`）。
    - PAC/WPAD 文件允许的模式：
    - http://<hostname/ip address\>:<port\>/<path\>/<Proxy\>.pac | 示例：`<http://wpad.myproxy.com:30/configuration/pac/Proxy.pac>`
    - https://<hostname/ip address\>:<port\>/<path\>/<wpad.dat\> | 示例：`<http://10.10.10.10/configuration/pac/wpad.dat>`
  - 直接/透明：不使用代理服务器，或使用透明代理。
    - 配置关键字“DIRECT”
    - 该关键字区分大小写

- **默认值：** 禁止 (已禁用)

浏览器内容重定向集成 Windows 身份验证支持

此设置简化了对使用集成 Windows 身份验证 (IWA) 的网站的登录。

- **作用：** 允许浏览器内容重定向使用您现有的 Windows 凭据自动登录网站。这意味着您无需重复输入用户名和密码。
- **选项：**
  - **允许：** 为使用 IWA 的网站启用单点登录 (SSO)。
  - **禁止：** (默认) 禁用 SSO，要求您每次都输入凭据。

浏览器内容重定向服务器获取代理身份验证

此设置控制浏览器内容重定向在从服务器获取内容时如何与您的 Web 代理交互。

- **作用：** 允许浏览器内容重定向使用您的 Windows 凭据向代理服务器进行身份验证，从而确保对 Web 内容的安全访问。
- **工作原理：** 启用后，浏览器内容重定向将自动获取并使用 Kerberos 服务票证向代理进行身份验证。
- **要求：** 您需要配置 PAC 文件以通过下游 Web 代理路由流量，并将代理设置为使用 Kerberos 身份验证。
- **选项：**
  - **允许：** 启用与代理服务器的 Kerberos 身份验证。
  - **禁止：** (默认) 浏览器内容重定向将使用基本身份验证或其他可用凭据向代理进行身份验证。

客户端传感器策略设置

客户端传感器部分包含用于控制如何在用户会话中处理移动设备传感器信息的策略设置。

允许应用程序使用客户端设备的物理位置

此设置确定在移动设备会话中运行的应用程序是否允许使用用户设备的物理位置。

默认情况下，禁止使用位置信息

当此设置被禁止时，应用程序尝试检索位置信息将返回“权限被拒绝”值。

当此设置被允许时，用户可以通过拒绝 Citrix Workspace™ 应用程序访问位置的请求来禁止使用位置信息。Android 和 iOS 设备会在每个会话中首次请求位置信息时进行提示。

在开发使用“允许应用程序使用客户端设备的物理位置”设置的托管应用程序时，请考虑以下事项：

- 确保支持位置功能的应用程序不依赖于位置信息的可用性，因为：
  - 用户可能不允许访问位置信息。
  - 在应用程序运行期间，位置可能不可用或可能发生变化。
  - 用户可能从不支持位置信息的不同设备连接到应用程序会话。
- 支持位置功能的应用程序必须：
  - 默认情况下关闭位置功能。
  - 在应用程序运行期间，向用户提供一个允许或禁止该功能的选项。
  - 为用户提供清除应用程序缓存的位置数据的选项。（Citrix Workspace 应用程序不缓存位置数据。）
- 启用位置功能的应用程序必须管理位置信息的粒度。这种管理可确保所获取的数据与应用程序的用途相符。此外，还应符合所有相关司法管辖区的法规。
- 使用位置服务时，强制实施安全连接（例如，使用 TLS 或 VPN）。将 Citrix Workspace 应用程序连接到受信任的服务器。
- 考虑就位置服务的使用征求法律意见。

桌面用户界面策略设置

“**桌面用户界面**”部分包含控制视觉效果（例如桌面壁纸、菜单动画和拖动图像）的策略设置。这些策略设置有助于管理客户端连接中使用的带宽。通过限制带宽使用，可以提高 WAN 上的应用程序性能。

> **重要提示：**
>
> 此版本不支持传统图形模式和桌面窗口管理器重定向 (DCR)。此策略仅在以下情况下用于向后兼容：
>
> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - 以前的 VDA 版本（与 Windows 7 和 Windows 2008 R2 配合使用）。

桌面窗口管理器重定向

此设置指定是否使用以下各项的处理能力进行本地 DirectX 图形渲染，以便为用户提供更流畅的 Windows 桌面体验：

- 用户设备上的图形处理单元 (GPU)
- 或者，
- 用户设备上的集成图形处理器 (IGP)

启用后，**桌面窗口管理器重定向**可提供高响应的 Windows 体验，同时保持服务器上的高可扩展性。

默认情况下，**桌面窗口管理器重定向**处于禁用状态。

要取消选择**桌面窗口管理器重定向**并减少用户会话中所需的带宽，请在将此设置添加到策略时选择**已禁用**。

桌面窗口管理器重定向图形质量

此设置指定用于桌面窗口管理器重定向的图形质量。

默认值为“高”。

从“高”、“中”、“低”或“无损”质量中选择。

桌面壁纸

此设置允许或阻止在用户会话中显示壁纸。

默认情况下，用户会话可以显示壁纸。

要取消选择桌面壁纸并减少用户会话所需的带宽，请在将此设置添加到策略时选择“**禁止**”。

菜单动画

此设置允许或阻止在用户会话中显示菜单动画。

默认情况下，允许菜单动画。

菜单动画是 Microsoft 个人偏好设置，旨在方便访问。启用后，它会导致菜单在短时间延迟后出现，可以通过滚动或淡入方式显示。菜单底部会出现一个箭头图标。当您指向该箭头时，菜单就会出现。

如果此策略设置设置为“**允许**”并且菜单动画 Microsoft 个人偏好设置已启用，则桌面会启用菜单动画。

> **注意：**

> 菜单动画 Microsoft 个人偏好设置的更改会影响桌面。请考虑将桌面设置为在会话结束时丢弃更改。在这种情况下，已启用菜单动画的用户在后续会话中可能没有菜单动画。对于需要菜单动画的用户，请在桌面的主映像中启用 Microsoft 设置，或确保桌面保留用户更改。

拖动时查看窗口内容

此设置允许或阻止在屏幕上拖动窗口时显示窗口内容。

默认情况下，允许查看窗口内容。

设置为 **允许** 时，拖动时整个窗口会随之移动。设置为 **禁止** 时，只有窗口轮廓会随之移动，直到您释放它。

最终用户监控策略设置

最终用户监控部分包含用于衡量会话流量的策略设置。

端点位置数据收集

默认情况下，此策略处于禁用状态。 启用后，将收集端点位置数据，包括端点设备的公共 IP 地址、国家/地区、城市和互联网服务提供商 (ISP)。 收集的数据将显示在 Citrix Director 或 Monitor 中，位于所选用户会话的**会话性能**选项卡下。

端点网络延迟测量间隔

默认情况下，此策略处于禁用状态。 此设置指定端点测量网络延迟的频率（以秒为单位）。 启用后，收集的数据将显示在 Citrix Director 或 Monitor 中，位于所选用户会话的**会话性能**选项卡下。

端点统计间隔

网络接口类型、信号强度、链接速度、传出吞吐量、传入吞吐量等端点统计信息可在 Director 或 Monitor UI 的会话拓扑中作为端点遥测数据提供。此遥测数据有助于排查最终用户会话问题。 端点统计信息间隔表示在 Director 或 Monitor UI 的会话拓扑中刷新端点遥测数据的频率（以秒为单位）。默认情况下，端点遥测功能已启用，并每 60 秒刷新一次。 收集的数据将显示在 Citrix Director 或 Monitor 中，位于所选用户会话的**会话性能**选项卡下。

ICA® 往返计算

此设置确定是否对活动连接执行 ICA 往返计算。

默认情况下，已启用活动连接的计算。

默认情况下，每个 ICA 往返测量启动都会延迟。此延迟会持续到出现指示用户交互的某些流量为止。此延迟的长度可能不确定，旨在防止 ICA 往返测量成为 ICA 流量的唯一原因。

ICA 往返计算间隔

此设置指定执行 ICA 往返计算的频率（以秒为单位）。

默认情况下，每 15 秒计算一次 ICA 往返。

空闲连接的 ICA 往返计算

此设置确定是否对空闲连接执行 ICA 往返计算。

默认情况下，不对空闲连接执行计算。

默认情况下，每个 ICA 往返测量启动都会延迟。此延迟会持续到出现指示用户交互的某些流量为止。此延迟的长度可能不确定，旨在防止 ICA 往返测量成为 ICA 流量的唯一原因。

增强桌面体验策略设置

增强桌面体验策略设置在服务器操作系统上运行会话，这些会话看起来像本地 Windows 7 桌面。

默认情况下，此设置是允许的。

如果虚拟桌面上存在带有 Windows 经典主题的用户配置文件，则此策略不会为该用户提供增强的桌面体验。假设一个用户使用 Windows 7 主题用户配置文件登录到运行 Windows Server 2012 的虚拟桌面。此外，此策略未配置或已禁用。在这种情况下，该用户会看到一条错误消息，指示无法应用主题。

在这两种情况下，重置用户配置文件都可以解决此问题。

如果您在具有活动用户会话的虚拟桌面上禁用此策略，则这些会话的界面在 Windows 7 和 Windows 经典桌面上会变得不一致。为避免这种不一致，请确保在更改此策略设置后重新启动虚拟桌面。然后删除虚拟桌面上的任何漫游配置文件。Citrix® 还建议删除虚拟桌面上的任何其他用户配置文件，以避免配置文件之间出现不一致。

假设您的环境中正在使用漫游用户配置文件。在这种情况下，请确保为所有共享配置文件的虚拟桌面启用或禁用增强桌面体验功能。

Citrix 不建议在运行服务器操作系统和客户端操作系统的虚拟桌面之间共享漫游配置文件。客户端和服务器操作系统的配置文件不同。在这两种类型之间共享漫游配置文件可能导致用户在两者之间移动时配置文件属性不一致。

文件重定向策略设置

“**文件重定向**”部分包含与客户端驱动器映射和客户端驱动器优化相关的策略设置。

自动连接客户端驱动器

此设置允许或阻止用户登录时自动连接客户端驱动器。

默认情况下，允许自动连接。

将此设置添加到策略时，请确保启用要自动连接的驱动器类型的设置。例如，要允许自动连接用户的 CD-ROM 驱动器，请配置此设置和“**客户端光驱**”设置。

以下策略设置相关：

- **客户端驱动器重定向**
- **客户端软盘驱动器**
- **客户端光驱**
- **客户端固定驱动器**
- **客户端网络驱动器**
- **客户端可移动驱动器**

客户端驱动器重定向

此设置启用或禁用用户设备上驱动器之间的文件重定向。

默认情况下，文件重定向已启用。

> **注意：**
>
> 客户端驱动器重定向策略设置不适用于使用通用 USB 重定向映射到会话的驱动器。

> 启用后，用户可以将文件保存到其所有客户端驱动器。禁用后，将阻止所有文件重定向。此配置适用于所有文件重定向设置，无论其状态如何。单独的文件重定向设置包括客户端软盘驱动器和客户端网络驱动器。

以下策略设置相关：

- **客户端软盘驱动器**
- **客户端光驱**
- **客户端固定驱动器**
- **客户端网络驱动器**
- **客户端可移动驱动器**

客户端固定驱动器

此设置允许或阻止用户访问或将文件保存到用户设备上的固定驱动器。

默认情况下，允许访问客户端固定驱动器。

将此设置添加到策略时，请确保“**客户端驱动器重定向**”设置存在并设置为“允许”。如果这些设置被禁用，则不会映射客户端固定驱动器，并且用户无法手动访问这些驱动器，无论“**客户端固定驱动器**”设置的状态如何。

配置“**自动连接客户端驱动器**”设置，以确保用户登录时自动连接固定驱动器。

客户端软盘驱动器

此设置允许或阻止用户访问或将文件保存到用户设备上的软盘驱动器。

默认情况下，允许访问客户端软盘驱动器。

将此设置添加到策略时，请确保“**客户端驱动器重定向**”设置存在并设置为“允许”。如果这些设置被禁用，客户端软盘驱动器将不会被映射，并且用户无法手动访问这些驱动器，无论“**客户端软盘驱动器**”设置的状态如何。

为确保用户登录时软盘驱动器自动连接，请配置“**自动连接客户端驱动器**”设置。

客户端网络驱动器

此设置允许或阻止用户通过用户设备访问文件并将其保存到网络（远程）驱动器。

默认情况下，允许访问客户端网络驱动器。

将此设置添加到策略时，请确保“**客户端驱动器重定向**”设置存在并设置为“允许”。如果这些设置被禁用，客户端网络驱动器将不会被映射，并且用户无法手动访问这些驱动器。无论“**客户端网络驱动器**”设置的状态如何，此配置都适用。

为确保用户登录时网络驱动器自动连接，请配置“**自动连接客户端驱动器**”设置。

客户端光驱

此设置允许或阻止用户访问文件或将其保存到以下位置：

- 用户设备上的 CD-ROM
- 用户设备上的 DVD-ROM
- 用户设备上的 BD-ROM 驱动器。

默认情况下，允许访问客户端光驱。

将此设置添加到策略时，请确保“**客户端驱动器重定向**”设置存在并设置为“**允许**”。如果这些设置被禁用，客户端光驱将不会被映射，并且用户无法手动访问这些驱动器。无论“**客户端光驱**”设置的状态如何，此配置都适用。

为确保用户登录时光驱自动连接，请配置“**自动连接客户端驱动器**”设置。

客户端可移动驱动器

此设置允许或阻止用户访问文件或将其保存到用户设备上的 USB 驱动器。

默认情况下，允许访问客户端可移动驱动器。

将此设置添加到策略时，请验证“**客户端驱动器重定向**”设置是否存在并设置为“允许”。如果这些设置被禁用，客户端可移动驱动器将不会被映射，并且用户无法手动访问这些驱动器。无论“**客户端可移动驱动器**”设置的状态如何，此配置都适用。

配置“**自动连接客户端驱动器**”设置，以确保用户登录时自动连接可移动驱动器。

主机到客户端重定向

此设置启用或禁用文件类型关联，以便在用户设备上打开 URL 和某些媒体内容。禁用时，内容将在服务器上打开。

默认情况下，文件类型关联处于禁用状态。

启用此设置后，以下 URL 类型将在本地打开：

- HTTP
- HTTPS
- 瑞尔播放器 和 QuickTime (RTSP)
- 瑞尔播放器 和 QuickTime (RTSPU)
- 旧版 Real Player (PNM)
- 微软媒体服务器 (MMS)

保留客户端驱动器盘符

此设置启用或禁用客户端驱动器映射到会话中的相同驱动器盘符。

默认情况下，不保留客户端驱动器盘符。

将此设置添加到策略时，请确保“**客户端驱动器重定向**”设置存在并设置为“允许”。

只读客户端驱动器访问

此设置允许或阻止用户和应用程序执行以下操作：

- 在映射的客户端驱动器上创建文件
- 更改映射客户端驱动器上的文件
- 更改映射客户端驱动器上的文件夹

默认情况下，可以更改映射客户端驱动器上的文件和文件夹。

如果设置为“已启用”，则文件和文件夹将以只读权限访问。

将此设置添加到策略时，请确保存在**客户端驱动器重定向**设置并将其设置为“允许”。

特殊文件夹重定向

此设置允许或阻止 Citrix Workspace™ 应用程序和 Web Interface 用户从会话中查看其本地“文档”和“桌面”特殊文件夹。

默认情况下，允许特殊文件夹重定向。

此设置可防止通过策略筛选的任何对象进行特殊文件夹重定向，无论其他位置存在的设置如何。当此设置被禁止时，为 StoreFront™、Web Interface 或 Citrix Workspace 应用程序指定的任何相关设置都将被忽略。

要定义哪些用户可以进行特殊文件夹重定向，请选择“**允许**”，并将此设置包含在针对您希望拥有此功能的用户进行筛选的策略中。此设置将覆盖所有其他特殊文件夹重定向设置。

阻止用户访问或将文件保存到其本地硬盘驱动器的策略设置也会阻止特殊文件夹重定向工作。出现这种情况是因为特殊文件夹重定向必须与用户设备进行交互。

将此设置添加到策略时，请确保存在**客户端固定驱动器**设置并将其设置为“允许”。

文件传输策略

默认情况下，文件传输处于启用状态。使用 Web Studio 更改这些策略，这些策略位于“**用户设置 - ICA\文件重定向**”下。使用文件传输策略时，请考虑以下事项：

- **适用于 Chrome OS/HTML5 的 Citrix Workspace 应用程序的文件传输** - 允许或阻止用户在 Citrix Virtual Apps and Desktops 会话与其设备之间传输文件。
- **适用于 Chrome OS/HTML5 的 Citrix Workspace 应用程序的文件上传** - 允许或阻止用户将其设备中的文件上传到 Citrix Virtual Apps and Desktops 会话。
- **适用于 Chrome OS/HTML5 的 Citrix Workspace 应用程序的文件下载** - 允许或阻止用户将文件从 Citrix Virtual Apps and Desktops 会话下载到其设备。

> **注意：**

> 文件传输策略仅适用于适用于 HTML5 的 Citrix Workspace 应用程序和适用于 Chrome OS 的 Citrix Workspace 应用程序。

使用异步写入

此设置启用或禁用异步磁盘写入。

默认情况下，异步写入处于禁用状态。

异步磁盘写入可以提高通过 WAN 进行文件传输和写入客户端磁盘的速度，WAN 通常具有相对较高的带宽和高延迟。但是，如果出现连接或磁盘故障，正在写入的客户端文件可能会处于未定义状态。如果出现此未定义状态，将弹出一个窗口通知用户受影响的文件。然后，用户可以采取补救措施，例如在重新连接时或磁盘故障得到纠正时重新启动中断的文件传输。

Citrix® 建议仅对需要远程连接且具有良好文件访问速度的用户启用异步磁盘写入。并且这些用户在连接或磁盘故障时可以轻松恢复丢失的文件或数据。

将此设置添加到策略时，请验证是否存在 **客户端驱动器重定向** 设置并将其设置为“允许”。如果此设置被禁用，则不会发生异步写入。

剪贴板重定向

剪贴板重定向是 Citrix Virtual Apps and Desktops™ 中的一项基本功能，可实现用户本地端点与其虚拟 Citrix 会话之间数据的无缝复制和粘贴。

剪贴板重定向允许用户在其本地设备上运行的应用程序与 Citrix 会话中的应用程序之间复制和粘贴数据，例如文本、图像和文件。这是通过将用户设备上的剪贴板映射到 VDA 上的剪贴板来实现的。默认情况下，允许剪贴板重定向。

剪贴板重定向通过 HDX™ 协议中的独立虚拟通道工作。额外的虚拟通道用于文件传输和拖放。当用户在其本地设备上复制数据时，Citrix Workspace™ 应用程序会拦截数据，并使其可用于粘贴到会话中运行的应用程序。实际数据将在数据粘贴到 VDA 上的应用程序时进行传输。从 Citrix 会话复制到客户端时，此过程反向工作。

这种从客户端到会话以及从会话到客户端的剪贴板重定向组合也称为双向剪贴板重定向。

> **注意：**

> 更多信息请参阅，Citrix Virtual Channels

关键概念

客户端到会话，也称为端点到会话或客户端到 VDA。在用户本地设备上复制（放置在剪贴板上）的数据可用于粘贴到虚拟会话中。

会话到客户端，也称为会话到端点或 VDA 到客户端）。从虚拟会话中的应用程序复制的数据可用于粘贴到用户的本地设备上。

跨会话（会话到会话或 VDA 到 VDA）。一种新的剪贴板传输方法，其中从一个 Citrix 会话复制的数据可以粘贴到另一个 Citrix 会话中，而无需存储在本地端点的剪贴板上。此功能在 Citrix Virtual Apps and Desktops™ 2507 版本中作为预览功能提供，被称为跨会话剪贴板交换功能。有关更多信息，请参阅“跨会话剪贴板”。

配置

剪贴板重定向通过 Citrix® 策略进行控制。这些策略提供了一系列设置，用于微调剪贴板重定向行为。

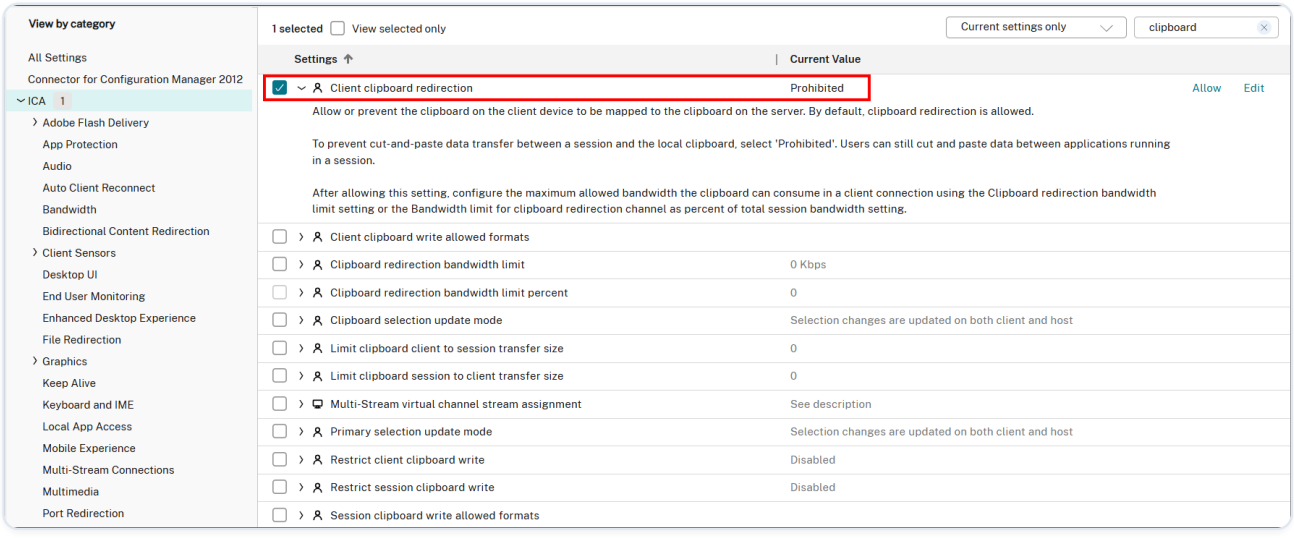
默认情况下，双向剪贴板重定向已启用：用户可以将其 Citrix 会话中的数据复制并粘贴到其本地端点，反之亦然。

核心设置

核心剪贴板重定向配置是“客户端剪贴板重定向策略”。此策略控制是否允许剪贴板重定向。默认情况下，剪贴板重定向是允许的。

禁用剪贴板重定向可以防止敏感数据意外或恶意传输到 Citrix 虚拟环境之外，从而提高安全性。它还有助于防止通过剪贴板将潜在有害数据引入 Citrix 环境。但是，这可能会对最终用户体验产生负面影响。

要禁止剪贴板重定向，请将“客户端剪贴板重定向策略”设置为“禁止”：



如果设置为“禁止”，剪贴板重定向将完全禁用，并且所有其他与剪贴板相关的策略都将被忽略。

用户仍然可以在其 Citrix 会话内部和本地端点设备上运行的应用程序之间复制和粘贴数据；但是，无法从其 Citrix 会话复制和粘贴数据，也无法向其 Citrix 会话复制和粘贴数据。

定向剪贴板控制

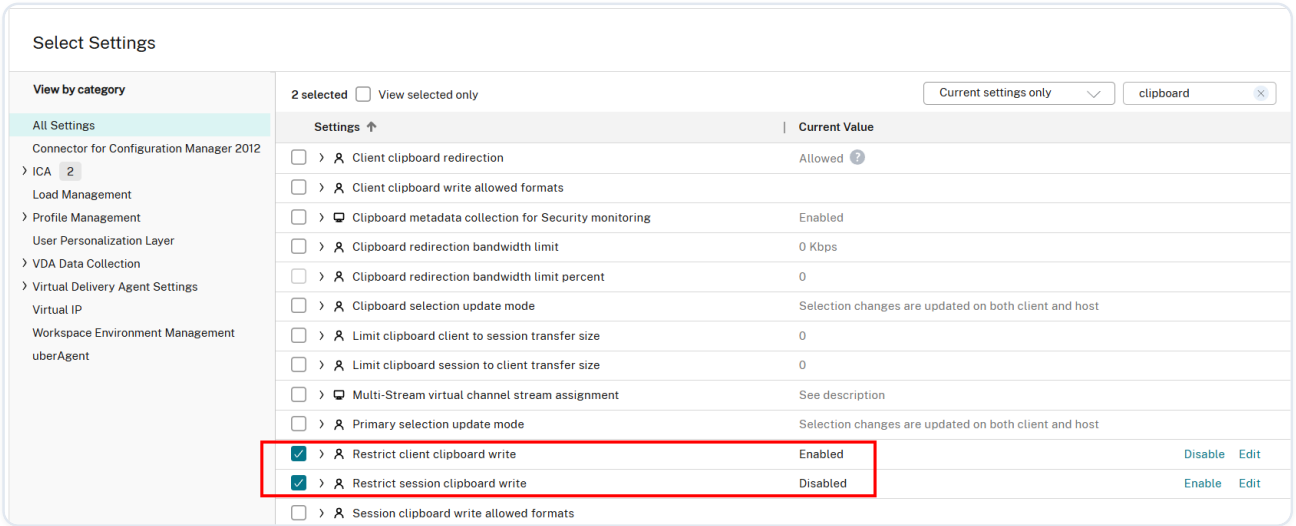
通过定向剪贴板控制，管理员可以对剪贴板数据流的方向进行精细控制。这也被称为单向剪贴板控制。

有两种主要的单向控制模式可用：

- **客户端到会话：** 在此配置中，使用“限制客户端剪贴板写入”策略，并且剪贴板数据被允许专门从用户的端点设备（客户端）流向远程 Citrix 会话。这意味着用户可以从其本地计算机复制信息并将其粘贴到 Citrix 会话中运行的应用程序中，但他们无法从 Citrix 会话复制数据并将其粘贴回其本地计算机。当从安全会话到控制较少的端点的数据泄露是一个重大问题时，此模式非常有用。
- **会话到客户端：** 在此配置中，“限制会话剪贴板写入策略”允许剪贴板数据专门从 Citrix 会话流向客户端设备。用户可以从远程会话中的应用程序复制信息并将其粘贴到其本地计算机上，但他们无法从其本地计算机复制数据并将其粘贴到 Citrix 会话中。当主要目标是防止潜在恶意或未经授权的数据从端点引入安全 Citrix 环境时，通常使用此设置。

下表描述了用于单向剪贴板控制的 Citrix 剪贴板策略：

剪贴板方向性	剪贴板策略
双向 - 会话到客户端和客户端到会话	客户端剪贴板重定向：已启用（默认）
单向 - 仅客户端到会话	客户端剪贴板重定向：已启用（默认）
限制客户端剪贴板写入：已启用	单向 - 仅会话到客户端
客户端剪贴板重定向：已启用（默认）	限制会话剪贴板写入：已启用



在上面的示例中，两个方向性剪贴板策略都已突出显示，在此配置中，仅允许客户端到会话的剪贴板重定向，因为“限制客户端剪贴板写入”设置已设置为“已启用”。

剪贴板格式控制

Citrix 剪贴板格式控制策略通过将数据传输限制为特定的剪贴板格式，从而控制会话与客户端之间以及反向复制和粘贴的数据类型，增强了剪贴板安全性。它可用于选择性地允许或拒绝某些剪贴板数据格式。

剪贴板交换格式用于在各种应用程序（从多媒体程序到复杂的电子表格和文字处理器）之间实现信息的无缝传输。这些格式定义了可复制、剪切和粘贴的数据的结构和编码，从而允许应用程序理解和处理交换的内容。

例如，当从 Web 浏览器复制文本并将其粘贴到 Word 文档中时，剪贴板会采用基于文本的格式。但是，如果复制的内容包含图像、表格或富文本格式，剪贴板将利用更复杂的格式（如 RTF（富文本格式）或 HTML（超文本标记语言））来保留原始外观和结构。同样，当在专用应用程序（例如 CAD 程序和演示工具）之间交换数据时，剪贴板可能会使用特定于应用程序的格式或常见的图元文件格式，以确保图形或复杂数据的准确表示。

剪贴板格式控制策略旨在与定向剪贴板控制策略结合使用。

借助剪贴板格式控制，管理员可以控制允许哪些格式，例如：

- 在两个方向上仅允许纯文本
- 仅允许会话到客户端的剪贴板传输纯文本和图像

或者，您可以限制从客户端粘贴到会话的格式，但允许所有格式从会话粘贴回客户端。

两个主要策略控制剪贴板格式的行为：

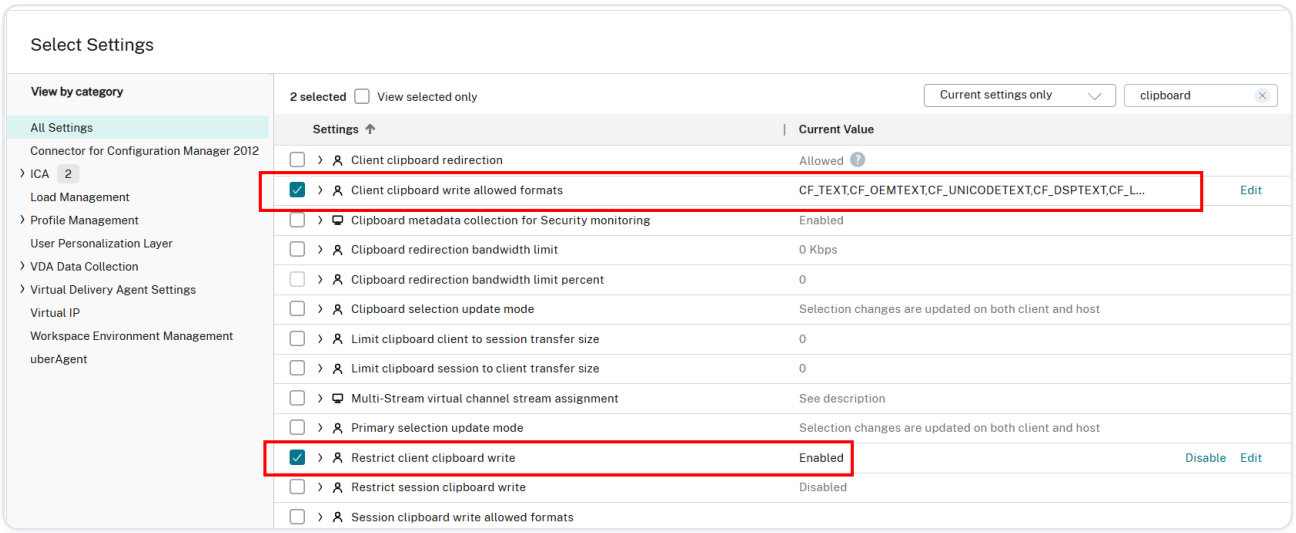
客户端剪贴板写入允许的格式： 此策略明确规定了允许从远程会话写入客户端剪贴板的剪贴板数据格式。例如，管理员可以配置此策略以仅允许将纯文本复制到客户端，从而防止传输可能包含恶意内容的富文本、图像或文件。

会话剪贴板写入允许的格式： 其次，此策略指定了允许从客户端复制到远程会话的剪贴板数据格式。此策略对于控制可以传输到远程环境中的信息类型至关重要。组织可能会将其限制为仅允许纯文本，从而防止用户无意或有意地将其本地计算机中的敏感文件或图像粘贴到安全性较低或未经授权的远程应用程序中。

> **注意：**

> 仅当相应的单向剪贴板策略也已设置时，才会评估剪贴板允许的格式。

> 要将客户端剪贴板写入格式限制为仅接受基于文本的数据格式，需要同时配置“限制客户端剪贴板写入”策略和“客户端剪贴板写入允许的格式”。在此示例中，“限制客户端剪贴板写入”需要设置为**已启用**，并且“客户端剪贴板写入允许的格式”需要包含所有剪贴板文本格式：



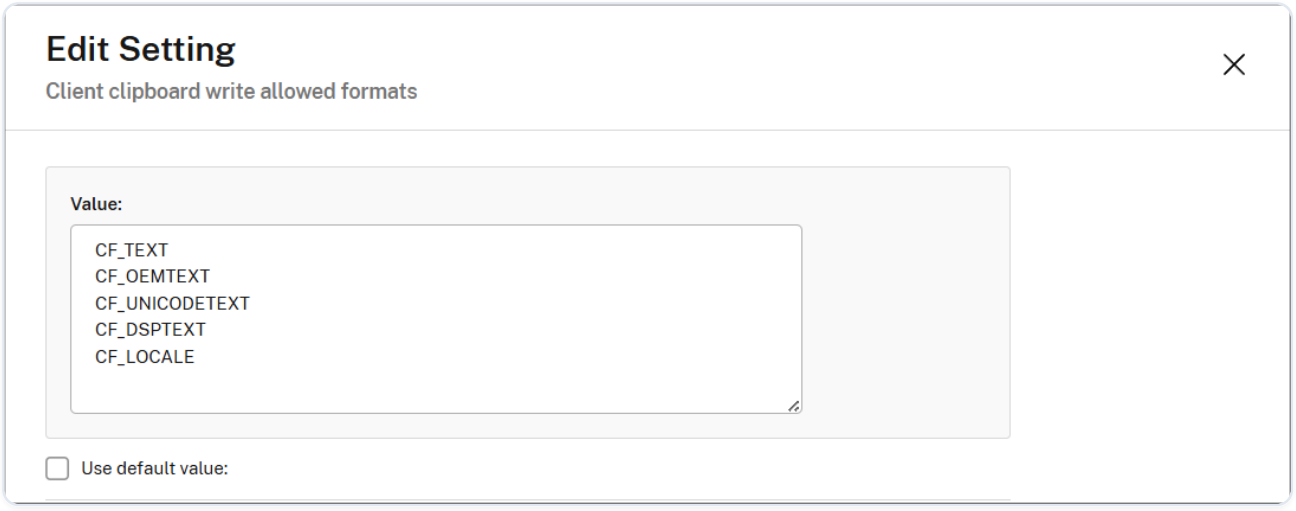
要配置写入格式限制，请编辑相应的策略并确保每个条目都放在单独的行上。

例如：

CF_TEXT CF_BITMAP

这是正确的，但以下是错误的：

CF_TEXT,CF_BITMAP



标准剪贴板数据格式

下表描述了标准剪贴板格式。

剪贴板格式	类型	描述
CF_TEXT	文本格式	标准 ANSI 字符集中的文本。每行以回车/换行符 (CR-LF) 组合结尾。
CF_OEMTEXT	文本格式	使用原始设备制造商 (OEM) 字符集的文本。类似于 CF_TEXT。
CF_UNICODETEXT	文本格式	Unicode 格式的文本。它不需要空终止符。
CF_LOCALE	文本格式	与剪贴板文本关联的区域设置标识符的句柄。这有助于正确解释文本的语言和区域设置。
CF_HTML*	文本格式	表示 HTML 格式的文本，允许在支持它的应用程序之间复制和粘贴富文本、链接和图像。
CF_BITMAP	图像格式	设备相关的位图。图像数据特定于某个输出设备。
CF_DIB	图像格式	设备无关位图。此格式包含颜色信息和尺寸，使其可以在任何设备上正确显示。
CF_DIBV5	图像格式	CF_DIB（设备无关位图，版本 5）的扩展，包含更高级的功能，例如颜色配置文件和用于透明度的 Alpha 通道。
CF_PALETTE	图像格式	颜色调色板的句柄。应用程序使用它来控制其他剪贴板数据的颜色，通常是位图。
CF_TIFF	图像格式	标记图像文件格式。一种常见的高质量图像格式，用于出版和摄影。
CF_METAFILEPIC	图元文件格式	图元文件图片结构的句柄。这是一种较旧的格式，用于存储

剪贴板格式	类型	描述
		GDI（图形设备接口）函数集合以重新创建图像。
CF_ENHMETAFILE**		增强型图元文件的句柄。这是 CF_METAFILEPICT 的更现代、更强大的版本，提供更好的图像质量和设备独立性。

注意：

- HTML 格式默认处于禁用状态。启用 HTML 格式剪贴板支持可能会带来安全风险。从网页复制内容时，任何嵌入式脚本也会被复制。如果此内容随后粘贴到呈现 HTML 的应用程序中，则脚本可能会被执行。启用此格式时请务必谨慎。
- 增强型图元文件剪贴板传输在 2511 版本之前的 Citrix Virtual Apps and Desktops™ 上不可用。 除了这些标准格式之外，Citrix® 还支持以下特定的剪贴板数据格式，例如数据交换格式和专用格式。

数据交换格式

剪贴板数据交换格式有助于在各种应用程序（例如多媒体程序或电子表格）之间传输数据。

剪贴板格式	描述
CF_SYLK	符号链接格式。Microsoft 创建的一种较旧的格式，用于在 Microsoft Excel 等电子表格应用程序之间交换数据。
CF_DIF	数据交换格式。一种基于文本的格式，用于在电子表格程序之间交换数据。
CF_RIFF	资源交换文件格式。一种用于存储多媒体数据（例如音频和视频）的容器格式。
CF_WAVE	波形音频格式。表示音频数据。

特殊和系统格式

这些格式用于特殊目的，例如处理文件拖放、私有数据或自定义渲染。

剪贴板格式	描述
CF_HDROP	已拖放文件列表的句柄。这用于文件系统的拖放操作（例如，将文件拖放到应用程序窗口中）。
CF_PENDATA	表示来自笔或手写笔的数据，用于笔式计算应用程序。
CF_OWNERDISPLAY	一种格式，其中将数据放置在剪贴板上的原始窗口负责在剪贴板查看器中绘制和更新内容。

CF_DSPTEXT、CF_DSPBITMAP、CF_DSPMETAFILEPICT、CF_DISPENHMETAFILE 是“显示”格式，它们对应于标准格式（TEXT、BITMAP 等），但用于可在剪贴板查看器应用程序中渲染的私有数据。它们旨在用于特定于应用程序的用途。

Citrix Virtual Apps and Desktops™ 剪贴板格式

CFX 剪贴板格式是自定义的 Citrix Virtual Apps and Desktops™ 剪贴板格式。与常规剪贴板格式相比，这些格式经过高度优化。

剪贴板格式	描述
CFX_RICHTEXT	用于高效传输格式化文本，包括不同的字体、大小、颜色以及粗体或斜体等样式
CFX_OfficeDrawingShape	处理 Microsoft Office 绘图对象。它允许用户复制和粘贴在 Office 应用程序（例如 Word、Excel 或 PowerPoint）中创建的矢量图形、图表和其他图形
CFX_BIFF8	这对应于 BIFF8（二进制交换文件格式 8），它是 Microsoft Excel 97-2003 的本机文件格式。CFX_BIFF8 是 Citrix 优化版本，用于在 Excel 电子表格之间复制和粘贴数据和公式。
CFX_FILE*	用于文件对象传输。当您在本地计算机上复制文件并将其粘贴到虚拟桌面（反之亦然）时，此格式管理数据传输。它是标准 CF_HDROP 格式的优化替代方案

注意：

要允许文件复制粘贴和拖放，您必须明确将 CFX_FILE 添加到允许的格式中。

自定义剪贴板格式

除了这些剪贴板格式之外，您还可以配置其他自定义剪贴板格式。这仅适用于那些已在 VDA 上的操作系统中注册的格式。

有关详细信息，请参阅自定义注册的剪贴板格式。

可转换剪贴板格式

Microsoft Windows 原生支持不同的剪贴板格式。复制和粘贴剪贴板内容时，Windows 会自动尝试将剪贴板数据转换为其他兼容的剪贴板格式，从而更轻松地将内容粘贴到不同的应用程序中。

当数据格式发布到剪贴板时，Windows 会自动添加其他格式，这些格式可以通过从最初发布的任何格式转换而来，以增加成功粘贴到其他应用程序的可能性。

如果目标应用程序请求源无法直接提供的格式，Windows 将自动将剪贴板数据从一种格式转换为另一种格式。

例如，从文字处理器复制格式化文本时，Windows 会向请求应用程序提供其他格式，例如纯文本以及最初发布的格式化文本。

再举一个例子，如果剪贴板数据包含 CF_TEXT 剪贴板格式的纯文本数据，并且粘贴数据的应用程序请求 CF_UNICODETEXT 格式的 Unicode 文本，Windows 将在粘贴过程中自动转换剪贴板数据。

注意：

在某些转换中，信息可能会丢失，例如自动将富文本转换为纯文本。

剪贴板格式	描述
CF_TEXT	CF_TEXT
	CF_OEMTEXT
	CF_UNICODETEXT

剪贴板格式	描述
	CF_LOCALE
CF_BITMAP	CF_BITMAP
	CF_DIB
	CF_DIBV5
CF_METAFILEPICT	CF_METAFILEPICT
	CF_ENHMETAFILE
CF_OEMTEXT	CF_TEXT
	CF_OEMTEXT
	CF_UNICODETEXT
	CF_LOCALE
CF_DIB	CF_BITMAP
	CF_DIB
	CF_DIBV5
CF_UNICODETEXT	CF_TEXT
	CF_OEMTEXT
	CF_UNICODETEXT
	CF_LOCALE
CF_ENHMETAFILE	CF_METAFILEPICT
	CF_ENHMETAFILE
CF_DIBV5	CF_BITMAP
	CF_DIB

剪贴板格式	描述
	CF_DIBV5

注意：

剪贴板格式转换取决于 Windows 操作系统，此表可能会在未来的操作系统版本中发生变化。

重要的是要了解 Windows 剪贴板系统并非在所有格式之间自由转换。自动转换仅限于少数核心类型，主要是在不同的文本编码和位图变体之间进行。

对于大多数其他格式，当源应用程序一次将多种格式放置到剪贴板上时，即可实现兼容性。例如，当您从 Excel 复制图表时，它可能会将数据作为 Office 绘图形状 (CFX_OfficeDrawingShape)、增强型图元文件 (CF_ENHMETAFILE) 和简单位图 (CF_DIB) 放置。这不是剪贴板的转换，而是源应用程序为不同的粘贴场景提供多种表示形式。

剪贴板格式控制和可转换格式

在设计剪贴板格式控制策略和跨会话剪贴板配置时，应考虑可转换格式。例如，如果您想明确允许仅将基于文本的内容从客户端复制到剪贴板，则必须将所有基于文本的格式添加到“会话剪贴板写入允许的格式”策略中。在此示例中，您必须将以下格式添加到策略中：

CF_TEXT

CF_UNICODETEXT

CF_DSPTEXT

CF_LOCALE

CF_OEMTEXT

同样，如果您想在将这些类型的数据从一个会话复制到另一个会话时，通过跨会话传输所有文件格式，则需要将所有文件剪贴板格式添加到 CrossSessionFormats 配置中：

CFX_FILES

CFX_HFDROP

剪贴板传输大小限制

通过剪贴板传输大小限制，您可以设置在单个复制粘贴剪贴板操作中可以传输的数据大小限制。默认情况下，这些设置处于禁用状态，并且客户端到会话以及会话到客户端的剪贴板传输没有限制。

传输大小限制有助于带宽管理。大型剪贴板传输会消耗大量网络带宽，尤其是在有许多并发用户的环境中。通过设置限制，管理员可以确保所有用户获得更流畅的性能并防止网络拥塞。

不受限制的剪贴板传输可能会带来安全风险。恶意软件或未经授权的用户可能会将会话中的大量敏感数据复制到会话中或从会话中复制出来。限制传输大小可作为防止此类数据泄露的预防措施。

配置剪贴板传输大小限制时，管理员应考虑以下因素：

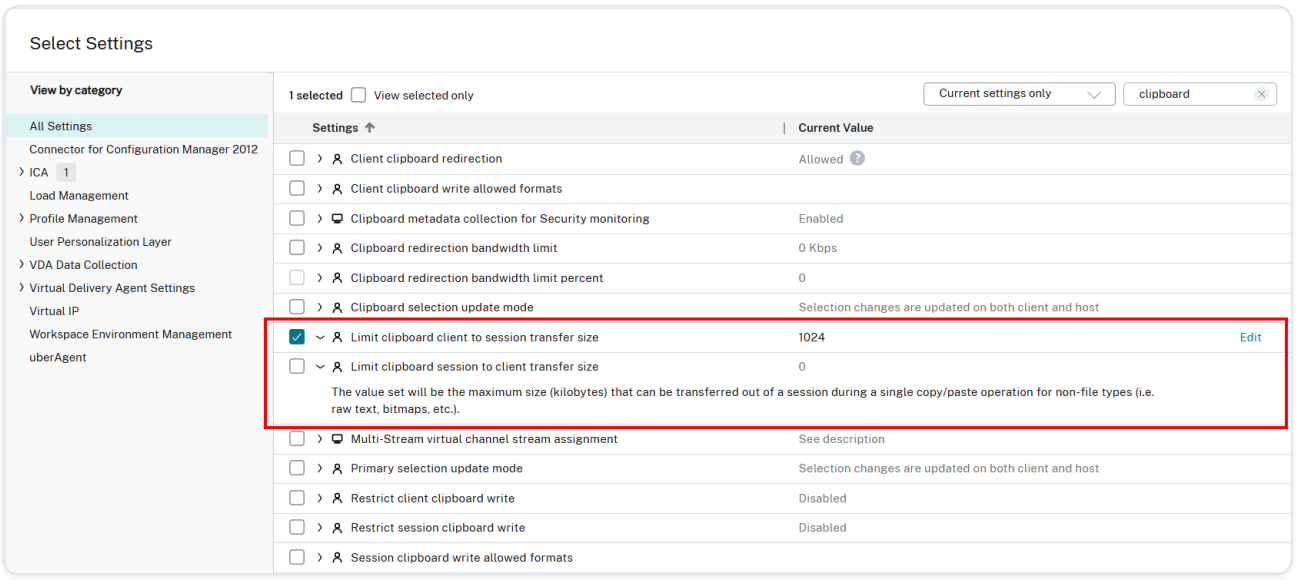
- 用户需求：用户的典型复制粘贴要求是什么？施加过于严格的限制可能会阻碍生产力。
- 带宽使用情况：可用的网络带宽是多少，预计有多少并发用户？
- 相关安全策略：组织的数据安全和合规性要求是什么？

两个主要设置提供了对剪贴板数据传输的精细控制：

限制剪贴板客户端到会话传输大小： 此设置配置可以从用户本地设备（客户端）复制并粘贴到远程会话（例如，虚拟桌面或无缝应用程序）中的最大数据大小（以千字节为单位）。

限制剪贴板会话到客户端传输大小： 其次，此设置控制可以从远程会话中复制并粘贴回用户本地设备的最大数据大小（以千字节为单位）。当用户在虚拟化环境中处理敏感数据并需要防止大量数据泄露到客户端时，这尤其重要。

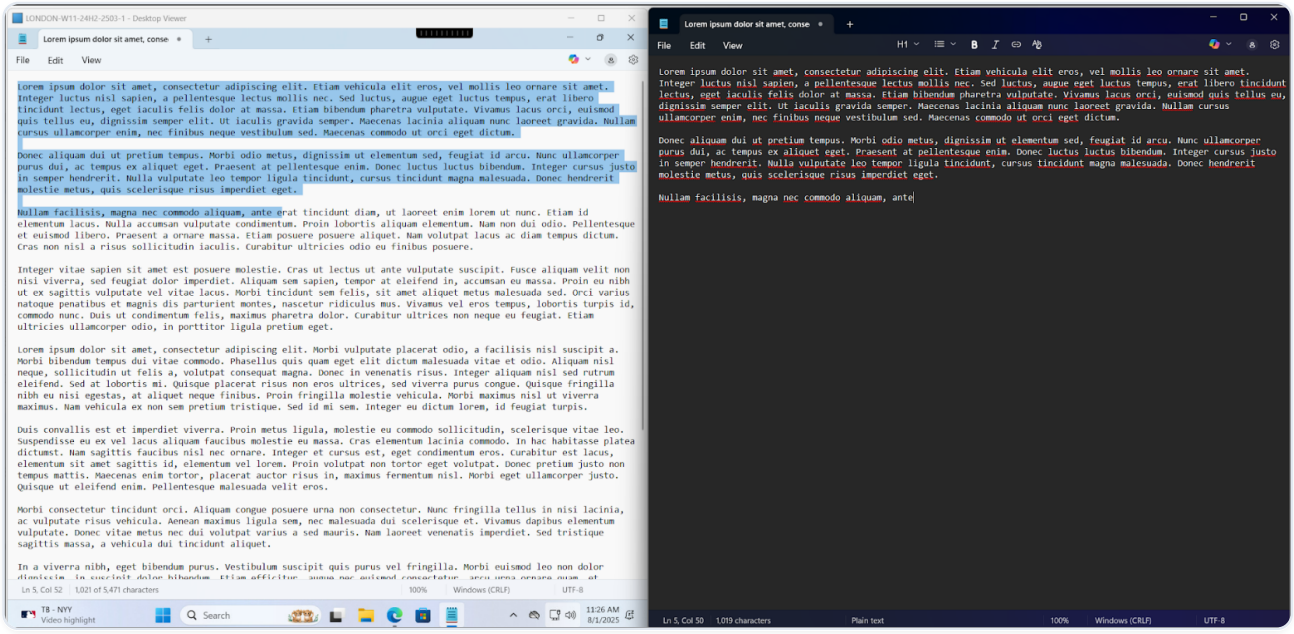
在此示例中，客户端到会话的剪贴板限制被限制为 1024 千字节：



注意：

> 大小限制基于数据大小（以千字节为单位，KB），而不是固定的字符数。由于字符编码（例如 Unicode）的可变性，可以复制的字符数会有所不同。例如，10 KB 的限制对于 Unicode 文本所能容纳的字符数将少于标准 ANSI 文本。

> 在以下示例中，“限制剪贴板会话到客户端传输大小”策略已设置为 1 KB。



启用此剪贴板传输大小限制后，所选文本是从左侧的 Citrix® 会话传输到右侧的本地记事本的最大字符数。如果用户尝试从该 Citrix 会话向其客户端复制更多字符，则文本不会被截断，而是整个粘贴操作都会失败。如果内容大于配置的最大传输大小，则尝试复制其他数据类型（例如图像或文件）也将失败。

设置此策略时，请考虑用户处理的文本数据类型。如果他们经常处理多语言内容或富文本，您可能需要设置更高的千字节限制，以适应 Unicode 文本更大的数据大小。

剪贴板传输大小限制将应用于**所有允许的剪贴板格式**。

剪贴板大小限制在所有允许的剪贴板格式中普遍强制执行。这意味着该限制决定了可以传输的最大数据量，无论数据类型如何（例如，文本、图像、文件）。

剪贴板共享范围

> **注意：**

> 剪贴板共享范围是该功能的通用版本 (GA)，该功能之前以“跨会话剪贴板交换”(Citrix Virtual Apps and Desktops 2507) 的名称作为预览版发布。它取代了早期的技术预览功能和文档。在

> GA 版本中，此功能已扩展，除了会话到会话共享外，还支持将 Chrome Enterprise Premium (CEP) 作为目标。

概述

许多组织会阻止用户将数据从其 Citrix 会话复制到本地设备，以降低数据泄露的风险。剪贴板共享范围允许您保留此保护，同时仍允许剪贴板数据在经批准的受控目标之间移动。

剪贴板共享范围可用于限制从 VDA 会话复制的剪贴板数据可以共享的位置，而无需将该数据提供给本地设备剪贴板。从会话复制的数据可以与另一个 VDA 会话或 Chrome Enterprise Premium (CEP) 共享，或两者都共享，但当配置了剪贴板共享范围时，它永远不会写入端点的本地剪贴板。这将敏感数据保留在受控环境中。

工作原理

剪贴板共享范围由单个 Citrix Studio 策略控制：**剪贴板共享范围。** 该策略定义了会话被允许共享剪贴板数据的一组目标：

VDA → VDA。剪贴板数据直接在用户的 Citrix 会话之间进行隧道传输。这些可以是已发布的桌面、已发布的应用程序或两者的组合。数据永远不会放置在本地设备剪贴板上。

VDA → CEP。剪贴板数据仅从 VDA 会话共享到 Chrome Enterprise Premium。数据永远不会放置在本地设备剪贴板上，并且无法实现 VDA 到 VDA 的剪贴板数据传输。

当策略保留为默认值（例如，剪贴板共享范围为 *“无限制”*）时，剪贴板数据将遵循现有剪贴板策略所管理的标准剪贴板重定向行为，并且不适用任何共享范围限制。“无限制”行为与 CVAD 2607 之前的剪贴板行为相同：默认行为不变，因此除非您明确配置不同的范围，否则现有部署不受影响。

除了“无限制”之外，在所有范围中，以下两点始终成立：

VDA → 客户端被阻止。剪贴板数据永远不会写入本地设备剪贴板。这是此功能提供的核心保护。

默认情况下，客户端 → VDA 被阻止，从本地设备复制到会话也被阻止。这是设计使然，目前不可配置。

要求

Windows VDA 2607 LTSR，以及 Citrix Workspace 应用程序 for Windows 2603.10 或更高版本。剪贴板共享范围仅在 Windows VDA 2607 LTSR 与 CWA for Windows 2608 结合使用时可用。要使用除默认值之外的任何配置范围，两者都必不可少。

不支持旧版 Citrix Workspace 应用程序客户端。除默认值（VDA、CEP 或 VDA 和 CEP）之外的任何配置范围都需要 CWA for Windows 2603.10 或更高版本。默认的“无限制”范围保留了现有的（2607 之前的）剪贴板行为，并且没有新的客户端要求。

当 VDA 的剪贴板共享范围配置为非默认的无限制范围时，VDA 与客户端之间（反之亦然）无法进行剪贴板传输。要允许在 CWA 2608 之前的客户端与已启用剪贴板共享范围的 VDA 之间进行剪贴板传输，客户端*必须*更新到 CWA 2608 或更高版本。

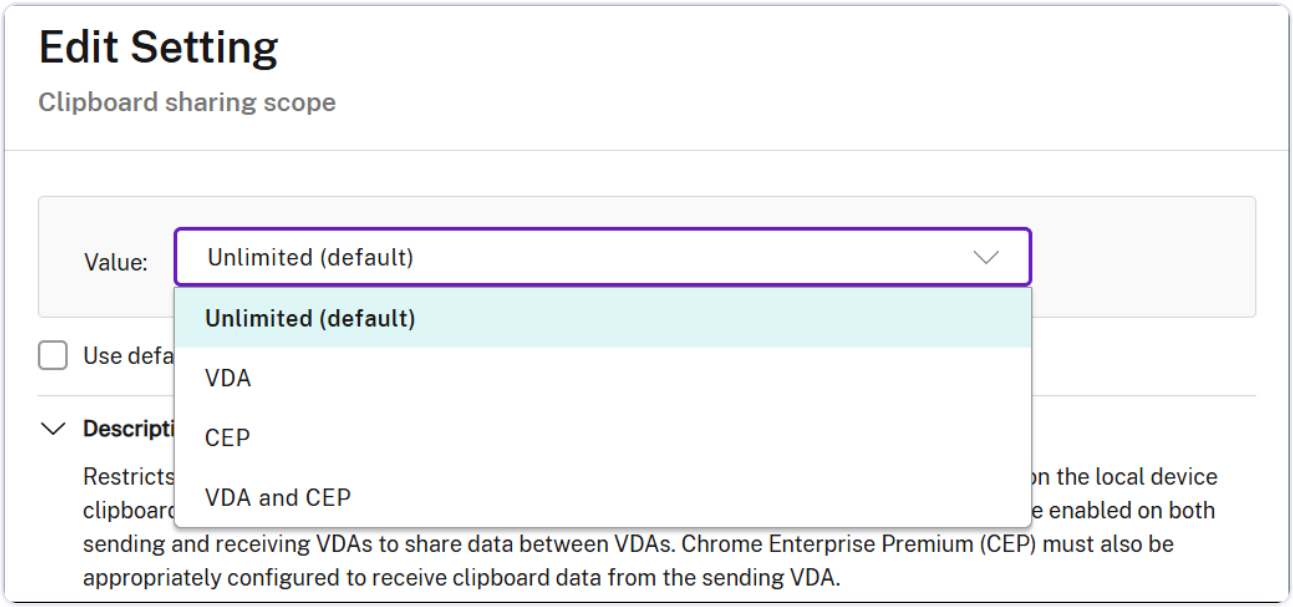
两个 VDA 都必须启用该策略（VDA 到 VDA 共享）。要在两个 VDA 会话之间共享剪贴板数据，发送 VDA 和接收 VDA 都必须启用剪贴板共享范围策略。这是设计使然，旨在防止通过接收目标 VDA 发生（意外）数据泄露。

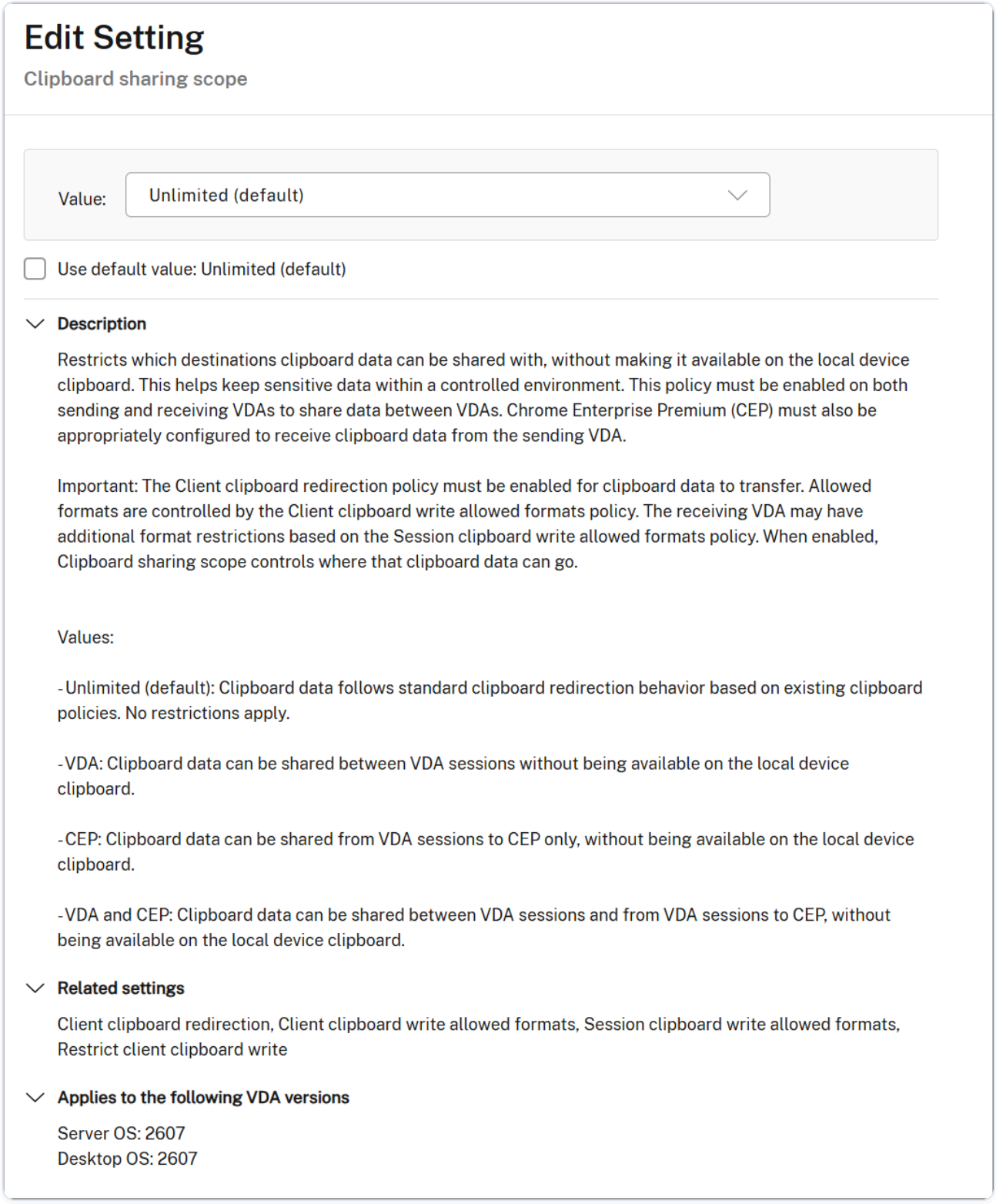
CEP 必须配置（CEP 共享）。要将剪贴板数据从 VDA 会话共享到 Chrome Enterprise Premium，必须正确配置 CEP 以接收来自发送 VDA 的剪贴板数据。

必须启用客户端剪贴板重定向。仅当启用客户端剪贴板重定向策略时，剪贴板数据才会传输。请参阅依赖项和相关策略。

配置

使用“剪贴板共享范围”策略限制剪贴板数据可以共享到的目标，而无需在本地设备剪贴板上提供该数据。这有助于将敏感数据保留在受控环境中。





必须在发送和接收 VDA 上启用此策略，才能在 VDA 之间共享数据。Chrome Enterprise Premium (CEP) 也必须正确配置，才能接收来自发送 VDA 的剪贴板数据。

重要提示：

必须启用客户端剪贴板重定向策略才能传输剪贴板数据。接收 VDA 可能会根据“会话剪贴板写入允许的格式”策略有额外的格式限制。启用后，“剪贴板共享范围”控制剪贴板数据可以传输到何处。

值	行为
无限制（默认）	剪贴板数据遵循基于现有剪贴板策略的标准剪贴板重定向行为。不适用任何限制。这与 2607 之前的剪贴板行为一致 — 默认行为未更改。
VDA	剪贴板数据可以在 VDA 会话之间共享，而无需在本地设备剪贴板上可用。剪贴板数据不能与本地端点共享。
CEP	剪贴板数据只能从 VDA 会话共享到 CEP，而无需在本地设备剪贴板上可用。
VDA 和 CEP	剪贴板数据可以在 VDA 会话之间以及从 VDA 会话共享到 CEP，而无需在本地设备剪贴板上可用。剪贴板数据无法与本地端点共享。

重要提示：

GA 时的行为更改：当剪贴板共享范围设置为 Unlimited 以外的任何值（即 VDA、CEP 或 VDA 和 CEP）时，客户端到 VDA 的剪贴板重定向（从本地设备复制到会话中）默认也会被阻止。这确保了一旦受控共享范围生效，数据就不会从本地端点剪贴板流入，除非您明确允许。

依赖项和相关策略

剪贴板共享范围与您现有的剪贴板策略协同工作。请同时配置以下内容：

客户端剪贴板重定向

必须启用此策略才能传输任何剪贴板数据。默认允许。

更多信息：客户端剪贴板重定向

客户端剪贴板写入允许的格式

此策略控制允许与客户端共享哪些剪贴板数据格式。

更多信息：客户端剪贴板写入允许的格式

会话剪贴板写入允许的格式

配置剪贴板范围后，接收 VDA 可能会通过此策略应用额外的格式限制。

更多信息：会话剪贴板写入允许的格式

限制和注意事项

除 Unlimited 之外的任何范围都需要 Citrix Workspace app for Windows 2608 或更高版本。旧版客户端不支持这些范围。

对于 VDA 到 VDA 共享，必须在发送和接收 VDA 上都启用该策略。如果仅在一侧启用，则不会发生共享。

对于 CEP 共享，必须将 CEP 配置为从发送 VDA 接收剪贴板数据。

默认情况下，将范围设置为除“无限制”以外的任何值都会阻止客户端到 VDA 的剪贴板。请参阅客户端到 VDA 的剪贴板行为。

配置示例

示例 1

为 VDA1 配置的剪贴板策略：

- **客户端剪贴板重定向**：已启用
- **剪贴板共享范围**：设置为仅 VDA

为 VDA2 配置的剪贴板策略：

- **客户端剪贴板重定向**：已启用
- **剪贴板共享范围**：设置为仅 VDA

在此示例中，两个 VDA 都配置了相同的剪贴板共享范围，最终用户将能够安全地将数据从 VDA1 复制到 VDA2，而剪贴板数据不会在本地端点剪贴板上可用。

客户端到 VDA 和 VDA 到客户端的剪贴板传输都被两个 VDA 阻止；剪贴板共享只能在 VDA1 和 VDA2 之间进行。

示例 2

为 VDA1 配置的剪贴板策略：

- **客户端剪贴板重定向**：已启用
- **剪贴板共享范围**：设置为仅 VDA

为 VDA2 配置的剪贴板策略：

- **客户端剪贴板重定向**：已启用
- **剪贴板共享范围**：设置为 VDA 和 CEP

此示例与上一个示例类似，因为两个 VDA 都配置了包含 VDA 范围的剪贴板共享范围，最终用户将能够安全地将数据从 VDA1 复制到 VDA2，而剪贴板数据不会在本地端点剪贴板上可用。

客户端到 VDA 和 VDA 到客户端的剪贴板传输对于两个 VDA 都被阻止；剪贴板共享只能在 VDA1 和 VDA2 之间进行。

此外，VDA2 将能够与 CEP 安全地共享剪贴板数据。

示例 3

为 VDA1 配置的剪贴板策略：

- **客户端剪贴板重定向**：已启用
- **剪贴板共享范围**：未设置或默认

为 VDA2 配置的剪贴板策略：

- **客户端剪贴板重定向**：已启用
- **剪贴板共享范围**：仅设置为 VDA

在此，用户可以将剪贴板数据从 VDA1 复制到 VDA2。由于 VDA1 上*未配置*剪贴板共享范围，因此剪贴板数据也将在本地端点上可用。

用户*无法*从 VDA2 复制到 VDA1，因为 VDA2 已启用剪贴板共享范围。

客户端到 VDA 的剪贴板共享也不限于 VDA1，但 VDA2 无法从客户端复制或向客户端复制，因为它已将剪贴板共享范围配置为仅限 VDA 共享。

示例 4

为 VDA1 配置的剪贴板策略：

- **客户端剪贴板重定向**：已启用
- **剪贴板共享范围**：设置为仅限 VDA

为 VDA2 配置的剪贴板策略：

- **客户端剪贴板重定向**：已启用
- **剪贴板共享范围**：设置为仅限 VDA
- **会话剪贴板写入允许的格式**：设置为仅限基于文本的格式

两个 VDA 都配置了相同的剪贴板共享范围，最终用户将能够安全地将数据从 VDA1 复制到 VDA2，而剪贴板数据不会在本地端点剪贴板上可用；但是，由于对 VDA2 将接受的剪贴板数据格式设置了额外的限制，因此只有基于文本的剪贴板数据才能粘贴到 VDA2 中。从 VDA1 到 VDA2，未定义任何剪贴板类型限制，因此，任何剪贴板数据类型都可以从 VDA2 粘贴到 VDA1。

客户端到 VDA 和 VDA 到客户端的剪贴板传输对两个 VDA 都被阻止；剪贴板共享只能在 VDA1 和 VDA2 之间进行。

场景和用例示例

正确配置剪贴板重定向策略是平衡用户生产力与企业安全性的关键。最佳配置取决于具体的用例。

以下是一些常见的用例示例：

标准知识工作者

对于大多数用户，例如知识工作者和典型的办公用户，目标是在本地和远程应用程序之间无缝复制粘贴文本和简单图像。在这种情况下，默认策略配置通常是足够的。

配置：

- 客户端剪贴板重定向：**允许**（默认）

敏感数据用例

考虑医疗保健或金融机构，用户需要将信息粘贴到安全会话中（例如，将患者数据粘贴到 EHR 中），但必须阻止将敏感数据复制到其本地设备。这有助于防止通过剪贴板意外泄露数据：

配置：

- 客户端剪贴板重定向：**允许**
- 限制客户端剪贴板写入：**已启用**（阻止从会话复制到客户端）
- 为了增强安全性，请启用限制会话剪贴板写入并使用会话剪贴板写入允许的格式，以仅允许纯文本 (CF_TEXT)。

或者，客户可以使用新的跨会话剪贴板功能（预览）来允许剪贴板会话到会话，同时阻止会话到客户端重定向。

开发人员和 IT 管理员

这些用户通常需要在本地计算机和 VDA 之间复制文件，例如脚本、日志文件或安装程序。这需要更宽松的配置。

配置：

- 客户端剪贴板重定向：**允许**
- 要启用从会话到客户端的文件复制，请确保“限制客户端剪贴板写入”为**禁用**，或者如果已启用，则将 CFX_FILE 格式添加到“客户端剪贴板写入允许的格式”列表中。
- 要启用从客户端到会话的文件复制，请确保“限制会话剪贴板写入”为**禁用**，或者如果已启用，则将 CFX_FILE 添加到“会话剪贴板写入允许的格式”列表中。

配置这些策略以针对包含开发人员或 IT 管理员的相关组，而不是单独将用户添加到策略中。

保持活动策略设置

“**保持活动**”部分包含用于管理 ICA® 保持活动消息的策略设置。

ICA 保持活动超时

此设置指定连续 ICA 保持活动消息之间的时间间隔（以秒为单位）。

默认情况下，保持活动消息之间的时间间隔为 60 秒。

指定发送 ICA 保持活动消息的时间间隔（1-3600 秒）。如果您的网络监控软件负责关闭非活动连接，请勿配置此设置。

ICA 保持活动消息

此设置启用或禁用定期发送 ICA 保持活动消息。

默认情况下，不发送保持活动消息。

启用此设置可防止断开损坏的连接。如果服务器未检测到活动，此设置可防止远程桌面服务 (RDS) 断开会话。服务器每隔几秒发送一次保持活动消息，以检测会话是否处于活动状态。如果会话不再处于活动状态，服务器会将该会话标记为已断开连接。

如果您正在使用会话可靠性，ICA 保持活动将不起作用。仅为不使用会话可靠性的连接配置 ICA 保持活动。

相关策略设置：会话可靠性连接。

本地应用访问策略设置

本地应用访问部分包含策略设置，用于管理用户的本地安装应用程序与托管应用程序的集成。这些策略设置管理托管桌面环境中的集成。

允许本地应用访问

此设置允许或阻止用户的本地安装应用程序与托管应用程序的集成。这些策略设置管理托管桌面环境中的集成。

当用户启动本地安装的应用程序时，该应用程序似乎在其虚拟桌面中运行，即使它实际上是在本地运行。

如果您将**允许本地应用访问**策略设置设为**已启用**，则不支持浏览器内容重定向，并且客户端通知区域电池状态不会显示在桌面会话中。

默认情况下，**允许本地应用访问**被禁止。

URL 重定向阻止列表

此设置指定将重定向到本地 Web 浏览器并在其中启动的网站。这些网站可能包括以下内容：

- 需要区域设置信息的网站，例如 msn.com 或 newsgoogle.com
- 包含富媒体内容的网站，在用户设备上呈现效果更好。

默认情况下，未指定任何站点。

URL 重定向允许列表

此设置指定将在其启动的环境中呈现的网站。

默认情况下，未指定任何站点。

移动体验策略设置

移动体验部分包含用于处理 Citrix Mobility Pack 的策略设置。

自动键盘显示

此设置启用或禁用在移动设备屏幕上自动显示键盘。

默认情况下，自动显示键盘处于禁用状态。

启动触摸优化桌面

此设置已禁用，不适用于 Windows 10 或 Windows Server 2016 计算机。

此设置决定了 Citrix Workspace™ 应用程序的整体界面行为。此设置允许或禁止使用针对平板电脑设备优化的触摸友好界面。

默认情况下，使用触摸友好界面。

要仅使用 Windows 界面，请将此策略设置设为“禁止”。

远程组合框

此设置确定可在移动设备会话中显示的组合框类型。将此策略设置设为“允许”以显示设备原生的组合框控件。当此设置被允许时，用户可以更改适用于 iOS 的 Citrix Workspace 应用程序会话设置以使用 Windows 组合框。

默认情况下，**远程组合框**功能处于禁用状态。

多媒体策略设置

“**多媒体**”部分包含用于管理用户会话中流式 HTML5 和 Windows 音频和视频的策略设置。

> **警告**
>
> 不正确地编辑注册表可能会导致严重问题，可能需要您重新安装操作系统。Citrix® 无法保证可以解决因不正确使用注册表编辑器而导致的问题。使用注册表编辑器风险自负。编辑注册表之前，请务必备份注册表。

多媒体策略

默认情况下，在 Delivery Controller™ 上设置的所有多媒体策略都存储在以下注册表中：

计算机策略：

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

用户策略：

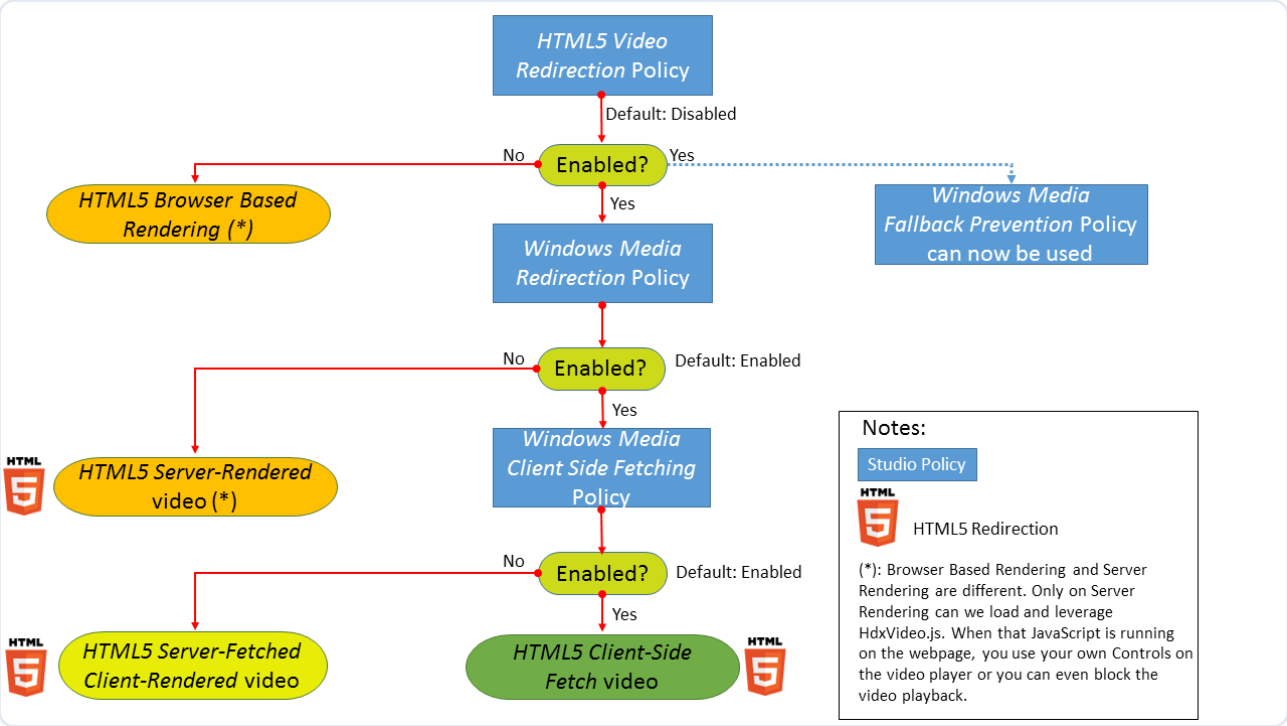
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{User Session ID}\User\MultimediaPolicies

要查找当前用户会话 ID，请在 Windows 命令行中发出 **qwinsta** 命令。

HTML5 视频重定向

控制并优化 Citrix Virtual Apps and Desktops™ 服务器向用户交付 HTML5 多媒体 Web 内容的方式。

默认情况下，此设置为禁用状态。



在此版本中，此功能仅适用于受控网页。它要求将 JavaScript 添加到提供 HTML5 多媒体内容的网页中，例如，内部培训站点上的视频。

要配置 HTML5 视频重定向：

1. 将文件 **HdxVideo.js** 从 VDA 安装的 %Program Files%/Citrix/ICA Service/HTML5 Video Redirection 复制到内部网页的位置。
2. 将此行插入到您的网页中（如果您的网页有其他脚本，请在这些脚本之前包含 **HdxVideo.js**）：

   ```
   <script src="HdxVideo.js" type="text/javascript"\></script>
   ```

注意： 如果 HdxVideo.js 不在您的网页的同一位置，请使用 **src** 属性指定其完整路径。

请注意，如果 JavaScript 未添加到您控制的网页中，并且用户播放 HTML5 视频。在这种情况下，Citrix Virtual Apps and Desktops™ 默认使用服务器端渲染。

要使 HTML5 视频重定向正常工作，请允许 ***Windows Media Redirection***。此策略对于服务器提取客户端渲染是强制性的，对于客户端提取是必需的。客户端提取反过来也要求允许*Windows Media 客户端内容提取*。

Microsoft Edge 不支持此功能。

HdxVideo.js 会将其自己的控件替换浏览器 HTML5 播放器控件。要检查 HTML5 视频重定向策略是否在某个网站上生效，请将播放器控件与 **HTML5 视频重定向**策略被禁止的场景进行比较：

（策略允许时为 Citrix 自定义控件）



（策略被禁止或未配置时为本机网页控件）



支持以下视频控件：

- 播放
- 暂停
- 查找
- 重复
- 音频
- 全屏

您可以查看一个 HTML5 视频重定向测试页面。

TLS、HTML5 视频重定向和浏览器内容重定向

您可以使用 HTML5 视频重定向来：

- 重定向来自 HTTPS 网站的视频
- 或者
- 浏览器内容重定向以重定向整个网站

注入到这些网站中的 JavaScript 必须与在 VDA 上运行的 Citrix HDX HTML5 视频重定向服务 (WebSocketService.exe) 建立 TLS 连接。VDA 上的证书存储中的 Citrix HDX HTML5 视频重定向服务会生成两个自定义证书，用于：

- 实现视频重定向
- 维护网页的 TLS 完整性

HdxVideo.js 使用 Secure WebSockets 与在 VDA 上运行的 WebSocketService.exe 进行通信。此进程以 Local System account 运行，并执行 SSL termination 和 user session mapping。

WebSocketService.exe 正在侦听 127.0.0.1 端口 9001。

限制视频质量

此设置仅适用于 Windows Media，不适用于 HTML5。它要求您启用 **Optimization for Windows Media multimedia redirection over WAN**。

此设置指定 HDX™ 连接允许的最大视频质量级别。配置后，最大视频质量将限制为指定值，从而确保在环境中保持多媒体服务质量 (QoS)。

默认情况下，此设置未配置。

要限制允许的最大视频质量级别，请选择以下选项之一：

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

在同一服务器上同时播放多个视频会消耗大量资源，并可能影响服务器的可伸缩性。

Microsoft Teams 重定向

此设置基于 HDX 技术启用 Microsoft Teams 优化。

如果启用此策略，并且您使用的是受支持的 Citrix Workspace™ 应用程序版本，则此注册表项在 VDA 上设置为 **1**。Microsoft Teams 应用程序读取此项以在 VDI 模式下加载。 请注意，无需手动设置注册表项。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

名称: MSTeamsRedirSupport

值: DWORD (1 - 开，0 - 关)

> **注意：**
>
> 假设您正在使用版本 1906.2 或更高版本的 VDA，以及没有在 Web Studio 中提供策略的旧版本 Controller。旧版本 Controller 的一个示例是版本 7.15。在这种情况下，HDX 优化在 VDA 上默认启用。如果 Workspace 应用程序版本为 1907 或更高版本，Microsoft Teams 将以优化模式启动。有关混合使用 7.15 LTSR Controller 和 CR VDA 的注意事项，请参阅知识中心文章 CTX205549。
>
> 在这种情况下，要为特定用户禁用此功能，可以覆盖注册表设置。通过使用组策略将登录脚本应用于用户的组织单位来覆盖注册表设置。

> 默认情况下，Microsoft Teams 重定向处于启用状态。

多媒体会议

此设置允许或阻止视频会议应用程序使用优化的网络摄像头重定向技术。

默认情况下，允许视频会议支持。

将此设置添加到策略时，请验证是否存在 **Windows Media 重定向**设置并将其设置为**允许**（默认值）。

使用**多媒体会议**时，请验证是否满足以下条件：

- 用于多媒体会议的网络摄像头的制造商提供的驱动程序已安装在客户端上。
- 在开始视频会议会话之前，将网络摄像头连接到用户设备。服务器在任何给定时间只使用一个已安装的网络摄像头。如果用户设备上安装了多个网络摄像头，服务器会尝试依次使用每个网络摄像头。此尝试会一直持续到成功创建视频会议会话为止。

当使用通用 USB 重定向来重定向网络摄像头时，不需要此策略。在这种情况下，请在 VDA 上安装网络摄像头驱动程序。

通过 WAN 优化 Windows Media 多媒体重定向

此设置仅适用于 Windows Media，不适用于 HTML5。此设置启用以下功能：

- 实时多媒体转码
- 允许通过降级网络将音频和视频媒体流式传输到移动设备
- 通过改进 Windows Media 内容在 WAN 上的交付方式来增强用户体验。

默认情况下，通过 WAN 交付 Windows Media 内容是经过优化的。

将此设置添加到策略时，请确保存在 **Windows Media 重定向**设置并将其设置为**允许**。

启用此设置后，将根据需要自动部署实时多媒体转码以启用媒体流。此外，即使在极端网络条件下，也能提供无缝的用户体验。

使用 GPU 优化通过 WAN 的 Windows Media 多媒体重定向

此设置仅适用于 Windows Media，并支持在虚拟投递代理 (VDA) 上的图形处理单元 (GPU) 中进行实时多媒体转码。它提高了服务器可伸缩性。GPU 转码仅在 VDA 具有受支持的 GPU 用于硬件加速时才可用。否则，转码将回退到 CPU。

注意：GPU 转码仅在 NVIDIA GPU 上受支持。

默认情况下，禁止在 VDA 上使用 GPU 优化通过 WAN 交付 Windows Media 内容。

将此设置添加到策略时，请确保存在以下设置并将其设置为“允许”：

- **Windows Media 重定向**
- **通过 WAN 优化 Windows Media 多媒体重定向设置**

Windows Media 回退预防

此设置适用于浏览器内容重定向、HTML5 和 Windows Media。要使其支持 HTML5，请将 **HTML5 视频重定向**策略设置为**允许**。

管理员可以使用 **Windows Media 回退预防**策略设置来指定尝试向用户交付流式内容的方法。

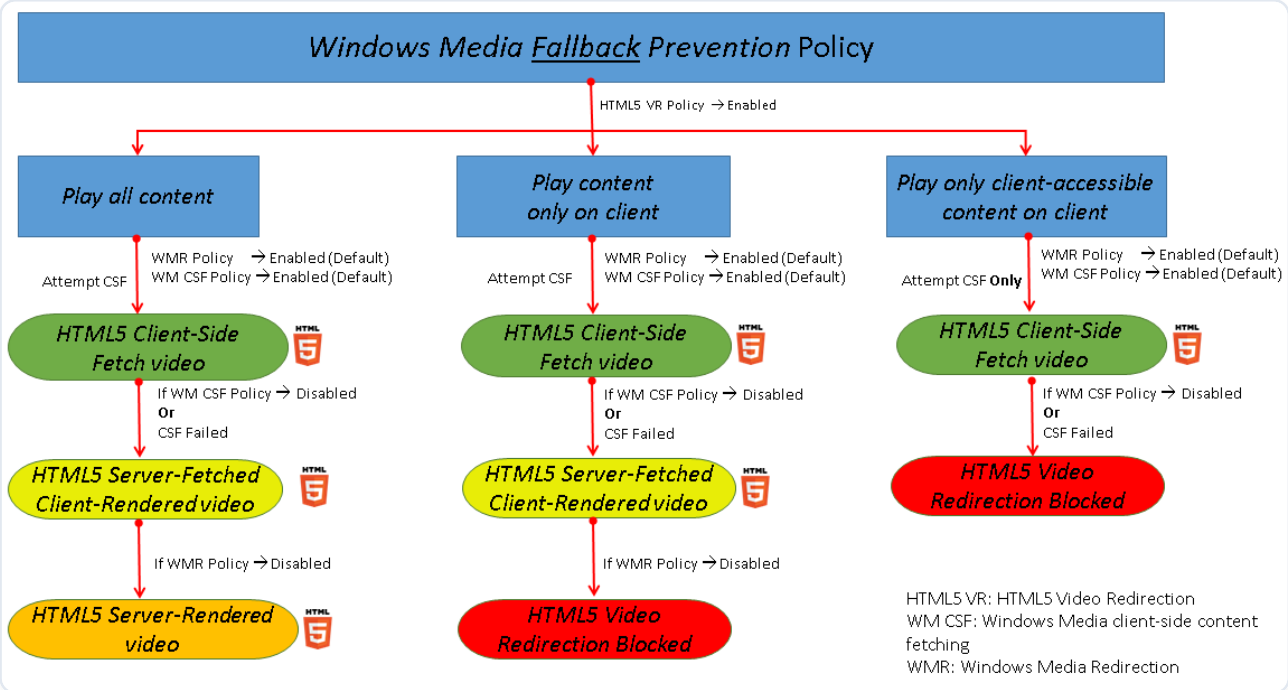
默认情况下，此设置未配置。当设置设为“未配置”时，其行为与**播放所有内容**相同。

要配置此设置，请选择以下选项之一：

- **播放所有内容**。尝试客户端内容获取，然后进行 Windows Media 重定向。如果失败，则在服务器上播放内容。
- **仅在客户端播放所有内容**。尝试客户端获取，然后进行 Windows Media 重定向。如果失败，则不播放内容。
- **仅在客户端播放客户端可访问的内容**。仅尝试客户端获取。如果失败，则不播放内容。

当内容无法播放时，播放器窗口中会显示以下错误消息（默认持续时间为 5 秒）：

“公司因资源不足而阻止了视频”



此错误消息的持续时间可以通过 VDA 上的以下注册表项进行自定义。如果注册表项不存在，则持续时间默认为 5 秒。

注册表路径因 VDA 架构而异：

`\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream`

或者

\HKLM\SOFTWARE\Citrix\HdxMediastream

注册表项：

名称: VideoLoadManagementErrDuration

类型: DWORD

范围: 1 - 直到 DWORD 限制 (默认值 = 5)

单位: 秒

Windows Media 客户端内容获取

此设置适用于 HTML5 和 Windows Media。此设置使用户设备能够直接从互联网或内网上的源提供商流式传输多媒体文件，而不是通过 XenApp 或 XenDesktop® 主机服务器。

默认情况下，此设置为**允许**。允许此设置可改善网络使用情况并提高服务器可伸缩性。这种改进是通过将媒体上的任何处理从主机服务器移动到用户设备来实现的。它还消除了在用户设备上安装高级多媒体框架（例如 Microsoft DirectShow 或 Media Foundation）的要求。用户设备只需具备从 URL 播放文件的能力。

将此设置添加到策略时，请确保存在 **Windows Media 重定向**设置并将其设置为**允许**。如果 **Windows Media 重定向**被禁用，则直接从源提供程序向用户设备流式传输多媒体文件也会被禁用。

Windows Media 重定向

此设置适用于 HTML5 和 Windows Media，并控制和优化服务器向用户交付流式音频和视频的方式。

默认情况下，此设置为**允许**。对于 HTML5，如果策略 **HTML5 视频重定向**为**禁止**，则此设置不生效。

启用此设置后，从服务器呈现的音频和视频质量会提高到与在用户设备上本地播放的音频和视频相当的水平。服务器以原始压缩形式将多媒体流式传输到客户端，并允许用户设备解压缩和呈现媒体。

Windows Media 重定向优化了使用符合 Microsoft DirectShow、DirectX Media Objects (DMO) 和 Media Foundation 标准的编解码器编码的多媒体文件。要播放给定的多媒体文件，用户设备上必须存在与多媒体文件编码格式兼容的编解码器。

默认情况下，Citrix Workspace 应用程序上禁用音频。要允许用户在 ICA® 会话中运行多媒体应用程序，请打开音频或授予用户在其 Citrix Workspace 应用程序界面中打开音频的权限。

仅当使用 Windows Media 重定向播放媒体的效果比使用基本 ICA 压缩和常规音频呈现的效果差时，才选择**禁止**。这种情况很少见，但可能在低带宽条件下发生，例如，对于关键帧频率较低的媒体。

Windows Media 重定向缓冲区大小

此设置为旧版设置，不适用于 HTML5。

此设置指定多媒体加速的缓冲区大小，范围为 1 到 10 秒。

默认情况下，缓冲区大小为 5 秒。

Windows Media 重定向缓冲区大小使用

此设置为旧版设置，不适用于 HTML5。

此设置启用或禁用使用在“**Windows Media 重定向缓冲区大小**”设置中指定的缓冲区大小。

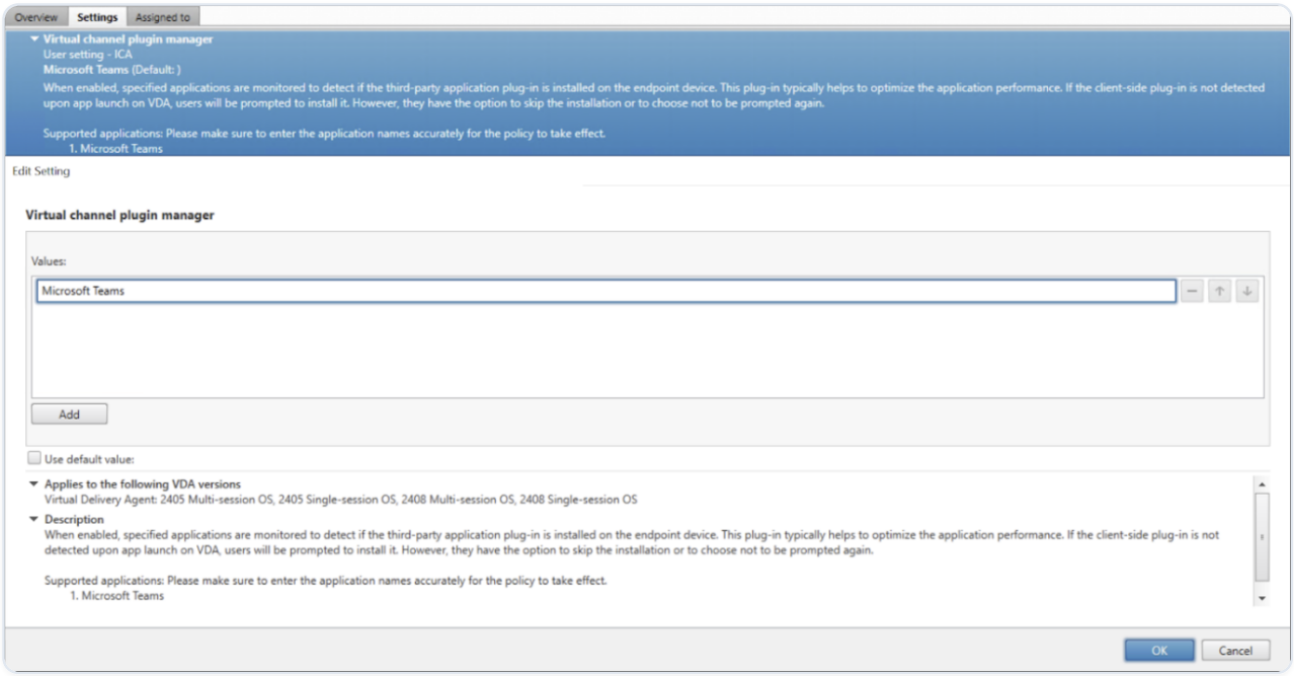
默认情况下，不使用指定的缓冲区大小。

如果此设置被禁用，或者未配置“**Windows Media 重定向缓冲区大小**”设置，则服务器将使用默认缓冲区大小值（五秒）。

虚拟通道插件管理器策略

虚拟通道插件管理器部分包含用于配置此功能的策略设置。

虚拟通道插件管理器旨在为某些指定应用程序在客户端端点上部署插件。插件管理器会检测在 VDA 上运行的特定应用程序，并提示用户在端点上安装插件，以便在运行应用程序时获得最佳体验。



- 管理员可以使用此策略并指定需要在其所有端点上安装插件的应用程序。
- 应用程序名称应与策略说明中“支持的应用程序”中提及的名称相同。
- 默认情况下，此策略处于禁用状态。
- 当前支持的应用程序
  - “微软 Teams”
- 将来，计划支持更多应用程序。

多流连接策略设置

多流连接部分包含用于管理会话中多个 ICA® 连接的服务质量 (QoS) 优先级的策略设置。

> **注意：**
>
> 如果启用了多流连接策略，则不支持 MTU 发现。

通过 UDP 传输音频

此设置允许或阻止在服务器上通过 UDP 传输音频。

默认情况下，服务器上允许通过 UDP 传输音频。

启用后，此设置会在服务器上打开一个 UDP 端口，以支持所有配置为使用通过 UDP 传输音频实时传输的连接。

音频 UDP 端口范围

此设置指定 Virtual Delivery Agent (VDA) 使用的端口号范围（最低端口号，最高端口号）。此规范有助于与用户设备交换音频数据包。VDA 尝试使用每个 UDP 端口对与用户设备交换数据，从最低端口开始，每次尝试递增两个。每个端口处理入站和出站流量。

默认情况下，此范围设置为 16500,16509。

多端口策略

此设置指定用于 ICA 流量的 TCP 端口，并为每个端口建立网络优先级。

默认情况下，主端口 (2598) 具有高优先级。

配置端口时，您可以分配以下优先级：

- **非常高：** 用于实时活动，例如网络摄像头会议
- **高：** 用于交互式元素，例如屏幕、键盘和鼠标
- **中：** 用于批量处理，例如客户端驱动器映射
- **低：** 用于后台活动，例如打印

每个端口都必须具有唯一的优先级。例如，您不能同时将“非常高”优先级分配给 CGP 端口 1 和 CGP 端口 3。

要从优先级中删除端口，请将端口号设置为 0。您不能删除主端口，也不能更改其优先级级别。

配置此设置时，请重新启动服务器。此设置仅在启用 **多流计算机** 设置策略设置时才生效。

多流计算机设置

此设置用于在服务器上启用或禁用多流。

默认情况下，多流处于禁用状态。如果您使用 Citrix SD-WAN™ 或第三方路由器来实现所需的服务质量，请配置多流计算机策略设置。

如果启用了多流，则不支持 MTU 发现（自适应传输的一项功能）。

配置此设置时，请重新启动服务器以确保更改生效。

> **重要提示：**
>
> 将此策略设置与带宽限制策略设置（例如“会话总带宽限制”）结合使用可能会产生意外结果。在策略中包含此设置时，请确保不包含带宽限制设置。

多流用户设置

此设置用于在用户设备上启用或禁用多流。

默认情况下，所有用户都禁用多流。如果您使用 Citrix SD-WAN 或第三方路由器来实现所需的服务质量，请配置多流用户设置。

此设置仅在启用了**多流计算机**设置策略设置的主机上生效。

> **重要提示：**
>
> 将此策略设置与带宽限制策略设置（例如“会话总带宽限制”）结合使用可能会产生意外结果。在策略中包含此设置时，请确保不包含带宽限制设置。

多流虚拟通道分配设置

此设置指定在使用多流时虚拟通道分配到的 ICA 流。

如果您不配置这些设置，虚拟通道将保留在其默认流中。要将虚拟通道分配给 ICA 流，请从虚拟通道名称旁边的“**流编号**”列表中选择所需的流编号（0、1、2、3）。

如果环境中使用了自定义虚拟通道，请单击“**添加**”，在“**虚拟通道**”下的文本框中指定虚拟通道名称，然后从其旁边的“**流编号**”列表中选择所需的流编号。您指定的名称必须是实际的虚拟通道名称，而不是友好名称。例如，CTXSBR 而不是 Citrix Browser Acceleration。

这些设置仅在您启用了多流计算机设置时才生效。

默认情况下，虚拟通道及其流分配如下：

- AppFlow®: 2
- 音频: 0
- 浏览器内容重定向: 2
- 客户端 COM 端口映射: 3
- 客户端驱动器映射: 2
- 客户端打印机映射: 3
- 剪贴板: 2
- CTXDND: 1 (**注意：** 这支持在 Citrix 会话和本地端点之间拖放文件。)
- DVC Plug-in（从 DVC 插件友好名称自动生成的静态 VC 名称，或管理员分配的名称）：2
- 最终用户体验监控：1

- 文件传输 (HTML5 Receiver)：2
- 通用数据传输：2
- ICA 控制：1
- 输入法编辑器：1
- 旧版客户端打印机映射 (COM1)：1, 3
- 旧版客户端打印机映射 (COM2)：2, 3
- 旧版客户端打印机映射 (LPT1)：1, 3
- 旧版客户端打印机映射 (LPT2)：2, 3
- 许可证管理：1
- Microsoft Teams/WebRTC 重定向：1
- 移动 Receiver：1
- 多点触控：1
- 端口转发: 2
- 远程音频和视频扩展 (RAVE): 2
- 无缝 (透明窗口集成): 1
- 传感器和位置: 1
- 智能卡: 1
- Thinwire 图形: 1
- 透明 UI 集成/登录状态: 2
- TWAIN 重定向: 2
- USB: 2
- 零延迟字体和键盘: 2
- 零延迟数据通道: 2

有关虚拟通道分配和优先级的更多信息，请参阅知识中心文章 CTX131001。

端口重定向策略设置

“**端口重定向**”部分包含客户端 LPT 和 COM 端口映射的策略设置。

对于 **7.0 之前的** Virtual Delivery Agent 版本，请使用以下策略设置来配置端口重定向。对于 VDA 版本 **7.0 到 7.8**，请使用注册表配置这些设置；请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。对于 VDA 版本 **7.9**，请使用以下策略设置。

自动连接客户端 COM 端口

此设置可在用户登录站点时启用或禁用用户设备上 COM 端口的自动连接。

默认情况下，客户端 COM 端口不会自动连接。

自动连接客户端 LPT 端口

此设置可在用户登录站点时启用或禁用用户设备上 LPT 端口的自动连接。

默认情况下，客户端 LPT 端口不会自动连接。

客户端 COM 端口重定向

此设置允许或阻止访问用户设备上的 COM 端口。

默认情况下，禁止 COM 端口重定向。

以下策略设置相关：

- COM 端口重定向带宽限制
- COM 端口重定向带宽限制百分比

客户端 LPT 端口重定向

此设置允许或阻止访问用户设备上的 LPT 端口。

默认情况下，LPT 端口重定向是禁止的。

LPT 端口仅供将打印作业发送到 LPT 端口的旧版应用程序使用。将打印作业发送到用户设备上的打印对象的旧版应用程序不使用这些端口。如今，大多数应用程序都可以将打印作业发送到打印机对象。此策略设置仅适用于托管打印到 LPT 端口的旧版应用程序的服务器。

请注意，尽管客户端 COM 端口重定向是双向的，但 LPT 端口重定向仅为输出，并且在 ICA 会话中仅限于 `\\client\LPT1` 和 `\\client\LPT2`。

以下策略设置相关：

- LPT 端口重定向带宽限制
- LPT 端口重定向带宽限制百分比

FIDO2 重定向

此设置启用或禁用 FIDO2 重定向。FIDO2 重定向允许用户利用虚拟机中的本地端点 FIDO2 组件。用户可以通过 FIDO2 安全密钥或在具有 TPM 2.0 和 Windows Hello 的设备上使用集成生物识别技术对虚拟会话进行身份验证。

当此设置为 **允许** 时，用户可以通过使用本地端点功能执行 FIDO2 身份验证。默认情况下，此设置为 **允许**。

打印策略设置

“打印”部分包含用于管理客户端打印的策略设置。

客户端打印机重定向

此设置控制当用户登录到会话时，客户端打印机是否映射到服务器。

默认情况下，允许客户端打印机映射。如果此设置被禁用，则不会自动创建会话的 PDF 打印机。

相关策略设置：自动创建客户端打印机

默认打印机

此设置指定如何在会话中建立用户设备上的默认打印机。

默认情况下，用户的当前打印机用作会话的默认打印机。

要使用当前远程桌面服务或 Windows 用户配置文件设置作为默认打印机，请选择“不调整用户的默认打印机”。如果选择此选项，默认打印机不会保存在配置文件中，并且不会根据其他会话或客户端属性而更改。会话中的默认打印机是会话中自动创建的第一个打印机，它可能是：

- 本地添加到 Windows 服务器的第一个打印机，位于 **控制面板 > 设备** 和 **打印机** 中。
- 第一个自动创建的打印机（如果服务器上没有本地添加的打印机）。

您可以使用此选项通过配置文件设置向用户提供最近的打印机（称为邻近打印）。

打印机分配

此设置提供了“默认打印机”和“会话打印机”设置的替代方案。使用单独的“默认打印机”和“会话打印机”设置来配置站点、大型组或组织单位的行为。使用“**打印机分配**”设置将大量打印机分配给多个用户。

此设置指定如何在会话中建立列出的用户设备上的默认打印机。

默认情况下，用户的当前打印机用作会话的默认打印机。

它还指定了为每个用户设备在会话中自动创建的网络打印机。默认情况下，未指定任何打印机。

- 设置默认打印机值时：

  要使用用户设备的当前默认打印机，请选择“不调整”。

要使用当前远程桌面服务或 Windows 用户配置文件设置作为默认打印机，请选择“不调整”。如果选择此选项，则默认打印机不会保存在配置文件中，并且不会根据其他会话或客户端属性进行更改。会话中的默认打印机是会话中第一个自动创建的打印机，它可能是：

  - 在 **控制面板 > 设备和打印机** 中本地添加到 Windows 服务器的第一个打印机。
  - 如果没有本地添加到服务器的打印机，则为第一个自动创建的打印机。

- 设置 **会话打印机值：添加打印机** 时，键入要自动创建的打印机的 UNC 路径。或者，单击 **浏览** 以在整个网络中搜索打印机。您还可以通过输入打印机服务器的 FQDN 或 NetBIOS 名称来浏览打印机。有关详细信息，请参阅会话打印机。添加打印机后，您可以在每次登录时为当前会话应用自定义设置。

打印机自动创建事件日志首选项

此设置指定在打印机自动创建过程中记录的事件。您可以选择不记录错误或警告、仅记录错误或记录错误和警告。

默认情况下，会记录错误和警告。

警告的一个示例是，无法安装打印机的本机驱动程序，而是安装了通用打印驱动程序。在这种情况下，要使用通用打印驱动程序，请将通用打印驱动程序使用设置配置为“仅使用通用打印”或“仅在请求的驱动程序不可用时使用通用打印”。

会话打印机

此设置指定要在会话中自动创建的网络打印机。在 ICA/HDX 会话中，Citrix Print Manager 服务 (CpSvc.exe) 在会话登录期间为 **会话打印机** 策略设置中指定的每个网络打印机创建网络打印机连接。它会在会话注销期间删除打印机。默认情况下，未指定任何打印机。

在 **会话打印机** 策略设置中，网络打印机可以驻留在 Windows 打印服务器或 Citrix Universal™ Print Server 上。

- **Windows 打印服务器：** 共享一个或多个网络打印机。它还具有使用网络打印机所需的本机打印机驱动程序。
- **通用打印服务器：** 已安装 Citrix Universal Print Server 软件的 Windows 打印服务器。

使用 Windows 打印服务器时，Citrix Print Manager 服务使用本机打印机驱动程序创建网络打印机连接。Citrix Virtual Apps™ 服务器必须安装本机打印机驱动程序。

当使用 Citrix Universal Print Server 时，Citrix Print Manager 服务使用本机打印机驱动程序、Citrix Universal Printer Driver 或 Citrix Universal XPS Printer Driver 创建网络打印机连接。您使用的驱动程序由通用打印驱动程序使用策略设置控制。

所有 Windows 打印机驱动程序目前都属于 v3 或 v4 驱动程序版本。有关详细信息，请参阅 支持 Microsoft V3 和 V4 打印机驱动程序体系结构。

要添加会话打印机并验证它们是否出现在会话中，请完成以下过程：

1. 登录 Web Studio，在左侧窗格中选择 **策略**，然后单击 **策略** 选项卡。
2. 选择 **会话打印机** 策略，然后单击 **编辑**。
3. 在 **编辑设置** 页面上，清除 **使用默认值** 复选框，然后按照以下步骤单击 **添加** 以添加打印机：
   a. 以 `\\<FQDN of the printer server>\<printer name>.` 格式输入打印机的 UNC 路径。或者，单击 **浏览** 以在整个网络中搜索打印机。您还可以通过输入打印机服务器的 FQDN 或 NetBIOS 名称来浏览打印机。

      > **注意：**
      >
      > 为确保您可以使用 **浏览** 搜索特定打印机，在配置打印机时，请确保在 **打印机设置 > 打印机属性 > 共享** 下选中 **在目录中列出** 选项。

   b. 默认情况下，您的用户名和密码用于浏览打印机服务器。如果需要不同的域凭据，请选择 **使用不同的域凭据进行浏览**，输入必要的用户名和密码，然后单击 **浏览**。
   c. 点击 **完成**。
4. 设置策略后，已发布的应用程序可能不显示会话打印机。出现此问题的原因可能是 Citrix Virtual Apps 服务器缺少打印机驱动程序，或者策略已创建但未启用。

   > **注意：**
   >
   > 如果会话打印机需要本机打印机驱动程序，并且 VDA 上未安装本机打印机驱动程序，则可能无法在会话中创建会话打印机。

5. 启动已发布的桌面，并在 **设备和打印机 > 控制面板** 中手动添加会话打印机。
6. 如果此操作失败，请调查 Citrix Virtual Apps 服务器与打印服务器之间的通信。考虑使用 RDP 运行测试。

等待创建打印机

使用 Delivery Controller 上的策略在 Citrix Virtual Desktops 上启用此功能。

等待创建打印机 (服务器桌面):

此设置允许在连接到会话时延迟，以便可以自动创建客户端重定向的打印机。

默认情况下，不会发生连接延迟。

等待创建打印机 (Citrix Virtual Apps):

运行以下 PowerShell cmdlet 允许在连接到多会话主机上运行的虚拟应用时延迟，以便在应用程序打开之前自动创建客户端重定向的打印机。

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation $true
```

默认情况下，不会发生连接延迟。

客户端打印机策略设置

“**客户端打印机**”部分包含客户端打印机的策略设置，包括自动创建客户端打印机、保留打印机属性以及连接到打印服务器的设置。

自动创建客户端打印机

此设置指定自动创建的客户端打印机。此设置会覆盖默认的客户端打印机自动创建设置。

默认情况下，所有客户端打印机都会自动创建。

此设置仅当“**客户端打印机重定向**”设置存在并设置为“**允许**”时才生效。

将此设置添加到策略时，请选择一个选项：

- **自动创建所有客户端打印机**：自动创建用户设备上的所有打印机。
- **仅自动创建客户端的默认打印机**：仅自动创建在用户设备上选择为默认打印机的打印机。
- **仅自动创建本地（非网络）客户端打印机**：仅自动创建通过 LPT、COM、USB、TCP/IP 或其他本地端口直接连接到用户设备的打印机。
- **不自动创建客户端打印机**：在用户登录时关闭所有客户端打印机的自动创建功能。选择此选项会导致远程桌面服务 (RDS) 中用于自动创建客户端打印机的设置覆盖低优先级策略中的此设置。

自动创建通用型通用打印机

此设置启用或禁用会话的通用 Citrix Universal™ 打印机对象的自动创建。这些会话仅包括正在使用与通用打印兼容的用户设备的会话。

默认情况下，通用 Universal Printer 对象不会自动创建。

以下策略设置相关：

- 通用打印驱动程序用法
- 通用驱动程序首选项

自动创建 PDF 通用打印机

此设置启用或禁用以下会话的 Citrix PDF 打印机自动创建功能：

- 适用于 Windows 的 Citrix Workspace 应用程序（从 VDA 7.19 开始）
- 适用于 Linux 的 Citrix Workspace™ 应用程序
- 适用于 MacOS 的 Citrix Workspace 应用程序
- 适用于 HTML5 的 Citrix Workspace 应用程序
- 适用于 Chrome 的 Citrix Workspace 应用程序

默认情况下，Citrix PDF 打印机不会自动创建。

客户端打印机名称

此设置选择自动创建的客户端打印机的命名约定。

默认情况下，使用标准打印机名称。

选择 **标准打印机名称** 以使用诸如“会话 3 中客户端名称的 HPLaserJet 4”之类的打印机名称。

选择 **旧式打印机名称** 以使用旧式客户端打印机名称，并保留与产品 XenDesktop 版本中存在的旧式打印机名称的向后兼容性。您可以在当前 Citrix Virtual Apps and Desktops 版本的产品中使用此选项。旧式打印机名称的示例是“Client/clientname#/HPLaserJet 4”。此选项安全性较低。

当您在从适用于 HTML5 的 Citrix Workspace 应用程序启动的会话中使用 Citrix PDF 打印机时，请将 **客户端打印机名称** 设置为默认值或选择 **标准打印机名称**。如果您选择 **旧式打印机名称**，则适用于 HTML5 的 Citrix Workspace 应用程序不支持 Citrix PDF 打印机选项。

直接连接到打印服务器

此设置启用或禁用从虚拟桌面或服务器托管应用程序到打印服务器的客户端打印机直接连接。在此处，客户端打印机托管在可访问的网络共享上。

默认情况下，直接连接处于启用状态。

如果网络打印服务器与虚拟桌面或服务器托管应用程序不在广域网 (WAN) 上，请启用直接连接。如果网络打印服务器与虚拟桌面或服务器托管应用程序在同一局域网 (LAN) 上，则直接通信可实现更快的打印。

如果网络跨越广域网 (WAN)，或者存在显著延迟或带宽受限，请禁用直接连接。打印作业将通过用户设备路由，然后重定向到网络打印服务器。发送到用户设备的数据经过压缩，因此数据在广域网 (WAN) 上传输时消耗的带宽更少。

如果两个网络打印机具有相同的名称，则使用与用户设备位于同一网络的打印机。

打印机驱动程序映射和兼容性

此设置指定适用于自动创建的客户端打印机的驱动程序替换规则。

此设置配置为从自动创建的客户端打印机列表中排除 Microsoft OneNote 和 XPS Document Writer。

定义驱动程序替换规则时，您可以允许或阻止使用指定驱动程序创建打印机。此外，您可以允许创建的打印机仅使用通用打印驱动程序。驱动程序替换会覆盖或映射用户设备提供的打印机驱动程序名称，从而在服务器上替换为等效驱动程序。这些规则使服务器应用程序能够访问与服务器具有相同驱动程序但驱动程序名称不同的客户端打印机。

您可以执行以下操作：

- 添加驱动程序映射
- 编辑现有映射
- 覆盖映射的自定义设置
- 删除映射
- 更改列表中驱动程序条目的顺序

添加映射时，输入客户端打印机驱动程序名称，然后选择要替换的服务器驱动程序。

打印机属性保留

此设置指定是否存储打印机属性以及存储位置。

默认情况下，系统会确定打印机属性是存储在用户设备上（如果可用）还是存储在用户配置文件中。

将此设置添加到策略时，请选择一个选项：

- 仅保存在客户端设备上适用于具有未保存的强制或漫游配置文件的用户设备。
- 仅保留在用户配置文件中适用于受带宽（此选项可减少网络流量）和登录速度限制的用户设备，或适用于使用旧版插件的用户。此选项将打印机属性存储在服务器上的用户配置文件中，并阻止与用户设备进行任何属性交换。此选项仅在使用远程桌面服务 (RDS) 漫游配置文件时适用。

- 仅在未保存在客户端时保留在配置文件中允许系统确定打印机属性的存储位置。打印机属性存储在用户设备上（如果可用）或用户配置文件中。尽管此选项最灵活，但它也可能减慢登录时间并占用额外的带宽进行系统检查。
- 不保留打印机属性可防止存储打印机属性。

保留和还原的客户端打印机

此设置启用或禁用用户设备上打印机的保留和重新创建。默认情况下，客户端打印机是自动保留和自动还原的。

保留的打印机是用户创建的打印机，它们会在下一次会话开始时重新创建或记住。当 Citrix Virtual Apps™ 重新创建保留的打印机时，它会考虑所有策略设置，但 **自动创建客户端打印机** 设置除外。

还原的打印机是管理员完全自定义的打印机，其保存状态永久附加到客户端端口。

CITRIX PDF 通用打印机驱动程序

Citrix PDF 通用打印机驱动程序使用户能够打印通过托管应用程序或在 Citrix Virtual Apps and Desktops 提供的虚拟桌面上运行的应用程序打开的文档。当用户选择 **Citrix PDF 打印机** 选项时，驱动程序会将文件转换为 PDF 并将 PDF 传输到本地设备。然后打开 PDF 以便从本地连接的打印机进行查看和打印。PDF 是 Citrix Universal Printing 支持的格式之一（除了 EMF 和 XPS）。 PDF 打印机可以使用 Citrix 策略启用、配置并设置为默认值。**Citrix PDF 打印机** 选项适用于适用于 Windows、Linux、MacOS、Chrome 和 HTML5 的 Citrix Workspace 应用程序用户。

> **注意：**
>
> Windows 端点需要 PDF 查看器。客户端必须具有在 Windows 上注册了文件类型关联的应用程序才能打开 PDF 文件。

驱动程序策略设置

驱动程序部分包含与打印机驱动程序相关的策略设置。

自动安装内置打印机驱动程序

> **注意**
>
> 此策略在此版本中不支持 VDA。

此设置启用或禁用从以下位置自动安装打印机驱动程序：

- Windows 内置驱动程序集
- 使用 `pnputil.exe /a` 在主机上暂存的驱动程序包

默认情况下，这些驱动程序会根据需要进行安装。

通用驱动程序首选项

> **注意：**
>
> 此策略设置的默认顺序将在 Citrix Virtual Apps and Desktops™ 的第四季度版本中更改。新的默认顺序将是：
>
> - EMF
> - XPS
> - 打印机控制语言5c
> - PCL4
> - PDF
> - PS
>
> 此设置指定通用打印机驱动程序的使用顺序，从列表中的第一个条目开始。

默认情况下，首选顺序为：

- EMF
- XPS
- 打印机控制语言5c
- PCL4
- PS

您可以添加、编辑或删除驱动程序，并更改列表中驱动程序的顺序。

通用打印驱动程序用法

此设置指定何时使用通用打印。

默认情况下，仅在请求的驱动程序不可用时才使用通用打印。

通用打印使用通用打印机驱动程序，而不是标准的特定型号驱动程序，这可能会简化主机上的驱动程序管理负担。通用打印驱动程序的可用性取决于用户设备、主机和打印服务器软件的功能。在某些配置中，通用打印可能不可用。

将此设置添加到策略时，从下表中选择一个选项：

选项	描述
仅使用打印机型号专用驱动程序	指定客户端打印机仅使用在登录期间自动创建的标准型号专用驱动程序。如果请求的驱动程序不可用，则无法自动创建客户端打印机。
仅使用通用打印	指定不使用任何标准型号专用驱动程序。仅使用通用打印驱动程序来创建打印机。
仅在请求的驱动程序不可用时使用通用打印	如果标准型号专用驱动程序可用，则使用它们来创建打印机。如果服务器上没有该驱动程序，则会自动使用相应的通用驱动程序创建客户端打印机。
仅在通用打印不可用时使用打印机型号专用驱动程序	如果通用打印驱动程序可用，则使用它。如果服务器上没有该驱动程序，则会自动使用相应的型号专用打印机驱动程序创建客户端打印机。

通用打印服务器策略设置

“**通用打印服务器**”部分包含用于处理通用打印服务器的策略设置。

SSL 密码套件

此设置指定通用打印客户端中用于加密打印数据流 (CGP) 连接的 SSL/TLS 密码套件集。

要控制通用打印客户端用于加密打印 Web 服务 (HTTPS/SOAP) 连接的密码套件包，请参阅 。

默认值：ALL

此设置具有以下值：ALL、COM 或 GOV。

每个值对应的密码套件如下：

ALL：

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM：

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV：

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL 合规模式

此设置指定通用打印客户端用于加密打印数据流 (CGP) 连接的 NIST 特别出版物 800-52 合规级别。

默认值: 无。

此设置具有以下值：

无。

加密打印数据流 (CGP) 连接使用默认合规模式。

SP800-52。

加密打印数据流 (CGP) 连接使用 NIST 特别出版物 800-52 合规模式。

SSL 已启用

此设置指定通用打印客户端是否将 SSL/TLS 用于以下各项：

- 打印数据流 (CGP) 连接
- Web 服务 (HTTP/SOAP) 连接

当您将 **通用打印服务器启用** 设置为 **启用并回退到 Windows 本机远程打印** 时，回退连接由 Microsoft Windows 网络打印提供程序建立。此设置不影响这些回退连接。

默认值: 禁用

此设置具有以下值：

已启用。

通用打印客户端使用 SSL/TLS 连接到通用打印服务器。

已禁用。

通用打印客户端使用 SSL/TLS 连接到通用打印服务器。

SSL FIPS 模式

此设置指定通用打印客户端用于打印数据流 (CGP) 连接的 SSL/TLS 加密模块是否在 FIPS 模式下运行。

默认值: 禁用

此设置具有以下值：

已启用。

FIPS 模式已开启。

已禁用。

FIPS 模式已关闭。

SSL 协议版本

此设置指定通用打印客户端使用的 SSL/TLS 协议版本。

默认值：ALL

此设置具有以下值：

ALL。

使用 TLS 版本 1.0、1.1 或 1.2。

TLSv1. 版本.

使用 TLS 版本 1.0。

TLSv1.1。

使用 TLS 版本 1.1。

TLSv1.2。

使用 TLS 版本 1.2。

SSL 通用打印服务器加密打印数据流 (CGP) 端口

此设置指定通用打印服务器加密打印数据流 (CGP) 端口的 TCP 端口号。此端口接收打印作业的数据。

默认值：443

SSL 通用打印服务器加密 WEB 服务 (HTTPS/SOAP) 端口

此设置指定通用打印服务器加密 Web 服务 (HTTPS/SOAP) 端口的 TCP 端口号。此端口接收打印命令的数据。

默认值: 8443

启用通用打印服务器

此策略启用或禁用 Citrix 通用打印服务器 (UPS) 的使用。将此策略设置应用于包含虚拟桌面或服务器托管应用程序的组织单位 (OU)。此策略设置包括回退选项，以便在请求的打印服务器上未安装或不可用 Citrix UPS 组件时，允许使用本机 Windows 远程打印服务连接到打印服务器。此策略的更改仅在 VDA 重新启动后生效。

默认情况下，通用打印服务器处于禁用状态。

将此设置添加到策略时，请选择以下选项之一：

- **启用并回退到 Windows 本机远程打印**：如果可能，通用打印服务器会为网络打印机连接提供服务。如果通用打印服务器不可用，则使用 Windows 打印提供程序。Windows 打印提供程序会继续处理以前使用 Windows 打印提供程序创建的所有打印机。
- **启用但不回退到 Windows 本机远程打印**：通用打印服务器专门为网络打印机连接提供服务。如果通用打印服务器不可用，则网络打印机连接将失败。此设置有效地禁用了通过 Windows 打印提供程序的网络打印。当包含此设置的策略处于活动状态时，以前使用 Windows 打印提供程序创建的打印机将不会被创建。
- **禁用**：通用打印服务器功能已禁用。当使用 UNC 名称连接到网络打印机时，不会尝试连接通用打印服务器。远程打印机的连接将继续使用 Windows 本机远程打印功能。

通用打印服务器打印数据流 (CGP) 端口

此设置指定通用打印服务器打印数据流通用网关协议 (CGP) 侦听器使用的 TCP 端口号。仅将此策略设置应用于包含打印服务器的组织单位 (OU)。

默认情况下，端口号设置为 7229。

有效端口号必须在 1-65535 范围内。

通用打印服务器打印流输入带宽限制 (KBPS)

此设置指定打印数据传输速率的上限（以千比特每秒为单位）。传输速率是根据使用 CGP 从每个打印作业传输到通用打印服务器的打印数据计算的。将此策略设置应用于包含虚拟桌面或服务器托管应用程序的组织单位 (OU)。

默认情况下，该值为 0，表示没有上限。

通用打印服务器 WEB 服务 (HTTP/SOAP) 端口

此设置指定 Universal Print Server 的 Web 服务 (HTTP/SOAP) 侦听器使用的 TCP 端口号。Universal Print Server 是一个可选组件，可用于在网络打印方案中使用 Citrix 通用打印驱动程序。

使用 Universal Print Server 时，打印命令通过 HTTP 上的 SOAP 从 Citrix Virtual Apps and Desktops 主机发送到 Universal Print Server。此设置修改 Universal Print Server 侦听传入 HTTP/SOAP 请求的默认 TCP 端口。

您必须将主机和打印服务器的 HTTP 端口配置为相同。如果端口配置不相同，则主机软件无法连接到 Universal Print Server。此设置更改 Citrix Virtual Apps and Desktops 上的 VDA。此外，您必须更改 Universal Print Server 上的默认端口。

默认情况下，端口号设置为 8080。

有效端口号必须在 0-65535 范围内。

用于负载平衡的通用打印服务器

此设置列出了在评估其他 Citrix® 打印策略设置后，用于在会话启动时建立的打印机连接进行负载平衡的 Universal Print Server。为优化打印机创建时间，Citrix 建议所有打印服务器都具有相同的共享打印机集。可添加用于负载平衡的打印服务器数量没有上限。

此设置还实现了打印服务器故障转移检测和打印机连接恢复。系统会定期检查打印服务器的可用性。如果检测到服务器故障，则该服务器将从负载平衡方案中移除。此外，该服务器上的打印机连接将重新分配给其他可用的打印服务器。当发生故障的打印服务器恢复时，它将返回到负载平衡方案中。

单击 **验证服务器** 以检查每个服务器是否为打印服务器，服务器列表是否不包含重复的服务器名称，以及所有服务器是否安装了相同的共享打印机集。此操作可能需要一些时间。

UNIVERSAL PRINT SERVER 停止服务阈值

此设置指定负载平衡器必须等待不可用打印服务器恢复的时间，然后才能确定该服务器已永久脱机并将其负载重新分配给其他可用打印服务器。

默认情况下，阈值设置为 180（秒）。

UNIVERSAL PRINT SERVER WEB 服务 (HTTP/SOAP) 连接超时

此设置指定 Universal Print Client 必须等待 Universal Print Server Web 服务 connect() 操作超时的时间（以秒为单位）。此设置具有以下值。所有这些值均为数字，单位（时间）为秒。

- 最小值为 0。
- 最大值为 60。

- 默认值为 10。

当超时时间介于 1 到 60（含）之间时，通用打印客户端会等待指定的时间以完成操作。该操作是连接 TCP 套接字操作。套接字是 Windows 操作系统的一项功能，允许通过 TCP/IP 网络进行进程间通信。

当超时时间为 0 时，通用打印客户端使用操作系统定义的默认超时。此配置是此更改之前通用打印客户端先前版本中可用的配置。

通用打印客户端是虚拟投递代理 (VDA) 的组件，负责与通用打印服务器通信。

> **注意：**
>
> 此策略设置适用于 VDA 7.35 及更高版本。

通用打印服务器 WEB 服务 (HTTP/SOAP) 接收超时

此设置指定通用打印客户端必须等待的秒数，直到通用打印服务器 Web 服务 recv() 操作超时。此设置具有以下值，所有这些值均为数字，单位为秒。

- 最小值为 0。
- 最大值为 60。
- 默认值为 10。

当超时时间介于 1 到 60（含）之间时，通用打印客户端会等待指定的时间以完成操作。该操作是接收 TCP 套接字操作。套接字是 Windows 操作系统的一项功能，允许通过 TCP/IP 网络进行进程间通信。

当超时时间为 0 时，通用打印客户端使用操作系统定义的默认超时。此配置是此更改之前通用打印客户端先前版本中可用的配置。

通用打印客户端是虚拟投递代理 (VDA) 的组件，负责与通用打印服务器通信。

> **注意：**
>
> 此策略设置适用于 VDA 7.35 及更高版本。

UNIVERSAL PRINT SERVER WEB 服务 (HTTP/SOAP) 发送超时

此设置指定 Universal Print Client 必须等待的秒数，直到 Universal Print Server Web 服务 send() 操作超时。此设置具有以下值。所有这些值都是数字，单位（时间）是秒。

- 最小值为 0。
- 最大值为 60。
- 默认值为 10。

当超时时间在 1 到 60 之间（含）时，Universal Print Client 会等待指定的时间以完成操作。该操作是发送 TCP 套接字操作。套接字是 Windows 操作系统的一项功能，允许通过 TCP/IP 网络进行进程间通信。

当超时时间为 0 时，Universal Print Client 使用操作系统定义的默认超时。此配置是此更改之前 Universal Print Client 早期版本中可用的配置。

Universal Print Client 是 VDA 中与 Universal Print Server 通信的组件。

> **注意：**
>
> 此策略设置适用于 VDA 7.35 及更高版本。

通用打印策略设置

通用打印部分包含用于管理通用打印的策略设置。

通用打印 EMF 处理模式

此设置控制在 Windows 用户设备上处理 EMF 后台打印文件的方法。

默认情况下，EMF 记录直接后台打印到打印机。

将此设置添加到策略时，请选择一个选项：

- 重新处理打印机的 EMF 强制重新处理 EMF 后台打印文件并通过用户设备上的 GDI 子系统发送。您可以将此设置用于需要 EMF 重新处理但可能不会在会话中自动选择的驱动程序。
- 直接后台打印到打印机，与 Citrix Universal™ 打印驱动程序一起使用时，可确保 EMF 记录后台打印并传送到用户设备进行处理。通常，这些 EMF 后台打印文件会直接注入到客户端的后台打印队列中。对于与 EMF 格式兼容的打印机和驱动程序，这是最快的打印方法。

通用打印图像压缩限制

此设置指定以下内容：

- 使用 Citrix Universal 打印驱动程序打印的图像可用的最高质量
- 使用 Citrix Universal 打印驱动程序打印的图像可用的最低压缩级别

默认情况下，图像压缩限制设置为最佳质量（无损压缩）。

如果选择“无压缩”，则仅对 EMF 打印禁用压缩。

将此设置添加到策略时，请选择一个选项：

- 无压缩
- 最佳质量（无损压缩）
- 高质量
- 标准质量
- 降低质量（最大压缩）

将此设置添加到包含**通用打印优化默认值**设置的策略时，请注意以下事项：

- 请考虑**通用打印图像压缩限制**设置中的压缩级别低于**通用打印优化默认值**设置中定义的级别。在这种情况下，图像将按照通用打印图像压缩限制设置中定义的级别进行压缩。
- 如果禁用压缩，则通用打印优化默认值设置的“所需图像质量”和“启用重量级压缩”选项在策略中不起作用。

通用打印优化默认值

此设置指定为会话创建通用打印驱动程序时打印优化的默认值。

- “所需图像质量”指定应用于通用打印的默认图像压缩限制。默认情况下，启用“标准质量”，这意味着用户只能使用标准或降低质量的压缩来打印图像。
- “启用重量级压缩”启用或禁用在不损失图像质量的情况下，将带宽降低到超出“所需图像质量”设置的压缩级别。默认情况下，重量级压缩处于禁用状态。
- “图像和字体缓存”设置指定是否缓存打印流中多次出现的图像和字体。此设置可确保每个唯一的图像或字体仅发送到打印机一次。默认情况下，嵌入式图像和字体会被缓存。这些设置仅在用户设备支持此行为时才适用。
- “允许非管理员修改这些设置”指定用户是否可以在会话中更改默认打印优化设置。默认情况下，不允许用户更改默认打印优化设置。

注意：所有这些选项都支持 EMF 打印。对于 XPS 打印，仅支持“所需图像质量”选项。

将此设置添加到包含**通用打印图像压缩限制**设置的策略时，请注意以下事项：

- 如果**通用打印图像压缩限制**设置中的压缩级别低于**通用打印优化默认值**设置中定义的级别，则图像将按照通用打印图像压缩限制设置中定义的级别进行压缩。
- 如果禁用压缩，则通用打印优化默认值设置中的“所需图像质量”和“启用重量级压缩”选项在策略中不起作用。

通用打印预览首选项

此设置指定是否对自动创建的或通用通用打印机使用打印预览功能。

默认情况下，自动创建的或通用通用打印机不使用打印预览。

将此设置添加到策略时，请选择一个选项：

- 不对自动创建的或通用通用打印机使用打印预览
- 仅对自动创建的打印机使用打印预览
- 仅对通用通用打印机使用打印预览
- 对自动创建的打印机和通用通用打印机都使用打印预览

通用打印质量限制

此设置指定在会话中生成打印输出时可用的最大每英寸点数 (dpi)。

默认情况下，“无限制”处于启用状态，这意味着用户可以选择其连接的打印机允许的最大打印质量。

如果配置此设置，它将限制用户可用的最大打印质量（以输出分辨率表示）。打印质量本身以及用户连接的打印机的打印质量功能都将受限于配置的设置。

例如，如果配置为“中等分辨率 (600 DPI)”，则用户只能以最高 600 DPI 的质量打印输出。此外，**通用打印机**对话框的**高级**选项卡上的**打印质量**设置仅显示最高为“中等质量 (600 DPI)”的解析度设置。

将此设置添加到策略时，请选择一个选项：

- 草稿 (150 DPI)
- 低分辨率 (300 DPI)
- 中分辨率 (600 DPI)
- 高分辨率 (1200 DPI)
- 无限制

安全策略设置

安全部分包含用于配置会话加密和登录数据加密的策略设置。

SecureICA 最低加密级别

此设置指定服务器与用户设备之间发送的会话数据的最低加密级别。

重要提示：对于 Virtual Delivery Agent 7.x，此策略设置只能用于通过 RC5 128 位加密启用登录数据的加密。其他设置仅用于与旧版 Citrix Virtual Apps and Desktops 的向后兼容性。

对于 VDA 7.x，会话数据的加密是使用 VDA 交付组的基本设置来配置的。如果为交付组选择了“启用 Secure ICA”，则会话数据将使用 RC5（128 位）加密进行加密。如果未为交付组选择“启用 Secure ICA”，则会话数据将使用基本加密进行加密。

将此设置添加到策略时，请选择一个选项：

- 基本加密使用非 RC5 算法加密客户端连接。它可防止数据流被直接读取，但可以解密。默认情况下，服务器对客户端-服务器流量使用基本加密。
- RC5（128 位）仅登录使用 RC5 128 位加密对登录数据进行加密，并使用基本加密对客户端连接进行加密。
- RC5（40 位）使用 RC5 40 位加密对客户端连接进行加密。
- RC5（56 位）使用 RC5 56 位加密对客户端连接进行加密。
- RC5（128 位）使用 RC5 128 位加密对客户端连接进行加密。

您为客户端-服务器加密指定的设置可以与您的环境和 Windows 操作系统中的任何其他加密设置进行交互。如果服务器或用户设备上设置了更高优先级的加密级别，则您为已发布的资源指定的设置可能会被覆盖。

您可以提高加密级别，以进一步保护某些用户的通信和消息完整性。如果策略要求更高的加密级别，则使用较低加密级别的 Citrix Receiver 将被拒绝连接。

SecureICA 不执行身份验证或检查数据完整性。要为您的站点提供端到端加密，请将 SecureICA 与 TLS 加密结合使用。

SecureICA 不使用 FIPS 兼容算法。如果此设置存在问题，请配置服务器和 Citrix Receiver 以避免使用 SecureICA。

SecureICA 使用 RFC 2040 中描述的 RC5 分组密码来实现机密性。块大小为 64 位（32 位字单元的倍数）。密钥长度为 128 位。轮数为 12。

RC5 分组密码的密钥在会话创建时协商。协商使用 Diffie-Hellman 算法执行。此协商使用 Diffie-Hellman 公共参数。这些参数在安装 Virtual Delivery Agent 时存储在 Windows 注册表中。公共参数不是秘密的。Diffie-Hellman 协商的结果是一个秘密密钥，RC5 分组密码的会话密钥由此派生。独立的会话密钥用于用户登录和数据传输。此外，独立的会话密钥用于往返 Virtual Delivery Agent 的流

量。因此，每个会话有四个会话密钥。秘密密钥和会话密钥不存储。RC5 分组密码的初始化向量也从秘密密钥派生。

服务器限制策略设置

服务器限制部分包含用于控制空闲连接的策略设置。

服务器空闲计时器间隔

此设置确定在用户没有输入的情况下，不间断的用户会话将保持多长时间。数据以毫秒为单位计算。

默认情况下，空闲连接不会断开连接（服务器空闲计时器间隔 = 0）。Citrix® 建议将此值设置为至少 60000 毫秒（60 秒）。

要显示策略，请选择**多个版本**，清除单会话操作系统版本，然后选择**服务器限制**。

> **注意**
>
> 使用此策略设置时，当会话在指定时间内处于空闲状态时，用户可能会看到一个“空闲计时器已过期”对话框。Citrix 策略设置不控制此 Microsoft 对话框消息。有关详细信息，请参阅 `<http://support.citrix.com/article/CTX118618>`。

会话限制策略设置

“**会话限制**”部分包含策略设置，这些设置控制会话在强制注销之前保持连接的时长。

断开连接的会话计时器

此设置启用或禁用一个计时器，该计时器指定断开连接的锁定桌面在会话注销之前保持锁定的时长。

如果此计时器已启用，则断开连接的会话将在计时器到期时注销。

默认情况下，断开连接的会话不会注销。

远程电脑访问断开连接会话计时器

此设置启用或禁用一个计时器，该计时器在计时器到期后注销断开连接的用户会话。如果启用此设置，请使用“**断开连接会话计时器间隔**”设置来指定断开连接的桌面在用户会话注销之前保持锁定的分钟数。

默认情况下，此设置为禁用状态。

断开连接的会话计时器间隔

此设置指定断开连接的锁定桌面在会话注销之前保持锁定的分钟数。

默认情况下，时间段为 1,440 分钟（24 小时）。

断开连接会话计时器 – 多会话

此设置启用或禁用一个计时器，以确定断开连接的 RDS 会话在注销之前可以持续多长时间。默认情况下，此计时器处于禁用状态，并且断开连接的会话不会注销。

断开连接会话计时器间隔 – 多会话

此设置确定断开连接的 RDS 会话在注销之前可以持续多少分钟。默认情况下，时间段为 1440 分钟（24 小时）。

会话连接计时器

此设置启用或禁用一个计时器，该计时器指定用户设备与桌面之间不间断连接的最长持续时间。如果此计时器已启用，则会话将在计时器到期时断开连接或注销。Microsoft 的“**达到时间限制时结束会话**”设置决定会话的下一个状态。

默认情况下，此计时器处于禁用状态。

会话连接计时器间隔

此设置指定用户设备与桌面之间不间断连接的最长分钟数。

默认情况下，最长持续时间为 1,440 分钟（24 小时）。

会话连接计时器 – 多会话

此设置启用或禁用一个计时器，该计时器指定用户设备与终端服务器之间不间断连接的最长持续时间。默认情况下，此计时器处于禁用状态。

会话连接计时器间隔 – 多会话

此设置指定用户设备与 RDS 会话之间不间断连接的最长分钟数。默认情况下，最长持续时间为 1440 分钟（24 小时）。

会话空闲计时器

当用户未提供任何输入时，此设置用于启用或禁用：

- 一个计时器，用于指定用户设备与桌面之间不间断连接的维护时长。

当此计时器到期时，会话将进入断开连接状态，并应用**断开连接会话计时器**。如果**断开连接会话计时器**被禁用，则会话不会注销。

默认情况下，此计时器处于启用状态。

会话空闲计时器间隔

当用户没有输入时，此设置用于指定：

- 用户设备与桌面之间不间断连接的维护分钟数。

默认情况下，空闲连接会维护 1,440 分钟（24 小时）。

会话空闲计时器 – 多会话

此设置启用或禁用计时器，以确定用户设备与终端服务器之间空闲连接的最长持续时间。默认情况下，此计时器处于禁用状态。

会话空闲计时器间隔 – 多会话

此设置指定用户设备与 RDS 会话之间空闲连接的分钟数。默认情况下，最长持续时间为 1440 分钟（24 小时）。

> **注意：**
>
> 使用 Citrix® 策略配置的多会话计算机的计时器设置预计会覆盖通过 Microsoft 组策略配置的计时器设置。为避免意外行为，我们建议您使用这两种方法之一来配置计时器设置。

会话管理策略设置

会话管理部分包括用于控制会话如何管理的策略设置。

关闭最后一个应用程序后断开已发布的应用程序会话

启用后，一旦该会话中的所有已发布的应用程序都已关闭，最终用户将从已发布的应用程序会话断开连接，而不是注销。

默认情况下，此设置处于禁用状态，当会话中的所有已发布的应用程序都关闭时，用户会话将注销。

会话可靠性策略设置

会话可靠性部分包含用于管理会话可靠性连接的策略设置。

会话可靠性连接

此设置允许或阻止在网络连接丢失期间保持会话打开。会话可靠性与客户端自动重新连接功能一起，允许用户在从网络中断中恢复后自动重新连接到其 Citrix Workspace™ 应用程序会话。默认情况下，会话可靠性处于“允许”状态。

Web Studio 中的设置对以下客户端强制执行：

- Citrix Workspace 应用程序 1808 及更高版本
- 适用于 Windows 的 Citrix Receiver 4.7 及更高版本。

Web Studio 策略会覆盖客户端上的 Citrix Receiver™ 组策略对象。Web Studio 中对这些策略的更新会将会话可靠性从服务器同步到客户端。

> **注意：**
>
> - 适用于 Windows 的 Citrix Receiver 4.7 及更高版本以及适用于 Windows 的 Citrix Workspace 应用程序 - 在 Web Studio 中设置策略。
> - 适用于 Windows 的 Citrix Receiver 4.7 之前的版本 - 在 Web Studio 中设置策略。同时在客户端上设置 Citrix Receiver 组策略对象模板以保持一致的行为。

当网络连接中断时，会话可靠性可使会话保持活动状态并显示在用户屏幕上。用户将继续看到他们正在使用的应用程序，直到网络连接恢复。

使用会话可靠性可使会话在服务器上保持活动状态。为了指示连接已丢失，用户显示会变得不透明。用户可能会在中断期间看到冻结的会话。当网络连接恢复时，用户可以恢复与应用程序的交互。会话可靠性会在不提示重新身份验证的情况下重新连接用户。

如果同时使用会话可靠性和客户端自动重新连接，这两个功能将依次工作。会话可靠性会在会话可靠性超时设置中指定的时间后关闭（或断开连接）用户会话。之后，客户端自动重新连接设置将生效，尝试将用户重新连接到断开连接的会话。

默认情况下，会话可靠性处于“允许”状态。

> **注意：**
>
> 使用 Citrix ADC 时，必须在 Citrix StoreFront > **管理 Citrix Gateway** / **安全票证颁发机构**中选择**启用会话可靠性**以代理 ICA 连接。

会话可靠性端口号

此设置指定传入会话可靠性连接的 TCP 端口号。

默认情况下，端口号设置为 2598。

会话可靠性超时

此设置指定时间长度（以秒为单位）。此时间是会话可靠性代理在允许会话断开连接之前等待用户重新连接的时间。

尽管您可以延长会话保持打开状态的时间，但此功能仅为方便起见，不会提示用户重新进行身份验证。会话打开的时间越长，用户无人看管设备并可能被未经授权的用户访问的可能性就越大。

默认情况下，超时设置为 180 秒（即三分钟）。

会话水印策略设置

会话水印部分包含用于配置此功能的策略设置。 启用此功能会导致 VDA 计算机的网络带宽和 CPU 使用率显著增加。我们建议您根据可用的硬件资源为选定的 VDA 计算机配置会话水印。

> **重要提示**
>
> 启用会话水印以使其他水印策略设置生效。为获得更好的用户体验，请勿启用两个以上的水印文本项。

启用会话水印

启用此设置后，会话显示将具有不透明的文本水印，其中显示会话特定信息。其他水印设置取决于此设置是否启用。

默认情况下，会话水印处于禁用状态。

包括客户端 IP 地址

启用此设置后，会话将显示当前客户端 IP 地址作为水印。

默认情况下，禁用“包括客户端 IP 地址”。

包括连接时间

启用此设置后，会话水印将显示连接时间。格式为 yyyy/mm/dd hh:mm。显示的时间基于系统时钟和时区。

默认情况下，禁用“包括连接时间”。

包括登录用户名

启用此设置后，会话将当前登录用户名显示为水印。显示格式为 USERNAME@DOMAINNAME。我们建议用户名最多为 20 个字符。当用户名超过 20 个字符时，可能会出现字符字体过小或截断，从而降低水印效果。

默认情况下，启用“包括登录用户名”。

包括 VDA 主机名

启用此设置后，会话将当前 ICA® 会话的 VDA 主机名显示为水印。

默认情况下，启用“包括 VDA 主机名”。

包括 VDA IP 地址

启用此设置后，会话将当前 ICA 会话的 VDA IP 地址显示为水印。

默认情况下，禁用 VDA IP 地址。

会话水印样式

此设置控制是显示单个水印文本标签还是多个标签。从“**值**”下拉菜单中选择“**多个**”或“**单个**”。

多个在会话中显示五个水印标签。一个在中心，四个在角落。

单个在会话中心显示一个水印标签。

默认情况下，会话水印样式为“多个”。

水印自定义文本

此设置允许您应用自定义文本（例如，公司名称）以显示在会话水印中。当您配置非空字符串时，它会在新行中显示文本，并附加水印中启用的其他信息。水印自定义文本限制为 25 个 Unicode 字符。如果配置的字符串较长，则会截断为 25 个字符。

没有默认文本。

从 Citrix Virtual Apps and Desktops™ 7 2206 开始，您可以使用文本中的自定义标签添加更多自定义项。因此，自定义文本中的最大字符数增加到 1024。

下表描述了水印设置的可用标签：

标记	描述	示例
`<font=value>`	允许您更改水印文本的字体。该值是 VDA 上可用字体的名称。	`<font=Courier New>`
`<fontzoom=value>`	允许您设置字体缩放因子的百分比。水印文本的 200% 缩放值为 200。	`<fontzoom=200>`

标记	描述	示例
`<position=value>`	允许您更改水印文本的位置。可选值为 `center`、`topleft`、`topright`、`bottomleft` 和 `bottomright`。此标记仅适用于单一样式。	`<position=topright>`
`<rotation=value>`	允许您旋转水印文本。该值以度为单位指定，范围为 -360 到 360。	`<rotation=45>`
`<style=value>`	允许您更改显示样式。此标记会覆盖会话水印样式策略。	`<style=single>`

可用的水印样式如下：

- 单一样式 - 会话中心显示一个水印文本标签。您可以使用位置标记更改其位置。
- x 样式或多重样式 - 会话中显示五个水印标签 - 一个在中心，每个角一个。
- 平铺 - 会话中显示多个标签。水印文本均匀地分布在整个屏幕上。

下表描述了用于更改水印文本的可用标记：

标记	描述
`<clientip>`	端点的 IP 地址。
`<date>`	会话建立的日期。
`<domain>`	登录用户帐户的域名。
`<hostname>`	VDA 的计算机名称。
`<newline>`	创建一个额外的行。
`<serverip>`	VDA 的 IP 地址。
`<time>`	会话建立时间。
`<username>`	用户的名称。

注意：

- **水印自定义文本**策略仅在**启用会话水印**策略已启用时生效。其默认值为*禁用*。
- 如果您使用标签来更改水印文本，则除**启用会话水印**之外的所有其他会话水印策略都将被忽略。如果您使用标签进行水印文本设置，则可以使用所有其他水印策略。

水印透明度

您可以指定水印不透明度，范围为 0 到 100。指定的值越大，水印越不透明。

默认情况下，值为 17。

时区控制策略设置

“**时区控制**”部分包含与在会话中使用本地时间相关的策略设置。

为旧版客户端估算本地时间

此设置启用或禁用估算用户设备的本地时区。这些设备包括向服务器发送不准确时区信息的用户设备。

默认情况下，服务器会在必要时估算本地时区。

此设置旨在用于不向服务器发送详细时区信息的旧版 Citrix Receiver 或 ICA 客户端。请注意，此设置与向服务器发送详细时区信息的 Citrix Receiver 配合使用。例如，受支持的 Windows 版 Citrix Receiver™。在这种情况下，此设置无效。

在会话断开连接或注销时恢复桌面操作系统时区

假设用户断开连接或注销会话。在这种情况下，此设置决定是否将单会话操作系统 VDA 的时区设置恢复为计算机的原始时区。如果启用此设置，当用户断开连接或注销时，VDA 会将计算机的时区恢复为其原始设置。要使此设置生效，请将“**使用客户端本地时间**”设置为“**使用客户端时区**”。

默认情况下，此设置处于启用状态。

使用客户端本地时间

此设置决定用户会话的时区设置。选项包括会话主机的时区（服务器时区）或用户设备的时区（客户端时区）。

默认情况下，使用会话主机的时区。

要使此设置在**多会话**会话主机中生效，请在组策略编辑器中启用“**允许时区重定向**”设置。该设置位于“**本地计算机策略**”>“**计算机配置**”>“**管理模板**”>“**Windows 组件**”>“**远程桌面服务**”>“**远程桌面会话主机**”>“**设备和资源重定向**”中。

> **重要提示：**
>
> 使用单会话 VDA 时，**Citrix Portica 时区服务 (CtxPicaTzSvc)** 会在 VDA 安装期间自动添加到“**更改时区**”用户权限分配策略中。如果您有任何策略或流程会从这些策略中删除用户或进程，请务必修改它们，以确保 Citrix 服务不会被删除。否则，时区重定向将不起作用。

TWAIN 设备策略设置

“**TWAIN 设备**”部分包含与以下内容相关的策略设置：

- 映射客户端 TWAIN 设备，例如数码相机或扫描仪
- 优化从服务器到客户端的图像传输

> **注意：**
>
> TWAIN 2.0 可在 Citrix Receiver for Windows 4.5 中获得支持。

客户端 TWAIN 设备重定向

TWAIN 设备使用 TWAIN 协议与服务器托管的图像处理应用程序通信。

此设置允许或阻止用户访问用户设备上的 TWAIN 设备。默认情况下，允许 TWAIN 设备重定向。

以下策略设置相关：

- TWAIN 压缩级别
- TWAIN 设备重定向带宽限制
- TWAIN 设备重定向带宽限制百分比

TWAIN 压缩级别

此设置指定从客户端到服务器的图像传输的压缩级别。使用“低”可获得最佳图像质量，使用“中”可获得良好图像质量，使用“高”可获得低图像质量。默认情况下，应用中等压缩。

USB 设备策略设置

USB 设备部分包含用于管理 USB 设备文件重定向的策略设置。

客户端 USB 设备优化规则

客户端 USB 设备优化规则可应用于设备，以禁用优化或更改优化模式。

当用户插入 USB 输入设备时，主机将检查 **USB 策略**设置是否允许该设备。如果允许该设备，主机将检查该设备的**客户端 USB 设备优化规则**。如果未指定任何规则，则设备不会进行优化。捕获模式 (04) 是签名设备的推荐模式。对于在高延迟下性能下降的其他设备，管理员可以启用交互模式 (02)。有关可用模式的说明，请参阅本文中的表格。

须知

- 对于 Wacom 签名板和数位板的使用，我们建议您禁用屏幕保护程序。有关如何禁用屏幕保护程序的步骤，请参阅本节末尾。
- 对 Wacom STU 签名板和数位板系列产品优化的支持已在 Citrix Virtual Apps and Desktops™ 策略的安装中预先配置。
- 签名设备可在 Citrix Virtual Apps and Desktops 中使用，并且无需驱动程序即可用作签名设备。Wacom 提供了更多可用于进一步自定义设备的软件。请参阅 `<http://www.wacom.com/>`。
- 绘图板。某些绘图输入设备可能在 PCI/ACPI 总线上显示为 HID 设备，并且不受支持。将这些设备连接到客户端上的 USB 主机控制器，以便在 Citrix Virtual Desktops 会话中进行重定向。

策略规则采用以空格分隔的 tag=value 表达式格式。支持以下标记：

标记名称	描述
模式	优化模式支持 class=**03** 的输入设备。支持的模式包括：无优化 - 值 **01**。交互模式 - 值 **02**。建议用于笔式数位板和 3D Pro 鼠标等设备。捕获模式 - 值 **04**。首选用于签名板等设备。
VID	来自设备描述符的供应商 ID，为四位十六进制数。
PID	来自设备描述符的产品 ID，为四位十六进制数字。
REV	来自设备描述符的修订版本 ID，为四位十六进制数字。
类	来自设备描述符或接口描述符的类。

标记名称	描述
子类	来自设备描述符或接口描述符的子类。
协议	来自设备描述符或接口描述符的协议。

示例

Mode=00000004 VID=067B PID=1230 class=03 #在捕获模式下运行的输入设备

Mode=00000002 VID=067B PID=1230 class=03 #在交互模式下运行的输入设备（默认）

Mode=00000001 VID=067B PID=1230 class=03 #在没有任何优化的情况下运行的输入设备

Mode=00000100 VID=067B PID=1230 # 设备设置优化已禁用（默认）

Mode=00000200 VID=067B PID=1230 # 设备设置优化已启用

禁用 Wacom 签名板设备的屏幕保护程序

对于 Wacom 签名板和数位板的使用，Citrix® 建议您按如下方式禁用屏幕保护程序：

1. 重定向设备后，安装 **Wacom-STU-Driver**。
2. 安装 **Wacom-STU-Display MSI** 以访问签名板控制面板。
3. 转到 **控制面板 > Wacom STU Display > STU430** 或 **STU530**，然后选择您型号对应的选项卡。
4. 选择 **更改**，然后在 UAC 安全窗口弹出时选择 **是**。
5. 选择 **禁用幻灯片放映**，然后选择 **应用**。

为一种签名板型号设置此设置后，它将应用于所有型号。

客户端 USB 设备重定向

此设置允许或阻止将 USB 设备重定向到用户设备以及从用户设备重定向 USB 设备。

默认情况下，USB 设备不会被重定向。

客户端 USB 设备重定向规则

此设置指定 USB 设备的重定向规则。

默认情况下，未指定任何规则。

当用户插入 USB 设备时，主机设备会依次对照每条策略规则进行检查，直到找到匹配项。任何设备的第一个匹配项都被视为最终结果。如果第一个匹配项是“允许”规则，则设备将远程连接到虚拟桌

面。如果第一个匹配项是“拒绝”规则，则设备仅可用于本地桌面。如果未找到匹配项，则使用默认规则。

策略规则采用 {Allow: | Deny:} 格式，后跟一组以空格分隔的 tag=value 表达式。支持以下标签：

标签名称	描述
VID	设备描述符中的供应商 ID
PID	设备描述符中的产品 ID
REL	设备描述符中的发布 ID
类	设备描述符或接口描述符中的类
子类	设备描述符或接口描述符中的子类
协议	设备描述符或接口描述符中的协议

创建策略规则时，请记住：

- 规则不区分大小写。
- 规则末尾可以有一个可选注释，以 # 开头。
- 空行和纯注释行将被忽略。
- 标签必须使用匹配运算符 =（例如，VID=067B_。
- 每条规则必须另起一行，或者作为分号分隔列表的一部分。
- 请参阅 USB Implementers Forum, Inc. 网站上提供的 USB 类代码。

管理员定义的 USB 策略规则示例：

- 允许: VID=067B PID=0007 # 另一家公司，另一个闪存驱动器
- 拒绝: Class=08 subclass=05 # 大容量存储
- 要创建拒绝所有 USB 设备的规则，请使用“DENY:”而不带其他标签。

客户端 USB 即插即用设备重定向

此设置允许或阻止在客户端会话中使用即插即用设备，例如摄像头或销售点 (POS) 设备。

默认情况下，允许即插即用设备重定向。当设置为“允许”时，特定用户或组的所有即插即用设备都将被重定向。当设置为“禁止”时，不重定向任何设备。

配置 USB 设备的自动重定向

启用 USB 支持后，USB 设备将自动重定向。此外，USB 用户首选项设置也配置为自动连接 USB 设备。

> **注意：**

> 在 Receiver for Windows 4.2 中，当在桌面设备模式下运行时，USB 设备也会自动重定向。此外，连接栏也不存在。在早期版本的 Citrix Receiver for Windows 中，USB 设备在以下情况下也会自动重定向：

> - 桌面设备模式
> - 虚拟机 (VM) 托管应用程序

> 并非总是最好重定向所有 USB 设备。用户可以从未自动重定向的 USB 设备列表中显式重定向设备。要阻止 USB 设备被列出或重定向，请在客户端端点或 DDC 策略上使用 DeviceRules。有关更多详细信息，请参阅管理指南。

> **注意：**

> 不正确地使用注册表编辑器可能会导致严重问题，甚至可能需要重新安装操作系统。Citrix 无法保证可以解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。在编辑注册表之前，请务必备份注册表。

USB 设备自动重定向的用户首选项设置

策略：

1. 打开 **本地组策略编辑器**，然后转到 **管理模板 > Citrix 组件 > Citrix Receiver™ > 远程处理客户端设备 > 通用 USB 远程处理**。
2. 打开 **新建 USB 设备**，选择 **已启用**，然后单击 **确定**。
3. 打开 **现有 USB 设备**，选择 **已启用**，然后单击 **确定**。

思杰接收器：

1. 转到 **Citrix Receiver 首选项 > 连接**。

2. 确保选中以下选项：

   - 会话启动时，自动连接设备
   - 会话运行时连接新设备时，自动连接设备。

3. 单击 **确定**。

所有注册表项和策略更改都应用于 Windows 客户端设备。

普通 USB 打印机重定向

普通 USB 打印机的最佳解决方案是使用专用的通用打印机驱动程序和虚拟通道来执行打印。默认情况下，普通 USB 打印机不会自动重定向。

普通打印机使用启发式方法检测。此外，例如，具有扫描功能的高级打印机可能需要使用 USB 支持进行重定向才能完全正常工作。

使用此注册表配置普通打印机是否自动重定向：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectPrinters

类型: DWORD

数据: 00000000

默认值为 0（不自动重定向）。将值更改为大于零的任何数字将启用 USB 支持以重定向普通 USB 打印机。

您还可以将 Active Directory 策略部署到此注册表项，并在两者都存在时覆盖非策略值：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectPrinters

类型: DWORD

数据: 00000000

普通音频设备重定向

与普通打印机类似，最佳用户体验是通过使用 ICA® 的专用音频虚拟通道从普通音频设备发送音频数据实现的。但是，您可能需要使用 USB 支持重定向某些专用设备。启发式方法用于确定哪些设备是普通音频设备。

在客户端端点上使用此注册表配置普通音频设备是否自动重定向：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectAudio

类型: DWORD

数据: 00000000

默认设置为 0 (不自动重定向)。将值更改为非零，将重定向支持 USB 的普通 USB 音频设备。

您可以使用 Active Directory 策略将此值部署到注册表项，并在两者都存在时覆盖非策略值：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectAudio

类型: DWORD

数据: 00000000

普通存储设备 (大容量存储设备) 重定向

对于普通存储设备，您可以使用专用虚拟通道获得最佳用户体验，例如执行优化的客户端驱动器映射。除了简单的文件读写之外，要执行某些特殊任务，例如刻录 CD/DVD 或访问加密文件系统设备，设备可能仍需要使用通用 USB 支持进行重定向。

使用启发式方法来确定哪些设备是普通存储设备。使用此注册表项配置是否自动重定向普通存储设备：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectStorage

类型: DWORD

数据: 00000000

默认设置为 0 (不自动重定向)。将值更改为非零，将重定向使用通用 USB 支持的普通 USB 存储设备。

您还可以使用 Active Directory 策略将此值部署到以下注册表项，并在两者都存在时覆盖非策略值：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectStorage

类型: DWORD

数据: 00000000

> **注意：**
>
> 如果您使用通用 USB 支持，则无法配置对普通存储设备的只读访问，而如果使用 CDM，则可以配置。

带硬件加密的 USB 闪存驱动器重定向

带硬件加密的 USB 闪存驱动器通常由一个加密存储分区和第二个 *实用程序* 分区组成，该分区包含用于解锁加密分区的实用程序。对于 USB 闪存驱动器设备，请使用专用的客户端驱动器映射/动态拇指驱动器映射 HDX 虚拟通道，该通道还执行优化，以实现最佳用户体验。

通用 USB 重定向对于以下情况是必需的：

- 非 Windows 客户端（例如，Linux 客户端）
- 客户限制（锁定）了用户对客户端本地功能的访问的客户端

通用 USB 重定向可以将任何不带硬件加密的 USB 存储设备重定向到单会话操作系统和多会话操作系统 VDA 会话中。

在 Citrix Virtual Apps and Desktops™ 7 1808 之前，带硬件加密的 USB 闪存驱动器无法以任何有用的方式重定向到单会话操作系统或多会话操作系统 VDA 会话中。Citrix Virtual Apps and Desktops 7 1808 中引入的一项新功能增强支持将带硬件加密的 USB 闪存驱动器进行通用 USB 重定向到单会话操作系统和多会话操作系统 VDA 会话中。 设备重定向后，其任何驱动器都不会显示在本地客户端上。因此，如果需要解锁驱动器，请在会话中执行此操作。此功能需要 Windows 更新 KB4074590。

普通静态图像设备（扫描仪和数码相机）

对于普通静态图像设备，请使用专用虚拟通道（例如 TWAIN 虚拟通道），该通道还执行优化，以实现最佳用户体验。这些设备必须符合行业标准。如果设备不合规或未按预期使用，则通用 USB 重定向可能是使用该设备的唯一方法。使用启发式方法来确定哪些设备是普通静态图像设备。

使用此注册表项配置普通静态图像设备是否自动重定向：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectImage

类型: DWORD

数据: 00000000

默认设置为 0（不自动重定向）。将值更改为非零，将使用通用 USB 重定向普通 USB 静态图像设备。

您还可以使用 Active Directory 策略将此值部署到此注册表项，并在两者都存在时覆盖非策略值：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectImage

类型: DWORD

数据: 00000000

设备特定设置

用于选择 Citrix 可优化设备的启发式方法并不总是与您的需求相符。Citrix 可优化设备的示例包括打印机、音频、视频、存储和静态图像设备。您可能希望控制未在上面列出的设备的自动重定向。您可以根据设备控制自动重定向。

例如，DemoTech 2,000 条形码阅读器无需使用 USB 支持进行重定向。它的供应商标识符为 12AB，产品标识符为 5678。这些十六进制数字可以在设备管理器中找到。

为防止其自动重定向，请创建此设备特定的注册表项：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名称: AutoRedirect

类型: DWORD

数据: 00000000

值为 0 可防止设备自动重定向。非零值表示必须考虑自动重定向设备（取决于用户首选项）。供应商和产品标识符之间有一个空格字符。

您还可以使用 Active Directory 策略将此值部署到此注册表项。如果两者都存在，它将覆盖非策略值：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名称: AutoRedirect

类型: DWORD

数据: 00000000

设备特定的 AutoRedirect 设置优先于上述更通用的 AutoRedirectXXX 值。Citrix 优化设备的默认启发式算法可能会将设备误判为通用设备。因此，将设备特定的 AutoRedirect 值设置为 1 以自动重定向它。

允许自动连接现有 USB 设备

此设置允许或阻止在会话开始时连接到端点的现有 USB 设备自动连接到远程会话。

将此设置添加到策略时，请选择以下选项之一：

- 在重定向可用 USB 设备前询问。
- 不自动重定向可用 USB 设备。
- 自动重定向可用 USB 设备。

默认情况下，选中“**在重定向可用 USB 设备前询问**”选项。根据所选策略，客户端“**首选项**”>“**设备**”部分中选择的选项可以被覆盖。

> **注意：**
>
> 目前，“**允许自动连接现有 USB 设备**”策略仅适用于适用于 Windows 的 Citrix Workspace™ 应用程序。

允许自动连接新插入的 USB 设备

此设置允许或阻止在会话期间插入到端点的 USB 设备自动连接到远程会话。

将此设置添加到策略时，请选择以下选项之一：

- 在重定向可用 USB 设备之前询问。
- 不要自动重定向可用 USB 设备。
- 自动重定向可用 USB 设备。

默认情况下，选中“**在重定向可用 USB 设备之前询问**”选项。根据所选策略，客户端“**首选项**”>“**设备**”部分中选择的选项可以被覆盖。

> **注意：**
>
> 当前，“**允许自动连接新插入的 USB 设备**”策略仅适用于适用于 Windows 的 Citrix Workspace 应用程序。

客户端 USB 设备重定向规则（版本 2）

此设置指定了用于筛选、拆分和自动连接 USB 设备到远程会话的规则。

选中此设置后，主机将使用在此设置中配置的设备规则覆盖 *客户端 USB 设备重定向规则* 设置。

有关详细信息，请参阅配置复合 USB 设备重定向。

虚拟通道允许列表策略设置

虚拟通道允许列表策略设置启用允许列表的使用，该列表指定允许在 ICA® 会话中打开哪些虚拟通道。

禁用时，允许所有虚拟通道。

启用时，仅允许 Citrix® 虚拟通道。

要使用自定义或第三方虚拟通道，请将虚拟通道添加到列表中。要将虚拟通道添加到列表中，请执行以下操作：

1. 输入虚拟通道名称，后跟逗号。
2. 输入访问该虚拟通道的进程路径。

可以列出更多可执行路径，路径之间用逗号分隔。

例如，

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

从 Citrix Virtual Apps and Desktops 7 2109 开始，虚拟通道允许列表默认启用。有关将虚拟通道添加到允许列表的详细信息，请参阅将虚拟通道添加到允许列表

如果您正在使用适用于 Skype for Business 的 HDX RealTime Optimization Pack，请将虚拟通道添加到允许列表。有关详细信息，请参阅 HDX RealTime Optimization Pack 文档。

> **重要提示：**
>
> 必须重新启动 VDA 计算机才能使设置生效。
>
> 有关虚拟通道的详细信息，请参阅 ICA 虚拟通道。

虚拟通道允许列表日志记录

您可以使用此策略设置配置虚拟通道允许列表日志记录级别。

以下选项可用：

选项	描述
已禁用	禁用所有日志事件。
仅记录警告	仅记录尝试打开且不在允许列表中的自定义虚拟通道的事件。
记录所有事件	记录所有事件

虚拟通道允许列表日志节流

您可以使用此策略设置来配置活动会话的事件日志记录频率。

每个虚拟通道的所有事件都将在首次出现时记录。在会话处于活动状态期间，重复事件将在节流期内被抑制。如果会话断开连接，节流期将重置。

用于 DVC 的虚拟通道允许列表

启用允许列表的使用，该列表指定允许在 ICA 会话中打开哪些动态虚拟通道。

禁用时，允许所有动态虚拟通道。

启用时，不允许任何动态虚拟通道。要将动态虚拟通道 (DVC) 与此功能结合使用，必须将 DVC 添加到列表中。要将 DVC 添加到列表中，请在会话主机中输入访问 DVC 的进程路径，后跟逗号，然后是客户端插件名称，后跟逗号和插件使用的侦听器名称。可以添加多个侦听器名称，用逗号分隔。

您可以使用通配符以允许插件支持的所有侦听器。

您还可以使用通配符替换进程路径中的单个目录名称、进程路径中的部分目录名称、替换可执行文件的名称或替换可执行文件的部分名称。

对此设置的更改仅在重新启动会话主机后生效。

示例：客户端插件：`DvcPlugin1.dll`, `DvcPlugin2.dll`, `DvcPlugin3.dll`

允许列表条目：`C:\Program Files\App\run1.2.exe,DvcPlugin1,` ListenerName1 `C:\Program Files*\run*.exe,DvcPlugin2,ListenerName1,ListenerName2` `C:\Program Files\App\run1.2.exe,DvcPlugin3,*`

视觉显示策略设置

“**视觉显示**”部分包含用于控制从虚拟桌面发送到用户设备的图像质量的策略设置。

简单图形的首选颜色深度

此策略设置在 VDA 7.6 FP3 及更高版本中可用。8 位选项在 VDA 7.12 及更高版本中可用。

此设置可以降低通过网络发送简单图形时的颜色深度。将每像素颜色深度降低到 8 位或 16 位可能会提高低带宽连接的响应能力。但是，此操作可能会导致图像质量略有下降。当 使用视频编解码器进行压缩 策略设置设置为**整个屏幕**时，不支持 8 位颜色深度。

默认的首选颜色深度为每像素 24 位。

如果在 VDA 7.11 及更早版本上应用 8 位设置，VDA 将回退到 24 位（默认）颜色深度。

目标帧率

此设置指定从虚拟桌面发送到用户设备的最大每秒帧数。

默认情况下，最大值为每秒 30 帧。

设置较高的每秒帧数（例如 30）可改善用户体验，但需要更多带宽。降低每秒帧数（例如 10）可在牺牲用户体验的情况下最大限度地提高服务器可伸缩性。对于 CPU 速度较慢的用户设备，请指定较低的值以改善用户体验。

支持的最大每秒帧速率为 60。

视觉质量

此设置指定用户设备上显示的图像所需的视觉质量。

默认情况下，此设置为“中”。

要指定图像质量，请选择以下选项之一：

- **低** - 建议用于带宽受限的网络，在这种情况下，可以牺牲视觉质量以提高交互性
- **中** - 在大多数用例中提供最佳性能和带宽效率
- **高** - 如果您需要视觉无损的图像质量，建议使用此设置
- **构建为无损** - 在网络活动高峰期向用户设备发送有损图像，并在网络活动减少后发送无损图像。此设置可提高带宽受限网络连接的性能
- **始终无损** - 当保留图像数据至关重要时，选择**始终无损**以确保有损数据永远不会发送到用户设备。例如，在显示不允许任何质量损失的 X 射线图像时。

动态图像策略设置

“**动态图像**”部分包含允许您移除或更改动态图像压缩的设置。

最低图像质量

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

此设置指定了自适应显示可接受的最低图像质量。使用的压缩越少，显示的图像质量越高。可选择超高、很高、高、正常或低压缩。

默认情况下，此设置为正常。

动态图像压缩

此设置指定是否启用自适应显示。自适应显示会根据可用带宽自动调整幻灯片放映中视频和过渡幻灯片的图像质量。启用自适应显示后，用户应能看到流畅运行的演示文稿，且质量不会降低。

默认情况下，自适应显示已启用。

对于 VDA 7.0 到 7.6 版本，此设置仅在启用旧版图形模式时适用。对于 VDA 7.6 FP1 及更高版本，此设置在启用旧版图形模式时适用，或者在禁用旧版图形模式且未使用视频编解码器压缩图形时适用。

启用旧版图形模式时，必须重新启动会话，策略更改才能生效。自适应显示与渐进式显示互斥；启用自适应显示会禁用渐进式显示，反之亦然。但是，渐进式显示和自适应显示可以同时禁用。渐进式显示作为一项旧版功能，不建议用于 XenApp 或 XenDesktop。设置渐进式阈值级别将禁用自适应显示。

渐进式压缩级别

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

此设置提供细节较少但初始显示速度更快的图像。

默认情况下，不应用渐进式压缩。

由正常有损压缩设置定义的更详细图像在可用时显示。使用很高或超高压缩可改善带宽密集型图形（例如照片）的观看效果。

要使渐进式压缩有效，其压缩级别必须高于有损压缩级别设置。

注意：与渐进式压缩相关的压缩级别提高，也增强了动态图像在客户端连接上的交互性。动态图像（例如旋转的三维模型）的质量会暂时降低，直到图像停止移动，此时将应用正常的有损压缩设置。

以下策略设置相关：

- 渐进式压缩阈值
- 渐进式重量级压缩

渐进式压缩阈值

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

此设置表示应用渐进式压缩的连接的最大带宽（以千比特/秒为单位）。此设置仅适用于低于此带宽的客户端连接。

默认情况下，阈值为每秒 2147483647 千比特。

以下策略设置相关：

- 渐进式压缩阈值
- 渐进式重量级压缩

目标最小帧率

此设置指定了系统在低带宽条件下尝试为动态图像维持的每秒最低帧率。

默认情况下，此值设置为 10fps。

对于 VDA 7.0 到 7.6 版本，此设置仅在启用旧版图形模式时适用。对于 VDA 7.6 FP1 及更高版本，此设置在禁用或启用旧版图形模式时均适用。

> **注意：**
>
> 目标最低帧率策略已弃用，并设置为 10 fps。最终用户可以通过使用图形状态指示器中的质量滑块来更改此设置。

静态图像策略设置

“**静态图像**”部分包含的设置使您能够删除或更改静态图像的压缩。

额外颜色压缩

此设置启用或禁用对通过带宽受限的客户端连接传输的图像使用额外颜色压缩，通过降低显示图像的质量来提高响应速度。

默认情况下，额外颜色压缩处于禁用状态。

启用后，仅当客户端连接带宽低于“额外颜色压缩阈值”时，才应用额外颜色压缩。当客户端连接带宽高于阈值或选择“禁用”时，不应用额外颜色压缩。

额外颜色压缩阈值

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用“旧版图形模式”策略设置时适用。

此设置表示连接的最大带宽（以千比特/秒为单位），低于此带宽时将应用额外颜色压缩。如果客户端连接带宽低于设定值，则在启用额外颜色压缩的情况下，将应用额外颜色压缩。

默认情况下，阈值为 8192 千比特/秒。

重量级压缩

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用“旧版图形模式”策略设置时适用。

此设置启用或禁用通过使用更高级但更占用 CPU 的图形算法，在不损失图像质量的情况下，将带宽减少到超出渐进式压缩的程度。

默认情况下，重量级压缩处于禁用状态。

如果启用，重量级压缩将应用于所有有损压缩设置。它在 Citrix Workspace™ 应用程序上受支持，但对其他插件无效。

以下策略设置相关：

- 渐进式压缩级别
- 渐进式压缩阈值

有损压缩级别

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

此设置控制通过带宽受限的客户端连接传输图像时使用的有损压缩程度。在这种情况下，不压缩显示图像可能会很慢。

默认情况下，选择中等压缩。

对于带宽密集型图像，为提高响应速度，请使用高压缩。在图像数据保存至关重要的情况下；例如，在显示不允许任何质量损失的 X 射线图像时，您可能不希望使用有损压缩。

相关策略设置：有损压缩阈值

有损压缩阈值

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

此设置表示应用有损压缩的连接的最大带宽（以千比特/秒为单位）。

默认情况下，阈值为 2147483647 千比特/秒。

将“有损压缩级别”设置添加到策略中且不包含指定的阈值，可以提高通过 LAN 显示高细节位图（例如照片）的速度。

相关策略设置：有损压缩级别

WebSockets 策略设置

WebSockets 部分包含用于通过适用于 HTML5 的 Citrix Workspace™ 应用程序访问虚拟桌面和托管应用程序的策略设置。WebSockets 功能通过在基于浏览器的应用程序和服务器之间进行双向通信来提高安全性并降低开销。此功能无需打开多个 HTTP 连接即可实现此目的。

WebSockets 连接

此设置允许或禁止 WebSockets 连接。

默认情况下，WebSockets 连接被禁止。

WebSockets 端口号

此设置标识传入 WebSocket 连接的端口。

默认情况下，值为 8008。

WebSockets 受信任的源服务器列表

此设置提供受信任的源服务器的逗号分隔列表（通常是适用于 Web 的 Citrix Workspace 应用程序），以 URL 形式表示。服务器仅接受源自这些地址之一的 WebSockets 连接。

默认情况下，通配符 * 用于信任所有 Citrix Workspace app for Web URL。

如果您选择在列表中键入地址，请使用以下语法：

\<protocol>://\<主机的完全限定域名>:

协议必须是 HTTP 或 HTTPS。如果未指定端口，则 HTTP 使用端口 80，HTTPS 使用端口 443。

通配符 `*` 可以在 URL 中使用，但不能作为 IP 地址 (`10.105.*.*`) 的一部分。

WIA 设备策略设置

WIA 设备部分包括用于使用 Windows 图像采集 (WIA) 管理扫描仪重定向的策略设置。

WIA 重定向

WIA 设备（例如数码相机和扫描仪）通过使用 WIA 框架与服务器托管的图像处理应用程序通信。此设置允许或禁止用户访问用户设备上的 WIA 设备。默认情况下，WIA 重定向被禁止。

有关符合 WIA 标准的设备的信息，请参阅 WIA 设备。

图形策略设置

“**图形**”部分包含用于控制用户会话中图像处理方式的策略设置。

允许视觉无损压缩

此设置允许对图形使用视觉无损压缩，而不是真正的无损压缩。视觉无损压缩比真正的无损压缩能提高性能，但会产生肉眼无法察觉的轻微损失。此设置会更改“视觉质量”设置值的使用方式。

默认情况下，此设置为禁用状态。

图形状态指示器

此设置配置图形状态指示器以在用户会话中运行。此工具允许用户查看有关活动图形模式的信息。

此信息包括视频编解码器、硬件编码、图像质量以及会话中使用的显示器等详细信息。借助图形状态指示器，用户还可以启用或禁用像素完美模式。

Citrix Virtual Apps and Desktops™ 2103 及更高版本包含一个图像质量滑块，可帮助用户在图像质量和交互性之间找到适当的平衡。

Citrix Virtual Apps and Desktops™ 2109 及更高版本包含通过使用图形状态指示器启动的用户界面配置虚拟显示布局的功能。

图形状态指示器取代了早期版本中的无损指示器工具。此策略为 Citrix Virtual Apps and Desktops 7.16 到 1809 版本启用了无损指示器。

> **注意：**
>
> “**图形状态指示器**”仅适用于桌面会话，不适用于无缝应用程序会话。

屏幕共享

此设置允许用户与其他用户共享其会话，包括屏幕内容、键盘和鼠标。

默认情况下，此设置为禁用状态。

VDA 尝试使用 TCP 端口范围内的端口来交换数据，从最低端口开始，并在每个后续连接上递增。该端口处理入站和出站流量。

默认情况下，TCP 端口范围设置为 52525-52625。

用于屏幕共享的端口必须添加到防火墙例外列表中。在安装 VDA 时，此选项显示为一个复选框。默认情况下，此选项未选中。

显示内存限制

此设置指定会话的最大视频缓冲区大小（以千字节为单位）。

对于 VDA 2308 及更早版本，请指定 128 到 4,194,303 之间的千字节数。如果未指定，则此设置默认为 65,536 千字节。

对于 VDA 2311 及更高版本，请指定任意千字节数。如果未指定或指定为 0，则此设置默认为无最大值。

> **注意：**
>
> 对于 VDA 2311 及更高版本，Citrix® 建议将此设置保留为默认值。
>
> 连接使用更高的分辨率和多个显示器需要更多内存。由于 HDX™ 仅为每个会话分配所需的显示内存量，因此请始终根据环境中配置的最高级别来计算所需的视频内存量。因此，如果只有部分用户需要超出默认值的内存，则增加显示内存限制不会对可扩展性产生负面影响。

所需的视频内存量可使用以下公式计算：

总视频内存 = ((32 / 8) x Σ)

示例 1

在以下示例中，我们将使用一个具有两个显示器的会话，其中一个分辨率为 1920x1080，另一个分辨率为 1280x720。

1. 计算分辨率乘积之和：
    - (1080 x 1920) + (720 x 1280)
    - = 2073600 + 921600
    - = 2995200
2. 计算总视频内存：
    - ((32 / 8) x 2995200)
    - = (4 x 2995200)
    - = 11,980,800 字节或 11,700 千字节

在此示例中，支持具有这两个显示器配置的会话需要 11,700 千字节的视频内存。

示例 2

当使用 4 个 4K 显示器时，根据上述公式，这些会话至少需要 129,600 千字节的视频内存。

对于这两个示例，当使用 VDA 2311 或更高版本时，Citrix 建议将显示内存限制保留为默认值。

显示模式降级首选项

> **注意：**
>
> 对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。
>
> 当达到会话显示内存限制时，此设置指定是先降级颜色深度还是分辨率。

默认情况下，颜色深度会首先降级。

当达到会话内存限制时，您可以降低显示图像的质量。您可以通过选择是先降级颜色深度还是分辨率来降低此质量。当颜色深度首先降级时，显示图像使用的颜色会减少。当分辨率首先降级时，显示图像每英寸使用的像素会减少。

要在颜色深度或分辨率降级时通知用户，请配置“在显示模式降级时通知用户”设置。

动态窗口预览

此设置启用或禁用以下情况下的无缝窗口显示：

- 翻转-
- 三维翻转
- 任务栏预览
- Windows 预览

WINDOWS AERO 预览选项	描述
任务栏预览	当用户将鼠标悬停在窗口的任务栏图标上时，该窗口的图像会显示在任务栏上方。
Windows 预览	当用户将鼠标悬停在任务栏预览图像上时，窗口的全尺寸图像会显示在屏幕上。
翻转	当用户按下 ALT+TAB 时，每个打开的窗口都会显示小的预览图标。

WINDOWS AERO 预览选项	描述
三维翻转	当用户按下 TAB+Windows 徽标键时，打开窗口的大图像会在屏幕上层叠显示。

默认情况下，此设置处于启用状态。

图像缓存

> **注意：**
>
> 对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

此设置启用或禁用会话中图像部分的缓存和检索。按部分缓存图像并在需要时检索这些部分可实现以下目的：

- 用户设备上的滚动更流畅
- 减少用户设备上通过网络传输的数据量
- 减少用户设备所需的处理量

默认情况下，图像缓存设置处于启用状态。

> **注意：**
>
> 图像缓存设置控制图像的缓存和检索方式。此设置不控制图像是否缓存。如果启用了旧版图形模式设置，则会缓存图像。

旧版图形模式 - 不受支持。仅用于向后兼容

> **重要提示：**
>
> 此版本不支持旧版图形模式和桌面组合重定向 (DCR)。此策略仅用于在使用 XenApp 7.15 LTSR、XenDesktop 7.15 LTSR 以及早期 VDA 版本（与 Windows 7 和 Windows 2008 R2 结合使用）时的向后兼容性。

> 此设置会禁用富图形体验。使用此设置可恢复到旧版图形体验，从而减少通过 WAN 或移动连接的带宽消耗。XenApp 和 XenDesktop 7.13 中引入的带宽减少功能使此模式变得过时。

默认情况下，此设置处于禁用状态，用户将获得富图形体验。

旧版图形模式支持以下各项：

- Windows 7 系统
- Windows Server 2008 R2 虚拟投递代理。

旧版图形模式不支持以下各项：

- Windows 8.x 和 10 版本
- Windows Server 2012、2012 R2 和 2016 版本。

有关在 XenApp 和 XenDesktop 7.6 FP3 或更高版本中优化图形模式和策略的更多信息，请参阅 CTX202687。

最大允许颜色深度

> **注意：**

> 对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

> 此设置指定会话允许的最大颜色深度。

默认情况下，最大允许颜色深度为每像素 32 位。

此设置仅适用于 Thinwire 驱动程序和连接。它不适用于将非 ThinWire 驱动程序用作主显示驱动程序的 VDA。这些 VDA 是使用 Windows 显示驱动程序模型 (WDDM) 驱动程序作为主显示驱动程序的 VDA。对于使用 WDDM 驱动程序作为主显示驱动程序的单会话操作系统 VDA（例如 Windows 8），此设置无效。对于使用 WDDM 驱动程序的 Windows 多会话操作系统 VDA（例如 Windows Server 2019），此设置可能会阻止用户连接到 VDA。

设置高颜色深度需要更多内存。要在达到内存限制时降低颜色深度，请配置**显示模式降级首选项**设置。当颜色深度降级时，显示的图像会使用较少的颜色。

显示模式降级时通知用户

> **注意：**

> 对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

> 当颜色深度或分辨率降级时，此设置会向用户显示简要说明。

默认情况下，禁用通知用户。

优化 3D 图形工作负载

此设置配置最适合图形密集型工作负载的相应默认设置。为工作负载侧重于图形密集型应用程序的用户启用此设置。仅当会话可用 GPU 时才应用此策略。任何明确覆盖此策略设置的默认设置的其他设置都将优先。

默认情况下，禁用优化 3D 图形工作负载。

排队和丢弃

> **注意：**
>
> 对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

> 此设置会丢弃被其他图像替换的排队图像。

默认情况下，排队和丢弃功能已启用。

此设置可在图形发送到用户设备时提高响应速度。配置此设置可能会导致动画因丢帧而变得卡顿。

使用视频编解码器进行压缩

允许在端点上提供视频解码时使用视频编解码器压缩图形。选择“**针对整个屏幕**”时，视频编解码器将作为所有内容的默认编解码器应用。选择“**针对活动变化区域**”时，视频编解码器将用于屏幕上不断变化的区域，其他数据则使用静态图像压缩和位图缓存。当端点上没有视频解码功能，或者指定“**不使用视频编解码器**”时，将使用静态图像压缩和位图缓存的组合。选择“**在首选时使用**”时，系统会根据各种因素进行选择。随着选择方法的增强，结果可能会因版本而异。

选择“**在首选时使用**”以允许系统尽力为当前场景选择适当的设置。

选择“**针对整个屏幕**”以优化用户体验和带宽，尤其是在大量使用服务器渲染的视频和 3D 图形的情况下。

选择“**针对活动变化区域**”以优化视频性能，尤其是在低带宽环境下，同时保持静态和缓慢变化内容的扩展性。多显示器部署支持此设置。

选择“**不使用视频编解码器**”以优化服务器 CPU 负载，并适用于没有大量服务器渲染视频或其他图形密集型应用程序的情况。

默认值为“**在首选时使用**”。

对视频使用硬件编码

此设置允许在可用时使用图形硬件，通过视频编解码器压缩屏幕元素。如果此类硬件不可用，VDA 将回退到使用软件视频编解码器的基于 CPU 的编码。

此策略设置的默认选项为“**已启用**”。

支持多显示器。

任何支持视频解码的 Citrix Workspace™ 应用程序都可以与硬件编码一起使用。

NVIDIA

对于 NVIDIA GRID GPU，多会话操作系统和单会话操作系统的 VDA 支持硬件编码。

NVIDIA GPU 必须支持 NVENC 硬件编码。有关支持的 GPU 列表，请参阅 NVIDIA 视频编解码器 SDK。

NVIDIA GRID 需要驱动程序版本 3.1 或更高版本。NVIDIA Quadro 需要驱动程序版本 362.56 或更高版本。Citrix 建议使用 NVIDIA Release R361 分支中的驱动程序。

无损文本与 NVENC 硬件编码不兼容。如果启用了无损文本，则无损文本优先于 NVENC 硬件编码。

支持对活动更改区域选择性使用 H.264 硬件编解码器。

支持视觉无损 (YUV 4:4:4) 压缩。视觉无损（图形策略设置，允许视觉无损压缩）需要 Citrix Workspace 应用程序 1808 或更高版本，或者 Citrix Receiver for Windows 4.5 或更高版本。

英特尔

对于 Intel Iris Pro 图形处理器，单会话操作系统和多会话操作系统的 VDA 支持硬件编码。

支持 Intel Broadwell 处理器系列 及更高版本中的 Intel Iris Pro 图形处理器。需要 Intel Remote Displays SDK 1.0 版，可从英特尔网站下载：Remote Displays SDK。

仅当视频编解码器策略设置为整个屏幕且**优化 3D 图形工作负载**策略被禁用时，才支持无损文本。

不支持视觉无损 (YUV 4:4:4)。

英特尔编码器可为最多八个编码会话提供良好的用户体验（例如，一个用户使用八个显示器，或八个用户各使用一个显示器）。如果需要超过八个编码会话，请检查虚拟机连接了多少个显示器。管理员决定按用户或按计算机配置此策略设置，以保持良好的用户体验。

AMD

对于 AMD，单会话操作系统的 VDA 支持硬件编码。

AMD GPU 必须支持 RapidFire SDK。例如，AMD Radeon Pro 或 FirePro GPU。

要使编码正常工作，请安装最新的 AMD 驱动程序。您可以从 `<https://www.amd.com/en/support>` 下载这些驱动程序。

无损文本与 AMD 硬件编码不兼容。如果启用了无损文本，则无损文本优先于 AMD 硬件编码。

支持选择性使用 H.264 硬件编解码器处理活动变化的区域。

缓存策略设置

本节包含在客户端连接带宽受限时，在用户设备上启用图像数据缓存的策略设置。

持久缓存阈值

注意： 对于 Virtual Delivery Agent 7.x，此策略设置仅在启用**旧版图形模式**策略设置时适用。

此设置将位图缓存到用户设备的硬盘上，从而可以重复使用以前会话中的大型常用图像。

默认情况下，阈值为每秒 3000000 位。

阈值表示低于此值时持久缓存功能生效。例如，使用默认值时，当带宽低于 3000000 bps 时，位图将缓存到用户设备的硬盘上。

高级策略设置

访问锁定文件时的重试次数

设置访问锁定文件时的重试次数。

如果禁用此策略，则使用默认值五次重试。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则使用默认值。

注销时处理 Internet Cookie 文件

某些部署会留下 `Index.dat` 未引用的额外 Internet Cookie。持续浏览后文件系统中留下的额外 Cookie 可能导致配置文件膨胀。此策略允许您启用 Profile Management 以强制处理 Index.dat 并删除额外 Cookie。此策略会增加注销时间，因此仅在遇到此问题后才启用它。

配置优先级：

1. 如果此处未配置此策略，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中未配置此策略，则不处理 Index.dat。

禁用自动配置

Profile Management 会检查任何 Citrix Virtual Desktops™ 环境（例如是否存在个人 vDisk），并相应地配置组策略。仅调整处于“未配置”状态的 Profile Management 策略，因此您所做的任何自定义都将保留。

此策略可加快部署速度并简化优化。您无需配置此策略。但是，在执行以下操作之一时，您可以禁用自动配置：

- 升级以保留早期版本中的设置
- 故障排除

您可以将自动配置视为一个动态配置检查器，它根据运行时环境自动配置默认策略设置。它消除了手动配置设置的需要。运行时环境包括：

- Windows 操作系统
- Windows 操作系统版本
- Citrix 虚拟桌面的存在
- 个人 vDisk 的存在

如果环境发生变化，自动配置可能会更改以下策略：

- 活动回写
- 始终缓存
- 注销时删除本地缓存的配置文件
- 删除缓存配置文件前的延迟
- 配置文件流技术

有关不同操作系统上策略的默认状态，请参阅下表：

	多会话操作系统	单会话操作系统
活动回写	启用	如果正在使用 Personal vDisk，则*禁用*；否则，启用。
始终缓存	已禁用	如果正在使用 Personal vDisk，则*禁用*；否则，启用。
注销时删除本地缓存的配置文件	启用	如果出现以下情况之一，则*禁用*：正在使用 Personal vDisk、已分配 Citrix Virtual Desktops 或未安装 Citrix Virtual Desktops；否则，启用。
删除缓存配置文件前的延迟	0 秒	如果用户更改不是持久性的，则为 60 秒；否则，为 0 秒。
配置文件流技术	启用	如果正在使用 Personal vDisk，则*禁用*；否则，启用。

但是，如果禁用自动配置，则上述所有策略都默认为**禁用**。

> **重要提示：**
>
> Personal vDisk 已弃用。有关详细信息，请参阅删除 PVD、AppDisks 和不受支持的主机。

> 从 Profile Management 1909 开始，您可以在 Windows 10（版本 1607 及更高版本）上获得改进的“开始”菜单体验。此改进是通过自动配置以下策略实现的：

- 将 `Appdata\Local\Microsoft\Windows\Caches` 和 `Appdata\Local\Packages` 添加到**要镜像的文件夹**。
- 将 `Appdata\Local\Microsoft\Windows\UsrClass.Dat*` 添加到**要同步的文件**。

配置优先级：

1. 如果此处未配置此设置，则使用 .ini 文件中的值。

2. 如果此处或 .ini 文件中未配置此设置，则会启用自动配置。在这种情况下，如果环境发生变化，Profile Management 设置可能会随之更改。

如果遇到问题，注销用户

允许您指定 Profile Management 在遇到问题时是否注销用户。

如果此策略被禁用或未配置，Profile Management 会在遇到问题时为用户提供临时配置文件。例如，用户存储不可用。

如果启用此策略，将显示错误消息并注销用户。此设置可以简化问题的故障排除。

配置优先级：

1. 如果此处未配置此设置，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中未配置此设置，则提供临时配置文件。

客户体验改善计划

默认情况下，客户体验改善计划处于启用状态，通过收集匿名统计数据和使用数据来帮助提高 Citrix® 产品的质量和性能。

如果此处未配置此设置，则使用 .ini 文件中的值。

启用 Outlook 搜索索引漫游

通过自动漫游 Outlook 搜索数据以及用户配置文件，允许基于用户的 Outlook 搜索体验。此功能需要在用户存储中额外空间来存储 Outlook 的搜索索引。

注销然后重新登录以使此策略生效。

Outlook 搜索索引数据库 – 备份和还原

允许您指定当“启用 Outlook 搜索索引漫游”策略启用时，Profile Management 在登录期间执行的操作。

如果此策略已启用，Profile Management 会在每次登录时成功装载数据库时备份搜索索引数据库。Profile Management 将备份视为搜索索引数据库的良好副本。当由于数据库损坏而导致装载搜索索引数据库的尝试失败时，Profile Management 会将搜索索引数据库还原到上次已知的良好副本。

> 注意：
>
> Profile Management 在成功保存新备份后删除以前保存的备份。备份会占用可用的 VHDX 存储空间。

为 OUTLOOK 搜索数据漫游启用并发会话支持

允许 Profile Management 在同一用户的并发会话中提供本机 Outlook 搜索体验。将此策略与 Outlook 搜索索引漫游策略结合使用。

启用此策略后，每个并发会话都使用单独的 Outlook OST 文件。

默认情况下，只能使用两个 VHDX 磁盘来存储 Outlook OST 文件（每个磁盘一个文件）。如果用户启动更多会话，其 Outlook OST 文件将存储在本地用户配置文件中。您可以指定用于存储 Outlook OST 文件的 VHDX 磁盘的最大数量。

启用 ONEDRIVE 容器

允许 OneDrive 文件夹随用户漫游。

OneDrive 容器是一种基于 VHDX 的文件夹漫游解决方案。Profile Management 在文件共享上为每个用户创建一个 VHDX 文件，并将用户的 OneDrive 文件夹存储到 VHDX 文件中。VHDX 文件在用户登录时附加，在用户注销时分离。

UWP 应用程序漫游

允许您启用 UWP（通用 Windows 平台）应用程序随用户漫游。因此，用户可以从不同的设备访问相同的 UWP 应用程序。

启用此策略后，Profile Management 允许 UWP 应用程序通过将应用程序存储在单独的 VHDX 磁盘上来随用户漫游。这些磁盘在用户登录时附加，在用户注销时分离。

配置优先级：

1. 如果此处未配置此设置，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中未配置此设置，则禁用此功能。

启用 UWP 应用程序加载加速

启用 UWP 应用加载加速。允许您加速 UWP 应用的加载并提高其在非持久性环境中的一致性。默认情况下，Windows 在每台计算机上本地存储 UWP 应用注册信息，该信息在非持久性环境中重启时可能会丢失。启用此策略后，Profile Management 会为每台计算机创建一个 VHDX 容器来存储 UWP 应用注册数据，从而加快用户登录并防止重启时数据丢失。

配置优先级：

1. 如果未使用 GPO、Studio 或 Workspace Experience Management (WEM) 配置此设置，则使用 .ini 文件中的值。
2. 如果未在任何位置配置此设置，则此功能将被禁用。

在登录时为用户组策略启用异步处理

Windows 为用户组策略提供了两种处理模式：同步和异步。Windows 使用注册表值来确定下次用户登录的处理模式。如果注册表值不存在，则应用同步模式。注册表值是计算机级别设置，不随用户漫游。因此，如果用户出现以下情况，异步模式将无法按预期应用：

- 登录到不同的计算机。
- 登录到已启用“注销时删除本地缓存配置文件”策略的同一台计算机。

启用此策略后，注册表值会随用户漫游。因此，每次用户登录时都会应用处理模式。

触发 VHD 磁盘压缩的空闲空间比率

当 启用 VHD 磁盘压缩 启用时适用。允许您指定触发 VHD 磁盘压缩的空闲空间比率。当用户注销时空闲空间比率超过指定值时，将触发磁盘压缩。

空闲空间比率 = (当前 VHD 文件大小 – 所需最小 VHD 文件大小*) ÷ 当前 VHD 文件大小

* 使用 Microsoft Windows 操作系统中 `MSFT_Partition` 类的 GetSupportedSize 方法获取。

触发 VHD 磁盘压缩的注销次数

当 启用 VHD 磁盘压缩 启用时适用。允许您指定触发 VHD 磁盘压缩的用户注销次数。

当自上次压缩以来的注销次数达到指定值时，将再次触发磁盘压缩。

禁用 VHD 磁盘压缩的碎片整理

当 启用 VHD 磁盘压缩 处于启用状态时适用。允许您指定是否禁用 VHD 磁盘压缩的文件碎片整理。

启用 VHD 磁盘压缩后，VHD 磁盘文件将首先使用 Windows 内置的 `defrag` 工具自动进行碎片整理，然后进行压缩。VHD 磁盘碎片整理可产生更好的压缩结果，而禁用它可以节省系统资源。

为配置文件容器启用多会话回写

在多会话场景中为配置文件容器启用回写。如果启用，所有会话中的更改都将回写到配置文件容器。否则，只有第一个会话中的更改会被保存，因为在配置文件容器中，只有第一个会话处于读/写模式。Citrix Profile Management 配置文件容器从 Citrix Profile Management 2103 开始支持。FSLogix Profile Container 从 Citrix Profile Management 2003 开始支持。

要将此策略用于 FSLogix Profile Container，请确保满足以下先决条件：

- FSLogix Profile Container 功能已安装并启用。
- 在 FSLogix 中，配置文件类型设置为 **尝试读写配置文件并回退到只读**。

复制用户存储

允许您在每次登录和注销时将远程用户配置文件存储复制到多个路径。这样做可让 Profile Management 为用户登录提供配置文件冗余。

启用此策略会增加系统 I/O 并可能延长注销时间。

> **注意：**
>
> 此功能适用于基于文件和基于容器的配置文件解决方案。

启用基于凭据的用户存储访问

默认情况下，Citrix Profile Management 模拟当前用户访问用户存储。如果您不希望 Profile Management 在访问用户存储时模拟当前用户，请启用此功能。您可以将用户存储放在当前用户无权访问的存储库（例如 Azure 文件）中。

为确保 Profile Management 可以访问用户存储，请将配置文件存储服务器的凭据保存在 Workspace Environment Management™ (WEM) 或 Windows 凭据管理器中。我们建议您使用 Workspace Environment Management，以消除在运行 Profile Management 的每台计算机上配置相同凭据的需要。如果您使用 Windows 凭据管理器，请使用本地系统帐户安全地保存凭据。

> **注意：**
>
> 此策略适用于基于文件和基于 VHDX 的用户存储。对于早于 2212 的 Profile Management 版本，此策略仅适用于基于 VHDX 的用户存储。

> 配置优先级：

1. 如果此处未配置此设置，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中未配置此设置，则默认情况下禁用此设置。

自定义 VHDX 文件的存储路径

Profile Management 提供以下基于 VHDX 的策略：配置文件容器、Outlook 搜索索引漫游和加速文件夹镜像。默认情况下，VHDX 文件存储在用户存储中。此策略允许您指定单独的路径来存储它们。

VHD 容器的默认容量

允许您指定 VHD 容器的默认存储容量（以 GB 为单位）。

配置优先级：

1. 如果此处未配置此策略，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中未配置此策略，则默认值为 50 (GB)。

在会话中自动重新连接 VHDX 磁盘

启用此策略后，Profile Management 可确保基于 VHDX 的策略具有高水平的稳定性。默认情况下，此策略处于启用状态。

启用此策略后，Profile Management 会监视 VHDX 策略正在使用的 VHDX 磁盘。如果任何磁盘被分离，Profile Management 会自动重新连接该磁盘。

配置文件容器自动扩展阈值

允许您指定配置文件容器触发自动扩展时存储容量的利用率百分比。

配置优先级：

- 如果此处未配置此策略，则使用 .ini 文件中的值。
- 如果此处或 .ini 文件中未配置此策略，则默认值为存储容量的 90 (%)。

配置文件容器自动扩展增量

允许您指定当触发自动扩展时，配置文件容器自动扩展的存储容量（以 GB 为单位）。

配置优先级：

- 如果此处未配置此策略，则使用 .ini 文件中的值。
- 如果此处或 .ini 文件中未配置此策略，则默认值为 10 (GB)。

配置文件容器自动扩展限制

允许您指定当触发自动扩展时，配置文件容器可以自动扩展到的最大存储容量（以 GB 为单位）。

配置优先级：

- 如果此处未配置此策略，则使用 .ini 文件中的值。
- 如果此处或 .ini 文件中未配置此策略，则默认值为 80 (GB)。

启用用户级策略设置

启用此策略后，计算机级策略设置可以在用户级别工作，并且用户级设置会覆盖计算机级设置。

配置优先级：

1. 如果此处未配置此策略，则使用 .ini 文件中的值。

2. 如果此处或 .ini 文件中未配置此策略，则禁用此策略。

设置用户组的优先级顺序

允许您指定用户组的优先级顺序。当用户属于具有不同策略设置的多个组时，此顺序决定哪个组优先。

当用户属于具有冲突策略设置的多个组时，请考虑以下事项：

- 如果用户属于此策略中定义的一个或多个组，则优先级最高的组优先。
- 如果用户不属于此策略中定义的任何组，则 SID 按字母顺序排列在最前面的组优先。

用户存储选择方法

允许您在有多个用户存储可用时指定用户存储选择方法。选项包括：

- **配置顺序。** Profile Management 选择最早配置的存储。
- **访问性能。** Profile Management 选择访问性能最佳的存储。

配置优先级：

1. 如果此处未配置此设置，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中未配置此设置，则使用**配置顺序**。

启用会话内配置文件容器在用户存储之间的故障转移

默认情况下，当部署多个用户存储时，配置文件容器故障转移仅在用户登录时发生。因此，配置文件冗余仅在用户登录时可用。此策略允许您将会话故障转移范围扩展到整个会话，从而确保整个会话期间的配置文件冗余。启用此策略后，如果 Profile Management 在会话期间与活动配置文件容器失去连接，它会自动切换到另一个可用的配置文件容器。

配置优先级：

1. 如果此处未配置此策略，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中未配置此策略，则此设置将被禁用。

配置文件加载超时

允许您启用配置文件加载超时功能并配置超时持续时间。Citrix Profile Management 会等待指定的超时时间来加载用户配置文件，然后切换到临时配置文件。 默认情况下，**配置文件加载超时**设置为 45 秒，有效范围为 0–1800 秒。要绕过配置文件加载并使用临时配置文件，请将超时设置为 0 秒。

配置优先级：

1. 如果此处未配置此策略，则使用 .ini 文件中的值。

2. 如果此处或 .ini 文件中均未配置此策略，则默认禁用此策略。

限制注销期间的配置文件同步

允许您指定在用户注销时同步多少个用户存储。 默认情况下，Citrix Profile Management 会在注销期间同步所有用户存储，并且只有在配置文件已在所有存储中同步后，注销才会完成。 减少同步的存储数量可以加快注销速度。对于非持久性计算机，未同步的存储将在下一个用户会话期间更新；而对于持久性计算机，未同步的存储将在后台同步。

配置优先级：

1. 如果此处未配置此策略，则使用 .ini 文件中的值。
2. 如果未在此处或 .ini 文件中配置此策略，则默认禁用此策略。注意：此设置仅在启用“复制用户存储”策略时适用。

在配置文件大小超出配额时通知用户

允许您为用户配置文件设置配额，并在用户配置文件大小超出配额时通知用户。

配置优先级：

1. 如果此处未配置此策略，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中均未配置此策略，则禁用此设置。

配置文件大小超出配额时的通知消息

在启用“**在配置文件大小超出配额时通知用户**”策略时适用。允许您设置用户收到的通知消息。

配置优先级：

1. 如果此处未配置此策略，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中均未配置此策略，则禁用此设置。

为计算机休眠启用多会话支持

允许您通过在休眠期间维护磁盘状态来启用系统休眠支持。它可确保休眠会话使用的 VHDX 磁盘不会重新分配给其他并发会话。因此，计算机从休眠状态恢复后，可以恢复用户配置文件，从而确保会话连续性。

配置优先级：

1. 如果此处未配置此策略，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中未配置此策略，则禁用此设置。

基本策略设置

本部分包含与 Profile Management 基本配置相关的策略设置。

启用配置文件管理

默认情况下，为方便部署，Profile Management 不处理登录或注销。仅在执行所有其他设置任务并测试 Citrix® 用户配置文件在您的环境中的性能后，才启用 Profile Management。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则 Profile Management 不会以任何方式处理 Windows 用户配置文件。

已处理的组

可以使用计算机本地组和域组（本地、全局和通用）。域组必须采用以下格式指定：DOMAIN NAME\GROUP NAME。

如果此处配置了此策略，则 Profile Management 仅处理这些用户组的成员。如果禁用此策略，则 Profile Management 处理所有用户。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则处理所有用户组的成员。

排除的组

您可以使用计算机本地组和域组（本地、全局和通用）来阻止处理特定的用户配置文件。以 DOMAIN NAME\GROUP NAME 形式指定域组。

如果此处配置了此设置，则 Profile Management 会排除这些用户组的成员。如果禁用此设置，则 Profile Management 不会排除任何用户。如果此处未配置此设置，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此设置，则不排除任何组的成员。

处理本地管理员的登录

指定是否处理 BUILTIN\Administrators 组成员的登录。在多会话操作系统（例如 Citrix Virtual Apps 环境）上，请考虑禁用或不配置此策略。在这种情况下，Profile Management 假定必须处理域用户的登录，而不是本地管理员的登录。在单会话操作系统（例如 Citrix Virtual Desktops 环境）上，会处理本地管理员登录。此策略允许具有本地管理员权限的域用户（通常是分配了虚拟桌面的 Citrix Virtual Desktops 用户）执行以下操作：

- 绕过任何处理
- 登录
- 解决桌面在使用 Profile Management 时遇到的问题

注意：域用户的登录可能会受到组成员身份施加的限制，这通常是为了确保符合产品许可。 如果禁用此策略，Profile Management 不会处理本地管理员的登录。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不处理管理员。

用户存储路径

设置目录（用户存储）的路径，用户设置（注册表更改和同步文件）将保存到该目录中。

路径可以是：

- 相对路径。它必须相对于主目录（主目录通常配置为 Active Directory 中用户的 #homeDirectory# 属性）。
- UNC 路径。它通常指定服务器共享或 DFS 命名空间。
- 已禁用或未配置。在这种情况下，假定值为 #homeDirectory#\Windows。

此策略可以使用以下类型的变量：

- 用百分号括起来的系统环境变量（例如，%ProfVer%）。系统环境变量通常需要额外设置。
- 用哈希符号括起来的 Active Directory 用户对象属性（例如，#sAMAccountName#）。
- Profile Management 变量。有关详细信息，请参阅 Profile Management 变量产品文档。

用户环境变量不能使用，`%username%` 和 `%userdomain%` 除外。您还可以创建自定义属性来完整定义组织变量，例如位置或用户。属性区分大小写。

示例：

- `\\server\share#sAMAccountName#` 将用户设置存储到 UNC 路径 `\\server\share\JohnSmith`（如果当前用户的 #sAMAccountName# 解析为 JohnSmith）
- `\\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!` 可能会扩展为 `\\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64`

重要提示：无论您使用何种属性或变量，请确保此策略展开到包含 NTUSER.DAT 的文件夹的上一级文件夹。例如，如果此文件包含在 `\\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile` 中，请将用户存储路径设置为 `\\server\profiles$\JohnSmith.Finance\Win8x64`（而不是 \UPM_Profile 子文件夹）。

有关在指定用户存储路径时使用变量的详细信息，请参阅以下主题：

- 在多个文件服务器上共享 Citrix 用户配置文件
- 在 OU 内部和跨 OU 管理配置文件
- 使用 Profile Management 实现高可用性和灾难恢复

如果“用户存储路径”已禁用，则用户设置将保存在主目录的 Windows 子目录中。

如果此策略已禁用，则用户设置将保存在主目录的 Windows 子目录中。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则使用主驱动器上的 Windows 目录。

迁移用户存储

指定以前保存用户设置（注册表更改和同步文件）的文件夹路径（您以前使用的用户存储路径）。

如果配置了此设置，则存储在以前的用户存储中的用户设置将迁移到“用户存储路径”策略中指定的当前用户存储。

该路径可以是绝对 UNC 路径，也可以是相对于主目录的路径。

在这两种情况下，您都可以使用以下类型的变量：

- 用百分号括起来的系统环境变量
- 用井号括起来的 Active Directory 用户对象属性

示例：

- 文件夹 `Windows\%ProfileVer%` 将用户设置存储在用户存储中名为 `Windows\W2K3` 的子文件夹中（如果 %ProfileVer% 是解析为 W2K3 的系统环境变量）。
- `\\server\share#SAMAccountName#` 将用户设置存储到 UNC 路径 `\\server\share\<JohnSmith>`（如果 `#SAMAccountName#` 解析为当前用户的 JohnSmith）。

在此路径中，您可以使用用户环境变量，但 `%username%` 和 `%userdomain%` 除外。

如果此设置被禁用，用户设置将保存在当前用户存储中。

如果此处未配置此设置，则使用 .ini 文件中的相应设置。

如果此处或 .ini 文件中未配置此设置，用户设置将保存在当前用户存储中。

主动回写

修改的文件和文件夹（但不包括注册表项）可以在会话期间、注销之前同步到用户存储。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则启用此策略。

脱机配置文件支持

此策略允许配置文件在最早可能的机会与用户存储同步。它面向漫游的笔记本电脑或移动设备用户。当网络断开连接时，即使在重新启动或休眠后，配置文件仍会完好无损地保留在笔记本电脑或设备上。当移动用户工作时，其配置文件会在本地更新。此外，当网络连接重新建立时，配置文件最终会与用户存储同步。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则禁用脱机配置文件。

主动回写注册表

将此策略与“主动回写”结合使用。修改的注册表项可以在会话期间同步到用户存储。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则禁用主动回写注册表。

会话锁定和断开连接时主动回写

如果同时启用此策略和**主动回写**策略，则仅当会话锁定或断开连接时，配置文件和文件夹才会被回写。

如果同时启用此策略以及**主动回写**和**主动回写注册表**策略，则仅当会话锁定或断开连接时，注册表项才会被回写。

脱机配置文件支持

启用脱机配置文件功能。此功能适用于通常从网络中移除的计算机。例如，笔记本电脑或移动设备，而非服务器或台式机。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则禁用脱机配置文件支持。

跨平台策略设置

本节包含与配置 **Profile Management 跨平台**设置功能相关的策略设置。

启用跨平台设置

默认情况下，为方便部署，跨平台设置处于禁用状态。通过启用此策略来开启处理，但仅在对该功能进行周密规划和测试后才能这样做。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不应用任何跨平台设置。

跨平台设置用户组

输入一个或多个 Windows 用户组。例如，您可以使用此策略仅处理来自测试用户组的配置文件。如果配置了此策略，则 Profile Management 的跨平台设置功能将仅处理这些用户组的成员。如果此策略被禁用，则该功能将处理由“已处理组”策略指定的所有用户。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则处理所有用户组。

跨平台定义路径

标识从下载包复制的定义文件的网络位置。此路径必须是 UNC 路径。用户必须对此位置具有读取权限，管理员必须对此位置具有写入权限。该位置必须是服务器消息块 (SMB) 或通用 Internet 文件系统 (CIFS) 文件共享。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不应用任何跨平台设置。

跨平台设置存储路径

设置跨平台设置存储的路径，即保存用户跨平台设置的文件夹。用户必须对此区域具有写入权限。该路径可以是绝对 UNC 路径，也可以是相对于主目录的路径。

此区域是用户存储的公共区域，其中包含多个平台共享的配置文件数据。用户必须对此区域具有写入权限。该路径可以是绝对 UNC 路径，也可以是相对于主目录的路径。您可以使用与 **用户存储路径** 相同的变量。

如果此策略被禁用，则使用路径 Windows\PM_CP。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则使用默认值。

创建跨平台设置的源

如果此策略在该平台的 OU 中启用，则将该平台指定为基础平台。此策略将数据从基础平台的配置文件迁移到跨平台设置存储。

每个平台自己的配置文件集都存储在单独的 OU 中。您必须决定使用哪个平台的配置文件数据来填充跨平台设置存储。它被称为基础平台。假设跨平台设置存储包含一个没有数据的定义文件，或者单个平台配置文件中的缓存数据比存储中的定义数据更新。在这种情况下，除非您禁用此策略，否则配置文件管理会将数据从单个平台配置文件迁移到存储。

> **重要提示：**
>
> 如果此策略在多个 OU 或多个用户或计算机对象中启用，则第一个用户登录的平台将成为基础配置文件。 默认情况下，此策略处于启用状态。

文件系统策略设置

本节包含以下策略设置：

- 用户配置文件中哪些文件在安装配置文件的系统和用户存储之间同步
- 用户配置文件中哪些目录在安装配置文件的系统和用户存储之间同步

排除策略设置

本节介绍用于配置用户配置文件中哪些文件和目录从同步过程中排除的策略设置。

排除列表 - 文件

同步期间忽略的文件列表。文件名必须是相对于用户配置文件 (%USERPROFILE%) 的路径。文件名和文件夹名中支持通配符，但只有文件名中的通配符会递归应用。

示例：

- `Desktop\Desktop.ini` 忽略 `Desktop` 文件夹中的文件 `Desktop.ini`
- `%USERPROFILE%*.tmp` 忽略整个配置文件中所有扩展名为 `.tmp` 的文件
- `AppData\Roaming\MyApp*.tmp` 忽略配置文件某一部分中所有扩展名为 `.tmp` 的文件
- `Downloads*\a.txt` 忽略 `Downloads` 文件夹的任何直接子文件夹中的 `a.txt`。

如果禁用此策略，则不排除任何文件。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不排除任何文件。

启用默认排除列表 - 目录

同步期间忽略的默认目录列表。使用此策略可以指定 GPO 排除目录，而无需手动填写。

如果禁用此策略，Profile Management 默认不排除任何目录。

如果此处未配置此策略，Profile Management 将使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，Profile Management 默认不排除任何目录。

排除列表 - 目录

同步期间忽略的文件夹列表。文件夹名称必须指定为相对于用户配置文件 (%USERPROFILE%) 的路径。文件夹名称中支持通配符，但不会递归应用。

示例：

- `Desktop` 忽略用户配置文件中的 `Desktop` 文件夹

如果此策略被禁用，则不排除任何文件夹。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不排除任何文件夹。

登录排除检查

此设置配置如果用户存储中的配置文件包含排除的文件或文件夹，Profile Management 将执行的操作。可能的策略设置和相应的操作列在下表中：

策略设置	操作
设置已禁用或“登录时同步排除的文件或文件夹”的值设置为默认值	当用户登录时，Profile Management 会将排除的文件或文件夹从用户存储同步到本地配置文件。
设置已设置为“登录时忽略排除的文件或文件夹”	当用户登录时，Profile Management 会忽略用户存储中排除的文件或文件夹。
设置已设置为“登录时删除排除的文件或文件夹”	当用户登录时，Profile Management 会删除用户存储中排除的文件或文件夹。
未在 Web Studio 中配置设置	使用 .ini 文件中的值
未在 Web Studio 或 .ini 文件中配置设置	当用户登录时，排除的文件或文件夹会从用户存储同步到本地配置文件。

大文件处理 - 要创建为符号链接的文件

为了提高登录性能并处理大文件，Profile Management 会创建符号链接，而不是复制此列表中的文件。

您可以在引用文件的策略中使用通配符；例如，`!ctx_localappdata!\Microsoft\Outlook*.OST`。

为了处理 Microsoft Outlook 的脱机文件夹文件 (`*.ost`)，请确保未将 **Outlook** 文件夹从 Profile Management 中排除。

这些文件无法在多个会话中同时访问。

同步策略设置

同步部分介绍了策略设置，用于指定用户配置文件中的哪些文件和文件夹在安装配置文件的系统与用户存储之间进行同步。

要同步的目录

默认情况下，Profile Management 会在安装用户配置文件的系统与用户存储之间同步用户配置文件。如果您将某个文件夹从同步中排除，此策略允许您将该排除文件夹的子文件夹重新包含到同步中。

此列表中的路径必须相对于用户配置文件。支持文件夹名称中的通配符，但不会递归应用。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则仅同步用户配置文件中未排除的文件夹。

要同步的文件

默认情况下，Profile Management 会在安装用户配置文件的系统与用户存储之间同步用户配置文件。如果您将某个文件夹从同步中排除，此策略允许您将该排除文件夹内的文件重新包含到同步中。

此列表中的路径必须相对于用户配置文件。文件名和文件夹名中都支持通配符，但只有文件名中的通配符会递归应用。通配符不能嵌套。

示例：

- `AppData\Local\Microsoft\Office\Access.qat` 指定了默认配置中排除的文件夹下的文件
- `AppData\Local\MyApp*.cfg` 指定了配置文件文件夹 `AppData\Local\MyApp` 及其子文件夹中所有扩展名为 `.cfg` 的文件

禁用此策略与启用此策略并配置空列表的效果相同。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则仅同步用户配置文件中未排除的文件。

要镜像的文件夹

此策略可帮助您解决涉及任何事务性文件夹（也称为引用文件夹）的问题。该文件夹包含相互依赖的文件，其中一个文件引用另一个文件。

镜像文件夹使 Profile Management 能够将事务性文件夹及其内容作为一个单一实体进行处理，从而避免配置文件膨胀。例如，您可以镜像 **Internet Explorer cookies** 文件夹，以便 Index.dat 与其索引的 Cookie 同步。在这种情况下，“后写入者优先”。因此，镜像文件夹中在多个会话中修改的文件将被最后一次更新覆盖，从而导致配置文件更改丢失。

例如，下表描述了用户浏览 Internet 时 Index.dat 如何引用 Cookie：

场景	INDEX.DAT 如何引用 COOKIE	
用户有两个 Internet Explorer 会话，每个会话都在不同的服务器上，并且他们在每个会话中访问不同的站点。	来自每个站点的 Cookie 都添加到相应的服务器。	来自每个站点的 Cookie 都添加到相应的服务器。
用户从第一个会话注销或在会话中途注销（如果配置了活动回写功能）	来自第二个会话的 Cookie 必须替换来自第一个会话的 Cookie。	

场景	INDEX.DAT 如何引用 COOKIE	
第一个和第二个会话合并，Index.dat 中对 Cookie 的引用变得过时	在新会话中进一步浏览会导致重复合并和臃肿的 Cookie 文件夹	

镜像 Cookie 文件夹解决了这个问题。在这种情况下，每次用户注销时，Cookie 都会被上次会话的 Cookie 覆盖。因此 Index.dat 保持最新。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不镜像任何文件夹。

加速文件夹镜像

同时启用此策略和**要镜像的文件夹**策略后，**Profile Management 会将镜像的**文件夹存储在基于 VHDX 的虚拟磁盘上。它在登录期间附加虚拟磁盘，并在注销期间分离虚拟磁盘。启用此策略消除了在用户存储和本地配置文件之间复制文件夹的需要，并加速了文件夹镜像。

文件重复数据删除策略设置

用户存储中不同用户配置文件之间可能存在相同的文件。在用户存储中存储重复的文件实例会增加存储成本。

文件重复数据删除策略允许 Profile Management 从用户存储中删除重复文件，并将文件的一个实例存储在中心位置（称为 *共享存储*）。这样做可以避免用户存储中的文件重复，从而节省存储成本。

要包含在共享存储中进行重复数据删除的文件

允许您启用文件重复数据删除并指定要包含在共享存储中进行重复数据删除的文件。

要从共享存储中排除的文件

允许您指定要从共享存储中排除的文件。请将此策略与 *要包含在共享存储中进行重复数据删除的文件* 策略结合使用。

要从配置文件容器中删除重复数据的文件的最小大小

允许您指定要从配置文件容器中删除重复数据的文件的最小大小。大小必须为 256 MB 或更大。

配置优先级：

1. 如果此处未配置此设置，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中未配置此设置，则值为 256。

文件夹重定向策略设置

本节包含策略设置，用于指定是否将配置文件中常见的文件夹重定向到共享网络位置。

授予管理员访问权限

此设置允许管理员访问用户重定向文件夹的内容。

> **注意：**
>
> 此设置向对域具有完全不受限制访问权限的管理员授予权限。

默认情况下，此设置处于禁用状态，用户被授予对其重定向文件夹内容的独占访问权限。

包含域名

此设置允许将 `%userdomain%` 环境变量作为 UNC 路径的一部分。此 UNC 路径是为重定向文件夹指定的。

默认情况下，此设置处于禁用状态。并且 `%userdomain%` 环境变量不作为为重定向文件夹指定的 UNC 路径的一部分。

AppData(Roaming) 策略设置

本部分包含用于将 **AppData(Roaming)** 文件夹的内容重定向到共享网络位置的策略设置。

APPDATA(ROAMING) 路径

此设置指定将 **AppData(Roaming)** 文件夹的内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

APPDATA(ROAMING) 的重定向设置

此设置指定如何重定向 **AppData(Roaming)** 文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。有关详细信息，请参阅 Path to user store 部分。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

联系人策略设置

本节包含用于将**联系人**文件夹内容重定向到共享网络位置的策略设置。

联系人路径

此设置指定**联系人**文件夹内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

联系人重定向设置

此设置指定如何重定向**联系人**文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

桌面策略设置

本节包含用于将 `Desktop` 文件夹的内容重定向到共享网络位置的策略设置。

桌面路径

此设置指定将 **桌面** 文件夹的内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

桌面的重定向设置

此设置指定如何重定向 **桌面** 文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

文档策略设置

本节包含用于将**文档**文件夹的内容重定向到共享网络位置的策略设置。

文档路径

此设置指定**文档**文件夹中的文件重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

文档路径设置必须启用，不仅用于将文件重定向到**文档**文件夹，还用于将文件重定向到**音乐**、**图片**和**视频**文件夹。

文档的重定向设置

此设置指定如何重定向**文档**文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

要控制如何重定向**文档**文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到“文档路径”策略设置中指定的 UNC 路径。
- 重定向到用户主目录。将内容重定向到用户主目录，通常在 Active Directory 中配置为用户的 #homeDirectory# 属性。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

下载策略设置

本节包含用于将“**下载**”文件夹的内容重定向到共享网络位置的策略设置。

下载路径

此设置指定“**下载**”文件夹中的文件重定向到的网络位置。

默认情况下，此设置为禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

下载的重定向设置

此设置指定如何重定向“**下载**”文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

收藏夹策略设置

本节包含用于将 **收藏夹** 文件夹的内容重定向到共享网络位置的策略设置。

收藏夹路径

此设置指定将 **收藏夹** 文件夹的内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

收藏夹的重定向设置

此设置指定如何重定向 **收藏夹** 文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

链接策略设置

本节包含用于将 **链接** 文件夹的内容重定向到共享网络位置的策略设置。

链接路径

此设置指定 **链接** 文件夹的内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，Profile Management 不会重定向指定的文件夹。

链接的重定向设置

此设置指定如何重定向 **链接** 文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，Profile Management 不会重定向指定的文件夹。

音乐策略设置

本节包含用于将“**音乐**”文件夹的内容重定向到共享网络位置的策略设置。

音乐路径

此设置指定“**音乐**”文件夹内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，Profile Management 不会重定向指定的文件夹。

音乐的重定向设置

此设置指定如何重定向“**音乐**”文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

要控制如何重定向“**音乐**”文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到“音乐路径”策略设置中指定的 UNC 路径。
- 相对于“文档”文件夹重定向。将内容重定向到相对于“文档”文件夹的文件夹。

要将内容重定向到相对于“**文档**”文件夹的文件夹，必须启用“**文档路径**”设置。

如果此处未配置此设置，Profile Management 不会重定向指定的文件夹。

图片策略设置

本节包含用于将“**图片**”文件夹的内容重定向到共享网络位置的策略设置。

图片路径

此设置指定“**图片**”文件夹的内容重定向到的网络位置。

默认情况下，此设置为禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

图片重定向设置

此设置指定如何重定向“**图片**”文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

要控制如何重定向“**图片**”文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到“图片路径”策略设置中指定的 UNC 路径。
- 相对于“文档”文件夹重定向。将内容重定向到相对于“文档”文件夹的文件夹。

要将内容重定向到相对于“**文档**”文件夹的文件夹，必须启用“**文档路径**”设置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

搜索策略设置

本节包含用于将 **搜索** 文件夹的内容重定向到共享网络位置的策略设置。

搜索的重定向设置

此设置指定如何重定向 **搜索** 文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，Profile Management 不会重定向指定的文件夹。

搜索路径

此设置指定重定向 **搜索** 文件夹内容的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，Profile Management 不会重定向指定的文件夹。

开始菜单策略设置

本节包含用于将“**开始菜单**”文件夹内容重定向到共享网络位置的策略设置。

开始菜单的重定向设置

此设置指定如何重定向“**开始菜单**”文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

开始菜单路径

此设置指定“**开始菜单**”文件夹内容重定向到的网络位置。

默认情况下，此设置为禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

视频策略设置

本节包含用于将“**视频**”文件夹内容重定向到共享网络位置的策略设置。

视频重定向设置

此设置指定如何重定向“**视频**”文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

要控制如何重定向“**视频**”文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到“视频路径”策略设置中指定的 UNC 路径。
- 相对于“文档”文件夹重定向。将内容重定向到相对于“文档”文件夹的文件夹。

要将内容重定向到相对于“**文档**”文件夹的文件夹，必须启用“**文档路径**”设置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

视频路径

此设置指定“**视频**”文件夹内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

日志策略设置

本节包含配置配置文件管理日志记录的策略设置。

活动目录操作

此设置启用或禁用 Active Directory 中执行的操作的详细日志记录。

默认情况下，此设置为禁用。

启用此设置时，请确保也启用了“**启用日志记录**”设置。

如果未在 Web Studio 中配置此设置，则使用 .ini 文件中的值。

如果未在 Web Studio 或 .ini 文件中配置此设置，则记录以下内容：

- 错误
- 常规信息

常见信息

此设置启用或禁用常见信息的详细日志记录。

默认情况下，此设置为禁用。

启用此设置时，请确保也启用了“**启用日志记录**”设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在 Web Studio 或 .ini 文件中配置此设置，则会记录以下内容：

- 错误
- 一般信息

常见警告

此设置启用或禁用常见警告的详细日志记录。

默认情况下，此设置处于禁用状态。

启用此设置时，请确保同时启用“**启用日志记录**”设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在 Web Studio 或 .ini 文件中配置此设置，则会记录以下内容：

- 错误
- 一般信息

启用日志记录

此设置启用或禁用调试（详细日志记录）模式下的 Profile Management 日志记录。在调试模式下，详细的状态信息会记录在位于“%SystemRoot%\System32\Logfiles\UserProfileManager”的日志文件中。

默认情况下，此设置处于禁用状态，并且仅记录错误。

Citrix® 建议仅在对 Profile Management 进行故障排除时启用此设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则仅记录错误。

文件系统操作

此设置启用或禁用文件系统中执行的操作的详细日志记录。

默认情况下，此设置为禁用。

启用此设置时，请确保也启用了 **启用日志记录** 设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果在 Web Studio 或 .ini 文件中未配置此设置，则记录以下内容：

- 错误
- 常规信息

文件系统通知

此设置启用或禁用文件系统通知的详细日志记录。

默认情况下，此设置为禁用。

启用此设置时，请确保也启用了 **启用日志记录** 设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在 Web Studio 或 .ini 文件中配置此设置，则会记录以下内容：

- 错误
- 常规信息

注销

此设置启用或禁用用户注销的详细日志记录。

默认情况下，此设置处于禁用状态。

启用此设置时，请确保同时启用**启用日志记录**设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在 Web Studio 或 .ini 文件中配置此设置，则会记录以下内容：

- 错误
- 常规信息

登录

此设置启用或禁用用户登录的详细日志记录。

默认情况下，此设置处于禁用状态。

启用此设置时，请确保同时启用**启用日志记录**设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在 Web Studio 或 .ini 文件中配置此设置，则会记录以下内容：

- 错误
- 常规信息

日志文件的最大大小

此设置指定 Profile Management 日志文件允许的最大大小（以字节为单位）。

默认情况下，此值设置为 1048576 字节 (1 MB)。

如果磁盘空间充足，Citrix 建议将此文件的大小增加到 5 MB 或更大。如果日志文件超出最大大小：

- 现有文件备份 (.bak) 将被删除
- 日志文件将重命名为 .bak
- 将创建一个新的日志文件

日志文件在 `%SystemRoot%\System32\Logfiles\UserProfileManager` 中创建。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则使用默认值。

日志文件路径

此设置指定用于保存配置文件管理日志文件的备用路径。

默认情况下，此设置处于禁用状态，日志文件保存在默认位置：%SystemRoot%\System32\Logfiles\UserProfileManager。

该路径可以指向本地驱动器或远程基于网络的驱动器 (UNC 路径)。远程路径在大型分布式环境中可能很有用，但它们可能会产生大量的网络流量，这可能不适合日志文件。对于具有持久性硬盘的预配虚拟机，请将本地路径设置为该驱动器。此设置可确保在计算机重新启动时保留日志文件。对于没有持久性硬盘的虚拟机，设置 UNC 路径可让您保留日志文件。但是，计算机的系统帐户必须对 UNC 共享具有写入权限。对于由脱机配置文件功能管理的任何笔记本电脑，请使用本地路径。

如果日志文件使用 UNC 路径，Citrix 建议对日志文件文件夹应用适当的访问控制列表。此设置可确保只有授权的用户或计算机帐户才能访问存储的文件。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则使用默认位置 %SystemRoot%\System32\Logfiles\UserProfileManager。

个性化用户信息

此设置启用或禁用个性化用户信息的详细日志记录。

默认情况下，此设置处于禁用状态。

启用此设置时，请确保同时启用“**启用日志记录**”设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在 Web Studio 或 .ini 文件中配置此设置，则会记录以下内容：

- 错误
- 常规信息

登录和注销时的策略值

此设置启用或禁用用户登录和注销时策略值的详细日志记录。

默认情况下，此设置为禁用。

启用此设置时，请确保同时启用“**启用日志记录**”设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在 Web Studio 或 .ini 文件中配置此设置，则会记录以下内容：

- 错误
- 常规信息

注册表操作

此设置启用或禁用对注册表中执行的操作进行详细日志记录。

默认情况下，此设置为禁用。

启用此设置时，请确保同时启用“**启用日志记录**”设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在 Web Studio 或 .ini 文件中配置此设置，则会记录以下内容：

- 错误
- 常规信息

注销时的注册表差异

此设置启用或禁用用户注销时注册表中任何差异的详细日志记录。

默认情况下，此设置处于禁用状态。

启用此设置时，请确保同时启用**启用日志记录**设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果在 Web Studio 或 .ini 文件中未配置此设置，则会记录以下内容：

- 错误
- 一般信息

配置文件处理策略设置

本节包含指定配置文件管理如何处理用户配置文件的策略设置。

删除缓存配置文件前的延迟

此设置指定在配置文件管理注销时删除本地缓存配置文件之前，可选的延迟时间（以分钟为单位）。

值为 0 会在注销过程结束时立即删除配置文件。配置文件管理每分钟检查一次注销。因此，值为 60 可确保在用户注销后一到两分钟内删除配置文件。此操作取决于上次检查发生的时间。如果您知道某个进程在注销期间保持文件或用户注册表配置单元处于打开状态，则延长延迟会很有用。对于大型配置文件，此过程还可以加快注销速度。

默认情况下，此值设置为 0，配置文件管理会立即删除本地缓存的配置文件。

启用此设置时，请确保也启用了“注销时删除本地缓存的配置文件”。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会立即删除配置文件。

注销时删除本地缓存的配置文件

此设置指定用户注销后是否删除本地缓存的配置文件。

启用此设置后，用户的本地配置文件缓存会在其注销后删除。Citrix® 建议为终端服务器启用此设置。

默认情况下，此设置处于禁用状态，用户的本地配置文件缓存在其注销后仍会保留。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则不会删除缓存的配置文件。

本地配置文件冲突处理

此设置配置了当用户配置文件同时存在于以下两个位置时，Profile Management 的行为方式：

- 用户存储
- 本地 Windows 用户配置文件（非 Citrix 用户配置文件）

默认情况下，Profile Management 使用本地 Windows 配置文件，但不会对其进行任何更改。

要控制 Profile Management 的行为方式，请选择以下选项之一：

- 使用本地配置文件。Profile Management 使用本地配置文件，但不会对其进行任何更改。
- 删除本地配置文件。Profile Management 删除本地 Windows 用户配置文件，然后从用户存储导入 Citrix 用户配置文件。
- 重命名本地配置文件。Profile Management 重命名本地 Windows 用户配置文件（用于备份），然后从用户存储导入 Citrix 用户配置文件。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则使用现有本地配置文件。

现有配置文件的迁移

此设置指定了如果用户在用户存储中没有当前配置文件，则在登录期间迁移到用户存储的配置文件类型。

如果用户在用户存储中没有配置文件，Profile Management 可以在登录期间“即时”迁移现有配置文件。之后，Profile Management 会在以下两种情况下使用用户存储配置文件：

- 当前会话
- 任何其他配置了相同用户存储路径的会话

默认情况下，本地配置文件和漫游配置文件都会在登录期间迁移到用户存储。

要指定登录期间迁移到用户存储的配置文件类型，请选择以下选项之一：

- 本地配置文件和漫游配置文件
- 本地
- 漫游
- 无（已禁用）

如果选择**无**，系统将使用现有的 Windows 机制创建配置文件，就像在未安装 Profile Management 的环境中一样。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会迁移现有的本地配置文件和漫游配置文件。

现有应用程序配置文件的自动迁移

此设置启用或禁用现有应用程序配置文件在不同操作系统之间的自动迁移。应用程序配置文件包括 `AppData` 文件夹中的应用程序数据和 `HKEY_CURRENT_USER\SOFTWARE` 下的注册表项。当您希望在不同操作系统之间迁移应用程序配置文件时，此设置会很有用。

例如，假设您将操作系统 (OS) 从 Windows 10 版本 1803 升级到 Windows 10 版本 1809。如果启用此设置，Profile Management 会在每个用户首次登录时自动将现有应用程序设置迁移到 Windows 10 版本 1809。因此，`AppData` 文件夹中的应用程序数据和 HKEY_CURRENT_USER\SOFTWARE 下的注册表项将被迁移。

如果存在多个现有应用程序配置文件，Profile Management 将按以下优先级顺序执行迁移：

1. 相同操作系统类型的配置文件（单会话操作系统到单会话操作系统，以及多会话操作系统到多会话操作系统）。
2. 相同 Windows 操作系统系列的配置文件；例如，Windows 10 到 Windows 10，或 Windows Server 2016 到 Windows Server 2016)。
3. 操作系统早期版本的配置文件；例如，Windows 7 到 Windows 10，或 Windows Server 2012 到 Windows 2016。
4. 最接近操作系统的配置文件。

注意： 必须通过在用户存储路径中包含变量“!CTX_OSNAME!”来指定操作系统的短名称。这样做可让 Profile Management 找到现有应用程序配置文件。

如果此处未配置此设置，则使用 .ini 文件中的设置。

如果此处或 .ini 文件中未配置此设置，则默认禁用此设置。

模板配置文件路径

此设置指定 Profile Management 用作模板以创建用户配置文件的路径。

指定的路径必须是包含 NTUSER.DAT 注册表文件以及模板配置文件所需的任何其他文件夹和文件的文件夹的完整路径。

注意：路径中不要包含 NTUSER.DAT。例如，对于文件 `\\myservername\myprofiles\template\ntuser.dat`，将位置设置为 `\\myservername\myprofiles\template`。

使用绝对路径，可以是 UNC 路径，也可以是本地计算机上的路径。例如，使用后者可以在 Citrix Provisioning™ Services 映像上永久指定模板配置文件。不支持相对路径。

注意：此设置不支持扩展 Active Directory 属性、系统环境变量或 `%USERNAME%` 和 `%USERDOMAIN%` 变量。

默认情况下，此设置处于禁用状态，新用户配置文件是根据用户首次登录的设备上的默认用户配置文件创建的。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则不使用任何模板。

模板配置文件覆盖本地配置文件

此设置允许模板配置文件在创建用户配置文件时覆盖本地配置文件。

假设用户没有 Citrix 用户配置文件，但有一个本地 Windows 用户配置文件。在这种情况下，如果此值已启用，则默认使用本地配置文件并将其迁移到用户存储。启用此策略设置后，模板配置文件可以在创建用户配置文件时覆盖所使用的本地配置文件。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则不使用任何模板。

模板配置文件覆盖漫游配置文件

此设置允许模板配置文件在创建用户配置文件时覆盖漫游配置文件。

假设用户没有 Citrix 用户配置文件，但有一个漫游 Windows 用户配置文件。在这种情况下，如果此值已启用，则默认使用漫游配置文件并将其迁移到用户存储。启用此策略设置后，模板配置文件可以在创建用户配置文件时覆盖所使用的漫游配置文件。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则不使用任何模板。

模板配置文件用作所有登录的 Citrix 强制配置文件

此设置允许 Profile Management 将模板配置文件用作创建所有用户配置文件的默认配置文件。

默认情况下，此设置处于禁用状态，新用户配置文件是从用户首次登录的设备上的默认用户配置文件创建的。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则不使用任何模板。

配置文件容器策略设置

配置文件容器

与用户配置文件关联的大型文件夹会导致登录缓慢。Citrix Profile Management 提供了一种基于 VHDX 的配置文件解决方案，可让您指定要包含在配置文件磁盘（VHDX 文件）中的文件夹。此解决方案通过将指定文件夹映射到存储在网络上的配置文件磁盘来减少登录时间。配置文件容器在登录期间附加包含这些文件夹的配置文件磁盘，从而无需将文件夹副本保存到本地配置文件。这样做可以缩短登录时间。

为配置文件容器启用本地缓存

此策略为 Citrix Profile Management 配置文件容器启用本地缓存支持。如果策略设置为**已启用**，则每个本地配置文件都充当其 Citrix Profile Management 配置文件容器的本地缓存。如果正在使用配置文件流技术，则按需创建本地缓存文件。否则，它们会在用户登录期间创建。要使用本地缓存功能，请将整个用户配置文件放入其 Citrix Profile Management 配置文件容器中。

要从配置文件容器中排除的文件夹

要从 Citrix Profile Management 配置文件容器中排除的文件夹列表。

要包含在配置文件容器中的文件夹

当其父文件夹被排除时，要保留在 Citrix Profile Management 配置文件容器中的文件夹列表。

此列表中的文件夹必须是排除文件夹的子文件夹。否则，此设置不起作用。

要包含在配置文件容器中的文件

要包含在 Citrix Profile Management 配置文件容器中的文件列表。

此列表中的文件必须位于排除文件夹内。否则，此设置不起作用。

要从配置文件容器中排除的文件

要从 Citrix Profile Management 配置文件容器中排除的文件列表。

启用 VHD 磁盘压缩

允许您为配置文件管理启用 VHD 磁盘压缩。如果启用，当满足特定条件时，VHD 磁盘会在用户注销时自动压缩。此策略使您能够节省配置文件容器、OneDrive 容器和镜像文件夹容器所占用的存储空间。

根据您的需求和可用资源，您可以使用高级设置中的“**触发 VHD 磁盘压缩的可用空间比率**”、“**触发 VHD 磁盘压缩的注销次数**”和“**禁用 VHD 磁盘压缩的碎片整理**”策略来调整默认的 VHD 压缩设置和行为。

为配置文件容器启用 VHD 自动扩展

允许您指定是否为配置文件容器启用 VHD 自动扩展。启用后，所有 VHD 自动扩展设置都将应用于配置文件容器。

配置优先级：

- 如果此处未配置此策略，则使用 .ini 文件中的值。
- 如果此处或 .ini 文件中均未配置此策略，则禁用此策略。

启用对 VHD 容器的独占访问

默认情况下，VHD 容器允许并发访问。启用此设置后，它们一次只允许一个访问。此功能适用于配置文件容器和 OneDrive 容器。

> **注意：**
>
> 在基于容器的配置文件解决方案中为配置文件容器启用此设置会自动禁用“*为配置文件容器启用多会话回写*”设置。

配置优先级：

1. 如果此处未配置此策略，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中均未配置此策略，则禁用此设置。

在登录期间配置文件容器不可用时注销用户

允许您在用户登录期间配置文件容器不可用时强制注销用户，并（可选）自定义用户看到的错误消息。

配置优先级：

1. 如果此处未配置此策略，则使用 .ini 文件中的值。
2. 如果此处或 .ini 文件中均未配置此策略，则禁用此设置。

访问配置文件容器的用户和组

允许您指定哪些 AD 域用户和组对配置文件容器具有 `Read & Execute` 权限。默认情况下，配置文件容器仅对其所有者可见。

配置优先级：

1. 如果此处未配置此策略，则使用 .ini 文件中的设置。
2. 如果此处或 .ini 文件中均未配置此策略，则配置文件容器仅对其所有者可见。

启用 BindLink 重定向

指定是否使用 Microsoft BindLink API 处理配置文件容器内的文件系统重定向。此功能默认禁用，并且仅在 Windows 11 24H2、Windows Server 2025 或更高版本（版本 10.0.25314.0 或更高）上受支持。

注册表策略设置

本节包含指定哪些注册表项包含在配置文件管理处理中或从中排除的策略设置。

排除列表

注销期间忽略的 HKCU 配置单元中的注册表项列表。

示例：Software\Policies

如果禁用此策略，则不排除任何注册表项。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不排除任何注册表项。

包含列表

注销期间处理的 HKCU 配置单元中的注册表项列表。

示例：Software\Adobe。

如果启用此策略，则仅处理此列表中的项。如果禁用此策略，则处理完整的 HKCU 配置单元。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则处理 HKCU 中的所有内容。

启用默认排除列表 - Profile Management 5.5

HKCU 配置单元中未同步到用户配置文件的注册表项的默认列表。使用此策略可以指定 GPO 排除文件，而无需手动填写。

如果禁用此策略，Profile Management 默认不排除任何注册表项。如果此处未配置此策略，Profile Management 将使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，Profile Management 默认不排除任何注册表项。

NTUSER.DAT 备份

启用 NTUSER.DAT 上一个已知良好副本的备份，并在发生损坏时回滚。

如果您未在此处配置此策略，配置文件管理将使用 .ini 文件中的值。如果您未在此处或 .ini 文件中配置此策略，配置文件管理将不会备份 NTUSER.DAT。

应用程序访问控制

允许您使用规则控制用户对文件、文件夹、注册表项和值的访问，或为文件、文件夹、注册表项和值实施计算机级重定向。

您可以通过两种方式创建应用程序规则：

- 基于 GUI 的工具 – **WEM Tool Hub > 应用程序访问控制规则生成器**
- PowerShell 工具 – 随 Profile Management 安装包提供

流式用户配置文件策略设置

本节包含指定 Profile Management 如何处理流式用户配置文件的策略设置。

始终缓存

此设置指定用户登录后 Profile Management 是否尽快缓存流式文件。用户登录后缓存文件可节省网络带宽，从而增强用户体验。

将此设置与“**配置文件流**”设置结合使用。

默认情况下，此设置处于禁用状态，并且用户登录后不会尽快缓存流式文件。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此设置未在此处或 .ini 文件中配置，则会禁用此设置。

始终缓存大小

此设置指定流式文件大小的下限（以 MB 为单位）。用户登录后，Profile Management 会尽快缓存此大小或更大的任何文件。

默认情况下，该值设置为 0（零），并使用缓存整个配置文件功能。启用缓存整个配置文件功能后，用户登录后，Profile Management 会在后台任务中从用户存储中获取所有配置文件内容。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此设置未在此处或 .ini 文件中配置，则会禁用此设置。

配置文件流技术

此设置启用和禁用 Citrix® 流式用户配置文件功能。启用后，仅当用户登录后访问配置文件文件和文件夹时，才会将其从用户存储中提取到本地计算机。挂起区域中的注册表项和文件会立即提取。

默认情况下，配置文件流式处理处于禁用状态。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此设置未在此处或 .ini 文件中配置，则会禁用此设置。

流式用户配置文件组

此设置根据 Windows 用户组指定 OU 中哪些用户配置文件是流式的。

启用后，仅流式传输指定用户组中的用户配置文件。所有其他用户配置文件都将正常处理。

默认情况下，此设置处于禁用状态，并且 OU 中的所有用户配置文件都将正常处理。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此设置在此处和 .ini 文件中均未配置，则所有用户配置文件都将进行处理。

启用配置文件流式处理排除

启用配置文件流式处理排除后：

- Profile Management 不会流式传输排除列表中的文件夹
- 用户登录时，所有文件夹都会立即从用户存储提取到本地计算机

有关详细信息，请参阅流式传输用户配置文件。

暂存区锁定文件的超时

此设置指定了在存储服务器无响应时用户存储保持锁定状态的情况下，用户文件从暂存区写回用户存储的天数。此行为可防止暂存区膨胀，并确保用户存储始终包含最新文件。

默认情况下，此设置设置为 1（一）天。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此设置在此处和 .ini 文件中均未配置，则使用默认值。

为暂存区启用配置文件流式处理

允许您为暂存区中的文件和文件夹启用配置文件流式处理功能。

启用配置文件流式处理时，暂存区用于确保配置文件一致性。它临时存储在并发会话中更改的配置文件和文件夹。

默认情况下，此策略处于禁用状态，并且登录时会将暂存区域中的所有文件和文件夹提取到本地配置文件。启用此策略后，暂存区域中的文件仅在请求时才提取到本地配置文件。将此策略与配置文件流技术策略结合使用，可确保在并发会话场景中获得最佳登录体验。

当“为文件夹启用配置文件流技术”策略处于启用状态时，此策略适用于暂存区域中的文件夹。

通过注册表管理的 HDX™ 功能

> **注意：**
>
> 不正确地编辑注册表可能导致严重问题，甚至可能需要重新安装操作系统。Citrix® 无法保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。编辑注册表之前，请务必备份注册表。
>
> 要在服务器上打开注册表编辑器，请运行 `regedit.exe`。然后导航到注册表项以添加或编辑设置。

设备

Bloomberg 键盘

Citrix Virtual Apps and Desktops™ 支持 Bloomberg 型号 4 和型号 3 右舷键盘。默认情况下，增强型 Bloomberg 键盘的支持处于禁用状态。

要在启动连接之前启用对 Bloomberg 键盘的支持，请在客户端计算机上设置以下注册表值：

- **项：** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **值名称：** `EnableBloombergHID`
- **值类型：** `DWORD`

- **值数据**：
  - `0` - 禁用
  - `1` - 启用

有关详细信息，请参阅Bloomberg 键盘。

映射的客户端驱动器

作为一项安全预防措施，当用户登录到 Citrix Virtual Apps and Desktops™ 时，服务器默认映射客户端驱动器，但不授予用户运行权限。要使用户能够运行驻留在映射客户端驱动器上的可执行文件，请通过编辑服务器上的注册表来覆盖此默认设置。

要允许访问，请编辑以下注册表值（如果不存在，请创建 **CDMSettings**）：

- **项**：`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`
- **值名称**：`ExecuteFromMappedDrive`
- **值类型**：`DWORD`
- **值数据**：
  - `1` - 允许权限
  - `0` - 拒绝映射驱动器上的权限

更改将在您编辑注册表后连接的会话中生效。

Citrix Virtual Apps and Desktops 7 2006 是第一个包含此注册表位置的版本。早期版本的 Citrix Virtual Apps and Desktops 使用了不同的注册表位置。

有关详细信息，请参阅客户端驱动器映射。

微软 Surface Pro 和 Surface Book 触控笔

Citrix Virtual Apps and Desktops 支持基于 Windows Ink 的应用程序的标准笔功能。默认情况下，此功能处于启用状态。

要禁用或启用此功能，请设置以下注册表值：

- **项**：`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **值名称**：`DisablePen`
- **值类型**：`DWORD`
- **值数据**:

- `1` - 禁用
- `0` - 启用

有关详细信息，请参阅 Microsoft Surface Pro 和 Surface Book 触控笔。

Windows 图像采集应用程序允许列表

此设置允许您控制 VDA 上的哪些应用程序可以访问 Windows 图像采集扫描仪重定向。

默认情况下，没有应用程序可以访问 Windows 图像采集。

要调整 VDA 上应用程序的 Windows 图像采集，请创建以下注册表设置:

- **项：** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`
- **值名称：** `WIAAllowedProcesses`

  选择并右键单击 **WIAAllowedProcesses**。选择 **新建 > 多字符串值** 并将新值重命名为 **AllowProcesses**。
- 值数据: 输入可以访问 Windows 图像采集的每个应用程序的完整路径和进程名称。每行提供一个应用程序。

对此设置的任何更改将在您下次在 VDA 上启动会话时生效。

通用

安全连接端口

当 VDA 上启用 TLS/DTLS 时，默认连接端口号为 443。要更改端口，请修改以下注册表值:

- **项：** `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **值名称**: `SSLPort`
- **值类型**: `DWORD`
- **值数据**: `443` (十进制)

HDX 直连

多会话会话主机中 HDX Direct 的默认超时为 60 秒。要更改超时，请修改以下注册表值：

- **项**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\HdxDirect`
- **值名称**: `HdxDirectInitiateTimeoutInSeconds`

- **值类型**: `DWORD`
- **值数据**: `60` (十进制)

HDX 缩减器

您可以配置要在会话主机中使用的 HDX 压缩算法 (Reducer) 版本。

要在单会话 VDA 中启用 Reducer V4，请设置以下注册表值：

- **项**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings`
- **值名称**: `ReducerOverrideMask`
- **值类型**: `DWORD`
- **值数据**: `23` (十进制)

要在多会话 VDA 中启用 Reducer V4，请设置以下注册表值：

- **项**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **值名称**: `ReducerOverrideMask`
- **值类型**: `DWORD`
- **值数据**: `23` (十进制)

配置 Rendezvous 版本

要配置要使用的 Rendezvous 版本，请设置以下注册表值：

- **项**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
- **值类型**: `DWORD`
- **值名称**: `GctRegistration`
- **值数据**：
  - `1` - 启用 V2
  - `0` - 启用 V1

配置自动登录到 VDA

此设置允许您在 Windows 10 单会话操作系统和多会话操作系统 VDA 上启用或禁用 **始终提示输入密码** Microsoft 策略设置。

如果**始终提示输入密码**已启用，则用户在启动远程会话时必须在 VDA 上输入凭据。如果此设置已禁用，则用户将自动连接到远程会话，而无需在 VDA 上提供凭据。

默认情况下，Microsoft 策略设置处于禁用状态。要启用或禁用**始终提示输入密码**设置，请在 VDA 上设置以下注册表值：

- **项**：`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica`
- **值名称**：`AutoLogon`
- **值类型**：`DWORD`
- **值数据**：
  - `1` - 禁用 Microsoft 策略设置，并允许用户自动登录到远程会话。
  - `0` – 启用 Microsoft 策略设置，并在用户启动远程会话时提示他们提供凭据。

禁用超时警告

默认情况下，会话不活动或空闲的用户会在会话自动断开连接前两分钟收到一条警告消息。

此设置禁用并删除以下情况下达到空闲会话超时限制的用户的警告消息：

- Windows 服务器 2004
- Windows 10 多会话 2004 或更高版本的多会话操作系统

要删除此警告，请在 VDA 上设置以下注册表值：

- **项**：`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP`
- **值名称**：`fEnableTimeoutWarning`
- **值类型**：`DWORD`
- **值数据**：
  - `1` - 禁用警告消息
  - `0` - 启用警告消息

要显示警告消息，请删除注册表值或将其设置为 `0`。

EDT MTU 发现

MTU 发现允许 EDT 在建立会话时自动确定最大传输单元 (MTU)。这样做可以防止 EDT 数据包碎片化，否则可能会导致性能下降或无法建立会话。

此设置默认启用。要禁用 EDT MTU 发现，请配置以下注册表值并重新启动会话主机：

- **项**：`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`

- **值名称：** `MtuDiscovery`
- **值类型：** `DWORD`
- **值数据：** `0`

要启用 MTU 重新发现，请配置以下注册表值并重新启动会话主机：

- **项：** `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\MtuRediscovery`
- **值名称：** `MtuReDiscovery`
- **值类型：** `DWORD`
- **值数据：** `1`
- **项：** `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\MtuRediscovery`
- **值名称：** `MtuReDiscoveryFrequency`
- **值类型：** `DWORD`
- **值数据：** `1`

这些设置是计算机范围的，会影响从受支持的客户端连接的所有会话。

EDT 超时

您可以将 VDA 中的 EDT 超时设置为 5 到 25 秒之间的任何值。默认 EDT 超时值为 10 秒。

- **项：** `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters`
- **值类型：** `DWORD`
- **值名称：** `edtConnectionTimeout`
- **值数据：** 5 到 25 之间的秒数（十进制）

您还可以为适用于 Windows 版本 2409.10 及更早版本的 Citrix Workspace 应用程序设置 EDT 超时：

- **项：** `HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT`
- **值类型：** `String / REG_SZ`
- **值名称：** `edtConnectionTimeout`
- **值数据：** 5 到 25 之间的秒数（十进制）

> **注意：**
>
> VDA 的超时设置将从版本 2503 开始由 Citrix Workspace 应用程序使用，从而无需在客户端设备上配置超时。

通用内容重定向

添加用于主机到客户端重定向的 URL 类型

默认情况下，我们支持以下 URL 类型的重定向：HTTP、HTTPS、RTSP、RTSPU、PNM 和 MMS。您可以通过在 Windows 客户端上创建以下注册表项和值来将 URL 类型添加到列表中。

- **项：** `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA`
- **值名称：** `ExtraURLProtocols`
- **值类型：** `REG_SZ`
- **值数据：** 指定所需的 URL 类型，用分号分隔。包括 URL 权限部分之前的所有内容。例如：`ftp://;mailto:;customtype1://;custometype2://`

您只能为 Windows 客户端添加 URL 类型。缺少此注册表设置的客户端会拒绝重定向回 Citrix 会话。客户端必须安装并配置一个应用程序来处理指定的 URL 类型。

有关详细信息，请参阅主机到客户端重定向。

客户端文件夹重定向

客户端文件夹重定向改变了客户端文件在主机端会话中可访问的方式。假设您在服务器上启用了客户端文件夹重定向，并且用户在用户设备上对其进行了配置。在这种情况下，用户指定的本地卷部分将被重定向。

要在服务器上启用客户端文件夹重定向，请设置以下注册表值：

- **项：** `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection`
- **值名称：** `CFROnlyModeAvailable`
- **值类型：** `DWORD`
- **值数据：** `1`

有关详细信息，请参阅客户端文件夹重定向。

针对特定网站集的主机到客户端重定向

要针对特定网站集启用主机到客户端重定向，请在服务器 VDA 上设置以下注册表值。

- **项：** `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **值名称：** `ValidSites`
- **值类型：** `REG_MULTI_SZ`
- **值数据：**指定完全限定域名 (FQDN) 的任意组合。在单独的行上键入多个 FQDN。仅包含 FQDN，不包含协议（`http://` 或 `https://`）。FQDN 只能在最左侧位置包含星号 (`*`) 作为通配符。此通配符匹配单个级别的域，这与 RFC 6125 中的规则一致。例如：

`www.example.com`

`*.example.com`

有关详细信息，请参阅主机到客户端重定向。

注销和断开连接时的本地应用程序行为

默认情况下，当用户从虚拟桌面注销或断开连接时，本地应用程序会继续运行。重新连接后，如果本地应用程序在虚拟桌面上可用，则会重新集成。要配置注销和断开连接时的本地应用程序行为，请在托管桌面中设置以下注册表值：

- **项：** `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies`
- **值名称：** `Session State`
- **值类型：** `DWORD`
- **值数据：**
  - `1` - 当用户注销或断开与虚拟桌面的连接时，本地应用程序会继续运行。重新连接后，如果本地应用程序在虚拟桌面上可用，则会重新集成。
  - `3` - 当用户注销或断开与虚拟桌面的连接时，本地应用程序会关闭。

有关详细信息，请参阅本地应用程序访问和 URL 重定向。

从主机到客户端重定向的默认列表中删除 URL 类型

要从默认重定向列表中删除 URL 类型，请在服务器 VDA 上创建以下注册表项和值。

- **项：** `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **值名称：** `DisableServerFTA`
- **值类型：** `DWORD`
- **值数据：** `1`
- **值名称：** `NoRedirectClasses`

- **值类型**：`REG_MULTI_SZ`
- **值数据**：指定以下值的任意组合：`http`、`https`、`rtsp`、`rtspu`、`pnm` 或 `mms`。在单独的行上键入多个值。例如：

`http`

`https`

`rtsp`

有关详细信息，请参阅主机到客户端重定向。

服务器 VDA 默认浏览器配置

您可以启用主机到客户端重定向，以取代服务器 VDA 上的任何默认浏览器配置。如果 Web URL 未重定向，Citrix 启动器会将该 URL 传递给 `command_backup` 注册表项中配置的浏览器。该项默认指向 Internet Explorer，但您可以修改它以包含不同浏览器的路径。

- 互联网探索者（默认）
  - **键**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **值名称**: `Default`
  - **值类型**: `REG_SZ`
  - **值数据**: `"c:\program files\internet explorer\iexplore.exe" "%1"`
  - **键**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **值名称**: `Default`
  - **值类型**: `REG_SZ`
  - **值数据**: `"c:\program files\internet explorer\iexplore.exe" "%1"`
- 谷歌浏览器
  - **键**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **值名称**: `Default`
  - **值类型**: `REG_SZ`
  - **值数据**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`
  - **键**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **值名称**: `Default`
  - **值类型**: `REG_SZ`

  - **值数据**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`

- 微软 Edge
  - **键**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **值名称**: `Default`
  - **值类型**: `REG_SZ`
  - **值数据**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`
  - **键**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **值名称**: `Default`
  - **值类型**: `REG_SZ`
  - **值数据**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`

已发布的应用程序的本地应用访问

本地应用访问将本地安装的 Windows 应用程序无缝集成到托管桌面环境中，而无需在不同桌面之间切换。要为已发布的应用程序提供访问权限，请在服务器上设置以下注册表值：

- **键**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`
- **值名称**: `ClientHostedAppsEnabled`
- **值类型**: `DWORD`
- **值数据**：
  - `1` - 启用
  - `0` - 禁用

有关详细信息，请参阅本地应用程序访问和 URL 重定向。

图形

CUDA 或 OpenCL 应用程序的 GPU 加速

默认情况下，在用户会话中运行的 CUDA 和 OpenCL 应用程序的 GPU 加速处于禁用状态。

要使用 CUDA 加速 POC 功能，请启用以下注册表设置：

- **项：** `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **值名称：** `CUDA`
- **值类型**: `DWORD`
- **值数据**: `00000001`

要使用 OpenCL 加速 POC 功能，请启用以下注册表设置：

- **项：** `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **值名称：** `OpenCL`
- **值类型**: `DWORD`
- **值数据**: `00000001`

有关详细信息，请参阅 Windows 多会话操作系统 GPU 加速

渐进模式

渐进模式默认处于禁用状态。您可以使用以下注册表值更改渐进模式状态：

- **项**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- **值类型**: `REG_DWORD`
- **值名称**: `ProgressiveDisplay`
- **值数据**:
  - `0` - 始终关闭（禁用渐进模式。此值为默认值。）
  - `1` - 自动（根据网络条件切换。）
  - 2 = 始终开启

有关详细信息，请参阅 渐进模式。

> **注意：**
>
> 渐进模式已弃用。Thinwire 是一种替代选项，可优化图像传输并保持缓存效率，同时提供渐进模式的几乎所有优势。

Windows 演示基础 (WPF) 渲染

HDX 3D Pro 允许在 Windows 多会话操作系统会话中运行的图形密集型应用程序在服务器的图形处理单元 (GPU) 上进行渲染。通过将 Windows Presentation Foundation (WPF) 渲染移动到服务器的 GPU，图形渲染不会降低服务器的 CPU 速度。

要使用服务器的 GPU 启用 WPF 应用程序渲染，请在运行 Windows 多会话操作系统的服务器注册表中创建以下设置：

1. 在 VDA 上打开注册表编辑器，然后转到以下项：

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. 创建或编辑以下注册表值：

   - AdapterHandle = 0x00000001
   - DevicePath = 0x00000001
   - 标志 = 0x00000412
   - WPF = 0x00000001

3. 使用 WPF 应用程序的可执行文件名称创建子项。例如，如果您的应用程序名为“mywpfapp.exe”，请创建以下项：

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe`

4. 重新启动服务器以使设置生效。

有关详细信息，请参阅 适用于 Windows 多会话操作系统的 GPU 加速 以及关于 充分利用 Windows 多会话操作系统上的 WPF 应用程序 的博客。

多媒体

网络摄像头软件压缩

如果网络摄像头支持硬件编码，HDX 视频压缩默认使用硬件编码。硬件编码可能比软件编码消耗更多带宽。要强制进行软件压缩，请将以下值添加到客户端：

- **键：** `HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`
- **值名称：** `DeepCompress_ForceSWEncode`
- **值类型：** `DWORD`
- **值数据：** `1`

有关详细信息，请参阅 HDX 网络摄像头视频压缩。

网络摄像头视频分辨率

如果媒体类型协商失败，HDX 将回退到默认的 VGA 分辨率（640 x 480 像素）。您可以使用客户端上的注册表项来配置默认分辨率。在设置以下注册表项之前，请确保摄像头支持指定的分辨率。

- **项**：`HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- 宽度
  - **值名称**：`DefaultWidth`
  - **值类型**：`DWORD`
  - **值数据**：所需的十进制宽度（例如：1280）
- 高度
  - **值名称**：`DefaultHeight`
  - **值类型**：`DWORD`
  - **值数据**：所需的十进制高度（例如 720）

摄像头视频压缩帧率

要调整首选视频帧率，请在客户端上编辑以下注册表值：

- **项**：`HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- **值名称**：`FramesPerSecond`
- **值类型**：`DWORD`
- **值数据**：`15`

如果网络摄像头不支持指定的帧率，应用程序将默认使用 15 FPS。

有关详细信息，请参阅 HDX 网络摄像头视频压缩。

Microsoft Teams 回退模式

如果 Microsoft Teams 未能在优化的 VDI 模式下加载（在 Teams/关于/版本中显示“Citrix HDX 未连接”），VDA 将回退到旧版 HDX 技术，例如网络摄像头重定向以及客户端音频和麦克风重定向。如果您使用的 Workspace 应用程序版本/平台操作系统不支持 Microsoft Teams 优化，则回退注册表项不适用。

要控制回退机制，请在 VDA 上设置以下注册表值之一：

- **项**（只需一个）：
  - **计算机设置**：`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams`

  - **用户设置：** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams`

- **值名称：** `DisableFallback`
- **值类型**: `DWORD`
- 值数据:
  - `1` - 禁用回退模式
  - `2` - 仅启用音频

如果该值不存在或设置为 0，则启用回退模式。此功能需要 Microsoft Teams 1.3.0.13565 或更高版本。有关详细信息，请参阅优化 Microsoft Teams。

使用 Citrix App Layering™ 对 Microsoft Teams 进行优化

如果使用 Citrix App Layering 在不同层中管理 VDA 和 Microsoft Teams 安装，请在从命令行使用 `ALLUSER=1` 标志安装 Microsoft Teams 之前，在 Windows 上创建一个名为 **PortICA** 的空注册表项。保留默认值名称、类型和数据。

- 注册表编辑器的 32 位版本密钥：`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`
- 注册表编辑器的 64 位版本密钥：`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

有关详细信息，请参阅优化 Microsoft Teams。

负载管理策略设置

“**负载管理**”部分包含用于在提供 Windows 多会话操作系统计算机的服务器之间启用和配置负载管理的策略设置。

有关计算负载评估器索引的信息，请参阅 CTX202150。

并发登录容忍度

此设置指定服务器可以接受的并发登录的最大数量。

默认情况下，此值设置为 2。

启用此设置后，负载平衡会尝试避免在同一时间在服务器 VDA 上有超过指定数量的活动登录。但是，此限制并未严格执行。要强制执行此限制（并导致超过指定数量的并发登录失败），请创建以下注册表项:

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit 类型: DWORD 值: 1

CPU 使用率

此设置指定 CPU 使用率的百分比级别，服务器在此级别报告满负载。启用后，服务器报告满负载的默认值为 90%。

默认情况下，此设置已禁用，CPU 使用率将从负载计算中排除。

CPU 使用率排除进程优先级

> **注意：**
>
> 在 Workspace Environment Management 管理计算机的场景中，将此设置与 CPU 优先级 设置一起使用可能会产生意外结果。如果您选择使用 CPU 优先级设置，建议您禁用此设置。

> 此设置指定优先级级别，在此级别，进程的 CPU 使用率将从 CPU 使用率负载索引中排除。

默认情况下，此值设置为 **低于正常** 或 **低**。

磁盘使用情况

此设置指定磁盘队列长度，在此长度下，服务器报告 75% 的满负载。启用后，磁盘队列长度的默认值为 8。

默认情况下，此设置已禁用，磁盘使用率将从负载计算中排除。

最大会话数

此设置指定服务器可托管的最大会话数。启用后，服务器可托管的最大会话数的默认设置为 250。

默认情况下，此设置处于启用状态。

内存使用情况

此设置指定服务器报告满负载时的内存使用量级别（以百分比表示）。启用后，服务器报告满负载的默认值为 90%。

默认情况下，此设置处于禁用状态，内存使用量不计入负载计算。

内存使用量基本负载

此设置指定基本操作系统的近似内存使用量。此外，它还以 MB 为单位定义了服务器被视为零负载的内存使用量阈值。

默认情况下，此值设置为 768 MB。

配置文件管理策略设置

本节包含用于启用和配置配置文件管理的策略设置。

有关其他信息，例如以下内容，请参阅配置文件管理策略：

- 等效的 .ini 文件设置的名称
- 哪个版本的配置文件管理是策略设置所需的

用户个性化层策略设置

为了启用用户层在虚拟投递代理中的挂载，请使用配置参数指定：

- 在网络上的何处访问用户层。
- 任何新用户层磁盘可以增长到多大。

为此，以下两个策略会出现在可用策略列表中：

- 用户层存储库路径 - 在“值”字段中输入路径，格式为“\\服务器名称或地址\文件夹名称”。
- 用户层大小 (GB) - Citrix® 建议的最小默认用户层大小为 10 GB。用户层是精简预配磁盘，会随着空间的使用而扩展到设定的大小。用户层的大小永远不会减小。

> **注意：**
>
> 增加用户层大小会影响新的用户层并扩展现有的用户层。减小层大小仅影响新的用户层。现有用户层的大小永远不会减小。

> 有关详细信息，请参阅用户个性化层。

虚拟投递代理策略设置

虚拟投递代理 (VDA) 部分包含用于控制 VDA 与站点控制器之间通信的策略设置。

重要提示：如果您未使用自动更新功能，VDA 需要这些设置提供的信息才能向 Delivery Controller™ 注册。由于注册需要此信息，因此您必须使用组策略编辑器配置以下设置，除非您在 VDA 安装期间提供此信息：

- 控制器注册 IPv6 网络掩码
- 控制器注册端口
- 控制器 SID

- 控制器
- 仅使用 IPv6 控制器注册
- 站点 GUID

控制器注册 IPv6 网络掩码

此策略设置允许管理员将 VDA 限制为仅使用首选子网（而不是全局 IP，如果已注册）。此设置指定 VDA 注册的 IPv6 地址和网络。VDA 仅注册与指定网络掩码匹配的第一个地址。此设置仅在启用“仅使用 IPv6 控制器注册”策略设置时有效。

默认情况下，此设置为空白。

控制器注册端口

仅当**启用控制器自动更新**设置被禁用时，才使用此设置。

此设置指定 VDA 在使用基于注册表的注册时用于向控制器注册的 TCP/IP 端口号。

默认情况下，端口号设置为 80。

控制器 SID

仅当“**启用控制器自动更新**”设置处于禁用状态时，才使用此设置。

此设置指定 VDA 在使用基于注册表的注册时用于向控制器注册的控制器安全标识符 (SID) 的空格分隔列表。此设置为可选设置，可与“**控制器**”设置结合使用，以限制用于注册的控制器列表。

默认情况下，此设置为空白。

控制器

仅当“**启用控制器自动更新**”设置处于禁用状态时，才使用此设置。

此设置指定 VDA 在使用基于注册表的注册时用于向控制器注册的控制器完全限定域名 (FQDN) 的空格分隔列表。此设置为可选设置，可与“**控制器 SID**”设置结合使用。

默认情况下，此设置为空白。

启用控制器自动更新

此设置使 VDA 能够在安装后自动向控制器注册。

VDA 注册后，与其注册的控制器会将当前控制器 FQDN 和 SID 列表发送给 VDA。VDA 将此列表写入持久性存储。每个控制器还会每 90 分钟检查一次站点数据库以获取控制器信息。如果发生以下任一情况，控制器会将其更新的列表发送给其注册的 VDA：

- 自上次检查以来已添加或删除了控制器
- 已发生策略更改

VDA 接受来自其收到的最新列表中所有控制器的连接。

默认情况下，此设置处于启用状态。

仅使用 IPv6 控制器注册

此设置控制 VDA 用于向控制器注册的地址形式：

- 启用后，VDA 使用计算机的 IPv6 地址向控制器注册。当 VDA 与控制器通信时，它使用以下地址顺序：全局 IP 地址、唯一本地地址 (ULA)、链路本地地址（如果没有其他 IPv6 地址可用）。
- 禁用后，VDA 使用计算机的 IPv4 地址向控制器注册并进行通信。

默认情况下，此设置为禁用状态。

站点 GUID

仅当**启用控制器自动更新**设置被禁用时才使用此设置。

此设置指定 VDA 在使用基于 Active Directory 的注册时用于向控制器注册的站点的全局唯一标识符 (GUID)。

默认情况下，此设置为空白。

HDX™ 3D Pro 策略设置

HDX 3D Pro 部分包含用于启用和配置面向用户的图像质量配置工具的策略设置。此工具使用户能够优化可用带宽的使用。为了实现此优化，图像质量和响应能力之间的平衡会实时调整。

启用无损

此设置指定用户是否可以使用图像质量配置工具启用和禁用无损压缩。默认情况下，用户无法选择启用无损压缩。

假设用户启用了无损压缩。在这种情况下，图像质量会自动设置为图像配置工具中可用的最大值。默认情况下，可以根据用户设备和主机的功能使用基于 GPU 或 CPU 的压缩。

HDX 3D Pro 质量设置

此设置指定图像质量配置工具中可供用户使用的最小值和最大值。使用这些值，用户可以在图像质量配置工具中定义图像质量调整范围。

指定介于 0 到 100（含）之间的图像质量值。最大值必须大于或等于最小值。

监视策略设置

“**监视**”部分包括用于进程、资源监视和应用程序故障监视的策略设置。

这些策略的范围可以根据以下内容定义：

- 站点
- 交付组
- 交付组类型
- 组织单位
- 标签

网络遥测

启用此设置可收集网络指标，例如会话吞吐量、重传和 L7 延迟，以便在 Citrix DaaS Monitor 中进行实时故障排除和历史报告。

启用此设置还会为 NetScaler Gateway 和 NetScaler Console 启用增强型 HDX Insight 通道。如果启用了 Secure HDX，则 HDX Insight 需要此功能。

进程和资源监视策略

CPU、内存和进程的每个数据点都从 VDA 收集并存储在监视数据库中。从 VDA 发送数据点会消耗网络带宽，而存储它们会占用监视数据库中的大量空间。请考虑您不希望针对特定范围（例如，特定的交付组或组织单位）监视资源数据或进程数据或两者。在这种情况下，建议禁用该策略。

启用进程监视

启用此设置以允许监视在装有 VDA 的计算机上运行的进程。CPU 和内存使用情况等统计信息将发送到监视服务。这些统计信息用于 Director 中的实时通知和历史报告。

此设置的默认值为“已禁用”。

启用资源监视

启用此设置以允许监视装有 VDA 的计算机上的关键性能计数器。统计信息（例如 CPU 和内存使用情况、IOPS 和磁盘延迟数据）将发送到监视服务。这些统计信息用于 Director 中的实时通知和历史报告。

此设置的默认值为“已启用”。

可扩展性

CPU 和内存数据每 5 分钟从每个 VDA 推送到数据库。进程数据（如果启用）每 10 分钟推送到数据库。IOPS 和磁盘延迟数据每 1 小时推送到数据库。

CPU 和内存数据

CPU 和内存数据默认**启用**。数据保留值如下（白金版许可证）：

数据粒度	天数
5 分钟数据	1 天
10 分钟数据	7 天
每小时数据	30 天
每日数据	90 天

IOPS 和磁盘延迟数据

IOPS 和磁盘延迟数据默认**启用**。数据保留值如下（白金版许可证）：

数据粒度	天数
每小时数据	3 天
每日数据	90 天

根据数据保留设置，存储一个 VDA 一年内的以下数据大约需要 276 KB 的磁盘空间：

- CPU
- 内存
- IOPS
- 磁盘延迟数据

计算机数量	所需近似存储空间
1	276 KB
1K	270 MB
40K	10.6 GB

进程数据

默认情况下，进程数据处于**已禁用**状态。建议根据需要在一部分计算机上启用进程数据。进程数据的默认数据保留设置如下：

数据粒度	天数
10 分钟数据	1 天
每小时数据	7 天

如果使用默认保留设置启用进程数据，则进程数据在一年内将占用每个 VDA 大约 1.5 MB，每个终端服务 VDA (TS VDA) 大约 3 MB。

计算机数量	VDA 所需的大致存储空间	TS VDA 所需的大致存储空间
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

注意：

前面提供的数字不包括索引空间。所有计算均为近似值，并根据部署情况而异。

可选配置

您可以修改默认保留设置以满足您的需求。但是，此配置会占用额外的存储空间。通过启用以下设置，您可以提高进程利用率数据的准确性。可以启用的配置包括：

ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

这些配置可以通过监控 PowerShell cmdlet 启用：Set-MonitorConfiguration

应用程序故障监控策略

默认情况下，“**应用程序故障**”选项卡仅显示多会话操作系统 VDA 的应用程序故障。应用程序故障监控的设置可以通过以下监控策略进行修改：

启用应用程序故障监控

使用此设置可配置应用程序故障监控，以监控应用程序错误或故障（崩溃和未处理的异常），或两者兼有。 通过将“**值**”设置为“**无**”来禁用应用程序故障监控。 此设置的默认值为“仅应用程序故障”。

在单会话操作系统 VDA 上启用应用程序故障监控

默认情况下，仅监控多会话操作系统 VDA 上托管的应用程序的故障。要监控单会话操作系统 VDA，请将策略设置为“**允许**”。 此设置的默认值为“**禁止**”。

从故障监控中排除的应用程序列表

指定不进行故障监控的应用程序列表。 默认情况下，此列表为空。

用于分析数据收集的策略

用于分析的 VDA 数据收集

使用此策略可启用或禁用 Monitor 服务收集 VDA 的性能和安全相关指标，以用于性能和安全分析。默认情况下，此策略为**允许**。将策略设置为**禁止**可停止从 VDA 收集数据。

用于安全监控的剪贴板位置元数据收集

使用此策略可启用或禁用 Broker 服务收集剪贴板位置元数据，以用于安全监控、审计和合规性。默认情况下，此策略为**已启用**。将策略设置为**已禁用**可停止从 VDA 收集数据。

用于性能监控的诊断数据收集

使用此策略可启用监控服务收集诊断数据，例如会话信息、UPM/EUEM 服务状态、Microsoft Teams 优化和连接协议。默认情况下，此策略为**已启用**。将策略设置为**已禁用**可停止从 VDA 收集数据。

存储规划提示

组策略。如果您对监控资源数据或进程数据不感兴趣，可以使用组策略关闭其中一个或两者。有关详细信息，请参阅 创建策略 的**组策略**部分。

数据整理。可以修改默认数据保留设置，以提前整理数据并释放存储空间。有关整理设置的详细信息，请参阅 使用 API 访问数据 中的“数据粒度和保留”。

虚拟 IP 策略设置

> **重要提示：**
>
> - Windows 10 Enterprise 多会话不支持远程桌面 IP 虚拟化 (虚拟 IP)，并且我们不支持在 Windows 10 Enterprise 多会话上使用远程桌面 IP 虚拟化或虚拟环回。
> - 远程桌面 IP 虚拟化 (虚拟 IP) 不支持在云托管计算机上使用。有关详细信息，请参阅 Microsoft 文档。

虚拟 IP 部分包含策略设置，用于控制会话是否拥有自己的虚拟环回地址。

虚拟 IP 环回支持

启用此设置后，每个会话都有自己的虚拟环回地址。禁用后，会话将没有单独的环回地址。

默认情况下，此设置为禁用状态。

虚拟 IP 虚拟环回程序列表

此设置指定可以使用虚拟环回地址的应用程序可执行文件。将程序添加到列表时，只需指定可执行文件的名称。无需指定完整路径。

默认情况下，未指定任何可执行文件。

虚拟 IP 环回端口排除

当应用程序调用此设置中指定的任何端口上的环回地址时，虚拟环回不会将调用更改为会话特定的环回地址。

工作区环境管理™ 策略设置

Workspace Environment Management (WEM) 部分包含策略设置，可帮助您管理 WEM 代理的运行方式。

(仅限 WEM 服务) 代理的代理配置

目前仅适用于 DaaS 部署。

指定 WEM 代理用于与 Citrix Cloud 通信的代理服务器。格式：`http://<FQDN or IP address>:<port number>`，例如 `<http://10.108.125.51:8080>`。

(仅限本地 WEM) 代理服务端口

目前仅适用于 DaaS 部署。

指定 WEM 代理用于连接到 WEM 基础结构服务器的端口。默认端口为 **8286**，对应于 `AgentPort` 命令行参数。

(仅限本地 WEM) 缓存数据同步端口

目前仅适用于 DaaS 部署。

(适用于 WEM 1912 及更高版本) 指定 WEM 代理用于将其本地缓存与 WEM 基础结构服务器同步的端口。默认端口为 **8288**，对应于 `CachedDataSyncPort` 命令行参数。

(仅限 WEM 服务) Citrix Cloud 连接器

指定 WEM 代理连接到的 Citrix Cloud Connector 计算机。为确保高可用性，请在每个资源位置部署至少两个 Cloud Connector。确保 Cloud Connector 和代理计算机位于同一 AD 域中。

用于基本部署的自定义设置

目前仅适用于 DaaS 部署。

自定义用于基本部署的代理设置。有关可用设置的更多信息，请参阅 Workspace Environment Management 文档。

(仅限 WEM 服务) 从 CVAD 服务发现 Citrix Cloud Connector

目前仅适用于 DaaS 部署。

当未配置 Cloud Connector 时，使 WEM 代理能够自动从 Citrix DaaS 部署中发现 Cloud Connector。成功发现后，代理将连接到相应的 Cloud Connector 计算机。

重要提示： 如果在代理安装期间配置了 Cloud Connector，或者如果已启用**Citrix Cloud Connectors**策略设置，则此设置不适用。

(仅限本地 WEM) 基础架构服务器

目前仅适用于 DaaS 部署。

指定 WEM 基础架构服务器的完全限定域名 (FQDN) 或 IP 地址。WEM 代理连接到此服务器以检索配置、更新其本地缓存并报告监视数据。

覆盖代理部署类型

目前仅适用于 DaaS 部署。

覆盖默认 WEM 代理部署类型。选择以下选项之一：

- 云服务 – 将代理连接到 Citrix Cloud 中的 WEM 服务，提供完整的 WEM 功能。
- 本地 – 将代理连接到本地 WEM 部署，提供完整的 WEM 功能。
- 基本部署 – 以单机模式运行 WEM，功能有限，不连接到 WEM 基础架构。
- 已禁用 – 禁用安装了代理的计算机上的所有 WEM 功能。

使用注册表配置 COM 端口和 LPT 端口重定向设置

在 VDA 7.0 到 7.8 版本中，**COM 端口和 LPT 端口**设置只能使用注册表进行配置。对于早于 7.0 的 VDA 版本以及 7.9 及更高版本的 VDA，这些设置可在 Web Studio 中配置。有关详细信息，请参阅端口重定向策略设置 和带宽策略设置。

COM 端口和 LPT 端口重定向的策略设置位于 VDA 映像或计算机上的 HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated 下。

要启用 COM 端口和 LPT 端口重定向，请按如下所示添加类型为 REG_DWORD 的新注册表项：

注意：不正确地编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix® 无法保证可以解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。在编辑注册表之前，请务必备份注册表。

注册表项	描述	允许的值
AllowComPortRedirection	允许或禁止 COM 端口重定向	1（允许）或 0（禁止）
LimitComBw	COM 端口重定向通道的带宽限制	数值
LimitComBWPercent	COM 端口重定向通道的带宽限制，占总会话带宽的百分比	0 到 100 之间的数值
AutoConnectClientComPorts	自动连接用户设备上的 COM 端口	1（允许）或 0（禁止）
AllowLptPortRedirection	允许或禁止 LPT 端口重定向	1（允许）或 0（禁止）
LimitLptBw	LPT 端口重定向通道的带宽限制	数值
LimitLptBwPercent	LPT 端口重定向通道的带宽限制，占总会话带宽的百分比	0 到 100 之间的数值
AutoConnectClientLptPorts	自动连接用户设备上的 LPT 端口	1（允许）或 0（禁止）

配置这些设置后，更改您的计算机目录以使用新的主映像或更新的物理机。下次用户注销时，桌面将使用新设置进行更新。

策略变更

Citrix Virtual Apps and Desktops™ 7 2607 LTSR 中没有策略更改。

管理

管理 Citrix Virtual Apps and Desktops™ 站点涵盖了各种项目和任务。

许可

创建站点时，需要与 Citrix 许可证服务器建立有效连接。之后，您可以从 Studio 完成多项许可任务，包括添加许可证、更改许可证类型或模型以及管理许可证管理员。您还可以从 Studio 访问许可证管理控制台。

应用程序

在交付组中管理应用程序，也可以在应用程序组中管理。

区域

在地理分散的部署中，您可以使用区域使应用程序和桌面更接近最终用户，从而提高性能。安装和配置站点时，所有控制器、计算机目录和主机连接都位于一个主区域中。之后，您可以使用 Studio 创建包含这些项目的卫星区域。站点拥有多个区域后，您将能够指示任何新创建的计算机目录、主机连接或添加的控制器将放置在哪个区域中。您还可以在区域之间移动项目。

连接和资源

如果您使用虚拟机管理程序或其他服务来托管向用户交付应用程序和桌面的计算机，则在创建站点时，您将创建与该虚拟机管理程序或其他服务的第一个连接。该连接的存储和网络详细信息构成了其资源。之后，您可以更改该连接及其资源，并创建更多连接。您还可以管理使用已配置连接的计算机。

本地主机缓存

当 Delivery Controller™ 与站点数据库之间的连接失败时，本地主机缓存允许站点中的连接代理操作继续进行。

虚拟 IP 和虚拟环回

Microsoft 虚拟 IP 地址功能为已发布的应用程序提供每个会话唯一的动态分配 IP 地址。Citrix 虚拟环回功能允许您配置依赖于与 localhost 通信的应用程序，以使用 localhost 范围内的唯一虚拟环回地址。

交付控制器

本文包含从站点添加和删除 Controller 时的注意事项和步骤。它还介绍了如何将 Controller 移动到其他区域或站点，以及如何将 VDA 移动到其他站点。

VDA 与 Controller 注册

在 VDA 能够帮助交付应用程序和桌面之前，它必须向 Controller 注册（建立通信）。Controller 地址可以通过多种方式指定，本文对此进行了介绍。至关重要的是，当站点中添加、移动和删除 Controller 时，VDA 必须具有最新的信息。

会话

保持会话活动对于提供最佳用户体验至关重要。多项功能可以优化会话的可靠性，减少不便、停机时间和生产力损失。

- 会话可靠性
- 自动客户端重新连接
- ICA® 保持活动
- 工作区控制
- 会话漫游

在 Studio 中使用搜索

当您想在 Studio 中查看有关计算机、会话、计算机目录、应用程序或交付组的信息时，请使用灵活的搜索功能。

标记

使用标记来标识计算机、应用程序、组和策略等项目。然后，您可以定制某些操作，使其仅应用于具有特定标记的项目。

IPv4/IPv6

Citrix Virtual Apps and Desktops™ 支持纯 IPv4、纯 IPv6 以及使用重叠 IPv4 和 IPv6 网络的双栈部署。本文介绍并阐释了这些部署。它还介绍了控制 IPv4 或 IPv6 使用的 Citrix 策略设置。

用户配置文件

默认情况下，安装 VDA 时会自动安装 Citrix Profile Management。如果您使用此配置文件解决方案，请查阅本文以获取一般信息。有关详细信息，请参阅 Profile Management 文档。

收集 Citrix 诊断工具 (CDF) 跟踪

CDFControl 实用程序是一个事件跟踪控制器或使用者，用于捕获从各种 Citrix 跟踪提供程序显示的 Citrix 诊断工具 (CDF) 跟踪消息。它旨在解决复杂的 Citrix 相关问题、解析筛选器支持以及收集性能数据。

思杰洞察服务

Citrix Insight Services (CIS) 是一个 Citrix 平台，用于实现检测、遥测和业务洞察生成。

思杰探查器

Citrix Scout 收集诊断信息并运行运行状况检查。您可以将结果用于 Citrix Virtual Apps and Desktops 部署中的主动维护。Citrix 通过 Citrix Insight Services 提供对诊断集合的全面自动化分析。您还可以使用 Scout 独立或在 Citrix 支持的指导下解决问题。

应用程序

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中移除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

简介

如果您的部署仅使用交付组（而不使用应用程序组），则将应用程序添加到交付组。如果您也有应用程序组，通常会将应用程序添加到应用程序组。此指导可简化管理。应用程序必须始终属于至少一个交付组或应用程序组。

在“添加应用程序”向导中，您可以选择一个或多个交付组，或一个或多个应用程序组，但不能同时选择两者。尽管您以后可以更改应用程序的组关联（例如，将应用程序从应用程序组移动到交付组），但最佳实践不鼓励增加这种复杂性。将应用程序保留在一种类型的组中。

当您将应用程序与多个组关联时，如果您没有足够的权限在所有这些组中查看应用程序，则可能会出现可见性问题。在这种情况下，请咨询具有更高权限的管理员，或扩展您的范围以包括与应用程序关联的所有组。

如果您向同一用户发布两个同名应用程序（可能来自不同的组），请更改 Web Studio 中的 `Application name (for user)` 属性。否则，用户会在 Citrix Workspace™ 应用程序中看到重复的名称。

您可以在添加应用程序时或之后更改其属性（设置）。您还可以在添加应用程序时或之后更改放置应用程序的应用程序文件夹。

有关详细信息，请参阅：

- 创建交付组
- 创建应用程序组
- 标签

添加应用程序

您可以在创建交付组或应用程序组时添加应用程序。这些过程在创建交付组和创建应用程序组中详细介绍。以下过程介绍了在创建组后如何添加应用程序。

须知：

- 您无法将应用程序添加到远程电脑访问交付组。
- 您无法使用“添加应用程序”向导从交付组或应用程序组中删除应用程序。这是一项单独的操作。

要添加一个或多个应用程序：

1. 在左侧窗格中选择“**应用程序**”，然后在操作栏中选择“**添加应用程序**”。
2. “添加应用程序”向导启动时会显示一个“**简介**”页面，您可以选择在以后启动此向导时不再显示该页面。
3. 该向导将引导您完成“**组**”、“**应用程序**”和“**摘要**”页面。完成每个页面后，单击“**下一步**”，直到到达“**摘要**”页面。

如果要将应用程序添加到单个交付组或应用程序组，请执行以下步骤（步骤 1 的替代方法）：

- **仅将应用程序添加到单个交付组：** 在步骤 1 中，在 Web Studio 左侧窗格中选择“**交付组**”，在中间窗格中选择一个交付组，然后在操作栏中选择“**添加应用程序**”。向导不会显示“**组**”页面。
- **仅将应用程序添加到单个应用程序组：** 在步骤 1 中，在 Web Studio 左侧窗格中选择“**应用程序**”，在中间窗格中选择一个应用程序组，然后在操作栏中应用程序组名称下选择“**添加应用程序**”条目。向导不会显示“**组**”页面。

组页面

此页面列出了站点中的所有交付组。如果您还创建了应用程序组，则此页面会列出应用程序组和交付组。您可以从任一组中进行选择，但不能同时从两组中进行选择。换句话说，您不能同时将应用

程序添加到应用程序组和交付组。通常，如果您正在使用应用程序组，请将应用程序添加到应用程序组，而不是交付组。

添加应用程序时，请选中至少一个交付组（或应用程序组，如果可用）旁边的复选框。每个应用程序都必须始终与至少一个组关联。

应用程序页面

单击“**添加**”以显示应用程序源。

- **从“开始”菜单：** 在所选交付组中的计算机上发现的应用程序。选择此源时，将启动一个新页面，其中包含发现的应用程序列表。选中要添加的应用程序的复选框，然后单击“**确定**”。

  如果您 (1) 选择了没有关联交付组的应用程序组，(2) 选择了具有关联交付组但这些交付组不包含任何计算机的应用程序组，或者 (3) 选择了不包含任何计算机的交付组，则无法选择此源。

- **手动：** 位于交付组中的 VDA 或网络中其他位置的应用程序。选择此源将打开一个新页面，您可以在其中通过以下方式指定要添加的应用程序：

  - 键入可执行文件的路径、工作目录、可选命令行参数以及管理员和用户的显示名称。
  - 从交付组中的 VDA 中选择一个应用程序。为此，请单击“**浏览**”，输入访问 VDA 的凭据，等待连接到 VDA，然后从 VDA 中选择一个应用程序。所选应用程序的属性会自动填充页面上的字段。

- **现有：** 以前添加到站点的应用程序。选择此源时，将启动一个新页面，其中包含发现的应用程序列表。选中要添加的应用程序的复选框，然后单击 **确定**。

  如果站点没有应用程序，则无法选择此源。

- **应用程序包：** App-V、MSIX、MSIX app attach 或 FlexApp 应用程序包中的应用程序。选择此源时，将启动“**从包中添加应用程序**”页面。选择一个应用程序包源，从结果显示中选择要添加的应用程序，然后选择“**确定**”。有关详细信息，请参阅部署和交付应用程序包。

- **应用程序组**：应用程序组。选择此源时，将启动一个新页面，其中包含应用程序组列表。（尽管显示内容也列出了每个组中的应用程序，但您只能选择组，而不能选择单个应用程序。）所选组中的所有当前和未来应用程序都将添加。选中要添加的应用程序组的复选框，然后单击 **确定**。

  如果 (1) 没有应用程序组，或者 (2) 所选交付组不支持应用程序组（例如，具有静态分配计算机的交付组），则无法选择此源。

如表中所示，如果不存在该类型的有效源，则无法选择“**添加**”列表中的某些源。不兼容的源（例如，不能将应用程序组添加到应用程序组）不包括在列表中。已添加到您所选组的应用程序无法选择。

您可以从此页面或以后更改应用程序的属性（设置）。

默认情况下，添加的应用程序放置在名为 `Applications` 的应用程序文件夹中。您可以从此页面或以后更改应用程序。如果您尝试添加应用程序，并且同一文件夹中存在同名应用程序，系统会提示您重命名要添加的应用程序。您可以接受提供的新名称，也可以拒绝，然后重命名应用程序或选择其他文件夹。例如，如果 `app` 已存在于"**应用程序**"文件夹中，并且您尝试将另一个名为 `app` 的应用程序添加到该文件夹，则会提供新名称 `app_1`。

摘要页面

如果您要添加 10 个或更少的应用程序，其名称将列在"**要添加的应用程序**"中。如果您要添加 10 个以上的应用程序，则会指定总数。

查看摘要信息，然后单击**完成**。

更改应用程序的组关联

添加应用程序后，您可以更改应用程序关联的交付组和应用程序组。

您可以将应用程序拖动到其他组。这是使用操作栏中命令的替代方法。

如果应用程序与多个交付组关联（无论是使用应用程序组还是直接关联），则可以使用组优先级来指定评估多个组的顺序。可以根据访问策略、用户列表或智能访问标记等因素将组排除在考虑范围之外，并且从组中选择的特定计算机可能会受到区域首选项、启动就绪状态以及任何标记限制等因素的影响。默认情况下，所有组的优先级均为 0（最高）。如果交付组具有相同的优先级，则选择负载最低的交付组来启动应用程序。在这种情况下，不考虑垂直负载平衡。

应用程序可以与包含可交付应用程序的共享（非专用）计算机的交付组关联。您还可以选择包含仅交付桌面的共享计算机的交付组，前提是 (1) 交付组包含共享计算机且是使用早于 7.9 的 XenDesktop 7.x 版本创建的，并且 (2) 您具有 `Edit delivery group` 权限。提交属性对话框时，交付组类型会自动转换为 `desktops and applications`。

1. 登录 Web Studio，在左侧窗格中选择"**应用程序**"，然后选择该应用程序。
2. 在操作栏中选择 **属性**。
3. 选择 **组** 页面。

    - 要添加组，请单击 **添加** 并选择 **应用程序组** 或 **交付组**。（如果您尚未创建任何应用程序组，则唯一条目是 **交付组**。）然后选择一个或多个可用组。与应用程序不兼容或已与应用程序关联的组无法选择。
    - 要删除组，请选择一个或多个组，然后单击 **删除**。如果删除组关联会导致应用程序不再与任何组关联，则会提醒您该应用程序将被删除。

- 要更改组的优先级，请选择该组，然后单击 **编辑优先级**。选择一个优先级值，然后单击 **确定**。

4. 完成后，单击 **应用** 以应用更改并保持窗口打开，或单击 **确定** 以应用更改并关闭窗口。

复制、启用或禁用、重命名或删除应用程序

以下操作可用：

- **复制：** 您可能希望复制应用程序以创建具有不同参数或属性的不同版本。复制应用程序时，它会自动使用唯一的后缀重命名并放置在原始应用程序旁边。您可能还希望复制应用程序，然后将其添加到不同的组。（复制后，移动应用程序最简单的方法是拖动它。）
- **启用或禁用：** 启用和禁用应用程序与启用和禁用交付组或应用程序组是不同的操作。
- **重命名：** 您一次只能重命名一个应用程序。如果您尝试重命名应用程序，并且同一文件夹或组中存在同名应用程序，系统会提示您指定不同的名称。
- **删除：** 删除应用程序会将其从与之关联的交付组和应用程序组中移除，但不会从最初用于添加应用程序的源中移除。删除应用程序与从交付组或应用程序组中移除应用程序是不同的操作。

要复制、启用、禁用、重命名或删除应用程序，请执行以下操作：

1. 在左侧窗格中选择 **应用程序**。
2. 在中间窗格中选择一个或多个应用程序，然后在操作栏中选择相应的任务。
3. 出现提示时，确认操作。

从交付组中删除应用程序

应用程序必须至少与一个交付组或应用程序组关联（属于）。如果您尝试从交付组中删除某个应用程序，而此操作将删除该应用程序与任何交付组或应用程序组的关联，则系统会通知您，如果继续操作，该应用程序将被删除。如果发生这种情况，并且您希望交付该应用程序，则必须从有效源再次添加它。

1. 在左窗格中选择 **交付组**。
2. 选择一个交付组。在中间下部窗格的 **应用程序** 选项卡上，选择要删除的应用程序。
3. 从操作栏中选择 **删除应用程序**。
4. 确认删除。

从应用程序组中删除应用程序

应用程序必须至少属于一个交付组或应用程序组。如果您尝试从应用程序组中删除某个应用程序，而此操作将导致该应用程序不再属于任何组，则系统会通知您，如果继续操作，该应用程序将被删除。如果发生这种情况，并且您希望交付该应用程序，则必须从有效源再次添加它。

1. 在左窗格中选择 **应用程序**。
2. 在中间窗格中选择应用程序组，然后选择一个或多个应用程序。
3. 在操作栏中选择 **从应用程序组中删除**。
4. 确认删除。

更改应用程序属性

您一次只能更改一个应用程序的属性。

要更改应用程序的属性：

1. 在左侧窗格中选择**应用程序**。
2. 选择一个应用程序，然后在操作栏中选择**编辑应用程序属性**。
3. 选择包含要更改的属性的页面。
4. 完成后，单击**应用**以应用所做的任何更改并保持窗口打开，或者单击**确定**以应用更改并关闭窗口。

在以下列表中，页面显示在括号中。

属性	页面
应用程序在 Citrix Workspace 应用程序中显示的类别/文件夹	交付
命令行参数；请参阅将参数传递给已发布的应用程序	位置
应用程序可用的交付组和应用程序组	组
描述	标识
文件扩展名和文件类型关联：应用程序自动打开哪些扩展名	文件类型关联
图标	交付

属性	页面
StoreFront™ 关键字	标识
限制；请参阅配置应用程序限制	交付
名称：用户和管理员看到的名称	标识
可执行文件路径；请参阅向已发布的应用程序传递参数	位置
用户桌面上的快捷方式：启用或禁用	交付
可见性：限制哪些用户可以在 Citrix Workspace 应用程序中看到该应用程序。不可见的应用程序仍然可以启动。要使其不可用且不可见，请将其添加到其他组。	限制可见性
工作目录	位置

应用程序更改可能要等到当前应用程序用户从其会话注销后才能生效。

配置应用程序限制

配置应用程序限制以帮助管理应用程序使用。例如，您可以使用应用程序限制来管理同时访问应用程序的用户数量。同样，应用程序限制可用于管理资源密集型应用程序的并发实例数量。该限制有助于维持服务器性能并防止服务质量下降。

此功能限制由 Controller 代理的应用程序启动次数（例如，从 Citrix Workspace 应用程序和 StoreFront 启动），而不是通过其他方法启动的正在运行的应用程序的数量。这意味着应用程序限制有助于管理员管理并发使用，但不能在所有场景中提供强制执行。例如，当 Controller 处于中断模式时，无法应用应用程序限制。

默认情况下，同时运行的应用程序实例数量没有限制。有多种应用程序限制设置。您可以配置其中任何一项或所有项。

- 交付组中所有用户并发运行的应用程序实例的最大数量。
- 交付组中每个用户一个应用程序实例。
- 每台计算机并发运行的应用程序实例的最大数量（仅限 PowerShell）。

如果配置了限制，当用户尝试启动超出配置限制的应用程序实例时，将生成错误消息。如果配置了多个限制，则在达到第一个限制时报告错误。

使用应用程序限制的示例：

- **最大并发实例数限制：** 在交付组中，您将应用程序 `Alpha` 的最大并发实例数配置为 15。之后，该交付组中的用户同时运行 15 个该应用程序的实例。如果该交付组中的任何用户现在尝试启动 `Alpha`，则会生成错误消息。`Alpha` 未启动，因为它将超出配置的并发应用程序实例限制 (15)。
- **每个用户一个实例的应用程序限制：** 在另一个交付组中，您为应用程序 `Beta` 启用了每个用户一个实例的选项。用户 Tony 成功启动了应用程序 `Beta`。当天晚些时候，当该应用程序仍在 Tony 的会话中运行时，他尝试启动 `Beta` 的另一个实例。系统会生成错误消息，并且 `Beta` 未启动，因为它将超出每个用户一个实例的限制。
- **最大并发实例数和每个用户一个实例的限制：** 在另一个交付组中，您将最大并发实例数配置为 10，并为应用程序 `Delta` 启用了每个用户一个实例的选项。之后，当该交付组中的 10 个用户各自运行一个 `Delta` 实例时，该交付组中任何其他尝试启动 `Delta` 的用户都将收到错误消息。`Delta` 未启动。如果当前 10 个 `Delta` 用户中的任何一个尝试启动该应用程序的第二个实例，他们将收到错误消息，并且第二个实例将不会启动。
- **每台计算机的最大并发实例数以及使用标记限制：** 应用程序 `Charlie` 具有许可和性能要求，这些要求决定了特定服务器上可以同时运行多少个实例。这些要求还决定了站点中所有服务器上可以同时运行多少个实例。

  每台计算机的应用程序实例限制会影响站点中的任何服务器（而不仅仅是特定交付组中的计算机）。假设您的站点有三台服务器。对于应用程序 `Charlie`，您将每台计算机的应用程序实例限制配置为 2。因此，站点范围内最多允许启动六个应用程序 `Charlie` 实例。（这是三台服务器上每台服务器两个 Charlie 实例的限制。）

  要将应用程序的使用限制为交付组中的特定计算机（除了限制站点中所有计算机上的实例之外）：

  - 为这些计算机使用标记功能。
  - 为该应用程序配置每台计算机的最大实例数限制。

如果应用程序通过 Controller 代理以外的方法启动（例如，当 Controller 处于中断模式时），并且超出了配置的限制，则用户无法启动更多实例，直到他们关闭足够的实例以不再超出限制。超出限制的实例不会被强制关闭。它们将被允许继续运行，直到其用户关闭它们。

如果您禁用会话漫游，则禁用每个用户一个实例的应用程序限制。如果您启用每个用户一个实例的应用程序限制，请不要配置允许在新设备上创建新会话的两个值中的任何一个。有关漫游的信息，请参阅会话。

要配置每个交付组的最大实例数限制和每个用户一个实例的限制：

1. 在左侧窗格中选择 **应用程序**，然后选择一个应用程序。
2. 在操作栏中选择 **编辑应用程序属性**。
3. 在 **交付** 页面上，选择以下选项之一。
   - **允许无限制使用应用程序**。同时运行的实例数量没有限制。这是默认设置。
   - **为应用程序设置限制**。有两种限制类型；指定其中一种或两种。
     - 指定每台计算机可同时运行的最大实例数
     - 将应用程序限制为每个用户一个实例
4. 单击 **确定** 以应用更改并关闭对话框，或单击 **应用** 以应用更改并保持对话框打开。

要配置每台计算机的最大实例数限制（仅限 PowerShell）：

- 在 PowerShell 中（对于 Citrix Cloud™ 部署使用远程 PowerShell SDK，对于本地部署使用 PowerShell SDK），输入带有 `MaxPerMachineInstances` 参数的相应 `BrokerApplication` cmdlet。
- 有关指导，请使用 `Get-Help` cmdlet。例如：

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

向已发布的应用程序传递参数

使用应用程序属性的“**位置**”页面输入命令行并向已发布的应用程序传递参数。

将已发布的应用程序与文件类型关联时，符号 `"%*"`（用双引号括起来的百分号和星号）将附加到应用程序命令行的末尾。这些符号用作传递给用户设备的参数的占位符。

如果已发布的应用程序未按预期启动，请验证其命令行是否包含正确的符号。默认情况下，当附加符号 `"%*"` 时，将验证用户设备提供的参数。对于使用用户设备提供的自定义参数的已发布应用程序，符号 `"%**"` 将附加到命令行以绕过命令行验证。如果应用程序的命令行中没有这些符号，请手动添加它们。

如果可执行文件的路径包含带空格的目录名（例如 `"C:\Program Files"`），请用双引号将应用程序的命令行括起来，以指示空格属于命令行。为此，请在路径周围添加双引号，并在 `%*` 符号周围添加另一组双引号。请务必在路径的结束引号和 `%*` 符号的开始引号之间包含一个空格。

例如，已发布的应用程序 Windows Media Player 的命令行是：

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **注意：**
>
> 用于启动已发布的应用程序的命令行中的最大字符数（包括参数）为 203。

排查已发布的应用程序的会话注销问题

发布应用程序时，仅指定已发布的应用程序的主可执行文件。但是，某些应用程序可能会生成在后台运行的额外（子）进程，并且当主已发布的应用程序关闭时，这些进程不会被相应的主可执行文件关闭。还可能从执行的脚本或特定的注册表项（例如 `Run` 和 `RunOnceKey`）创建额外进程。这些应用程序可能会阻止正常注销，导致会话残留或挂起，并可能导致会话无法关闭且用户无法注销。

在这种情况下，您需要使用 Citrix Director 重置或退出这些会话。

为了帮助识别和排查会话未正确注销的问题，Citrix 提供了三个注册表项。识别和排查由于这些问题导致会话未正确注销是一个三步过程：

1. 识别哪些会话的已发布应用程序正在阻止正常注销
2. 识别这些已发布的应用程序是否生成任何额外（子）进程
3. 将这些进程添加到指定的注册表项以防止它们阻止注销

步骤 2：识别这些已发布的应用程序是否生成任何其他（子）进程

确定某个已发布的应用程序会阻止正常注销后，下一步是确定此应用程序在运行时是否会生成其他进程。

您可以阅读 `HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` 以确定在关闭已发布的应用程序时是否有任何进程正在阻止正常注销。

在以下示例中，密钥 `LogoffCheckerBlockingProcess` 包含以下条目：

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

这些进程阻止了正常注销。

> **注意：**
>
> 将 替换为要检查的会话的正确会话 ID。

步骤 3：将这些进程添加到指定的注册表项以防止它们阻止注销

您可以将这些进程添加到以下注册表项，以防止它们在将来的会话中阻止注销：

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules

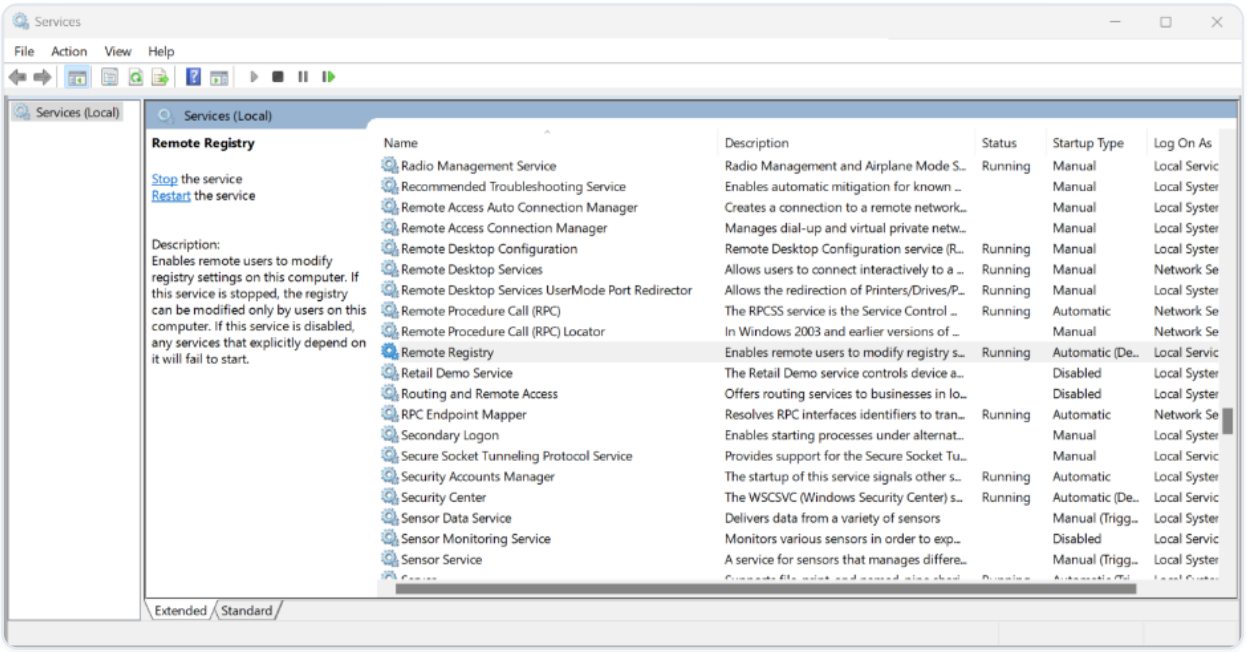
Type:REG_SZ

String:MyAppName.exe
```

有关 `LogoffCheckSysModules` 的更多信息，请参阅从已发布的应用程序正常注销使会话处于活动状态。

分步故障排除指南

1. 在受测 VDA 下启动远程注册表服务：
    a. 在“控制面板”中，选择“**管理工具 > 服务**”。
    b. 右键单击“**远程注册表服务**”，然后选择“**属性**”。
    c. 在“**启动类型**”下，从下拉菜单中选择“**自动**”。



2. 在测试 VDA 上关闭 Windows 防火墙，或创建入站防火墙规则以启用端口 455：

   a. 在“控制面板”中，选择 **Windows Defender 防火墙 > 高级设置**。

   b. 右键单击“**入站规则**”并选择“**新建规则**”。

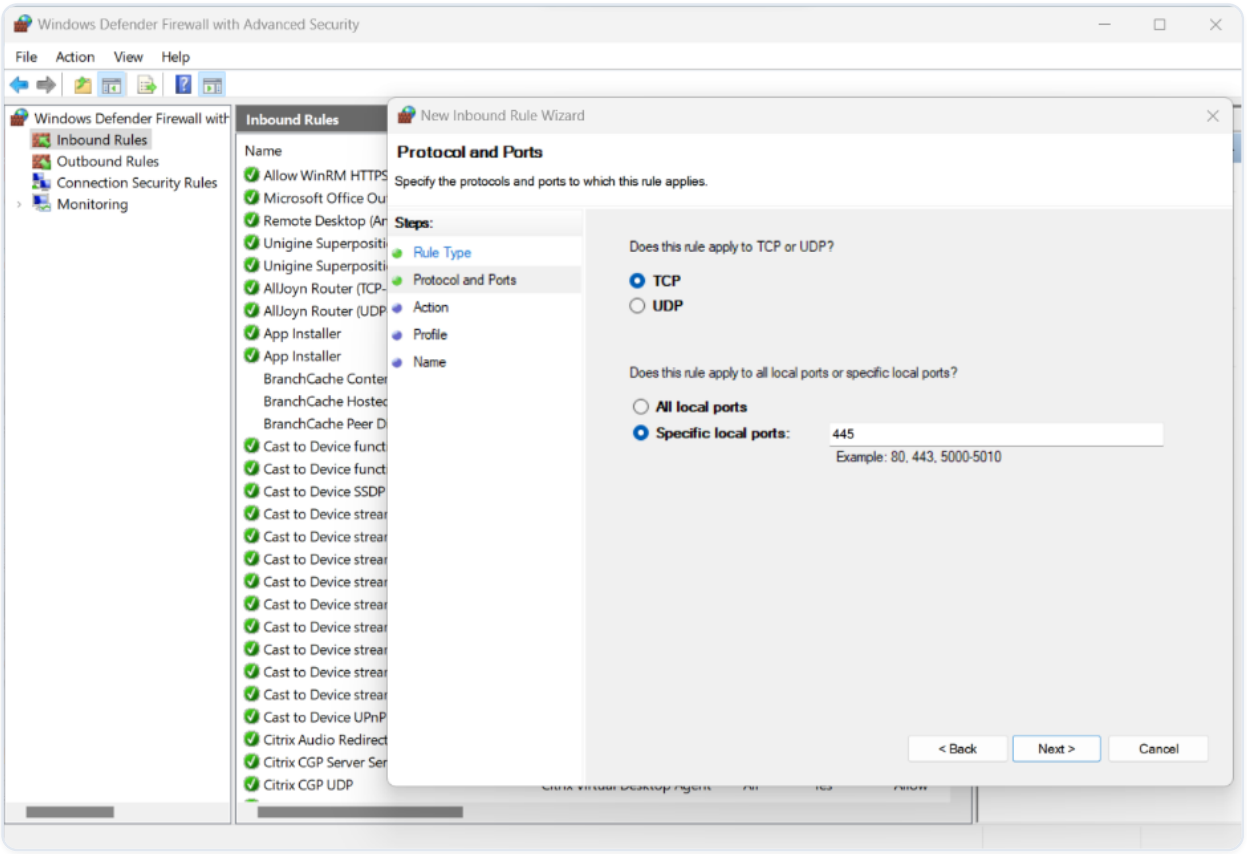
   c. 在“**新建入站规则向导**”中，选择“**端口**”。

   d. 在“**协议和端口**”页面上，选择“**TCP 和特定本地端口**”。输入 `445` 作为本地端口。

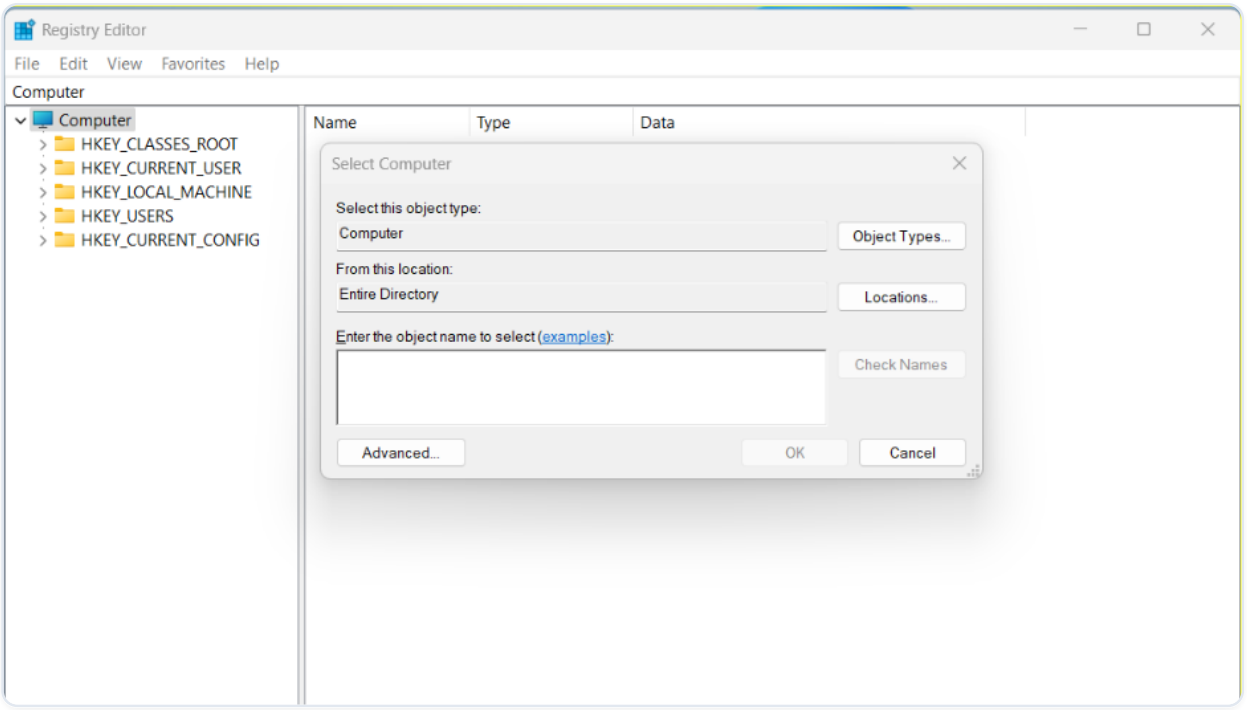
   e. 在“**操作**”页面上，选择“**允许连接**”。

   f. 选择要应用新入站规则的防火墙配置文件。

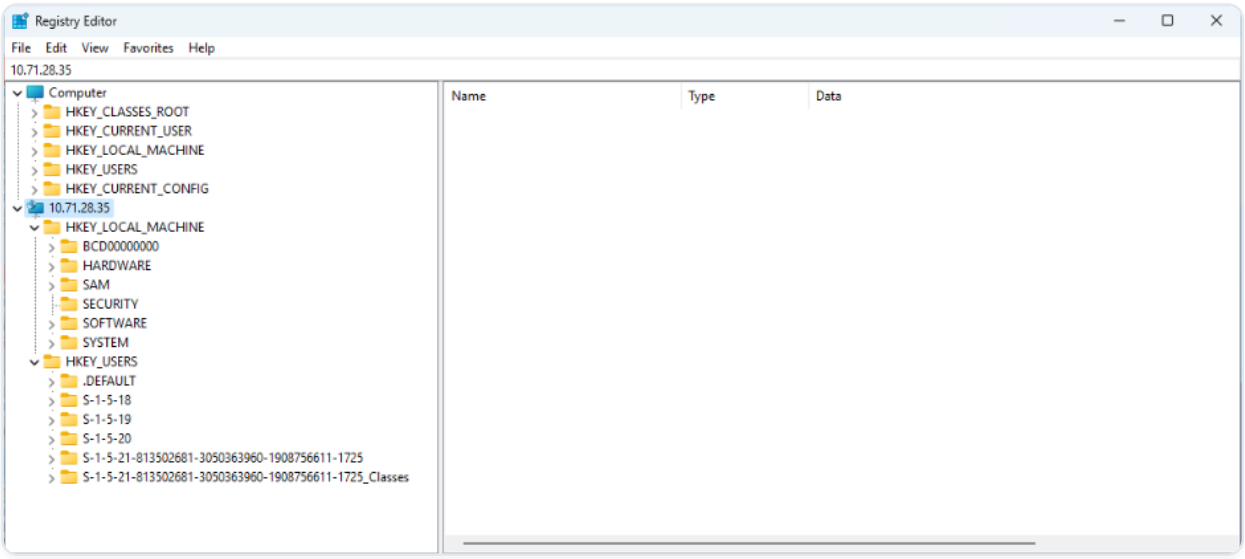
   g. 命名防火墙规则，然后选择“**完成**”以退出“**新建入站规则向导**”。



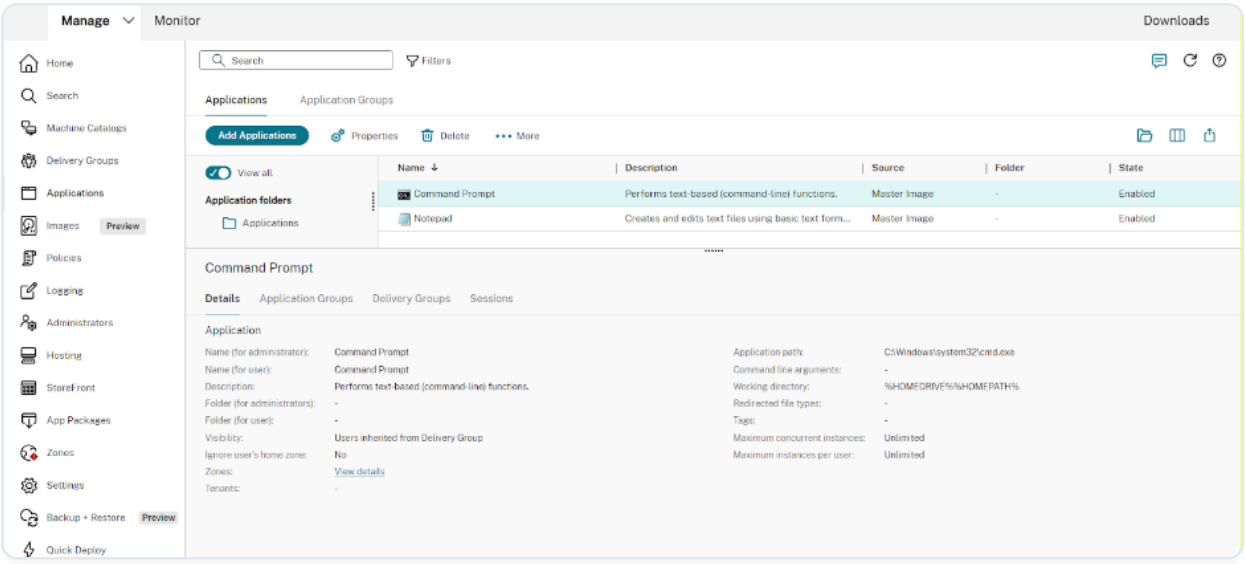
3. 从同一域中的另一台 VM（可以是 DC、DDC 或另一台 VDA）运行 `Regedit` 并连接到远程注册表。



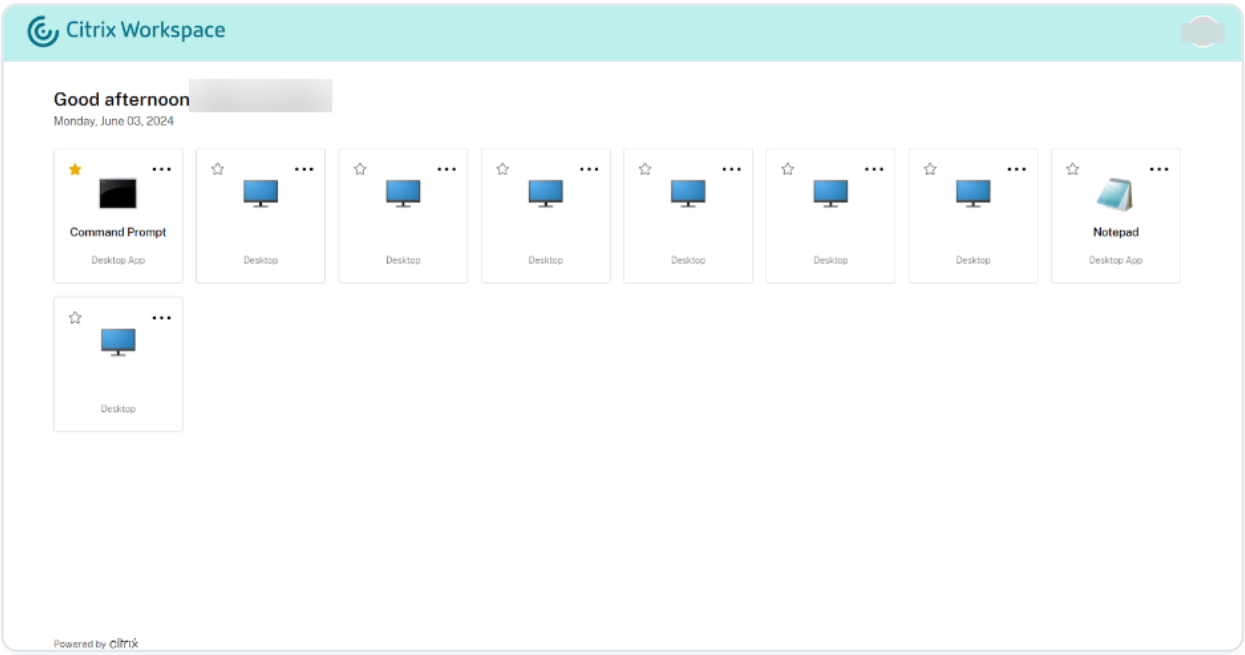
4. 输入测试 VDA 的 IP 地址，然后单击“**确定**”。 `regedit` 树必须显示测试 VDA 的分支。



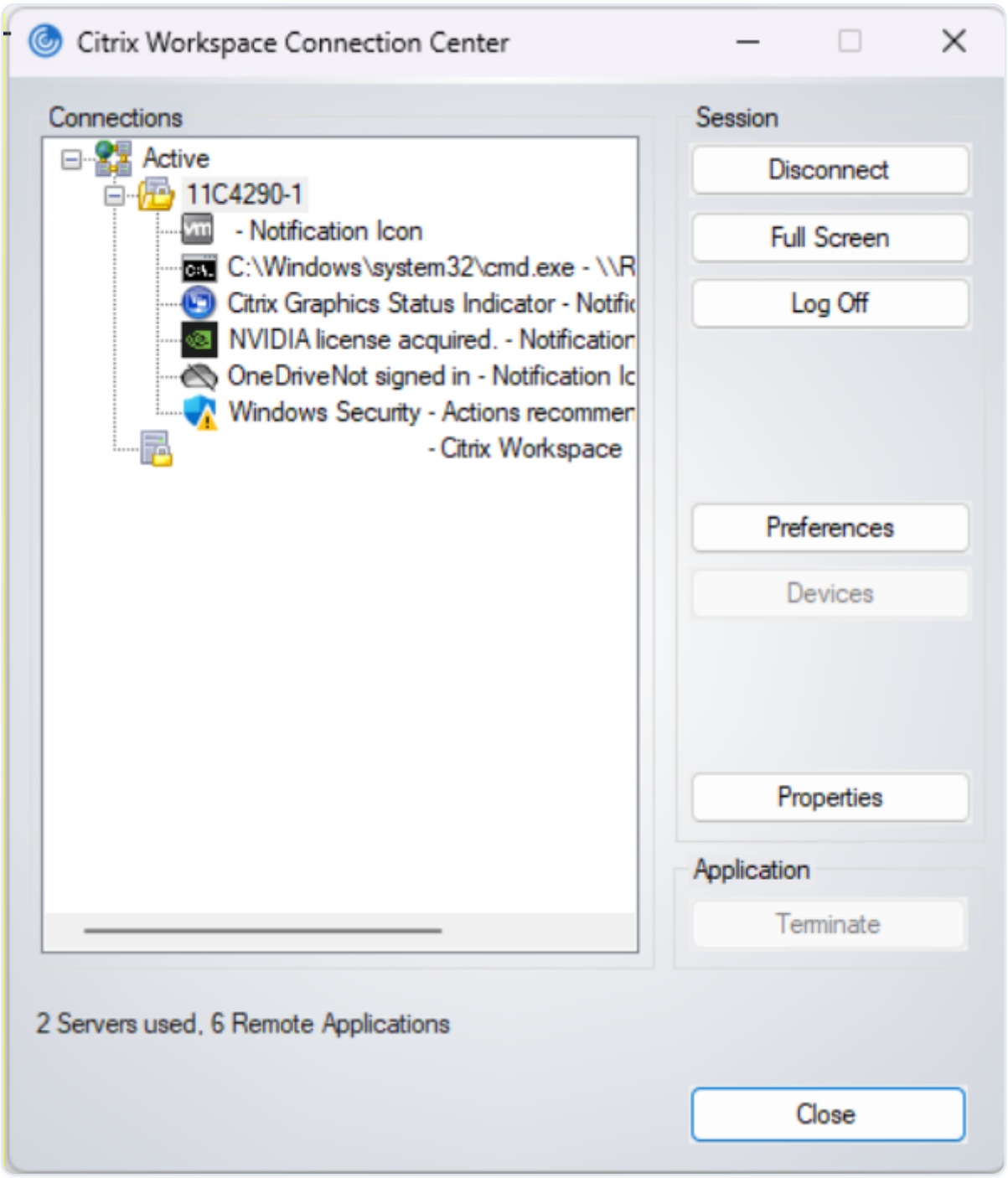
5. 打开“**命令提示符**”已发布的应用程序。



在 Citrix Workspace 上显示**命令提示符**应用程序。



6. 在客户端上打开**连接中心**。这用于在关闭已打开的无缝应用程序后，监控会话何时注销。我们可以从下图中看到，命令提示符进程 `c:\Windows\system32\cmd.exe` 在远程 VDI 上处于活动状态。



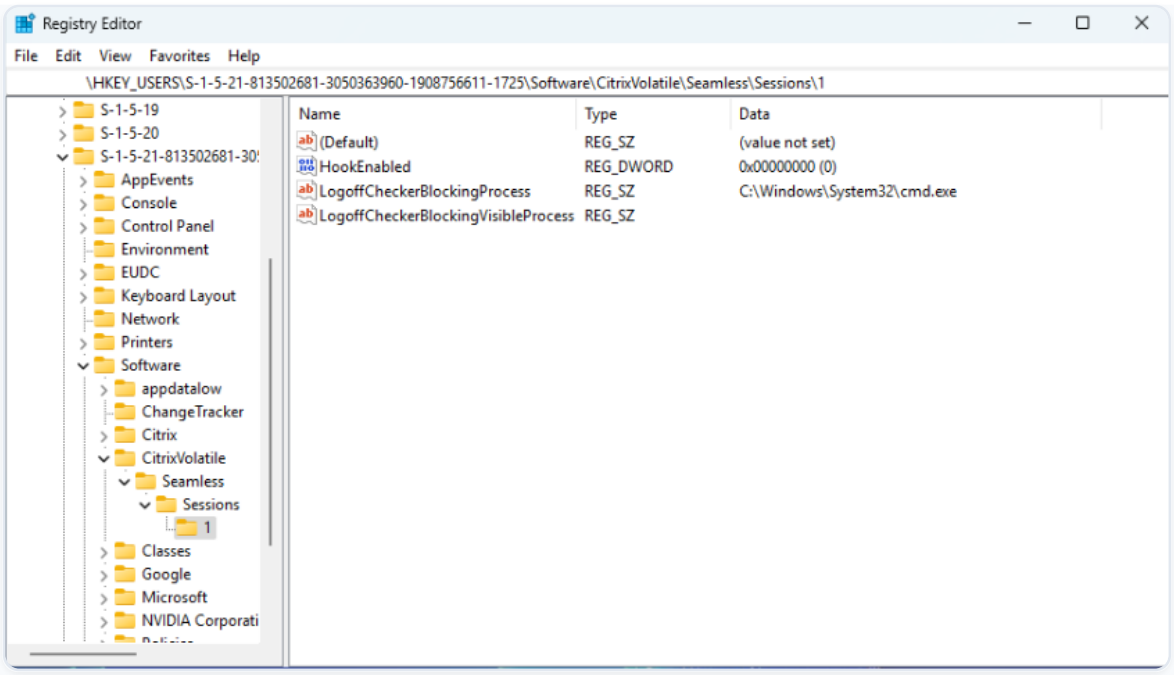
7. 从运行 **regedit** 的 VDA，转到以下远程 IP 位置： `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

> **注意：**

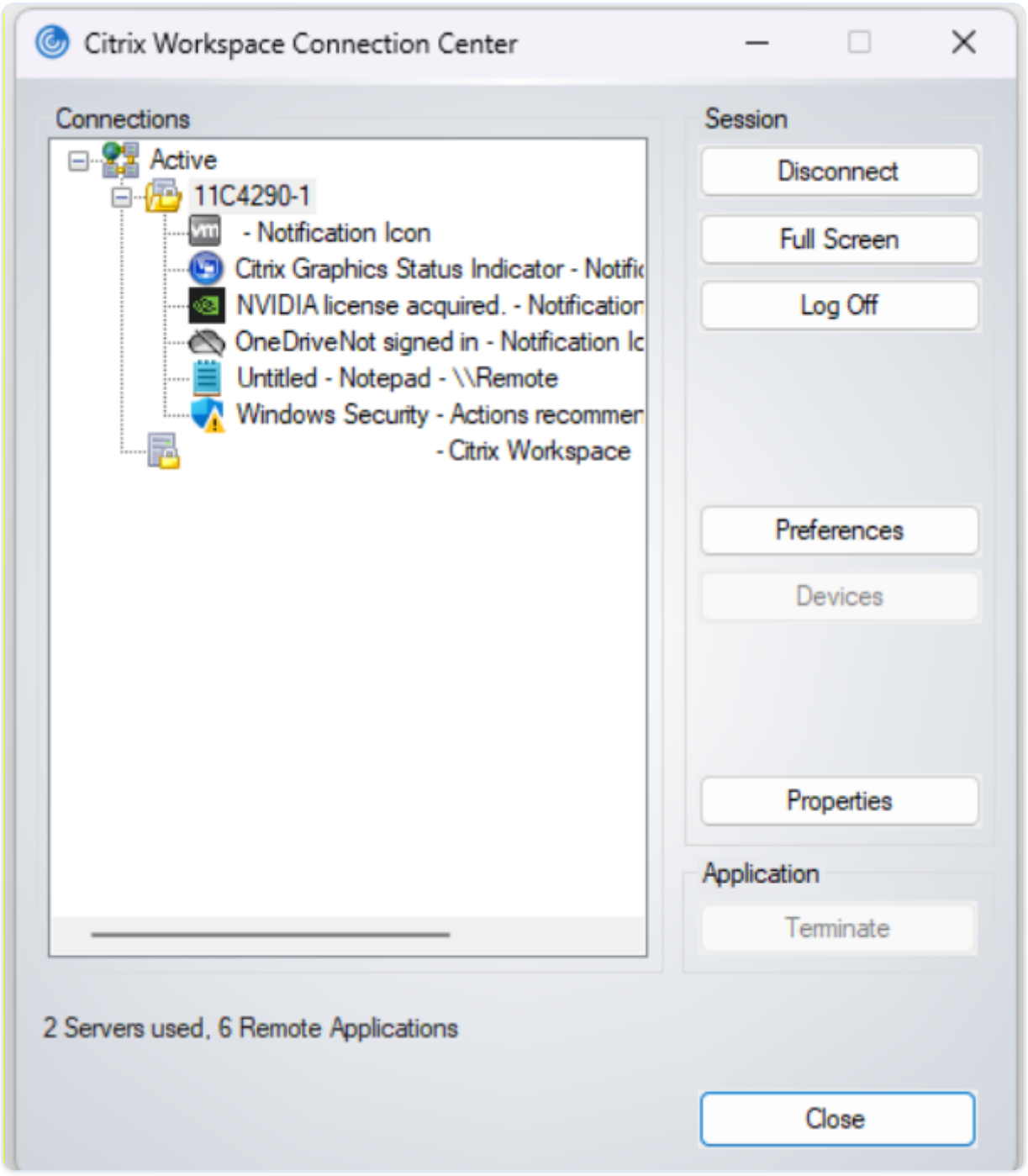
> 每次打开新会话时，此路径都会更改。

8. 这里有两个要读取的键（不要在此处更改它们）：**LogoffCheckBlockingProcess** 和 **LogoffCheckerBlockingVisibleProcess**。这些键显示任何阻止注销的程序。第一个必须显示 `C:\Windows\System32\cmd.exe`，因为它已打开且尚未关闭。

> **注意：**
>
> **LogoffCheckBlockingProcess** 和 **LogoffCheckerBlockingVisibleProcess** 不得手动编辑。手动编辑这些注册表值可能会导致会话不稳定。

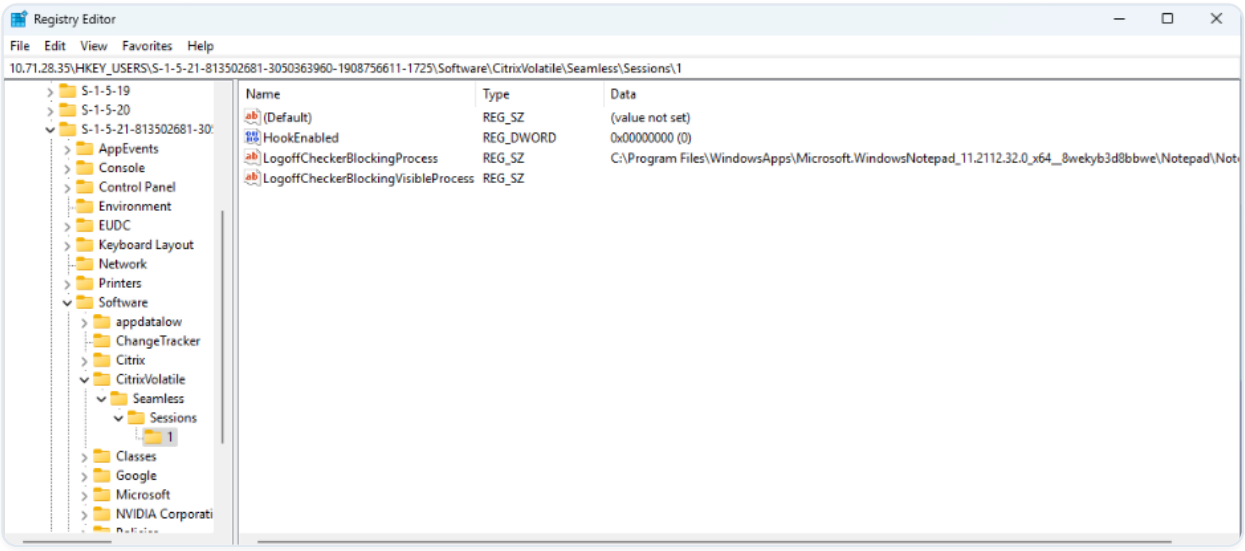


9. 单击右上角的 **X** 以退出 **Seamless CMD**。
10. 检查连接中心以查看会话是否关闭。关闭可能需要长达 30 秒。如果会话关闭，则没有应用程序或进程阻止正常注销。



11. 如果会话未关闭，请按 F5 刷新 **regedit** 输出。
12. 再次检查 **LogoffCheckBlockingProcess** 和 **LogoffCheckerBlockingVisibleProcess** 的内容。CMD 不应再存在，但应该有另一个列出的进程。任何当前阻止会话注销的进程都必须在此处显示。

    在这种情况下，在命令提示符关闭之前，**Notepad.exe** 从已发布的命令提示符中打开，并且此远程记事本进程正在阻止正常注销。



13. 记下此可执行文件的路径以及它出现在哪个键中，然后将其输入到远程树下的以下注册表项中：

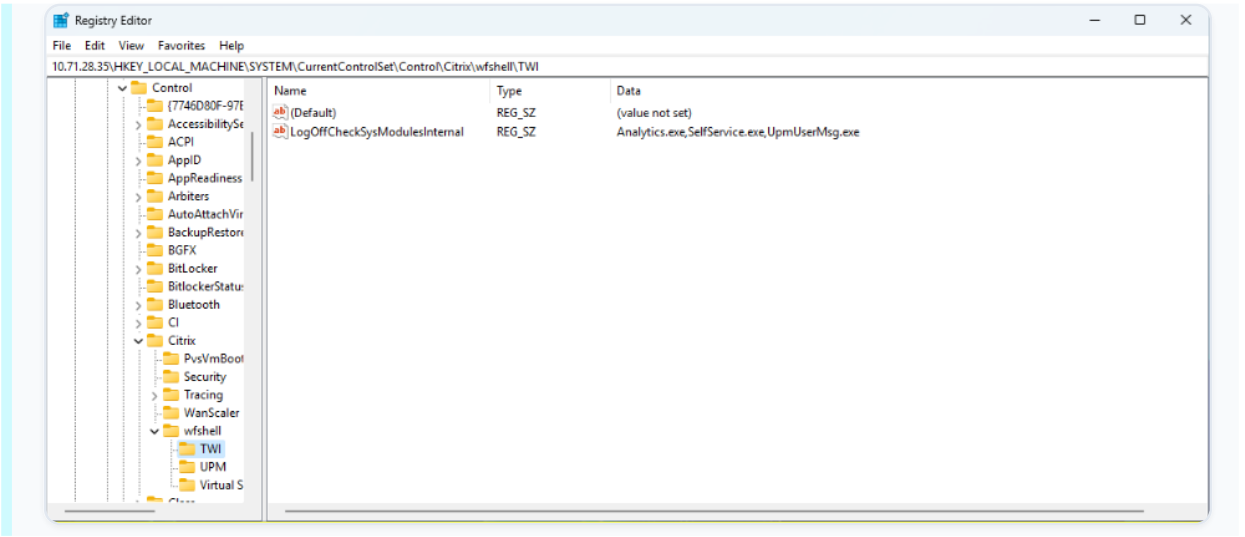
    - 如果它出现在 **LogoffCheckBlockingProcess** 中：

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - 如果它出现在 **LogoffCheckerBlockingVisibleProcess** 中：

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **注意：**
>
> 如果该键中已有一个或多个条目，请在末尾添加一个逗号，并在逗号后放置新条目。



14. 从客户端上的连接中心注销会话，然后重新打开远程应用程序。
15. 重复步骤 9-16，直到在关闭远程应用程序后的 30 秒内自动注销会话。

> **注意：**

故障排除后，如果需要，请恢复临时防火墙更改以允许远程注册表访问。

如何修改 LogonUI 以在打开已发布的应用程序时全尺寸查看 Windows 免责声明消息

LogonUI 窗口缩放已改进，适用于未发生身份验证直通的场景。**LogonUI** 窗口根据所使用的显示器分辨率和 DPI 设置进行缩放，这可确保完整的 **LogonUI** 窗口可见，而不会出现任何剪裁。

窗口的像素大小也可以在注册表中手动设置。

1. 使用 **运行** 命令上的 `regedit` 打开 **注册表编辑器**。
2. 转到 `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`。
3. 创建两个新的 DWORD 键：**LogonUIWidth** 和 **LogonUIHeight**。
4. 将键的值设置为 **LogonUI** 窗口所需的像素宽度和高度。

   手动设置 **LogonUI** 窗口大小时，将禁用自动缩放。

注意：

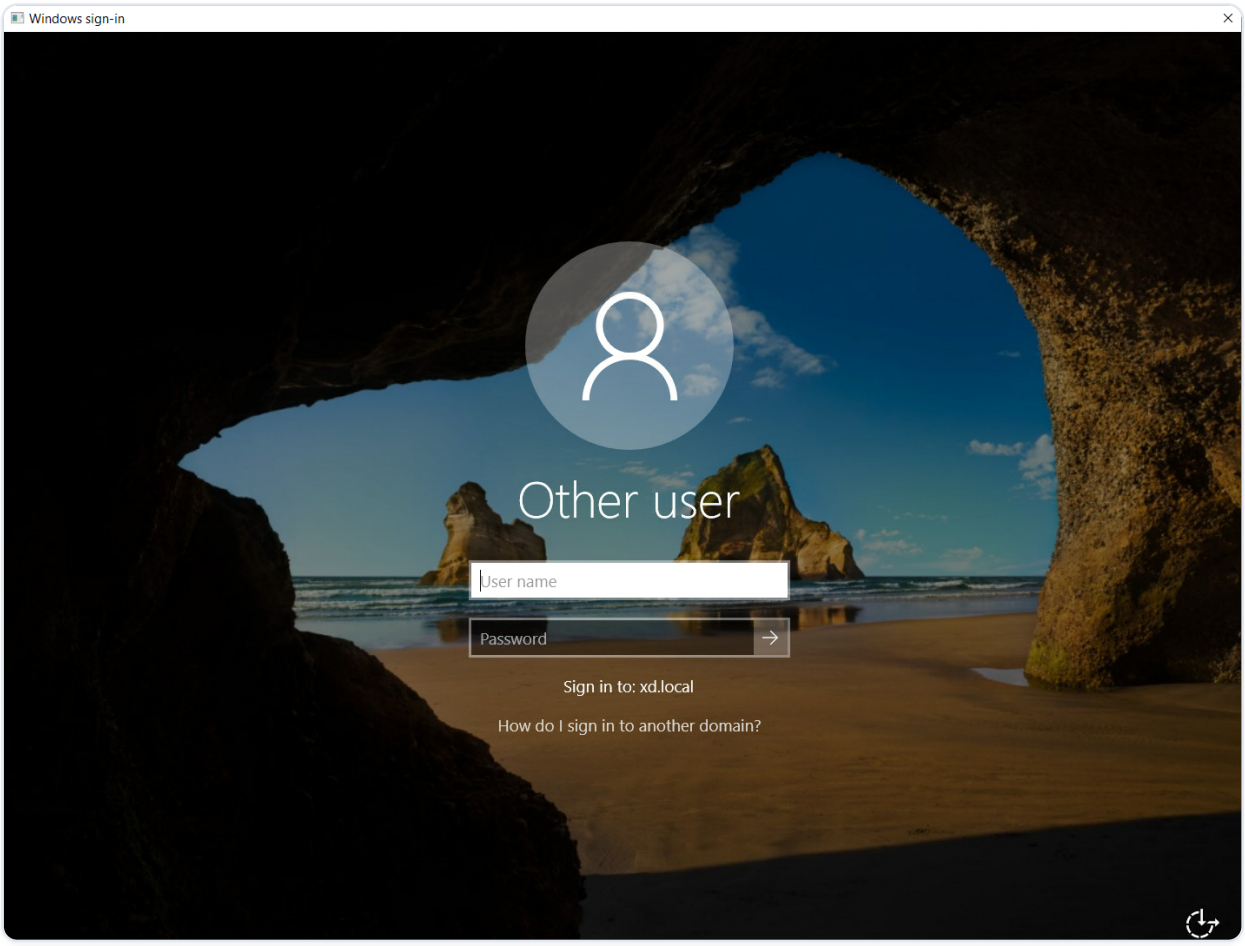
这些注册表路径已从 2407 及更高版本更改。旧的注册表值将被忽略并弃用。

默认情况下，**LogonUI** 窗口包含一个带有关闭按钮的标题栏，最终用户可以在需要时断开会话。

禁用标题栏

您可以使用以下注册表项禁用 **LogonUI** 窗口中的标题栏：

1. 在“**运行**”命令上使用 `regedit` 打开注册表编辑器。
2. 转到 `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`。
3. 创建新的 DWORD 键：**LogonUICaption**，并将该键的值设置为 `0`。



管理应用程序文件夹

默认情况下，您添加到交付组的新应用程序会放置在名为“**应用程序**”的文件夹中。您可以在创建交付组、添加应用程序或之后指定不同的文件夹。

须知：

- 您无法重命名或删除“应用程序”文件夹，但可以将其包含的所有应用程序移动到您创建的其他文件夹中。
- 文件夹名称可以包含 1–64 个字符。允许使用空格。
- 文件夹最多可以嵌套五层。
- 文件夹不必包含应用程序。允许空文件夹。
- 文件夹在 Web Studio 中按字母顺序排列，除非您移动它们或在创建时指定不同的位置。
- 只要每个文件夹都有不同的父文件夹，您就可以拥有多个同名文件夹。同样，只要每个应用程序位于不同的文件夹中，您就可以拥有多个同名应用程序。
- 您必须拥有 `View Applications` 权限才能查看文件夹中的应用程序，并且必须拥有 `Edit Application Properties` 权限才能删除、重命名或删除包含应用程序的文件夹中的所有应用程序。

- 以下大多数过程都要求使用 Web Studio 中的操作栏执行操作。或者，您可以使用右键单击菜单或拖动项目。例如，如果您在不打算的位置创建或移动了文件夹，则可以将其拖放到正确的位置。
- Web Studio 中的所有节点（例如，**计算机目录**、**交付组**、**应用程序**和**应用程序组**）在后端共享相同的文件夹树。为避免重命名或移动文件夹时出现名称冲突，请在不同节点之间为一级文件夹使用唯一的名称。

  如果您使用 `New-BrokerAdminFolder` SDK cmdlet 创建文件夹并希望它显示在**应用程序**节点下，则必须使用 `Set-BrokerAdminFolderMetadata` cmdlet 添加 `ContainsApplications` 元数据。

  示例：

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplications -Value true
  ```

要管理应用程序文件夹，请在左侧窗格中选择**应用程序**。请参阅以下列表以获取指导。

- **要查看所有文件夹（不包括嵌套文件夹）：** 单击文件夹列表上方的**显示所有**。
- **要在最高级别（非嵌套）创建文件夹：** 选择**应用程序**文件夹。要将新文件夹放置在**应用程序**以外的现有文件夹下，请选择该文件夹。然后，在操作栏中选择**创建文件夹**。输入名称。
- **要移动文件夹：** 选择该文件夹，然后在操作栏中选择**移动文件夹**。一次只能移动一个文件夹，除非该文件夹包含嵌套文件夹。（移动文件夹最简单的方法是拖动它。）
- **要重命名文件夹：** 选择该文件夹，然后在操作栏中选择**重命名文件夹**。输入名称。
- **要删除文件夹：** 选择该文件夹，然后在操作栏中选择**删除文件夹**。当您删除包含应用程序和其他文件夹的文件夹时，这些对象也会被删除。删除应用程序会从交付组中删除应用程序分配。它不会从计算机中删除应用程序。
- **要将应用程序移动到文件夹中：** 选择一个或多个应用程序。然后，在操作栏中选择**移动应用程序**。选择该文件夹。

在创建交付组或应用程序组时，您还可以在**应用程序**页面上将要添加的应用程序放置在文件夹中。默认情况下，添加的应用程序会放入**应用程序**文件夹中。单击**更改**以选择或创建文件夹。

控制已发布的桌面上的应用程序本地启动

当用户从已发布的桌面中启动已发布的应用程序时，您可以控制该应用程序是在该桌面会话中启动还是作为已发布的应用程序启动。Citrix Workspace 应用程序会在 VDA 上的 Windows 注册表中搜索应用程序的安装路径，如果存在，则启动应用程序的本地实例。否则，将启动应用程序的托管实

例。如果您启动未安装在 VDA 上的应用程序，则会启动托管应用程序。有关详细信息，请参阅 vPrefer 启动。

在 PowerShell 中（在 Citrix Cloud 部署中使用远程 PowerShell SDK 或在本地部署中使用 PowerShell SDK），您可以更改此操作。

在 `New-Broker` 应用程序或 `Set-BrokerApplication` cmdlet 中，使用 `LocalLaunchDisabled` 选项。例如：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

默认情况下，此选项的值为 false (`-LocalLaunchDisabled $false`)。从已发布的桌面中启动已发布的应用程序时，该应用程序将在该桌面会话中启动。

如果将此选项的值设置为 true (`-LocalLaunchDisabled $true`)，则会启动已发布的应用程序。这将从已发布的桌面（使用适用于 Windows 的 Citrix Workspace 应用程序）为已发布的应用程序创建一个单独的附加会话。

要求和限制：

- 应用程序的 `ApplicationType` 值必须为 `HostedOnDesktop`。
- 此选项仅通过相应的 PowerShell SDK 提供。目前在 Web Studio 图形界面中不可用。
- 此选项最低要求：StoreFront 3.14、适用于 Windows 的 Citrix Receiver 4.11 和 Delivery Controller 7.17。

应用程序包

应用程序包是 Citrix® 管理的预配置应用程序部署。它们允许应用程序虚拟化，这意味着应用程序独立于用户设备的操作系统和界面运行。

应用程序包简化了应用程序管理，减少了 IT 开销，并确保应用程序在其整个生命周期中安全且功能正常。

Citrix 支持以下打包技术，用于向用户交付应用程序：

- App-V 应用程序
- MSIX 和 MSIX app attach 应用程序
- FlexApp 应用程序
- Elastic App 应用程序
- Cloudpaging 应用程序

本文将引导您了解如何在 Citrix Virtual Apps and Desktops™ 环境中部署和交付这些打包的应用程序。

> **注意：**
>
> - 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。
> - 我们不建议交替使用 Web Studio 和 Citrix Studio 来部署和交付应用程序包。它们各自使用不同的机制，这可能导致差异，例如 App-V 服务器信息在一个中显示正确而在另一个中不显示。此外，请注意 Citrix Studio 仅支持 App-V。

App-V 应用程序

应用程序虚拟化 (App-V) 是一种 Microsoft 技术，允许流式传输和访问应用程序，而无需在最终用户设备上安装。Citrix Virtual Apps and Desktops 可以使用 App-V 交付应用程序，提供一种集中高效的方式来管理各种客户端计算机上的应用程序。

有关交付 App-V 打包应用程序时所涉及的组件和概念的更多信息，请参阅 Microsoft 文档：适用于 Windows 客户端的应用程序虚拟化 (App-V) 概述。

重要术语

- **管理服务器**：提供一个集中式控制台来管理 App-V 基础结构，并将虚拟应用程序交付给 App-V 桌面客户端和远程桌面服务客户端。App-V 管理服务器负责身份验证、请求以及提供管理员所需的安全、计量、监控和数据收集功能。该服务器使用 Active Directory 和支持工具来管理用户和应用程序。
- **发布服务器**：为 App-V 客户端提供特定用户的应用程序，并托管用于流式传输的虚拟应用程序包。它从管理服务器获取包。
- **动态配置文件**：App-V 包可以使用动态配置文件进行自定义，这些文件应用于包后，可用于更改其特性。例如，您可以使用它们来定义额外的应用程序快捷方式和行为。有关详细信息，请参阅动态配置文件

动态配置文件

Citrix App-V 支持两种类型的动态配置文件。文件设置在应用程序启动时应用：

- **部署配置文件**为所有用户提供机器范围的配置。这些文件应命名为 `<packageFileName>_DeploymentConfig.xml` 并与它们所应用的 App-V 包位于同一文件夹中。单管理员和双管理员管理都支持这些文件。
- **用户配置文件**提供用户特定的配置，支持对包进行按用户自定义。单管理员支持以下列格式命名的用户配置文件：`<packageFileName>_[UserSID | Username | GroupSID | GroupName_]UserConfig.xml`，并位于它们所应用的 App-V 包的同一文件夹中。

  当特定包存在多个用户配置文件时，它们按以下优先级应用：

  a. 用户 SID

  b. 用户名

  c. AD 组 SID（第一个找到的获胜）

  d. AD 组名称（第一个找到的获胜）

  e. 默认值

  例如：

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml

MyAppVPackage_joeblogs_UserConfig.xml

MyAppVPackage_S-1-5-32-547_UserConfig.xml

MyAppVPackage_Power Users_UserConfig.xml

MyAppVPackage_UserConfig.xml
```

> **注意：**
>
> 文件名的用户特定部分也可以选择出现在末尾（例如 `MyAppVPackage_UserConfig_joeblogs.xml`）。

> **重要提示：**

> 当存在打开了包中应用程序的用户会话时，您无法应用对动态部署配置的更改。如果其他用户（但不是当前用户）打开了包中的应用程序，则可以应用对动态用户配置文件进行的更改。

动态配置文件位置

在单一管理员管理中，Citrix App-V 组件仅处理动态配置文件，这些文件与其 App-V 包位于同一文件夹中。

当启动包中的应用程序时，对相应动态配置文件的任何更改都将重新应用。如果您的动态配置文件与其包位于不同的位置，请使用映射文件将包映射到其部署配置文件。

要创建映射文件：

1. 打开一个新文本文件。
2. 对于每个动态配置文件，添加一行，使用 `<PackageGuid> : path` 格式指定包的路径。

   例如：

   ```
   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
   ```

3. 将文件另存为 `ctxAppVDynamicConfigurations.cfg`，并将其放在与包相同的文件夹中。

每次启动包中的应用程序时，都会在与 App-V 包相同的 UNC 共享上向上递归搜索整个目录层次结构以查找此文件。

方法

您可以使用以下方法交付和管理 App-V 包：

- **双管理员**：在此方法中，Citrix Virtual Apps and Desktops 和 App-V 服务器协同工作以交付和管理软件包。此方法要求 Citrix Virtual Apps and Desktops 定期刷新 App-V 服务器状态的快照视图。它会产生硬件、基础架构和管理开销。Citrix Virtual Apps and Desktops 和 App-V 服务器必须保持同步，尤其是用户权限。

  此方法最适用于紧密耦合的 App-V 和 Citrix 部署。在此方法中：

  - **App-V 管理服务器**处理动态配置文件
  - **应用程序包交付组件**安装在 VDA 计算机上：管理应用程序启动所需的相应发布服务器的注册。

  这可确保发布服务器在适当的时间为用户同步。发布服务器使用其配置的设置来维护应用程序包生命周期的其他方面（例如登录时刷新和连接组）。

- **单一管理员**：应用程序包存储在网络共享上。Citrix Virtual Apps and Desktops 独立交付和管理软件包。

  此方法可减少开销，因为部署中不需要 App-V 服务器和数据库基础结构。

  在此方法中，您将 App-V 包存储在网络共享上，并将其元数据从该位置上传到您的环境。然后，安装在 VDA 计算机上的应用程序包交付组件按如下方式管理和交付应用程序：

  - 当应用程序启动时，处理部署配置文件和用户配置文件。
  - 管理主机上包生命周期的所有方面。

> **注意：**
>
> - 您可以同时使用一种或两种管理方法。换句话说，当您将应用程序添加到交付组时，这些应用程序可以来自 App-V 服务器或网络共享上的 App-V 包。
> - 如果您同时使用两种管理方法，并且 App-V 包在两个位置都有动态配置文件，则将使用 App-V 服务器中的文件（双重管理）。
> - 在 Web Studio 导航窗格中选择“应用程序包”时，显示屏会显示包名称和类型。“**包类型**”列指示用于交付包的技术以及它们在“**应用程序库**”中的引用位置。选择包时，详细信息窗格会列出包中的应用程序和快捷方式。

MSIX 和 MSIX 应用附加应用程序

MSIX 是一种 Windows 应用程序包格式，可为所有 Windows 应用程序提供现代打包体验。MSIX 适用于各种 Windows 应用程序类型，包括 Win32、.NET 和 UWP 应用程序。

MSIX 应用附加利用预先扩展到虚拟硬盘上的 MSIX 包，这些包可以根据需要挂载到目标计算机，而不是流式传输包内容。它可以缩短部署时间、减少网络流量并降低目标计算机上的 IOPS，但需要额外的工作来创建和维护应用附加磁盘。

Citrix Virtual Apps and Desktops 通过安装在 VDA 计算机上的“**应用程序包交付组件**”向用户交付 MSIX 和 MSIX app attach 应用程序。此组件管理主机上包生命周期的所有方面。

有关 MSIX 和 MSIX app attach 的更多信息，请参阅 Microsoft 文档：MSIX documentation 和 App Attach in Azure Virtual Desktop。

> **注意：**

- 我们支持桌面和服务器 VDA 上的本机 MSIX 包，以及仅在桌面 VDA 上支持 `.vhd`、`.vhdx` 和 `.cim` 磁盘映像格式的 MSIX app attach。
- Microsoft 不为 Server 2019 提供 AppAttach 实现。虽然 AppAttach 存在于 Server 2022 和 2025 中，但 Microsoft 不支持这些版本上的 AppAttach。因此，我们也不支持 Server 2022 和 2025 上的 AppAttach。
- 在 Windows Server 2019 上启用旁加载。
- 确保 VDA 信任用于签署软件包的证书。

FlexApp 应用程序

FlexApp 是 Liquidware 开发的一种应用程序分层解决方案，它可以在不通过传统应用程序安装过程修改底层基础映像的情况下，将任何应用程序附加到 Windows 会话。

FlexApp One 应用程序封装在一个可共享的单个文件中，使其无需在 Windows 会话上额外添加应用程序层即可运行。用户可以通过单击容器文件启动应用程序，这会快速将一个或多个应用程序集成到他们的 Windows 工作区中。

Citrix 通过安装在 VDA 计算机上的 App Packages Delivery Component 和 FlexApp 交付代理向用户交付 FlexApp 应用程序。这两个组件管理主机上软件包生命周期的所有方面。

Elastic App 应用程序

Elastic App 技术是 Citrix App Layering 的一项功能，它允许您在登录时动态地将应用程序层分配给用户，而不是将其安装到基础映像中。借助 Elastic App 技术，应用程序会跟随用户在不同的虚拟机之间移动，确保用户始终可以访问所需的应用程序，而不会使主映像变得臃肿。

Citrix Virtual Apps and Desktops 通过 Citrix Personalization 组件和 Application Layering Enterprise Layer Manager (ELM) 向用户交付 Elastic App 应用程序。这两个组件管理主机上包生命周期的所有方面。有关 Application Layering Enterprise Layer Manager 的更多信息，请参阅Citrix App Layering™ 文档。

Cloudpaging 应用程序

Cloudpaging 是 Numecent 的应用程序流技术，它将应用程序交付到 Windows 会话，而无需更改基础映像。

借助 Cloudpaging，应用程序几乎可以即时启动，因为最初只流式传输一小部分代码（通常不到 10%）。当用户访问其余组件时，它们会在后台流式传输，从而提供无缝体验。

对于 Citrix 环境，VDA 上的应用程序包交付组件与 Numecent Cloudpaging Player 协同工作，以管理应用程序生命周期。Citrix 组件协调交付，而 Cloudpaging Player 则处理会话内的按需流式传输和执行。

配置要求

请考虑以下配置详细信息：

云分页播放器和注销检查系统模块

将虚拟发布的应用程序与 Cloudpaging 容器结合使用时，请配置以下设置以允许会话注销：

设置	值
注册表项	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`
值名称	`LogoffCheckSysModules`
值类型	`REG_SZ`
值数据	`CoreHelper.exe`

允许列表中的 URL

除了标准的 URL 允许列表要求外，VDA 还需要访问以下端点：

参数	值
URL	`external-api.cloudpager.net`
端口	443
客户端	Cloudpager PoSh 模块
基于 Web 的正向代理配置	• 允许出站访问 • 需进行身份验证绕过
描述	Cloudpager PowerShell 模块

（可选）您可以创建一个专用交付组，其中包含一个仅用于执行 Cloudpager 发现的 VDA，以限制所需的白名单 URL。我们建议创建一个交付组，其中包含安装了 **VDA 版本 2511 或更高版本**和**应用程序包交付组件**的计算机。

有关 Cloudpager Client 网络和防火墙要求的更多信息，请参阅 Numecent 知识库文章。

部署和交付应用程序包

先决条件

为了支持交付 App-V、MSIX、MSIX app attach、FlexApp 包、Elastic App 应用程序和 Cloudpaging 包，您必须首先在 VDA 计算机上安装“**应用程序包交付组件**”。有关详细信息，请参阅在 VDA 计算机上安装应用程序包交付组件。

在 VDA 计算机上安装应用程序包交付组件

应用程序包交付组件管理 App-V、MSIX、MSIX app attach、FlexApp、Elastic App 和 Cloudpaging 格式的应用程序包的发布过程。默认情况下，在安装 VDA 时不会安装此组件。您可以在 VDA 安装期间或之后安装此组件。

要在 VDA 安装期间安装此组件，请使用以下任一方法：

- 在安装向导中，转到“**附加组件**”页面，然后选择“**应用程序包交付组件**”复选框。
- 在命令行界面中，使用 `/includeadditional "Citrix Personalization for App-V – VDA"` 选项。

要在 VDA 安装后安装此组件，请执行以下步骤：

1. 在 VDA 计算机上，转到“**控制面板 > 程序 > 程序和功能**”，右键单击“**Citrix Virtual Delivery Agent**”，然后选择“**更改**”。
2. 在出现的向导中，转到“**附加组件**”页面，然后启用“**应用程序包交付组件**”复选框。

> **注意：**
>
> - Microsoft App-V 桌面客户端是用于在用户设备上运行 App-V 包中的虚拟应用程序的组件。Windows 10（1607 或更高版本）以及 Windows Server 2019 及更高版本已包含此 App-V 客户端软件。您只需在 VDA 计算机上启用它。有关详细信息，请参阅此 Microsoft 文档文章：启用 App-V 内置客户端。
> - 对于 FlexApp 应用程序，请在 VDA 上安装 FlexApp One 代理以及应用程序包交付组件。

- 对于 Elastic App 应用程序，请在 VDA 上安装启用 App Layering 的映像以及应用程序包交付组件。
- 对于 Cloudpaging 应用程序，请在 VDA 上安装Cloudpaging Player以及应用程序包交付组件。

安装 FLEXAPP ONE 代理

1. 在 VDA 上启动管理员命令提示符。
2. 找到任何 FlexApp One 包的网络路径。
3. 输入以下命令：

```
\\path\to\any\FlexAppOnePackage.exe --install
```

4. 接受出现的任何提示。

安装启用 APP LAYERING 的映像

1. 设置应用程序分层。 请按照 Citrix App Layering 文档中的说明进行操作。该过程包括：
   a. 设置企业层管理器 (ELM)。
   b. 导入黄金 OS 映像。
   c. 创建一个平台层。
   d. 创建应用程序层。
   e. 在 ELM 中，选中要交付的每个应用程序层的“**为 Studio 应用程序包启用此应用程序层**”复选框。
2. 在 VDA 计算机上安装包含 Elastic Layering 组件的映像。您可以使用以下方法之一：
   a. 从 ELM 部署已启用 Elastic Layering 的映像。
   b. 在计算机上手动安装 VDA 并在设置过程中选择 Elastic Layering 组件。

安装 CLOUDPAGING 播放器

1. 在 VDA 上打开管理员命令提示符。
2. 转到包含 Cloudpaging Player 安装程序的文件夹。
3. 运行以下命令以静默安装播放器并配置 SaaS 控制台 URL。根据需要替换占位符值：

```
cloudpaging-player-setup-x64-release.exe /S /v"/qn ADDLOCAL=ALL
REG_BASTOKENPATHORURL=https://your-tenant-url/api/token"
```

4. （可选）安装后通过检查以下注册表值来验证配置：
   - **路径：** `HKEY_LOCAL_MACHINE\SOFTWARE\Numecent\StreamingCore\Settings\Launcher`
   - **名称：** `BaseTokenPathOrURL`
   - **数据：** 该值必须与您在安装期间指定的 URL 匹配。

交付打包的应用程序

完成安装 (#prerequisites) 后，请执行以下操作以向用户交付打包的应用程序：

1. (#store-application-packages-on-network-shares) 在网络共享上存储应用程序包。
2. (#upload-application-packages-into-your-environment) 将应用程序包上传到您的环境。
3. (#add-applications-to-delivery-groups) 将应用程序添加到交付组。
4. 要启用相互依赖的 App-V 包的自动交付，请 (#optional-create-isolation-groups-for-app-v-packages) 创建隔离组。

在网络共享上存储应用程序包

设置基础结构后，生成应用程序包并将其存储在网络位置，例如 UNC 或 SMB 网络共享或 Azure 文件共享。

详细步骤如下：

1. 生成应用程序包。有关详细信息，请参阅 Microsoft 文档：创建和管理 App-V 虚拟化应用程序。
2. 在网络位置存储应用程序包：
   - 对于 **App-V Single Admin**：将包和相应的动态配置文件 (App-V) 存储在 UNC 或 SMB 网络共享或 Azure 文件共享上。
   - 对于 **App-V Dual Admin**：从 UNC 路径将包发布到 App-V 管理服务器。（不支持从 HTTP URL 发布。）
   - 对于 **MSIX 或 MSIX app attach**：将包存储在 UNC 或 SMB 网络共享或 Azure 文件共享上。
   - 对于 **FlexApp**：将包存储在 UNC 或 SMB 网络共享或 Azure 文件共享上。
   - 对于 **Elastic App**：将包存储在 UNC 或 SMB 网络共享或 Azure 文件共享上。
   - 对于 **Cloudpaging**：将软件包存储在 UNC 或 SMB 网络共享或 Azure 文件共享上。

3. 确保 VDA 对软件包存储路径具有读取权限：

   - 如果您将软件包存储在 AD 域中的 UNC 或 SMB 网络共享上，请授予 VDA 计算机对存储路径的读取权限。为此，您可以明确授予计算机的 AD 帐户对共享的读取权限，或者将该帐户包含在具有该权限的 AD 组中。
   - 如果您将软件包存储在 Azure 文件共享上，请首先授予用户帐户对 Azure 中存储路径的读取权限。接下来，配置在 VDA 计算机上运行的 `ctxAppVService` 以使用该用户帐户访问软件包存储路径。有关详细步骤，请参阅更改用户登录帐户。

更改用户登录帐户

在以下两种情况下更改用户登录帐户：

- 要使用链接的 AD 帐户访问 Azure 文件共享上的软件包：
  - 连接实体必须是用户帐户，而不是计算机帐户，因为 Microsoft Entra ID 不会向文件共享上的计算机帐户授予读取权限。
- 如果 MSIX 和 MSIX AppAttach 软件包包含服务：
  - 软件包必须使用在本地计算机上具有管理权限的用户帐户发布，然后才能发布给任何非管理用户。这是安装打包服务所必需的，并且软件包只能发布给用户，而不能发布给计算机，这使得默认的 LocalService 帐户不适用。

VDA 调用 `ctxAppVService` 来访问软件包存储路径并执行需要管理权限的操作。默认情况下，`ctxAppVService` 在计算机的 LocalService 帐户的上下文中运行，该帐户使用计算机的身份向 AD 进行身份验证，不适用于上述场景。

在任何一种情况下，都必须重新配置服务以使用具有本地管理权限并已授予对软件包存储位置（无论是 SMB 共享还是 Azure 文件共享）读取访问权限的 AD 用户帐户，具体如下：

1. 启动“**服务**”，右键单击“**ctxAppVService**”，然后选择“**属性**”。
2. 在“**登录**”选项卡上，选择“**此帐户**”：
   a. 输入一个具有本地管理权限和对软件包存储路径的读取权限的用户帐户。
   b. 输入用户密码两次。
3. 单击 **确定**。

将应用程序包上传到您的环境

根据需要将应用程序包存储到网络位置后，将其上传到您的环境以进行交付。根据需要使用以下任一方法：

- 批量上传
- 逐个上传

准备工作

Citrix Virtual Apps and Desktops 使用 VDA 计算机设置与网络位置的连接以进行包发现。因此，请事先创建交付组，并确保组中至少有一个 VDA 满足以下要求：

- VDA 版本：
  - 要发现 App-V 包：2203 或更高版本
  - 要发现 MSIX 和 MSIX app attach 包：2209 或更高版本
  - 要发现 FlexApp 包：2311 或更高版本以及 FlexApp Agent 软件
  - 要发现 ElasticApp 包：2511 或更高版本以及启用 App Layering 的映像
  - 要从 Cloudpager 控制台发现 Cloudpaging 包：2511 或更高版本
  - 要从网络共享发现 Cloudpaging 包：2607 LTSR 或更高版本
- 应用程序包交付组件：已安装
- 包位置权限：读取（有关详细信息，请参阅 在网络共享上存储应用程序包。）
- 电源：开
- 状态：已注册

批量上传应用程序包

将网络位置中的包上传到您的环境。上传前，请确保您已准备好以下各项：

- 满足 准备工作 要求的交付组
- 网络位置路径

要批量上传包，请执行以下步骤：

1. 在左侧窗格中，选择 **应用程序包**。
2. 在“**包发现**”选项卡上，单击“**创建发现配置文件**”按钮。“**创建发现配置文件**”页面随即出现。
3. 在 **名称** 字段中，输入配置文件的描述性名称。
4. 在 **交付组** 字段中，单击 **选择交付组**。接下来，选择一个满足 准备工作 中所述要求的交付组，然后单击 **确定**。
5. 在 **位置类型** 字段中，根据存储包的位置选择 **Microsoft App-V 服务器**、**网络共享** 或 **Numecent Cloudpager**，然后完成相应的设置：
   - 如果您选择了 **Microsoft App-V 服务器**，请输入以下信息：

- 管理服务器的 URL。示例：`http://appv-server.example.com`
- 管理服务器管理员的登录凭据。
- 发布服务器的 URL 和端口号。示例：`http://appv-server.example.com:3330`

- 如果您选择了 **Network share**，请指定以下信息：
  - 输入网络共享的 UNC 路径（示例：`\\Package-Server\apps\`）。对于 *Elastic App packages*，请输入 ELM 中 **System's Network File Share SMB path** 的 UNC 路径。
  - 选择要上传的包类型。选项包括 **App-V**、**MSIX**、**MSIX app attach**、**FlexApp**、**Elastic App** 和 **Cloudpaging**。
  - 指定是否在子文件夹中搜索包。

    > **注意：**
    >
    > 如果您在包含 `cim` 映像的文件夹结构中搜索 MSIX app attach 包，请确保选择**搜索**子文件夹。否则，磁盘将无法正确发现。

- 如果选择了 **Numecent Cloudpager**（这意味着 Cloudpaging 应用程序存储在 Cloud Pager Console 上），请输入以下信息：
  - Cloudpager 控制台 URL。示例：`https://cloudpagerconsole.my.org`
  - PowerShell API 密钥。
  - AppLauncher MSID。

6. 单击“**创建发现配置文件**”。

“**创建发现配置文件**”页面关闭，新添加的配置文件将显示在配置文件列表中。Citrix Virtual Apps and Desktops 使用交付组中的 VDA 将软件包上传到您的环境。上传完成后，“状态”字段显示 *导入成功*。相应的软件包将显示在“**软件包**”选项卡上。

> **注意：**
>
> 要在源位置检查软件包更新并将其导入到您的环境，请在配置文件列表中选择该位置，然后单击“**检查更新**”。

逐个上传应用程序包

将应用程序包从网络共享上传到您的环境。上传之前，请确保已准备好以下各项：

- 满足准备工作中规定的要求的交付组
- 网络位置路径。

要将软件包上传到您的环境，请执行以下步骤：

1. 在左侧窗格中，选择“**应用程序包**”。
2. 在“**软件包**”选项卡上，单击“**添加软件包**”按钮。此时将显示“**添加软件包**”页面。
3. 在“**交付组**”字段中，单击“**选择交付组**”。接下来，选择一个符合准备工作中规定的要求的交付组，然后单击“**确定**”。
4. 在“**程序包完整路径**”字段中，根据需要输入路径：
   - 要一次上传多个程序包，请输入它们的完整路径，用分号分隔 (`;`)。示例：`\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - 要上传网络共享上存在的所有程序包，请输入存储路径。示例：`\\package-Server\apps\`
5. 单击“**添加程序包**”。

   应用程序程序包将显示在“**程序包**”选项卡上。

将应用程序添加到交付组

将应用程序程序包完全上传到您的环境后，根据需要将其应用程序添加到一个或多个交付组。这样，与这些交付组关联的用户就可以访问这些应用程序。

> **注意：**
>
> - 您可以通过交付组将打包的应用程序交付给单会话 VDA 和多会话 VDA。
> - 默认情况下，最终用户可以访问分配给与其*单会话*（或称为*桌面*）VDA 关联的交付组的所有打包应用程序。要将打包应用程序在*桌面* VDA 上的可见性限制为特定用户或组，请转到“**应用程序**”节点，选择该应用程序，然后选择“**编辑应用程序属性 > 限制可见性**”进行更改。请参阅限制应用程序的可见性

要将程序包中的一个或多个应用程序添加到多个交付组，请执行以下步骤：

1. 在左侧窗格中，选择 **App Packages**。

2. 在 **Packages** 选项卡上，根据需要选择一个包。
3. 在操作栏中，单击 **Add Delivery Groups**。将显示 **Assign Applications to Delivery Groups** 页面。
4. 根据需要选择软件包中的一个或多个应用程序，然后单击“**下一步**”。
5. 在交付组列表中，选择要分配应用程序的组，然后单击 **Next**。

> **注意：**
>
> - 如果您选择了 MSIX 或 MSIX app attach 包，则列表中仅显示 VDA 版本为 2106 或更高版本的交付组。
> - 如果您选择了 *FlexApp* 包，则列表中仅显示 VDA 版本为 2402 或更高版本的交付组。
> - 如果选择了 *Elastic App* 软件包，则列表中仅显示 VDA 版本为 2511 或更高版本的交付组。
> - 如果您选择了 *Cloudpaging* 包，则列表中仅显示 VDA 版本为 2511 或更高版本的交付组。

6. 单击“**完成**”。

要将各种包中的应用程序添加到多个交付组，请执行以下步骤：

1. 在左侧窗格中，选择 **App Packages**。
2. 在 **Applications** 选项卡上，选择 **Add Applications**。
3. 在 **Groups** 页面上，根据需要选择一个或多个交付组。
4. 在 **Applications** 页面上，按如下方式选择一个或多个应用程序包：
    a. 单击 **Add**，然后选择 **Application packages**。
    b. 选择所需的软件包配置文件类型（例如，App-V 单管理员）。此类型的所有软件包都会显示。
    c. 根据需要选择一个或多个包。
    d. 单击 **OK**，然后单击 **Next**。
    e. 要添加不同包类型的更多应用程序，请重复步骤 a 到 d。
5. 单击“**完成**”。

您还可以在以下情况下将打包的应用程序添加到交付组：

- 创建交付组。有关详细信息，请参阅 创建交付组。
- 编辑现有交付组或应用程序组。有关详细信息，请参阅 添加应用程序。

（可选）为 APP-V 包创建隔离组

您可以创建隔离组，以实现相互依赖的 App-V 软件包的自动交付。

> **注意：**
>
> 隔离组支持 App-V 单管理员方法。如果您使用的是 App-V 双管理员方法，则可以通过在 Microsoft App-V 基础结构中创建*连接组*来实现相同的目标。有关详细信息，请参阅此 Microsoft 文档文章：关于连接组文件。

关于隔离组

隔离组是相互依赖的应用程序包的集合，这些包必须在同一个 Windows 沙盒中运行才能创建虚拟环境。Citrix App-V 隔离组与 App-V 连接组相似但不完全相同。隔离组包括两种类型的软件包：

- **显式应用程序包**：具有特定许可要求的应用程序。您可以通过将这些应用程序添加到交付组来将其限制为特定范围的用户。
- **自动应用程序包**：无论是否添加到交付组，始终对所有用户可用的应用程序。

例如，应用程序 `app-a` 需要 JRE 1.7 才能运行。您可以创建一个隔离组，其中包含 app-a（标记为*显式*）和 JRE 1.7（标记为*自动*）。接下来，将 `app-a` 的 App-V 软件包添加到一个或多个交付组。当用户启动 app-a 时，JRE 1.7 会随之自动部署。

当用户在隔离组中启动标记为 *显式* 的 App-V 应用程序时，Citrix Virtual Apps and Desktops 会检查用户在交付组中对该应用程序的访问权限。如果用户有权访问该应用程序，则同一隔离组中的任何 *自动* 应用程序包都将对用户可用。

您无需将*自动*软件包添加到任何交付组。如果隔离组中还有另一个*显式*应用程序包，则只有当该包位于同一交付组中时，该包才对用户可用。

创建 App-V 隔离组

创建隔离组并将相互依赖的应用程序包添加到其中。详细步骤如下：

1. 在**隔离组**选项卡上，单击**添加隔离组**。
2. 输入隔离组的名称和描述。环境中的所有 App-V 单管理员软件包都会显示在**可用软件包**列表中。
3. 从**可用软件包**列表中，根据需要选择一个应用程序，然后单击向右箭头。所选应用程序将显示在**隔离组中的软件包**列表中。

4. 在“**部署**”字段中，为应用程序选择“**显式**”或“**自动**”。
5. 重复步骤 2-3 以添加更多程序包。
6. 要调整列表中程序包的顺序，请单击向上或向下箭头。
7. 单击 **保存**。

> **注意：**
>
> 隔离组配置会导致在 VDA 上创建 App-V 连接组。部署方案可能变得复杂，并且 App-V 客户端支持一次只在一个活动连接组中的程序包。建议您避免将同一个程序包添加到属于同一个交付组的两个不同隔离组中。

最佳实践

- 要部署 App-V 程序包，请使用 PowerShell 命令 `Enable-AppV` 在 VDA 上启用 App-V 子系统。
- 要部署 MSIX（和 AppAttach）程序包，VDA 必须信任用于签署这些程序包的证书。
- 在 Windows Server 2019 上，启用旁加载以部署 MSIX 程序包。Windows 10、11、Windows Server 2022 和 2025 不需要旁加载。
- App Attach 在 Windows Server 2019 上根本没有实现，并且目前 Microsoft（或 Citrix 扩展）在 Windows Server 2022 或 2025 上不支持它。

高级

以下高级主题提供了额外的配置选项和控件，用于在 Citrix Virtual Apps and Desktops 中微调打包应用程序的发现、更新和交付方式，超越了基本的应用程序包工作流程。

自动化打包应用程序发布

您可以使用 PowerShell 命令自动化打包应用程序发布：

在 Delivery Controller™ 上，运行以下 PowerShell 命令:

1. 加载包发现模块中存在的命令:

```
Import-Module "D:
\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```

> **注意:**

> 软件包发现模块的版本可以在 Citrix Virtual Apps and Desktops ISO 上找到，路径如步骤 1 中所述。

2. 软件包发现模块必须来自支持您正在发布的软件包类型的 Citrix Virtual Apps and Desktops 版本的 ISO，即 FlexAppOne 应用程序需要 2311 或更高版本。我们建议使用最新版本。
3. 检索相关的交付组 ID 和打包应用程序 ID:

```
Get-BrokerDesktopGroup | Format-Table Uid, Name

Get-AppLibAppVApplication | Format-Table Uid, Name
```

4. 发布包并创建相应的 BrokerMachineConfigurations:

```
Publish-PackagedApplication -AppLibararyApplicationUid
<AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
```

5. 同步 Broker 配置，这些配置稍后会发送到 VDA 上的 Broker 代理:

```
Update-DesktopGroupMachineConfigurations -DesktopGroupUid
<DesktopGroup.Uid>
```

> **注意:**
>
> 请务必在通过 PowerShell 命令行发布或从交付组中删除打包应用程序后运行 PowerShell 命令 `Update-DesktopGroupMachineConfigurations`。否则，有关已发布应用程序的信息将无法正确发送到 VDA，并且启动会失败。

限制应用程序可见性

在 Citrix Virtual Apps and Desktops 环境中，当软件包中的应用程序发布到桌面时，系统会遵循这些应用程序的 Active Directory (AD) 用户和组可见性设置。但是，即使用户只能看到软件包中的一个应用程序，也必须将整个软件包部署到虚拟桌面（或无缝应用程序）会话，因为单个软件包组件无法在 VDA 上细分。此外，在 VDA 2503 版本之前，初始发布后降低应用程序可见性的更改不会导致在后续桌面启动时清理以前发布的软件包。此外，其他可见性层（例如桌面与工作区可见性）在这些 AD 可见性分配之上运行。

您可以控制打包应用程序是必须显示在 Workspace 中，还是部署到用户的 VDI 桌面会话。打包应用程序发布后，您可以使用 PowerShell 命令 `Set-BrokerApplication -Name "MyApp" -PackagedApplicationVisibility "Workspace|Desktop|WorkspaceAndDesktop"` 更新 `BrokerApplictaion` 上的 `PackagedApplicationVisibility` 属性。

`PackagedApplicationVisibility` 的默认值为 `WorkspaceAndDesktop`。

值 `Workspace`: 应用程序仅显示在 WorkspaceApp 中，可用于无缝 AppLaunch，但应用程序不会自动发布到用户启动的任何桌面会话。

值 `Desktop`：从 WorkspaceApp 隐藏应用程序图标，使其无法进行无缝 AppLaunch，但如果用户通过其 AD 组设置也可以访问该应用程序，则该应用程序仍可部署到用户的桌面会话。

> **注意：**
>
> 发布到单会话静态桌面的打包应用程序在 Workspace App 中永远不可用，无论此设置中配置的值如何。

从 App-V 完整基础架构迁移到单一管理员工作流

Microsoft App-V 完整基础架构（双管理员）即将终止支持。要继续交付 App-V 软件包和其他受支持的容器格式，请迁移到 Citrix 单一管理员模型。

单一管理员模型消除了对 App-V 管理和发布服务器的依赖，并将软件包管理集中到 Studio 中。

单一管理员模型的优势

转向单一管理员工作流可简化您的架构并优化软件包管理。

简化的架构

在单一管理员模型中，VDA 直接从文件共享检索软件包。Citrix 管理元数据、发布和隔离逻辑。

功能	完整基础架构（双管理员）	单一管理员（CITRIX 管理）
管理	App-V 管理控制台	Citrix 工作室 或 Web 工作室
数据库	必需 (SQL Server)	无（元数据存储在 Citrix 站点数据库中）
发布	App-V 发布服务器	思杰 VDA (`ctxAppVService`)

功能	完整基础架构（双管理员）	单一管理员（CITRIX 管理）
程序包源	UNC 共享（与管理服务器同步）	UNC 共享、SMB 共享或 Azure 文件
逻辑	连接组	Citrix 隔离组

战略优势

通过迁移到单一管理员，您还可以消除**同步延迟**。

- 在双管理员模型中，您必须同步 App-V 管理服务器，然后同步 Studio。
- 在单管理员模型中，当您在文件共享上更新包并在 Studio 中选择**刷新**时，更新后的包将在下次用户登录时可用。

迁移工作流

请按照以下步骤将您现有的 App-V 完整基础结构迁移到 Citrix 单管理员工作流：

1. 步骤 1：准备目标环境
2. 步骤 2：将包导入 Citrix 库

步骤 1：准备目标环境

在导入包之前，请确保您的基础结构和 VDA 已准备好支持单管理员模型。

1. **共享存储库**

   a. 确定托管您的 `.appv` 包的 UNC 共享。

   b. 确保 VDA 计算机帐户（例如，域计算机）对共享和 NTFS 权限都具有**读取**访问权限。

2. **VDA**

   确保所有 VDA 都已安装 **App Packages Delivery Component**。要在安装后添加此组件，请执行以下操作：

   a. 运行 VDA 安装程序。

   b. 在**程序和功能**中选择**更改**。

   c. 添加 **应用程序包交付组件**。

3. **XML 配置文件**

   将 `_DeploymentConfig.xml` 和 `_UserConfig.xml` 文件移动到与相应 `.appv` 文件*相同*的文件夹中。

在单一管理员模型中，VDA 从文件共享上的程序包文件夹而不是从中央 App-V 数据库读取配置文件。

步骤 2：将程序包导入 CITRIX 库

准备好环境后，将现有 App-V 程序包导入 Citrix 应用程序库。

1. 在 Citrix Studio 中，转到**配置** > **应用程序包**。
2. 如果您正在完全迁移，请删除与 App-V 管理服务器的任何现有连接。
3. 选择**添加程序包**并将其指向程序包的 UNC 路径。
4. Citrix 会扫描该文件夹并将程序包名称、版本和应用程序 ID 导入 Citrix 应用程序库。

导入后，您可以根据需要将应用程序分配给交付组。

> **注意：**
>
> **vPrefer 策略（可选）**：如果您希望应用程序在本地 VDA 上启动而不是重定向到远程服务器，请在您的 VDA 上启用 **vPrefer** GPO。

排除 App-V 应用程序故障（单一管理员模型）

如果 App-V 程序包（在单一管理员模型中）无法启动或未显示在用户会话中，请使用以下指南来识别和解决常见问题。

问题	描述	解决方案
包发现和“编目失败”错误	在 Studio 中添加包时，出现错误提示文件无法访问或元数据无效。	1. 验证权限。确保 Delivery Controller 计算机帐户（例如，`DOMAIN\DDC01$`）对托管包的 UNC 路径的共享和 NTFS 级别都具有**读取**权限。

问题	描述	解决方案	
		2. 检查 XML 完整性。 确保 `.appv` 文件和 `_DeploymentConfig.xml` 文件具有相同的文件名开头，并且位于同一文件夹中。	
应用程序启动失败 (错误代码： 0x80070005 或 0x80040154)	用户点击应用程序图标后，出现 **Citrix 启动**屏幕，但应用程序未打开。	1. 验证 VDA 组件。 确保 VDA 上安装了 **App Packages Delivery Component**。 确认存在以下文件：`C:\Program Files\Citrix\AppV\ctxAppVService.exe`。 2. 检查 VDA 权限。 由于 VDA 从文件共享中拉取程序包，因此 VDA 计算机帐户（例如 `DOMAIN\VDA-HR01$`）必须对	

问题	描述	解决方案	
		UNC 路径具有**读取**访问权限。 3. 验证 App-V 客户端配置。 • 在 VDA 上运行以下 PowerShell 命令：`Get-AppvClientConfiguration`。 • 如果您的程序包需要脚本，请确保 `EnablePackageScripts` 设置为 `$True`。	
隔离组冲突	插件（例如 Excel 加载项）无法看到其父应用程序。	1. 在 Studio 中，转到 **应用程序包** > **隔离组**。 2. 确保两个程序包都已添加到同一隔离组。 在单一管理员模型中，VDA 上的 App-V 客户端根据 Delivery Controller 提供的配置管理这些应用程序的虚拟连接。	

问题	描述	解决方案
首次启动缓慢（缓冲）	首次启动大型 App-V 软件包（例如 AutoCAD 或 ArcGIS）需要几分钟。	1. 在 VDA 上，检查以下注册表项：`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AppV\Client\Streaming` 2. 将 `Autoload` 设置为 `2`（自动加载所有以前使用的软件包）以提高后续启动性能。 3. 检查网络性能。确保网络共享上的 SMB 签名或防病毒扫描没有限制传输速度。

有用的 PowerShell 命令（在 VDA 上运行）

要验证 Citrix 是否已成功将软件包交付到 VDA，请在 PowerShell 窗口中运行以下命令：

命令	目的
`Get-AppvClientPackage`	显示当前缓存到 VDA 或发布到 VDA 的所有 App-V 软件包。
`Get-CtxAppvPackage`	显示由 Citrix 代理管理的软件包。
`Start-Service ctxAppVService`	重新启动 Citrix App-V 编排服务。

通用 Windows 平台应用

有关通用 Windows 平台 (UWP) 应用的信息，请参阅以下 Microsoft 文档：

- 什么是通用 Windows 平台 (UWP) 应用？
- Windows 程序包管理器

要求和限制

Citrix Virtual Apps and Desktops™ 支持在以下 Windows 计算机上将 UWP 应用与 VDA 结合使用：

- Windows 10 及更高版本
- Windows Server 2016 及更高版本

VDA 最低版本必须为 7.11。

以下 Citrix Virtual Apps and Desktops™ 功能在使用 UWP 应用程序时不受支持或受限：

- 不支持文件类型关联。
- 不支持本地应用访问。
- 动态预览：如果会话中运行的应用重叠，预览将显示默认图标。UWP 应用不支持用于动态预览的 Win32 API。
- 操作中心远程处理：UWP 应用可以使用操作中心在会话中显示消息。这些消息目前不会重定向到端点以显示给用户。

不支持从同一服务器启动 UWP 应用和非 UWP 应用。请将 UWP 应用和非 UWP 应用放置在单独的交付组或应用程序组中。

由于机器上安装的所有 UWP 应用程序都会被枚举，Citrix® 建议禁用用户对 Windows 应用商店的访问。这可以防止一个用户安装的 UWP 应用程序被其他用户访问。

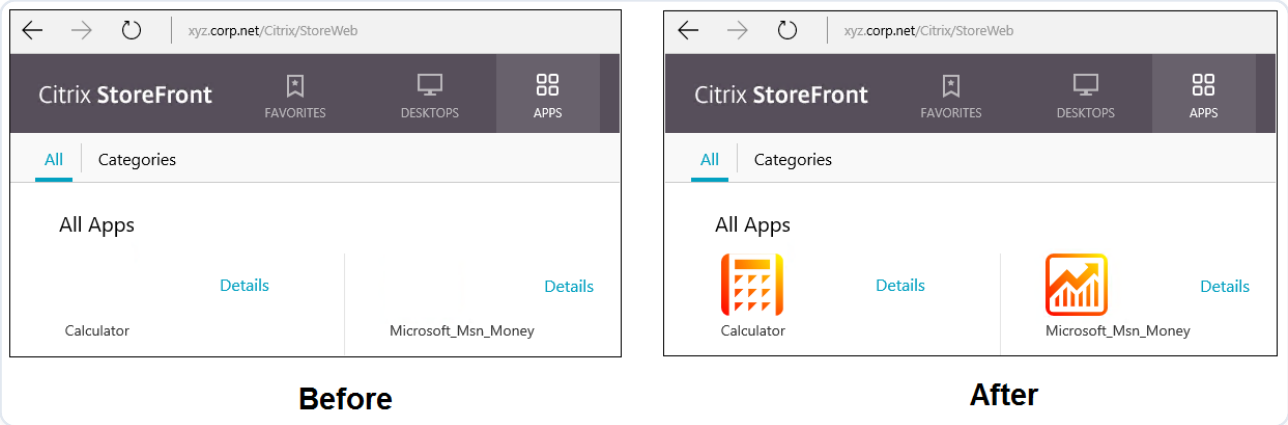
在旁加载期间，UWP 应用程序会安装在计算机上，并可供其他用户使用。当其他用户启动该应用程序时，它会被安装，并且操作系统会更新其 AppX 数据库以指示该用户“已安装”。

从在固定或无缝窗口中启动的已发布的 UWP 应用程序开始的正常注销可能会阻止 VDA 会话关闭并强制注销用户。发生这种情况时，VDA 会话中剩余的几个进程会阻止其正常关闭。要解决此问题，请确定是哪个进程阻止 VDA 会话关闭，然后按照 CTX891671 中的指导将其添加到“LogoffCheckSysModules”注册表项值中。

UWP 应用程序的应用程序显示名称和描述可能不正确。在将应用程序添加到交付组时，请编辑并更正这些属性。

请查看 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/whats-new/known-issues.html) 以了解任何其他问题。

目前，一些 UWP 应用程序具有启用透明度的白色图标，这导致图标在 StoreFront 显示的白色背景下不可见。为避免此问题，您可以更改背景。例如，在 StoreFront 计算机上，编辑文件 `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`。在文件末尾，添加 `.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`。下图说明了此示例的更改前后对比。



在 Windows Server 2016 及更高版本上，启动 UWP 应用程序时也可能会启动服务器管理器。为防止这种情况发生，您可以使用 `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon` 注册表项禁用服务器管理器在登录时自动启动。有关详细信息，请参阅 `<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`。

安装和发布 UWP 应用程序

默认情况下启用对 UWP 应用程序的支持。

要在 VDA（或主映像）上安装一个或多个 UWP 应用程序，请使用以下方法之一：

- 使用部署映像服务和管理 (DISM) 等工具，从适用于企业的 Windows 应用商店完成脱机安装，以将应用程序部署到桌面映像。有关详细信息，请参阅 Windows 程序包管理器。
- 旁加载应用程序。有关详细信息，请参阅 在 Windows 客户端设备中旁加载业务线 (LOB) 应用。
- 直接从适用于企业的 Windows 应用商店为每个目标用户安装 UWP 应用程序。

要在 Citrix Virtual Apps 或 Citrix Virtual Desktops™ 中添加（发布）一个或多个 UWP 应用程序，请执行以下操作：

1. UWP 应用安装到计算机后，将 UWP 应用添加到交付组或应用程序组。您可以在创建组时或之后执行此操作。在“**应用程序**”页面上，在“**添加**”菜单中，选择“**从‘开始’菜单**”。

2. 应用程序列表出现时，选择要发布的 UWP 应用。
3. 继续向导或关闭编辑对话框。

要禁用在 VDA 上使用通用应用，请在 `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` 中添加注册表设置 **EnableUWASeamlessSupport** 并将其设置为 **0**。

卸载 UWP 应用

当您使用 `Remove-AppXPackage` 等命令卸载 UWP 应用时，该项目仅针对管理员卸载。要从可能已启动和使用该应用的用户计算机中删除该应用，请在每台计算机上运行删除命令。您无法通过一个命令从所有用户的计算机中卸载 AppX 包。

备份或迁移您的配置

此功能可帮助您备份配置。备份与还原功能相结合，可轻松实现站点信息从本地到云端或从一个云站点到另一个云站点的迁移。它还有助于在紧急情况下立即恢复站点。

您可以使用以下方法进行备份：

1. 备份 + 还原
    a. 与 Web Studio 集成。
2. 自动化配置工具 (ACT)
    a. 基于 PowerShell 的工具。安装该工具即可使用。请参阅下载自动化配置。

备份可用于：

1. 还原
2. 迁移

Citrix® 建议将以下工具用于所述场景。

备份

环境	用例	推荐工具	特殊注意事项	链接
DaaS 和本地部署	按需和计划备份	备份 + 恢复	Citrix 保留备份，用户可在需要时下载	使用 Web Studio 进行备份和还原(/zh-cn/citrix-virtual-

环境	用例	推荐工具	特殊注意事项	链接
				apps-desktops/2607-ltsr/manage-deployment/backup-restore-studio.html)
DaaS 和本地部署	按需和计划备份	ACT	用户保留备份	使用自动化配置工具进行备份和恢复

迁移

环境	用例	推荐工具	特殊注意事项	链接
本地部署到云	将一个本地站点迁移到 DaaS	ACT		从本地部署迁移到云
	将多个本地站点整合到一个 DaaS 站点	ACT	站点合并	将多个本地站点合并到一个云站点
本地部署到本地部署	将一个本地站点迁移到另一个本地站点	ACT		POC 指南:自动化配置工具 - 本地到本地迁移
	将多个本地站点整合到另一个本地站点	ACT	站点合并	POC 指南:自动化配置工具 本地到本地迁移
				将多个本地站点合并到一个云站点
云到云	将一个 DaaS 站点迁移到另一个 DaaS 站点	ACT		从云迁移到云(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/manage-deployment/

环境	用例	推荐工具	特殊注意事项	链接
				migrate-cloud-to-cloud.html)
将多个 DaaS 站点整合到一个 DaaS 站点	站点合并	ACT		从云迁移到云(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/manage-deployment/migrate-cloud-to-cloud.html)
				将多个本地站点迁移到一个云站点(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/manage-deployment/multi-site-merge.html)

备份和恢复配置

此功能允许管理员备份您的云配置。它确保您的 Citrix® 配置始终有一个可用副本，随时可以使用。备份与恢复功能相结合，可以轻松地将站点信息从本地迁移到云端，或从一个云站点迁移到另一个云站点。如果发生意外更改，选择一个备份并选择恢复，只需点击几下，您就可以再次运行。您还可以选择备份和恢复特定组件。

此功能允许您备份和恢复以下内容：

- 标签
- 管理员角色
- 管理范围
- 主机连接

> **注意：**

> 您现在可以备份主机连接。每次都必须输入密钥。将执行预导入检查模式，仅针对已导入或更新的主机连接要求输入密钥。

- StoreFront™
- 交付组
- 应用程序组
- 应用程序
- AppV隔离组
- 应用程序库包发现
- 组策略
- 用户区域偏好设置
- 手动预配或 PVS 预配的计算机目录
- 管理文件夹
  - 应用程序文件夹
  - 交付组文件夹
  - 计算机目录文件夹
- SiteSettings

> **重要提示：**
>
> - 确保按照列表中的顺序还原不同的组件。例如，如果要还原应用程序、交付组和组策略，则必须遵循以下顺序：
>   - 交付组
>   - 应用程序
>   - 组策略
> - 您无法备份或还原 MCS 计算机目录。

备份类型

使用以下选项根据您的要求执行备份：

- **按需**：实时备份站点配置。此操作会备份当前的 Citrix Cloud™ 站点配置。
- **计划**：按计划间隔备份站点配置。此操作会按所述间隔重复进行。

> **注意：**
>
> 只有拥有完全权限的管理员和云管理员才能执行按需或计划备份和还原。

使用 Web Studio 进行备份和恢复

本文介绍了您可以在控制台左侧窗格中提供的“**备份和恢复**”节点上执行的操作。

“**备份和恢复**”允许管理员从 Web Studio 执行备份。

设置存储位置

在创建备份之前，您必须设置一个存储位置来存储备份。

1. 在 Web Studio 中，单击“**管理**”。
2. 在左侧菜单中，选择“**备份+恢复**”。
3. 在“**备份和恢复**”选项卡中，单击“**设置存储**”。

   设置备份存储位置(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/first-time-backup-storage-1.png)
4. 从下拉列表中，选择“**存储类型**”。存储类型可以是文件存储或 Azure 存储。

   > **注意：**
   >
   > - 该位置必须可供所有 Delivery Controller 访问。
   > - 如果访问该文件夹需要用户名和密码，请确保公司密码策略不会限制密码的有效期。
5. 选择以下各项：
   - 最大备份数
   - 最大固定备份数
   - 最大自动固定备份
6. 单击**保存**以保存存储位置，或单击**保存并创建备份**以保存存储位置并创建备份。

设置存储位置后，即可创建备份。

创建按需备份

1. 在 Web Studio 中，单击**管理**。
2. 在左侧菜单中，选择**备份和还原**。
3. 如果已设置存储位置但不存在备份，系统会提示您创建备份。

   创建初始备份(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/backup-after-storage-creation.png)

   如果存在现有备份，您可以单击**创建备份**。
4. 在**创建备份**页面上，输入备注，然后单击**创建备份**。

   将显示一个摘要活动，其中显示正在以触发备份的管理员的名义备份的备份组件。
5. 备份成功完成后，它将作为行项目列在**备份和还原**选项卡下。
6. 选择特定备份可在**详细信息**选项卡中查看有关该备份的更多信息。
7. 要删除备份，请右键单击备份，然后单击**删除备份**。

固定备份

Citrix® 存储最近 30 个备份。当您创建的备份超过 30 个时，系统会按照创建顺序删除旧备份。对于在 30 个备份限制之外创建的每个新备份，系统都会删除最早创建的备份。固定备份用于防止自动删除特定备份。您最多可以固定 5 个备份。如果存在固定备份，我们除了保留 30 个备份外，还会保留所有固定备份，这意味着您最多可以保留 35 个备份——30 个非固定备份和 5 个固定备份。

1. 右键单击要固定的备份。

创建计划备份

创建符合您组织要求的备份计划，以自动执行备份和还原过程。备份在后台以您选择的频率（每日、每周、每月或其他合适的频率）运行。

1. 转到“计划”选项卡，然后选择**创建计划**。
2. 在**创建计划**页面上，输入以下内容：

   - **启用此计划**：选择**是**以启用此备份计划。
   - **名称**：输入备份计划的名称。
   - **描述**：输入描述。
   - **时区**：选择您选择的时区。

- **频率**：选择运行备份的频率。
- **每隔**：输入计划必须重复的天数。
- **开始日期**：输入开始日期。
- **备份开始时间**：以 24 小时制输入您希望备份开始的时间。

3. 选择**完成**。

限制计划备份

您可以将计划备份限制为每天一次，以避免出现相同的备份。

1. 转到“**备份和还原**”节点的“**设置**”选项卡。
2. 在“**计划备份**”框中单击“**更改**”。
3. 切换开关以启用将计划备份限制为每天一次。

自动固定计划备份

自动固定计划备份会自动固定由所选计划创建的备份。只能选择一个计划进行自动固定。

使用自动固定计划备份，您最多可以保留六个计划备份。达到最大限制时，将删除最旧的自动固定备份。

> **注意：**
>
> Citrix 最多存储六个自动固定备份。系统会在第六个备份之后按创建顺序删除旧备份。对于在六个备份限制之外创建的每个新备份，系统会删除最先创建的备份。

1. 转到“**备份和还原**”节点的“**设置**”选项卡。
2. 选择一个计划备份以进行自动固定。
3. 切换开关以启用自动固定计划。
4. 选择一个计划，然后单击“**保存**”。

编辑备份存储

您可以编辑备份存储设置，以更改存储类型和位置、最大备份数、最大固定备份数和最大自动固定备份数。

1. 转到“**备份和还原**”节点的“**设置**”选项卡。
2. 在“**存储**”框中单击“**更改**”。

3. 在“**编辑备份存储**”对话框中更改存储设置。

还原

此功能允许管理员从备份中还原站点配置。我们允许您一次还原一个组件。

> **注意：**
>
> - 一次只还原一个组件可确保在还原过程中不会因组件之间的依赖关系而发生冲突。
> - 还原主机连接的工作流程与其他组件不同，因为每次尝试还原主机连接时都需要输入密钥。单击“**还原备份**”后，您会看到一个用于输入密钥的对话框。例如，在 Azure 中，输入用于创建连接的字母数字应用程序密钥。

1. 在 Web Studio 中，单击“**管理**”。
2. 在左侧菜单中，选择“**备份和还原**”。
3. 从列表中单击特定备份。
4. 单击“**还原备份**”。
5. 在“**还原备份**”窗口中，输入以下内容：

   - **组件**：选择要还原的组件。
   - **筛选器**：以逗号分隔的列表形式指定要还原的成员名称。例如，筛选单词 *chrome* 只会还原名称为 chrome 的对象。同样，短语 `chr` 会还原以 `chr` 开头的对象。

     要查看组件成员，请选择一个备份并导航到“**详细信息 > 组件**”。选择一个组件，然后单击“**查看组件成员**”。
   - **检查模式**：选择“**是**”以确认在执行实际还原操作时必须还原的内容。此选项会预先评估还原所需的一切，而不会实际触发还原。例如，当为应用程序组件运行还原过程时，它会显示将要还原的应用程序列表。

     > **注意：**
     >
     > 检查模式不会执行实际的还原。此选项也不会检查组件之间的任何依赖关系。为获得最佳结果，我们建议一次在一个组件上使用检查模式。
   - **还原类型**：选择以下其中一项：

  - **仅缺失**：使用此还原类型将组件和成员添加到站点。即使要还原的备份具有不同的配置，此选项也不会更改现有组件和成员。
  - **缺失并更新现有**：使用此还原类型将组件添加到站点并更新它们。如果备份和现有组件具有不同的配置，此选项将使用备份的配置更新现有组件和成员。

- **备注**：输入任何备注。

6. 选择**还原**。

还原操作完成后，还原结果将列在**还原**窗口中。所有还原操作都列在**历史记录**选项卡下。

历史记录

您可以在**历史记录**选项卡中跟踪所有备份和还原操作。

在**操作**下，您可以查看所有已删除的备份和备份历史记录。

要查看备份的详细信息：

1. 转到**历史记录**选项卡。
2. 选择一个备份操作，然后单击**查看详细信息**。

备份结果为您提供以下详细信息：

- 持续时间
- 备注
- 管理员名称
- 已备份的组件

使用“**历史记录**”页面右上角的搜索栏搜索特定备份。例如：您可以搜索由特定管理员执行的备份，或在特定日期执行的备份。

使用自动化配置工具进行备份和恢复

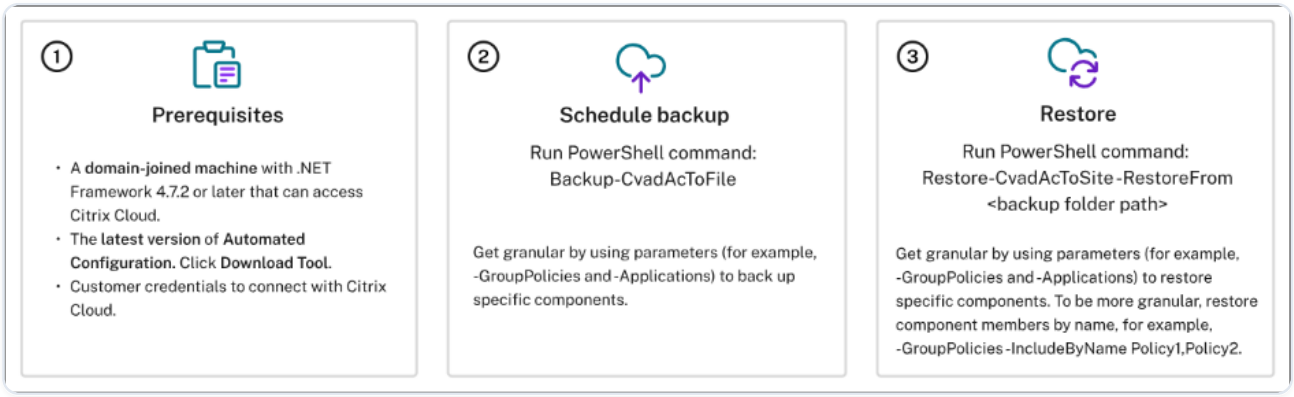
自动化配置工具允许您在以下环境中进行按需和计划备份：

- Citrix 虚拟应用和桌面™
- DaaS

自动化配置工具可用于以下目的：

- 备份和恢复（按需和计划备份）
- 迁移（按需备份）

用于迁移的自动化配置工具



Citrix 虚拟应用和桌面™

备份配置的先决条件

- 所有版本的 Citrix Virtual Apps and Desktops。
- 运行 Auto Config 的计算机。此设备可以是：
  - 交付控制器™
  - 一台已加入域的计算机，安装了 .NET Framework 4.7.2 或更高版本以及 Citrix PowerShell SDK。对于 Citrix PowerShell，您必须安装 Web Studio。

备份

1. 安装 Automated Configuration。有关详细信息，请参阅下载 Automated Configuration。
2. 双击 **Auto-Config**。
3. 在 PowerShell 窗口中，运行命令 `Backup-CvadAcToFile` 以导出所有组件。导出本地配置不会对其进行修改。

首次运行该命令后，该过程会在以下位置创建包含 `.yml` 配置文件的文件夹：`%HOMEPATH%\Documents\Citrix\AutoConfig`。

该文件夹包含最近导出的备份文件，并且每个以前的备份都存储在一个子文件夹中。

还原

1. 双击 **Auto-Config**。
2. 运行以下命令执行还原：

```
Restore-CvadAcToSite -Environment OnPrem -RestoreFolder <folder path of the backup files>
```

3. 运行命令后，验证导出状态，日志文件夹位于：`%HOMEPATH%\Documents\Citrix\AutoConfig`。
4. 如果存在任何错误或异常，请参阅日志文件中的 **Fixups** 部分。

DaaS

备份配置的先决条件

- 已安装活动资源位置和连接器的 DaaS 环境。
- 连接到访问 Citrix Cloud 的站点。有关详细信息，请参阅系统和连接要求。

> **注意**
>
> 您无法使用自动化配置工具从云中备份 MCS。

备份

备份以下文件：

- 包含您的客户 ID、客户端 ID 和密钥信息的 `CustomerInfo.yml` 文件。有关检索客户 ID、客户端 ID 和密钥过程的更多信息，请参阅 生成客户 ID、客户端 ID 和密钥。有关如何将此信息添加到 `CustomerInfo.yml` 文件的信息，请参阅 填充客户信息文件。
- 包含云中资源位置映射信息的 `ZoneMapping.yml` 文件。有关如何映射区域的更多信息，请参阅 填充区域映射文件。
- 包含主机连接信息的 `CvadAcSecurity.yml` 文件。

1. 安装 Automated Configuration。有关详细信息，请参阅安装 Automated Configuration。

> **注意**
>
> 对于 DaaS 备份，请将自动化配置安装在具有 Internet 访问权限且管理员可以直接访问的计算机上。

1. 双击 **Auto Config**。
2. 在 PowerShell 窗口中，运行以下命令进行备份：`Export-CvadAcToFile`

首次运行该命令后，该过程会在以下位置创建一个包含 .yml 配置文件的新文件夹：`%HOMEPATH%\Documents\Citrix\AutoConfig`

该文件夹包含最近导出的备份文件，并且每个以前的备份都存储在一个子文件夹中。

还原

1. 双击 **Auto Config**。
2. 在 PowerShell 窗口中，运行以下命令执行还原：

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

3. 运行命令后，验证导出状态，您可以在 `%HOMEPATH%\Documents\Citrix\AutoConfig` 找到日志文件夹。
4. 如果存在任何错误或异常，请参阅日志文件中的“**修复**”部分。

精细迁移

> **注意**
>
> 有关组件迁移顺序的更多信息，请参阅组件迁移顺序。

还原整个组件

要还原组件，必须选择一个或多个参数。

例如，要还原整个交付组和计算机目录组件，请运行以下命令：

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups
-MachineCatalogs
```

还原组件成员

要还原一个或多个组件成员，请使用 `IncludeByName` 功能。您必须使用 `Restorefolder` 参数以及所选组件和包含列表来调用 `Restore` cmdlet。

例如，要从备份中还原两个组策略：

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -GroupPolicies
-IncludeByName Policy1,Policy2
```

还原完整的云站点配置

要还原所有组件或整个云站点，请运行以下命令：

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

用于备份和恢复的自动化配置工具

Automated Configuration 工具命令会触发 Web Studio 使用的备份和还原 API。

`BckRstr` cmdlet 会记录到控制台。不会在 `\Documents\Citrix\AutoConfig` 中创建包含日志信息的文件夹。

注意：

在 Citrix Virtual Apps and Desktops 和 Citrix DaaS™ 中备份配置的先决条件与 PowerShell 会话中的自动化配置工具的先决条件相同。

备份

要在 Delivery Controller 上启动新的备份操作，请在 PowerShell 窗口中运行 `New-BckRstrBackup`。

恢复

要从现有备份中恢复单个组件的成员，请在 PowerShell 窗口中运行 `Restore-BckRstrBackups`。

有关命令的完整列表，请参阅用于备份和恢复的自动化配置工具 cmdlet。

备份和恢复的最佳实践

本文提供了一些建议，可帮助您更好地规划备份和恢复。

类别	最佳实践
安排备份	设置默认备份计划，该计划可以根据您预期站点配置更改的频率，以每日、每周或每月频率运行。将此默认计划设置为不那么活跃的时间段，例如周末或午夜。有关计划备份的信息，请参阅创建计划备份。

类别	最佳实践
	如果您定义了多个备份计划，并且这些计划可能在同一天运行，请使用“**备份和恢复**”节点上的“**设置**”选项卡将限制重置为每天一次备份。
管理备份	始终固定黄金副本备份，以便在达到 30 个备份限制时保留它们。右键单击备份以固定选定的备份。

常见问题

自定义管理员可以执行备份和恢复吗?

否。备份和恢复功能仅限于具有完全权限的管理员。

我们可以备份选择性组件吗?

否。目前，按需备份和计划备份会备份整个站点配置。组件具有多个依赖项和先决条件。为确保正确解决这些依赖项，您可以完整备份组件。但是，您可以恢复选择性组件。

我们可以下载备份?

目前，使用 ACT 下载备份。您可以从适用于虚拟应用程序和桌面的自动化配置下载 ACT。

我们可以备份和恢复 MCS 目录?

目前，我们无法备份和恢复 MCS 目录。您可以使用 ACT 备份您的 MCS 目录并将其导入到另一个站点。

迁移配置到 Citrix Cloud™

自动化配置工具 (ACT) 允许将 Citrix Virtual Apps and Desktops™ 配置（策略、应用程序、目录、管理员角色、范围及其他）从一个或多个本地站点迁移到 Citrix Cloud 上托管的 Citrix DaaS。它还可用于在不同的云区域或租户之间迁移信息。

此工具可发现并导出一个或多个本地站点，作为一组配置文件，您可以选择对其进行编辑。然后可以将这些文件的配置导入到 Citrix DaaS 中。 迁移分阶段进行，通过多次运行该工具，您可以轻松实现所需的配置状态。

ACT 不仅仅是一个一次性迁移工具。您可以使用它来管理日常云操作，例如：

- 自动化从测试或暂存云帐户到生产云帐户的传输
- 备份和恢复您的配置
- 将一个云环境拆分为多个云

以下 *2 分钟*视频提供了自动化配置的快速概览。

<iframe src="https://www.youtube.com/embed/uyQ9o2L1DXQ" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
有关自动化配置的其他信息，请参阅 Tech Zone 上的 概念验证：自动化配置工具。

要深入了解如何移动部署并为迁移准备本地配置，请参阅 Tech Zone 上的 部署指南：将 Citrix Virtual Apps and Desktops 从本地迁移到 Citrix Cloud。

已知限制

- 通过 Machine Creation Services™ 预配的计算机目录具有特殊注意事项。有关 MCS 的更多信息，请参阅 了解迁移 Machine Creation Services 预配的目录。

迁移配置的先决条件

要从 Citrix Virtual Apps and Desktops™ *导出*配置，您需要：

- Citrix Virtual Apps and Desktops：当前版本及其直接前身，或 Citrix Virtual Apps and Desktops、XenApp and XenDesktop® LTSR：所有版本
- 一台已加入域的计算机，安装了 .NET Framework 4.7.2 或更高版本以及 Citrix PowerShell SDK。此 SDK 会自动安装在 Delivery Controller 上。（要在本地 Delivery Controller 以外的计算机上运行，必须安装 Citrix Studio，因为 Studio 会安装正确的 PowerShell 管理单元。Studio 安装程序可在 Citrix Virtual Apps and Desktops 安装介质 上找到。）

要将配置*导入*到 Citrix DaaS 中，您需要：

- 一台可访问 Citrix Cloud 的计算机。这不必是 Delivery Controller™ 或已加入域的计算机。
- 已预配 Citrix DaaS。
- 一个已安装连接器并已加入与本地设置相同域的活动资源位置。
- 必须允许并提供访问 Citrix Cloud 的站点的连接。有关详细信息，请参阅 系统和连接要求。

> **注意：**
>
> 自动化配置不能安装在 Cloud Connector 系统上。

关键步骤

1. 下载自动化配置工具并查看系统要求。请参阅 下载自动化配置。

2. 使用从 Citrix Cloud 门户生成的 `CustomerName`、`CustomerID` 和 `SecretKey` 值填充 `CustomerInfo.yml` 文件。请参阅 生成客户 ID、客户端 ID 和密钥 和 填充客户信息文件。
3. 如果本地站点包含多个区域，请更新 `ZoneMapping.yml` 文件以将区域映射到 Citrix DaaS 资源位置。请参阅 填充区域映射文件。
4. 如果站点包含多个托管连接，请使用每个迁移到 Citrix DaaS 的主机类型的连接信息更新 `CvadAcSecurity.yml` 文件。如果只有一个主机连接，请使用该主机连接的连接信息更新 `CvadACSecurity.yml` 文件。请参阅 更新主机连接的安全文件。
5. 打开 ACT 并使用 `Export-CvadAcToFile` 命令导出您的本地站点。有关支持迁移的组件列表，请参阅 支持的迁移对象。有关导出步骤的信息，请参阅 导出本地配置。
6. 使用 `Merge-CvadAcToSite` 命令分阶段导入组件。或者，一次性迁移整个站点。确保按照 组件迁移顺序 中列出的顺序迁移组件。有关导入步骤的信息，请参阅 运行导入。
7. 激活云站点。请参阅 激活站点。

下载自动化配置

从 Citrix 下载 下载并安装 Automated Configuration 工具。

升级自动化配置

为防止功能出错，请始终使用最新版本的 ACT。

要了解您的工具版本，请执行以下操作：

1. 双击 **Auto Config** 图标。将显示一个 PowerShell 窗口。
2. 运行以下命令以检查您的版本号。

```
Get-CvadAcStatus
```

3. 将您的工具版本与 Citrix 下载 中列出的版本进行比较。最新版本的工具位于该处。
4. 下载并安装最新版本的工具。您*无需*卸载旧版本即可升级 Automated Configuration。

注意：

在 Automated Configuration 中运行 cmdlet 以访问云时，如果有可供下载的新版本，该工具会提醒您。有关 cmdlet 的更多信息，请参阅 Automated Configuration 工具 cmdlet。

生成客户 ID、客户端 ID 和密钥

要将本地站点迁移到 Citrix DaaS，请使用 Citrix Cloud 门户中的客户 ID、客户端 ID 和密钥填充 `CustomerInfo.yml` 文件。

要检索客户 ID：

1. 登录您的 Citrix Cloud 帐户并选择客户。
2. 单击网格图标并选择 **身份和访问管理**。
3. 导航到 **API 访问 > 安全客户端**。客户 ID 将显示在该页面上。

要检索客户端 ID 和密钥：

1. 在“**安全客户端**”页面上，在框中输入一个名称。此名称用于区分多个客户端 ID 和密钥。
2. 单击“创建客户端”以创建客户端 ID 和密钥。
3. 将客户端 ID 和密钥复制到安全位置，并下载包含此信息的 `.csv` 文件。使用 `.csv` 文件填充 `CustomerInfo.yml` 文件。

> **注意：**
>
> - 客户端 ID 和密钥不会过期。如果它们遭到泄露，请立即使用“**垃圾桶**”图标将其删除并创建新的。
> - 如果密钥丢失或遗忘，则无法检索；必须创建新的客户端 ID 和密钥。

填充客户信息文件

`CustomerInfo.yml` 文件消除了每次运行 cmdlet 时都需要提供客户信息参数的需要。可以使用 cmdlet 参数覆盖任何客户信息。

使用 `New-CvadAcCustomerInfoFile` cmdlet 创建 `CustomerInfo.yml` 文件。

> **重要提示：**
>
> 不要手动编辑 `CustomerInfo.yml` 文件。这样做可能会导致意外的格式错误。

> `New-CvadAcCustomerInfoFile` cmdlet 具有以下必需参数。

- CustomerId: 客户 ID。

- ClientId: 在 Citrix Cloud 上创建的客户客户端 ID。
- Secret: 在 Citrix Cloud 上创建的客户密钥。

示例：

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId
6813EEA6-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaaw==
```

您还可以使用指向下载的 `security.csv` 文件的 `SecurityCsvFileSpec` 参数创建 `CustomerInfo.yml`。您还必须指定 CustomerId。

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:
\Users\my_user_name\downloads/security.csv -CustomerId markhof123
```

使用 `Set-CvadAcCustomerInfoFile` cmdlet 更新 `CustomerInfo.yml` 文件。此 cmdlet 仅更改客户端 ID。

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

以下是 CustomerInfo.yml 文件的示例。

```
# Created/Updated on 2020/01/29 16:46:47

CustomerId: 'markhof123'

ClientId: '6713FEA6-46CC-4F8A-BC71-539F2DDK5384'

Secret: 'TwBLaaabbbaaaaaaaaaaw=='

Environment: Production

AltRootUrl: ''

StopOnError: False

AlternateFolder: ''

Locale: 'en-us'

Editor: 'C:\Program Files\Notepad++\notepad++.exe'
```

```
Confirm: True

DisplayLog: True
```

填充区域映射文件

本地区域等同于云资源位置。与其他站点组件不同，您无法自动将本地区域导入到云中。相反，必须使用 `ZoneMapping.yml` 文件手动映射。如果区域名称未与现有资源位置名称关联，则可能会发生导入失败。

如果本地站点只有一个区域且云站点只有一个资源位置，则自动化配置工具会建立正确的关联，从而无需手动管理 `ZoneMapping.yml` 文件。

但是，如果本地站点有多个区域或云站点有多个资源位置，则手动更新 `ZoneMapping.yml` 文件以反映本地区域到云资源位置的正确映射。

`ZoneMapping.yml` 文件位于 `%HOMEPATH%\Documents\Citrix\AutoConfig` 中。`.yml` 文件的内容是一个字典，其中区域名称作为键，资源位置名称作为值。

例如，一个具有名为“Zone-1”的主区域和名为“Zone-2”的辅助区域的本地 Citrix Virtual Apps and Desktops 站点将迁移到具有两个新创建的云资源位置（名为“Cloud-RL-1”和“Cloud-RL-2”）的 Citrix DaaS 部署。在这种情况下，ZoneMapping.yml 将按如下方式配置：

```
            Zone-1: Cloud-RL-1



            Zone-2: Cloud-RL-2
```

注意：

在冒号和资源位置名称之间添加一个空格。如果区域或资源位置名称中包含空格，请用引号将名称括起来。

更新主机连接的安全文件

可以使用 ACT 导出和导入主机连接及其关联的管理程序。

将管理程序添加到主机连接需要特定于管理程序类型的安全信息。出于安全考虑，此信息无法从本地站点导出。您必须手动提供信息，以便自动化配置能够成功地将主机连接和管理程序导入到云站点。

导出过程会在 `%HOMEPATH%\Documents\Citrix\AutoConfig` 中创建 `CvadAcSecurity.yml` 文件，其中包含特定管理程序类型所需的每个安全项目的占位符。在导入到云站点之前，您必须更新 `CvadAcSecurity.yml` 文件。管理员更新会在多次导出中保留，并根据需要添加新的安全占位符。安全项目永远不会被删除。有关详细信息，请参阅手动更新 CvadAcSecurity.yml 文件

```
HostConn1:

ConnectionType: XenServer®

UserName: root

PasswordKey: rootPassword

HostCon2:

ConnectionType: AWS

ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH

SecretKey: TwBLaaaaaaaaaaaaaaaaw==

Region: East
```

每个管理程序的安全信息

以下列出了每种管理程序类型所需的安全信息。

- XenServer、超V、威睿
  - 用户名
  - 明文密码
- 微软 Azure
  - 订阅 ID
  - 应用程序 ID
  - 应用程序密钥

- AWS
  - 服务账户 ID
  - 应用程序密钥
  - 区域

特殊安全注意事项

所有安全信息均以明文形式输入。如果不建议使用明文，则可以使用 **Studio** 手动创建主机连接和关联的管理程序。主机连接和管理程序名称必须与其本地对应项完全匹配，以便可以成功导入使用主机连接的计算机目录。

导出您的 Citrix Virtual Apps and Desktops 本地配置

使用 `export` PowerShell 命令，您可以导出现有的本地配置并获取必要的 `.yml` 文件。这些文件用于将所需的配置导入 Citrix Cloud。

支持的迁移对象

自动化配置支持移动以下组件的配置：

- 标签
- 委派管理
  - 范围
  - 角色
- 主机连接
  - 单个资源池
  - 管理范围
- 计算机目录
  - 管理范围
  - 计算机
  - 远程电脑访问、物理、池化、预配、MCS、分配
- StoreFront™
- 交付组
  - 访问策略

    - 管理范围关联
    - 应用程序访问策略
    - 分配策略
    - 授权/桌面策略
    - 电源计划
    - 会话延迟
    - 会话预启动
    - 重启计划
    - 标签
- 应用程序组
    - 管理范围关联
    - 交付组
    - 用户和组
- 应用程序
    - 应用程序文件夹
    - 图标
    - 应用程序
    - Broker 配置的 FTA
    - 标签
- 组策略
- 用户区域首选项

导出本地配置

1. 双击 **Auto Config** 图标。将显示一个 PowerShell 窗口。
2. 运行以下命令以导出所有组件。导出本地配置 *不会* 以任何方式更改它。

```
Export-CvadAcToFile
```

首次运行任何 cmdlet 后，将创建一个包含 `.yml` 配置文件和日志的导出文件夹。该文件夹位于 `%HOMEPATH%\Documents\Citrix\AutoConfig`。每次后续导出都会创建一个子文件夹。父文件夹 `%HOMEPATH%\Documents\Citrix\AutoConfig` 始终包含最新导出的文件。

> **注意：**
>
> 如果 Delivery Controller 上未安装 Automated Configuration，请在使用 PowerShell 工具之前运行 `import-module Citrix.AutoConfig.Commands`。如果使用 **Auto Config** 图标打开 Automated Configuration，则不需要此步骤。
>
> 如果遇到任何错误或异常，请参阅日志文件中的 **Fixups** 部分。

将配置导入 Citrix DaaS

> **重要提示：**
>
> - 将本地部署迁移到云时，请确保包含 Citrix 设置的域和 OU GPO 已迁移到云。Citrix Web Studio™ 不支持 GPMC，因此域和 OU GPO 在 Web Studio 中不可见。Citrix 策略引擎对位于域和 OU 中的 VDA 和用户强制执行域和 OU GPO。登录 VDA 后，用户可能会看到域和 OU GPO 中的策略已应用于其会话。但是，管理员无法看到这些策略和设置，这可能会导致混淆。

组件迁移顺序

此处列出了组件及其依赖项。组件的依赖项必须在导入或合并之前就位。如果缺少依赖项，可能会导致导入或合并命令失败。如果导入或合并失败，日志文件的 **Fixups** 部分会显示缺少的依赖项。

1. 标签
   - 无前置依赖项
2. 委派管理
   - 无前置依赖项
3. 主机连接
   - CvadAcSecurity.yml 中的安全信息

4. 计算机目录
    - Active Directory 中存在的计算机
    - 主机连接
    - 标签
5. StoreFront
6. 交付组
    - Active Directory 中存在的计算机
    - Active Directory 中存在的用户
    - 计算机目录
    - 标签
7. 应用程序组
    - 交付组
    - 标签
8. 应用程序
    - 交付组
    - 应用程序组
    - 标签
9. 组策略
    - 交付组
    - 标签
10. 用户区域首选项

运行导入

1. 双击 **Auto Config** 图标。将出现一个 PowerShell 窗口。
2. 运行以下命令以导入所有组件。

```
Merge-CvadAcToSite
```

使用新的当前状态验证预期状态。各种导入选项控制导入结果是与本地站点相同还是其子集。

运行 cmdlet 后，将创建一个包含 `.yml` 配置文件和日志的导出文件夹。该文件夹位于 `%HOMEPATH%\Documents\Citrix\AutoConfig`。

如果遇到任何错误或异常，请参阅日志文件中的 **Fixups** 部分。

> **注意：**
>
> 如果 Delivery Controller 上未安装 Automated Configuration，请在使用 PowerShell 工具之前运行 `import-module Citrix.AutoConfig.Commands`。如果您使用 **Auto Config** 图标打开 Automated Configuration，则无需执行此步骤。

要恢复到原始 Citrix DaaS 配置，请参阅备份 Citrix DaaS 配置。

了解导入操作

导入过程旨在准确执行更新，仅执行必要的更新并验证所有更新均已正确完成。所有导入操作都遵循以下步骤：

1. 读取导出的 .yml 文件（预期状态）。
2. 读取云（当前状态）。
3. 将导入前的云状态备份到 .yml 文件（如有必要，可以恢复预备份）。
4. 评估预期状态和当前状态之间的差异。这决定了要进行哪些更新。
5. 进行更新。
6. 重新读取云（新的当前状态）。
7. 将导入后的云状态备份到 .yml 文件（如有必要，可以恢复后备份）。
8. 将新的当前状态与预期状态进行比较。
9. 报告比较结果。

精细迁移

> **重要提示：**
>
> 有关组件迁移顺序的更多信息，请参阅组件迁移顺序。

您可以仅选择性地迁移组件，甚至仅迁移组件名称。

- 支持的组件参数包括 `MachineCatalogs`、`Tags` 等。
- 支持的组件名称参数包括 `IncludeByName` 和 `ExcludeByName` 参数以及其他参数。

有关参数及其使用方法的更多信息，请参阅精细迁移参数。

激活站点

本地和云站点中的交付控制器都控制着资源，例如代理桌面、应用程序和重新启动计算机。当一组通用资源由两个或更多站点控制时，就会出现问题。这种情况可能在从本地站点迁移到云站点时发生。本地和云交付控制器都可能管理同一组资源。这种双重管理可能导致资源变得不可用和无法管理，并且难以诊断。

站点激活允许您控制活动站点的控制位置。

站点激活通过交付组维护模式进行管理。当站点处于非活动状态时，交付组将置于维护模式。对于活动站点，将从交付组中移除维护模式。

站点激活不影响或管理 VDA 注册或计算机目录。

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

所有 cmdlet 都支持 `IncludeByName` 和 `ExcludeByName` 筛选。此参数允许您选择哪些交付组可以更改其维护模式。可以根据需要选择性地更改交付组。

导入并将控制权转移到云端

以下是关于如何从本地站点导入并转移控制到云站点的高级描述。

1. 将本地站点导出并导入到云中。确保任何导入 cmdlet 上都不存在 `-SiteActive` 参数。本地站点处于活动状态，云站点处于非活动状态。默认情况下，云站点交付组处于维护模式。
2. 验证云内容和配置。
3. 在非工作时间，将本地站点设置为非活动状态。`-SiteActive` 参数必须不存在。所有本地站点交付组都处于维护模式。
    - `Set-CvadAcSiteActiveStateOnPrem`
4. 将云站点设置为活动状态。`-SiteActive` 参数必须存在。没有云站点交付组处于维护模式。
    - `Set-CvadAcSiteActiveStateCloud -SiteActive`
5. 验证云站点处于活动状态，本地站点处于非活动状态。

将控制权转回本地站点

要将控制权从云站点转移到本地站点：

1. 在非工作时间，将云站点设置为非活动状态。所有云站点交付组都处于维护模式。
    - `Set-CvadAcSiteActiveStateCloud`
2. 将本地站点设置为活动状态。没有本地站点交付组处于维护模式。
    - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

其他站点激活信息

- 如果没有进行电源管理的计算机，也没有重启计划（这通常意味着也没有主机连接），则所有云交付组都可以作为活动组导入。导入后，将 `-SiteActive` 添加到 `Merge-CvadAcToSite` / `Import-CvadAcToSite` 或运行 `Set-CvadAcSiteActiveStateCloud -SiteActive`。
- 如果计算机已进行电源管理或存在重启计划，则需要不同的过程。例如，在这种情况下从本地切换到云时，使用 `Set-CvadAcSiteActiveStateOnPrem` 将本地站点设置为非活动状态。然后，使用 `Set-CvadAcSiteActiveStateCloud -SiteActive` 将云站点设置为活动状态。
- `Set-CvadAcSiteActiveStateCloud` 和 `Set-CvadAcSiteActiveStateOnPrem` cmdlet 也用于反转此过程。例如，运行不带 `-SiteActive` 参数的 `Set-CvadAcSiteActiveStateCloud`，然后运行带 `-SiteActive` 参数的 `Set-CvadAcSiteActiveStateOnPrem`。

了解迁移 Machine Creation Services 预配的目录

> **注意：**
>
> 此功能仅在 3.0 及更高版本中可用。通过在 Automated Configuration 中使用 `Get-CvadAcStatus` 检查您的版本。

> Machine Creation Services (MCS) 目录创建两种不同类型的目录：

- 当对计算机所做的更改丢失或恢复时（通常是发布应用程序的服务器操作系统）– 这是一种池化 VDI / 多会话用例
- 当对计算机所做的更改在重启后保留时（通常是具有专用用户的客户端操作系统）– 这是一种静态 VDI 用例

可以在 Citrix Studio 的目录节点中查看目录的“用户数据:”值来确认目录类型。

> **注意：**
>
> 无法使用 Automated Configuration 从云中备份 MCS。

池化 VDI / 多会话目录

带有“用户数据: 丢弃”的目录是池化 VDI 目录，只能迁移主映像和配置。这些目录中的任何虚拟机都不会被迁移。这是因为虚拟机的生命周期由您从中导入的站点维护，这意味着每次计算机开机时，其状态都可能发生变化。这使得导入变得不可能，因为虚拟机的导入数据会很快变得不同步。

当您使用该工具迁移这些目录时，它会创建目录元数据并启动主映像创建，但不会导入任何计算机。

由于此过程的创建时间取决于主映像的大小，因此工具中的导入命令仅启动 MCS 目录创建，而不等待其完成。导入完成后，请使用云部署中的 Studio 监视目录创建进度。

主映像创建完成后，您可以预配计算机。请考虑容量因素，因为您的本地使用会消耗容量。

使用该目录的所有其他对象（交付组、应用程序、策略等）都可以导入，无需等待主映像创建。目录创建完成后，可以将计算机添加到导入的目录中，然后用户可以启动其资源。

> **注意：**
>
> 使用工具中可用的相同命令来迁移目录和所有其他对象。

静态 VDI 目录

> **注意：**
>
> 由于此操作会导入存储在数据库中的低级详细信息，因此必须从具有数据库访问权限的计算机运行此过程。

> 静态 VDI 目录会迁移主映像、配置和所有虚拟机。与池化 VDI 用例不同，无需创建任何映像。

VDA 必须指向连接器才能向云注册。

请参阅激活站点部分，以激活云站点，从而使重新启动计划、电源管理和其他项目由云控制。

迁移完成后，如果您想从本地站点删除此目录，则必须选择**保留 VM 和 AD 帐户**。否则，它们将被删除，云站点将指向已删除的 VM。

迁移后更新 MCS 标签以检测孤立资源

将本地配置迁移到云站点，或将云配置迁移到另一个云站点后，对于持久性 VM，您必须更新 MCS 站点 ID 标签，以便正确检测孤立资源。为此，请使用 PowerShell 命令 `Set-ProvResourceTags`。目前，此功能适用于 Azure。

详细步骤如下：

1. 使用新的 Citrix 站点更新 MCS 站点 ID 标签，使用 PowerShell 命令 `Set-ProvResourceTags`。例如：

   ```
   Set-ProvResourceTags -ProvisioningSchemeUid xxxxx  [-VMName <String>]
   [-VMBatchSize XX] [-ResourceType XX]
   ```

   或者，

   ```
   Set-ProvResourceTags -ProvisioningSchemeName xxxxx  [-VMName <String>]
   [-VMBatchSize XX] [-ResourceType XX]
   ```

参数详细信息如下：

- `ProvisioningSchemeUid` 或 `ProvisioningSchemeName` 是强制参数。
- `VMName` 是可选参数。如果未指定 `VMName`，则更新此计算机目录中所有 VM 的标签。
- `VMBatchSize` 是一个可选参数，用于将所有 VM 分批。如果未指定 `VMBatchSize`，则应用默认值 (10)。范围是 1 到 60。
- `ResourceType` 可以是以下之一：
  - `MachineCatalog`：用于更新计算机目录资源的标签。
  - `VirtualMachine`：用于更新 VM 相关资源的标签。
  - `All`：（默认 ResourceType）：用于更新计算机目录和 VM 相关资源的标签。

将多个站点合并为一个站点

自动化配置的多站点支持提供了一种将多个本地站点合并到一个云站点的方法。

多站点支持为每个本地站点的组件名称添加唯一的名称前缀和后缀，以确保在将多个本地站点合并到一个云站点后名称的唯一性。

可以为每个本地站点的以下组件分配前缀和后缀。

- `AdminScope`
- `AdminRole`
- `ApplicationAdmin`
- `ApplicationFolder`
- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`
- `GroupPolicy`
- `HostConnection`
- `MachineCatalog`
- `StoreFront™`
- `Tag`

应用程序文件夹支持添加前缀、添加后缀和重新根目录。重新根目录会将一个额外的顶级文件夹添加到应用程序的现有文件夹结构中。

前缀和后缀规则

1. 前缀和后缀不能包含以下任何特殊字符：`\ , / ; : # . * ? = < > | ( ) " ' { } [ ]`
2. 前缀和后缀可以包含尾随空格，但不能包含前导空格。
3. 前缀和后缀必须用双引号引起来才能包含尾随空格。
4. 前缀和后缀在导入、合并和添加时应用。源 .yml 文件永远不会被修改。
5. 前缀和后缀处理会在适用时自动为依赖组件名称添加前缀或后缀。例如，如果计算机目录名称以“East”为前缀，则引用它们的交付组也将以“East”为前缀。
6. 如果组件名称已以前缀或后缀开头，则不会添加任何前缀或后缀。组件名称不能包含两个相同的重复前缀或后缀。
7. 前缀和后缀可以单独使用，也可以组合使用。
8. 在组件上使用前缀或后缀是可选的。

> **注意：**

> Studio 按字母顺序显示组件。

按站点对组件进行分组

使用前缀来直观地对来自单个站点的组件进行分组。每个站点都列在其自己的组中，前缀按字母顺序控制不同站点组的排序。

按名称分组组件

使用后缀来直观地分组来自多个站点的同名组件。来自不同站点的同名组件会交替显示。

前缀和后缀映射文件

站点前缀设置从 SiteMerging.yml 文件开始，该文件包含一个或多个本地站点的站点前缀和后缀映射。您可以手动管理 SiteMerging.yml 文件，也可以使用 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/manage-deployment/auto-config-cmdlets-migration.html#merging-multiple-on-premises-sites-cmdlets) 部分中列出的可用 cmdlet。

导出本地站点

只有在导出本地站点后才能开始合并。要导出本地站点，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/manage-deployment/migrate.html#export-on-premises-configuration)。

中央导出目标文件夹

本节中描述的方法将多个站点导出放置到中央文件共享位置。`SiteMerging.yml` 文件、`CustomerInfo.yml` 文件和所有导出文件都驻留在该文件共享位置，这使您能够从一个独立于本地站点的位置执行导入。

云访问操作从不引用本地站点或 Active Directory，因此您可以在任何地方执行云访问操作。

直接文件共享

有两种方法可以实现此目的：

- (#direct-file-share)：要从直接文件共享导入、合并或添加，您必须决定要从哪台计算机执行云访问操作。
- 使用 `SiteMerging.yml` 的文件共享引用：此方法使用站点前缀集中的 `SiteRootFolder` 成员，并降低在导出、导入、合并或添加时定位到错误文件夹的几率。

如果您不使用中央文件共享方法，则从各个 Delivery Controller 执行导入、合并或添加。在迁移到云的每个 Delivery Controller 上创建并复制 `SiteMerging.yml` 文件。默认位置是 `%HOMEPATH%\Documents\Citrix\AutoConfig`。您必须指定 `-SiteName` 参数才能选择正确的站点前缀。

直接文件共享

导出、导入、合并和新建/添加操作提供了一个参数，用于指定除默认文件夹 *%HOMEPATH%\Documents\Citrix\AutoConfig* 之外的目标或源文件夹。以下示例使用位于 `\\share.central.net` 的中央文件共享，管理员已拥有访问权限，并已根据需要提供了凭据。

要将导出目标设定为特定站点文件夹，请使用 `–TargetFolder` 参数：

从东部交付控制器™::

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\SiteEast
```

从西部交付控制器::

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\SiteWest
```

导出完成后，创建 `CustomerInfo.yml` 和 `SiteMerging.yml` 文件并将其放置在 `\\share.central.net\AutoConfig` 中。

> **注意：**
>
> 使用此直接文件共享引用方法时，创建 `SitePrefixes.yml` 时请勿使用 `SiteRootFolder` 参数。
>
> 要从直接文件共享导入、合并或添加，您必须决定要从哪台计算机执行云访问操作。选项包括：

- 其中一台已安装该工具的本地 Delivery Controller。
- 托管文件共享的计算机。
- 另一台计算机。

自动化配置必须安装在访问云的计算机上。既不使用本地 PowerShell SDK、交付控制器，也不使用 Active Directory，因此访问云的执行要求比导出要求更简单。

要将东部交付控制器合并到云中：

`Merge-CvadAcToSite –SiteName East –SourceFolder \`
`\share.central.net\AutoConfig\SiteEast -CustomerInfoFileSpec \`
`\share.central.net\AutoConfig\CustomerInfo.yml`

要将西部交付控制器合并到云中：

`Merge-CvadAcToSite –SiteName West –SourceFolder \`
`\share.central.net\AutoConfig\SiteWest -CustomerInfoFileSpec \`
`\share.central.net\AutoConfig\CustomerInfo.yml`

以下是上一个示例中使用的 `SitePrefixes.yml` 示例文件。

```
East:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"

  HostConnectionPrefix: "East_"

  MachineCatalogPrefix: "East_"

  StoreFrontPrefix: "East_"

  TagPrefix: "East_"
```

```
  AdminScopeSuffix: "_east"

  AdminRoleSuffix: "_east"

  ApplicationAdminSuffix: "_east"

  ApplicationFolderSuffix: "_east"

  ApplicationGroupSuffix: "_east"

  ApplicationUserSuffix: "_east"

  DeliveryGroupSuffix: "_east"

  GroupPolicySuffix: "_east"

  HostConnectionSuffix: "_east"

  MachineCatalogSuffix: "_east"

  StoreFrontSuffix: "_east"

  TagSuffix: "_east"

West:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "Western "

  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "
```

```
DeliveryGroupPrefix: "Western "

GroupPolicyPrefix: "Western "

HostConnectionPrefix: "Western "

MachineCatalogPrefix: "Western "

StoreFrontPrefix: "Western "

TagPrefix: "Western "

AdminScopeSuffix: ""

AdminRoleSuffix: ""

ApplicationAdminSuffix: ""

ApplicationFolderSuffix: ""

ApplicationGroupSuffix: ""

ApplicationUserSuffix: ""

DeliveryGroupSuffix: ""

GroupPolicySuffix: ""

HostConnectionSuffix: ""

MachineCatalogSuffix: ""

StoreFrontSuffix: ""

TagSuffix: ""
```

使用 SiteMerging.yml 的文件共享引用

此方法使用站点前缀集中的 `SiteRootFolder` 成员。虽然此方法比直接文件共享方法更复杂，但它降低了在导出、导入、合并或添加时定位错误文件夹的可能性。

首先，在 SiteMerging.yml 文件中为每个站点设置 `SiteRootFolder`。您必须在共享位置执行此操作。

```
New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \
\share.central.net\AutoConfig\SiteEast -SitePrefixesFolder \
\share.central.net\AutoConfig
```

```
New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest
-SitePrefixesFolder \\share.central.net\AutoConfig
```

在此示例中，East 是完全限定的文件夹规范，而 West 是相对文件夹规范。

要使用 SiteMerging.yml 文件将导出目标设置为特定于站点的文件夹，请执行以下操作：

从东部交付控制器：

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile -SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

来自西部交付控制器：

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

导出 cmdlet 使用 `CustomerInfo.yml` 文件夹位置来查找 `SiteMerging.yml` 文件。对于东部，`SiteRootFolder` 是完全限定的。它按原样使用。对于西部，`SiteRootFolder` 不是完全限定的。它与 `CustomerInfo.yml` 文件夹位置结合使用，以检索西部的完全限定文件夹位置。

要将 East Delivery Controller 合并到云中：

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

要将 West Delivery Controller 合并到云中：

```
Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

以下是上一个示例中使用的 `SitePrefixes.yml` 示例文件。

```
  East:

  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"

  HostConnectionPrefix: "East_"

  MachineCatalogPrefix: "East_"

  StoreFrontPrefix: "East_"

  TagPrefix: "East_"

  AdminScopeSuffix: "_east"

  AdminRoleSuffix: "_east"

  ApplicationAdminSuffix: "_east"

  ApplicationFolderSuffix: "_east"

  ApplicationGroupSuffix: "_east"

  ApplicationUserSuffix: "_east"
```

```
  DeliveryGroupSuffix: "_east"

  GroupPolicySuffix: "_east"

  HostConnectionSuffix: "_east"

  MachineCatalogSuffix: "_east"

  StoreFrontSuffix: "_east"

  TagSuffix: "_east"

West:

  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"

  AdminScopePrefix: "Western "

  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "

  MachineCatalogPrefix: "Western "

  StoreFrontPrefix: "Western "

  TagPrefix: "Western "
```

```
AdminScopeSuffix: ""

AdminRoleSuffix: ""

ApplicationAdminSuffix: ""

ApplicationFolderSuffix: ""

ApplicationGroupSuffix: ""

ApplicationUserSuffix: ""

DeliveryGroupSuffix: ""

GroupPolicySuffix: ""

HostConnectionSuffix: ""

MachineCatalogSuffix: ""

StoreFrontSuffix: ""

TagSuffix: ""
```

如果未使用集中式文件共享方法，并且从各个交付控制器执行导入、合并或添加操作，则在每个迁移到云中的交付控制器上创建并复制 `SiteMerging.yml` 文件。默认位置为 *%HOMEPATH%\Documents\Citrix\AutoConfig*。您必须指定 `-SiteName` 参数以选择正确的站点前缀。

合并站点

Citrix® 建议分步执行云操作，并在执行下一个云操作之前对每个结果进行完整审查。例如，如果将三个站点合并到一个云站点：

1. 使用适当的 `SiteName` 值将初始站点合并到云中。
2. 在 Studio 中查看结果。
3. 如果结果不正确，请确定问题及其原因，进行更正，然后重新运行合并。如有必要，请删除云组件，并使用 `Remove-CvadAcFromSite` 针对所选组件和成员从头开始。如果结果正确，请继续。
4. 如果初始合并正确，则将第二个站点合并到单个云站点。
5. 重复步骤 2 和 3。

6. 如果第二次合并正确，则将第三个站点合并到单个云站点。
7. 重复步骤 2 和 3。
8. 从用户的角度审查资源，并验证视图处于所需状态。

使用站点前缀删除组件

您可以通过在 `Remove-CvadAcFromSite` cmdlet 的 `-IncludeByName` 参数上使用前缀来选择性地删除单个站点组件。在以下示例中，West Delivery Controller 交付组不正确。要仅删除 West 站点的交付组：

```
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName “Western *”
```

要删除所有 West 组件，请按顺序运行以下 cmdlet。

1. `Remove-CvadAcFromSite –GroupPolicies –IncludeByName “Western *”`
2. `Remove-CvadAcFromSite –Applications –IncludeByName “Western *”`
3. `Remove-CvadAcFromSite – ApplicationGroups –IncludeByName “Western *”`
4. `Remove-CvadAcFromSite –DeliveryGroups –IncludeByName “Western *”`
5. `Remove-CvadAcFromSite –MachineCatalogs –IncludeByName “Western *”`
6. `Remove-CvadAcFromSite –HostConnections –IncludeByName “Western *”`
7. `Remove-CvadAcFromSite –Tags –IncludeByName “Western *”`

要删除 East 组件的组策略，请使用以下后缀：

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName “*_east”
```

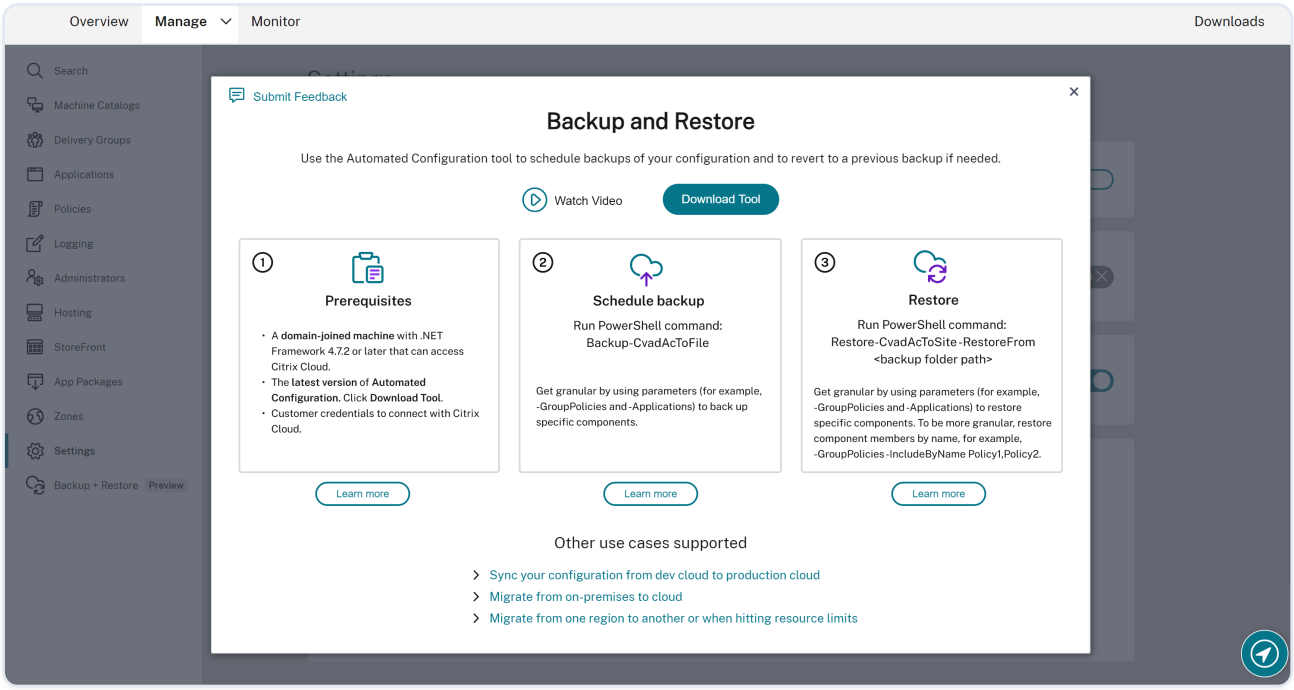
从云到云的迁移

自动化配置允许您自动将云配置移动到另一个云站点，或允许您恢复自己的云站点。

使用自动化配置可以解决许多用例：

- 将您的站点从测试或暂存环境同步到生产环境
- 备份和恢复您的配置
- 达到资源限制
- 从一个区域迁移到另一个区域

在 Citrix Cloud™ 上的 Studio 中，请参阅“备份和恢复”节点，以获取有关自动化配置以及如何使用它将您的配置从云迁移到云的信息。



迁移配置的先决条件

对于备份和恢复您的配置，您需要：

- 已预配 Citrix DaaS™。
- 一个已安装连接器的活动资源位置。
- 必须允许并提供对访问 Citrix Cloud 的站点的连接。有关详细信息，请参阅系统和连接要求。

> **注意：**
>
> 无法使用自动化配置从云中备份 MCS。

备份您的 Citrix DaaS 配置

要求

在备份 Citrix DaaS 配置之前，请执行以下操作：

1. 使用您的客户 ID、客户端 ID 和包含的密钥信息填充 `CustomerInfo.yml` 文件。有关如何检索客户 ID、客户端 ID 和密钥的更多信息，请参阅 生成客户 ID、客户端 ID 和密钥。有关如何将此信息添加到 `CustomerInfo.yml` 文件的信息，请参阅 填充客户信息文件。

运行备份命令时，`CustomerInfo.yml` 必须包含您从中进行备份的源站点客户的详细信息。

运行还原命令时，`CustomerInfo.yml` 必须包含您将配置还原到的目标站点客户的详细信息。

1. 使用映射云中资源位置的信息填充 `ZoneMapping.yml` 文件。有关如何映射区域的更多信息，请参阅 填充区域映射文件。
2. 如果您有主机连接，则必须在 `CvadAcSecurity.yml` 文件中输入相应的信息。请参阅 更新主机连接的安全文件

备份 Citrix DaaS 配置的步骤

1. 安装自动化配置。

> **注意：**
>
> 对于云到云迁移，自动化配置可以安装在管理员可以直接访问的、可访问互联网的计算机上。

2. 双击 **Auto Config** 图标。将显示一个 PowerShell 窗口。
3. 运行以下命令进行备份。

```
Backup-CvadAcToFile
```

首次运行任何 cmdlet 后，将创建一个包含 `.yml` 配置文件和日志的导出文件夹。该文件夹位于 `%HOMEPATH%\Documents\Citrix\AutoConfig`。

如果遇到任何错误或异常，请参阅日志文件中的 **Fixups** 部分。

将配置还原到 Citrix DaaS

1. 双击 **Auto Config** 图标。将显示一个 PowerShell 窗口。
2. 运行以下命令执行还原。

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

将预期状态与新的当前状态进行验证。

运行 cmdlet 后，将创建一个包含 `.yml` 配置文件和日志的导出文件夹。该文件夹位于 *%HOMEPATH%\Documents\Citrix\AutoConfig*。

如果遇到任何错误或异常，请参阅日志文件中的 **Fixups** 部分。

备份和还原过程可保护您免受意外的云站点配置更改或损坏。虽然自动化配置在每次进行更改时都会创建备份，但此备份反映的是更改发生之前云站点配置的状态。为了保护自己，您需要定期备份云站点配置并将其保存在安全的位置。如果发生不希望的更改或损坏，可以使用备份在粒度或完整站点配置级别修复更改或损坏。

精细迁移

> **重要提示：**

> 有关组件迁移顺序的详细信息，请参阅组件迁移顺序。

还原所有组件

还原一个组件涉及选择一个或多个组件参数。

要还原：

- 整个交付组和计算机目录组件
- 完整的云站点配置

请遵循以下示例：

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

还原组件成员

恢复一个或多个组件成员使用 `IncludeByName` 功能。`Restore` cmdlet 与 `RestoreFolder` 参数以及选定的单个组件和包含列表一起调用。

要从备份中恢复两个组策略，请遵循以下示例：

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss



-GroupPolicies -IncludeByName   Policy1,Policy2
```

```
-DeliveryGroups -MachineCatalogs
```

激活站点

站点激活允许您控制哪个站点处于活动状态并控制您的资源。有关详细信息，请参阅激活站点。

将云配置迁移到本地

本文介绍了如何备份您的云配置并将其迁移到本地站点。

迁移配置的先决条件

- 具有至少一个已注册 VDA 的 Citrix Virtual Apps and Desktops™ 本地环境。
- Citrix Virtual Apps and Desktops™ 本地环境，运行以下版本之一：
  - 最新的长期服务版本 (LTSR) - 2402。
  - 任何当前版本 (CR) - 2308、2311。
- 在已加入域且安装了 .Net 4.7.2 或更高版本的计算机上运行自动化配置工具 (ACT) 命令。
- 安装了 Citrix PowerShell SDK 的计算机。PowerShell SDK 包含在 Citrix Delivery Controller™ 安装程序中。

注意：

- 如果您在其他计算机上运行 ACT，则该计算机必须已加入域，并且 Studio 必须安装正确的 PowerShell 管理单元。要获取安装程序，请访问 Citrix Virtual Apps and Desktops下载网站。
- 在本地站点中，我们建议将 ACT 安装在 Delivery Controller 上。ACT 可以通过桌面图标启动。
- 如果打算从标准 Powershell 窗口使用 ACT，则必须执行以下命令：`Import-Module Citrix.AutoConfig.Commands`

ACT 不属于系统 PowerShell 路径的一部分，因此必须显式导入

主要步骤

请按照说明完成将您的云配置迁移到本地环境的操作：

1. 备份云配置
2. 修改 YML 文件
3. 将配置导入到本地

备份云配置

1. 安装 **自动化配置**。
2. 运行 `New-CvadAcCustomerInfoFile` 以创建 **CustomerInfo.yml** 文件。有关更多信息，请参阅填充客户信息文件。
3. 运行命令 `Backup-CvadAcToFile` 以备份您的云配置。

> **注意：**
>
> - 首次运行任何 cmdlet 后，将创建一个包含 .yml 配置文件和日志的导出文件夹。该文件夹位于 `%HOMEPATH%\Documents\Citrix\AutoConfig`。
> - 如果遇到任何错误或异常，请参阅日志文件中的 **Fixups** 部分。
> - Backup-CvadToFile 不支持参数 `IncludeByName` 或 `ExcludeByName`。

> **重要提示：**
>
> Citrix 建议将所有组件一起备份。

修改 YML 文件

修改位于 `%HOMEPATH%\Documents\Citrix\AutoConfig` 的 `.yml` 文件，以包含下表中描述的本地详细信息：

YML 文件	参数	描述	示例
CustomerInfo.yml	环境	将 Environment 更改为 OnPrem。环境参数值区分大小写。	
ZoneMapping.yml	DaaS:CVAD	将您的云资源位置映射到您的本地区域。	它必须是旧区域:新区域

YML 文件	参数	描述	示例
CvadAcSecurity.yml	管理程序: 连接类型: ‘ ‘ 用户名: ‘ ’ 密码: ‘ ‘	添加管理程序用户名和密码。	如果管理程序是 XenServer，XenServer: ConnectionType: ‘XenServer’ Username: ‘root’ Password: ‘ ‘

将配置导入到本地

1. 根据您的要求，在本地站点中运行以下任一命令：
   a. `Merge-CvadAcToSite` - 如果存在正在运行的本地站点，并且您希望将云配置合并到其中。
   b. `Import-CvadAcToSite -Environment OnPrem` - 如果本地配置不可用，并且您正在导入云配置以创建一个新的本地配置。

> **重要提示：**
>
> Citrix 建议一次导入一个组件，以避免冲突。

迁移本地配置到本地站点

本文介绍了使用自动化配置工具 (ACT) 将本地配置从一个站点迁移到另一个本地站点的步骤。

要求

- 两个本地站点必须加入同一域。
- 使用 Citrix Virtual Apps and Desktops™ 2305 版或更高版本。

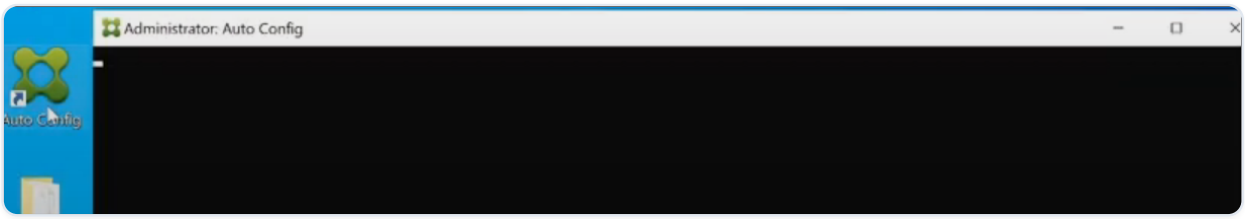
步骤

1. 下载自动化配置工具并查看系统要求。请参阅 下载自动化配置。
2. 打开 ACT 并使用以下命令导出您的本地站点。

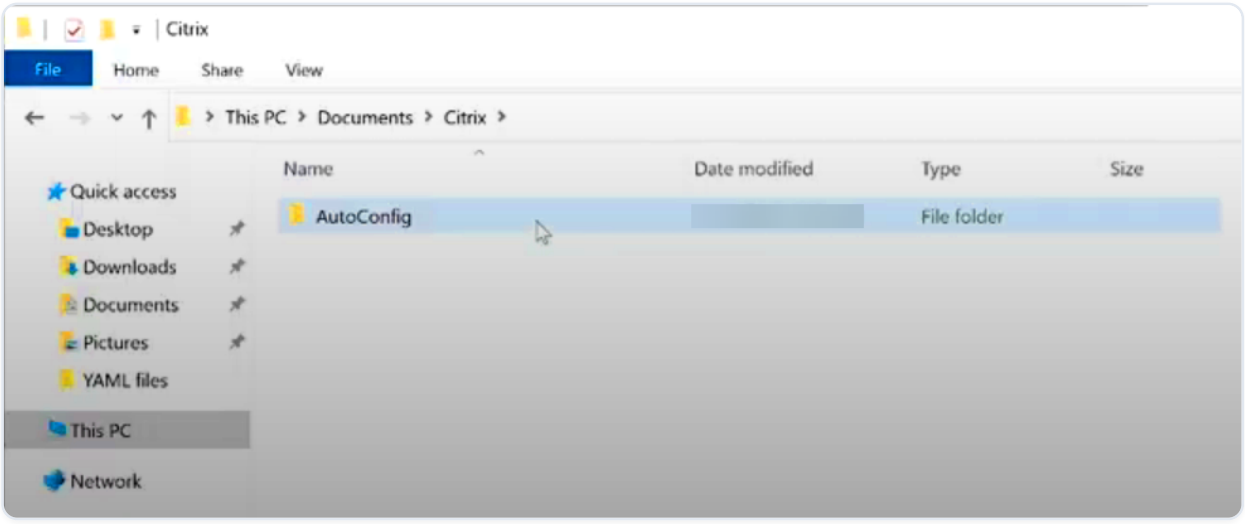
   ```
   Export-CvadAcToFile
   ```

   请参阅 支持的迁移对象 以获取支持迁移的组件列表。有关导出步骤的信息，请参阅 导出本地配置。父文件夹 `%HOMEPATH%\\Documents\\Citrix\\AutoConfig` 始终包含最新导出的文件。

3. 在目标站点上启动 ACT。您应该会看到一个 `AutoConfig` 文件夹创建在 `%HOMEPATH%\\Documents\\Citrix` 中。



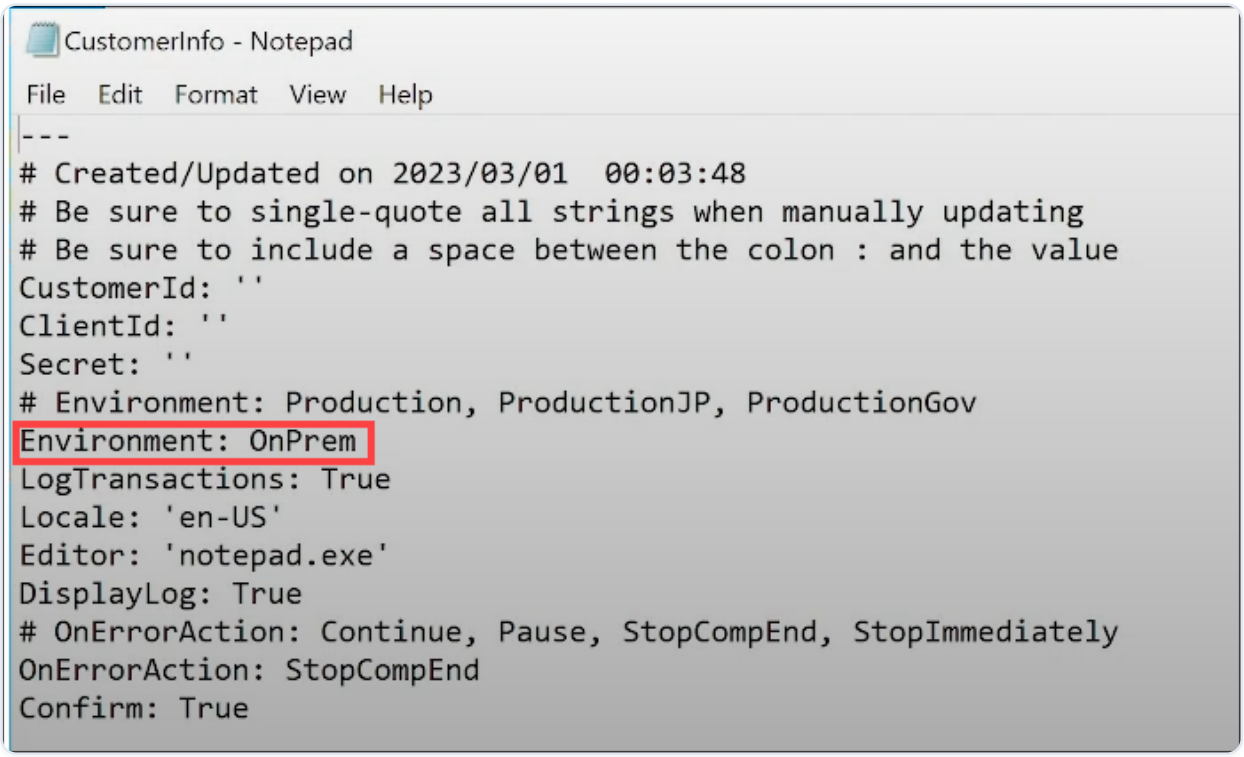
4. 将 `.yml` 文件从源站点的 **Export** 文件夹复制到目标站点的 `%HOMEPATH%\\Documents\\Citrix\\AutoConfig` 文件夹。



5. 使用 `Set-CvadAcCustomerInfoFile` 命令指定您正在使用的环境。例如：

```
Set-CvadAcCustomerInfoFile -Environment OnPrem
```

此命令更新 **CustomerInfo** 文件中的环境信息。



6. 使用以下命令迁移配置文件。

```
Import-CvadAcToFile
```

如果您想从不同的文件夹导入而不是 `AutoConfig` 文件夹，请运行以下命令：

```
Import-CvadAcToFile -Sourcefolder PATH
```

注意：

如果您正在迁移主机连接，则使用每种主机类型的连接信息更新 `CvadAcSecurity.yml` 文件。请参阅 更新主机连接的安全文件。

如果遇到任何错误或异常，请参阅日志文件中的“修复”部分。

7. 使用 Web Studio 验证您的配置是否已迁移到目标站点。

用于迁移的自动化配置工具 cmdlet

此页面列出了该工具支持的所有用于迁移用例的 cmdlet 和参数。

所有 cmdlet 都接受以下类型之一的参数。

- 字符串
- 字符串列表
- 布尔值：`$true` 或 `$false`
- SwitchParameter：参数存在表示 `$true`；参数不存在表示 `$false`

> **注意：**
>
> SwitchParameter 是 true 或 false 选择的首选方法，但由于历史遗留问题，工具中仍使用布尔值。

下表是所有 cmdlet 的摘要。请参阅每个单独的部分，以了解每个 cmdlet 支持哪些参数。

类别	命令	描述
本地到云迁移	`Export-CvadAcToFile`	将本地文件导出到 YAML 文件。
	`Import-CvadAcToSite`	将 YAML 文件导入到云中。支持创建、更新和删除操作。
	`Merge-CvadAcToSite`	将 YAML 文件导入到云中。支持创建和更新操作。
	`New-CvadAcToSite`	将 YAML 文件导入到云中。支持创建和更新操作。
	`Sync-CvadAcToSite`	一步完成导出和导入。
	精细迁移 对于组件，请使用上述命令的参数。示例：`MachineCatalogs`、`Tags`。对于组件名称，请使用上述命令的参数。示例：`IncludeByName`、`ExcludeByName`。	选择性地仅迁移组件或组件名称
云到云 cmdlet	`Backup-CvadAcToFile`	备份云站点中的所有配置。

类别	命令	描述
	`Restore-CvadAcToSite`	将备份的 YAML 文件恢复到云站点。此云站点可以与源云站点相同或不同。
	`Remove-CvadAcFromSite`	从云中移除组件成员。
	精细迁移 对于组件，请使用上述命令的参数。示例：`MachineCatalogs`、`Tags`。对于组件名称，请使用上述命令的参数。示例：`IncludeByName`、`ExcludeByName`。	选择性地仅迁移组件或组件名称
其他基本 cmdlet	`Compare-CvadAcToSite`	比较本地 .yml 文件与云配置。
与先决条件相关的 cmdlet	`New-CvadAcCustomerInfoFile`	创建客户信息文件。
	`Set-CvadAcCustomerInfoFile`	更新现有客户信息文件。
支持和故障排除 cmdlet	`New-CvadAcZipInfoForSupport`	将所有日志和 .yml 文件压缩成一个 zip 文件，发送给 Citrix® 以获取支持。
	`Get-CvadAcStatus`	用于测试连接性并确保满足所有先决条件。返回有关工具的信息，例如版本号以及与云的连接和连接器状态。
	`Test-CvadAcConnectionWithSite`	测试与云站点的连接。
	`Find-CvadAcConnector`	查找现有连接器并确定其运行状态。
	`Get-CvadAcCustomerSites`	返回所有客户站点的列表。

类别	命令	描述
	`New-CvadAcTemplateToFile`	为选定的组件创建模板文件。
	`Show-CvadAcDocument`	在默认浏览器中显示此文档。
	`Find-CvadAcInFile`	“在文件中查找”搜索组件 YAML 文件，查找与一个或多个可能包含通配符的名称匹配的成员。
站点激活 cmdlet	`Set-CvadAcSiteActiveStateOnPrem`	将本地站点的状态设置为活动或非活动。
	`Set-CvadAcSiteActiveStateCloud`	将云站点的状态设置为活动或非活动。
合并多个本地站点 cmdlet	`New-CvadAcSiteMergingInfo`	创建一个站点合并前缀/后缀信息集。
	`Set-CvadAcSiteMergingInfo`	更新现有的站点合并前缀/后缀信息集。
	`Remove-CvadAcSiteMergingInfo`	移除现有站点合并前缀/后缀信息集。

有关参数及其使用方法的更多信息，请参阅精细迁移参数。

基本 cmdlet

本地到云 cmdlet

- `Export-CvadAcToFile` - 将本地文件导出到 YAML 文件。

  从本地设置导出配置。这是自动化配置的默认导出操作。不会对本地站点配置进行任何修改。导出的文件将放置在 *%HOMEPATH%\Documents\Citrix\AutoConfig* 目录中一个唯一命名的 **Export** 子文件夹中。*%HOMEPATH%\Documents\Citrix\AutoConfig* 文件夹始终包含最新导出的本地站点配置。

  参数：

名称	说明	必需？	类型
按组件迁移	请参阅 按组件迁移		开关参数
按对象名称筛选	请参阅按对象名称筛选		字符串列表
`TargetFolder`	指定导出目标文件夹。		字符串
`Locale`	指定可导出的人类可读文本的语言。		字符串
`Quiet`	禁止将日志记录到控制台。		开关参数
`AdminAddress`	指定 Delivery Controller 的 DNS 或 IP 地址，前提是导出未在 Delivery Controller 上运行。		字符串
`CheckUserAndMachines`	验证用户和计算机是否在 Active Directory 中。不在 Active Directory 中的用户和计算机可能会导致导入失败。		`$true` 或 `$false`
`ZipResults`	将备份的 YAML 文件压缩成一个 zip 文件。该文件与备份的 YAML 文件位于同一文件夹中，并与该文件夹同名。		开关参数

返回：

- 请参阅 Cmdlet 返回值

将数据导入云端有三种方式。运行特定的 cmdlet 可能会导致云站点上出现以下三种操作组合之一：

- 添加、更新和删除

- 仅添加和更新
- 仅添加

命令小程序	添加	更新	删除
导入	X	X	X
合并	X	X	
新建	X		

- `Import-CvadAcToSite` - 将 YAML 文件导入到云。支持创建、更新和删除操作。

  将所有本地文件导入到云。此命令可确保云的最终状态与本地状态相同。此选项会删除云中存在的任何更改。导入的站点配置文件源自 *%HOMEPATH%\Documents\Citrix\AutoConfig*。*请谨慎使用。*

  参数：

名称	说明	必需？	类型
按组件迁移	请参阅 按组件迁移 。		开关参数
按对象名称筛选	请参阅 按对象名称筛选。		字符串列表
云访问参数	请参阅 云访问参数 。		开关参数
`SourceFolder`	标识 *%HOMEPATH%\Documents\Citrix\AutoConfig* 的替代根文件夹。		字符串
`Locale`	指定可导出的人类可读文本的语言。		字符串
`Quiet`	禁止将日志记录到控制台。		开关参数

名称	说明	必需？	类型
`DisplayLog`	在 cmdlet 完成时显示日志文件。设置为 `$false` 可禁止显示日志。		`$true` 或 `$false`
`Merge`	设置为 `$true` 时，仅将组件添加到云站点。不删除组件。设置为 `$false` 可删除组件。		`$true` 或 `$false`
`AddOnly`	设置为 `$true` 时，仅添加新组件，不更新或删除现有组件。设置为 `$false` 可允许更新和删除。当此参数为 `$true` 时，将忽略 `Merge`。		`$true` 或 `$false`
`MergePolicies`	合并策略设置和筛选器。仅当要导入的策略已存在于云 DDC 中时，才会发生合并。合并策略的结果是，云 DDC 策略除了包含任何要导入的新设置和筛选器外，还包含其已有的设置和筛选器。请注意，当设置和筛选器发生冲突时，导入的值优先。		开关参数
`OnErrorAction`	请参阅 OnErrorAction parameter。		字符串

返回：

◦ 请参阅 Cmdlet 返回值

- `Merge-CvadAcToSite` - 将 YAML 文件导入到云。支持创建和更新操作。

  将本地文件合并到云中，但不删除云中或本地站点中的任何组件。这会保留云中已进行的更改。如果 Citrix Cloud 中存在同名组件，此命令可以修改该组件。这是自动化配置的默认导入操作。合并的站点配置文件源自 *%HOMEPATH%\Documents\Citrix\AutoConfig*。

  参数：

名称	说明	必需？	类型
按组件迁移	请参阅 按组件迁移 。		开关参数
按对象名称筛选	请参阅 按对象名称筛选。		字符串列表
云访问参数	请参阅 云访问参数 。		开关参数
`SourceFolder`	标识 *%HOMEPATH%\Documents\Citrix\AutoConfig* 的替代根文件夹。		字符串
`Locale`	指定可导出的人类可读文本的语言。		字符串
`Quiet`	禁止将日志记录到控制台。		开关参数
`DisplayLog`	在 cmdlet 完成时显示日志文件。设置为 `$false` 可禁止显示日志。		`$true` 或 `$false`
`Merge`	设置为 `$true` 时，仅将组件添加到云站点。不删除组件。设置为		`$true` 或 `$false`

名称	说明	必需？	类型
	`$false` 可删除组件。		
`AddOnly`	设置为 `$true` 时，仅添加新组件，不更新或删除现有组件。设置为 `$false` 可允许更新和删除。当此参数为 `$true` 时，将忽略 `Merge`。		`$true` 或 `$false`
`MergePolicies`	合并策略设置和筛选器。仅当要导入的策略已存在于云 DDC 中时，才会发生合并。合并策略的结果是，云 DDC 策略除了包含任何要导入的新设置和筛选器外，还包含其已有的设置和筛选器。请注意，当设置和筛选器发生冲突时，导入的值优先。		开关参数
`OnErrorAction`	请参阅 OnErrorAction parameter。		字符串

返回：

- 请参阅 Cmdlet 返回值

- `New-CvadAcToSite` - 将 YAML 文件导入到云。支持创建和更新操作。

  将本地站点配置导入到云，但只添加新组件。现有云站点组件既不更新也不删除。如果您的现有云站点组件必须保持不变，请使用此命令。

  参数：

名称	说明	必需？	类型
按组件迁移	请参阅 按组件迁移 。		开关参数
按对象名称筛选	请参阅 按对象名称筛选。		字符串列表
云访问参数	请参阅 云访问参数 。		开关参数
`SourceFolder`	标识 *%HOMEPATH%\Documents\Citrix\AutoConfig* 的替代根文件夹。		字符串
`Locale`	指定可导出的人类可读文本的语言。		字符串
`Quiet`	禁止将日志记录到控制台。		开关参数
`DisplayLog`	在 cmdlet 完成时显示日志文件。设置为 `$false` 可禁止显示日志。		`$true` 或 `$false`
`OnErrorAction`	请参阅 OnErrorAction parameter。		字符串

返回：

- 请参阅 Cmdlet 返回值

- `Sync-CvadAcToSite` - 一步完成导出和导入。

  Sync 在一步中执行导出和导入。使用 `SourceTargetFolder` 参数指定导出/导入目标文件夹。

  参数：

名称	描述	必需？	类型
按组件迁移	请参阅 按组件迁移		开关参数
按对象名称筛选	请参阅按对象名称筛选		字符串列表
云访问参数	请参阅云访问参数		开关参数
`SourceTargetFolder`	指定导出/导入目标文件夹。		字符串
`Locale`	指定可导出的人类可读文本的语言。		字符串
`AdminAddress`	指定未在交付控制器上执行导出时交付控制器的 DNS 或 IP 地址。		字符串
`Quiet`	禁止将日志记录到控制台。		开关参数
`DisplayLog`	在 cmdlet 完成时显示日志文件。设置为 `$false` 可禁止显示日志。		`$true` 或 `$false`
`Merge`	设置为 `$true` 时，仅将组件添加到云站点。不删除组件。设置为 `$false` 可删除组件。		`$true` 或 `$false`
`AddOnly`	设置为 `$true` 时，仅添加新组件，不更新或删除现有组件。设置为 `$false` 可允许更新和删除。当此参数为 `$true` 时，将忽略 `Merge`。		`$true` 或 `$false`

名称	描述	必需？	类型
`MergePolicies`	合并策略设置和筛选器。仅当要导入的策略已存在于云 DDC 中时，才会发生合并。合并策略的结果是，云 DDC 策略除了包含任何要导入的新设置和筛选器外，还包含其已有的设置和筛选器。请注意，当设置和筛选器发生冲突时，导入的值优先。		开关参数

返回：

- 请参阅 Cmdlet 返回值

云到云 cmdlet

- `Backup-CvadAcToFile` - 备份云站点中的所有配置。

  将您的云配置导出到 .yml 文件。此备份可用于备份和还原过程，以还原丢失的组件。

  参数：

名称	描述	必需？	类型
按组件迁移	请参阅 按组件迁移		切换参数
云访问参数	请参阅 云访问参数		切换参数
`TargetFolder`	指定导出目标文件夹。		字符串
`Locale`	指定可导出的人类可读文本的语言。		字符串
`Quiet`	抑制向控制台记录日志。		切换参数

名称	描述	必需？	类型
`DisplayLog`	在 cmdlet 完成时显示日志文件。设置为 `$false` 以抑制日志显示。		`$true` 或 `$false`
`ZipResults`	将备份的 YAML 文件压缩成一个 zip 文件。该文件与备份的 YAML 文件位于同一文件夹中，并与该文件夹同名。		切换参数

返回内容：

- 请参阅 Cmdlet 返回值

- `Restore-CvadAcToSite` - 将备份的 YAML 文件还原到云站点。此云站点可以与源云站点相同，也可以不同。

  将云站点还原到以前的配置。导入的文件源自使用 `-RestoreFolder` 参数指定的文件夹，该参数标识包含要还原到云站点的 .yml 文件的文件夹。这必须是完全限定的文件夹规范。此 cmdlet 可用于恢复到以前的配置，或用于备份和还原云站点。此命令可以添加、删除和更新您的云站点。

  参数：

名称	描述	必需？	类型
按组件迁移	请参阅 按组件迁移 。		切换参数
按对象名称筛选	请参阅 按对象名称筛选。		字符串列表
云访问参数	请参阅 云访问参数 。		切换参数
`RestoreFolder`	标识包含要还原到云站点的 .yml 文件的文件夹。这必须是完		字符串

名称	描述	必需？	类型
	全限定的文件夹规范。		
`Locale`	指定可导出的人类可读文本的语言。		字符串
`Quiet`	抑制向控制台记录日志。		切换参数
`DisplayLog`	在 cmdlet 完成时显示日志文件。设置为 `$false` 以抑制日志显示。		`$true` 或 `$false`
`Merge`	设置为 `$true` 时，仅将组件添加到云站点。不移除组件。设置为 `$false` 可移除组件。		`$true` 或 `$false`
`AddOnly`	设置为 `$true` 时，仅添加新组件，不更新或删除现有组件。设置为 `$false` 以允许更新和删除。当此参数为 `$true` 时，将忽略 `Merge`。		`$true` 或 `$false`
`MergePolicies`	合并策略设置和筛选器。仅当要导入的策略已存在于云 DDC 中时，才会发生合并。合并策略的结果是，云 DDC 策略除了包含正在导入的任何新设置和筛选器之外，还包含其已有的设置和筛选器。请注意，当设置和筛选器		切换参数

名称	描述	必需？	类型
	发生冲突时，导入的值优先。		
`OnErrorAction`	请参阅 OnErrorAction parameter。		字符串

返回内容：

- 请参阅 Cmdlet 返回值

- `Remove-CvadAcFromSite` – 从云中移除组件成员。

  可以重置整个站点或从组件中移除成员项（例如，从目录列表中移除一个计算机目录）。这可以与 `IncludeByName` 参数结合使用，以选择性地移除特定成员。

  参数：

名称	描述	必需？	类型
按组件迁移	请参阅 按组件迁移		切换参数
按对象名称筛选	请参阅 按对象名称筛选		字符串列表
云访问参数	请参阅 云访问参数		切换参数
`Quiet`	抑制向控制台记录日志。		切换参数
`DisplayLog`	在 cmdlet 完成时显示日志文件。设置为 `$false` 以抑制日志显示。		`$true` 或 `$false`

  返回内容：

  - 请参阅 Cmdlet 返回值

其他基本 cmdlet

- `Compare-CvadAcToSite` - 将本地 .yml 文件与云配置进行比较，生成由 `Import`、`Merge` 或 `Restore` cmdlet 进行的更改报告。

  参数：

名称	描述	必需？	类型
按组件迁移	请参阅按组件迁移。		SwitchParameters
按对象名称筛选	请参阅按对象名称筛选。		字符串列表
云访问参数	请参阅云访问参数。		SwitchParameters
`SourceFolder`	指定 *%HOMEPATH%\Documents\Citrix\AutoConfig* 的替代根文件夹。		字符串
`Locale`	指定可导出的可读文本的语言。		字符串
`Quiet`	抑制向控制台记录日志。		SwitchParameter
`DisplayLog`	在 cmdlet 完成时显示日志文件。设置为 `$false` 可抑制日志显示。		`$true` 或 `$false`
`Merge`	当设置为 `$true` 时，仅将组件添加到云站点。不移除组件。设置为 `$false` 可移除组件。		`$true` 或 `$false`
`AddOnly`	当设置为 `$true` 时，仅添加新组件，不更新或删除现有组件。设置为		`$true` 或 `$false`

名称	描述	必需？	类型
	`$false` 可允许更新和删除。当此参数为 `$true` 时，将忽略 `Merge`。		
`OnErrorAction`	参见 OnErrorAction 参数。		字符串

返回：

- 参见 Cmdlet 返回值

粒度迁移参数

按组件迁移

以下组件可以通过支持它们的 cmdlet 进行指定。当未指定任何组件参数时，`All` 选项会自动选中。为避免错误，我们建议您按以下顺序迁移组件：

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`
- `UserZonePreference`

按对象名称筛选

按组件名称迁移

`IncludeByName` 和 `ExcludeByName` 参数允许按名称在 cmdlet 中包含和排除组件成员。在任何受支持的 cmdlet 中，一次只能选择一个组件（例如，交付组）。如果组件成员同时存在于这两个区域中，则排除将覆盖任何其他参数，并且会在日志修复列表中创建一个条目，用于标识被排除的组件和成员名称。

`IncludeByName` 和 `ExcludeByName` 采用组件成员名称列表。任何名称都可以包含一个或多个通配符。支持两种类型的通配符。当任何成员名称包含特殊字符时，组件成员名称列表必须用单引号括起来。

- * 匹配任意数量的字符
- ? 匹配单个字符

`IncludeByName` 和 `ExcludeByName` 还可以采用一个文件，其中包含成员列表，每个成员可以是显式的或包含通配符。文件中的每一行可以包含一个成员。成员名称中的前导和尾随空格将被去除。文件名必须以 @ 符号开头并用单引号括起来（PowerShell 要求，以避免 @ 被重新解释）。可以列出多个文件，也可以与成员名称混合使用。

合并所有名称以 `DgSite1` 开头并包含 `Home2` 的交付组的示例如下所示：

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

按交付组名称

`ByDeliveryGroupName` 根据应用程序和应用程序组的交付组名称进行筛选。此参数始终是一个包含列表，用于根据其交付组关联来标识要包含的成员。

`ByDeliveryGroupName` 接受交付组名称列表。任何名称都可以包含一个或多个通配符。支持两种类型的通配符。

- * 匹配任意数量的字符
- ? 匹配单个字符

以下示例合并了引用所有以 `EastDg` 开头的交付组名称的所有应用程序。

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

排除已禁用

`ExcludeDisabled` 从导入操作中筛选出所有已禁用的应用程序和应用程序组。
`ExcludeDisabled` 默认为 `false`，这意味着无论其启用状态如何，所有应用程序和应用程序组都将被导入。

按计算机名称

`ByMachineName` 根据计算机目录和交付组的计算机名称进行筛选。此参数始终是一个包含列表，用于根据其计算机名称关联来标识要包含的成员。

`ByMachineName` 接受计算机名称列表，其中任何名称都可以包含一个或多个通配符。支持两种类型的通配符。

- * 匹配任意数量的字符
- ? 匹配单个字符

当导出或导入并使用 `ByMachineName` 且计算机名称筛选器导致计算机目录或交付组中没有计算机时，该计算机目录或交付组将从导出或导入中排除。

> **注意：**
>
> 在任何导入类型 cmdlet 中使用 `ByMachineName` 会导致 `MergeMachines` 设置为 `$true` 。

合并计算机

当 `MergeMachines` 设置为 `$true` 时，它指示导入操作仅将计算机添加到计算机目录或交付组。计算机不会被移除，从而允许增量添加操作。

`MergeMachines` 默认为 false，这意味着如果计算机不在计算机目录或交付组的 .yml 文件中，则会被移除。当使用 `ByMachineName` 时，`MergeMachines` 会设置为 `$true`，但可以通过将 `MergeMachines` 设置为 false 来覆盖此设置。

先决条件相关的 cmdlet

- `New-CvadAcCustomerInfoFile` - 创建客户信息文件。默认情况下，客户信息文件位于 *%HOMEPATH%\Documents\Citrix\AutoConfig*。

  参数:

名称	描述	必需？	类型
`CustomerId`	客户 ID。	x	字符串
`ClientId`	在 Citrix Cloud 上创建的客户客户端 ID。使用此参数时，	有条件地	字符串

名称	描述	必需？	类型
	必须指定 CustomerId 和 Secret。		
`Secret`	在 Citrix Cloud 上创建的客户密钥。使用此参数时，必须指定 CustomerId 和 ClientId。	有条件地	字符串
`Environment`	生产、政府生产或日本生产环境。		枚举
`LogFileName`	将日志文件前缀从 CitrixLog 更改为其他内容。		字符串
`AltRootUrl`	仅在 Citrix 的指导下使用。		字符串
`StopOnError`	在首次出现错误时停止操作。		`$true` 或 `$false`
`TargetFolder`	使用指定的文件夹作为根文件夹，而不是 *%HOMEPATH%\Documents\Citrix\AutoConfig*。		字符串
`Locale`	使用指定的区域设置，而不是从运行该工具的系统派生的区域设置。		字符串
`Editor`	使用指定的编辑器在每个 cmdlet 完成时显示日志。Notepad.exe 是默认编辑器。此参数必须包含编辑器的完全限定文件规范，并且编辑器必须将日志文件		字符串

名称	描述	必需？	类型
	规范作为其唯一参数。		
`SecurityCsvFileSpec`	指向从 Citrix Identity and Access Management 下载的 SecurityClient.csv 文件的完全限定文件规范。使用此参数时必须指定 CustomerId。		字符串

返回：

- 请参阅 Cmdlet 返回值

- `Set-CvadAcCustomerInfoFile` - 更新现有客户信息文件。仅更改 cmdlet 指定的参数。CustomerInfo.yml 文件中所有未指定的参数值保持不变。

  参数:

名称	描述	必需？	类型
`CustomerId`	客户 ID。		字符串
`ClientId`	在 Citrix Cloud 上创建的客户客户端 ID。		字符串
`Secret`	在 Citrix Cloud 上创建的客户密钥。		字符串
`Environment`	生产、政府生产或日本生产环境。		枚举
`LogFileName`	将日志文件前缀从 CitrixLog 更改为其他内容。		字符串

名称	描述	必需？	类型
`StopOnError`	在首次出现错误时停止操作。		`$true` 或 `$false`
`TargetFolder`	使用指定的文件夹作为根文件夹，而不是 *%HOMEPATH%\Documents\Citrix\AutoConfig*。		字符串
`Locale`	使用指定的区域设置，而不是从运行该工具的系统派生的区域设置。		字符串
`Editor`	使用指定的编辑器在每个 cmdlet 完成时显示日志。Notepad.exe 是默认编辑器。此参数必须包含编辑器的完全限定文件规范，并且编辑器必须将日志文件规范作为其唯一参数。		字符串
`SecurityCsvFileSpec`	指向从 Citrix Identity and Access Management 下载的 SecurityClient.csv 文件的完全限定文件规范。使用此参数时必须指定 CustomerId。		字符串

返回：

- 请参阅 Cmdlet 返回值

先决条件相关参数

除了 云访问参数 之外，以下参数可与先决条件相关的 cmdlet 一起使用：

- `Environment` – 生产或 ProductionGov 环境。
- `LogFileName` – 将日志文件前缀从 CitrixLog 更改为其他内容。
- `StopOnError` – 在首次出现错误时停止操作。
- `AlternateRootFolder` – 使用指定的文件夹作为根文件夹，而不是 *%HOMEPATH%\Documents\Citrix\AutoConfig*。
- `Locale` – 使用指定的区域设置，而不是从运行该工具的系统派生的区域设置。
- `Editor` – 使用指定的编辑器在每个 cmdlet 完成时显示日志。Notepad.exe 是默认编辑器。此参数必须包含编辑器的完全限定文件规范，并且编辑器必须将日志文件规范作为其唯一参数。

支持和故障排除 cmdlet

- `New-CvadAcZipInfoForSupport` - 将所有日志文件和 .yml 文件压缩到一个 zip 文件中，以发送给 Citrix 以获取支持。客户敏感信息（CustomerInfo.yml 和 CvadAcSecurity.yml）不包含在 zip 文件中。Icon.yml 文件也因其大小而被排除。zip 文件放置在 *%HOMEPATH%\Documents\Citrix\AutoConfig* 中，并根据日期和时间戳命名为 *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*。此 zip 文件也可以用作备份。

  参数：

名称	描述	必需？	类型
`TargetFolder`	指定用于创建和保存 zip 文件的目标文件夹。		字符串
`Quiet`	禁止向控制台记录日志。		SwitchParameter

  返回:

  - 带有 zip 文件名和位置的 zip 文件显示在命令提示符中。

- `Get-CvadAcStatus` - 用于测试连接性并确保满足所有先决条件。返回有关工具的信息，例如版本号以及与云的连接和连接器状态。

  参数：

名称	描述	必需？	类型
云访问参数	请参阅 云访问参数		开关参数

名称	描述	必需？	类型
`SiteId`	标识要连接的站点。		字符串
`AdminAddress`	这是用于验证管理员访问级别的本地 Delivery Controller 的 DNS 或 IP 地址。如果未在 Delivery Controller 上运行该工具，则需要此项。		字符串

返回:

- 显示每个项目的结果。

- `Test-CvadAcConnectionWithSite` – 测试与云站点的连接，以验证通信连接是否正常工作。此 cmdlet 使用云访问参数或 CustomerInfo.yml 文件来指定客户连接信息。

  参数：

名称	描述	必需？	类型
云访问参数	请参阅 云访问参数		开关参数
`Quiet`	禁止向控制台记录日志。		SwitchParameter

  返回:

  - 测试结果显示在命令行上。

- `Find-CvadAcConnector` - 定位现有连接器并确定其运行状态。此 cmdlet 使用 CustomerInfo.yml 文件中的信息或客户 ID 参数来定位客户的连接器。

  参数：

名称	描述	必需？	类型
`CustomerInfoFileSpec`	指向客户信息文件的文件规范，用于覆盖默认位置和名称。当		字符串

名称	描述	必需？	类型
	提供了 `CustomerId` 参数时，此参数将被忽略。		
`CustomerId`	客户 ID。此参数会覆盖 CustomerInfo.yml 文件中的相同值。		字符串

返回:

- 结果显示在命令行中。

- `Get-CvadAcCustomerSites` - 返回所有客户站点的列表。此 cmdlet 使用云访问参数或 CustomerInfo.yml 文件来指定客户连接信息。

  参数：

  - 请参阅 云访问参数

  返回:

  - 显示找到的客户站点 ID 列表。

- `New-CvadAcTemplateToFile` – 为选定组件创建模板文件，允许您手动创建导入文件。

  参数：

名称	描述	必需？	类型
按组件迁移	请参阅 按组件迁移		开关参数
`TargetFolder`	指定导出目标文件夹。		字符串

  返回:

  - 请参阅 Cmdlet 返回值

- `Show-CvadAcDocument` - 在默认浏览器中显示此文档。

  参数：

- 无。

返回:

- 在默认 Web 浏览器中显示此网页。

- `Find-CvadAcInFile` - 文件内查找会搜索组件 YAML 文件，查找与一个或多个可能包含通配符的名称匹配的成员。结果是找到的成员的报告。文件内查找一次只能搜索一个组件。文件内查找会搜索当前文件夹和所有子文件夹中的所有 YAML 文件。使用 `FindSourceFolder` 限制要搜索的文件数量。

  参数：

名称	描述	必需？	类型
按组件迁移	请参阅按组件迁移。注意：`-All` 值无效。		开关参数
`IncludeByName`	一个列表，指定在将站点活动状态设置为活动时要包含的交付组名称。名称中支持“*”和“?”通配符。		字符串列表
`Unique`	仅报告唯一找到的成员。		SwitchParameter
`IncludeYaml`	包含成员特定的 YAML。		SwitchParameter
`FindSourceFolder`	查找开始搜索的文件夹。		字符串
`DisplayLog`	在 cmdlet 完成时显示日志文件。设置为 `$false` 可禁止显示日志。		SwitchParameter
`Quiet`	禁止向控制台记录日志。		SwitchParameter

  返回：

◦ 为指定组件创建包含已找到成员的报告。

站点激活 cmdlet

有关激活站点和这些 cmdlet 用法的更多信息，请参阅激活站点。

- `Set-CvadAcSiteActiveStateOnPrem` - 将本地站点的状态设置为活动或非活动。

  参数：

名称	描述	是否必需？	类型
云访问参数	请参阅云访问参数		SwitchParameters
`SiteActive`	存在时，将本地站点设置为活动状态，并从所有交付组中移除维护模式。如果此参数不存在，则在所有交付组上设置维护模式。		SwitchParameter
`IncludeByName`	一个列表，指定在将站点活动状态设置为活动时要包括的交付组名称。名称中支持“*”和“?”通配符。		字符串列表
`ExcludeByName`	一个列表，指定在将站点活动状态设置为活动时要排除的交付组名称。名称中支持“*”和“?”通配符。		字符串列表
`Quiet`	抑制向控制台记录日志。		SwitchParameter
`DisplayLog`	在 cmdlet 完成时显示日志文件。设置为 `$false` 可抑制日志显示。		`$true or $false`

  返回值：

- 请参阅 Cmdlet 返回值

- `Set-CvadAcSiteActiveStateCloud` - 将云站点状态设置为活动或非活动。

  参数：

名称	描述	是否必需？	类型
云访问参数	请参阅云访问参数		SwitchParameters
`SiteActive`	如果存在，则将云站点设置为活动状态，从而从所有交付组中移除维护模式。如果此参数不存在，则所有交付组都将设置为维护模式。		SwitchParameter
`IncludeByName`	一个列表，指定在将站点活动状态设置为活动时要包括的交付组名称。名称中支持“*”和“?”通配符。		字符串列表
`ExcludeByName`	一个列表，指定在将站点活动状态设置为活动时要排除的交付组名称。名称中支持“*”和“?”通配符。		字符串列表
`Quiet`	抑制向控制台记录日志。		SwitchParameter
`DisplayLog`	在 cmdlet 完成时显示日志文件。设置为 `$false` 可抑制日志显示。		`$true or $false`

  返回值：

  - 请参阅 Cmdlet 返回值

合并多个本地站点的 cmdlet

有关站点合并和这些 cmdlet 用法的更多信息，请参阅 将多个站点合并到一个站点。

- `New-CvadAcSiteMergingInfo` - 创建站点合并前缀/后缀信息集。最初无需了解所有前缀或后缀。它们可以通过 `Set-CvadAcSiteMergingInfo` 或手动编辑 SiteMerging.yml 文件进行更新。 参数：

名称	描述	是否必需？	类型
`SiteName`	用于标识特定站点的所有前缀/后缀集的名称。它可以与实际站点的名称匹配，但不是必需的。	x	字符串
站点合并参数	请参阅站点合并参数		开关参数
`Quiet`	禁止向控制台记录日志。		开关参数

  返回：

  - 无

- `Set-CvadAcSiteMergingInfo` - 更新现有站点合并前缀/后缀信息集。

  参数：

名称	描述	是否必需？	类型
`SiteName`	用于标识特定站点的所有前缀/后缀集的名称。它可以与实际站点的名称匹配，但不是必需的。	x	字符串
站点合并参数	请参阅站点合并参数		开关参数
`Quiet`	禁止向控制台记录日志。		开关参数

  返回：

  - 无

- `Remove-CvadAcSiteMergingInfo` - 删除现有的站点合并前缀/后缀信息集。

  参数：

  - `SiteName` – 标识站点前缀和后缀集。这是一个字符串，是必需的。

  返回：

  - 无

站点合并参数

运行站点合并 cmdlet 时可以使用以下参数。所有列出的参数均为字符串。

- `SiteName` – 用于标识特定站点的所有前缀/后缀集的名称。它可以与实际站点的名称匹配，但不是必需的。SiteName 是一个必需参数。
- `AdminScopedPrefix` – 应用于管理员范围的前缀。
- `ApplicationPrefix` - 应用于应用程序的前缀。
- `ApplicationFolderPrefix` – 应用于应用程序文件夹的前缀；`ApplicationFolderPrefix` 可以与 `ApplicationFolderRoot` 结合使用。
- `ApplicationFolderRoot` – 应用程序文件夹的新根文件夹。这将创建一个额外的文件夹层次结构。`ApplicationFolderRoot` 可以与 `ApplicationFolderPrefix` 结合使用。
- `ApplicationGroupPrefix` – 应用程序组的前缀。
- `ApplicationUserPrefix` – 应用于用户看到的应用程序名称的前缀。
- `ApplicationAdminPrefix` – 应用于管理员看到的应用程序名称的前缀。
- `DeliveryGroupPrefix` – 应用于交付组的前缀。
- `GroupPolicyPrefix` – 策略名称要应用的前缀。
- `HostConnectionPrefix` – 主机连接要应用的前缀。
- `MachineCatalogPrefix` – 计算机目录要应用的前缀。
- `StoreFrontPrefix` – StoreFront™ 名称要应用的前缀。
- `TagPrefix` – 标签要应用的前缀。
- `AdminScopedSuffix` – 管理员范围要应用的后缀。
- `ApplicationSuffix` - 应用程序要应用的后缀。
- `ApplicationFolderSuffix` – 应用程序文件夹要应用的后缀；`ApplicationFolderSuffix` 可以与 `ApplicationFolderRoot` 结合使用。

- `ApplicationGroupSuffix` – 应用程序组的后缀。
- `ApplicationUserSuffix` – 用户看到的应用程序名称要应用的后缀。
- `ApplicationAdminSuffix` – 管理员看到的应用程序名称要应用的后缀。
- `DeliveryGroupSuffix` – 交付组要应用的后缀。
- `GroupPolicySuffix` – 策略名称要应用的后缀。
- `HostConnectionSuffix` – 主机连接要应用的后缀。
- `MachineCatalogSuffix` – 计算机目录要应用的后缀。
- `StoreFrontSuffix` – 要应用于 StoreFront 名称的后缀。
- `TagSuffix` – 要应用于标签的后缀。
- `SiteRootFolder` – 用于导出和导入的完全限定文件夹名称；这可以是本地文件夹或文件共享。

通用参数

云访问参数

所有访问云的 cmdlet 都支持以下额外参数。

> **注意：**
>
> CustomerId、ClientId 和 Secret 可以放在 CustomerInfo.yml 文件中，也可以使用以下参数通过 cmdlet 指定。当它们在两个位置都指定时，cmdlet 参数优先。

- `CustomerId` – 在 Rest API 中使用的客户 ID，访问所有 Rest API 都需要此 ID。您的客户 ID 位于 Citrix Cloud 中。
- `ClientId` – 在 Citrix Cloud 身份和访问管理网站上创建的 clientID。这是获取所有 Rest API 身份验证所需的持有者令牌所必需的。
- `Secret` – 在 Citrix Cloud 身份和访问管理网站上创建的密钥。这是获取所有 Rest API 身份验证所需的持有者令牌所必需的。
- `CustomerInfoFileSpec` – 指向客户信息文件的文件规范，用于覆盖默认位置和名称。

迁移模式参数

修改云站点配置的 cmdlet (`Import`、`Restore`、`Merge`、`New` 和 `Sync`) 支持以下额外参数，以提供更大的灵活性。

- `CheckMode` – 执行导入操作，但不进行任何更改。所有预期更改都会在导入完成前报告。您可以使用此命令在导入发生前测试导入。
- `BackupFirst` – 在修改云配置之前，将云内容备份到 .yml 文件。此功能默认启用。
- `Confirm` – 如果为 true，则提示用户确认他们要更改云站点配置。`Remove` cmdlet 由于其破坏性，会显示提示。如果不需要提示，例如在自动化脚本中运行，请将其设置为 false。`Confirm` 默认为 true。
- `SecurityFileFolder` – 这是包含 CustomerInfo.yml 文件的完全限定文件夹，该文件可能指向本地文件夹或可能受身份验证控制的网络共享文件夹。该工具不会提示输入凭据；必须在运行该工具之前获取对受控资源的访问权限。
- `SiteName` – 指定导入时要使用的站点合并前缀和后缀集。
- `SiteActive` – 指定导入的站点是活动还是非活动状态。默认情况下，此参数设置为 `$false`，表示导入的站点处于非活动状态。

日志显示参数

`Export`、`Import`、`Sync`、`Restore`、`Backup`、`Compare` 和 `Remove` cmdlet 在操作完成后显示日志文件。您可以通过将 `-DisplayLog` 参数设置为 `$false` 来抑制显示。默认情况下，使用 Notepad.exe 显示日志文件。您可以在 CustomerInfo.yml 文件中指定不同的编辑器。

```
Editor: C:\Program Files\Notepad++\notepad++.exe
```

Cmdlet 返回值

ActionResult

所有 cmdlet 都返回以下值。

```
public class ActionResult

{

    public bool                         Overall_Success;

    public Dictionary&lt;string, string>   Individual_Success;

    public object                       CustomResult;

}
```

`Overall_Success` 返回一个布尔值，显示 cmdlet 在所有选定组件中的总体成功情况：true 表示成功，false 表示不成功。

`Individual_Success` 为每个主要组件返回一个或三个值。组件的结果可以是 Success、Failure 或 Skipped。Skipped 表示该组件未被 cmdlet 选中执行。

`CustomResult` 特定于 cmdlet。

CustomResult

`Import`、`Merge`、`Restore`、`Sync`、`Compare`、`Compare File` 和 `Remove` 将以下自定义结果信息返回到 `EvaluationResultData` 的单个实例。

> **注意：**
>
> `Export` 和 `Template` cmdlet 不返回自定义结果。

```
 public class EvaluationResultData

 {

     public Dictionary&lt;string, Dictionary&lt;string, ActionResultValues
>> EvaluationResults;

     public int                  Added;

     public int                  Updated;

     public int                  Deleted;

     public int                  NoChange;

     public int                  TotalChanged;

     public EvaluationResults     OverallResult;

     public string               CloudBackupFolder;

     public string               SourceBackupFolder;

 }
```

```
 Where:

 public enum ActionResultValues

{

     Add,

     Update,

     Delete,

     Identical,

     DoNothing

 }

 public enum EvaluationResults

 {

     Success,

     Failure,

     Skipped

 }
```

`EvaluationResults` 显示一个列表，其中每个选定组件有一个条目。键是组件名称，值是每个组件成员的列表以及对该组件成员执行的操作。操作可以是 `ActionResultValues` 值中的任何一个。

`Added`、`Updated`、`Deleted` 和 `NoChange` 依次表示已添加、已更新、已删除或未执行操作的组件成员总数。

`TotalChanged` 是 `Added`、`Updated` 和 `Deleted` 的总和。

`OverallResult` 是一个布尔值，指示 cmdlet 的结果。True 表示所有组件都完全成功，False 表示处理一个或多个组件失败。

`CloudBackupFolder` 是在 cmdlet 执行任何云修改操作之前，云站点配置备份的完全限定文件规范。

`SourceBackupFolder` 是 cmdlet 完成后创建的源文件备份的完全限定文件规范。默认情况下，这些文件位于 *%HOMEPATH%\Documents\Citrix\AutoConfig*。

PowerShell 帮助

每个 cmdlet 都提供 PowerShell 帮助。所有参数都随每个 cmdlet 一起记录，并附有 cmdlet 的简要说明。要访问任何 cmdlet 的帮助，请在 cmdlet 前键入 `Get-Help`。

```
Get-Help Import-CvadAcToSite
```

用于备份和还原的自动化配置工具 cmdlet

此页面列出了该工具支持的所有 cmdlet 和参数，用于触发 Web Studio 使用的备份和还原 API。

备份存储 cmdlet

Get-BckRstrStorage

此 cmdlet 仅适用于本地部署。获取保存备份的存储的详细信息。

参数：

参数	描述
`CustomerId`	获取持有者令牌所需的客户 ID。
`CientId`	获取持有者令牌所需的客户端 ID。
`Secret`	获取持有者令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件以替代先前参数的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境的类型：Production、ProductionGov、ProductionJP、OnPrem。

参数	描述
`Quiet`	用于抑制控制台输出的参数。

Set-BckRstrStorage

此 cmdlet 仅适用于本地部署。设置保存备份的新存储。

参数：

参数	描述
`CustomerId`	获取持有者令牌所需的客户 ID。
`CientId`	获取不记名令牌所需的客户端 ID。
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件（替代以前的参数）的参数。有关如何设置安全配置文件，请参阅 (https://www.citrix.com/blogs/2016/07/01/introducing-remote-powershell-sdk-v2-for-citrix-cloud/)。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于禁止向控制台输出的参数。
`MaximumBackups`	在创建新备份时，备份清理过程删除最旧备份之前，要保留的未固定备份的最大数量。

参数	描述
`MaximumPinnedBackups`	要保留的固定备份的最大数量。这些备份不会被清理过程删除。
`BlobStorageType`	存储类型：`FileStorage` 或 `CustomerAzureStorage`。
`FileStoragefolder`	`BlobStorageType` `FileStorage` 选项的完全限定文件夹规范。
`Info1`	对于 `FileStorage`，可选 `UserName` 对于 `CustomerAzureStorage`，Azure SAS URL
`Info2`	对于 `FileStorage`，可选密码
`Info3` 和 `Info4`	未使用

测试备份恢复存储

此 cmdlet 仅适用于本地部署。测试以确定定义的存储是否有效。

对于 `FileStorage`，测试会验证文件夹是否存在且可写入。

对于 `CustomerAzureStorage`，测试会验证 SAS URL 具有正确的权限，并且当前日期在 URL 的开始日期和结束日期之间。

如果有效则返回 `true`，如果无效则返回 `false`。

参数：

参数	描述
`CustomerId`	获取不记名令牌所需的客户 ID。
`CientId`	获取不记名令牌所需的客户端 ID。

参数	描述
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于替代先前参数以识别现有安全配置文件的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于抑制控制台输出的参数。

备份 cmdlet

Get-BckRstrBackups

枚举存储在备份或还原 Blob 存储位置中的备份。对于 Citrix Virtual Apps and Desktops™，此位置由管理员通过 WebStudio 设置。对于 DaaS，这是预先存在的客户 Azure 存储。使用 `Get-BckRstrBackupsWithDetiails` 获取每个备份的完整信息。备份详细信息包括：

- 备份名称
- 备注
- 已固定（true 或 false）
- 备份日期和时间
- 历史记录 UID
- 相关 UID（上次还原历史记录的 UID）
- 相关日期和时间
- 如果在检查模式下运行，则相关
- 持续时间（秒）
- 管理员名称
- 列出每个组件及其成员数量的详细信息。

参数：

参数	描述
`CustomerId`	获取不记名令牌所需的客户 ID。
`CientId`	获取不记名令牌所需的客户端 ID。
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件以替代先前参数的参数。有关如何设置安全配置文件，请参阅 (https://www.citrix.com/blogs/2016/07/01/introducing-remote-powershell-sdk-v2-for-citrix-cloud/)。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于抑制控制台输出的参数。

Get-BckRstrBackupsMembers

枚举存储在所选备份中的单个组件的成员。成员名称以简单列表形式返回。

组件包括：

- 标签
- AdminScopes
- AdminRoles
- AdminAdministrators（仅限本地部署）
- HostConnections
- 图标
- AdminFolders
- MachineCatalogs
- StoreFronts
- DeliveryGroups
- ApplicationGroups

- ApplicationFolders
- 应用程序
- AppVServers
- AppLibPackageDiscovery
- AppVIsolationGroups
- 组策略
- 用户区域首选项
- 站点数据
- 区域（仅限本地部署）

参数：

参数	描述
`CustomerId`	获取持有者令牌所需的客户 ID。
`CientId`	获取持有者令牌所需的客户端 ID。
`Secret`	获取持有者令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件（替代先前参数）的参数。有关如何设置安全配置文件，请参阅 (https://www.citrix.com/blogs/2016/07/01/introducing-remote-powershell-sdk-v2-for-citrix-cloud/) [XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud]。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于抑制控制台输出的参数。
`BackupName`	备份的名称。`.zip` 扩展名是可选的。
`Component`	要包含在备份中的组件。

New-BckRstrBackup

在 Delivery Controller 上启动新的备份操作。此操作与 `New-BckRstrBackup` cmdlet 异步。

参数：

参数	描述
`CustomerId`	获取不记名令牌所需的客户 ID。
`CientId`	获取不记名令牌所需的客户端 ID。
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件（替代以前的参数）的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于禁止向控制台输出的参数。
`Notes`	有关备份的备注。
`PollForCompletion`	用于轮询 Delivery Controller 上运行的操作直到操作完成的参数。除非指定了 `Quite` 参数，否则轮询会将进度和完成结果记录到控制台。

固定备份 cmdlet

Set-BckRstrPinBackups

固定备份，使其不会作为 Delivery Controller 备份清理过程的一部分被删除。

参数：

参数	描述
`CustomerId`	获取不记名令牌所需的客户 ID。

参数	描述
`CientId`	获取不记名令牌所需的客户端 ID。
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件（替代以前的参数）的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于抑制控制台输出的参数。
`BackupName`	备份的名称。`.zip` 扩展名是可选的。

Set-BckRstrUnpinBackups

取消固定备份，使其可在 Delivery Controller 备份清理过程中删除。

参数：

参数	描述
`CustomerId`	获取不记名令牌所需的客户 ID。
`CientId`	获取不记名令牌所需的客户端 ID。
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件（替代以前的参数）的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。

参数	描述
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于抑制控制台输出的参数。
`BackupName`	备份的名称。`.zip` 扩展名是可选的。

删除备份 cmdlet

移除备份恢复备份

删除一个或多个备份。

参数：

参数	描述
`CustomerId`	获取持有者令牌所需的客户 ID。
`CientId`	获取持有者令牌所需的客户端 ID。
`Secret`	获取持有者令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于识别现有安全配置文件以替代以前参数的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于抑制控制台输出的参数。
`IncludeByName`	用于指定要考虑恢复的组件成员的筛选器。这是一个逗号分隔的筛选器值列表，可以包含通配符 `*` 和 `?`。

计划备份 cmdlet

Get-BckRstrSchedules

获取备份计划列表。

参数：

参数	描述
`CustomerId`	获取不记名令牌所需的客户 ID。
`CientId`	获取不记名令牌所需的客户端 ID。
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件（替代以前的参数）的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于抑制控制台输出的参数。
`BackupName`	备份名称。`.zip` 扩展名是可选的。
`Notes`	要设置或更改的备注。

New-BckRstrSchedule

创建新的备份计划。

参数：

参数	描述
`CustomerId`	获取不记名令牌所需的客户 ID。
`CientId`	获取不记名令牌所需的客户端 ID。

参数	描述
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件（替代以前的参数）的参数。有关如何设置安全配置文件，请参阅 (https://www.citrix.com/blogs/2016/07/01/introducing-remote-powershell-sdk-v2-for-citrix-cloud/)。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于禁止向控制台输出的参数。
`Name`	计划名称。
`Frequency`	频率类型：每日、每周或每月。
`Day`	如果频率是每日。
`DaysInWeek`	如果频率是每周。
`DayInMonth`	如果频率是每月。
`WeekInMonth`	如果频率是每月。
`StartDate`	格式为 `M/d/yy`
`StartTime`	以 24 小时制指定的开始时间。
`FrequencyFactor`	每 n 次运行一次，例如每天（值 = 1）或每隔一天（值 = 2）
`Description`	计划备份的描述
`Enabled`	用于启用此备份计划的参数。启用时为 `True` ，禁用时为 `false`
`TimeZoneId`	Windows 时区 ID

Set-BckRstrSchedule

修改现有备份计划。提供名称或 Uid 以选择要修改的计划。

参数：

参数	描述
`CustomerId`	获取持有者令牌所需的客户 ID。
`CientId`	获取持有者令牌所需的客户端 ID。
`Secret`	获取持有者令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于替代先前参数的参数，以标识现有安全配置文件。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于抑制控制台输出的参数。
`Name`	计划名称。
`Uid`	是否更改计划名称。
`Frequency`	频率类型：每日、每周或每月。
`Day`	如果频率是每日。
`DaysInWeek`	如果频率是每周。
`DayInMonth`	如果频率是每月。
`WeekInMonth`	如果频率是每月。
`StartDate`	格式为 `M/d/yy`
`StartTime`	指定为 24 小时制的开始时间。

参数	描述
`FrequencyFactor`	每 n 次运行一次，例如每天（值 = 1）或每隔一天（值 = 2）
`Description`	计划备份的描述
`Enabled`	用于启用此备份计划的参数。启用时为 `True`，禁用时为 `false`
`TimeZoneId`	Windows 时区 ID

Set-BckRstrScheduleEnabled

启用现有备份计划。提供名称或 Uid 以选择要启用的计划。

参数：

参数	描述
`CustomerId`	获取不记名令牌所需的客户 ID。
`CientId`	获取不记名令牌所需的客户端 ID。
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件（替代先前参数）的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于抑制控制台输出的参数。
`Name`	计划名称。
`Uid`	如果计划名称需要更改。

Set-BckRstrScheduleDisabled

禁用现有备份计划。提供名称或 Uid 以选择要禁用的计划。

参数：

参数	描述
`CustomerId`	获取持有者令牌所需的客户 ID。
`CientId`	获取持有者令牌所需的客户端 ID。
`Secret`	获取持有者令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件以替代先前参数的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于抑制控制台输出的参数。
`Name`	计划名称。
`Uid`	如果计划名称需要更改。

限制备份 cmdlet

Set-BckRstrOptions

将计划备份限制为每天一次，以避免出现相同的备份。

参数：

参数	描述
`CustomerId`	获取不记名令牌所需的客户 ID。
`CientId`	获取不记名令牌所需的客户端 ID。

参数	描述
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件（替代以前的参数）的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于禁止向控制台输出的参数。
`OneScheduledBackupPerDay`	用于将计划备份限制为每天一次以避免出现相同备份的参数。

还原 cmdlet

恢复-备份恢复备份

从现有备份中还原单个组件的成员。

参数：

参数	描述
`CustomerId`	获取不记名令牌所需的客户 ID。
`CientId`	获取不记名令牌所需的客户端 ID。
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件（替代以前的参数）的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。

参数	描述
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于禁止向控制台输出的参数。
`BackupName`	备份的名称。`.zip` 扩展名是可选的。
`Component`	要包含在备份中的组件。
`Notes`	有关备份的备注。
`CheckMode`	用于标识将要还原但未执行实际还原的组件成员的参数。
`RestoreType`	还原类型：MissingOnly 或 MissingUpdateExisting。
`IncludeByName`	用于指定要考虑还原的组件成员的筛选器。这是一个逗号分隔的筛选器值列表，可以包含通配符 `*` 和 `?`。

历史记录 cmdlet

Get-BckRstrHistory

获取所有操作的历史记录详细信息列表。

参数：

参数	描述
`CustomerId`	获取不记名令牌所需的客户 ID。
`CientId`	获取不记名令牌所需的客户端 ID。
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件（替代以前的参数）的参数。有关如何设置安全配置文件，请

参数	描述
	参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于禁止向控制台输出的参数。

Get-BckRstrSpecificBackupHistory

获取特定备份的历史详细信息列表。

参数：

参数	描述
`CustomerId`	获取不记名令牌所需的客户 ID。
`CientId`	获取不记名令牌所需的客户端 ID。
`Secret`	获取不记名令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件（替代以前的参数）的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于禁止向控制台输出的参数。
`BackupName`	备份的名称。`.zip` 扩展名是可选的。

Set-BckRstrNotes

设置或更改历史记录中的备注。

参数：

参数	描述
`CustomerId`	获取持有者令牌所需的客户 ID。
`CientId`	获取持有者令牌所需的客户端 ID。
`Secret`	获取持有者令牌所需的密钥。
`CustomerInforFileSpec`	包含安全和环境信息的客户信息文件的完全限定文件规范。
`ProfileName`	用于标识现有安全配置文件并替代以前参数的参数。有关如何设置安全配置文件，请参阅 XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud。
`Environment`	生产环境类型：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	用于抑制控制台输出的参数。
`BackupName`	备份的名称。`.zip` 扩展名是可选的。
`Notes`	要设置或更改的备注。

故障排除自动化配置和附加信息

> **重要提示：**
>
> 对于自动化配置中常见的错误消息和相应的解决方案，请参阅知识中心文章 CTX277730 中的 *故障排除常见问题解答*。

自动化配置工具错误

自动化配置工具操作有时会产生错误。发生这种情况时，在处理诸如计算机目录、交付组或组策略等组件时可能会出现故障。使用 `OnErrorAction` 和延续参数可以帮助您在处理过程中捕获错误、解决错误并从中断处继续。

默认的 `OnErrorAction` 值为 `StopCompEnd`。发生错误时，工具会完成当前组件的处理。不会处理其他组件，并且错误不会传递给下游的依赖组件。解决任何错误后，您可以重新运行应用了任何延续参数的 cmdlet。

OnErrorAction 参数

您可以在迁移命令上定义 `OnErrorAction` 参数值，以控制工具在处理组件时如何响应发现的错误。

此表显示了参数值及其说明：

值	描述
`Continue`	尝试处理尽可能多的所有组件。
`Pause`	在处理结束时暂停，并提示您继续或停止。
`StopCompEnd`	尝试尽可能多地处理组件。组件完成后停止。（默认）
`StopImmediately`	发现错误时处理停止。

迁移 cmdlet

您可以将 `OnErrorAction` 参数应用于以下迁移命令：

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

示例：`Merge-CvadAcToSite -OnErrorAction StopImmediately`

恢复参数

这些参数定义了工具在操作因错误暂停或停止后如何恢复。

您可以将恢复参数应用于包含以下 `OnErrorAction` 参数值之一的迁移 cmdlet：

- `Pause`
- `StopCompEnd`
- `StopImmediately`

此表显示了参数值及其说明：

值	描述
`-AllRemaining`	需要一个起始组件。处理从起始组件开始，并处理所有剩余组件。将处理多个组件。
`-Resume`	使用 `CurrentComponent.txt` 中的组件作为起始点。所有剩余项设置为 true。将处理多个组件。
`-Repeat`	使用 `CurrentComponent.txt` 中的组件作为起始点。所有剩余项设置为 false。仅处理一个组件。

最后处理的组件存储在 AutoConfig 文件夹中的 `CurrentComponent.txt` 文件中。不建议编辑此文件。 如果您指定 `-Resume` 或 `-Repeat`，并且 `CurrentComponent.txt` 缺失或无效，则处理将停止，并提示您选择一个组件。

在 CustomerInfo.yml 文件中设置 OnErrorAction

您还可以在 `CustomerInfo.yml` 文件中设置 `OnErrorAction` 值。使用以下 cmdlet 设置这些值：

- 对于新文件：`New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`
- 对于现有文件：`Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

日志

运行任何 cmdlet 都会创建一个日志文件并在主历史日志文件中生成一个条目。所有操作日志文件都放置在备份文件夹中。所有日志文件名都以 `CitrixLog` 开头，然后显示自动配置操作以及 cmdlet 执行的日期和时间戳。日志不会自动删除。

主历史日志位于 `*%HOMEPATH%\Documents\Citrix\AutoConfig*` 中，文件名为 **History.Log**。每次 cmdlet 执行都会生成一个主日志条目，其中包含执行的日期、操作、结果、备份和日志文件位置。

您还可以使用 `New-CvadAcZipInfoForSupport` cmdlet 收集日志以发送给 Citrix 以获得支持。此 cmdlet 将所有日志和 .yml 文件压缩到一个 zip 文件中。客户敏感信息（CustomerInfo.yml 和 CvadAcSecurity.yml）不包含在 zip 文件中。Icon.yml 文件也因其大小而被排除。zip 文件放置在

%HOMEPATH%\Documents\Citrix\AutoConfig 中，并根据日期和时间戳命名为 *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*。此 zip 文件也可以用作备份。

每个日志文件都包含以下内容：

- 操作的名称以及是否启用了检查模式
- 开始和结束日期和时间
- 每个组件操作的多个条目以及成功/失败通知
- 已执行操作的摘要，包括各种已创建对象的计数
- 适用的建议修复
- 适用的备份文件夹位置
- 主日志位置
- 持续时间

诊断文件

诊断文件可帮助您确定和解决问题。运行操作时会创建以下文件。它们位于 *%HOMEPATH%\Documents\Citrix\AutoConfig* 下特定于操作的子文件夹中。在提供问题解决支持信息时，请包含这些文件。

导出

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

此文件统计为将站点配置导出到文件而进行的所有 Broker PowerShell SDK 调用。

导入、合并、还原、同步、备份、比较

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

此文件记录每个 Rest API 调用和相关信息。

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

此文件包含所有 `Add`、`Update` 和 `Delete` Rest API 内容。

依赖项导致的问题

导入和合并可能会因缺少依赖项而失败。一些常见问题包括：

1. 组策略缺少交付组筛选器。常见原因是未导入交付组。
2. 应用程序导入或合并失败。常见原因是缺少未导入的交付组或应用程序组。

3. 应用程序组缺少 RestrictToTag。常见原因是未导入标签。
4. 主机连接失败。常见原因是 CvadAcSecurity.yml 文件中缺少安全信息。
5. 计算机目录失败。常见原因是未导入主机连接。
6. 计算机目录和交付组中缺少计算机。常见原因是 Active Directory 中未找到计算机。
7. 交付组中缺少用户。常见原因是 Active Directory 中未找到用户。

建议

- 请勿同时运行多个自动化配置实例。同时运行多个实例会在云站点中产生不可预测的结果。如果发生这种情况，请重新运行一个自动化配置实例，使站点恢复到预期状态。
- 在运行自动化配置时，请勿在 Studio 中操作或更改数据。
- 请务必在 Studio 中目视验证合并、导入或还原结果，以确保云站点符合预期。

文件夹

默认文件夹根位置

所有自动化配置工具操作都在根文件夹或其内部的子文件夹中进行。根文件夹位于 *%HOMEPATH%\Documents\Citrix\AutoConfig*。

导出

所有导出的文件都放置在两个文件夹位置，以方便使用并提供导出历史记录。导出的文件始终放置在根文件夹中。副本放置在名为 **Export** 的子文件夹中，并带有导出日期和时间。

根文件夹始终包含最新导出的本地站点配置。每个 **Export** 子文件夹都包含在指定日期和时间完成的导出，从而维护导出历史记录。您可以使用任何 **Export** 子文件夹来配置云站点。自动化配置不会删除或修改现有导出子文件夹。

导入/合并/同步/比较

`Import`、`Merge` 和 `Compare` 操作始终源自根文件夹中的文件。每个操作都会创建一个子文件夹，根文件夹中的文件会复制到该子文件夹，从而提供云站点更改源文件的历史记录。

还原

`Restore` 操作使用现有子文件夹来配置云站点。源文件夹在所需的 `-RestoreFolder` 参数上指定。与其它命令不同，不会创建新子文件夹，因为 `Restore` 操作使用现有子文件夹。还原文件夹可以是根文件夹，但仍必须在 `-RestoreFolder` 参数上指定。

备份

自动化配置初始化、更新和备份云站点配置。随着时间的推移，云站点上可能会更改许多不同的配置。为了便于长期使用并保留历史更改，自动化配置使用一种保留方案来保存此更改历史记录，并提供一种还原到早期状态的方法。

云站点配置备份始终会创建到名为 **Backup** 的子文件夹中，其中包含备份的日期和时间。自动化配置不会删除或修改现有导出子文件夹。

您可以使用备份来还原特定组件或整个配置。要还原整个交付组和计算机目录组件，请使用以下 cmdlet：

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> **注意：**
>
> 上述 cmdlet 中的备份文件信息基于您自己的备份。

> 要还原整个云站点配置，请使用以下 cmdlet：

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss
```

> **注意：**
>
> 上述 cmdlet 中的备份文件信息基于您自己的备份。

更改默认根文件夹

`Export`、`Import`、`Merge`、`Sync` 和 `Compare` 操作可以使用 `–AlternateFolder` 参数更改默认根文件夹。每个操作子文件夹的创建和管理与之前所述相同。

复制到子文件夹的文件

所有具有“.yml”扩展名的文件都会复制到操作子文件夹中，但以下文件除外：

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

自动化故障安全云站点备份

在运行更改配置的操作之前，会创建当前云站点配置的备份。这包括 `Import`、`Merge`、`Sync` 和 `Restore` 参数。备份始终位于操作子文件夹下的一个子文件夹中。

对于 `Restore`，备份文件夹是 `-RestoreFolder` 参数中指定的文件夹的子文件夹。

自动化

自动化配置工具 cmdlet 可以在自动化脚本中运行，无需管理员干预，方法是抑制提示并在 cmdlet 完成时抑制日志结果的显示。您还可以通过使用 CustomerInfo.yml 文件来设置参数以实现相同目的。

将以下参数添加到云修改 cmdlet 以抑制提示的显示。

`-Confirm $false`

将以下参数添加到 cmdlet 以抑制在 cmdlet 完成时显示日志。

`-DisplayLog $false`

将以下参数添加到 cmdlet 以抑制向 PowerShell 命令窗口记录日志。

`-Quiet`

另一种方法是，可以将以下参数放置在 CustomerInfo.yml 文件中。

`Confirm: False`

`DisplayLog: False`

从非 Delivery Controller™ 的 PC 导出

自动化配置工具使用多个 Citrix PowerShell SDK 将本地站点配置导出到文件。这些 SDK 会自动安装在 Delivery Controller 上，使工具无需额外操作即可在 Delivery Controller 上运行。在非 Delivery Controller 计算机上运行时，需要安装工具所需的 Citrix PowerShell SDK 集。此 SDK 集是 Citrix Studio 的一部分，可以从 Citrix Virtual Apps and Desktops™ 安装介质安装。

> **注意：**
>
> 自动化配置无法在 Cloud Connector 上运行。

迁移到 Citrix Cloud™ Government 和日本控制平面

Citrix Cloud Government 和日本控制平面环境使用不同的访问点来验证和分配访问令牌。此独特要求适用于任何访问云的自动化配置工具。请执行以下步骤以在这些环境中使用自动化配置。

1. 在 *%HOMEPATH%\Documents\Citrix\AutoConfig* 文件夹中，编辑 CustomerInfo.yml。
2. 根据您要连接的环境，将以下行之一添加到 CustomerInfo.yml（如果已存在，则进行更改）。

   ```
   Environment: 'ProductionGov'
   ```

   或

   ```
   Environment: 'ProductionJP'
   ```

现在可以在这些环境中使用自动配置。

Citrix Cloud 数据收集

有关 Citrix Cloud 收集哪些信息的信息，请参阅 Citrix Cloud Services 客户内容和日志处理。

其他资源

讨论论坛

访问 Citrix 自动配置讨论论坛。

视频

在 YouTube 上观看 Citrix Virtual Apps and Desktops 自动配置工具揭秘。

培训

云学习中心包含构建服务部署的分步视频指南，包括本文中描述的任务。请参阅 将 Citrix Virtual Apps and Desktops 迁移到 Citrix Cloud 学习路径。

自动缩放™

> **注意：**
>
> 此功能仅在 Web Studio 中可用。

Autoscale 是一项功能，可提供一致、高性能的解决方案，主动管理您的计算机电源。它旨在平衡成本和用户体验。

Autoscale 能够对交付组中所有已注册的单会话和多会话操作系统机器进行主动电源管理。

Autoscale 功能包括：

- 基于计划和基于负载的设置
- 动态会话超时
- Autoscale 标记的机器（云爆发）
- 用户注销通知

典型用例

以下是 Autoscale 常用的场景。

- 基于计划的机器开机以处理预期工作负载

  Autoscale 允许管理员以 30 分钟为粒度调整开机容量，并允许在不同日期设置不同的计划。如果预期工作负载不稳定，建议配置容量缓冲区，以避免用户等待机器开机。

- 云爆发用例

  Autoscale 提供了仅管理交付组中一部分机器电源的灵活性。为此，请对一台或多台机器应用标签，然后配置 Autoscale 仅管理已标记机器的电源。

  此功能在云爆发用例中非常有用，在此类用例中，您希望在基于云的资源处理额外需求（即爆发工作负载）之前，使用本地资源（或预留的公共云实例）来处理工作负载。

- 缓慢增长的用户或季节性用户

  当组织的用户缓慢增加且不希望提前预置全部容量时，动态预置功能会有所帮助。此功能会持续评估交付组上的负载，并根据当前负载情况动态地增加或减少交付组中的计算机数量。管理员必须为交付组上的负载定义高水位线和低水位线才能创建计算机。管理员可以选择定义要预置的最大计算机数量以及要应用于这些计算机的标签。

支持的 VDA 托管平台

Autoscale 支持 Citrix Virtual Apps and Desktops 支持的所有平台。这包括各种基础架构平台，例如 XenServer、Amazon Web Services、Google Cloud Platform、Microsoft Azure Resource Manager、VMware vSphere 等。有关支持平台的完整列表，请参阅 Citrix Virtual Apps and Desktops 的系统要求。

> **注意：**

> 将公共云主机连接添加到部署时，您需要混合权利许可证。有关混合权利许可证的信息，请参阅通过混合权利进行过渡和升级 (TTU)。有关添加许可证的信息，请参阅创建站点。

支持的工作负载

Autoscale 支持多会话操作系统和单会话操作系统交付组。需要注意以下三个用户界面：

- 适用于多会话操作系统交付组（以前称为 RDS 交付组）的 Autoscale 用户界面
- 适用于单会话操作系统随机（池）交付组（以前称为池 VDI 交付组）的 Autoscale 用户界面
- 适用于单会话操作系统静态交付组（以前称为静态 VDI 交付组）的 Autoscale 用户界面

有关不同交付组的用户界面的详细信息，请参阅Autoscale 用户界面。

优势

Autoscale 功能具有以下优势：

- 为您提供一种单一、一致的机制来对交付组中的计算机进行电源管理。
- 通过基于负载或基于计划的电源管理，或两者的组合来为计算机供电，从而确保可用性并控制成本。
- 要监控成本节省和容量利用率等指标，并启用通知，请使用 Director。

观看两分钟视频

以下视频快速介绍了 Autoscale。

<iframe src="https://www.youtube.com/embed/5yxERrFZQ68" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Autoscale™ 入门

Autoscale 是一项功能，它提供一致、高性能的电源管理解决方案，可根据配置的计划或负载需求主动扩展交付组。

Autoscale 适用于所有类型的交付组：

- 单会话静态操作系统
- 单会话随机操作系统
- 多会话随机操作系统

本文介绍了 Autoscale 的基本概念，并提供了有关如何为交付组启用和配置 Autoscale 的指导。

基本概念

在开始之前，请了解 Autoscale 中的以下基本概念：

- 容量和计算机注册
- 跨多个计算机目录进行扩展
- 计算机预配和会话需求
- 实例大小注意事项
- 计划
- 高峰和非高峰时段
- 关机延迟
- 池大小
- 容量缓冲区
- 负载指数
- Autoscale 和维护模式
- 计算机成本
- 纵向扩展交付组
- 纵向缩减交付组
- 排空状态

容量和计算机注册

Autoscale 在确定容量时仅包括已向站点注册的计算机。未注册的已开机计算机无法接受会话请求。因此，它们不包含在交付组的整体容量中。

跨多个计算机目录进行扩展

在某些站点中，多个计算机目录可能与单个交付组关联。Autoscale 会随机从每个目录中开机计算机，以满足计划或会话需求。

例如，一个交付组有两个计算机目录：目录 A 有三台已开机计算机，目录 B 有一台已开机计算机。如果 Autoscale 需要开机一台额外的计算机，它可能会从目录 A 或目录 B 中开机一台计算机。

计算机预配和会话需求

交付组关联的计算机目录必须有足够的计算机，以便在需求增加和减少时进行开机和关机。如果会话需求超过交付组中注册计算机的总数，Autoscale 会确保所有注册计算机都已开机。但是，**Autoscale 不会预配额外的计算机**。

> **注意：**
>
> 如果交付组有 63 台计算机，并且在非工作时间设置了 10% 的缓冲区容量，那么根据 Autoscale 计算，在非工作时间必须开启 6.3 台计算机。为了处理小数位值，规则如下：
>
> - 四舍五入到最接近的整数：例如，如果值为 6.4，则开启 6 台计算机。如果值为 6.7，则开启 7 台计算机。
> - 对于任何小于 1 的非零值，四舍五入到 1。例如，如果值为 0.2 或 0.9，则开启 1 台计算机。

实例大小注意事项

如果您在公有云中适当调整实例大小，则可以优化成本。我们建议您预配较小的实例，只要它们符合您的工作负载性能和容量要求。

较小的实例托管的用户会话少于较大的实例。因此，Autoscale 会更快地将计算机置于耗尽状态，因为最后一个用户会话注销所需的时间更少。结果，Autoscale 会更快地关闭较小的实例，从而降低成本。

计划

Autoscale 根据您设置的计划开启和关闭交付组中的计算机。

计划包括每个时间段的活动计算机数量，并定义了高峰时间和非高峰时间。

计划设置因交付组类型而异。有关详细信息，请参阅：

- 多会话操作系统交付组
- 单会话操作系统随机交付组
- 单会话操作系统静态交付组

高峰和非高峰时段

高峰和非高峰时段用于指示在一天中的特定时段使用哪个容量缓冲区值。您可以定义高峰时段，将剩余的未定义时段留作非高峰时段。

关机延迟

关机延迟是指在 Autoscale 关闭一台计算机之前，该计算机开机后必须经过的最短分钟数。这可以防止计算机在会话需求波动期间反复开关机。默认情况下，关机延迟为 30 分钟。您可以将其设置为 0-60 分钟的范围。

池大小

池大小是指在一天中的特定时段内必须保持开机状态的计算机数量。

容量缓冲区

容量缓冲区用于在当前需求中添加备用容量，以应对动态负载增加。需要注意以下两种情况：

- 对于多会话操作系统交付组，容量缓冲区定义为交付组总容量（以负载指数计）的百分比。
- 对于单会话操作系统交付组，容量缓冲区定义为交付组中计算机总数的百分比。

容量缓冲区是一个滚动缓冲区，因为它根据当前使用情况进行计算和应用，而不是在配置的池大小之上进行计算和应用。

例如，假设一个交付组有 10 台计算机，当前时段的池大小为 1 台计算机，容量缓冲区为 10%。当根据计划定义的 1 台已开机计算机的负载达到 10% 容量缓冲区不再满足的程度时，会额外开机一台计算机。如果在第二台计算机开机后负载降低，并且有足够的空闲负载容量来满足 10% 容量缓冲区，Autoscale 会准备关闭 1 台计算机。

负载指数

> **重要提示：**

> 负载指数仅适用于多会话交付组。

> 负载指数指标决定了计算机接收用户登录请求的可能性。它是根据为并发登录、会话、CPU、磁盘和内存使用情况配置的 **Citrix 负载管理策略**设置计算的。

负载指数范围为 0 到 10,000。默认情况下，当一台计算机托管 250 个会话时，它被视为满载：

- 数字“0”表示一台未加载的计算机。负载指数值为 0 的计算机处于基线负载。
- 数字“10,000”表示一台满载的计算机，无法再运行任何会话。

Autoscale 和维护模式

处于维护模式的计算机，无论其可用性状态如何，都被视为整体池大小计算的一部分。因此，池中的所有计算机都可能处于维护模式。但是，这些计算机不包括在容量缓冲区计算中，确保它们立即可用。为确保特定百分比的计算机可供用户连接，请相应调整池大小和缓冲区值。

计算机成本

每小时计算机实例成本是所用计算容量的每小时成本（美元）。此设置用于计算 Autoscale 设置的成本节省。要查看节省情况，请转到 **Monitor > Trends > Machine usage**。

扩展交付组

Autoscale 会在启用了 Autoscale 的交付组中开启额外的计算机，当：

1. 交付组的 Autoscale 计划指示必须开启更多计算机以应对当前时间段。
2. 交付组上的当前负载已超出容量缓冲区。

开启计算机的条件：

1. 未处于维护模式。
2. 管理程序未处于维护模式。
3. 已关机并已注销。
4. 属于需要扩展的交付组
5. 没有待处理的电源操作。

缩减交付组

当满足以下条件时，Autoscale 会关闭 Autoscale 启用的交付组中的计算机：

1. Autoscale 计划指定必须关闭计算机，以满足当前时间段的配置计算机数量。
2. 交付组的当前负载已降低，导致开机计算机数量超出满足池大小和容量缓冲区所需数量。

Autoscale 通过关闭超出满足池大小和容量缓冲区所需数量的冗余计算机来缩减交付组。

缩减过程包括两个步骤：

1. 将所需数量的计算机置于排空状态。
2. 选择所有已排空的计算机以进行关机。

符合关机条件的计算机必须满足以下条件：

1. 未处于维护模式
2. 管理程序未处于维护模式
3. 当前已开机
4. 已注册为可用或正在启动后等待注册
5. 已排空且没有活动会话
6. 没有待处理的电源操作
7. 满足关机延迟

排空状态

Autoscale 尝试将交付组中已开机的计算机数量缩减到配置的池大小和容量缓冲区。

为实现此目标，Autoscale 会将会话最少的冗余计算机置于“排空状态”，并在所有会话注销后将其关闭。当会话需求减少且计划所需的计算机数量少于已开机的计算机数量时，就会出现此行为。

计算机排空的条件：

1. 已开机
2. 未处于维护模式
3. 管理程序未处于维护模式
4. 属于需要缩减的交付组
5. 当前活动会话数量最少

> **注意：**
>
> - 已开机至少达到关机延迟指定时间的计算机优先进入排空状态。
> - 处于排空状态的计算机不再托管新的会话启动，并等待现有会话注销。只有当所有会话都注销后，计算机才会关机。但是，如果没有立即可用于会话启动的计算机，Autoscale 宁愿将这些会话启动定向到处于排空状态的计算机，而不是启动一台新计算机。

> Autoscale 会逐一将多余的计算机置于“排空状态”：
>
> - 如果两台或更多计算机具有相同数量的活动会话，Autoscale 会排空已开机达到指定关机延迟时间的计算机。
>
>   这样做可以避免将最近开机的计算机置于排空状态，因为这些计算机最有可能拥有最少的会话。
> - 如果两台或更多计算机已开机达到指定的关机延迟时间，Autoscale 会随机逐一排空这些计算机。

处于排空状态的计算机不再托管新的会话启动，并等待现有会话注销。只有当所有会话都注销后，计算机才会成为关机候选。但是，如果没有立即可用于会话启动的计算机，Autoscale 宁愿将这些会话启动定向到处于排空状态的计算机，而不是启动一台新计算机。

当满足以下任一条件时，计算机将退出排空状态：

- 计算机已关机。

- 计算机所属的交付组已禁用 Autoscale。
- Autoscale 使用该计算机来满足计划或负载需求。当计划（基于计划的扩展）或当前需求（基于负载的扩展）所需的计算机数量超过当前已开机的计算机数量时，就会出现这种情况。

> **重要提示：**
>
> 如果没有立即可用于会话启动的计算机，Autoscale 宁愿将这些会话启动定向到处于排空状态的计算机，而不是启动一台新计算机。托管会话启动的处于排空状态的计算机仍将保持排空状态。

显示排空状态

您可以使用 PowerShell 或 Web Studio 确定哪些计算机处于排空状态。

使用 PowerShell

运行 `Get-BrokerMachineV2` PowerShell cmdlet 以查看计算机的 **IsDraining** 和 **DrainingReason** 属性。

例如：`Get-BrokerMachineV2 -Property IsDraining,DrainingReason,MachineName | Format-Table MachineName,IsDraining,DrainingReason`

- **IsDraining**：当计算机处于排空状态时，此布尔属性为 `True`；当计算机不处于排空状态时，此布尔属性为 `False`。
- **DrainingReason**：此属性提供了计算机处于排空状态的具体原因。其默认值为 `NotDraining`。当计算机正在排空时，**DrainingReason** 会显示以下值之一：
  - **AutoscaleScaleDown**：Autoscale 启动排空状态是为了缩减交付组中已开机计算机的数量，以满足配置的池大小和容量缓冲区要求。当会话需求减少或计划需要更少计算机时，会发生这种情况。
  - **NaturalRebootCycle**：计算机正在排空，作为计划重启周期的一部分，采用“等待会话结束”重启模式。计算机在重启前会等待活动会话结束。
  - **RebootCycle**：计算机正在排空，作为计划重启周期的一部分，采用“强制注销”重启模式。在计算机重启前，活动会话会被强制注销。
  - **MaintenanceMode**：管理员将计算机置于维护模式。
  - **HypervisorInMaintenanceMode**：托管计算机的管理程序连接处于维护模式。
  - **MaintenanceCycle**：计算机正在排空，作为 VUS 维护周期操作的一部分，例如操作系统磁盘重置。

- **GuestOSDraining**：客户操作系统明确地将自身设置为排空模式（例如，通过注册表设置）。此原因仅适用于多会话计算机。
- **GuestOSDrainingUntilRestart**：客户操作系统将自身设置为排空模式，该模式将持续到下一次重启。此原因仅适用于多会话计算机。

使用 Web Studio

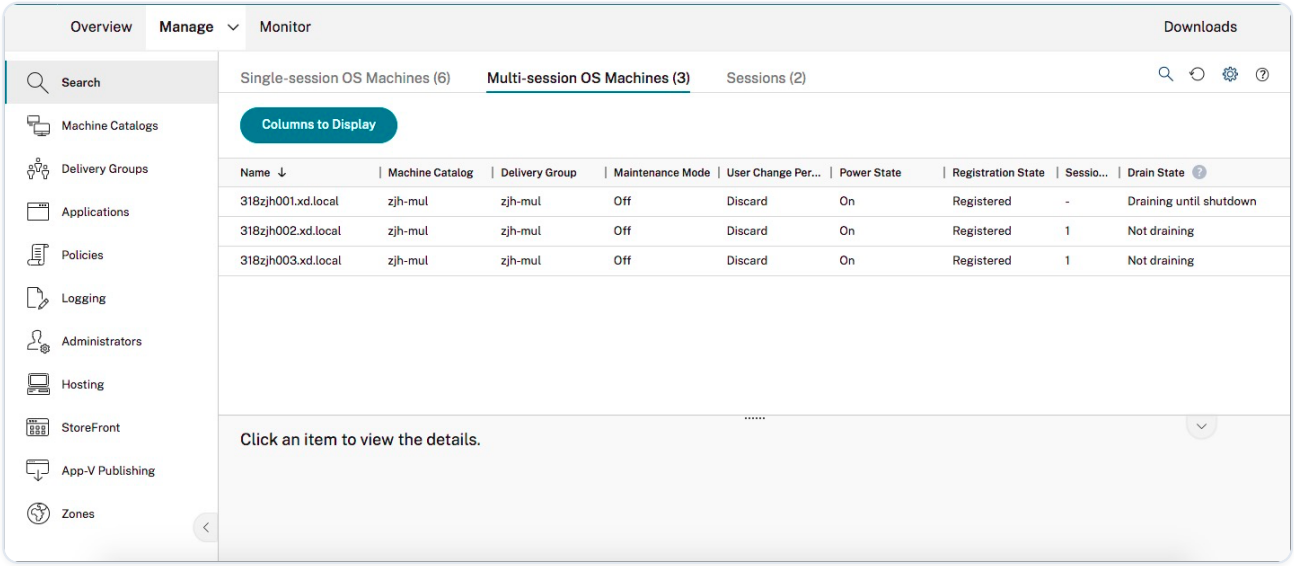
> **注意：**
>
> 虽然 `IsDraining` 和 `DrainingReason` 属性适用于单会话和多会话计算机（其中 `GuestOSDraining` 原因特定于多会话），但 Web Studio 中的**排空状态**列历来仅适用于多会话计算机以显示这些状态。

要在 Web Studio 中显示处于排空状态的计算机，请执行以下操作：

1. 导航到**搜索**节点，然后单击**要显示的列**。
2. 在**要显示的列**窗口中，选中**排空状态**旁边的复选框。
3. 单击**保存**以退出**要显示的列**窗口。

排空状态列可以显示以下信息：

- **排空直到关机。** 当计算机处于排空状态直到关机时显示。
- **未排空。** 当计算机尚未处于排空状态时显示。

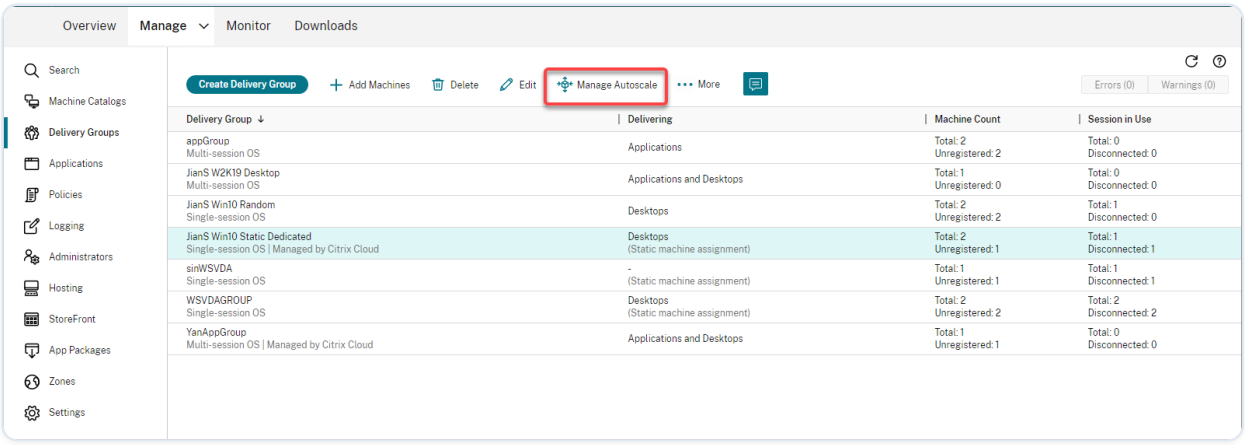


为交付组启用 Autoscale

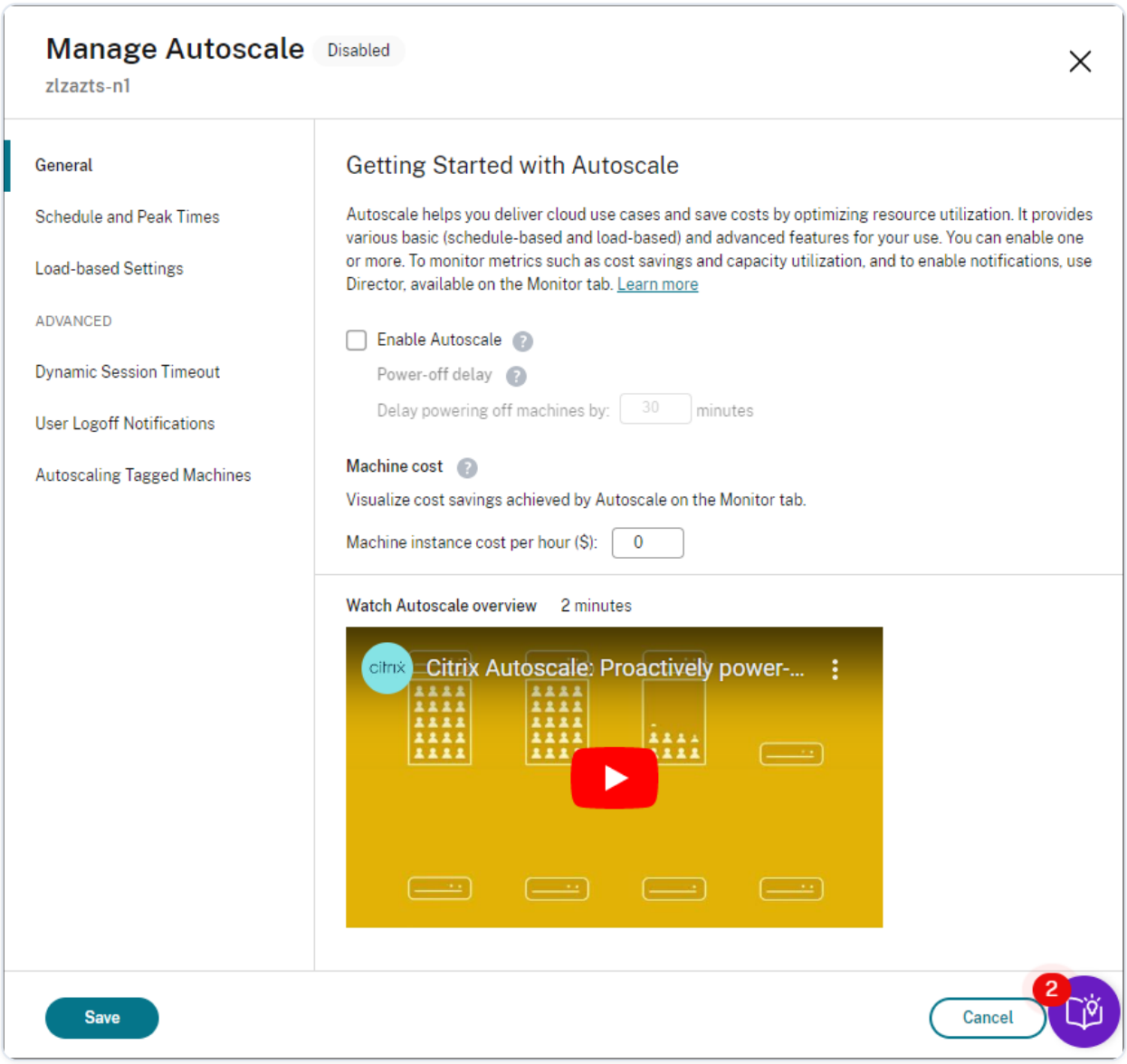
创建交付组时，Autoscale 默认处于禁用状态。要使用 Web Studio 为交付组启用和配置 Autoscale，请执行以下步骤：

您还可以使用 PowerShell 命令为交付组启用和配置 Autoscale。有关详细信息，请参阅 Broker PowerShell SDK 命令。

1. 在左侧窗格中选择**交付组**。
2. 选择要管理的交付组，然后单击**管理 Autoscale**。



3. 在**管理 Autoscale** 页面上，选中**启用 Autoscale** 复选框以启用 Autoscale。启用 Autoscale 后，页面上的选项将启用。



4. 要根据您的组织需求更改默认设置，请完成以下设置：

   - 设置计划
   - 为了更高效地关闭非活动计算机，请使用动态会话超时和用户注销通知
   - 要对交付组中的部分计算机进行电源管理，请使用Autoscale 标记的计算机

要禁用 Autoscale，请清除 **Autoscale** 复选框。页面上的选项将变为灰色，表示所选交付组的 Autoscale 已禁用。

重要提示：

- 如果禁用 Autoscale，所有由 Autoscale 管理的计算机将保持禁用时的状态。

- 禁用 Autoscale 后，处于耗尽状态的计算机将退出耗尽状态。有关耗尽状态的更多信息，请参阅耗尽状态。
- “**基于负载的设置**”页面上针对单会话操作系统静态交付组和单会话操作系统随机交付组的“**电源策略**”操作独立于 Autoscale 设置（启用或禁用）。

将排空中的计算机从 Autoscale 计算中排除

此功能允许您防止因重新启动计划而正在排空的计算机计入 Autoscale 容量目标。通过排除这些计算机，您可以优化资源调配并避免过度调配。

例如：您有一个多会话操作系统计算机的交付组，配置了 Autoscale 和定期重新启动计划。当计算机进入排空状态以进行重新启动时，Autoscale 通常仍将其计为可用容量。这可能会不必要地触发额外计算机的调配。通过启用此功能，您可以指示 Autoscale 在计算容量时忽略这些排空中的计算机。这可确保只有主动可用的计算机才计入目标，从而提高资源利用率并降低运营成本。

适用性

此功能适用于包含**多会话操作系统计算机 (RDS)** 的交付组。

限制

- 此功能不适用于单会话操作系统计算机。
- 当您根据“计算机数量”（而不是“百分比”）配置 Autoscale 时，系统不会将处于排空状态的计算机从 Autoscale 计算中排除。

重要注意事项

- 属性 `ExcludeNaturalRebootDrainingFromAutoscale` 在交付组中配置。
- 属性 `ExcludeNaturalRebootDrainingFromAutoscale` 的默认值为 `False`。这意味着排空中的计算机默认包含在 Autoscale 计算中。

先决条件

- 配置多会话操作系统交付组。
- 为目标交付组启用并配置 Autoscale。最好使用“计算机百分比”进行缩放。
- 为交付组配置重新启动计划，以使计算机进入耗尽状态。

如何配置

您可以使用 PowerShell 命令在交付组级别配置此功能。

1. 确保功能切换 `ExcludeNaturalRebootDrainingFromAutoscale` 已启用。您可以通过在 PowerShell 中运行 `Get-ConfigEnabledFeature` 并在输出列表中检查该切换来验证。

   > **注意：**
   >
   > 如果切换已禁用，则无法修改交付组属性。

2. 将交付组属性设置为排除耗尽的计算机。

   a. 以管理员权限打开 PowerShell。

   b. 识别您的多会话操作系统交付组。

   c. 使用 `Set-BrokerDesktopGroup` cmdlet 将交付组的 `ExcludeNaturalRebootDrainingFromAutoscale` 属性设置为 `$True`：

   ```
   Set-BrokerDesktopGroup -Name "<YourDeliveryGroupName>"
   -ExcludeNaturalRebootDrainingFromAutoscale $True
   ```

   将 `<YourDeliveryGroupName>` 替换为交付组的实际名称。

   d. 通过运行以下命令验证属性是否设置为 `True`：

   ```
   Get-BrokerDesktopGroup -Name "<YourDeliveryGroupName>" | Select
   Name, ExcludeNaturalRebootDrainingFromAutoscale
   ```

   输出应显示 `ExcludeNaturalRebootDrainingFromAutoscale : True`。

3. 配置 Autoscale 和重新启动计划（如果尚未配置）。

   确保您的交付组已启用 Autoscale 并配置了重新启动计划，以使计算机进入排空状态。

   a. 在 Web Studio 中，编辑您的交付组。

   b. 转到 **管理 Autoscale** 并配置高峰/非高峰计划，确保已启用 Autoscale。如果您打算排除排空中的计算机，请根据“计算机百分比”设置您的计划。

   c. 转到 **重新启动计划** 并创建或编辑一个计划，使计算机进入排空状态（例如，对于云部署使用 **平稳重新启动**，对于本地部署使用 **排空会话后重新启动所有计算机**）。

监视和故障排除

问题：即使您启用了该功能，会话有时也会启动到排空中的计算机上。

原因：这是预期行为。如果其他合适的非排空计算机不可用，处于排空状态的计算机仍可作为“最后手段”用于会话启动。此功能主要影响 Autoscale 的预配/取消预配计算。它不影响代理的会话启动逻辑本身。

解决方案：这不是问题，而是预期设计。为了最大程度地减少会话进入排空中的计算机，请确保您的 Autoscale 缓冲区和容量足以保持足够的非排空计算机可用以满足需求。

具有用户会话的 VM 的 Autoscale 选项

Autoscale 可以管理分配的和池化的计算机，优化其电源和可用性。以下内容提供了 PowerShell 命令和 UI 设置，用于根据高峰和非高峰时段以及分配的和池化的计算机的用户会话来控制计算机电源状态。

分配的计算机专用于单个用户，而池化计算机在多个用户之间共享。

> **注意：**
>
> - Citrix Studio 中的会话限制策略，尤其是“*断开连接会话计时器*”和“*会话空闲计时器*”，对于管理用户会话至关重要，即使未启用 Citrix Autoscale 也是如此。这些策略定义了会话在终止前可以保持断开连接或空闲状态的时长，确保资源利用率并防止会话被锁定。此策略设置可用于分配的计算机和池化计算机，尤其是运行多会话 VDA 的计算机。有关详细信息，请参阅会话限制策略设置。
> - `Get-BrokerMachine` PowerShell 命令已弃用。请使用 `Get-BrokerMachineV2` 作为替代方案。

对于分配的计算机

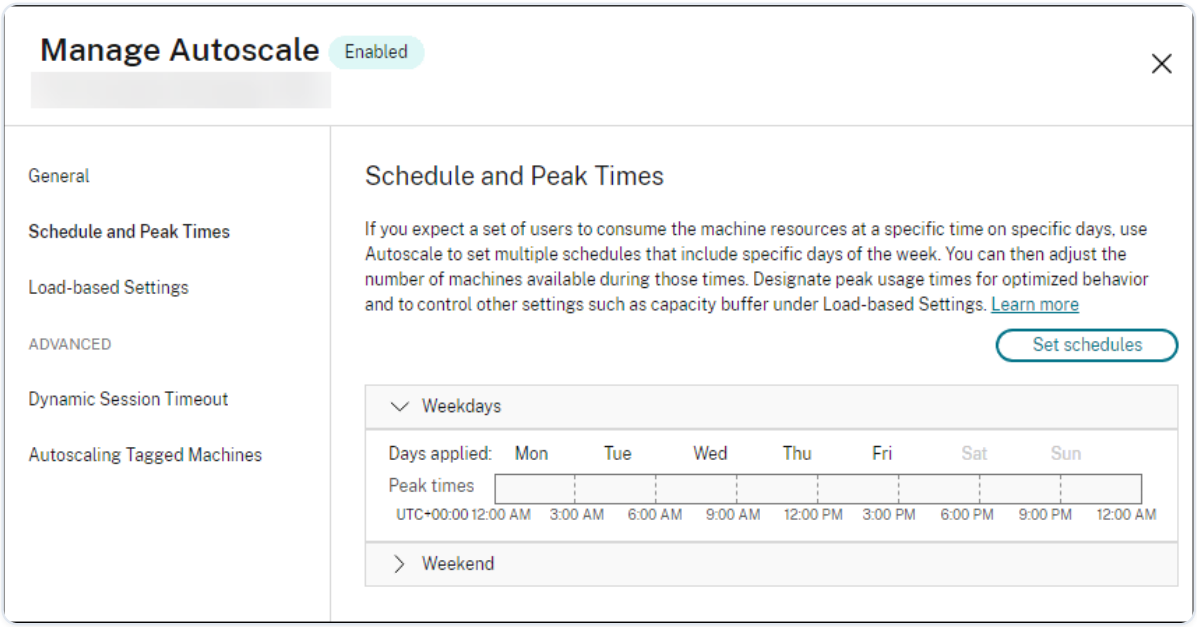
- 要在高峰期开始时自动开启静态交付组中分配的单会话计算机，请使用 PowerShell 命令：

```
Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssigned $True
```

- 为确保在高峰期发现的任何已关闭的分配计算机都能重新启动，还要启用 `AutomaticPowerOnForAssignedDuringPeak`。

```
Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssigned $True
-AutomaticPowerOnForAssignedDuringPeak $True
```

- 如果您希望虚拟机仅在用户启动会话时才开启，请执行以下任一操作：
  - 将 `AutomaticPowerOnForAssigned` 和 `AutomaticPowerOnForAssignedDuringPeak` 设置为 `False`。
  - 使用 UI 界面将所有时间定义为非高峰期，完全没有高峰期。请参阅基于计划的设置。在非高峰期，如果 Autoscale 管理的分配计算机上没有用户会话，则会将其关闭。



- 如果所有计算机都在高峰期由 Autoscale 开启，请使用 UI 界面设置等待时间（以分钟为单位）以及操作，例如，如果计算机由 Autoscale 开启后没有用户登录，则不执行任何操作、挂起或关闭。请参阅电源策略。

对于池化计算机

要在会话注销后自动关闭池化计算机，请将交付组的 PowerShell 命令 `ShutdownAfterUse` 设置为 `True`。例如：

```
Set-BrokerDesktopGroup -Name “DesktopGroupName” -ShutdownDesktopsAfterUse
$true
```

监视指标

为交付组启用 Autoscale 后，您可以从 Director 监视 Autoscale 管理的计算机的以下指标。

- 计算机使用情况
- 预计节省
- 计算机和会话的警报通知
- 计算机状态

- 负载评估趋势

> **注意：**
>
> 首次为交付组启用 Autoscale 时，可能需要几分钟才能显示该交付组的监视数据。 如果为交付组启用 Autoscale 然后又禁用，监视数据仍可用。Autoscale 以 5 分钟为间隔收集监视数据。

> 有关指标的更多信息，请参阅监视 Autoscale 管理的计算机。

Autoscale 在休眠的 VM 上

您可以通过 Autoscale 可配置设置休眠 VM。使用 PowerShell 命令 `Get-BrokerDesktopGroups`、`New-BrokerDesktopGroups` 或 `Set-BrokerDesktopGroups` 将以下正值设置为参数 `AutoscaleScaleDownActionDuringPeak`（高峰期）或 `AutoscaleScaleDownActionDuringOffPeak`（非高峰期），以定义电源操作：

- 0：缩减时关闭 VM
- 1：缩减时挂起（休眠 VM）

无法休眠的 VM 将被关闭。

如果交付组启用了休眠功能，您可以为休眠的 VM 配置重新启动计划。在重新启动周期中，VM 会恢复，然后关闭。重新启动计划可以设置为每周、每天、每月和一次。您可以配置多个计划。但是，从休眠中恢复的 VM 可能需要几分钟。

Autoscale 还可以在高峰期启动处于休眠状态的多会话远程桌面服务 (RDS) 和没有会话的共享单会话 VM。这些 VM 可以是 MCS 和非 MCS 计算机目录中的。

更多信息

有关 Autoscale 的更多信息，请参阅 Tech Zone 中的 Citrix Autoscale。

基于计划和基于负载的设置

Autoscale™ 如何管理计算机电源

Autoscale 根据所选计划开启和关闭计算机电源。Autoscale 允许您设置多个计划，其中包括一周中的特定日期，并调整这些时间段内可用的计算机数量。如果您希望一组用户在特定日期的特定时间使用计算机资源，Autoscale 有助于提供优化的体验。请注意，这些计算机将在计划期间保持开机状态，无论其上是否有会话运行。

> **注意：**
>
> Autoscale 支持任何电源管理的计算机。

> 计划基于交付组的**时区**。要更改时区，您可以在交付组中更改用户设置。有关详细信息，请参阅管理交付组。

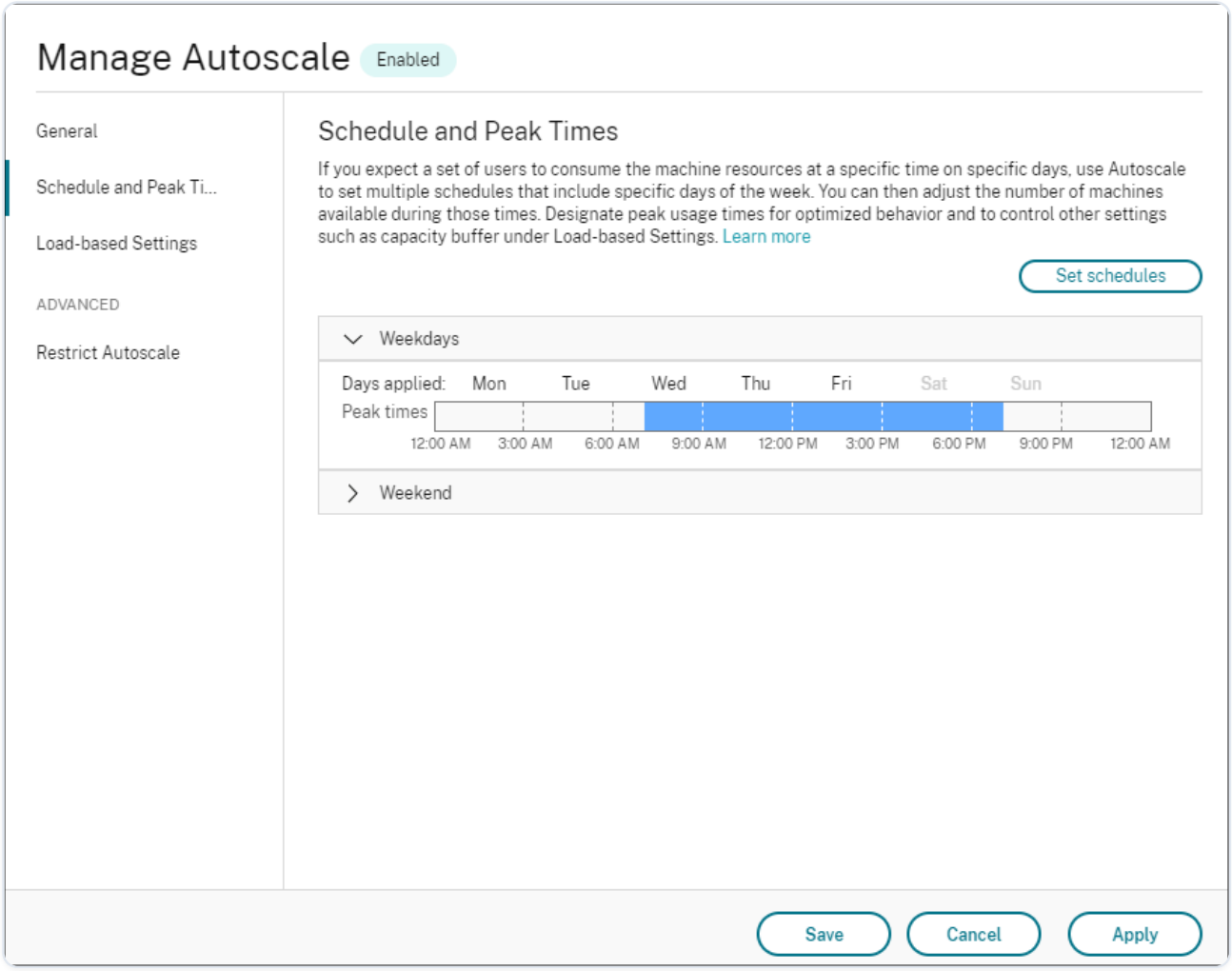
Autoscale 有两个默认计划：*工作日*（周一至周五）和*周末*（周六和周日）。默认情况下，**工作日**计划在高峰时段从上午 07:00 到下午 06:30 保持一台计算机开机，在非高峰时段不保持任何计算机开机。默认容量缓冲区在高峰时段和非高峰时段均设置为 10%。默认情况下，**周末**计划不保持任何计算机开机。

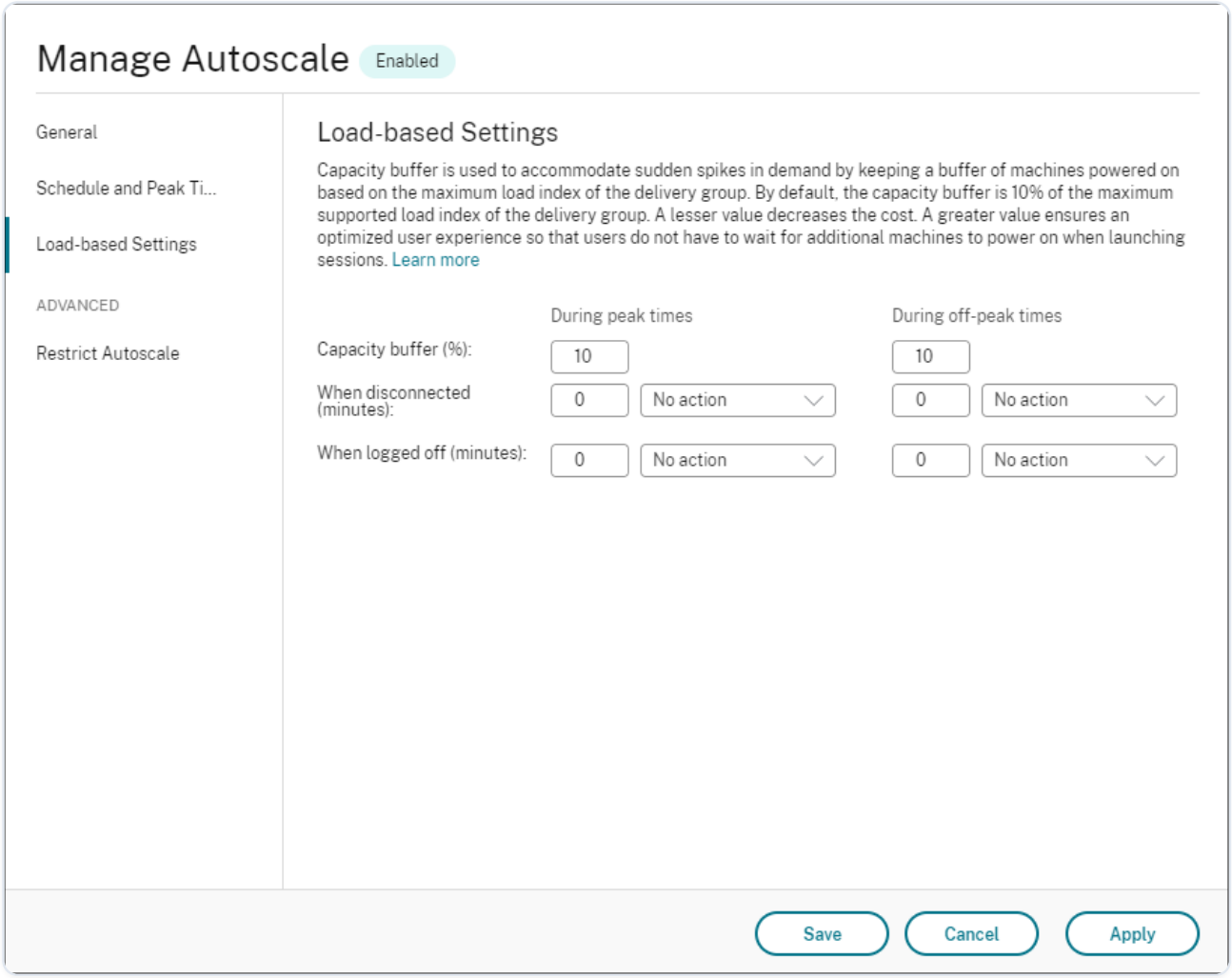
> **注意：**
>
> Autoscale 在其计算中，仅将那些已向站点注册的计算机视为可用容量的一部分。“已注册”表示计算机可供使用或已在使用中。这样做可确保只有能够接受用户会话的计算机才包含在交付组的容量中。

用户界面

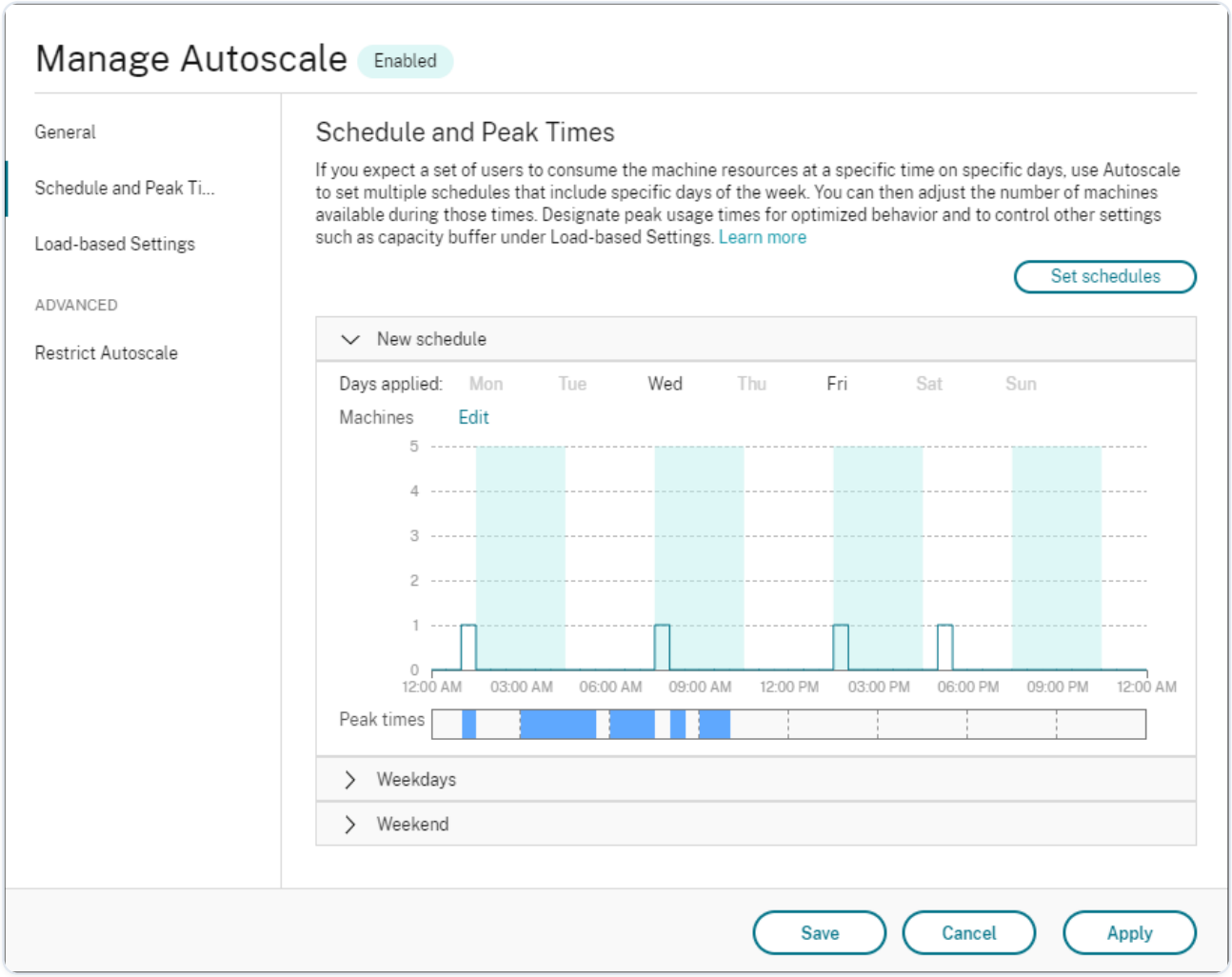
有三种类型的用户界面需要注意。

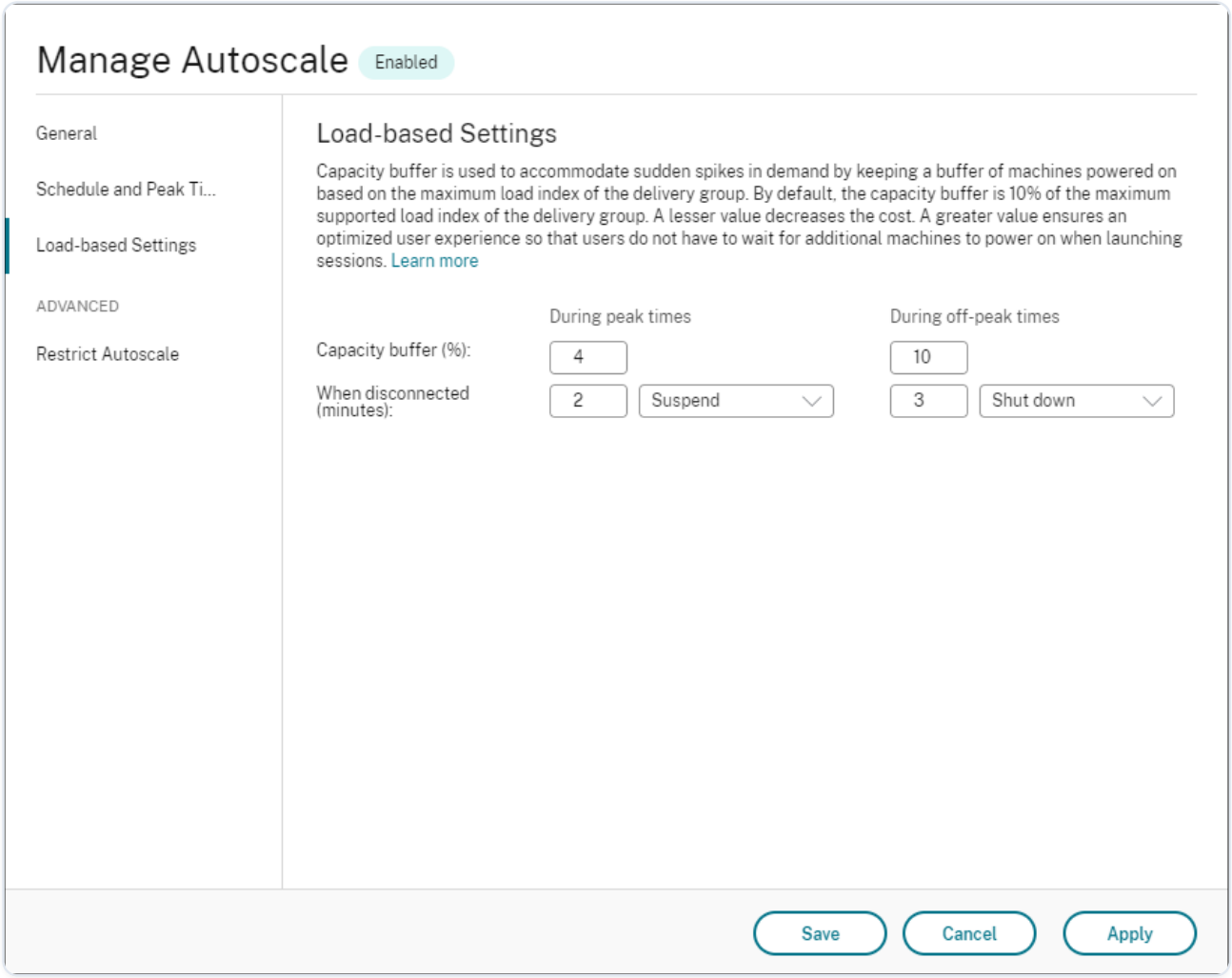
*单会话操作系统静态交付组*的用户界面：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
Weekdays
Days applied: Mon Tue Wed Thu Fri Sat Sun
Peak times
12:00 AM 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM 6:00 PM 9:00 PM 12:00 AM
Weekend
Save
Cancel
Apply

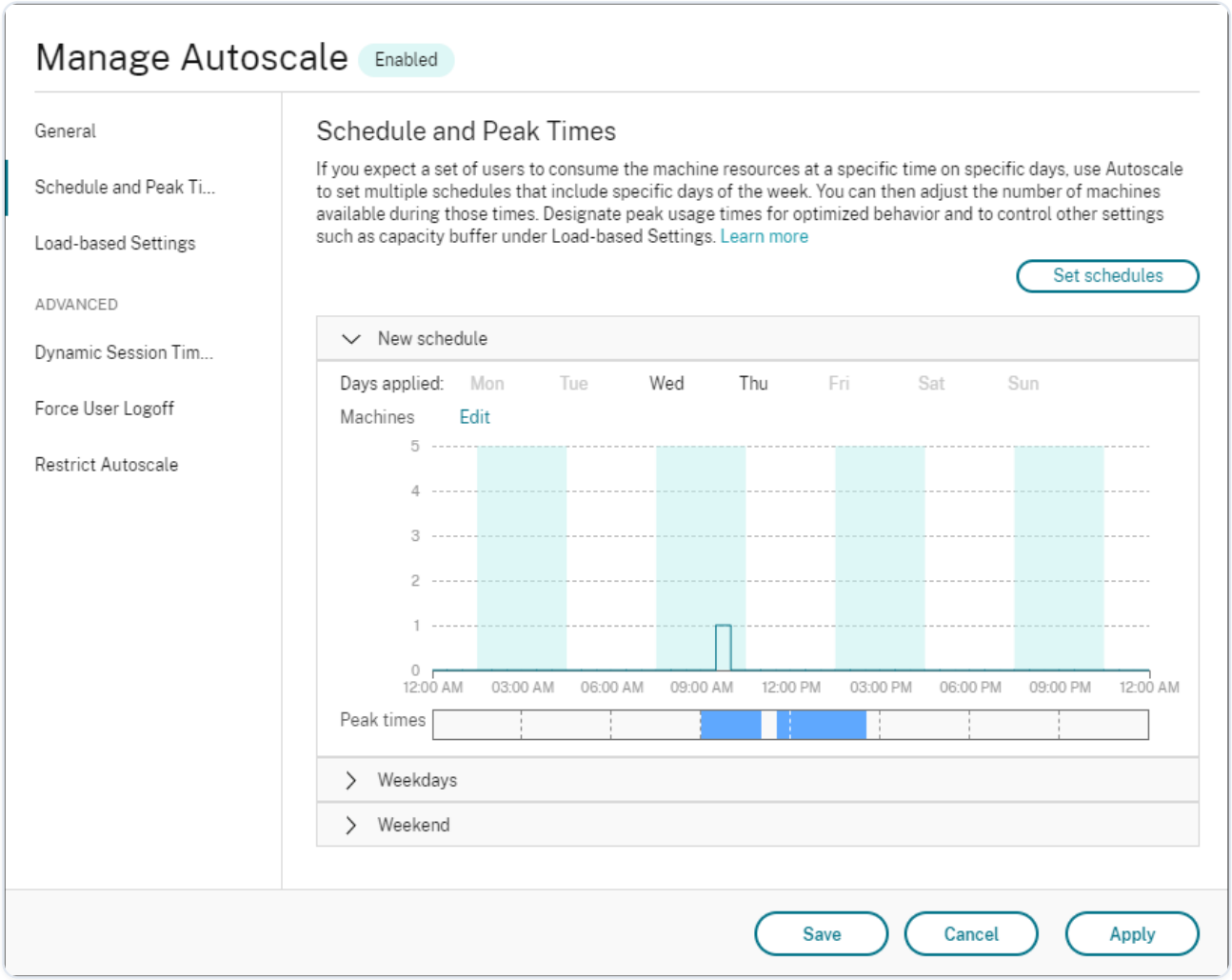


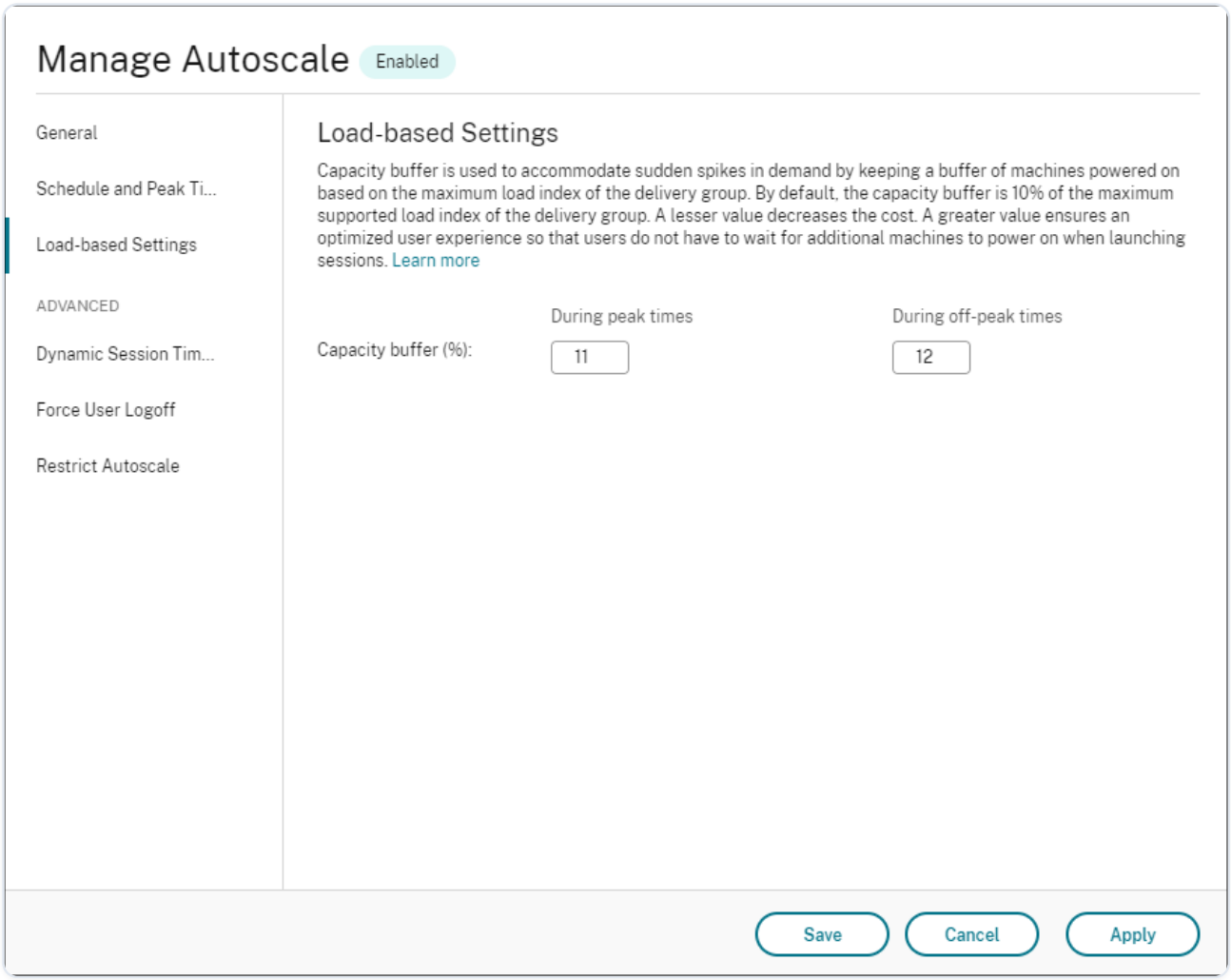
*单会话操作系统随机交付组*的 Autoscale 用户界面：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



Autoscale 用户界面，适用于 *多会话操作系统交付组*：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Dynamic Session Tim...
Force User Logoff
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



基于计划的设置

Autoscale 计划。允许您添加、编辑、选择和删除计划。

应用日期。突出显示您应用于所选计划的日期。其余日期显示为灰色。

编辑。允许您按小时或半小时分配计算机。您可以按数量和百分比分配计算机。

注意：

- 此选项仅在 Autoscale 用户界面中可用，适用于多会话操作系统和单会话操作系统随机交付组。
- **编辑**旁边的直方图绘制了在不同时间段内运行的计算机数量或百分比。
- 您可以通过单击**高峰时段**上方的**编辑**来针对每个时间段**分配计算机**。根据您在**要启动的计算机**窗口中从菜单中选择的选项，您可以按数量或百分比分配计算机。

- 对于多会话操作系统交付组，您可以每天以 30 分钟的粒度增量单独设置运行计算机的最小数量。对于单会话操作系统随机交付组，您可以每天以 60 分钟的粒度增量单独设置运行计算机的最小数量。

要定义自己的计划，请执行以下步骤：

1. 在**管理 Autoscale** 窗口的**计划和高峰时段**页面上，单击**设置计划**。
2. 在**编辑 Autoscale 计划**窗口中，选择要应用于每个计划的日期。您还可以根据需要删除计划。
3. 单击**完成**以保存计划并返回**计划和高峰时段**页面。
4. 选择适用的计划并根据需要进行配置。
5. 单击“**应用**”以退出“**管理 Autoscale**”窗口或配置其他页面上的设置。

重要提示：

- Autoscale 不允许同一天在不同计划中重叠。例如，如果在 schedule1 中选择了星期一之后又在 schedule2 中选择了星期一，则 schedule1 中的星期一将自动清除。
- 计划名称不区分大小写。
- 计划名称不能为空或仅包含空格。
- Autoscale 允许字符之间有空格。
- 计划名称不得包含以下字符：\ / ; : # . * ? = < > \| ( ) { } " ' `。
- Autoscale 不支持重复的计划名称。为每个计划输入不同的名称。
- Autoscale 不支持空计划。这意味着未选择日期的计划不会保存。

注意：

选定计划中包含的日期会突出显示，而未包含的日期则会灰显。

基于负载的设置

高峰时段。允许您为选定计划中应用的日期定义高峰时段。您可以通过右键单击水平条形图来执行此操作。定义高峰时段后，其余未定义的时间默认为非高峰时段。默认情况下，上午 7:00 到晚上 7:00 的时间段被定义为选定计划中包含的日期的**高峰时段**。

重要提示：

- 对于多会话操作系统交付组，高峰时段条形图用于容量缓冲区。
- 对于单会话操作系统交付组，高峰时段条形图用于容量缓冲区，并控制注销和/或断开连接后触发的操作。
- 您可以为多会话操作系统和单会话操作系统交付组以 30 分钟的粒度定义计划中包含的日期的峰值时间。或者，您可以使用 `New-BrokerPowerTimeScheme PowerShell` 命令。有关详细信息，请参阅Broker PowerShell SDK 命令。

容量缓冲区。允许您保留已开机计算机的缓冲区。值越小，成本越低。值越大，可确保优化的用户体验，以便在启动会话时，用户无需等待额外的计算机开机。默认情况下，高峰时段和非高峰时段的容量缓冲区为 10%。如果将容量缓冲区设置为 0（零），则用户在启动会话时可能需要等待额外的计算机开机。Autoscale 允许您分别为高峰时段和非高峰时段确定容量缓冲区。

杂项设置

提示：

- 您可以选择使用 Broker PowerShell SDK 配置杂项设置。有关详细信息，请参阅 Broker PowerShell SDK 命令。
- 要了解与断开连接和注销设置相关的 SDK 命令，请参阅 `<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`。

断开连接时。允许您指定断开连接的锁定计算机在会话断开连接后保持开机状态的时长，然后才将其挂起或关机。如果指定了时间值，则计算机将在指定的断开连接时间过去后挂起或关机，具体取决于您配置的操作。默认情况下，未对断开连接的计算机分配任何操作。您可以分别为高峰时段和非高峰时段定义操作。为此，请单击向下箭头，然后从菜单中选择以下选项之一：

- **无操作**。如果选择此选项，则计算机在会话断开连接后仍保持开机状态。Autoscale 不会对其执行任何操作。

- **挂起**。如果选择此选项，则当指定的断开连接时间过去后，Autoscale 会暂停计算机而不会将其关机。选择“**挂起**”后，以下选项将变为可用。
  - **在（分钟）内未重新连接时**。挂起的计算机在断开连接的用户重新连接时仍可供其使用，但不可供新用户使用。要使计算机再次可用以处理所有工作负载，请将其关机。指定超时（以分钟为单位），在此超时后 Autoscale 将其关机。
- **关机**。如果选择此选项，则当指定的断开连接时间过去后，Autoscale 会将计算机关机。

注意：

此选项仅在 Autoscale 用户界面中适用于单会话操作系统随机和静态交付组。

注销时。允许您指定计算机在会话注销后保持开机状态的时长，然后才将其挂起或关机。如果指定了时间值，则计算机将在指定的注销时间过去后挂起或关机，具体取决于您配置的操作。默认情况下，未对已注销的计算机分配任何操作。您可以分别为高峰时段和非高峰时段定义操作。为此，请单击向下箭头，然后从菜单中选择以下选项之一：

- **无操作**。如果选择此选项，则计算机在会话注销后仍保持开机状态。Autoscale 不会对其执行任何操作。
- **挂起**。如果选择此选项，则当指定的注销时间过去后，Autoscale 会暂停计算机而不会将其关机。
- **关机**。如果选择此选项，则当指定的注销时间过去后，Autoscale 会将计算机关机。

注意：

此选项仅在 Autoscale 用户界面中适用于单会话操作系统静态交付组。

电源管理单会话操作系统计算机，这些计算机在会话断开连接的情况下过渡到不同的时间段

重要提示：

- 此增强功能仅适用于会话断开连接的单会话操作系统计算机。它不适用于会话已注销的单会话操作系统计算机。

- 要使此增强功能生效，您需要为适用的交付组启用 Autoscale。否则，在时间段转换时不会触发断开连接电源策略操作。

在早期版本中，过渡到需要执行操作（断开连接操作为“**挂起**”或“**关机**”）的时间段的单会话操作系统计算机仍保持开机状态。如果计算机在不需要执行任何操作（断开连接操作为“**无**”）的时间段（高峰或非高峰时段）断开连接，则会发生这种情况。

从本版本开始，当指定的断开连接时间过去后，Autoscale 会根据为目标时间段配置的断开连接操作来挂起或关闭计算机。

例如，您为单会话操作系统交付组配置以下电源策略：

- 将 `PeakDisconnectAction` 设置为“无”
- 将 `OffPeakDisconnectAction` 设置为“关机”
- 将“OffPeakDisconnectTimeout”设置为“10”

注意：

有关断开连接操作电源策略的更多信息，请参阅 `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>` 和 `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`。

在早期版本中，在高峰时段会话断开连接的单会话操作系统计算机在从高峰期过渡到非高峰期时仍保持开机状态。从本版本开始，`OffPeakDisconnectAction` 和 `OffPeakDisconnectTimeout` 策略操作在时间段转换时应用于单会话操作系统计算机。因此，计算机在过渡到非高峰期 10 分钟后会关机。

如果您想恢复到以前的行为（即，对从高峰期过渡到非高峰期或从非高峰期过渡到高峰期且会话已断开连接的计算机不执行任何操作），请执行以下操作之一：

- 将“LegacyPeakTransitionDisconnectedBehaviour”注册表值设置为 1（true；启用以前的行为）。默认情况下，该值为 0（false；在时间段转换时触发断开连接电源策略操作）。
  - 路径: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - 名称: LegacyPeakTransitionDisconnectedBehaviour

  - 类型：REG_DWORD
  - 数据: 0x00000001 (1)

- 使用 `Set-BrokerServiceConfigurationData` PowerShell 命令配置设置。例如：
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

在周期转换时对其应用电源策略操作之前，计算机必须满足以下条件：

- 具有断开连接的会话。
- 没有待处理的电源操作。
- 属于一个单会话操作系统交付组，该交付组转换到不同的时间段。
- 有一个会话在某个时间段（高峰或非高峰时段）断开连接，并转换到分配了电源操作的时间段。

容量缓冲区的工作原理

容量缓冲区用于在当前需求中添加备用容量，以应对动态负载增加。需要注意以下两种情况：

- 对于多会话操作系统交付组，容量缓冲区定义为交付组总容量（以负载指数计）的百分比。有关负载指数的更多信息，请参阅负载指数。
- 对于单会话操作系统交付组，容量缓冲区定义为交付组总容量（以计算机数量计）的百分比。

注意：

在将 Autoscale 限制为标记计算机的场景中，容量缓冲区定义为交付组中标记计算机总容量（以负载指数计）的百分比。

Autoscale 允许您分别为高峰时段和非高峰时段设置容量缓冲区。容量缓冲区字段中的值越小，成本越低，因为 Autoscale 启动的备用容量越少。值越大，可确保优化的用户体验，从而使用户在启动会话时无需等待额外的计算机启动。默认情况下，容量缓冲区为 10%。

重要提示：

当总备用容量降至交付组总容量的“X”百分比以下时，容量缓冲区会导致计算机启动。这样做可以保留所需百分比的备用容量。

多会话操作系统交付组

机器何时启动?

重要提示：

如果选择了计划，Autoscale 将启动计划中配置为启动的所有计算机。Autoscale 会在计划期间保持指定数量的计算机处于启动状态，无论负载如何。

当交付组中已启动的计算机数量无法满足以负载指数计的缓冲区容量需求时，Autoscale 会启动额外的计算机。例如，假设您的交付组有 20 台计算机，并且有 3 台计算机计划作为基于计划的扩展的一部分启动，容量缓冲区为 20%。最终，在没有负载的情况下，将启动 4 台计算机。这是因为需要 4 x 10k 的负载指数作为缓冲区；因此至少需要启动 4 台计算机。这种情况可能发生在高峰时段、计算机负载增加、新会话启动以及向交付组添加新计算机时。请注意，Autoscale 仅启动符合以下条件的计算机：

- 计算机未处于维护模式。
- 计算机运行所在的虚拟机管理程序未处于维护模式。
- 机器当前已关机。
- 机器没有待处理的电源操作。

机器何时关机?

重要提示：

- 如果选择了计划，Autoscale 将根据该计划关闭机器。
- Autoscale 不会关闭在计划中配置为在计划期间保持开机的机器。

当有足够多的机器（包括缓冲区）来支持交付组中目标数量的开机机器时，Autoscale 会关闭多余的机器。这种情况可能发生在非高峰时段、机器负载降低、会话注销以及从交付组中移除机器时。Autoscale 仅关闭符合以下条件的机器：

- 机器及其运行所在的虚拟机管理程序未处于维护模式。
- 机器当前已开机。

- 机器已注册为可用或在启动后等待注册。
- 机器没有活动会话。
- 机器没有待处理的电源操作。
- 机器满足指定的关机延迟。这意味着机器已开机至少“X”分钟，其中“X”是为交付组指定的关机延迟。

示例场景

假设您有以下场景：

- **交付组配置**。您希望 Autoscale 管理电源的交付组包含 10 台机器（M1 到 M10）。
- **Autoscale 配置**
  - 容量缓冲区设置为 10%。
  - 所选计划中不包含任何计算机。

此场景按以下顺序执行：

1. 没有用户登录。
2. 用户会话增加。
3. 更多用户会话启动。
4. 由于会话终止，用户会话负载降低。
5. 用户会话负载进一步降低，直到会话负载仅由本地资源处理。

有关 Autoscale 在上述场景中如何工作的详细信息，请参阅下文。

- 无用户负载（初始状态）
  - 一台计算机（例如 M1）已开机。计算机开机是因为配置了容量缓冲区。在这种情况下，10（计算机数量）x 10,000（负载指数）x 10%（配置的容量缓冲区）等于 10,000。因此，一台计算机已开机。
  - 已开机计算机 (M1) 的负载指数值处于基线负载（负载指数等于 0）。
- 第一个用户登录
  - 会话被定向到在计算机 M1 上托管。
  - 已开机计算机 M1 的负载指数增加，并且计算机 M1 不再处于基线负载。
  - Autoscale 开始启动一台额外的计算机 (M2) 以满足需求，因为配置了容量缓冲区。
  - 计算机 M2 的负载指数值处于基线负载。

- 用户增加负载
  - 会话在计算机 M1 和 M2 之间进行负载平衡。因此，已启动计算机（M1 和 M2）的负载指数增加。
  - 总备用容量在负载指数方面仍高于 10,000。
  - 计算机 M2 的负载指数值不再处于基线负载。
- 更多用户会话启动
  - 会话在计算机（M1 和 M2）之间进行负载平衡。因此，已启动计算机（M1 和 M2）的负载指数进一步增加。
  - 当总备用容量在负载指数方面降至 10,000 以下时，Autoscale 开始启动一台额外的计算机 (M3) 以满足需求，因为配置了容量缓冲区。
  - 计算机 M3 的负载指数值处于基线负载。
- 更多用户会话启动
  - 会话在计算机（M1 到 M3）之间进行负载平衡。因此，已启动计算机（M1 到 M3）的负载指数增加。
  - 总备用容量在负载指数方面高于 10,000。
  - 计算机 M3 的负载指数值不再处于基线负载。
- 由于会话终止，用户会话负载降低
  - 用户从会话注销或空闲会话超时后，机器 M1 到 M3 上释放的容量将重新用于托管其他用户启动的会话。
  - 当总备用容量在负载指数方面增加到 10,000 以上时，Autoscale 会将其中一台机器（例如 M3）置于耗尽状态。因此，除非发生新的变化，否则其他用户启动的会话将不再定向到该机器。例如，最终用户负载再次增加或其它机器负载最低。
- 用户会话负载持续降低
  - 机器 M3 上的所有会话终止且指定的关机延迟超时后，Autoscale 会关闭机器 M3。
  - 更多用户终止其会话后，已开机机器（M1 和 M2）上释放的容量将重新用于托管其他用户启动的会话。
  - 当总备用容量在负载指数方面增加到 10,000 以上时，Autoscale 会将其中一台机器（例如 M2）置于耗尽状态。因此，其他用户启动的会话将不再定向到该机器。
- 用户会话负载持续降低，直到没有会话

- 机器 M2 上的所有会话终止且指定的关机延迟超时后，Autoscale 会关闭机器 M2。
- 已开机机器 (M1) 的负载指数值处于基线负载。由于配置了容量缓冲区，Autoscale 不会将机器 M1 置于耗尽状态。

> **注意：**
>
> 对于多会话操作系统交付组，当用户注销会话时，对桌面的所有更改都将丢失。但是，如果已配置，用户特定的设置会随用户配置文件漫游。

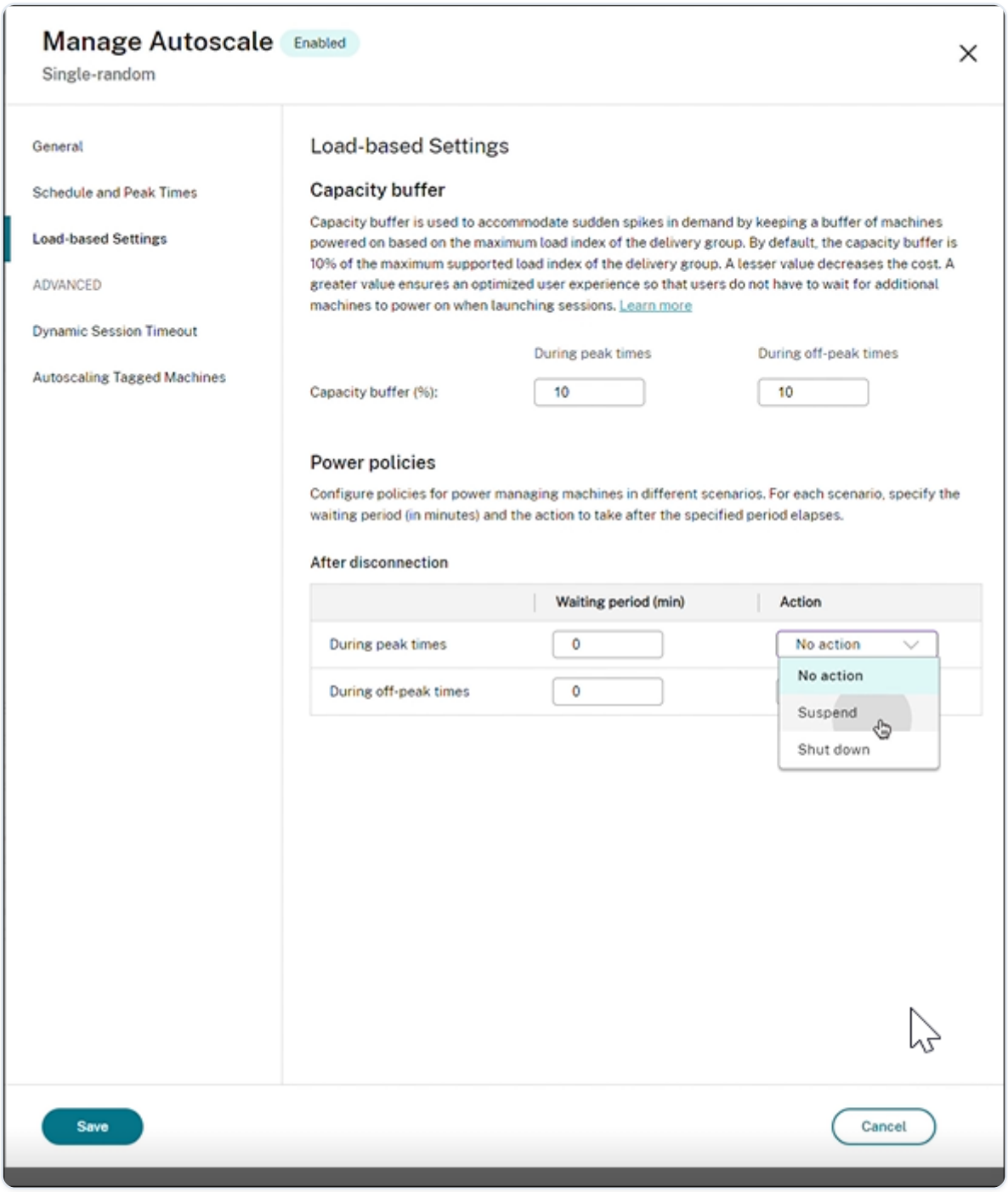
单会话操作系统随机交付组

容量缓冲区用于通过根据交付组中的机器总数保持一定数量的开机机器来适应需求的突然激增。默认情况下，容量缓冲区是交付组中机器总数的 10%。

如果机器数量（包括容量缓冲区）超过当前已开机机器的总数，则会启动额外的机器以满足需求。如果机器数量（包括容量缓冲区）少于当前已开机机器的总数，则多余的机器将根据您配置的操作关闭或挂起。

电源策略

配置策略以管理不同场景下机器的电源。对于每个场景，您可以指定等待时间（以分钟为单位）以及指定时间结束后要执行的操作。电源策略适用于单会话操作系统随机交付组和单会话操作系统静态交付组。



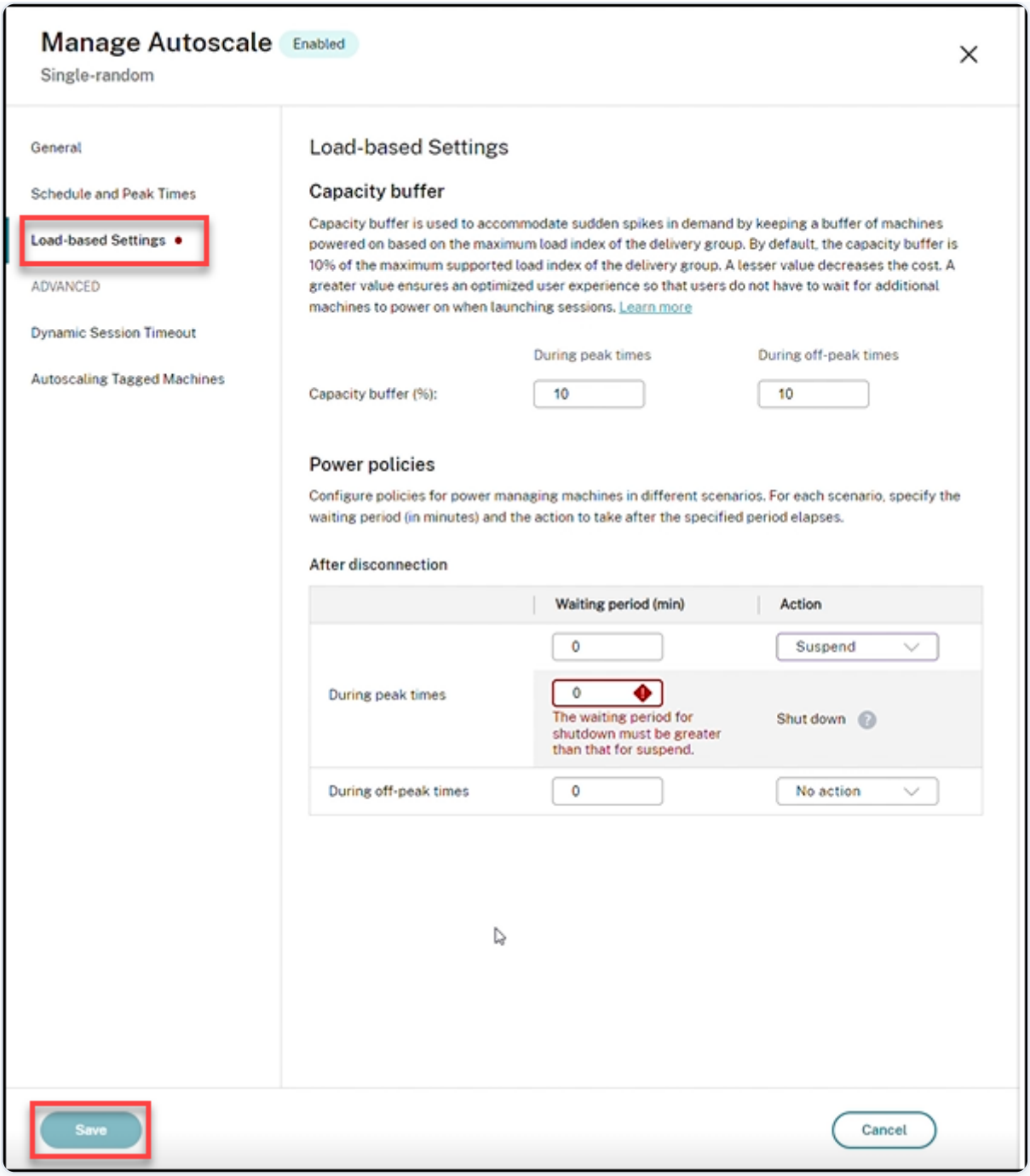
断开连接后，以下设置适用于高峰时段和非高峰时段：

- 您可以从下拉列表中设置等待时间（以分钟为单位）以及操作，例如无操作、挂起或关机。
- 如果选择挂起操作，请配置额外的等待时间以关闭计算机。

注意：

- 在高峰时段和非高峰时段，关机操作的等待时间必须大于挂起操作的等待时间。

- 挂起的计算机仅在断开连接的用户重新连接时才可访问。要使挂起的计算机可供新用户使用，请将其关闭。
- 如果挂起和关机字段的时间设置不正确，则会禁用**保存**选项，并且导航项旁边还会出现一个红点，指示设置错误。



例如

- 如果您将等待时间设置为 12 分钟，并将第一个操作选择为无操作，那么在 12 分钟结束后，计算机将继续保持开机状态。

- 如果您将等待时间设置为 15 分钟，并将第一个操作选择为挂起，将第二个等待时间设置为 20 分钟，那么在 15 分钟结束后，计算机将挂起。在第二个等待时间结束后，计算机将关机。
- 如果您将等待时间设置为 18 分钟，并将第一个操作选择为关机，那么在 18 分钟结束后，计算机将关机。

示例场景

假设您有以下场景：

- **交付组配置**。您希望 Autoscale 管理电源的交付组包含 10 台计算机（M1 到 M10）。
- **Autoscale 配置**
  - 容量缓冲区设置为 10%。
  - 所选计划中不包含任何计算机。

此场景按以下顺序执行：

1. 没有用户登录。
2. 用户会话增加。
3. 更多用户会话启动。
4. 由于会话终止，用户会话负载减少。
5. 用户会话负载进一步减少，直到会话负载仅由本地资源处理。

有关 Autoscale 在上述场景中如何工作的详细信息，请参见下文。

- 无用户负载（初始状态）
  - 一台计算机 (M1) 已开机。计算机开机是因为配置了容量缓冲区。在这种情况下，10（计算机数量）x 10%（配置的容量缓冲区）等于 1。因此，一台计算机已开机。
- 第一个用户登录
  - 用户首次登录以使用桌面时，会从托管在已开机计算机上的桌面池中为用户分配一个桌面。在这种情况下，会从计算机 M1 为用户分配一个桌面。
  - Autoscale 开始开机一台额外的计算机 (M2) 以满足需求，因为配置了容量缓冲区。
- 第二个用户登录
  - 用户从机器 M2 分配到一个桌面。
  - 由于配置了容量缓冲区，Autoscale 开始启动一台额外的机器 (M3) 以满足需求。
- 第三位用户登录

  - 用户从机器 M3 分配到一个桌面。
  - 由于配置了容量缓冲区，Autoscale 开始启动一台额外的机器 (M4) 以满足需求。
- 一位用户注销
  - 用户注销或用户桌面超时后，释放的容量（例如 M3）可用作缓冲区。因此，由于容量缓冲区配置为 10%，Autoscale 开始关闭机器 M4。
- 更多用户注销，直到没有用户
  - 更多用户注销后，Autoscale 关闭机器（例如 M2 或 M3）。
  - 即使没有用户留下，Autoscale 也不会关闭剩余的一台机器（例如 M1），因为该机器被保留为备用容量。

> **注意：**
>
> 对于单会话操作系统随机交付组，当用户注销会话时，对桌面的所有更改都将丢失。但是，如果配置，用户特定的设置会随用户配置文件漫游。

单会话操作系统静态交付组

容量缓冲区用于通过根据交付组中未分配机器的总数保持一定数量的已开机未分配机器来应对突发的需求高峰。默认情况下，容量缓冲区是交付组中未分配机器总数的 10%。

> **重要提示：**
>
> 交付组中的所有机器都分配完毕后，容量缓冲区在开机或关机方面不起作用。

> 如果机器数量（包括容量缓冲区）超过当前已开机机器的总数，则会启动额外的未分配机器以满足需求。如果机器数量（包括容量缓冲区）少于当前已开机机器的总数，则会关闭或挂起多余的机器，具体取决于您配置的操作。

对于单会话操作系统静态交付组，Autoscale：

- 仅当适用的单会话操作系统交付组的 `AutomaticPowerOnForAssigned` 属性设置为 true 时，才在高峰时段开启分配的计算机，在非高峰时段关闭。
- 如果计算机已关闭，并且其所属交付组的 `AutomaticPowerOnForAssignedDuringPeak` 属性设置为 true，则在高峰时段自动开启该计算机。

要了解容量缓冲区如何与分配的计算机配合使用，请考虑以下事项：

- 容量缓冲区仅在交付组具有一台或多台未分配的计算机时才起作用。
- 如果交付组没有未分配的计算机（交付组中的所有计算机都已分配），则容量缓冲区在开启或关闭计算机方面不起作用。
- `AutomaticPowerOnForAssignedDuringPeak` 属性决定了在高峰时段是否开启分配的计算机。如果设置为 true，Autoscale 会在高峰时段保持计算机开启。即使计算机已关闭，Autoscale 也会将其开启。

电源策略

配置策略以管理不同场景下计算机的电源。对于每种场景，您可以指定等待时间（以分钟为单位）以及指定时间结束后要执行的操作。电源策略适用于单会话操作系统随机交付组和单会话操作系统静态交付组。

单会话操作系统静态交付组电源策略设置(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/single-session-os-static-dg-power-policies-settings.png)

对于**断开连接后**和**注销后**，以下设置在高峰时段和非高峰时段均适用：您可以从下拉列表中设置等待时间（以分钟为单位）以及操作，例如无操作、挂起或关机。

如果 Autoscale 开启计算机后没有用户登录，以下设置仅在高峰时段适用：您可以在高峰时段从下拉列表中设置等待时间（以分钟为单位）以及操作，例如无操作、挂起或关机。

示例场景

假设您有以下场景：

- **交付组配置**。您希望 Autoscale 管理电源的交付组包含 10 台计算机（M1 到 M10）。
- **Autoscale 配置**
  - 机器 M1 到 M3 已分配，机器 M4 到 M10 未分配。
  - 高峰和非高峰时段的容量缓冲区设置为 10%。
  - 根据选定的计划，Autoscale 在上午 09:00 到下午 06:00 之间对机器进行电源管理。

有关 Autoscale 在上述场景中如何工作的详细信息，请参见下文。

- 计划开始时间 – 上午 09:00
  - Autoscale 开启机器 M1 到 M3 的电源。
  - 由于配置了容量缓冲区，Autoscale 会开启一台额外的机器（例如 M4）的电源。机器 M4 未分配。

- 第一个用户登录
  - 用户首次登录以使用桌面时，系统会从托管在未分配的已开机机器上的桌面池中为该用户分配一个桌面。在此示例中，系统会从机器 M4 为该用户分配一个桌面。该用户后续登录时将连接到首次使用时分配的同一桌面。
  - 由于配置了容量缓冲区，Autoscale 开始开启一台额外的机器（例如 M5）的电源以满足需求。
- 第二个用户登录
  - 系统会从未分配的已开机机器中为该用户分配一个桌面。在此示例中，系统会从机器 M5 为该用户分配一个桌面。该用户后续登录时将连接到首次使用时分配的同一桌面。
  - 由于配置了容量缓冲区，Autoscale 开始开启一台额外的机器（例如 M6）的电源以满足需求。
- 用户注销
  - 当用户从其桌面注销或桌面超时时，Autoscale 会在上午 09:00 到下午 06:00 之间保持机器 M1 到 M5 的电源开启。当这些用户下次登录时，他们将连接到首次使用时分配的同一桌面。
  - 未分配的计算机 M6 正在等待为传入的未分配用户提供桌面。
- 计划结束 – 下午 06:00
  - 下午 06:00，Autoscale 关闭计算机 M1 到 M5。
  - 由于配置了容量缓冲区，Autoscale 保持未分配的计算机 M6 处于开机状态。该计算机正在等待为传入的未分配用户提供桌面。
  - 在交付组中，计算机 M6 到 M10 是未分配的计算机。

动态会话超时

此功能允许您为高峰和非高峰使用时间配置断开连接和空闲会话超时，以实现更快的计算机排空和节省成本。此功能适用于：

- 单会话和多会话操作系统计算机。
- 交付组中的所有计算机，无论它们是否标记为自动缩放。

VDA 会报告空闲时间超过 10 分钟的会话的空闲时间，因此动态会话超时无法在会话空闲 10 分钟内断开空闲会话。较小的值会更快地移除滞留会话，从而降低成本。

Autoscale 多会话操作系统 - 动态会话超时(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/autoscale-session-timeout-ms.png)

注意：

- 此功能始终适用于多会话操作系统交付组。
- 对于单会话操作系统交付组，此功能适用于版本 2206 CR 或更高版本，或 2203 LTSR CU3 或更高版本的 VDA。确保这些 VDA 至少注册到 Citrix Cloud™ 一次。不可用时，将显示以下用户界面：

动态会话超时不可用(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/autoscale-session-timeout-unavailable.png)

- Autoscale™ 动态超时旨在节省成本。如果用于安全目的，配置的超时可能会与您的 GPO 或管理控制台策略冲突。发生冲突时，较短的超时将优先。

空闲会话超时。启用或禁用一个计时器，该计时器指定在没有用户输入的情况下保持不间断用户连接的时间。计时器到期后，会话将进入断开连接状态，并应用**断开连接会话超时**。如果**断开连接会话超时**被禁用，则会话不会注销。

重要提示：

- 如果您指定的值小于或等于 10 分钟（600 秒），Autoscale 会在相关会话空闲 10 分钟后断开连接。这是因为 Autoscale 依赖于 VDA 报告的会话空闲时间。VDA 仅报告空闲时间超过 10 分钟的会话的空闲时间。
- 如果用户在达到空闲会话超时的最后 5 分钟内与空闲会话进行交互，则该会话仍可进入断开连接状态。

断开连接会话超时。启用或禁用一个计时器，该计时器指定断开连接的桌面在会话注销之前保持锁定的时间。如果启用，则在计时器到期时注销断开连接的会话。

常见问题

动态会话超时功能是否仅适用于标记为自动缩放的计算机?

动态会话超时功能适用于交付组中的所有计算机，无论它们是否已标记为自动缩放。

当会话因动态会话超时而注销时，未标记的计算机是否也包含在已标记计算机的自动缩放目标中?

动态会话超时功能与自动缩放标记功能无关。如果动态会话超时导致会话终止，则在计算机排空直到关闭的过程中，未标记的计算机也可能被关闭。

自动缩放标记的计算机（云爆发）

> **注意：**
>
> 此功能以前称为“限制自动缩放”。

简介

Autoscale 提供了仅管理交付组中一部分机器电源的灵活性。为此，请对一台或多台机器应用标签，然后配置 Autoscale 仅管理已标记机器的电源。

此功能在云爆发用例中非常有用，在这些用例中，您希望使用本地资源（或预留的公共云实例）在基于云的资源处理额外需求（即爆发工作负载）之前处理工作负载。要让本地计算机（或预留实例）首先处理工作负载，您必须结合使用标记限制和区域首选项。

标记限制指定由 Autoscale 进行电源管理的计算机。区域首选项指定首选区域中的计算机来处理用户启动请求。有关详细信息，请参阅标记和区域首选项。

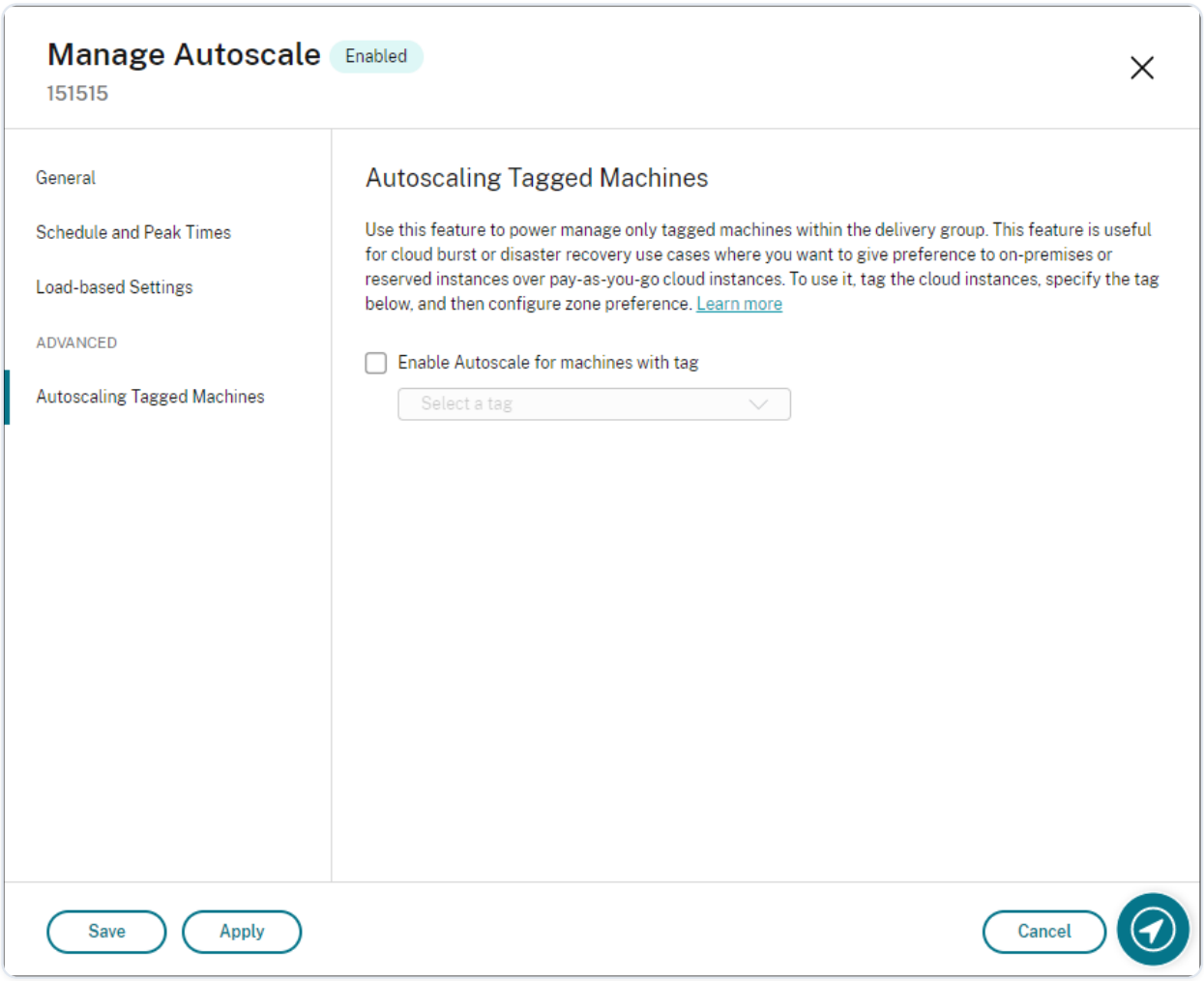
要自动缩放某些标记的计算机，您可以使用“管理”控制台或 PowerShell。

使用“管理”控制台自动缩放某些标记的计算机

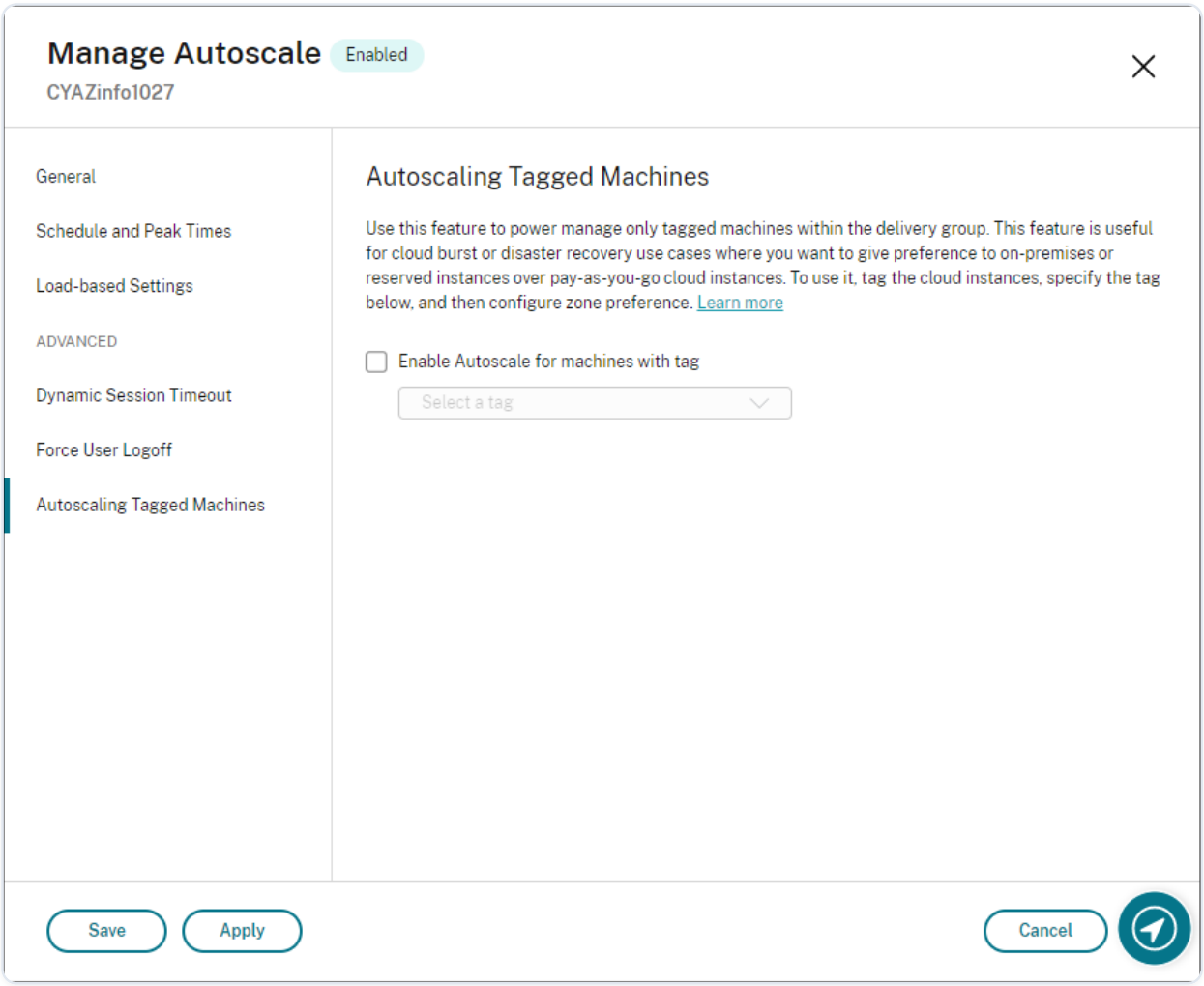
要自动缩放某些标记的计算机，请完成以下步骤：

1. 创建一个标记，并将该标记应用于交付组中适用的计算机。有关详细信息，请参阅管理标记和标记限制。
2. 选择交付组，然后打开“**管理自动缩放**”向导。
3. 在“**自动缩放标记的计算机**”页面上，选择“**为带有标记的计算机启用自动缩放**”，从列表中选择一个标记，然后单击“**应用**”以保存更改。

   单会话操作系统*静态*和*随机*交付组的用户界面：



*多会话操作系统交付组*的用户界面：



警告：

- 自动缩放带有特定标记的计算机可能会导致直方图自动更新，以反映每个标记的计算机数量。在“**计划和高峰时间**”页面上，您可以根据需要手动为每个时间段分配计算机。
- 您不能删除正在标记的计算机上使用的标签。要删除该标签，您必须首先删除标签限制。

应用标签限制后，您可能希望稍后将其从交付组中删除。为此，请转到 **管理 Autoscale > 自动缩放标记的计算机** 页面，然后清除 **为带有标签的计算机启用 Autoscale**。

警告：

- 如果您在未清除 **为带有标签的计算机启用 Autoscale** 的情况下从适用的计算机中删除标签，则在打开 **管理 Autoscale** 向导时可能会收到警告。从计算机中删除标签可能导致

> Autoscale 没有可管理的计算机，因为您在 Autoscale 中指定的标签已失效。要解决此警告，请转到 **自动缩放标记的计算机** 页面，删除无效标签，然后单击 **应用** 以保存更改。

控制 Autoscale 何时启动资源

您还可以根据未标记计算机的使用情况，控制 Autoscale 何时开始启动标记的计算机。这有助于您进一步优化标记或公共云工作负载的消耗。

为此，请完成以下步骤：

1. 在 **自动缩放标记的计算机** 页面上，选择 **控制 Autoscale 何时开始启动标记的计算机**。
2. 输入您希望在高峰时段和非高峰时段达到的未标记计算机使用率百分比，然后单击 **应用**。支持的值：0–100。

控制 Autoscale 何时开始启动标记的计算机(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/autoscale-powers-on-tagged-machines.png)

> **提示：**
>
> 此百分比控制 Autoscale 何时开始启动标记的计算机。当百分比低于阈值（默认值 10%）时，Autoscale 开始启动标记的计算机。当百分比超过阈值时，Autoscale 进入关机模式。输入百分比时，请考虑两种情况：
>
> - 对于单会话操作系统交付组：该值定义为处于空闲状态的未标记计算机总数的百分比。示例：您有 10 台未标记的单会话操作系统计算机。当只剩一台没有会话时，Autoscale 开始启动一台标记的计算机。
> - 对于多会话操作系统交付组：该值定义为可用未标记计算机的总容量（以负载指数计）的百分比。示例：您有 10 台未标记的多会话操作系统计算机。当它们负载达到 90% 时，Autoscale 开始启动一台标记的计算机。

使用 PowerShell 自动缩放某些标记的计算机

> **注意：**
>
> `Get-BrokerMachine` PowerShell 命令已弃用。请使用 `Get-BrokerMachineV2` 作为替代方案。

要直接使用 PowerShell SDK，请完成以下步骤：

1. **创建标签。** 使用 New-Brokertag PowerShell 命令创建标签。
   - 例如：`$managed = New-BrokerTag Managed`。在这种情况下，此标记名为“Managed”。有关 New-Brokertag PowerShell 命令的详细信息，请参阅 `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>`。
2. **将标记应用于计算机**。使用 Get-Brokermachine PowerShell 命令将标记应用于您希望 Autoscale 进行电源管理的目录中的计算机。
   - 例如：`Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`。在这种情况下，此目录名为“cloud”。
   - 有关 Get-Brokermachine PowerShell 命令的详细信息，请参阅 `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>`。

   注意：

   应用标记后，您可能会向目录中添加新计算机。该标记*不会*自动应用于这些新计算机。
3. **将带标记的计算机添加到您希望 Autoscale 进行电源管理的交付组。** 使用 Get-BrokerDesktopGroup PowerShell 命令向包含计算机的交付组添加标记限制（换句话说，即“将启动限制为具有标记 X 的计算机”）。
   - 例如：`Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`。在这种情况下，交付组的 UID 为 1。
   - 有关 Get-BrokerDesktopGroup PowerShell 命令的详细信息，请参阅 `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`。

应用标记限制后，您可能希望稍后将其从交付组中删除。为此，请使用 Get-BrokerDesktopGroup PowerShell 命令。

示例：`Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscaleTagUid $null`。在这种情况下，交付组的 UID 为 1。

注意：

未标记的计算机在用户将其关闭后会自动重新启动。此行为可确保它们更快地可用于处理工作负载。可以使用 `Set-BrokerDesktopGroup` 的 `AutomaticRestartForUntaggedMachines` 属性在每个桌面组上启用或禁用此功能。有关详细信息，请参阅 `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`。

示例场景

假设您有以下方案：

- **计算机目录配置**。有两个计算机目录（C1 和 C2）。
  - 目录 C1 包含 5 台计算机（M1 到 M5），这些计算机位于本地部署中。
  - 目录 C2 包含 5 台计算机（M6 到 M10），这些计算机位于云部署中。
- **标签限制**。一个名为“Cloud”的标签被创建并应用于目录 C2 中的机器 M6 到 M10。
- **区域配置**。创建了两个区域（Z1 和 Z2）。
  - 包含目录 C1 的区域 Z1 对应于本地部署。
  - 包含目录 C2 的区域 Z2 对应于云部署。
- **交付组配置**
  - 交付组包含 10 台机器（M1 到 M10），其中 5 台来自目录 C1（M1 到 M5），5 台来自目录 C2（M6 到 M10）。
  - 机器 M1 到 M5 手动开机，并在整个计划期间保持开机状态。
- **Autoscale 配置**
  - 容量缓冲区设置为 10%。
  - Autoscale 仅管理带有“Cloud”标签的机器。在这种情况下，Autoscale 管理云机器 M6 到 M10。
- **已发布的应用程序或桌面配置**。为已发布的桌面（例如）配置了区域首选项，其中对于用户启动请求，区域 Z1 优先于区域 Z2。
  - 区域 Z1 被配置为已发布的桌面的首选区域（主区域）。

该场景按以下顺序执行：

1. 没有用户登录。
2. 用户会话增加。
3. 用户会话进一步增加，直到所有可用的本地计算机都被占用。
4. 更多用户会话启动。
5. 由于会话终止，用户会话减少。
6. 用户会话进一步减少，直到会话负载仅由本地计算机处理。

有关 Autoscale 在上述场景中如何工作的详细信息，请参见下文。

- 无用户负载（初始状态）
  - 本地计算机 M1 到 M5 都已开机。
  - 云中的一台计算机（例如 M6）已开机。该计算机开机是因为配置了容量缓冲区。在这种情况下，10（计算机数量）x 10,000（负载指数）x 10%（配置的容量缓冲区）等于 10,000。因此，一台计算机已开机。
  - 所有已开机计算机（M1 到 M6）的负载指数值处于基线负载（负载指数等于 0）。
- 用户登录
  - 会话通过配置的区域首选项被定向到计算机 M1 到 M5 上托管，并在这些本地计算机之间进行负载均衡。
  - 已开机计算机（M1 到 M5）的负载指数值增加。
  - 已开机计算机 M6 的负载指数值处于基线负载。
- 用户增加负载，消耗所有本地资源
  - 会话通过配置的区域首选项被定向到计算机 M1 到 M5 上托管，并在这些本地计算机之间进行负载均衡。
  - 所有已开机计算机（M1 到 M5）的负载指数值已达到 10,000。
  - 已开机计算机 M6 的负载指数值保持在基线负载。
- 又有一名用户登录
  - 会话溢出区域首选项，并被定向到云计算机 M6 上托管。
  - 所有已开机计算机（M1 到 M5）的负载指数值已达到 10,000。

  - 已开机计算机 M6 的负载指数值增加，不再处于基线负载。当总备用容量的负载指数降至 10,000 以下时，Autoscale 会根据配置的容量缓冲区启动一台额外的计算机 (M7) 以满足需求。请注意，启动计算机 M7 可能需要一些时间。因此，在计算机 M7 准备就绪之前可能会有延迟。

- 更多用户登录
  - 会话被定向到计算机 M6 上托管。
  - 所有已开机计算机（M1 到 M5）的负载指数值已达到 10,000。
  - 已开机计算机 M6 的负载指数值进一步增加，但总备用容量的负载指数仍高于 10,000。
  - 已开机计算机 M7 的负载指数值保持在基线负载。
- 更多用户登录
  - 计算机 M7 准备就绪后，会话将被定向到计算机 M6 和 M7 上托管，并在这些计算机之间进行负载平衡。
  - 所有已开机计算机（M1 到 M5）的负载指数值已达到 10,000。
  - 计算机 M7 的负载指数值不再处于基线负载。
  - 已开机机器（M6 和 M7）的负载指数值增加。
  - 总备用容量在负载指数方面仍高于 10,000。
- 由于会话终止，用户会话负载降低。
  - 用户从其会话注销或空闲会话超时后，机器 M1 到 M7 上释放的容量将重新用于托管其他用户启动的会话。
  - 当总备用容量在负载指数方面增加到 10,000 以上时，Autoscale 会将其中一台云机器（M6 到 M7）置于排空状态。因此，除非发生新的变化（例如，用户负载再次增加或其它云机器负载最低），否则其他用户启动的会话将不再定向到该机器（例如 M7）。
- 用户会话负载进一步降低，直到不再需要一台或多台云机器。
  - 机器 M7 上的所有会话终止且指定的关机延迟超时后，Autoscale 会关闭机器 M7。
  - 所有已开机机器（M1 到 M5）的负载指数值可能会降至 10,000 以下。
  - 已开机机器（M6）的负载指数值降低。
- 用户会话进一步减少，直到不再需要云机器。
  - 即使机器 M6 上没有用户会话，Autoscale 也不会将其关闭，因为它被保留为备用容量。

- 由于配置了容量缓冲区，Autoscale 会保持剩余的云机器 M6 处于开机状态。该机器正在等待为传入用户提供桌面。
- 只要本地机器有可用容量，会话就不会被定向到机器 M6 上托管。

Autoscale™ 插件

Autoscale 插件是一种插件模型，您可以通过它直接操作虚拟机的电源管理。您可以偏离与虚拟机电源管理相关的标准 Autoscale 设置，转而针对不同场景使用不同的设置。当前可用的插件有：

- Autoscale 节假日插件
- 智能 Autoscale 计划插件

Autoscale 节假日插件

您可以使用 Autoscale 节假日插件来处理节假日的不同设置。例如，在工作日，您希望大部分虚拟机保持开机状态。但是，默认情况下（没有插件），工作日计划仍然适用于公共节假日。为了处理这种情况，该插件允许在指定的节假日日期关闭虚拟机。

使用 Studio 创建自定义节假日计划

使用 Studio 创建自定义计划，以便在特定日期（例如节假日）关闭交付组中未使用的虚拟机，从而减少不必要的资源消耗。

> **注意：**
>
> - 自定义计划在创建后一天生效。
> - 对于已标记的计算机，此功能仅适用于交付组内已标记的计算机。

要创建自定义计划：

1. 在 Studio 中，转到 **交付组**。右键单击交付组并选择 **管理 Autoscale**。
2. 在 **常规** 页面上，选择 **启用 Autoscale**。
3. 在**计划**页面上，单击**创建计划**。
4. 输入计划名称。
5. 选择一个或多个您希望交付组中的虚拟机关闭的日期。

   如果要将此计划另存为模板以供其他交付组使用，请单击 **另存为模板**。
6. 点击“**完成**”以创建自定义计划。

您现在应该会在“**计划**”页面上的“**自定义**”下看到已创建的自定义计划。

要编辑自定义计划：

1. 对于要编辑的计划，单击“**操作**”下的铅笔图标。您可以进行以下编辑：
   - 禁用自定义计划：关闭“**启用**”切换按钮。
   - 更改或应用模板。
   - 更改计划的名称。
   - 更改计划的日期。
2. 点击“**完成**”以应用更改。

您还可以删除自定义计划。

> **注意：**
>
> 删除交付组也会删除其自定义计划。已保存的模板不会被删除。

使用 PowerShell 配置节假日日期

将 Autoscale 节假日插件与交付组关联，并配置节假日日期，以便插件可以在配置的日期关闭 VM。为此，请运行以下命令：

1. 运行 `Get-BrokerAutoscalePlugin` 以获取节假日插件的 UID。

   ```
   (Get-BrokerAutoscalePlugin -Name
   Citrix.AutoscalePlugin.HolidaySchedule).Uid
   ```

   记下 `HolidaySchedule` 插件的 UID 值。假设 `HolidaySchedule` 插件的 UID 为 1。
2. 获取要与插件关联的交付组的 UID。例如：

   ```
   $dgUid = (Get-BrokerDesktopGroup 'My Group Name').Uid
   ```

3. 将 `HolidaySchedule` 插件与交付组 `(-AutoscalePluginUid “<HolidaySchedule plugin UID>”)` 关联，并指定所需的节假日日期。例如：

```
New-BrokerAutoscaleGroupPlugin -Name "Company Holidays"
-DesktopGroupUid $dgUid -AutoscalePluginUid 1 -Configuration
'{"Holidays":["2024-11-28","2024-11-29","2024-12-25"]}'
```

记下创建的 `AutoscaleGroupPlugin` 的 UID（插件与交付组之间的关联）。

注意：

关联的名称在给定交付组的关联中必须是唯一的。例如，一个交付组只能有一个名为“公司假期”的关联，但一个或多个其他交付组也可能有名为“公司假期”的关联。

更改节假日日期

您可以使用 `Set-BrokerAutoscaleGroupPlugin` PowerShell 命令并指定 `AutoscaleGroupPlugin` 的 UID 来更改指定的节假日日期。例如，假设 `AutoscaleGroupPlugin` 的 UID 为 2。

```
Set-BrokerAutoscaleGroupPlugin 2 -Configuration '{"Holidays":
["2024-11-28","2024-11-29"]}'
```

重要注意事项

使用 Autoscale 节假日插件时，请考虑以下事项：

- 当 Autoscale 节假日插件处于活动状态时，所有 VDA 都处于关闭状态，系统不会以降低的容量运行。任何新的启动请求都会得到处理，但用户可能会因为 VDA 正在准备启动而遇到延迟。
- 交付组必须指定时区。
- 日期格式必须为“yyyy-mm-dd”。
- 计划覆盖（覆盖标准 Autoscale 设置）会在前一天 22:00 提前一天生成。22:00 之后，无法添加、删除或更改下一天的任何计划覆盖。
- 同一个 Autoscale 插件可以与多个交付组关联。为每个交付组运行 `New-BrokerAutoscaleGroupPlugin`，然后配置该组所需的节假日。
- 最新的 `Set-BrokerAutoscalePlugin -Configuration` 命令会用指定的新节假日覆盖所有现有节假日。

智能 Autoscale 计划插件

智能 Autoscale 是一种数据驱动的 Autoscale 功能，具有最少的管理设置，可让您配置交付组的性能目标。性能目标值范围为 1 到 99，该值指定了用户体验和成本之间的目标平衡：

- 较低的值优先考虑成本节约。
- 高值优先考虑用户体验。

性能目标与历史使用数据相结合，可计算一天中每个 30 分钟块的最佳缓冲区容量（要开机的 VM 数量）。因此，每天开始时会计算 48 个最佳缓冲区容量。

最佳缓冲区容量取代了高峰/非高峰缓冲区容量和池大小，以管理可用计算机。

用于计算最佳缓冲区容量的历史使用数据包括：

- 客户的每分钟登录用户数
- 平均虚拟机开机时间（以分钟为单位）
- 平均虚拟机密度（每台虚拟机用户数）.

先决条件

启用智能自动缩放的先决条件如下：

- 交付组必须是共享交付组。
- 交付组必须已启用自动缩放。
- 在为桌面组配置智能自动缩放之前，交付组必须至少有 90 天的历史数据。您可以使用以下命令将 `ConnectionLogLifetimeHours` 从 48 小时增加到 90 天：

```
Set-BrokerServiceConfigurationData Logging.ConnectionLogLifetimeHours
-SettingValue 2160.
```

重要注意事项

- 交付组必须指定时区。
- 计划覆盖项会在前一天 22:00 提前一天生成。22:00 之后，无法添加、删除或更改下一天的任何计划覆盖项。
- 同一个自动缩放插件可以与多个交付组关联。为每个交付组运行 `New-BrokerAutoscaleGroupPlugin`，然后配置该组所需的性能目标。
- 最新的 `Set-BrokerAutoscalePlugin -Configuration` 命令将使用指定的新假期覆盖所有现有假期。

配置性能目标

将 `IntelligentAutoscaleSchedules` 插件与交付组关联并配置性能目标，以便性能目标与历史使用数据相结合，可以计算一天中每个 30 分钟块的最佳缓冲区容量。为此，请运行以下命令：

1. 运行 `Get-BrokerAutoscalePlugin` 以获取智能 Autoscale 插件的 UID。记下 `IntelligentAutoscaleSchedules` 插件的 UID 值。

   ```
   (Get-BrokerAutoscalePlugin -Name
   Citrix.AutoscalePlugin.IntelligentAutoscaleSchedules).Uid
   ```

   假设 `IntelligentAutoscaleSchedules` 插件的 UID 为 2。

2. 获取要将插件与之关联的交付组的 UID。例如：

   ```
   $dgUid = (Get-BrokerDesktopGroup 'My Group Name').Uid
   ```

3. 将 `IntelligentAutoscaleSchedules` 插件与交付组 (`-AutoscalePluginUid "<IntelligentAutoscaleSchedules value>"`) 关联，并指定性能目标值。

   ```
   New-BrokerAutoscaleGroupPlugin -DesktopGroupUid $dgUid
   -AutoscalePluginUid 2 -Configuration '{"PerformanceTarget":70}'
   ```

4. 记下创建的 `AutoscaleGroupPlugin` 的 UID（插件与交付组之间的关联）。

更新性能目标值

您可以使用 `Set-BrokerAutoscaleGroupPlugin` PowerShell 命令并指定 `AutoscaleGroupPlugin` 的 UID 来更新指定的性能目标值。例如，假设 AutoscaleGroupPlugin 的 UID 为 2。

```
Set-BrokerAutoscaleGroupPlugin 2 -Configuration '{"PerformanceTarget":70}'
```

配置 Autoscale 组插件自动批准

要允许计划覆盖（覆盖标准 Autoscale 设置），请在 `BrokerAutoscaleGroupPlugin` 中配置以下两个属性：

- `AutoApprove`
  - 如果 `True` ：表示插件生成的任何计划覆盖都将自动接受。

  - 如果 `False`：仅当目标日期在 ApprovedUntil 属性中指定的日期或之前时，才接受该计划。

  如果 `AutoApprove` 为 `False` 且 `ApprovedUntil` 日期未设置或已过，则生成的任何计划覆盖都将被丢弃而不会使用。

- `ApprovedUntil`：
  - 如果 `AutoApprove` 为 `False`，并且您指定 `ApprovedUntil` 日期，则插件生成的计划覆盖将自动接受为目标日期的计划。

例如，假设 `AutoscaleGroupPlugin` 的 UID 为 2。

- 要为该桌面组启用自动批准：

```
Set-BrokerAutoscaleGroupPlugin 2 -AutoApprove $true
```

- 要启用自动批准直到未来某个日期：

```
Set-BrokerAutoscaleGroupPlugin 2 -ApprovedUntil "2025-01-01"
```

用户注销通知（原“强制用户注销”）

> **重要提示：**

> 此功能仅在 Autoscale™ 用户界面中适用于多会话基于应用程序的交付组。

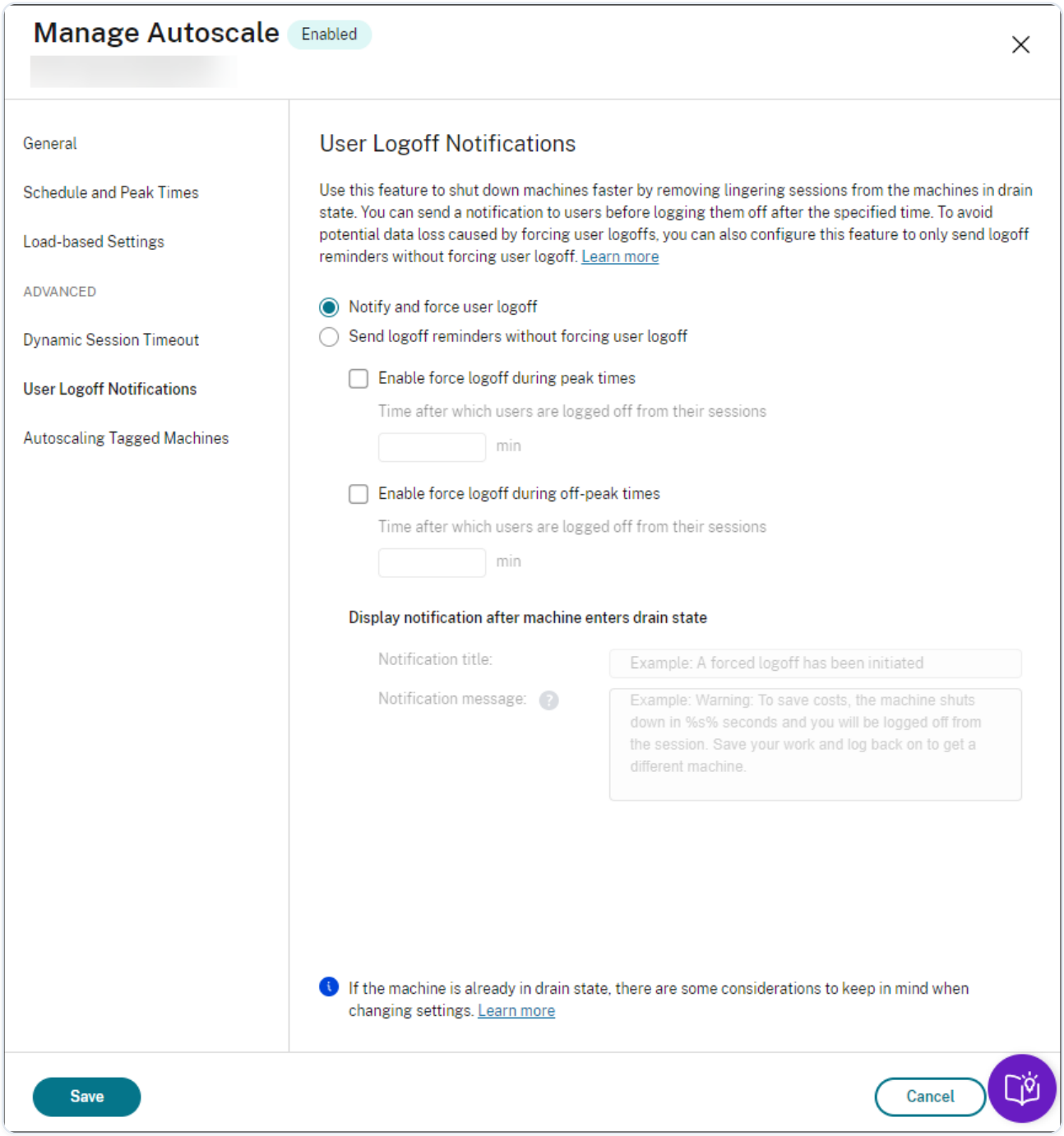
> 为了更好地实现成本节约，Autoscale 允许您强制注销滞留会话。它通过允许您向用户发送自定义通知并指定一个宽限期来实现，宽限期过后会话将被强制注销。这仅适用于处于 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/manage-deployment/autoscale.html#drain-state) 的计算机，而不适用于所有已开机的计算机。为避免因强制用户注销而导致潜在数据丢失，您可以改为将此功能配置为仅发送注销提醒，而不强制用户注销。

您有以下两个选项：

- **通知并强制用户注销**
- **发送注销提醒，但不强制用户注销**

通知并强制用户注销

如果选中，Autoscale 将在下方指定的时间过后将用户从其会话中注销。



在高峰时段启用强制注销。如果选中，Autoscale 将在指定时间过后，在高峰时段将这些用户从其会话中注销。

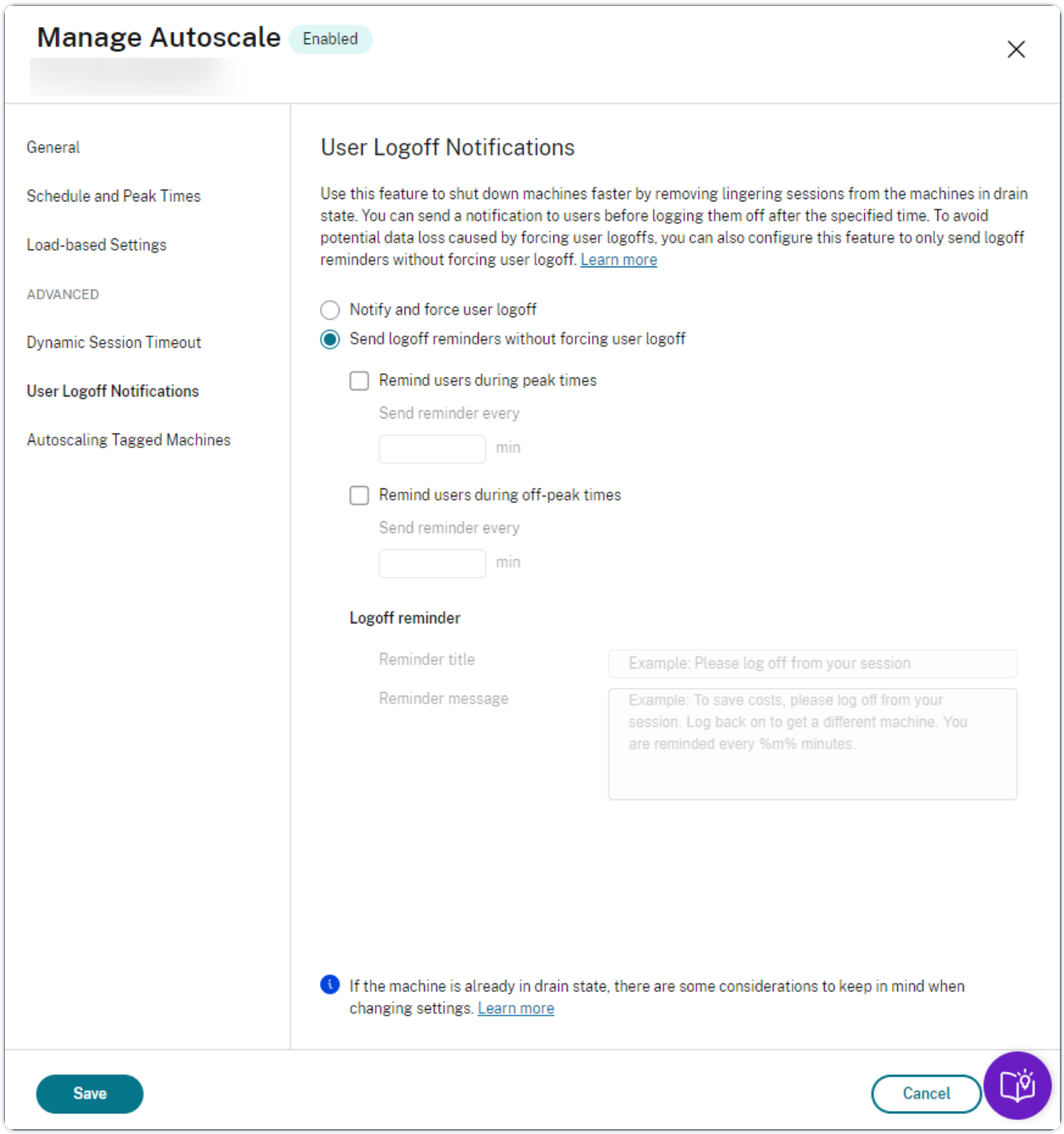
在非高峰时段启用强制注销。如果选中，Autoscale 将在指定时间过后，在非高峰时段将这些用户从其会话中注销。

计算机进入耗尽状态后显示通知。允许您在用户的计算机进入耗尽状态后向其发送通知。

- **通知标题**。允许您指定要发送给用户的通知标题。示例：`A forced logoff has been initiated.`.
- **通知消息**。允许您指定要发送给用户的通知内容。您可以使用 %s% 或 %m% 作为变量来指示消息中的指定时间。要以秒表示时间，请使用 %s%。要以分钟表示时间，请使用 %m%。示例：`Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`.

发送注销提醒而不强制用户注销

如果选中，用户将在其计算机进入耗尽状态后收到注销提醒。此提醒可配置为按以下指定的时间间隔发送。



在高峰时段提醒用户。如果选中，用户将在高峰时段每 X 分钟收到一次注销其会话的提醒（X 表示指定时间）。

在非高峰时段提醒用户。如果选中，用户将在非高峰时段每 X 分钟收到一次注销其会话的提醒（X 表示指定时间）。

注销提醒。允许您配置在用户计算机进入耗尽状态后发送给用户的提醒。

- **提醒标题**。允许您指定要发送给用户的提醒标题。示例：`Please log off from your session`。
- **提醒消息**。允许您指定要发送给用户的消息。示例：`Please log off from your session and log back on to save costs`。

注意事项

如果计算机已处于耗尽状态，更改设置时请考虑以下事项：

- 如果您将设置从**发送注销提醒而不强制用户注销**更改为**通知并强制用户注销**，新设置将立即生效。
- 如果您将设置从**通知并强制用户注销**更改为**发送注销提醒而不强制用户注销**，新设置要等到计算机下次进入耗尽状态时才会生效。用户仍将被强制注销。

分析 Autoscale™ 设置的有效性

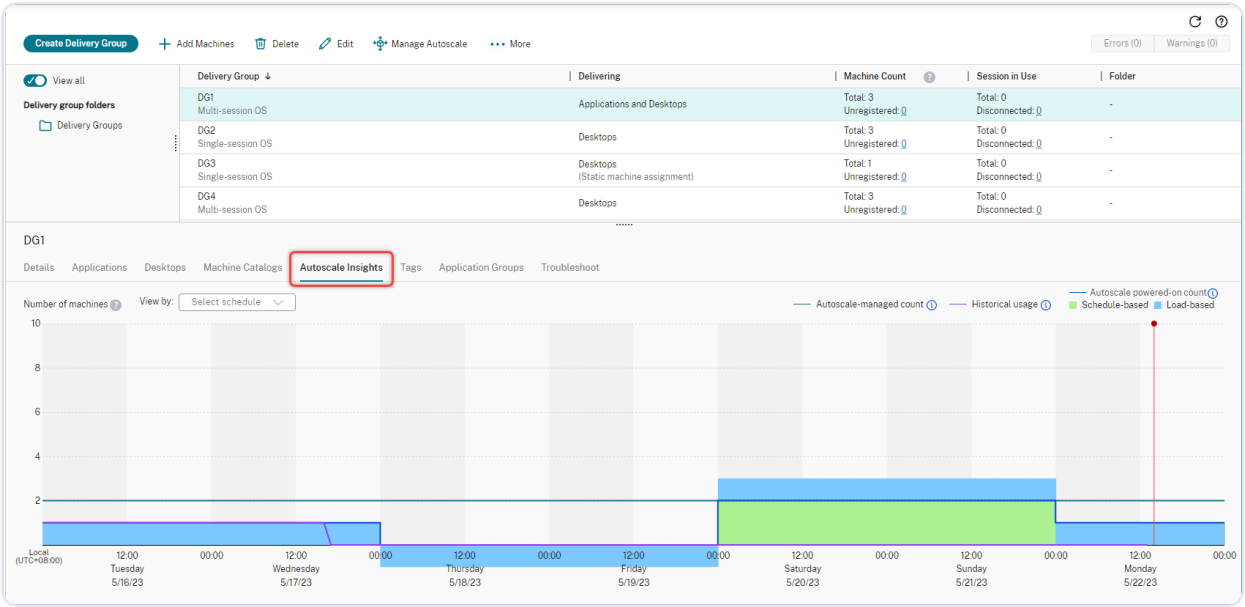
本文介绍如何根据前一周的计算机使用情况分析 Autoscale 设置的有效性。通过分析，您可以获得以下关于 Autoscale 设置有效性的见解：

- 识别因过度预配而造成的财务浪费。
- 确定用户体验是否因预配不足而受到负面影响。
- 确保预配的容量与计算机使用情况正确对齐。

要实现此目标，请按照以下步骤操作：

1. 选择一个已启用 Autoscale 的交付组。
2. 在底部窗格中，单击“**Autoscale Insights**”选项卡。

   将显示以下图表，其中显示了前一周的计算机使用数据与根据 Autoscale 设置要开机的计算机数量之间的比较。



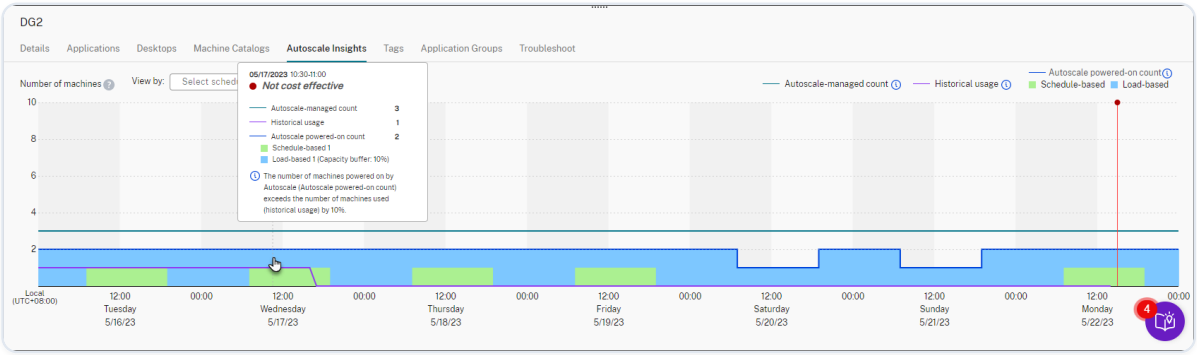
* 红色垂直线表示当前时间。

下表提供了此图表中显示的指标的说明。

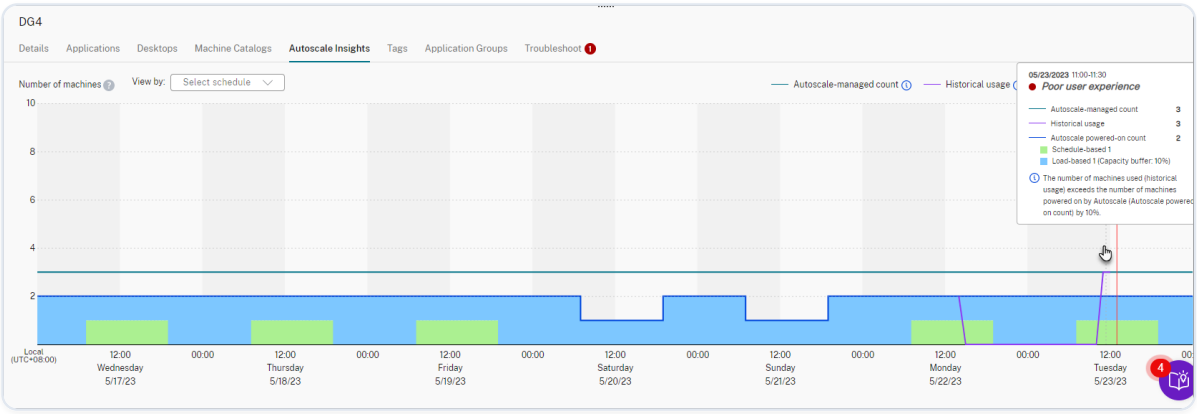
指标	说明
Autoscale 管理的计数	Autoscale 管理的计算机总数。Autoscale 管理的计数 = 交付组中的计算机总数 – 维护模式下的计算机数量 – 未标记为 Autoscale 的计算机数量（如果启用了标记 Autoscale 功能）。
Autoscale 已开机计数	Autoscale 已开机的计算机总数。Autoscale 已开机计数 = 基于计划的计算机数量 + 基于负载的计算机数量。
历史使用情况	已交付给用户的计算机数量。
基于计划	根据 Autoscale 基于计划的设置开机的计算机数量（**注意：** 基于计划的设置不适用于静态单会话操作系统类型的交付组）。
基于负载	根据 Autoscale 基于负载的设置开机的计算机数量。

3. 要检查 Autoscale 设置在特定时间段的有效性，请将鼠标悬停在图表上的该时间段上。此时将出现一个信息框，显示比较结果和详细的计算机数量：

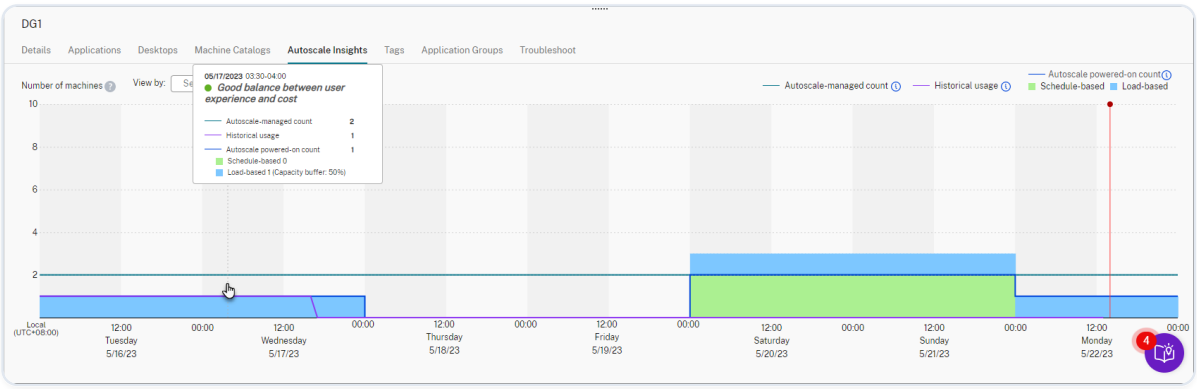
   - **不具成本效益**。历史使用率低于 Autoscale 设置（Autoscale 已开机计数）的 90%。因此，可能存在容量浪费。



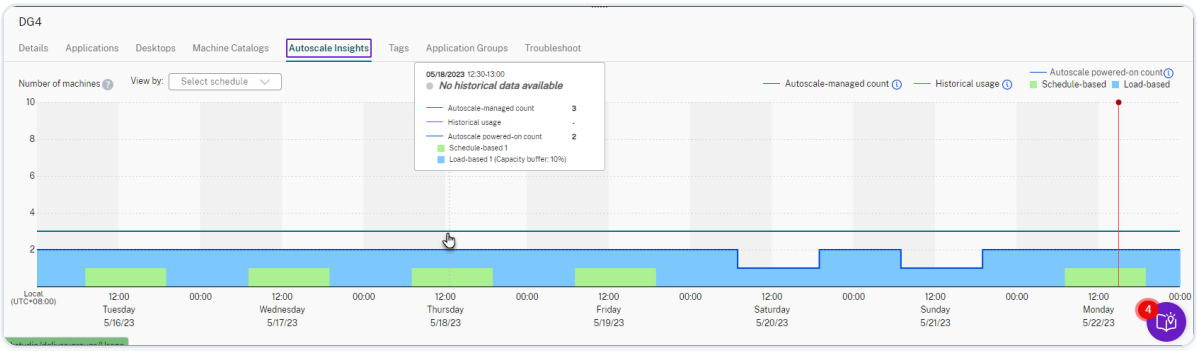
   - **用户体验不佳**。历史使用率超过 Autoscale 设置（Autoscale 已开机计数）的 110%。因此，用户可能会遇到计算机开机等待时间过长的问题。



- **用户体验和成本之间的良好平衡**。历史使用情况与 Autoscale 设置（Autoscale 开机计数）之间的差异小于 10%。Autoscale 设置与历史使用情况保持一致。



- **无可用历史数据**。无可用历史数据。可能的原因包括 Autoscale 在交付组中启用时间不足一周。



4. 要根据 Autoscale 计划突出显示日期范围，请从“**查看方式**”字段中选择该计划。
5. 根据您的分析，调整 Autoscale 设置。有关详细信息，请参阅基于计划和基于负载的设置。

Broker PowerShell SDK 命令

您可以使用 Broker PowerShell SDK 为交付组配置 Autoscale。要使用 PowerShell 命令配置 Autoscale，您必须使用 PowerShell SDK 7.21.0.12 或更高版本。有关 PowerShell SDK 的更多信息，请参阅 SDK 和 API。

Set-BrokerDesktopGroup

禁用或启用现有 BrokerDesktopGroup 或更改其设置。有关此 cmdlet 的更多信息，请参阅 `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`。

示例

有关如何使用 PowerShell cmdlet 的详细信息，请参阅以下示例。

启用 Autoscale™

- 假设您要为名为“MyDesktop”的交付组启用 Autoscale。使用 `Set-BrokerDesktopGroup` PowerShell 命令。例如：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -AutoscalingEnabled $true`

分别为高峰时段和非高峰时段配置容量缓冲区

- 假设您要为名为“MyDesktop”的交付组将高峰时段的容量缓冲区设置为 20%，非高峰时段设置为 10%。使用 `Set-BrokerDesktopGroup` PowerShell 命令。例如：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

配置**断开连接超时**设置

- 假设您要为名为“MyDesktop”的交付组将高峰时段的**断开连接超时**值设置为 60 分钟，非高峰时段设置为 30 分钟。使用 `Set-BrokerDesktopGroup` PowerShell 命令。例如：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

配置**注销超时**设置

- 假设您要为名为“MyDesktop”的交付组将高峰时段的**注销超时**值设置为 60 分钟，非高峰时段设置为 30 分钟。使用 `Set-BrokerDesktopGroup` PowerShell 命令。例如：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

配置**关机延迟**设置

- 假设您要为名为“MyDesktop”的交付组将关机延迟设置为 15 分钟。使用 `Set-BrokerDesktopGroup` PowerShell 命令。例如：

- `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PowerOffDelay 15`

配置一个时间段，在此期间关机延迟不生效

- 假设您希望名为“MyDesktop”的交付组在 30 分钟后才生效关机延迟。使用 `Set-BrokerDesktopGroup` PowerShell 命令。例如：
  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -SettlementPeriodBeforeAutoShutdown 30`。

配置**计算机实例成本**设置

- 假设您希望将名为“MyDesktop”的交付组的每小时计算机实例成本设置为 0.2 美元。使用 `Set-BrokerDesktopGroup` PowerShell 命令。例如：
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -MachineCost 0.2`

从自动缩放池中排除维护模式虚拟机

- 考虑一个包含 10 台计算机的交付组，其中 2 台计算机处于维护模式。自动缩放缓冲区容量设置为 50%。假设您想将维护模式下的虚拟机从自动缩放池中排除，则将 `PoolSizeExcludesMaintenanceMode` 设置为 `True`。自动缩放将启动 4 台计算机，因为维护模式下的 2 台计算机不包含在计算机池中。使用 `Set-BrokerDesktopGroup` PowerShell 命令。例如：
  - `PS C:\> Set-BrokerDesktopGroup -PoolSizeExcludesMaintenanceMode $true`

  单会话交付组的 `PoolSizeExcludesMaintenanceMode` 默认值为 `False`。

  多会话交付组的 `PoolSizeExcludesMaintenanceMode` 默认值为 `True`。

New-BrokerPowerTimeScheme

为交付组创建 BrokerPowerTimeScheme。有关详细信息，请参阅 `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>`。

示例

假设您想为 UID 值为 3 的交付组创建电源时间方案。新方案涵盖周末、周一和周二。上午 8:00 到下午 6:30 的时间段定义为方案中包含的日期的高峰时段。对于高峰时段，池大小（保持开机的计算机数量）为 20。对于非高峰时段，为 5。您可以使用 `Set-BrokerDesktopGroup` PowerShell 命令。例如：

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { 5 } else { 20 } } )`

- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

动态会话超时参数

以下 Broker PowerShell SDK cmdlet 已通过支持多个新参数进行了扩展，以实现动态会话超时：

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

这些参数包括：

- **DisconnectPeakIdleSessionAfterSeconds** – 表示在高峰时段空闲会话断开连接后的秒数。此属性的默认值为 0，表示在高峰时段禁用其关联行为。大于 0 的值仅在高峰时段为交付组启用其行为。
- **DisconnectOffPeakIdleSessionAfterSeconds** - 表示在非高峰时段空闲会话断开连接后的秒数。此属性的默认值为 0，表示在非高峰时段禁用其关联行为。大于 0 的值仅在非高峰时段为交付组启用其关联行为。
- **LogoffPeakDisconnectedSessionAfterSeconds** - 表示在高峰时段断开连接的会话终止后的秒数。此属性的默认值为 0，表示在高峰时段禁用其关联行为。大于 0 的值仅在高峰时段为交付组启用其关联行为。
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - 表示在非高峰时段断开连接的会话终止后的秒数。此属性的默认值为 0，表示在非高峰时段禁用其关联行为。大于 0 的值仅在非高峰时段为交付组启用其关联行为。

示例

假设您想为名为“MyDesktop”的交付组在高峰时段将空闲会话超时设置为 3,600 秒。使用 `Set-BrokerDesktopGroup` PowerShell 命令。例如：

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -DisconnectOffPeakIdleSessionAfterSeconds 3600`

这样做会断开名为“MyDesktop”的桌面组中在非高峰时段空闲超过 1 小时的会话。

Citrix 洞察服务

Citrix Insight Services (CIS) 是一个 Citrix 平台，用于仪器、遥测和业务洞察生成。其仪器和遥测功能使技术用户（客户、合作伙伴和工程师）能够自我诊断和修复问题并优化其环境。有关 CIS 及其工作原理的详细信息和最新信息，请参阅 `<https://cis.citrix.com>`（需要 Citrix 帐户凭据）。

上传到 Citrix 的所有信息均用于故障排除和诊断目的，以及提高产品质量、可靠性和性能，但须遵守：

- Citrix Insight Services 策略，网址为 `<https://cis.citrix.com/legal>`
- Citrix 隐私策略，网址为 `<https://www.cloud.com/privacy-policy>`

此 Citrix Virtual Apps and Desktops™ 版本支持以下技术。

- Citrix Virtual Apps and Desktops™ 安装和升级分析
- Citrix 客户体验改善计划 (CEIP)
- Citrix 回传
- Citrix 探测

安装和升级分析

当您使用完整产品安装程序部署或升级 Citrix Virtual Apps and Desktops 组件时，有关安装过程的匿名信息会收集并存储在您安装/升级组件的计算机上。此数据用于帮助 Citrix 改善客户的安装体验。

信息本地存储在 `%ProgramData%\Citrix\CTQs` 下。

在完整产品安装程序的图形界面和命令行界面中，此数据的自动上传默认处于启用状态。

- 您可以在注册表设置中更改默认值。如果在安装/升级之前更改注册表设置，则在使用完整产品安装程序时将使用该值。
- 如果使用命令行界面安装/升级，可以通过在命令中指定选项来覆盖默认设置。

控制自动上传：

- 控制安装/升级分析数据自动上传的注册表设置（默认值 = 1）：
  - 位置：`HKLM:\Software\Citrix\MetaInstall`
  - 名称：SendExperienceMetrics
  - 值：0 = 禁用，1 = 启用

- 使用 PowerShell，以下 cmdlet 可禁用安装/升级分析数据的自动上传：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
SendExperienceMetrics -PropertyType DWORD -Value 0
```

- 要使用 XenDesktopServerSetup.exe 或 XenDesktopVDASetup.exe 命令禁用自动上传，请包含 `/disableexperiencemetrics` 选项。

  要使用 XenDesktopServerSetup.exe 或 XenDesktopVDASetup.exe 命令启用自动上传，请包含 `/sendexperiencemetrics` 选项。

Citrix 客户体验改善计划

当您参与 Citrix 客户体验改善计划 (CEIP) 时，匿名统计数据和使用信息会发送给 Citrix，以帮助 Citrix 改进 Citrix 产品的质量和性能。有关详细信息，请参阅 https://more.citrix.com/XD-CEIP。

在站点创建或升级期间注册

创建站点（安装第一个 Delivery Controller™ 后）时，您将自动注册 CEIP。首次数据上传大约在创建站点七天后进行。

创建站点后，您可以随时停止参与。在 Web Studio 左窗格中选择“**设置**”节点，然后关闭“**Citrix 客户体验改善计划**”设置。

升级 Citrix Virtual Apps and Desktops 部署时：

- 如果您从不支持 CEIP 的版本进行升级，系统会询问您是否要参与。
- 如果您从支持 CEIP 的版本进行升级，并且已启用参与，则 CEIP 将在升级后的站点中启用。
- 如果您从支持 CEIP 的版本升级，并且已禁用参与，则升级后的站点中会禁用 CEIP。
- 如果您从支持 CEIP 的版本升级，并且参与状态未知，系统会询问您是否要参与。

收集的信息是匿名的，因此上传到 Citrix Insight Services 后无法查看。

安装 VDA 时的注册

默认情况下，当您安装 Windows VDA 时，会自动注册 CEIP。您可以在注册表设置中更改此默认值。如果您在安装 VDA 之前更改注册表设置，则会使用该值。

控制 CEIP 自动注册的注册表设置（默认值 = 1）：

位置：`HKLM:\Software\Citrix\Telemetry\CEIP` 名称：Enabled 值：0 = 禁用，1 = 启用

默认情况下，`Enabled` 属性在注册表中是隐藏的。如果未指定，则启用自动上传功能。

使用 PowerShell，以下 cmdlet 可禁用 CEIP 注册：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled
-PropertyType DWORD -Value 0
```

收集的运行时数据点会定期作为文件写入输出文件夹（默认 %programdata%/Citrix/VdaCeip）。

首次数据上传大约在您安装 VDA 七天后进行。

安装其他产品和组件时的注册

您在安装相关 Citrix 产品、组件和技术（例如 Citrix Provisioning™、AppDNA、Citrix License Server、适用于 Windows 的 Citrix Workspace™ 应用程序、Universal Print Server 和 Session Recording）时，也可以参与 CEIP。有关安装和参与默认值的详细信息，请参阅其文档。

Citrix 回拨

当您在 Citrix Virtual Apps and Desktops 中安装某些组件和功能时，系统会提供参与 Citrix Call Home 的机会。Call Home 会收集诊断数据，然后定期将包含这些数据的遥测包直接上传到 Citrix Insight Services（通过默认端口 443 上的 HTTPS），以进行分析和故障排除。

在 Citrix Virtual Apps and Desktops 中，Call Home 作为后台服务运行，名称为 Citrix Telemetry Service。

Call Home 调度功能在 Citrix Scout 中也可用。有关详细信息，请参阅 Citrix Scout。

收集了什么

Citrix Diagnostic Facility (CDF) 跟踪记录了对故障排除有用的信息。Call Home 收集了 CDF 跟踪的子集，这些跟踪在故障排除常见故障（例如 VDA 注册和应用程序/桌面启动）时非常有用。此技术称为始终开启跟踪 (AOT)。AOT 日志保存在磁盘上的 C:\ProgramData\Citrix\TelemetryService\CitrixAOT 中。

> **注意：**
>
> `ProgramData` 文件夹是隐藏的。要显示它，请单击 **View** > **Show** > **Hidden items**。

> Call Home 不收集任何其他 Windows 事件跟踪 (ETW) 信息，也无法配置为这样做。

Call Home 还收集其他信息，例如：

- Citrix Virtual Apps and Desktops 在 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` 下创建的注册表。
- Citrix 命名空间下的 Windows Management Instrumentation (WMI) 信息。
- 正在运行的进程列表。
- 存储在 `%PROGRAMDATA%\Citrix\CDF` 中的 Citrix 进程的崩溃转储。
- 安装和升级信息。这可以包括完整的产品元安装程序日志、失败的 MSI 日志、MSI 日志分析器的输出、StoreFront™ 日志、许可兼容性检查日志以及初步站点升级测试的结果。

跟踪信息在收集时会被压缩。Citrix Telemetry Service 最多保留 10 MB 的压缩近期跟踪信息，最长保留时间为八天。

- 压缩数据使 Call Home 能够在 VDA 上保持较小的占用空间。
- 跟踪信息保存在内存中，以避免在预配的计算机上产生 IOP。
- 跟踪缓冲区使用循环机制在内存中保留跟踪。

Call Home 收集 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/manage-deployment/call-home-datapoints.html) 中列出的关键数据点。

配置和管理摘要

您可以在使用完整产品安装向导时或之后使用 PowerShell cmdlet 注册 Call Home。注册后，默认情况下，诊断信息会在当地时间每周日凌晨 3:00 左右收集并上传到 Citrix。上传时间会在指定时间的基础上随机化，间隔为两小时。这意味着使用默认计划的上传会在凌晨 3:00 到 5:00 之间进行。

如果您不想按计划上传诊断信息（或者您想更改计划），您可以使用 PowerShell cmdlet 手动收集和上传诊断信息，或将其存储在本地。

当您注册计划的 Call Home 上传以及手动将诊断信息上传到 Citrix 时，您需要提供 Citrix 帐户或 Citrix Cloud™ 凭据。Citrix 会将这些凭据交换为上传令牌，该令牌用于识别客户并上传数据。凭据不会保存。

上传发生时，通知将通过电子邮件发送到与 Citrix 帐户关联的地址。

如果您在安装组件时启用了 Call Home，则可以(#disable-call-home)。

先决条件

- 计算机必须运行 PowerShell 3.0 或更高版本。
- Citrix Telemetry Service 必须在计算机上运行。

- 系统变量 `PSModulePath` 必须设置为 Telemetry 的安装路径，例如 `C:\Program Files\Citrix\Telemetry Service\`。

在组件安装期间启用 Call Home

在 VDA 安装或升级期间： 当您使用完整产品安装程序中的图形界面安装或升级 Virtual Delivery Agent 时，系统会询问您是否要参与 Call Home。有两个选项：

- 参与 Call Home。
- 不参与 Call Home。

如果您正在升级 VDA 并且之前已注册 Call Home，则不会显示该向导页面。

在 Controller 安装或升级期间： 当您使用图形界面安装或升级 Delivery Controller 时，系统会询问您是否要参与 Call Home。有三个选项：

如果服务器应用了具有策略设置“作为服务登录”的 Active Directory GPO，则在安装 Controller 时，无法在安装向导的 Call Home 页面上配置信息。有关详细信息，请参阅 CTX218094。

如果您正在升级 Controller 并且之前已注册 Call Home，则不会询问您是否参与。

PowerShell 命令

PowerShell 帮助提供了全面的语法，包括这些常见用例中未使用的 cmdlet 和参数的说明。

要使用代理服务器进行上传，请参阅 配置代理服务器。

- **启用计划上传：** 诊断集合会自动上传到 Citrix。如果您不为自定义计划输入其他 cmdlet，则使用默认计划。

  ```
  $cred = Get-Credential

  Enable-CitrixCallHome -Credential $cred
  ```

  要确认已启用计划上传，请输入 `Get-CitrixCallHome`。如果已启用，则返回 `IsEnabled=True` 和 `IsMasterImage=False`。

- **为从主映像创建的计算机启用计划上传：** 在主映像中启用计划上传可省去配置计算机目录中创建的每台计算机的麻烦。

  `Enable-CitrixCallHome -Credential $cred -MasterImage`

  要确认已启用计划上传，请输入 **Get-CitrixCallHome**。如果已启用，则返回 `IsEnabled=True` 和 `IsMasterImage=True`。

- **创建自定义计划：** 为诊断集合和上传创建每日或每周计划。

```
$timespan = New-TimeSpan –Hours hours -Minutes minutes

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
-UploadFrequency {Daily|Weekly}
```

示例：

以下 cmdlet 创建一个计划，用于在每天晚上 10:20 捆绑和上传数据。Hours 参数使用 24 小时制。当 `UploadFrequency` 参数值为 Daily 时，如果指定了 `DayOfWeek` 参数，则会忽略该参数。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

要确认计划，请输入 `Get-CitrixCallHomeSchedule`。在前面的示例中，它返回 `StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`。

以下 cmdlet 会创建一个计划，用于在每周三晚上 10:20 捆绑和上传数据。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed
-UploadFrequency Weekly
```

要确认计划，请输入 `Get-CitrixCallHomeSchedule`。在前面的示例中，它返回 `StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`。

禁用 Call Home

您可以使用 PowerShell cmdlet 或通过 Citrix Scout 禁用 Call Home。

即使禁用 Call Home 计划上传，AOT 日志也会收集并保存到磁盘。（禁用计划上传时，AOT 日志不会自动上传到 Citrix。）您可以禁用 AOT 日志的收集和本地存储。

使用 PowerShell 禁用 Call Home

运行以下 cmdlet 后，诊断数据将不会自动上传到 Citrix。（您仍然可以使用 Citrix Scout 或遥测 PowerShell cmdlet 上传诊断数据。）

`Disable-CitrixCallHome`

要确认 Call Home 已禁用，请输入 `Get-CitrixCallHome`。如果已禁用，则返回 `IsEnabled=False` 和 `IsMasterImage=False`。

使用 Citrix Scout 禁用收集计划

要使用 Citrix Scout 禁用诊断收集计划，请按照 计划收集 中的指导进行操作。在步骤 3 中，单击 **Off** 以取消所选计算机的计划。

禁用 AOT 日志收集

运行以下 cmdlet（将 `Enabled` 字段设置为 `false`）后，将不会收集 AOT 日志。

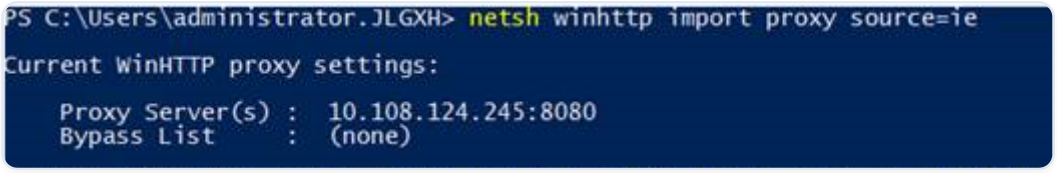
```
Enable-CitrixTrace -Listen'{"trace":{"enabled":false,"persistDirectory":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300}}'
```

`Listen` 参数包含 JSON 格式的参数。

为 Call Home 上传配置代理服务器

在启用 Call Home 的计算机上完成以下任务。以下过程中的示例图包含服务器地址和端口 10.158.139.37:3128。您的信息将有所不同。

1. 在浏览器中添加代理服务器信息。在 Internet Explorer 中，选择 **Internet 选项 \> 连接 \> 局域网设置**。选择“**为 LAN 使用代理服务器**”并输入代理服务器地址和端口号。
2. 在 PowerShell 中，运行 `netsh winhttp import proxy source=ie`。



3. 使用文本编辑器编辑 TelemetryService.exe 配置文件，该文件位于 `C:\Program Files\Citrix\Telemetry Service`。添加红色框中显示的信息。



4. 重新启动 Telemetry Service。

在 PowerShell 中运行 Call Home cmdlet。

手动收集和上传诊断信息

您可以使用 CIS 网站将诊断信息包上传到 CIS。您还可以使用 PowerShell cmdlet 收集诊断信息并将其上传到 CIS。

要使用 CIS 网站上传捆绑包，请执行以下操作：

1. 使用您的 Citrix 帐户凭据登录 Citrix Insight Services。
2. 选择 **我的工作区**。
3. 选择 **运行状况检查**，然后导航到数据所在的位置。

CIS 支持多个用于管理数据上传的 PowerShell cmdlet。本文档涵盖了两种常见情况下的 cmdlet：

- 使用 `Start-CitrixCallHomeUpload` cmdlet 手动收集诊断信息包并将其上传到 CIS。（该捆绑包不会在本地保存。）
- 使用 `Start-CitrixCallHomeUpload` cmdlet 手动收集数据并在本地存储诊断信息包。这允许您预览数据。稍后，使用 `Send-CitrixCallHomeBundle` cmdlet 手动将该包的副本上传到 CIS。（您最初保存的数据仍保留在本地。）

PowerShell 帮助提供了全面的语法，包括这些常见用例中未使用的 cmdlet 和参数的说明。

当您输入 cmdlet 将数据上传到 CIS 时，系统会提示您确认上传。如果 cmdlet 在上传完成之前超时，请在系统事件日志中检查上传状态。如果服务已在执行上传，则上传请求可能会被拒绝。

收集数据并将捆绑包上传到 CIS：

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string]
[-Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploadHeader string] [-AppendHeaders string] [-Collect string]
[<CommonParameters>]
```

收集数据并将其保存在本地：

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
strings] [<CommonParameters>]
```

以下参数有效：

- **Credential：** 将上传定向到 CIS。
- **InputPath：** 要包含在捆绑包中的 zip 文件位置。这可能是 Citrix 支持请求的附加文件。请务必包含 .zip 扩展名。
- **OutputPath：** 诊断信息的保存位置。在本地保存 Call Home 数据时，此参数是必需的。
- **Description and Incident Time：** 有关上传的自由格式信息。
- **SRNumber：** Citrix 技术支持事件编号。
- **Name：** 标识捆绑包的名称。
- **UploadHeader：** JSON 格式的字符串，指定上传到 CIS 的上传标头。
- **AppendHeaders：** JSON 格式的字符串，指定上传到 CIS 的附加标头。
- **Collect：** JSON 格式的字符串，指定要收集或省略的数据，格式为 {'collector': {'enabled':Boolean}}，其中 Boolean 为 true 或 false。 有效的收集器值为：
  - 'WMI 信息'
  - '进程'
  - '注册表
  - '崩溃报告'
  - '跟踪'
  - '文件'
  - 'MSI 文件'
  - '本地数据'

- '站点数据'
- 'SFB 数据'

默认情况下，除了 'sfb' 之外的所有收集器都已启用。

'sfb' 收集器旨在按需使用，以诊断 Skype for Business 问题。除了 'enabled' 参数之外，'sfb' 收集器还支持 'account' 和 'accounts' 参数来指定目标用户。请使用以下形式之一：

- "-收集 " `{'sfb':{'account':'domain\user1'}}` "
- "-收集 " `{'sfb':{'accounts':['domain\user1', 'domain\user2']}}` "

- **常见参数：** 请参阅 PowerShell 帮助。

上传之前本地保存的数据：

`Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<CommonParameters>]`

`Path` 参数指定了之前保存的捆绑包的位置。

示例：

以下 cmdlet 请求将 Call Home 数据（不包括来自 WMI 收集器的数据）上传到 CIS。此数据与 Citrix Provisioning VDA 的注册失败有关，该失败在下午 2:30 记录，对应 Citrix 支持案例 123456。除了 Call Home 数据之外，文件 “`c:\Diagnostics\ExtraData.zip`” 也被包含在上传的捆绑包中。

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:
\Diagnostics\ExtraData.zip" -Description "Registration failures with
Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name
"RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}"
-UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

以下 cmdlet 保存与 Citrix 支持案例 223344 相关联的 Call Home 数据，该案例记录于上午 8:15。数据保存在网络共享上的 mydata.zip 文件中。除了 Call Home 数据之外，文件 “`c:\Diagnostics\ExtraData.zip`” 将被包含在保存的捆绑包中。

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \
\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"
-Description "Diagnostics for incident number 223344" -IncidentTime "8:15"
-SRNumber 223344
```

以下 cmdlet 上传您之前保存的数据捆绑包。

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

思杰 Scout

简介

Citrix Scout 收集诊断信息并运行运行状况检查。您可以使用结果来维护您的 Citrix Virtual Apps and Desktops™ 部署。Citrix 通过 Citrix Insight Services 提供诊断信息收集的全面自动化分析。您还可以自行或在 Citrix 支持的指导下使用 Scout 解决问题。

您可以将收集文件上传到 Citrix，以获取 Citrix 支持的分析和指导。或者，您可以将收集文件保存到本地以供自己查看，然后稍后将收集文件上传到 Citrix 进行分析。

Scout 提供以下过程：

- **收集：** 在您在站点中选择的计算机上运行一次性诊断信息收集。然后，您可以将文件上传到 Citrix 或将其保存到本地。
- **跟踪和重现：** 在您选择的计算机上启动手动跟踪。然后，您在这些计算机上重现问题。重现问题后，跟踪将停止。然后，Scout 会收集其他诊断信息并将其上传到 Citrix，或将文件保存到本地。
- **计划：** 计划诊断信息收集在您选择的计算机上每天或每周的指定时间进行。文件会自动上传到 Citrix。
- **运行状况检查：** 运行检查以评估站点及其组件的运行状况和可用性。您可以对 Delivery Controllers、Virtual Delivery Agents (VDAs)、StoreFront™ 服务器和 Citrix License Servers 运行运行状况检查。如果在检查期间发现问题，Scout 会提供详细报告。每次 Scout 启动时，它都会检查更新的运行状况检查脚本。如果有新版本可用，Scout 会自动下载它们，以便在下次运行运行状况检查时使用。

> **注意：**
>
> **跟踪和重现**、**计划**和**运行状况检查**过程目前不适用于 Linux VDA。

> 本文介绍的图形界面是使用 Scout 的主要方式。此外，您还可以使用 PowerShell 配置一次性或计划的诊断信息收集和上传。请参阅 Call Home。

在何处运行 Scout：

- 在本地部署中，从 Delivery Controller™ 运行 Scout 以捕获诊断信息或对一个或多个 Virtual Delivery Agent (VDA)、Delivery Controller、StoreFront 服务器、Federated Authentication Service (FAS) 服务器和许可证服务器运行检查。您也可以从 VDA 运行 Scout 以收集本地诊断信息。

  > **注意：**
  >
  > 目前，Scout 不支持在 FAS 服务器上诊断 FAS 配置问题的*健康检查*。

- 在使用了 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops™ 服务）的 Citrix Cloud 环境中，从 VDA 运行 Scout 以收集本地诊断信息。

Scout 应用程序的日志存储在 `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log` 中。此文件可用于故障排除。

收集了什么

Scout 收集的诊断信息包括 Citrix Diagnostic Facility (CDF) 跟踪日志文件。还包括 CDF 跟踪的一个子集，称为 Always-on Tracing (AOT)。AOT 信息在排查 VDA 注册和应用程序/桌面启动等常见问题时会很有帮助。不收集其他 Windows 事件跟踪 (ETW) 信息。

收集内容包括：

- Citrix Virtual Apps and Desktops 在 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` 下创建的注册表项。
- **Citrix 命名空间**下的 Windows Management Instrumentation (WMI) 信息。
- 正在运行的进程。
- 存储在 `%PROGRAMDATA%\Citrix\CDF` 中的 Citrix 进程的崩溃转储。
- CSV 格式的 Citrix 策略信息。
- 安装和升级信息。收集内容可包括完整的产品元安装程序日志、失败的 MSI 日志、MSI 日志分析器的输出、StoreFront 日志、许可兼容性检查日志以及初步站点升级测试的结果。

关于跟踪信息：

- 跟踪信息在收集时会进行压缩，以减小在计算机上的占用空间。
- 在每台计算机上，Citrix Telemetry Service 最多保留八天的压缩近期跟踪信息。
- 从 Citrix Virtual Apps and Desktops 7 1808 开始，AOT 跟踪默认保存到本地磁盘。（在早期版本中，跟踪保存在内存中。）默认路径 = `C:\ProgramData\Citrix\TelemetryService\CitrixAOT`。
- 从 Citrix Virtual Apps and Desktops 7 1811 开始，保存到网络共享的 AOT 跟踪会与其他诊断信息一起收集。
- 您可以使用 `Enable-CitrixTrace` cmdlet 或 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen` 注册表字符串修改最大大小（默认值 = 10 MB）和切片持续时间。
- 跟踪会追加到文件中，直到文件达到 `MaxSize` 的 10%。

有关 Scout 收集的数据点的列表，请参阅Call Home 关键数据点。

Scout 配置

可以将 Scout 配置为在 Linux VDA 上运行。有关 Linux VDA 和遥测的更多信息，请参阅与 Citrix 遥测服务集成

Linux VDA 可能会自动更改 `ctxtelemetry` 套接字端口或遥测服务端口。如果是这样，您必须手动配置端口。

1. 导航到 C:\Program Files\Citrix\Telemetry Service
2. 打开 ScoutUI.exe.config 文件。
3. 将 LinuxVDATelemetryServicePort 或 LinuxVDATelemetryWakeupPort 的值更改为在 Linux VDA 上配置的值：

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. 保存更改并关闭文件。
2. 再次打开 Scout 以确保它加载最新的配置。

关于运行状况检查

运行状况检查数据存储在 `C:\ProgramData\Citrix\TelemetryService\` 下的文件夹中。

站点运行状况检查

站点运行状况检查包含在环境测试服务中，该服务提供对 FlexCast Management Architecture (FMA) 服务的全面评估。除了检查服务可用性外，这些检查还会查找其他运行状况指标，例如数据库连接。

站点运行状况检查在 Delivery Controller 上运行。根据您的站点大小，这些检查可能需要长达一小时才能完成。

DELIVERY CONTROLLER 配置检查

作为站点运行状况检查的一部分，Delivery Controller 配置检查会根据 Citrix 对 Virtual Apps and Desktops 站点的建议，验证是否存在以下问题：

- 一个或多个 Delivery Controller 处于失败状态。
- 站点中只有一个 Delivery Controller。
- Delivery Controller 版本不同。

除了满足运行状况检查的权限和要求外，Delivery Controller 配置检查还需要：

- 至少有一个 Controller 已开机。
- 在控制器上运行的代理服务。
- Controller 与站点数据库之间的连接正常。

VDA 运行状况检查

VDA 运行状况检查可识别常见的 VDA 注册、会话启动和时区重定向问题的可能原因。

对于 VDA 上的注册，Scout 会检查：

- VDA 软件安装
- VDA 计算机域成员身份
- VDA 通信端口可用性
- VDA 服务状态
- Windows 防火墙配置
- 与 Controller 的通信
- 与 Controller 的时间同步
- VDA 注册状态

对于 VDA 上的会话启动，Scout 会检查：

- 会话启动通信端口可用性

- 会话启动服务状态
- 会话启动 Windows 防火墙配置
- VDA 远程桌面服务客户端访问许可证
- VDA 应用程序启动路径
- 会话启动注册表设置

对于 VDA 上的时区重定向，Scout 会检查：

- Windows 修补程序安装
- Citrix 修补程序安装
- Microsoft 组策略设置
- Citrix 组策略设置

对于 VDA 上的 Profile Management，Scout 会检查：

- 虚拟机管理程序检测
- 预配检测
- Citrix 虚拟应用和桌面
- 个人 vDisk 配置
- 用户存储
- Profile Management 服务状态检测
- Winlogon.exe 挂钩测试

要对 Profile Management 运行检查，必须在 VDA 上安装并启用 Profile Management。有关 Profile Management 配置检查的详细信息，请参阅知识中心文章 CTX132805。

StoreFront 运行状况检查

StoreFront 检查验证：

- Citrix Default Domain 服务正在运行
- Citrix Credential Wallet 服务正在运行
- StoreFront 服务器到 Active Directory 端口 88 的连接
- StoreFront 服务器到 Active Directory 端口 389 的连接
- 基本 URL 具有有效的 FQDN
- 可以检索到基本 URL 的正确 IP 地址

- IIS 应用程序池正在使用 .NET 4.0
- 证书是否绑定到主机 URL 的 SSL 端口
- 证书链是否完整
- 证书是否已过期
- 证书是否即将过期（30 天内）

许可证服务器检查

许可证服务器检查验证：

- Delivery Controller 到许可证服务器的连接
- 许可证服务器防火墙远程访问状态
- Citrix 许可服务状态
- 许可证服务器许可证缓存模式状态
- 许可证服务器端口连接
- Citrix 供应商守护程序 (CITRIX) 是否正在运行
- 系统时钟是否同步
- Citrix 许可服务是否在本地服务帐户下运行
- `CITRIX.opt` 文件的存在
- 客户成功服务资格日期
- Citrix 许可证服务器更新
- 许可证服务器证书是否在 Delivery Controller 的受信任根存储中

除了满足运行运行状况检查的 权限和要求 外，许可证服务器还必须加入域。否则，将无法发现许可证服务器。

运行运行状况检查

运行状况检查过程包括选择计算机、开始检查，然后查看结果报告。

1. 启动 Scout。从计算机的“**开始**”菜单中，选择“**Citrix > Citrix Scout**”。在打开的页面上，单击“**运行状况检查**”。
2. 选择计算机。单击“**查找计算机**”以发现计算机。“**选择计算机**”页面列出了在此站点中发现的所有 VDA、Delivery Controller 和许可证服务器。您可以按计算机名称筛选显示。选中要从中收集诊断信息的每台计算机旁边的复选框，然后单击“**继续**”。

要添加其他组件类型（例如 StoreFront 服务器和 VDA 计算机），请参阅手动添加计算机 和导入 VDA 计算机。您无法手动添加 Citrix Provisioning™ 服务器或许可证服务器。

Scout 会自动对每台选定的计算机启动验证测试，确保其符合验证测试 中列出的条件。如果验证失败，则会在“**状态**”列中发布一条消息，并且该计算机的复选框将被清除。您可以选择：

- 解决问题，然后再次选中该计算机的复选框。这将触发验证测试的重试。
- 跳过该计算机（保持其复选框未选中）。不会对该计算机运行健康检查。

验证测试完成后，单击 **继续**。

3. 对选定的计算机运行健康检查。摘要列出了运行测试的计算机（您选择并通过验证测试的计算机）。单击 **开始检查**。

   检查期间和检查之后：

   - **状态** 列指示计算机的当前检查状态。
   - 要停止所有正在进行的检查，请单击页面右下角的 **停止检查**。（您无法取消单个计算机的健康检查，只能取消所有选定的计算机。已完成检查的计算机信息将保留。）.
   - 当所有选定计算机的检查完成后，右下角的 **停止检查** 按钮将变为 **完成**。
   - 如果检查失败，您可以在 **操作** 列中单击 **重试**。
   - 如果检查完成且未发现任何问题，则 **操作** 列为空。
   - 如果检查发现问题，请单击 **查看详细信息** 以显示结果。
   - 所有选定计算机的检查完成后，请勿单击 **返回**。（如果单击，检查结果将丢失。）

4. 检查完成后，单击 **完成** 返回 Scout 启动页面。

健康检查结果

对于生成报告的 Citrix 检查，报告包含：

- 生成结果报告的时间和日期
- 已检查的计算机
- 检查在目标计算机上查找的条件

权限和要求

权限：

- 要收集诊断信息：
  - 对于要从中收集诊断信息的每台计算机，您必须是本地管理员和域用户。

    - 您必须具有在每台计算机的 LocalAppData 目录中写入的权限。

- 要运行运行状况检查：
    - 您必须是域用户组的成员。
    - 您必须是完全管理员，或者具有对站点具有只读和 **运行环境测试** 权限的自定义角色。
    - 将脚本执行策略设置为至少 `RemoteSigned` 以允许脚本运行。例如：`Set-ExecutionPolicy RemoteSigned`。**注意：** 其他脚本执行权限也可以。
- 启动 Scout 时使用 **以管理员身份运行**。

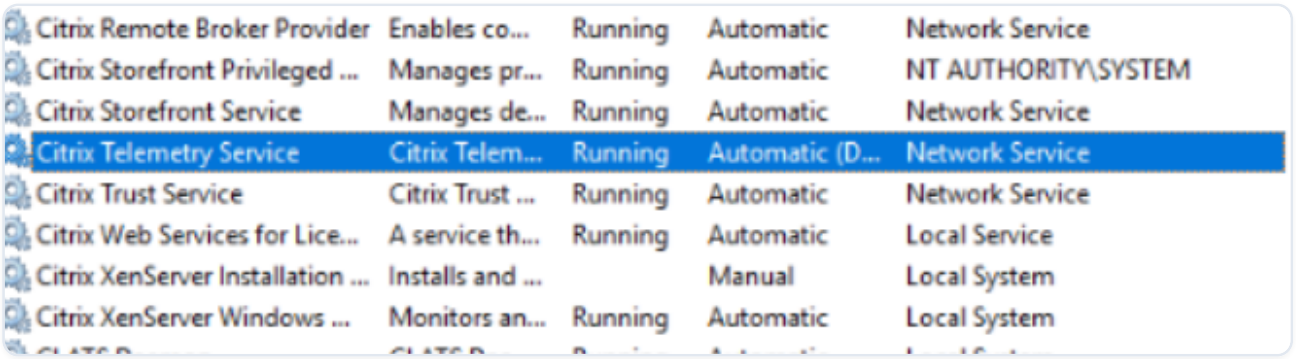
对于从中收集诊断信息或运行运行状况检查的每台计算机：

- Scout 必须能够与计算机通信。
- 必须启用文件和打印机共享。
- 必须启用 PSRemoting 和 WinRM。计算机还必须运行 PowerShell 3.0 或更高版本。
- Citrix Telemetry Service 必须在计算机上运行。
- 必须在计算机上启用 Windows Management Infrastructure (WMI) 访问。
- 要设置诊断信息收集计划，计算机必须运行兼容的 Scout 版本。

请勿在路径名中指定的用户名称中使用美元符号 ($)。这会阻止诊断信息的收集。

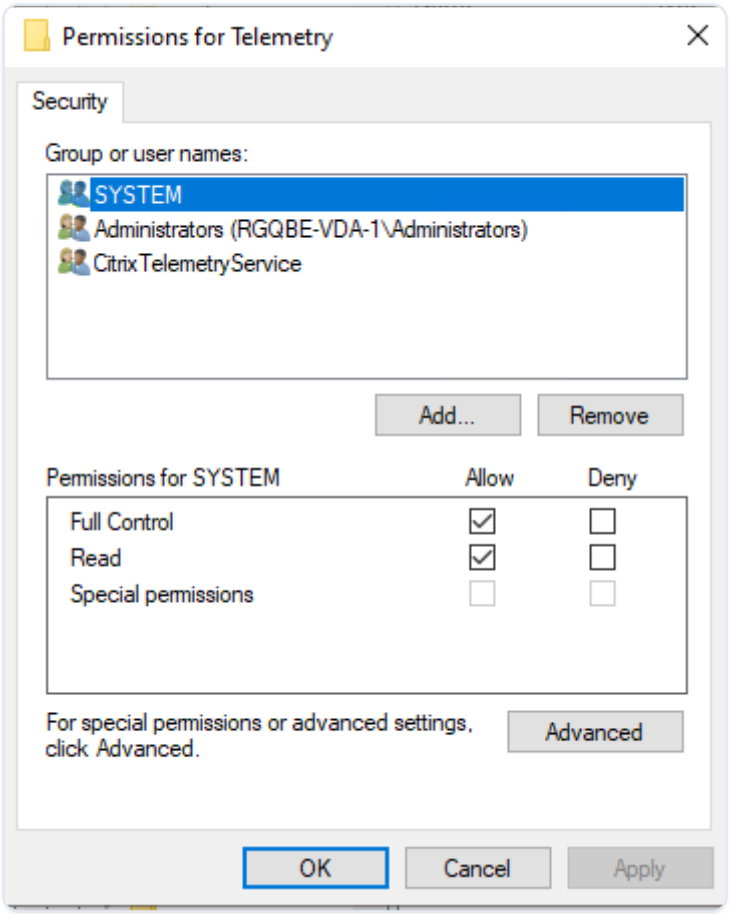
Scout 会对您选择的计算机运行验证测试，以确保满足这些要求。

适用于 Windows 的 Telemetry Service 在网络服务上运行。

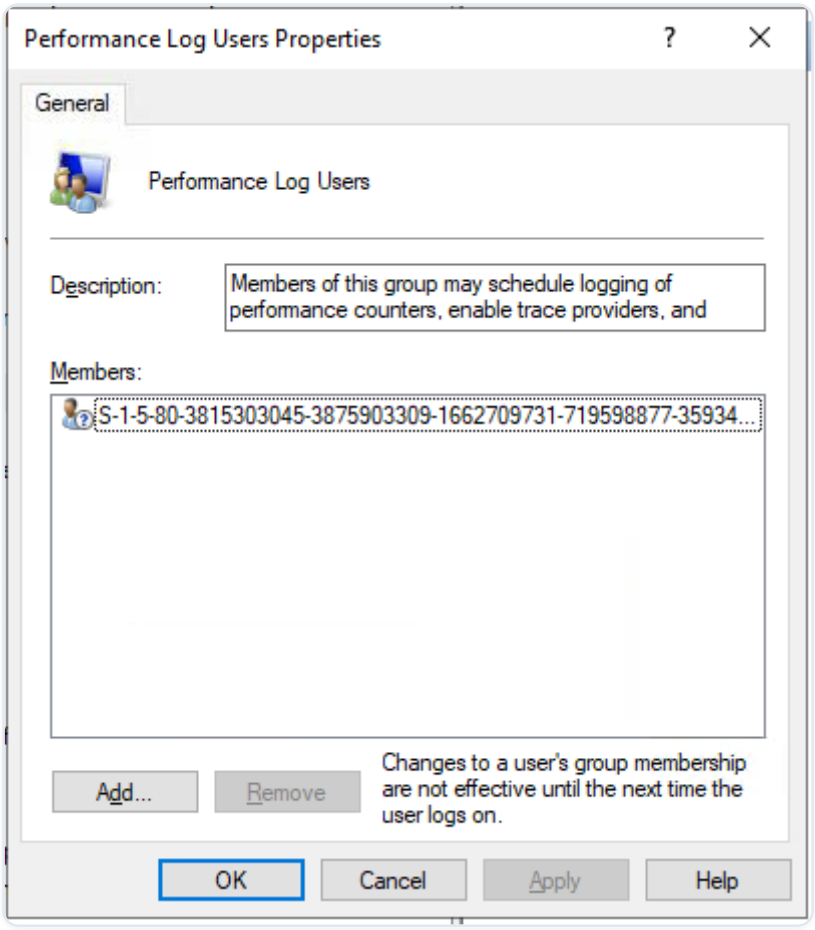


AOT 跟踪文件夹保存在 `C:\ProgramData\Citrix\TelemetryService\CitrixAOT` 中。

只有管理员组、系统和 Telemetry Service SID 中的用户才有权访问 `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry` 注册表。



卸载 Telemetry Service 后，Telemetry Service SID 仍保留在“性能日志用户”组中，但您可以手动将其删除。



验证测试

在诊断信息收集或运行状况检查开始之前，将为每台选定的计算机自动运行验证测试。这些测试可确保满足要求。如果某台计算机的测试失败，Scout 将显示一条消息，其中包含建议的纠正措施。

- **Scout 无法访问此计算机** - 请确保：
  - 计算机已开机。
  - 网络连接正常工作。（这可能包括验证您的防火墙是否已正确配置。）
  - 文件和打印机共享已启用。有关说明，请参阅 Microsoft 文档。
- **启用 PSRemoting 和 WinRM** - 您可以同时启用 PowerShell 远程处理和 WinRM。使用**以管理员身份运行**，运行 `Enable-PSRemoting` cmdlet。有关详细信息，请参阅 cmdlet 的 Microsoft 帮助。
- **Scout 需要 PowerShell 3.0（最低版本）** - 在计算机上安装 PowerShell 3.0（或更高版本），然后启用 PowerShell 远程处理。
- **无法访问此计算机上的 LocalAppData 目录** - 确保该帐户具有在此计算机上的 LocalAppData 目录中写入的权限。
- **找不到 Citrix Telemetry Service** - 确保 Citrix Telemetry Service 已安装并在计算机上启动。

- **无法获取计划** - 将计算机升级到 XenApp 和 XenDesktop 7.14（最低版本）。
- **WMI 未在计算机上运行** - 确保已启用 Windows Management Instrumentation (WMI) 访问。
- **WMI 连接被阻止** - 在 Windows 防火墙服务中启用 WMI。
- **需要更高版本的 Citrix Telemetry Service** - （仅针对“收集”和“跟踪与重现”检查版本。）升级计算机上的 Telemetry Service 版本（请参阅安装和升级）。如果您不升级该服务，则该计算机将不包括在**收集**或**跟踪与重现**操作中。
- **Scout 无法连接到此计算机上的 systemd 套接字** - 请确保：
  - 端口 7503 已打开。验证 `systemd ctxtelemetry.socket` 正在计算机上的端口 7503 上侦听。如果 `ctxtelemetry.socket` 端口已更改，则端口可能不同。请参阅Scout 配置 以调整端口。
  - 网络连接正常工作。（这可能包括验证您的防火墙是否已正确配置。）
- **Linux VDA 遥测服务未在此计算机上启动** - 确保：
  - 端口 7502 已打开。验证 Linux VDA 遥测服务是否已安装并在计算机上启动。如果遥测服务端口已更改，则端口可能不同。请参阅 Scout 配置 以调整端口。
  - 网络连接正常工作。（这可能包括验证您的防火墙是否已正确配置。）

版本兼容性

此版本的 Scout (3.x) 旨在 Citrix Virtual Apps and Desktops（或最低 XenApp and XenDesktop 7.14）控制器和 VDA 上运行。

| 功能 | 侦察兵 2.23 | 侦察兵 3.0 | --- | --- | ---| -- | 支持 Citrix Virtual Apps and Desktops（以及 XenApp 和 XenDesktop 7.14 到 7.18） | 是 | 是 支持 XenDesktop 5.x、7.1–7.13 | 是 | 否 支持 XenApp 6.x、7.5 到 7.13 | 是 | 否 随产品提供 | 7.1–7.13 | 从 7.14 开始 可从 CTX 文章下载 | 是 | 否 捕获 CDF 跟踪 | 是 | 是 捕获始终开启的跟踪 (AOT) | 否 | 是 允许收集诊断数据 | 最多同时 10 台计算机（默认） | 无限制（取决于资源可用性） 允许将诊断数据发送到 Citrix | 是 | 是 允许将诊断数据保存到本地 | 是 | 是 支持 Citrix Cloud™ 凭据 | 否 | 是 支持 Citrix 凭据 | 是 | 是 支持用于上传的代理服务器 | 是 | 是 调整计划 | N/A | 是 脚本支持 | 命令行（仅限本地控制器） | PowerShell 使用 Call Home cmdlet（安装了遥测服务的任何计算机） 运行状况检查 | 否 | 是 数据掩码 | 否 | 从 3.17 开始

安装和升级

默认情况下，当您安装或升级 VDA 或 Controller 时，Scout 会作为 Citrix Telemetry Service 的一部分自动安装或升级。

如果在安装 VDA 时省略 Citrix Telemetry Service，或者以后删除了该服务，请从 Citrix Virtual Apps and Desktops 安装介质上的 `x64\Virtual Desktop Components` 或 `x86\Virtual Desktop Components` 文件夹运行 `TelemetryServiceInstaller_xx.msi`。

选择“**收集**”或“**跟踪和重现**”操作时，如果计算机运行的是旧版 Citrix Telemetry Service，系统会通知您。Citrix 建议使用最新支持的版本。如果您未在该计算机上升级 Telemetry Service，则该计算机不会包含在“**收集**”或“**跟踪和重现**”操作中。要升级 Telemetry Service，请使用与安装它相同的过程。

上传授权

如果您计划将诊断集合上传到 Citrix，则必须拥有 Citrix 或 Citrix Cloud 帐户。（这些是您用于访问 Citrix 下载或访问 Citrix Cloud Control Center 的凭据。）验证您的帐户凭据后，将颁发一个令牌。

如果您使用 Citrix 帐户或 Citrix Cloud 帐户进行身份验证，请单击链接以使用默认浏览器通过 HTTPS 访问 Citrix Cloud。输入 Citrix Cloud 凭据后，将显示令牌。复制令牌，然后将其粘贴到 Scout 中。然后，您可以在 Scout 向导中继续操作。

令牌存储在运行 Scout 的计算机本地。要启用下次运行“**收集**”或“**跟踪和重现**”时使用该令牌，请选中“**存储令牌并在将来跳过此步骤**”复选框。

每次在 Scout 启动页面上选择“**计划**”时，都必须重新授权。创建或更改计划时不能使用存储的令牌。

使用代理进行上传

如果要使用代理服务器将集合上传到 Citrix，可以指示 Scout 使用为浏览器 Internet 属性配置的代理设置。或者，您可以指定代理服务器的 IP 地址和端口号。

查找计算机

对于“**收集**”、“**跟踪和重现**”和“**计划**”过程，Scout 会列出其自动发现的 Controller 和 VDA。

从 Citrix Virtual Apps and Desktops LTSR 2607 开始，当 Scout 在 StoreFront 服务器上运行时，它还会自动发现同一 StoreFront 服务器组中的其他服务器，并将其列在“**选择计算机**”页面上，以用于“**收集**”、“**跟踪和重现**”和“**计划**”。要使自动发现正常工作，必须满足以下先决条件：

- Scout 必须在 StoreFront 计算机本身上运行。在“**收集**”、“**跟踪和重现**”和“**计划**”过程中，在 Delivery Controller 上运行 Scout 不会发现 StoreFront 服务器组的成员。
- 该计算机上必须存在 `Citrix.StoreFront` PowerShell 模块。
- 仅当服务器组包含多个服务器时，才会发现其他 StoreFront 服务器。在单服务器部署中，仅列出本地服务器。

Scout 选择计算机页面，显示自动发现的 StoreFront 服务器组成员(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/scout-collect-window.png)

从 Delivery Controller 运行 Scout 运行状况检查 时，单击“**查找计算机**”以发现计算机，包括 Delivery Controller、VDA、许可证服务器和 StoreFront 服务器。

当您从非 Delivery Controller 的已加入域的计算机运行 Scout 运行状况检查时，Scout 无法自动发现计算机。您需要手动添加计算机 或导入 VDA 计算机。

手动添加计算机

在 Scout 列出其发现的 Controller 和 VDA 后，您可以手动添加部署中的其他计算机，例如 StoreFront 服务器、许可证服务器和 Citrix Provisioning 服务器。

运行运行状况检查 时：

- 域中的 Citrix 许可证服务器会自动发现。您无法手动添加许可证服务器。
- 运行状况检查目前不支持 Citrix Provisioning 服务器。

在列出已发现计算机的任何 Scout 页面上，单击“**+ 添加计算机**”。键入要添加的计算机的 FQDN，然后单击“**继续**”。根据需要重复此操作以添加其他计算机。（尽管输入 DNS 别名而不是 FQDN 可能看起来有效，但运行状况检查可能会失败。）

手动添加的计算机始终显示在计算机列表的顶部，位于已发现计算机的上方。

识别手动添加的计算机的一种简单方法是行右端的红色删除按钮。只有手动添加的计算机才具有该按钮。已发现的计算机没有。

要删除手动添加的计算机，请单击行右端的红色按钮。确认删除。重复此操作以删除其他手动添加的计算机。

Scout 会记住手动添加的计算机，直到您将其删除。当您关闭并重新打开 Scout 时，手动添加的计算机仍会显示在列表顶部。

在 StoreFront 服务器上使用 **Trace & Reproduce** 时，不会收集 CDF 跟踪。但是，会收集所有其他跟踪信息。

> **注意：**
>
> 从 Citrix Virtual Apps and Desktops LTSR 2607 开始，当 Scout 在 StoreFront 服务器上运行时，同一 StoreFront 服务器组中的服务器会自动列出 (请参阅 查找计算机)。如果您需要包含不属于自动发现组的 StoreFront 服务器，请使用“**+ 添加计算机**”按钮。从 Citrix Virtual Apps and Desktops LTSR 2507 开始，当 Scout 在 StoreFront 计算机上运行时，此按钮仅显示在“

> **收集**”页面上（不显示在“**跟踪和重现**”或“**计划**”页面上）。*TelemetryService* 的旧版本不支持此功能。

导入 VDA 计算机

您可以在运行 运行状况检查 时导入部署中的 VDA 计算机。

1. 在 Delivery Controller 或 Connector 上，使用 PowerShell 命令生成计算机列表文件。在 Connector 上，您必须输入 Citrix 凭据并在弹出对话框中选择客户。

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
   ```

2. 将 machineList.txt 文件复制到要启动 Scout 运行状况检查的已加入域的计算机。
3. 在 Scout 运行状况检查页面上，单击“**添加计算机**”。
4. 选择“**Windows VDA**”计算机类型。
5. 单击“**导入 VDA 计算机**”。
6. 选择 machineList.txt 文件。
7. 单击“**打开**”。

导入的 VDA 计算机将显示在 Scout 运行状况检查页面上。

收集诊断信息

“**收集**”过程包括选择计算机、启动诊断信息收集，然后将包含收集信息的文件上传到 Citrix 或将其保存到本地。

1. 启动 Scout。从计算机的“**开始**”菜单中，选择“**Citrix > Citrix Scout**”。在打开的页面上，单击“**收集**”。
2. 选择计算机。
   - 在 Controller 上，“**选择计算机**”页面列出了站点中的所有 VDA 和 Controller。您可以按计算机名称筛选显示。要手动添加其他计算机（例如 StoreFront 或 Citrix Provisioning 服务器），请参阅手动添加计算机。
   - 在 StoreFront 上，“**选择计算机**”页面列出了本地计算机以及同一 StoreFront 服务器组中自动发现的任何其他服务器。要包含自动发现组之外的服务器，请参阅手动添加计算机。
   - 在其他组件（例如 VDA 服务器）上，“**选择计算机**”页面仅列出本地计算机。不支持手动添加计算机。

选中要从中收集诊断信息的每台计算机旁边的复选框，然后单击“**继续**”。

Scout 会自动在每台选定的计算机上启动验证测试，确保其符合验证测试中列出的条件。如果验证失败，“**状态**”列中会显示一条消息，并且该计算机的复选框将被取消选中。您可以选择：

- 解决问题，然后再次选中该计算机的复选框。这将触发验证测试的重试。
- 跳过该计算机（使其复选框保持未选中状态）。将不会从该计算机收集诊断信息。

验证测试完成后，单击“**继续**”。

3. 收集诊断信息。摘要列出了所有从中收集诊断信息的计算机（您选择并通过验证测试的计算机）。单击“**开始收集**”。

   收集期间：

   - “**状态**”列指示计算机的当前收集状态。
   - 要停止单个计算机上正在进行的收集，请在该计算机的“**操作**”列中单击“**取消**”。
   - 要停止所有正在进行的收集，请单击页面右下角的“**停止收集**”。已完成收集的计算机的诊断信息将保留。要恢复收集，请在每台计算机的“**操作**”列中单击“**重试**”。
   - 当所有选定计算机的收集完成后，右下角的“**停止收集**”按钮将变为“**继续**”。
   - 要再次收集诊断信息，请在该计算机的“**操作**”列中单击“**再次收集**”。较新的收集会覆盖较早的收集。
   - 如果收集失败，您可以在“**操作**”列中单击“**重试**”。只有成功的收集才会被上传或保存。
   - 在所有选定计算机的收集完成后，请勿单击“**返回**”。（如果单击，收集将丢失。）

   收集完成后，单击“**继续**”。

4. 保存或上传收集。选择是将文件上传到 Citrix，还是将其保存在本地计算机上。

   如果您选择立即上传文件，请继续执行步骤 5。

   如果您选择将文件保存在本地：

   - 将出现一个 Windows“**保存**”对话框。导航到所需位置。
   - 本地保存完成后，将显示并链接文件的路径名。您可以查看该文件。您可以稍后将文件上传到 Citrix。请参阅 CTX136396。

   单击“**完成**”返回 Scout 启动页面。您无需完成此过程中的任何其他步骤。

5. 对上传进行身份验证，并可选择指定代理。有关详细信息，请参阅 上传授权。

   - 如果您尚未通过 Scout 进行身份验证，请继续执行此步骤。

- 如果您已通过 Scout 进行身份验证，默认使用存储的授权令牌。如果这是您想要执行的操作，请选择此选项并单击“**继续**”。系统不会提示您输入此收集的凭据。请继续执行步骤 6。
- 如果您之前已通过身份验证，但想重新授权并获取新令牌，请单击 **Change/Reauthorize** 并继续此步骤。

选择是使用 Citrix 凭据还是 Citrix Cloud 凭据来验证上传。单击 **Continue**。凭据页面仅在您未使用存储的令牌时显示。

在凭据页面上：

- 如果要使用代理服务器进行文件上传，请单击 **Configure proxy**。您可以指示 Scout 使用为浏览器 Internet 属性配置的代理设置。或者，您可以输入代理服务器的 IP 地址和端口号。关闭代理对话框。
- 对于 Citrix Cloud 帐户，请单击 **Generate token**。您的默认浏览器将启动到显示令牌的 Citrix Cloud 页面。复制令牌，然后将其粘贴到 Scout 页面上。
- 对于 Citrix 帐户，请输入您的凭据。

完成后，单击 **Continue**。

6. 输入有关上传的信息。

   - 名称字段包含所收集诊断文件的默认名称。这对于大多数收集来说已足够，尽管您可以更改名称。（如果您删除默认名称并将名称字段留空，则会使用默认名称。）
   - （可选）指定一个 8 位数的 Citrix Support 案例编号。
   - 在可选的 **Description** 字段中，描述问题并指明问题发生的时间（如果适用）。

   完成后，单击 **Start Upload**。

   在上传过程中，页面左下角会显示已完成上传的近似百分比。要取消正在进行的上传，请单击 **Stop Upload**。

   上传完成后，将显示其位置的 URL 并提供链接。您可以按照链接转到 Citrix 位置以查看上传分析，也可以复制该链接。

   单击 **Done** 返回 Scout 启动页面。

跟踪和重现

跟踪和重现过程包括选择计算机、启动跟踪、重现问题、完成诊断信息收集，然后将文件上传到 Citrix 或将其保存到本地。

此过程与标准**收集**过程类似。但是，它允许您在计算机上启动跟踪，然后在这些计算机上重新创建问题。所有诊断信息收集都包含 AOT 跟踪信息。此过程添加 CDF 跟踪以帮助进行故障排除。

1. 启动 Scout。从计算机的**开始**菜单中，选择 **Citrix > Citrix Scout**。在打开的页面上，单击**跟踪和重现**。
2. 选择计算机。**选择计算机**页面列出了站点中的所有 VDA 和控制器。您可以按计算机名称筛选显示。选中要从中收集跟踪和诊断信息的每台计算机旁边的复选框。然后单击**继续**。

   在 StoreFront 上，**选择计算机**页面列出了本地计算机以及同一 StoreFront 服务器组中自动发现的任何其他服务器。要包括自动发现组之外的服务器，请参阅手动添加计算机。

   要手动添加其他计算机（例如 StoreFront 或 Citrix Provisioning 服务器），请参阅手动添加计算机。

   Scout 会自动在每台选定的计算机上启动验证测试，确保其符合验证测试中列出的条件。如果某台计算机的验证失败，则会在**状态**列中发布一条消息，并且该计算机的复选框将被取消选中。您可以选择：

   - 解决问题，然后再次选中该计算机的复选框。这将触发验证测试的重试。
   - 跳过该计算机（使其复选框保持未选中状态）。不会从该计算机收集诊断信息和跟踪。

   验证测试完成后，单击**继续**。
3. 启动跟踪。摘要列出了从中收集跟踪的所有计算机。单击**开始跟踪**。

   在一台或多台选定的计算机上，重现您遇到的问题。在此过程中，跟踪收集会继续。重现问题完成后，在 Scout 中单击**继续**。这将停止跟踪。

   停止跟踪后，指示您是否在跟踪期间重现了问题。
4. 从计算机收集诊断信息。单击**开始收集**。收集期间：

   - **状态**列指示计算机的当前收集状态。
   - 要停止单个计算机上正在进行的收集，请在该计算机的**操作**列中单击**取消**。
   - 要停止所有正在进行的收集，请单击页面右下角的**停止收集**。已完成收集的计算机的诊断信息将保留。要恢复收集，请在每台计算机的**操作**列中单击**重试**。
   - 当所有选定计算机的收集完成后，右下角的**停止收集**按钮将变为**继续**。
   - 要从计算机再次收集诊断信息，请在该计算机的**操作**列中单击**再次收集**。较新的收集会覆盖较早的收集。
   - 如果收集失败，您可以在**操作**列中单击**重试**。只有成功的收集才会上传或保存。
   - 所有选定计算机的收集完成后，请勿单击**返回**。（如果单击，收集将丢失。）

收集完成后，单击**继续**。

5. 保存或上传收集。选择是将文件上传到 Citrix 还是将其保存到本地。

   如果您选择立即上传文件，请继续执行步骤 6。

   如果您选择将文件保存到本地：

   - 将显示一个 Windows 保存对话框。选择所需位置。
   - 本地保存完成后，将显示并链接文件的路径名。您可以查看该文件。请记住：您可以稍后从 Citrix 上传文件；有关 Citrix Insight Services，请参阅 CTX136396。

   单击**完成**返回 Scout 启动页面。您无需完成此过程中的任何其他步骤。

6. 对上传进行身份验证，并可选择指定代理。有关此过程的详细信息，请查看 上传授权。

   - 如果您尚未通过 Scout 进行身份验证，请继续执行此步骤。
   - 如果您已通过 Scout 进行身份验证，则默认使用存储的授权令牌。如果这是您想要执行的操作，请选择此选项并单击 **Continue**。系统不会提示您输入此集合的凭据。继续执行步骤 7。
   - 如果您之前已进行身份验证，但想要重新授权并获取新令牌，请单击 **Change/Reauthorize** 并继续执行此步骤。

   选择您是要使用 Citrix 凭据还是 Citrix Cloud 凭据来验证上传。单击 **Continue**。凭据页面仅在您未使用存储的令牌时显示。

   在凭据页面上：

   - 如果要为文件上传使用代理服务器，请单击 **Configure proxy**。您可以指示 Scout 使用为浏览器 Internet 属性配置的代理设置。或者，您可以输入代理服务器的 IP 地址和端口号。关闭代理对话框。
   - 对于 Citrix Cloud 帐户，请单击 **Generate token**。您的默认浏览器将启动到 Citrix Cloud 页面，其中显示一个令牌。复制该令牌，然后将其粘贴到 Scout 页面上。
   - 对于 Citrix 帐户，请输入您的凭据。

   完成后，单击 **Continue**。

7. 提供有关上传的信息。

   输入上传详细信息：

   - 名称字段包含所收集诊断文件的默认名称。这对于大多数集合来说已足够，尽管您可以更改名称。（如果您删除默认名称并使名称字段为空，则会使用默认名称。）
   - （可选）指定一个 8 位数的 Citrix 支持案例编号。

- 在可选的“描述”字段中，描述问题并指明问题发生的时间（如果适用）。

完成后，单击 **Start Upload**。

在上传过程中，页面左下角会显示上传完成的大致百分比。要取消正在进行的上传，请单击 **停止上传**。

上传完成后，将显示其位置的 URL 并提供链接。您可以单击该链接转到 Citrix 位置以查看上传分析，也可以复制该链接。

单击 **完成** 返回 Scout 启动页面。

Scout 支持 TraceLogging 提供程序

以前，Scout 仅支持 Windows 性能提供程序，该提供程序需要额外的解码文件，并且仅跟踪同一提供程序的单个会话中的会话和事件。

从 Citrix Virtual Apps and Desktops 2411 版本开始，Scout 支持 TraceLogging 提供程序。此提供程序不需要额外的解码文件，并且可以为同一提供程序启用并接收来自最多八个跟踪会话的事件。此功能默认启用。

启用附加日志收集

启用附加日志收集 功能允许您将跟踪和重现功能与更多工具（例如 perfmon、Netsh、DebugView 和 Wireshark）结合使用。

从 2407 版本开始，当您启用附加日志收集时，Scout 会自动检测计算机上安装的 CDC 相关工具，并在 zip 包中自动收集 CDC 工具相关的跟踪日志。您可以自定义这些 zip 文件并将其附加到 Scout。通过此自动化，您可以更有效地使用 Citrix Scout，这有助于您快速诊断问题。

> **注意：**
>
> 这仅适用于本地计算机。
>
> 要启用附加日志收集，请确保已安装以下所需工具，并在指定位置手动创建其目录。

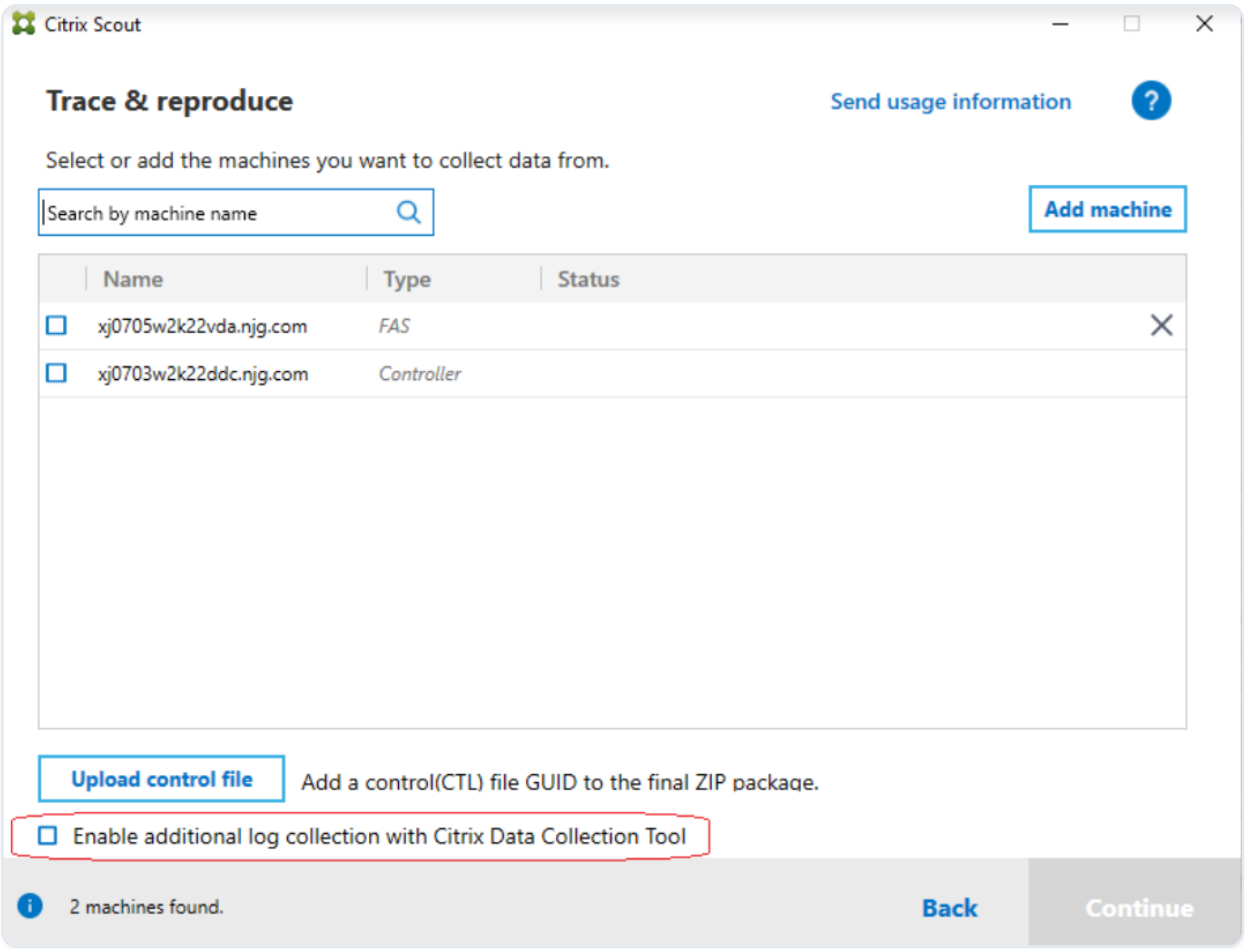
工具安装位置：

- **Procdump** 日志：下载 **Procdump** 并将其放置在 %ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\Procdump\procdump.exe
- **StoreFront** 日志：下载 **DbgView** 并将其放置在 %ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\Dbgview.exe

- **Procmon** 日志：下载 **Process Monitor** 并将其放置在 %ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\ProcessMonitor\Procmon.exe
- **Wireshark** 日志：在您的系统上手动安装 **Wireshark**。

要收集其他日志：

1. 在 Scout 主页上，单击“**跟踪和重现**”。
2. 在“**选择或添加计算机**”页面上，勾选本地计算机的复选框以从该页面收集数据。状态必须显示为 *已验证*。
3. 选中“**使用 Citrix 数据收集工具启用其他日志收集**”复选框以启用其他日志收集。
4. 单击“**上传控制文件**”按钮以加载一个 CTL 文件。此按钮允许您在 AOT 收集列表中添加其他 GUID，以便使用 Scout 进行 AOT 收集。
5. 单击“**继续**”并按照 跟踪和重现 说明进行操作。
6. 完成后，检查 zip 文件中的日志。日志已压缩到 *CDCLogs* 文件夹中。



注意：

如果选择 Procmon 工具进行跟踪，则 Process Monitor 日志可能会快速增长。请确保仅选择所需的工具。您还可以在 *%temp%\Scout-CDC-Log* 下监视日志的大小。

安排收集

注意：

您目前可以安排收集，但不能安排运行状况检查。

计划过程包括选择计算机，然后设置或取消计划。计划的收集会自动上传到 Citrix。（您可以使用 PowerShell 界面在本地保存计划的收集。请参阅 Citrix Call Home。）

1. 启动 Scout。从计算机的“开始”菜单中，选择“**Citrix > Citrix Scout**”。在打开的页面上，单击“**计划**”。
2. 选择计算机。站点中的所有 VDA 和控制器都已列出。您可以按计算机名称筛选显示。

   在 StoreFront 上，“**选择计算机**”页面列出了本地计算机以及同一 StoreFront 服务器组中自动发现的任何其他服务器。要包含自动发现组之外的服务器，请参阅手动添加计算机。

   使用图形界面安装 VDA 和 Controller 时，如果设置了 Call Home 计划（请参阅Citrix Call Home），Scout 默认会显示这些设置。您可以使用此版本的 Scout 首次启动计划的收集，或更改以前配置的计划。

   尽管您在组件安装期间按每台计算机启用了/禁用了 Call Home，但在 Scout 中配置的计划会影响您选择的所有计算机。

   选中要从中收集诊断信息的每台计算机旁边的复选框，然后单击“**继续**”。

   要手动添加其他计算机（例如 StoreFront 或 Citrix Provisioning 服务器），请参阅手动添加计算机。

   Scout 会自动对每台选定的计算机启动验证测试，确保其符合验证测试中的条件。如果某台计算机的验证失败，则会在“**状态**”列中发布一条消息，并且该计算机的复选框将被取消选中。您可以选择：

   - 解决问题，然后再次选中该计算机的复选框。这将触发验证测试的重试。
   - 跳过该计算机（使其复选框保持未选中状态）。不会从该计算机收集诊断信息（或跟踪）。

   验证测试完成后，单击“**继续**”。

摘要页面列出了应用了计划的计算机。单击“**继续**”。

3. 设置计划。指明您希望何时收集诊断信息。请记住：该计划会影响所有选定的计算机。

   - 要为选定的计算机配置每周计划，请单击“**每周**”。选择星期几。输入收集开始的时间（24 小时制）。
   - 要为选定的计算机配置每日计划，请单击“**每日**”。输入收集开始的时间（24 小时制）。
   - 要取消选定计算机的现有计划（且不替换为其他计划），请单击“**关闭**”。这将取消之前为这些计算机配置的任何计划。

   单击“**继续**”。

4. 对上传进行身份验证，并可选择指定代理。有关此过程的详细信息，请查看上传授权。请记住：使用 Scout 计划时，不能使用存储的令牌进行身份验证。

   选择是使用 Citrix 凭据还是 Citrix Cloud 凭据来验证上传。单击 **继续**。

   在凭据页面上：

   - 如果要使用代理服务器进行文件上传，请单击 **配置代理**。您可以指示 Scout 使用为浏览器 Internet 属性配置的代理设置。或者，您可以输入代理服务器的 IP 地址和端口号。关闭代理对话框。
   - 对于 Citrix Cloud 帐户，请单击 **生成令牌**。您的默认浏览器将启动到 Citrix Cloud 页面，其中显示一个令牌。复制该令牌，然后将其粘贴到 Scout 页面上。
   - 对于 Citrix 帐户，请输入您的凭据。

   完成后，单击 **继续**。

   查看已配置的计划。单击 **完成** 返回 Scout 启动页面。

   在收集过程中，每台选定计算机的 Windows 应用程序日志都包含有关收集和上传的条目。

数据屏蔽

使用 Citrix Scout 收集的诊断信息可能包含安全敏感信息。Citrix Scout 数据屏蔽功能允许您在将诊断文件上传到 Citrix 之前屏蔽其中的敏感数据。

Scout 数据屏蔽配置为屏蔽 IP 地址、计算机名称、域名、用户名、管理程序名称、交付组名称、目录名称、应用程序名称和 SID。

> **注意：**

> CDF 跟踪已加密，无法屏蔽。

> Linux VDA 日志已压缩为 `.tar.gz2` 格式，无法屏蔽。

收集新诊断信息并执行数据屏蔽

要使用 Citrix Scout 数据屏蔽功能，请从命令行启动 Scout。

1. 在 Windows 中，以管理员身份打开命令提示符。
2. 转到 Scout 的安装目录：`cd C:\Program Files\Citrix\Telemetry Service`。
3. 启动 Scout：`ScoutUI.exe datamasking`。
4. 单击“**收集**”或“**跟踪和重现**”以收集诊断信息。
5. 收集完成后，选择“**启用数据掩码**”。此选项默认启用。
6. 配置数据掩码。您可以使用默认规则或自定义规则。
7. 选择是上传还是保存诊断信息集合。
   - 如果选择“**将诊断信息集合上传到 Citrix**”，则会将已掩码的诊断文件上传到 Citrix。
   - 如果选择“**将诊断信息集合保存到本地计算机**”，则原始诊断信息和已掩码的诊断信息都将保存到指定位置。

对现有诊断信息执行数据掩码

1. 在 Windows 中，以管理员身份打开命令提示符。
2. 转到 Scout 的安装目录：`cd C:\Program Files\Citrix\Telemetry Service`。
3. 直接在数据掩码模式下启动 Scout：`ScoutUI.exe datamasking filePath`。
4. 选择“启用数据掩码”以继续。此选项默认启用。
5. 配置数据掩码。您可以使用默认规则运行数据掩码，也可以自定义规则。
6. 选择是上传还是保存诊断集合。
   - 如果选择**将诊断集合上传到 Citrix**，则会将屏蔽的诊断文件上传到 Citrix。
   - 如果选择**将诊断集合保存到本地计算机**，则原始诊断和屏蔽诊断都将保存到指定位置。

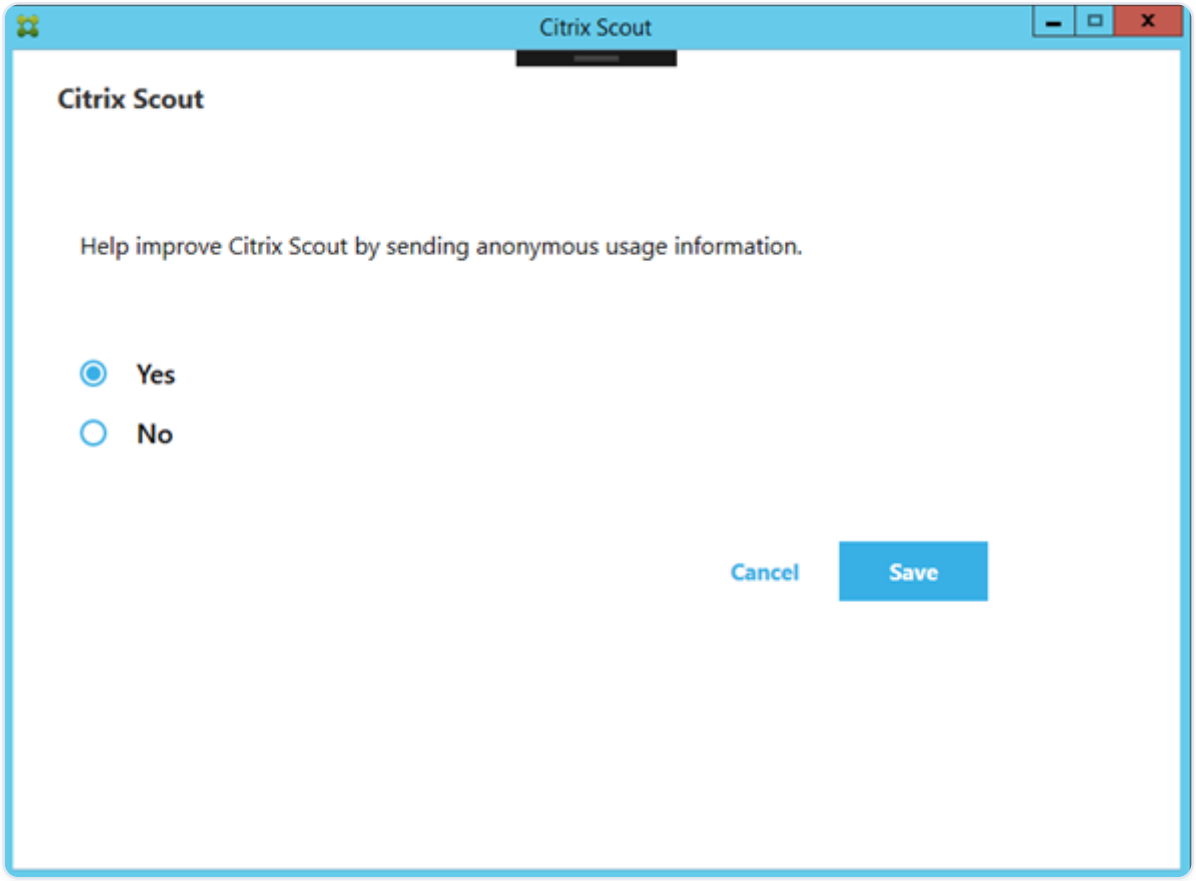
屏蔽数据文件和映射文件位置

上传或保存诊断集合后，单击链接以打开原始诊断和屏蔽诊断，并打开映射信息文件。

使用情况数据收集

使用 Scout 时，Citrix 会使用 Google Analytics 收集匿名使用情况数据，以用于未来的产品功能和改进。数据收集默认启用。

要更改使用情况数据收集和上传，请单击 Scout UI 中的**设置**齿轮。然后，您可以选择**是**或**否**来决定是否发送信息，然后单击**保存**。



Scout 功能的命令行界面

您现在可以使用 Scout 功能的命令行界面，从而无需打开 Scout UI 即可收集所需的日志和数据。此功能为高级用户提供了便利，可以自动执行目标计算机或站点的本地或远程日志或跟踪过程。此功能默认启用。

已为以下功能添加了命令：

- 帮助
- 收集诊断信息
- 启动跟踪
- 停止跟踪
- 列出正在进行的跟踪会话

- 启动和停止 CDC

> **注意：**
>
> 运行远程跟踪会话时，必须在 VDA 和 DDC 上安装新的遥测版本。需要此安装是因为 Scout 命令行从 Citrix Virtual Apps and Desktops 2411 版开始受支持，而 `TelemetryService` 的旧版本不支持此功能。

下表描述了新添加的命令：

帮助

命令行界面	描述	示例
`ScoutCLI.exe -h`	显示上下文相关的帮助。	`ScoutCLI.exe -h` `ScoutCLI.exe -help`

收集诊断的命令

命令行界面	描述	示例
`ScoutCLI.exe Collect -exclude <collector>`	从指定的收集器中排除诊断信息（Windows 管理规范 (WMI) 进程、注册表、崩溃报告、标头、跟踪、`msi`、`vcu`、工具遥测和本地数据）。	`ScoutCLI.exe collect -exclude wmi, localdata -output "C:/Logs/mydata.zip"`
`ScoutCLI.exe Collect -output <filename>`	指定输出日志文件的保存位置，并以 `.zip` 作为后缀。	
`ScoutCLI.exe Collect -fqdn <hostname>`	收集站点中指定计算机上的诊断信息。	`ScoutCLI.exe collect -fqdn hostname -exclude wmi, localdata -output "C:/Logs/mydata.zip"`

启动跟踪

命令行界面	描述	示例
`ScoutCLI.exe StartTrace -guids <filename (xxx.ctl)>`	收集指定 GUID 的目标模块日志。	本地计算机跟踪启动示例 - `ScoutCLI.exe StartTrace -guids C:\Logs\provider1.ctl -output C:\Logs\xxx.etl -name session1 -level 16 -max 50`；远程计算机跟踪启动示例 - `ScoutCLI.exe StartTrace -fqdn hostname -guids C:\Logs\provider1.ctl -output C:\Logs\xxx.etl -name session1 -level 16 -max 50`
`ScoutCLI.exe StartTrace -output <filename>`	指定保存输出日志文件的位置，后缀为 .etl。	
`ScoutCLI.exe StartTrace -name <session name>`	定义跟踪会话的名称。	
`ScoutCLI.exe StartTrace -level <value>`	选择日志级别以记录目标诊断详细信息。默认值为 16。	
`ScoutCLI.exe StartTrace -max <value>`	指定日志文件的最大大小（MB）。默认值为 50。	
`ScoutCLI.exe StartTrace -fqdn <hostname>`	在站点中的指定计算机上开始跟踪。	

停止跟踪

命令行界面	描述	示例
`ScoutCLI.exe StopTrace -name <session name>`	停止指定的跟踪会话。	`ScoutCLI.exe StopTrace -name session1`
`ScoutCLI.exe StopTrace -fqdn <hostname>`	在站点中的指定计算机上停止跟踪。需要 -o 选项来指定远程 `.etl` 复制到的本地路径。	`ScoutCLI.exe StopTrace -fqdn hostname -name session1 -output C:\Logs\xxx.etl`
`ScoutCLI.exe StopTrace -output <filename>`	指定保存输出日志文件的位置，后缀为 .etl。	

列出正在进行的跟踪会话

命令行界面	描述	示例
`ScoutCLI.exe ListSession -name <session name>`	显示指定跟踪会话的详细信息。如果未指定名称，则显示所有正在运行的跟踪会话的详细信息。	`ScoutCLI.exe ListSession -name session1`
`ScoutCLI.exe ListSession -fqdn <hostname>`	显示站点中指定计算机上的跟踪详细信息。	`ScoutCLI.exe ListSession -fqdn hostname -name session1`

启动和停止 CDC

命令行界面	描述	示例
`ScoutCLI.exe StartCDC -config <filename>`	指定 Citrix Diagnostic Collectors (CDC) 工具参数的 JSON 配置文件。	`ScoutCLI.exe StartCDC -config xxx.json -path C:\Logs`
`ScoutCLI.exe StartCDC -path <folder>`	指定输出日志文件的保存位置。	
`ScoutCLI.exe StopCDC`	停止 CDC 工具的收集。	`ScoutCLI.exe StopCDC`

Call Home 关键数据点

Call Home 收集以下关键数据点。

(M) = 仅在手动收集期间捕获 (PowerShell cmdlet `Start-CitrixCallHomeUpload`)

文件名	类别	数据组
		计算机
		XD站点
		站点信息
		Broker 数据库信息 (M)

		已安装的数据库版本 (M)
		Broker 服务状态 (M)
		已注册的服务实例 (M)
		Broker 许可证测试 (M)
		活动 HDX™ 会话 (M)
		Broker 管理员
		Broker 管理员权限
		RDS 配置（包括 LicensingSettings、SessionSettings、SpecifiedLicenseServers 和 RegisteredLicenseServers）
		监控服务 (M)（包括 MonitorConfiguration、MonitorDataStore、MonitorDBConnection、MonitorDBSchemaVersion、MonitorService、MonitorServiceAddedCapability、MonitorServiceInstance、MonitorServiceStatus 和 MonitorInstalledDBVersion）
		配置日志记录
		连接日志
		管理程序连接 (M)
		代理管理程序连接
		管理程序警报
		目录
		多会话操作系统代理 (M)

		单会话操作系统代理 (M)
		已发布的应用程序
		交付组
		已配置的交付代理

		Citrix 已安装组件
		Citrix 代理服务信息
		代理服务配置文件
		计算机创建服务™ 配置文件
		主机服务配置文件
		AD 身份服务配置文件
		配置服务配置文件
		配置日志服务配置文件
		委派管理服务配置文件
		环境测试服务配置文件
		监视服务配置文件
		Storefront™ 服务配置文件
		工作站代理配置文件
		Citrix VDA 信息
		Citrix XD 热修复
		Citrix_VirtualChannel_Graphics_Enum
		Citrix_VirtualChannel_Flash_Enum

		Citrix_VirtualChannel_Printer_Enum

		计算机
		BIOS
		内存信息
		处理器
		PnP 设备
		设备
		磁盘驱动器
		逻辑驱动器
		页面文件使用情况
		网络适配器
		网络适配器配置
		ipConfig
		视频控制器
		IDE 控制器
		SCSI 控制器

		HKLM:\Software\Wow6432Node\Citrix
		HKLM:\System\CurrentControlSet\Control\Citrix

		HKLM:\SOFTWARE\Policies\Citrix
		HKLM:\Software\Microsoft\Cryptography
		HKLM:\Software\Wow6432Node\Microsoft\Cryptography
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Windows
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
		HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\SYSTEM\CurrentControlSet\Control\Print\Environments
		HKLM:\System\CurrentControlSet\Control\Session Manager
		HKLM:\System\CurrentControlSet\Control\Terminal Server
		HKCU:\Control Panel\Desktop

		HKLM:\SOFTWARE\Classes\ShockwaveFlash.ShockwaveFlash\CurVer
		HKLM:\SYSTEM\CurrentControlSet\Control\SystemInformation
		HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem
		HKLM:\SYSTEM\CurrentControlSet\Control\Windows
		HKLM:\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

		驱动程序
		环境变量
		操作系统
		进程
		服务
		服务包
		组策略结果
		Microsoft 热修复程序
		网络统计
		PNP 驱动程序

		系统事件日志

		AOT（始终开启的跟踪）
		崩溃转储

		运行时间
		内存
		计算机系统
		处理器
		视频控制器
		磁盘驱动器
		浏览器信息
		重启次数
		内存使用情况
		磁盘使用情况
		ICA 会话分辨率
		ICA 颜色深度
		元安装程序-客户体验改善计划-机器 ID

		存储数量
		服务器组中的服务器数量
		每个存储的 Delivery Controller™ 数量
		HTTPS 已启用
		为 Citrix Receiver™ 启用经典体验

		适用于 Citrix 接收器的 HTML5 接收器设置
		为 Citrix Receiver 启用工作区控制
		Store 的远程访问已启用
		网关数量
		用于集成 NetScaler® 身份验证的显式 JSON 服务

在系统启动时收集 Citrix 诊断工具 (CDF) 跟踪

CDFControl 实用程序是一个事件跟踪控制器或使用者，用于捕获来自各种 Citrix 跟踪提供程序的 Citrix 诊断工具 (CDF) 跟踪消息。它旨在解决复杂的 Citrix 相关问题、解析筛选器支持并收集性能数据。要下载 CDFControl 实用程序，请参阅 CTX111961。

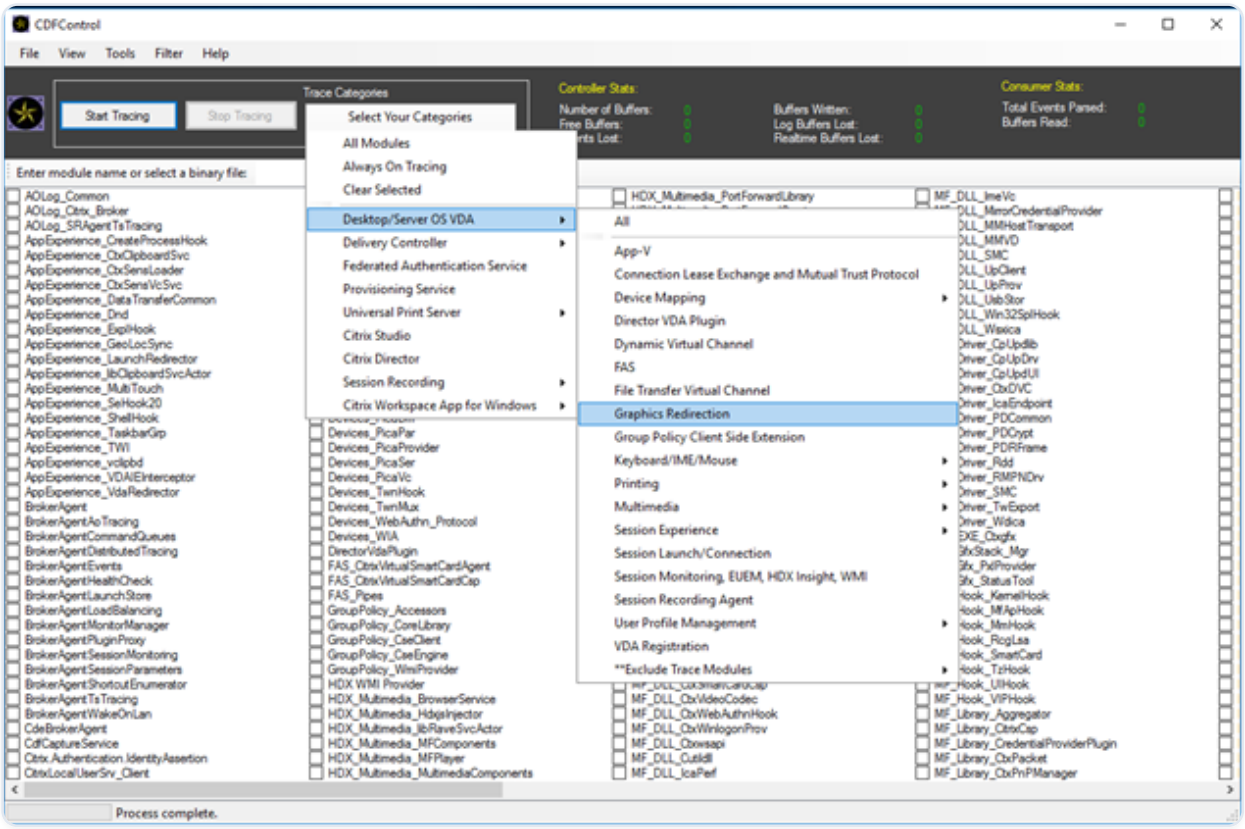
在系统启动时收集跟踪

使用以下过程在系统启动时收集 CDF 跟踪。您需要管理员权限。

1. 启动 **CDFControl**，然后从**工具**菜单中选择**选项**。
2. 在**用于捕获启动跟踪的启动跟踪文件路径**部分中指定跟踪文件路径。然后单击**保存**。

3. 选择 Citrix 支持建议的**跟踪类别**。（在以下示例中，选择了**图形重定向**。该选择仅为示例。我们建议您为正在排查的特定问题启用提供程序。）



4. 选择**启动跟踪**，然后从**工具**菜单中选择**启用**。

   选择**启用**后，动画栏开始滚动。此活动不影响过程。继续执行下一步。

5. 启用**启动跟踪**后，关闭 **CDFControl 实用程序**并重新启动系统。
6. 启动 **CDFControl** 实用程序。系统重新启动并出现错误后，通过从**工具**菜单中选择**启动跟踪**并单击**禁用**来禁用启动跟踪。
7. 转到步骤 2 中指定的跟踪文件路径，并收集跟踪日志文件 (.etl) 进行分析。

委派管理

注意：

从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

委派管理模型提供了灵活性，可根据您的组织希望如何委派管理活动（使用基于角色和基于对象的控制）进行匹配。委派管理适用于所有规模的部署，并允许您随着部署复杂性的增加配置更精细的权限。委派管理使用三个概念：管理员、角色和范围。

- **管理员：** 管理员代表一个人或一群人，由其 Active Directory 帐户标识。每个管理员都与一个或多个角色和范围对相关联。
- **角色：** 角色代表一项职能，并具有与之关联的已定义权限。例如，“交付组管理员”角色具有“创建交付组”和“从交付组中删除桌面”等权限。管理员可以为一个站点拥有多个角色，因此一个人可以是交付组管理员，也可以是计算机目录管理员。角色可以是内置的，也可以是自定义的。

  内置角色包括：

角色	权限
完全管理员	可以执行所有任务和操作。完全管理员始终与“所有”范围结合使用。
只读管理员	除了全局信息外，可以查看指定范围内的所有对象，但不能更改任何内容。例如，具有“范围=伦敦”的只读管理员可以查看所有全局对象（例如配置日志记录）和任何伦敦范围的对象（例如伦敦交付组）。但是，该管理员无法查看纽约范围内的对象（假设伦敦和纽约范围不重叠）。
帮助台管理员	可以查看交付组，并管理与这些组关联的会话和计算机。可以查看受监控交付组的计算机目录和主机信息。还可以对这些交付组中的计算机执行会话管理和计算机电源管理操作。
计算机目录管理员	可以创建和管理计算机目录，并将计算机预配到其中。可以从虚拟化基础架构、Provisioning Services 和物理机构建计算机目录。此角色可以管理基础映像和安装软件，但不能将应用程序或桌面分配给用户。
交付组管理员	可以交付应用程序、桌面和计算机；还可以管理关联的会话。还可以管理应用程序和桌面配置，例如策略和电源管理设置。
主机管理员	可以管理主机连接及其关联的资源设置。不能向用户交付计算机、应用程序或桌面。

角色	权限
成本管理员	可以监控和查看 Azure MCS 目录的成本详细信息，特别是过去 30 天内产生的总成本以及当前和前一个 30 天期间的比较。

在某些产品版本中，您可以创建自定义角色以匹配您的组织要求，并更详细地委派权限。您可以使用自定义角色在控制台中以操作或任务的粒度分配权限。

- **作用域：** 作用域表示对象的集合。作用域用于以与您的组织相关的方式对对象进行分组（例如，销售团队使用的交付组集）。对象可以存在于多个作用域中；您可以将对象视为带有一个或多个作用域标签。有一个内置作用域：“所有”，其中包含所有对象。完全管理员角色始终与“**所有**”作用域配对。

示例

XYZ 公司决定根据部门（会计、销售和仓库）及其桌面操作系统（Windows 7 或 Windows 8）来管理应用程序和桌面。管理员创建了五个作用域，然后为每个交付组标记了两个作用域：一个用于它们所使用的部门，另一个用于它们所使用的操作系统。

创建了以下管理员：

管理员	角色	作用域
domain/fred	完全管理员	所有（完全管理员角色始终具有“所有”作用域）
domain/rob	只读管理员	所有
domain/heidi	只读管理员，技术支持管理员	所有销售
domain/warehouseadmin	帮助台管理员	仓库
domain/peter	交付组管理员、计算机目录管理员	Win7

- Fred 是完全管理员，可以查看、编辑和删除系统中的所有对象。
- Rob 可以查看站点中的所有对象，但无法编辑或删除它们。
- Heidi 可以查看所有对象，并可以在销售范围内的交付组上执行技术支持任务。这使她能够管理与这些组关联的会话和计算机；她无法对交付组进行更改，例如添加或删除计算机。

- 任何属于 warehouseadmin Active Directory 安全组的成员都可以查看并对仓库范围内的计算机执行技术支持任务。
- Peter 是一名 Windows 7 专家，可以管理所有 Windows 7 计算机目录，并可以交付 Windows 7 应用程序、桌面和计算机，无论它们属于哪个部门范围。管理员曾考虑将 Peter 设置为 Win7 范围的完全管理员。但是，她决定不这样做，因为完全管理员还对所有未限定范围的对象（例如“站点”和“管理员”）拥有完全权限。

如何使用委派管理

通常，管理员的数量及其权限的粒度取决于部署的规模和复杂性。

- 在小型或概念验证部署中，一两个管理员负责所有事务。没有委派。在这种情况下，使用内置的完全管理员角色（具有“所有”范围）创建每个管理员。
- 在具有更多计算机、应用程序和桌面的大型部署中，需要更多的委派。多个管理员可能具有更具体的功能职责（角色）。例如，其中两名是完全管理员，其他是技术支持管理员。此外，管理员可能只管理特定对象组（范围），例如计算机目录。在这种情况下，创建新范围，并创建具有内置角色之一和相应范围的管理员。
- 更大的部署可能需要更多（或更具体）的范围，以及具有非常规角色的不同管理员。在这种情况下，编辑或创建更多范围，创建自定义角色，并使用内置或自定义角色以及现有和新范围创建每个管理员。

为了灵活性和易于配置，您可以在创建管理员时创建范围。您还可以在创建或编辑计算机目录或连接时指定范围。

创建和管理管理员

当您以本地管理员身份创建站点时，您的用户帐户会自动成为完全管理员，对所有对象拥有完全权限。站点创建后，本地管理员没有特殊权限。

完全管理员角色始终具有所有范围；您无法更改此设置。

默认情况下，管理员处于启用状态。如果您现在正在创建管理员，但该人员稍后才会开始管理职责，则可能需要禁用该管理员。对于现有已启用的管理员，您可能希望在重新组织对象/范围时禁用其中几个，然后在准备好使用更新的配置上线时重新启用它们。如果禁用完全管理员会导致没有已启用的完全管理员，则无法禁用该完全管理员。在创建、复制或编辑管理员时，可以使用启用/禁用复选框。

在复制、编辑或删除管理员时，如果您删除角色/范围对，它只会删除该管理员的角色与范围之间的关系。它不会删除角色或范围。它也不会影响配置了该角色/范围对的任何其他管理员。

要创建和管理管理员，请按照以下步骤操作：

1. 登录到 Web Studio，在左侧窗格中单击**管理员**，然后单击**管理员**选项卡。
2. 按照您要完成的任务的说明进行操作：

   - **创建管理员：** 在操作栏中单击**创建管理员**。键入或浏览到用户帐户名，选择或创建范围，然后选择角色。新管理员默认处于启用状态；您可以更改此设置。
   - **复制管理员：** 选择管理员，然后在操作栏中单击**复制管理员**。键入或浏览到用户帐户名。您可以选择并编辑或删除任何角色/范围对，并添加新的角色/范围对。新管理员默认处于启用状态；您可以更改此设置。
   - **编辑管理员：** 选择管理员，然后在操作栏中单击**编辑管理员**。您可以编辑或删除任何角色/范围对，并添加新的角色/范围对。
   - **删除管理员：** 选择管理员，然后在操作栏中单击**删除管理员**。如果删除完全管理员会导致没有已启用的完全管理员，则无法删除该完全管理员。

上方窗格显示您创建的管理员。选择一个管理员可在下方窗格中查看其详细信息。**警告**列指示与管理员关联的角色和范围对是否包含不可用的角色或范围。如果关联的角色和范围对包含不可用的角色或范围，则会出现以下警告消息：

- 关联的角色或范围不可用

> **重要提示：**
>
> 仅当关联的角色和范围对包含不可用的角色、不可用的范围或两者都包含时，才会出现警告消息。
>
> 要从管理员中删除角色和范围对，请完成以下步骤之一：

- 删除角色和范围对。

  a. 在操作栏中，点击 **编辑管理员**。

  b. 在 **管理员名称和详细信息** 窗口中，选择角色和范围对，然后点击 **删除**。

  c. 点击 **保存** 退出。

- 删除管理员。

  a. 在操作栏中，点击 **删除管理员**。

  b. 在确认窗口中，点击 **删除**。

创建和管理角色

管理员创建或编辑角色时，只能启用其自身拥有的权限。这可以防止管理员创建权限高于其当前权限的角色，然后将其分配给自己（或编辑已分配给他们的角色）。

角色名称最多可包含 64 个 Unicode 字符；不能包含：反斜杠、正斜杠、分号、冒号、井号、逗号、星号、问号、等号、左箭头或右箭头、管道符、左方括号或右方括号、左括号或右括号、引号或撇号。描述最多可包含 256 个 Unicode 字符。

您无法编辑或删除内置角色。如果任何管理员正在使用自定义角色，则无法删除该角色。

> **注意：**
>
> 只有某些产品版本支持自定义角色。只有支持自定义角色的版本才会在操作栏中显示相关条目。

要创建和管理角色，请执行以下步骤：

1. 登录 Web Studio，在左侧窗格中点击 **管理员**，然后点击 **角色** 选项卡。
2. 按照说明完成您要执行的任务：
   - **查看角色详细信息：** 选择角色。下部窗格列出了该对象的类型以及与该角色关联的权限。点击下部窗格中的 **管理员** 选项卡以查看当前拥有此角色的管理员列表。
   - **创建自定义角色：** 在操作窗格中单击**创建角色**。输入名称和描述。选择对象类型和权限。
   - **复制角色：** 选择角色，然后在操作栏中单击**复制角色**。根据需要更改名称、描述、对象类型和权限。
   - **编辑自定义角色：** 选择角色，然后在操作栏中单击**编辑角色**。根据需要更改名称、描述、对象类型和权限。
   - **删除自定义角色：** 选择角色，然后在操作栏中单击**删除角色**。出现提示时，确认删除。

创建和管理范围

创建站点时，唯一可用的作用域是“所有”作用域，该作用域无法删除。

您可以使用以下过程创建作用域。您还可以在创建管理员时创建作用域；每个管理员必须至少与一个角色和作用域对关联。创建或编辑桌面、计算机目录、应用程序或主机时，您可以将其添加到现有作用域。如果不将其添加到作用域，它们将保留在“所有”作用域中。

站点创建无法限定作用域，也不能是委派管理对象（作用域和角色）。但是，无法限定作用域的对象包含在“所有”作用域中。（完全管理员始终拥有“所有”作用域。）计算机、电源操作、桌面和会话未直接限定作用域。管理员可以通过关联的计算机目录或交付组获得对这些对象的权限。

创建和管理作用域的规则：

- 作用域名称最多可包含 64 个 Unicode 字符。作用域名称不能包含：反斜杠、正斜杠、分号、冒号、井号、逗号、星号、问号、等号、左箭头、右箭头、管道符、左方括号或右方括号、左括号或右括号、引号或撇号。
- 作用域描述最多可包含 256 个 Unicode 字符。
- 复制或编辑作用域时，请记住，从作用域中删除对象可能会导致管理员无法访问这些对象。如果编辑后的作用域与一个或多个角色配对，请确保作用域更新不会导致任何角色/作用域对无法使用。

要创建和管理作用域，请执行以下步骤：

1. 登录 Web Studio，在左侧窗格中单击**管理员**，然后单击**作用域**选项卡。
2. 按照您要完成的任务的说明进行操作：
    - **创建作用域：** 在操作栏中单击**创建新作用域**。输入名称和描述。要包含特定类型的所有对象（例如，交付组），请选择对象类型。要包含特定对象，请展开类型，然后选择单个对象（例如，销售团队使用的交付组）。
    - **复制范围：** 选择范围，然后在操作栏中单击**复制范围**。输入名称和描述。根据需要更改对象类型和对象。
    - **编辑范围：** 选择范围，然后在操作栏中单击**编辑范围**。根据需要更改名称、描述、对象类型和对象。
    - **删除范围：** 选择范围，然后在操作栏中单击**删除范围**。出现提示时，确认删除。

设置租户管理

设置租户管理可在单个 Citrix Virtual Apps and Desktops™ 站点中创建管理分区。每个租户都有独立的资源和配置，例如计算机目录和交付组。有权访问特定租户的管理员只能管理与该租户关联的资源和配置。示例用例包括在单个站点中拥有不同业务孤岛（独立部门或单独的 IT 管理团队）的公司。

从宏观层面来看，设置租户管理的工作流程包括：

1. 创建租户
2. 为租户添加管理员

创建租户

通过创建租户范围来创建租户。详细步骤如下：

1. 登录 Web Studio，在左侧窗格中单击**管理员**，然后单击**范围**选项卡。
2. 单击*创建范围**以开始创建租户。
3. 输入租户范围的以下详细信息：
    a. 为范围键入一个描述性名称。此名称也用作租户的标识符。
    b. （可选）输入简要描述。
    c. 选择**租户范围**。
    d. 如有必要，选择与租户关联的对象。您还可以在创建或管理对象时将对象添加到租户范围。
    e. 单击**确定**以完成创建。

完成后，您可以看到：

- 新的租户范围记录将显示在“范围”列表中，在**类型**列中标识为**租户**。
- 范围名称显示在**所有租户**下拉列表中，该列表位于 Web Studio 的右上角。

使用租户范围时，请记住以下注意事项：

- 租户属性遵循分层分配顺序：Hosting > Machine Catalogs > Delivery Groups > Applications。较低级别的对象从较高级别的对象继承租户属性。例如，为租户范围选择交付组时，请确保同时选择关联的托管和计算机目录。否则，交付组无法继承租户的属性。
- 创建租户范围后，您可以通过修改对象来编辑租户分配。当租户分配发生更改时，它仍然受限于必须分配给相同租户或这些租户的子集的约束。但是，当租户分配更改时，较低级别的对象不会重新评估。更改租户分配时，请确保对象受到适当的限制。例如，如果计算机目录可用于 `TenantA` 和 `TenantB`，则可以为 `TenantA` 创建一个交付组，并为 `TenantB` 创建一个交付组。（`TenantA` 和 `TenantB` 都与该计算机目录关联。）然后，您可以将计算机目录更改为仅与 `TenantA` 关联。因此，与 `TenantB` 关联的交付组将变为无效。

添加租户管理员

通过分配具有管理员角色和租户的用户帐户来添加租户管理员。

要添加租户管理员，请按照以下步骤操作：

1. 登录 Web Studio，在左侧窗格中单击**管理员**，然后单击**管理员**选项卡。
2. 单击**添加管理员**，并按照以下步骤完成：
    a. 键入或浏览到用户帐户名称，然后单击**下一步**。

b. 选择 **自定义访问**，然后根据需要选择一个或多个角色（例如，计算机目录管理员）。

c. 单击每个角色旁边的 **编辑范围**，将范围从 **所有** 更改为所需的租户范围，然后单击 **保存**。

3. 单击**下一步**。
4. 在 **查看和确认** 页面上，单击 **发送邀请**。

创建报告

您可以创建两种类型的委派管理报告：

- 一份 HTML 报告，其中列出了与管理员关联的角色/范围对，以及每种对象类型（例如，交付组和计算机目录）的单独权限。您可以从 Web Studio 生成此报告。

  要创建此报告，请按照以下步骤操作：

  a. 登录 Web Studio，在左侧窗格中单击 **管理员**

  b. 选择一个管理员，然后在操作栏中单击 **创建报告**。

  您也可以在创建、复制或编辑管理员时请求此报告。

- 一份 HTML 或 CSV 报告，将所有内置和自定义角色映射到权限。您可以通过运行名为 OutputPermissionMapping.ps1 的 PowerShell 脚本来生成此报告。

  要运行此脚本，您必须是完全管理员、只读管理员或具有读取角色权限的自定义管理员。该脚本位于：Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts。

  语法：

  `OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]`

参数	描述
`-Help`	显示脚本帮助。
`-Csv`	指定 CSV 输出。默认值 = HTML
`-Path string`	输出写入位置。默认值 = stdout
`-AdminAddress string`	要连接的 Delivery Controller™ 的 IP 地址或主机名。默认值 = localhost

参数	描述
`-Show`	（仅当也指定了 `-Path` 参数时有效）当您将输出写入文件时，`-Show` 会导致输出在适当的程序（例如 Web 浏览器）中打开。
通用参数	`Verbose`、`Debug`、`ErrorAction`、`ErrorVariable`、`WarningAction`、`WarningVariable`、`OutBuffer` 和 `OutVariable`。有关详细信息，请参阅 Microsoft 文档。

以下示例将 HTML 表写入名为 Roles.html 的文件，并在 Web 浏览器中打开该表。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

-Path Roles.html –Show
```

以下示例将 CSV 表写入名为 Roles.csv 的文件。该表不显示。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

–CSV -Path Roles.csv
```

在 Windows 命令提示符下，前面的示例命令是：

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'

-CSV -Path Roles.csv"
```

交付控制器

注意：

> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

> Delivery Controller 是服务器端组件，负责管理用户访问、代理和优化连接。Controller 还提供用于创建桌面和服务器映像的 Machine Creation Services™。

一个站点必须至少有一个 Controller。安装初始 Controller 后，您可以在创建站点时或之后添加更多 Controller。在一个站点中拥有多个 Controller 有两个主要好处。

- **冗余：** 最佳做法是，在生产站点中，始终在不同的物理服务器上至少部署两个 Controller。如果一个 Controller 出现故障，其他 Controller 可以管理连接并管理站点。
- **可扩展性：** 随着站点活动的增长，Controller 上的 CPU 利用率和数据库活动也会随之增长。额外的 Controller 使您能够处理更多用户以及更多应用程序和桌面请求，并可以提高整体响应能力。

每个 Controller 都直接与站点数据库通信。在具有多个区域的站点中，每个区域中的 Controller 都与主区域中的站点数据库通信。

> **重要提示：**
>
> 站点配置完成后，请勿更改 Controller 的计算机名称或域成员身份。

VDA 如何向 Controller 注册

VDA 必须先向站点中的 Delivery Controller 注册（建立通信），然后才能使用。有关 VDA 注册的信息，请参阅VDA 向 Controller 注册。

添加、删除或移动 Controller

要添加、删除或移动 Controller，您必须拥有 数据库 一文中列出的服务器角色和数据库角色权限。

不支持在 SQL 群集或 SQL 镜像安装中的节点上安装 Controller。

将 Delivery Controller™ 添加到站点时，请务必将该计算机的登录凭据添加到用于高可用性的任何副本 SQL Server。

如果您的部署使用数据库镜像：

- 在添加、删除或移动 Controller 之前，请确保主体数据库和镜像数据库均正在运行。此外，如果您将脚本与 SQL Server Management Studio 结合使用，请在运行脚本之前启用 SQLCMD 模式。
- 要在添加、删除或移动 Controller 后验证镜像，请运行 PowerShell `Get-configdbconnection` cmdlet。该 cmdlet 可确保在连接字符串中已将故障转移伙伴设置为镜像。

添加、删除或移动控制器后：

- 如果启用了自动更新，VDA 将在 90 分钟内收到更新的控制器列表。
- 如果未启用自动更新，请确保为所有 VDA 更新了控制器策略设置或 ListOfDDCs 注册表项。将控制器移动到另一个站点后，请在这两个站点上更新策略设置或注册表项。

添加控制器

您可以在创建站点时以及之后添加控制器。您不能将使用此软件的早期版本安装的控制器添加到使用此版本创建的站点。

1. 在包含受支持操作系统的服务器上运行安装程序。安装 Delivery Controller 组件以及您想要的任何其他核心组件。完成安装向导。
2. 如果您尚未创建站点，请在此控制器上运行 Citrix Site Manager 以创建站点。此控制器的 IP 地址将自动添加到新站点。

   如果您计划生成初始化数据库的脚本，请在生成脚本之前添加控制器。
3. 如果您已创建站点，请执行以下步骤：

   a. 在此控制器上运行 Citrix Site Manager，单击 **Join an existing site**，然后键入要加入的站点中控制器的地址。

   b. 运行 Studio configuration tool 将控制器添加到 Web Studio。

删除控制器

从站点中删除控制器不会卸载 Citrix 软件或任何其他组件。此操作会从数据库中删除控制器，使其无法再用于代理连接和执行其他任务。如果您删除控制器，以后可以将其重新添加到同一站点或另一个站点。一个站点至少需要一个控制器，因此您不能删除 Web Studio 中列出的最后一个控制器。

从站点中删除控制器时，不会删除控制器登录到数据库服务器的凭据。这可以避免意外删除同一计算机上其他产品服务使用的登录凭据。如果不再需要，必须手动删除登录凭据。删除登录凭据需要 `securityadmin` 服务器角色权限。

删除控制器后：

- 使用自动更新的 VDA 会重新注册到其他可用的控制器。仅当启用了自动更新机制并且 VDA 可以访问其他控制器（在与已删除控制器相同的辅助区域中，或在本地部署的主区域中）时，才会发生此重新注册。
- 更新 Citrix StoreFront 中的控制器信息。有关详细信息，请参阅管理控制器。
- 在 Citrix StoreFront 中，更新通过 Citrix Gateway 进行远程访问的安全票证颁发机构 (STA) URL。有关详细信息，请参阅管理安全票证颁发机构。
- 在 Citrix Gateway 中，更新任何虚拟服务器 STA URL。有关详细信息，请参阅Citrix Gateway。

> **重要提示：**
>
> 在从站点中删除控制器之前，请勿从 Active Directory 中删除该控制器。

1. 确保控制器已开机，以便 Web Studio 可以加载并显示您要删除的控制器。
2. 在 Web Studio 完全加载控制器后，验证控制器上的所有服务是否正在运行，并且控制器保持开机状态。
3. 登录 Web Studio，在左侧窗格中选择**设置**。
4. 找到**交付控制器**磁贴，然后单击**编辑**。
5. 在**管理交付控制器**页面上，选择要删除的控制器。
6. 选择**删除控制器**。如果您没有正确的数据库角色和权限，系统会提供生成脚本的选项，该脚本允许您的数据库管理员为您删除控制器。

   Web Studio 在删除控制器之前会执行预检查。如果控制器已关机且不处于以下服务状态，则可以安全删除：

   - 未知
   - 待定故障
   - 旧版本
   - 新版本
   - 版本更改正在进行中
   - 缺少强制功能

   如果 Controller 未关闭电源且处于上述任何服务状态，Web Studio 会提示您关闭 Controller 的电源。

7. 您必须从数据库服务器中删除 Controller 的计算机帐户。删除之前，请检查其他服务是否正在使用该帐户。

使用 Web Studio 删除 Controller 后，流向该 Controller 的流量可能会在短时间内持续存在，以确保当前任务的正确完成。如果您想在短时间内强制删除 Controller，Citrix 建议您关闭安装该 Controller 的服务器，或从 Active Directory 中删除该服务器。然后，重新启动站点上的其他 Controller，以确保不再与已删除的 Controller 进行通信。

将 Controller 移动到其他区域

如果您的站点包含多个区域，您可以将 Controller 移动到不同的区域。有关此移动如何影响 VDA 注册和其他操作的信息，请参阅区域。

1. 在左侧窗格中选择 **Zone**（区域）。
2. 在中间窗格中选择一个区域，然后选择一个 Controller。
3. 在操作栏中选择 **Move Items**（移动项目）。
4. 在出现的 **Move Items**（移动项目）页面上，选择要将 Controller 移动到的区域。
5. 单击 **保存**。

将 VDA 移动到其他站点

如果 VDA 是使用 Citrix Provisioning™ 预配的或是一个现有映像，则可以在升级时或将测试站点中创建的 VDA 映像移动到生产站点时，将 VDA 移动到另一个站点（从站点 1 到站点 2）。使用 Machine Creation Services (MCS) 预配的 VDA 无法从一个站点移动到另一个站点。MCS 不支持更改 VDA 检查以向 Controller 注册的 ListOfDDCs。使用 MCS 预配的 VDA 始终检查与其创建所在站点关联的 ListOfDDCs。

有两种方法可以将 VDA 移动到另一个站点：使用安装程序或 Citrix 策略。

安装程序

运行安装程序并添加控制器，指定站点 2 中某个控制器的 FQDN（DNS 条目）。

仅当未使用“控制器”策略设置时，才在安装程序中指定控制器。

组策略编辑器

以下示例在站点之间移动多个 VDA。

1. 在站点 1 中创建包含以下设置的策略，然后将策略筛选到交付组级别，以启动站点之间的分阶段 VDA 迁移。
    - 控制器：包含站点 2 中一个或多个控制器的 FQDN（DNS 条目）。

- 启用控制器自动更新：设置为已禁用。

2. 交付组中的每个 VDA 都会在新策略发布后 90 分钟内收到警报。VDA 会忽略其收到的控制器列表（因为自动更新已禁用）；它会选择策略中指定的控制器之一，该策略列出了站点 2 中的控制器。
3. 当 VDA 成功向站点 2 中的控制器注册时，它会收到站点 2 的 ListOfDDCs 和策略信息，这些信息默认启用了自动更新。VDA 在站点 1 中注册的控制器不在站点 2 中的控制器发送的列表中。因此，VDA 会重新注册，从站点 2 列表中的控制器中进行选择。从那时起，VDA 会自动使用来自站点 2 的信息进行更新。

有关如何使用组策略编辑器的信息，请参阅 Citrix 策略 文档。

Web Studio 主页

Web Studio 主页概述了您的 Citrix Virtual Apps and Desktops™ 部署和工作负载，并提供了可帮助您充分利用订阅的信息。本文介绍了此页面上可用的小组件：

- 站点详细信息
- 资源
- 会话
- 最近
- 错误和警告
- 入门

您可以通过添加、删除或重新定位小组件来自定义此主页，以满足您的需求。

站点详细信息

此小组件可让您一目了然地了解 Citrix Virtual Apps and Desktops 站点。它显示了关键信息，例如您的许可证类型、Studio 版本以及 Delivery Controller 的版本和状态。

要诊断站点问题，请选择**测试站点**以运行数据库运行状况、连接性、委派管理、VDA 更新就绪情况、注册状态等检查。此操作在升级期间特别有用，有助于确保您的站点在部署前后都稳定且就绪。

资源

此小组件概述了您的 Citrix Virtual Apps and Desktops 部署：

- **资源**。显示已部署资源的数量及其按类别划分的计数。

资源	按类别查看计数
计算机	单击**计算机**，选择一个状态，然后将鼠标悬停在圆环图上以查看详细信息。可用选项包括：**可用性状态**（可用、使用中、关闭和不可用）、**注册状态**（已注册和未注册）以及**维护状态**（维护中和非维护中）。按可用性状态查看计算机计数时，可以单击某个状态以查看相应的计算机详细信息。
应用程序	单击**应用程序**并将鼠标悬停在圆环图上以查看详细信息。
交付组	单击**交付组**并将鼠标悬停在圆环图上以查看详细信息。
计算机目录	单击**计算机目录**并将鼠标悬停在圆环图上以查看详细信息。

- **过去 7 天启动的会话**。显示过去七天中每天启动的桌面和应用程序会话数。要深入了解更多详细信息，请单击转到 Director。

会话

此小组件概述了您过去 7 天的 Citrix Virtual Apps and Desktops 工作负载。显示过去七天中每天启动的桌面和应用程序会话数。

最近

此小组件显示您最近在 Web Studio 中访问过的对象的历史记录。它可帮助您快速查看对象访问历史记录。单击列表中的对象名称可直接转到该对象在其相应节点中的位置。

请记住以下几点：

- 该列表本地存储在您的浏览器缓存中。清除缓存、切换浏览器或使用隐身模式会重置该列表。
- 该列表仅限于您在过去 30 天内访问过的最后 100 个对象。
- 此列表仅记录单个对象的视图或操作。如果您一次选择*多个*对象，则它们*不*会记录在列表中。
- *不*跟踪以下对象：
  - **设置**、**许可**和**日志记录**节点中的对象。
  - **策略**节点中**比较**和**建模**选项卡中的对象。

- **备份和恢复**节点中**历史记录**和**设置**选项卡中的对象。

入门

此小组件将引导您完成一系列问题，以帮助您设置 Citrix Virtual Apps and Desktops 部署。通过回答这些问题，您可以快速配置部署。

错误和警告

集中显示部署中的错误和警告：

- 列出以下配置节点中存在的错误数量和警告数量：区域、计算机、计算机目录、交付组、托管和映像。单击数字可将您链接到相应节点的 UI。
- 列出站点中的高优先级错误以及建议的操作。

自定义主页

要自定义主页，请按照以下步骤操作：

1. 登录 Web Studio。

   此时将显示主页。
2. 单击主页右上角的 **Edit** 图标。
3. 要重新定位小组件，请将其拖动到所需位置。
4. 要从主页中删除小组件，请单击小组件右上角的 **Delete** 图标。
5. 要将小组件添加回主页，请单击主页右上角的 **Add widget** 图标。
6. 单击 **Done** 以保存更改。

IPv4/IPv6 支持

此版本支持纯 IPv4、纯 IPv6 以及使用重叠 IPv4 和 IPv6 网络的双栈部署。

以下组件仅支持 IPv4。所有其他组件均支持 IPv4 和 IPv6。

- XenServer®
- 不受**仅使用 IPv6 控制器注册**策略设置控制的虚拟投递代理 (VDA)

IPv6 通信通过两个与 VDA 连接相关的 Citrix® 策略设置进行控制。

- **强制使用 IPv6 的主要设置：**仅使用 IPv6 控制器注册。

  此策略设置控制 VDA 用于向 Delivery Controller 注册的地址形式。

启用后，VDA 将使用按以下优先级选择的单个 IPv6 地址向 Controller 注册并与之通信：全局 IP 地址、唯一本地地址 (ULA)、链路本地地址（仅当没有其他 IPv6 地址可用时）。

禁用后，VDA 将使用计算机的 IPv4 地址向 Controller 注册并与之通信。这是默认值。

如果团队频繁使用 IPv6 网络，请根据已启用**仅使用 IPv6 控制器注册**策略设置的映像或组织单位 (OU) 为这些用户发布桌面和应用程序。

如果团队频繁使用 IPv4 网络，请根据已禁用**仅使用 IPv6 控制器注册**策略设置的映像或 OU 为这些用户发布桌面和应用程序。

- **定义 IPv6 网络掩码的从属设置：**控制器注册 IPv6 网络掩码。

  一台计算机可以有多个 IPv6 地址。此策略设置允许管理员将 VDA 限制为仅使用首选子网（如果已注册），而不是全局 IP。此设置指定 VDA 注册的网络。VDA 仅注册与指定网络掩码匹配的第一个地址。

  此设置仅在启用**仅使用 IPv6 控制器注册策略**设置时有效。默认值 = 空字符串

部署注意事项

如果您的环境包含 IPv4 和 IPv6 网络，请为仅限 IPv4 的客户端和可以访问 IPv6 网络的客户端创建单独的交付组配置。可以考虑使用命名、手动 Active Directory 组分配或 SmartAccess 筛选器来区分用户。 如果连接在 IPv6 网络上启动，然后您尝试从仅具有 IPv4 访问权限的客户端再次连接，则会话重新连接可能会失败。

注意：如果您已启用DNS 解析已启用，则这些注意事项不适用。

使用 Web Studio 为 思杰虚拟应用和桌面™ 许可

> **注意：**

> - 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 唯一的管理控制台。Citrix Studio（基于 MMC）已从安装程序中移除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。
> - 许可证激活服务 (LAS) 是一种新的基于云的许可解决方案，它提供了传统 Citrix® 旧版许可的替代方案。LAS 引入了新的激活模块，确保了无缝且现代的许可证管理方法。有关更多信息，请参阅 许可证激活服务。

> 在 Web Studio 中，如果许可证服务器与 Web Studio 位于同一域或受信任域中，您可以管理和跟踪许可。有关许可任务的信息，请参阅 许可文档 和 多类型许可。

下表列出了支持的版本和许可模型：

产品	版本	许可模型
思杰虚拟应用	高级版、增强版、标准版	并发
思杰虚拟桌面	高级版、增强版、标准版	用户/设备和并发

有关更多信息，请参阅 并发许可证 和 用户/设备许可证。

支持的当前版本 (CR) 和长期服务版本 (LTSR)

Citrix 强烈建议您始终使用 (/zh-cn/licensing/current-release.html)，以受益于其中可能包含的任何功能或安全改进。

> **注意：**
>
> License Server VPX 已弃用，将不再接收任何维护或安全修复。建议使用 11.16.6 或更早版本 License Server VPX 的客户尽快迁移到 (/zh-cn/licensing/current-release.html)。

> 有关 Citrix 产品生命周期日期的更多信息，请参阅产品矩阵。

有关旧版产品和产品版本的信息，请参阅旧版产品矩阵。

您必须是完整的许可证管理员才能完成以下任务。要在 Web Studio 中查看许可证信息，管理员必须至少具有“读取许可”委派管理权限。内置的“完全管理员”和“只读管理员”角色具有该权限。

使用 Web Studio 从 Citrix 下载并安装许可证

1. 登录 Web Studio 并在左侧窗格中选择 **Licensing**。
2. 在操作栏中选择 **Allocate Licenses**。
3. 输入许可证访问代码。您在购买或续订许可证后会收到 Citrix 发送的电子邮件。
4. 选择一个产品并选择 **Allocate Licenses**。该产品可用的许可证将被分配和下载。为特定许可证访问代码分配并下载所有许可证后，您不能重复使用该许可证访问代码。要使用同一代码进行其他交易，请登录“我的帐户”。

添加存储在本地计算机或网络上的许可证

1. 登录 Web Studio 并在左侧窗格中选择 **Licensing**。
2. 在操作栏中选择 **Add Licenses**。
3. 浏览到许可证文件并将其添加到许可证服务器。

更改许可证服务器

1. 登录 Web Studio 并在左侧窗格中选择 **Licensing**。
2. 在操作栏中选择 **Change License Server**。
3. 以 *name:port* 形式键入许可证服务器地址，其中 name 是 DNS、NetBIOS 或 IP 地址。如果未指定端口号，则使用默认端口 (27000)。

选择要使用的许可证类型

- 配置站点时，指定许可证服务器后，系统会提示您选择要使用的许可证类型。如果服务器上没有许可证，则会自动选择在没有许可证的情况下使用产品 30 天试用期的选项。
- 如果服务器上有许可证，则会显示其详细信息，您可以选择其中一个。或者，您可以将许可证文件添加到服务器，然后选择该文件。

更改产品版本和许可模式

1. 登录 Web Studio 并在左侧窗格中选择 **Licensing**。
2. 在操作栏中选择 **Edit Product Edition**。
3. 更新相应的选项。

要访问许可证管理控制台，请在操作栏中选择 **License Administration Console**。控制台会立即显示，或者如果仪表板配置为受密码保护，则会提示您输入许可证管理控制台凭据。有关如何使用控制台的详细信息，请参阅许可文档。

> **注意：**
>
> 在 Web Studio 中切换许可证时，更改最多需要 5 分钟才能显示在 Citrix Director 中。例如，如果您在 Advanced 和 Premium 之间切换。

添加许可管理员

1. 登录 Web Studio 并在左侧窗格中选择 **Licensing**。

2. 选择**许可管理员**选项卡。
3. 在操作栏中选择**添加许可管理员**。
4. 浏览到要添加为管理员的用户并选择权限。

更改许可管理员的权限或删除许可管理员

1. 登录到 Web Studio 并在左侧窗格中选择**许可**。
2. 选择**许可管理员**选项卡，然后选择管理员。
3. 在操作栏中选择**编辑许可管理员**或**删除许可管理员**。

添加许可管理员组

1. 登录到 Web Studio 并在左侧窗格中选择**许可**。
2. 选择**许可管理员**选项卡。
3. 在操作栏中选择**添加许可管理员组**。
4. 浏览到要用作许可管理员的组并选择权限。添加 Active Directory 组会向该组中的用户授予许可管理员权限。

更改许可管理员组的权限或删除许可管理员组

1. 登录到 Web Studio 并在左侧窗格中选择**许可**。
2. 选择**许可管理员**选项卡，然后选择管理员组。
3. 在操作栏中选择**编辑许可管理员组**或**删除许可管理员组**。

查看许可证信息

登录 Web Studio 并在左侧窗格中选择**许可**。将显示站点的许可证使用情况和设置摘要，以及指定许可证服务器上当前安装的所有许可证的列表。

确保站点的许可设置（包括产品类型、许可证版本和许可模型）与您配置的许可证服务器使用的许可证匹配。如果不匹配，您可能需要下载或分配现有许可证以匹配站点的许可证设置。

运行命令 `Get-Brokersite` 以获取以下许可信息：

- TotalUniqueLicenseUsers
- PeakConcurrentLicenseUsers
- PeakConcurrentLicensedDevice

注意：

使用云许可 API 获取 Citrix DaaS 中的信息。有关云许可 API 的信息，请参阅管理 Citrix Cloud 许可的 API。

查看许可证过期警报

Web Studio 从 Citrix 许可证服务器查询许可证文件过期日期。如果许可证文件即将过期或已过期，Web Studio 会在“概览”选项卡上向管理员发出警报。

相关链接

- 请参阅Citrix 针对年度和基于期限的零售许可证的本地订阅。
- 请参阅具有混合权利的过渡和升级 (TTU)。

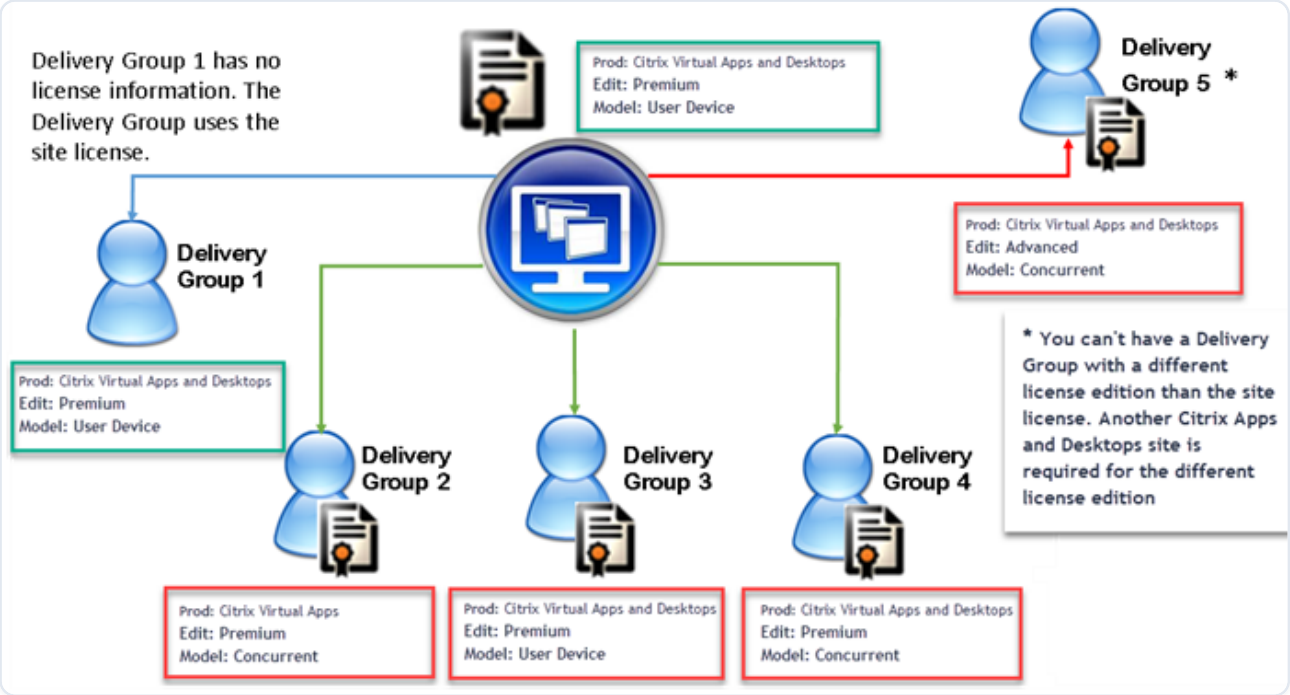
多类型许可

注意：

- License Activation Service 不支持多类型许可。
- 交付组级别的许可证覆盖已弃用。Citrix Virtual Apps and Desktops 现在仅使用站点级许可证设置。

多类型许可支持在单个 Citrix Virtual Apps and Desktops 站点上为交付组使用不同许可证类型。**类型**是产品 ID (XDT 或 MPS) 和模型 (UserDevice 或 Concurrent) 的单一组合。交付组必须使用与站点级别配置的相同产品版本 (PLT/Premium 或 ENT/Advanced)。在为您的 Citrix Virtual Apps and Desktops 部署配置多类型许可时，请注意本文末尾的特殊注意事项。

如果未配置多类型许可，则只有在为单独站点配置时才能使用不同许可证类型。交付组使用站点许可证。有关配置多类型许可时的重要通知限制，请参阅特殊注意事项。



要确定使用不同类型许可证的交付组，请使用以下 Broker PowerShell cmdlet：

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

要安装许可证，请使用：

- 思杰工作室
- 思杰许可管理器
- citrix.com

客户成功服务日期特定于每个许可证文件以及每个产品和模型。设置不同的交付组可能彼此具有不同的客户成功服务日期。

特殊注意事项

多类型许可具有不同于常规 Citrix Virtual Apps and Desktops™ 许可的功能。

对于配置为使用与站点配置不同类型的交付组，Director 或 Studio 不会发出警报和通知：

- 当接近许可限制或许可突发模式的触发或到期时，没有信息。
- 当特定组出现问题时，没有通知。

配置为多类型许可的交付组仅使用该许可类型，并且在完全使用后不会回退到站点配置。

尽管 Citrix Virtual Apps Standard 和 Citrix Virtual Desktops™ Standard 许可版本名称都表明它们是 Standard，但它们并非同一版本。多类型许可不适用于 Citrix Virtual Apps Standard 和 Citrix Virtual Desktop Standard 许可。

许可兼容性矩阵

此表详细说明了旧产品名称、新产品名称以及相关的特性名称。四个兼容性列指定了哪些产品和许可模型组合与多类型许可兼容。CCU 和 CCS 代表并发许可，UD 代表用户/设备许可。



代理 PowerShell SDK

DesktopGroup 对象具有这两个属性，您可以使用关联的 New-BrokerDesktopGroup 和 Set-BrokerDesktopGroup cmdlet 进行操作。

名称	值	限制
LicenseModel	一个参数（并发或用户设备），用于指定组的许可模型。如果未指定，则使用站点范围的许可模型。	如果功能开关被禁用，尝试设置属性将失败。
ProductCode	一个文本字符串，XDT（适用于 Citrix Virtual Desktops）或 MPS（适用于 Citrix Virtual Apps™），用于指定该组的许可产品 ID。如果未指定，则使用站点范围的产品代码。	如果功能开关被禁用，尝试设置属性将失败。

有关 LicenseModel 和 ProductCode 的更多信息，请参阅 about_Broker_Licensing。

New-BrokerDesktopGroup

创建桌面组以管理桌面组的代理。有关此 cmdlet 的更多信息，请参阅 `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>`。

Set-BrokerDesktopGroup

禁用或启用现有代理桌面组或更改其设置。有关此 cmdlet 的更多信息，请参阅 `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`

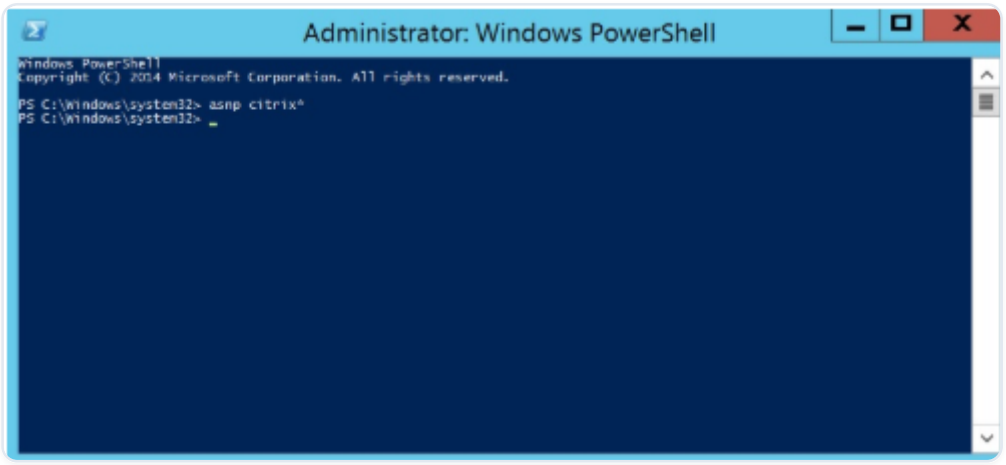
Get-BrokerDesktopGroup

检索符合指定条件的桌面组。Get-BrokerDesktopGroup cmdlet 的输出包括组的 **ProductCode** 和 **LicenseModel** 属性。如果尚未使用 New-BrokerDesktopGroup 或 Set-BrokerDesktopGroup 设置这些属性，则返回 null 值。如果为 null，则使用站点范围的许可模型和产品代码。有关此 cmdlet 的更多信息，请参阅 `<https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>`。

为每个交付组配置不同的许可产品和模型

> **注意：**
>
> 您不能在单个交付组上配置两种或更多不同类型的产品、版本或许可模型。如果您有不同类型的产品、版本或许可模型，请在单独的交付组中进行配置。

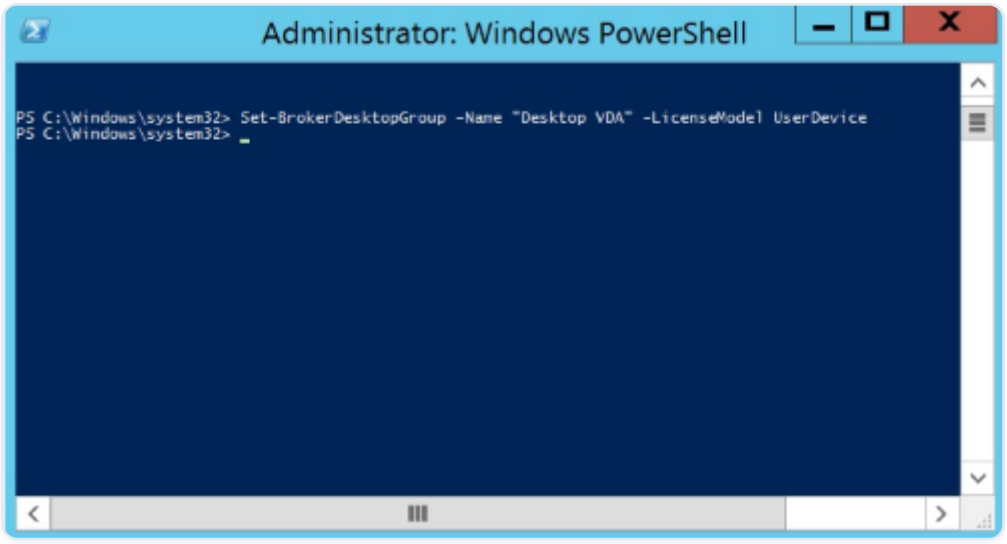
1. 以管理员权限打开 PowerShell 并添加 Citrix 管理单元。



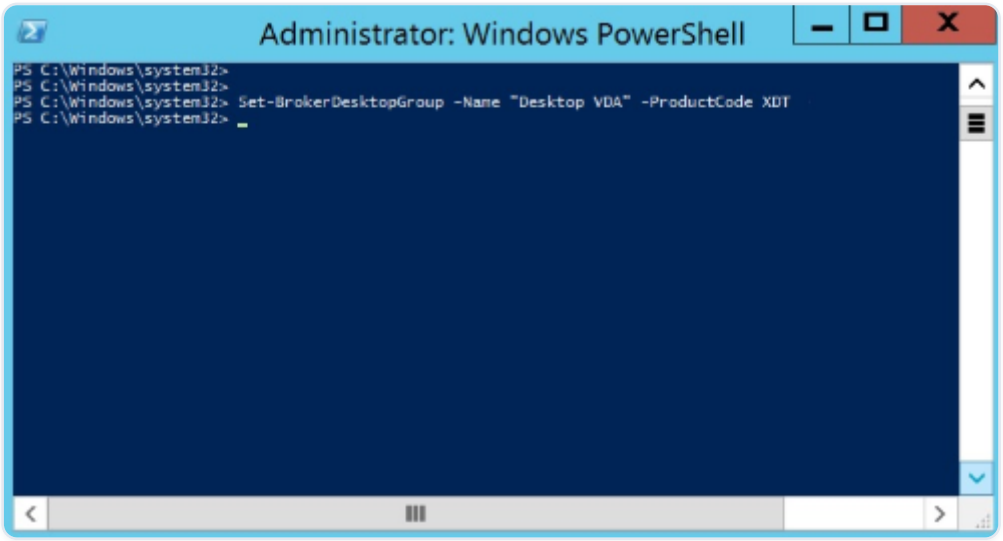
2. 运行命令 **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** 以查看当前许可证配置。查找参数 **LicenseModel** 和 **ProductCode**。如果您之前未配置这些参数，它们可能为空白。

> **注意：**
>
> 如果交付组未设置许可信息，则默认为 **站点级别站点许可证**。

3. 通过运行命令更改许可模型：**Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel**。

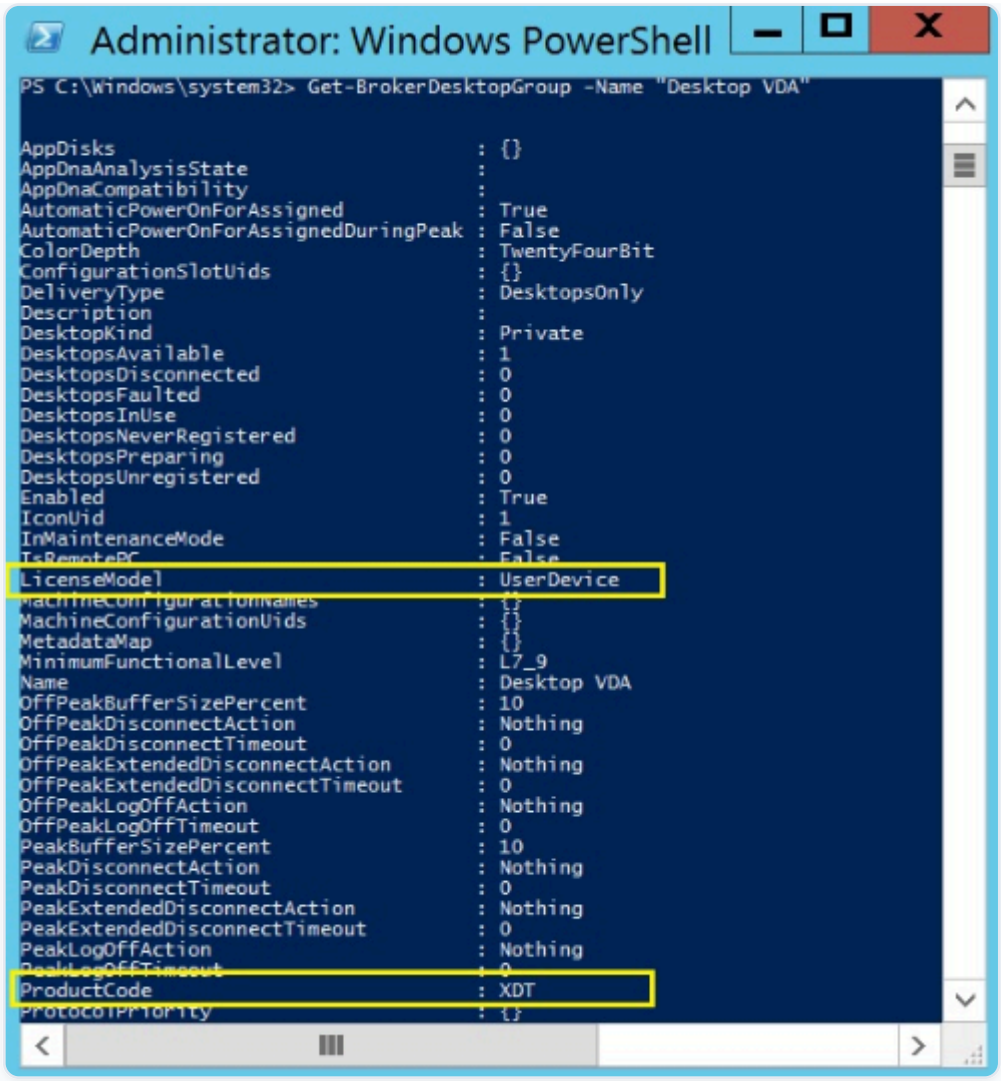


4. 通过运行以下命令更改许可证产品：**Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode**。



5. 输入命令 **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** 以验证更改。

> **注意：**
>
> 您不能在同一站点中混合搭配版本。例如，高级版和增强版许可证。如果您拥有不同版本的许可证，则需要多个站点。



6. 通过运行与前面步骤中描述的相同的 **Set-BrokerDesktopGroup** 命令，并将其值设置为 **$null**，来删除许可证配置。

> **注意：**
>
> Studio 不显示每个交付组的许可证配置。使用 PowerShell 查看当前配置。

示例

此 PowerShell cmdlet 示例说明了如何为两个现有交付组设置多类型许可，以及如何创建和设置第三个交付组。

要查看与交付组关联的许可证产品和许可证模型，请使用 **Get-BrokerDesktopGroup** PowerShell cmdlet。

1. 我们将第一个交付组设置为 XenApp® 和并发。

   Set-BrokerDesktopGroup -Name "适用于 Citrix Virtual Apps Premium 并发版的交付组" -ProductCode MPS -LicenseModel Concurrent

2. 我们将第二个交付组设置为 XenDesktop® 和并发。

   Set-BrokerDesktopGroup -Name "适用于 Citrix Virtual Desktops Premium 并发版的交付组" -ProductCode XDT -LicenseModel Concurrent

3. 我们创建并设置第三个交付组，用于 XenDesktop 和用户设备。

   New-BrokerDesktopGroup -Name "Citrix Virtual Desktops Premium UserDevice 的交付组" -PublishedName "我的桌面" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

许可证激活服务

许可证激活服务 (LAS) 是一种新的基于云的许可解决方案，它提供了传统 Citrix® 旧版许可的替代方案。LAS 引入了新的激活模块，确保了无缝且现代的许可证管理方法。

LAS 简化了 Citrix 许可体验。不再需要生成、下载或安装许可证访问代码或文件到许可证服务器。您只需升级许可证服务器并向 Citrix Cloud 注册。兼容产品指向许可证服务器后，它们可以自动激活。

激活后，许可证服务器会定期与许可证激活服务通信，以保持其激活状态最新。LAS 采用云技术构建，提高了性能并确保没有停机时间。如果由于任何原因，许可证服务器或 LAS 无法访问，系统将进入许可证缓存模式，该模式旨在保护系统免于未授权并避免中断。有关详细信息，请参阅许可证缓存模式。

有关 LAS 的更多详细信息，请参阅许可文档许可证激活服务。

有关许可的常见问题解答，请参阅许可常见问题解答。

先决条件

- 安装或更新许可证服务器到版本 11.17.2 build 53100 或更高版本。
- 许可证服务器需要可靠且持续的 Internet 连接。

注意事项

- 在 Web Studio 提示激活之前，所有 Delivery Controller 都必须与 LAS 兼容。单个站点可以使用旧版许可证或 LAS。

- 您可以将多个许可证服务器注册到同一个 Citrix Cloud ID (CCID) 或 OrgID。但是，一个站点只能配置为指向一个许可证服务器。

限制

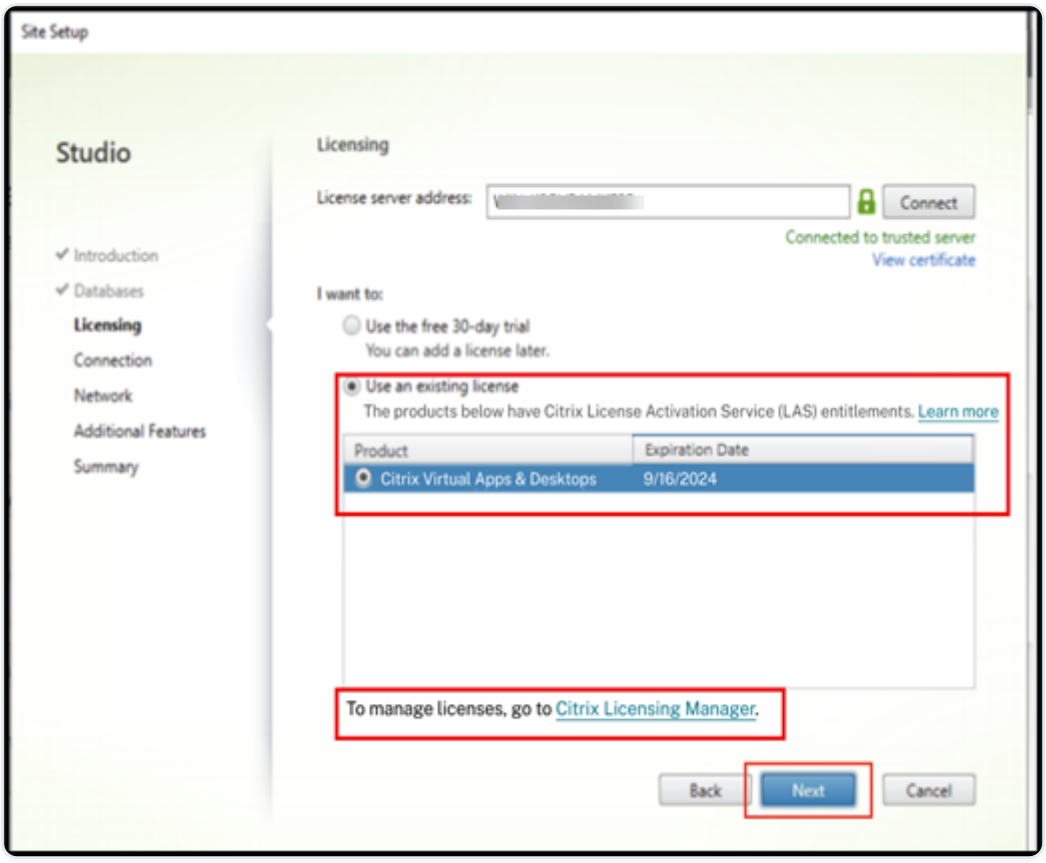
- 迁移到 LAS 会将产品版本设置为 **Premium**，并将许可证模型设置为 **Concurrent**，但这在将来可能会发生变化。请勿使用 PowerShell 修改许可证配置，因为这可能会影响注册和会话启动。
- 您只能使用 Web Studio 将 Citrix Virtual Apps and Desktops™ 站点从现有旧版许可证迁移到 LAS。

主要步骤

1. 安装或升级许可证服务器到版本 11.17.2 build 53100 或更高版本，并按照如何为许可证激活服务配置许可证服务器中提到的说明配置 LAS。
2. 安装 Citrix Virtual Apps and Desktops™ 2411 或更高版本。安装核心组件，例如 Citrix Delivery Controller、Citrix Studio、Web Studio 和 Citrix Director。

   > **注意：**
   >
   > Citrix Virtual Apps and Desktops 站点中的所有 Delivery Controller 都必须与 LAS 兼容。

3. 安装所需组件后，使用 Citrix Site Manager 创建站点。有关创建站点的信息，请参阅创建站点。如果许可证服务器配置为使用 LAS，则 Metainstaller 会显示授权。授权会随其相应的许可证到期日期一起提供。



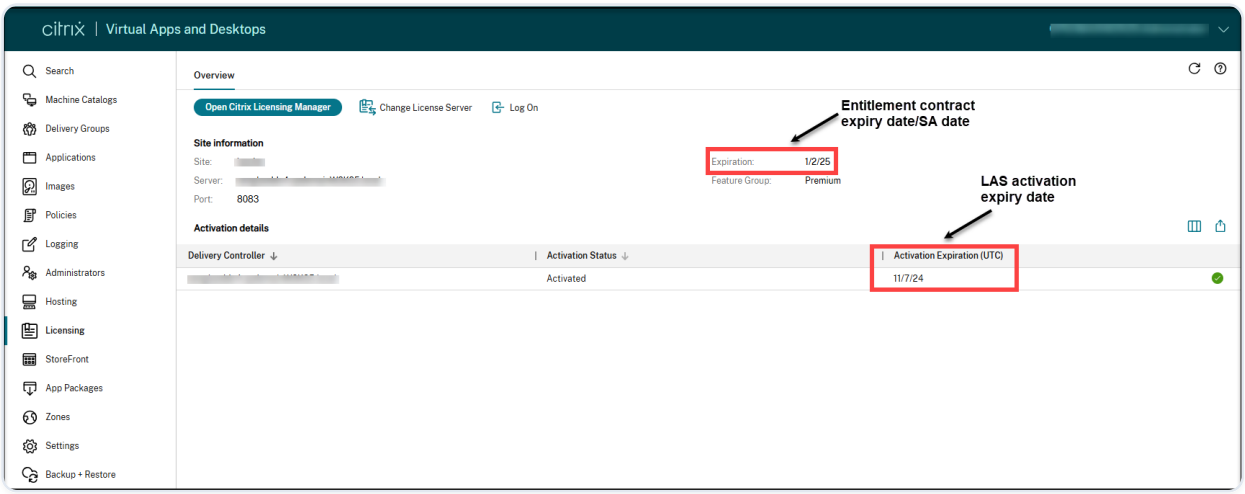
> **注意：**
>
> 如果许可证服务器未升级到最新许可证服务器版本，您会收到错误消息。

4. 检查许可详细信息。
5. 将旧版许可迁移到 LAS。

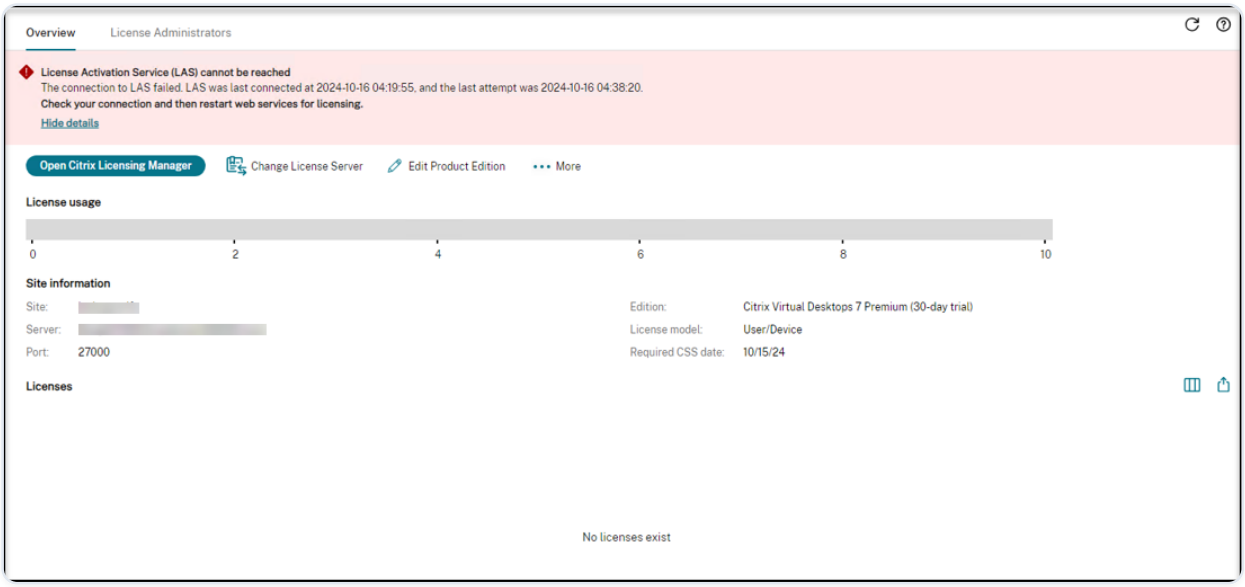
检查许可详细信息

创建站点后，使用 Web Studio 检查许可详细信息。

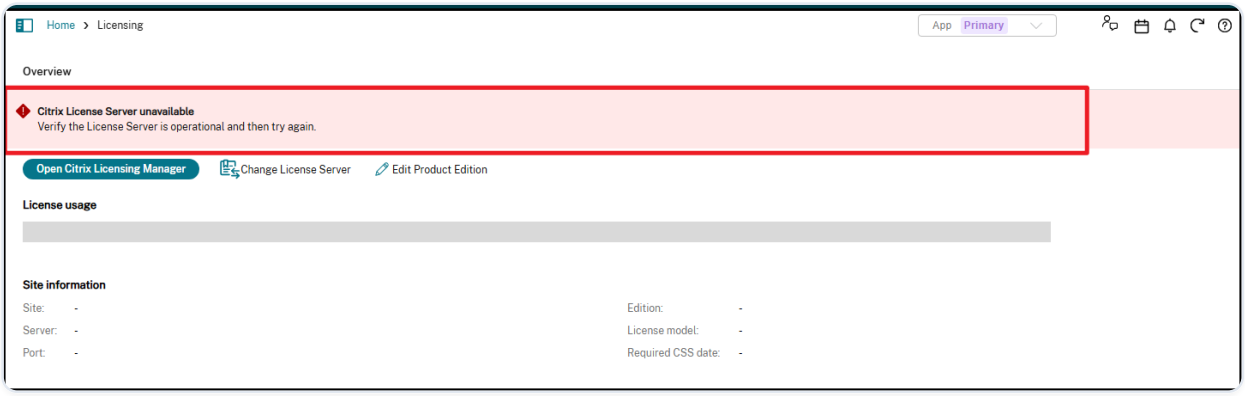
1. 在 Web Studio 中，选择**许可**节点。
2. 在**概述**选项卡上，检查 Citrix Virtual Apps and Desktops 站点是否具有相应的许可证，或者在使用 LAS 功能时许可证是否已过期。



如果 LAS 无法访问，您可能会看到错误消息：



如果许可证服务器不可用，您可能会看到错误消息：



如果您的许可证服务器仍在使用旧版许可证，并且 Citrix Virtual Apps and Desktops 站点支持 LAS，则 Web Studio 会提示您向 Citrix Cloud 注册许可证服务器。

注册许可证服务器以使用 LAS(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/register-license-server.png)

将旧版许可迁移到 LAS

如果您已将许可证服务器注册到 Citrix Cloud 并拥有必要的权利，则必须按照以下特定顺序将现有 Citrix Virtual Apps and Desktops 站点从旧版许可迁移到 LAS，而不会影响用户会话。

1. **升级许可证服务器：** 将许可证服务器升级到最低支持版本。
2. **升级 Delivery Controller：** 将站点中的所有 Delivery Controller 升级到 LAS 支持的版本。
3. **删除交付组许可证分配：**
   - 在单击**迁移到 LAS** 之前，手动删除在站点级别以下设置的任何许可证分配（即，删除交付组级别的许可证分配）。
4. **确认分配：** 验证 LAS 分配是否准确。
5. **单击迁移到 LAS：**
   - 完成上述步骤后，单击**迁移到 LAS**。

     从旧版许可证迁移到 LAS(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/migrate-to-las.png)
   - 迁移到 LAS 后，Citrix Virtual Apps and Desktops 站点的**许可证版本**设置为 **Citrix Virtual Apps and Desktops Premium**，**许可证模型**配置为**并发**。

从 LAS 回滚到旧版许可

要从 LAS 回滚到旧版许可，请执行以下操作：

1. 运行以下 PowerShell 命令。

   ```
   Set-ConfigSite -UseLicenseActivationService $false
   ```

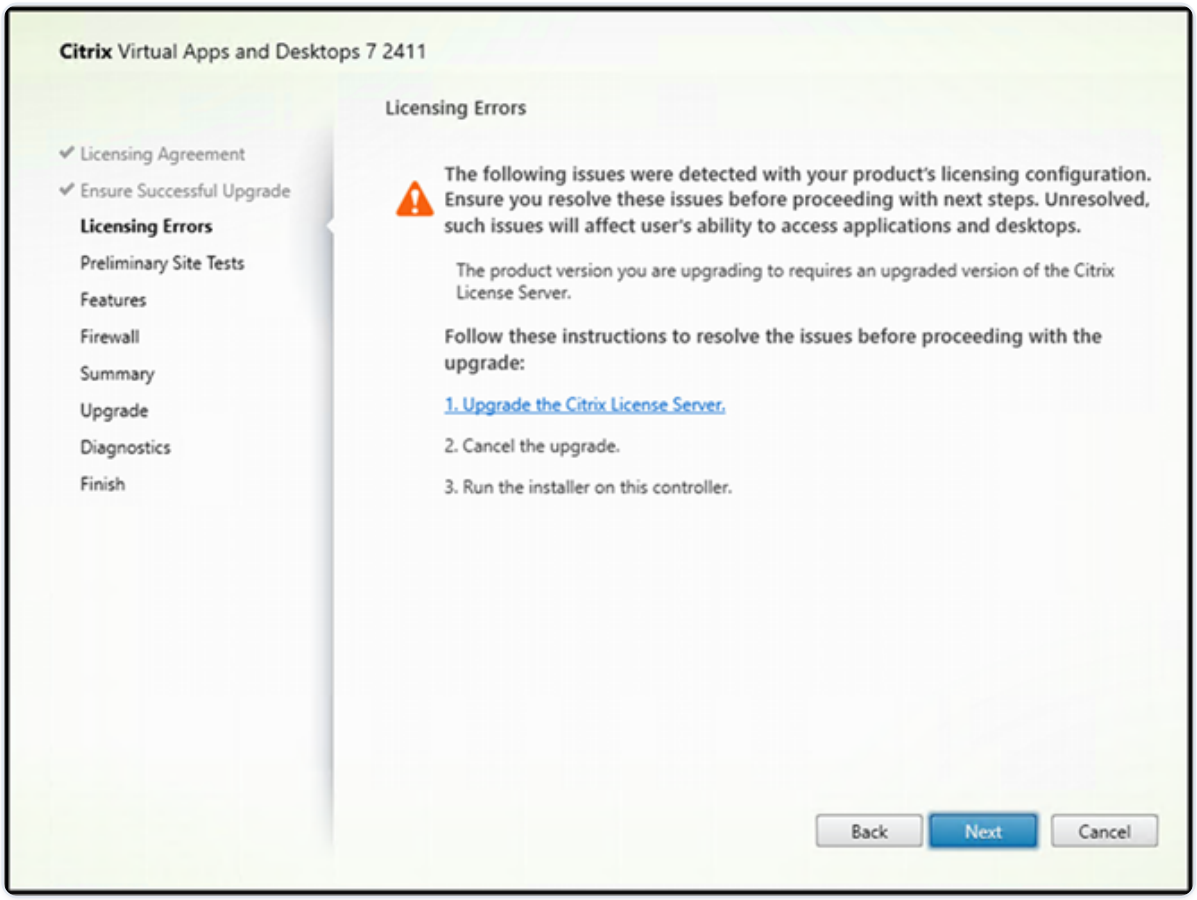
2. 在 Web Studio 中配置旧版许可证。

> **注意：**
>
> 这些步骤仅用于临时故障排除。旧版许可证文件即将终止服务 (EOL)，并且在 April 15, 2026 之后将无法运行。为确保服务不中断，我们建议迁移到许可证激活服务 (LAS)。有关详细信息，请参阅公告。

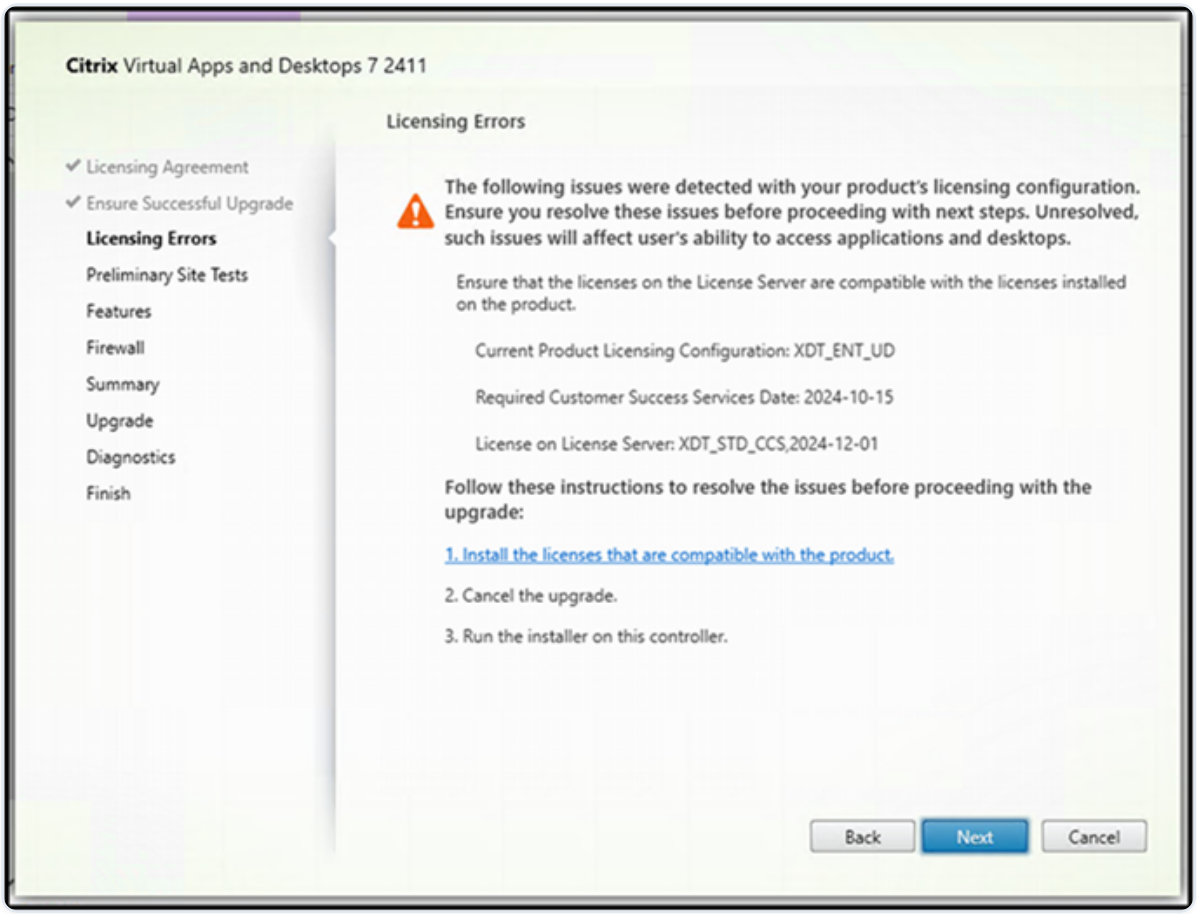
升级的重要注意事项

当您从任何早期版本的 Citrix Virtual Apps and Desktops 升级到 2411 及更高版本时，请将许可证服务器升级到最新版本（版本 11.2.17 build 53100 或更高版本）。

- 在使用元安装程序 UI 升级时，您会在许可证错误页面上收到以下错误：
  - 如果您不升级到最新的许可证服务器版本：



  - 如果存在任何不兼容性，例如许可证服务器过时或许可证不可用：



- 如果您使用命令行进行升级，请运行以下命令以避免升级失败（假设您位于已装载 ISO 中的 \x64 文件夹内）：

1. 运行以下命令：

```
\x64\Licensing\CitrixLicensing.exe /quiet
```

如果您已将许可二进制文件复制到任何本地驱动器，则运行以下命令：

```
\x64\Licensing\CitrixLicensing.exe /quiet /l install.log
```

2. 运行以下命令：

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components
"CONTROLLER,WEBSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
```

卸载核心组件

在升级期间，如果您首先使用命令 `\x64\Licensing\CitrixLicensing.exe /quiet` 或 `\x64\Licensing\CitrixLicensing.exe /quiet /l install.log` 安装了许可证服务器，然后安装了核心组件，则请按照相同的顺序进行卸载：

1. 使用命令行卸载许可证服务器：

```
CitrixLicensing.exe /quiet /uninstall /l uninstall.log
```

2. 使用 GUI 或命令行卸载组件。有关信息，请参阅 删除组件。

如果您使用命令行 `XenDesktopServerSetup.exe` 或 `removeall` 卸载许可证服务器和组件，请清理注册表项和剩余文件。

清理注册表项：

1. 搜索注册表项 `Citrix Licensing` 并删除该条目。通常，您可以在以下位置找到该条目：

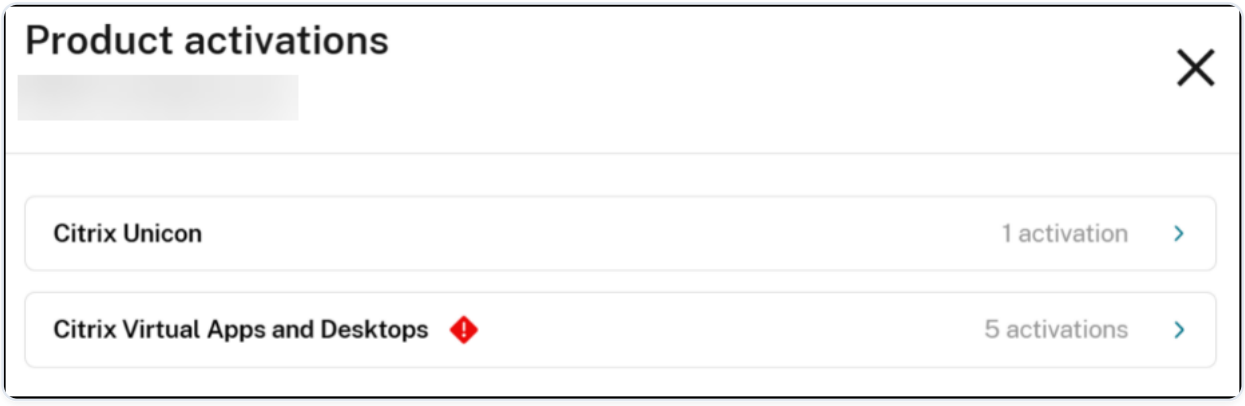
```
"Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\
```

2. 删除注册表项中 **Uninstall String** 指向的文件夹。

故障排除

如果许可证服务器在 Citrix Cloud 中的状态显示为非绿色，请执行以下操作以了解可能存在问题的激活的详细信息：

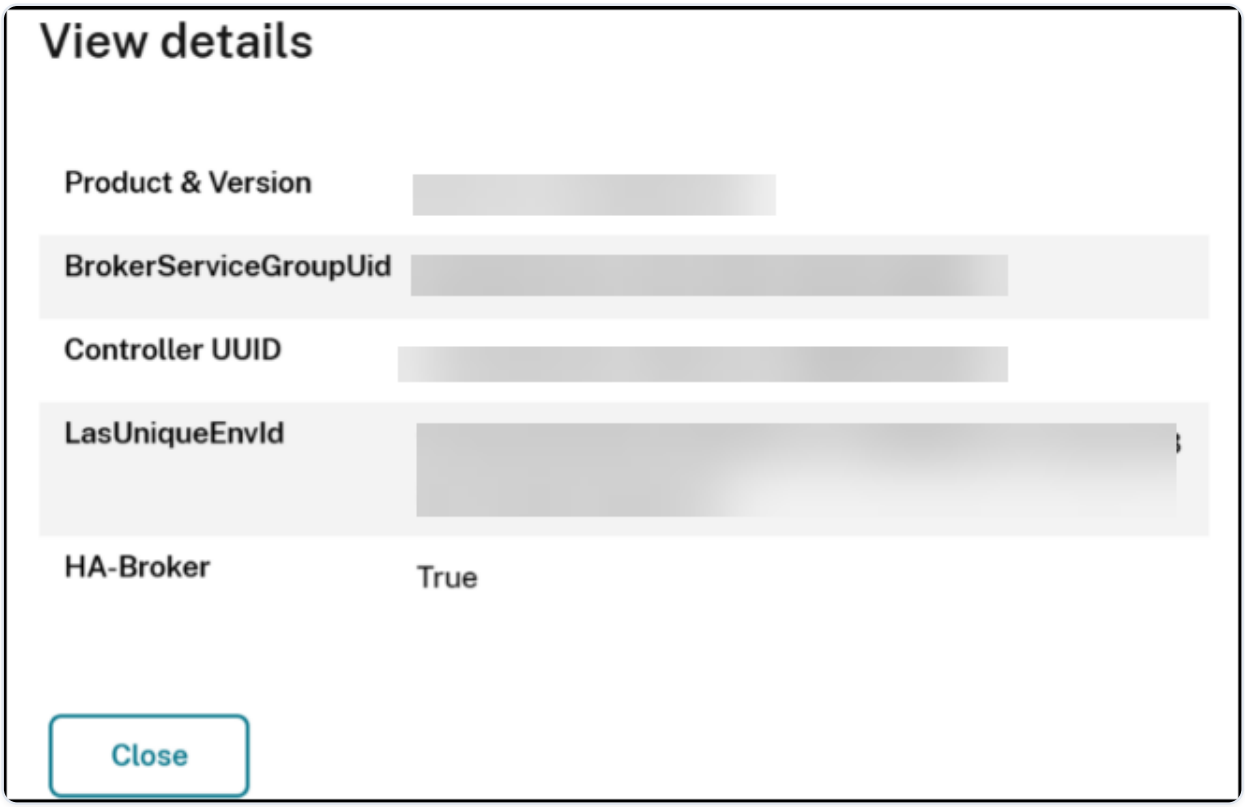
1. 在 Citrix Cloud 中，导航到 **许可 > 许可部署 > 许可证服务器**。
2. 单击 Citrix Virtual Apps and Desktops 旁边的展开按钮 **>** 以查看已激活的 Delivery Controllers 列表。



3. 单击激活旁边的 **View details** 以查看详细信息。

   ID 是用于标识激活的唯一标识符。

   提供了以下详细信息：



   - **Product & Version**：产品版本模型 (Product_Edition_Model) 和产品配置为在通过 LAS 激活时使用的烧录日期 (Burn In Date)。BurnInDate 通常是产品的发布日期。
   - **BrokerServiceGroupUid**：Broker 服务组的 UID。
   - **Controller UUID**：交付控制器的 UUID。
   - **LasUniqueEnvId**：LAS 为激活提供的实例的唯一 ID。
   - **HA-Broker**：指示它是 HA broker 还是主 broker 的 True 或 False。

要将已激活的主机详细信息与实际主机进行映射，请在该主机上运行以下命令。

- `Get-BrokerSite`：将屏幕上显示的 **BrokerServiceGroupUid** 值与命令的 `BrokerServiceGroupId` 输出进行比较。
- `Get-BrokerController`：将屏幕上显示的 **Controller UUID** 值与命令的 UUID 输出进行比较。

与许可事件相关的事件查看器日志

事件 ID	描述
1112	Citrix Broker Service 未能为用户与资源建立连接。站点的产品和版本许可配置不允许此类型的资源。请检查是否已为此站点选择了正确的许可证。
1150	Citrix Broker Service 已成功联系许可证服务器。
1151	Citrix Broker Service 无法联系许可证服务器。请确保许可证服务器正常运行，并且 XenDesktop 配置中标识许可证服务器的详细信息正确无误。
1152	此 XenDesktop 站点在许可证服务器上没有所需的许可证。请使用许可证管理控制台将相关产品许可证添加到许可证服务器。
1153	此 XenDesktop 站点的许可证已过期。Citrix Broker 服务将从许可证服务器请求新许可证。
1154	此控制器已进入许可证缓存模式，因为它无法联系许可证服务器。在此控制器停止提供桌面和应用程序会话之前，您还有 2 小时。
1155	Citrix Broker 服务现在将停止提供桌面和应用程序会话。由于持续无法与许可证服务器通信，此控制器不再处于或无法进入许可证缓存模式。请确保许可证服务器正常运行，如有必要，请使用许可证管理控制台将相关许可证添加到许可证服务器。
1156	Citrix Broker 服务正在成功与许可证服务器通信。此控制器不再处于许可证缓存模式。
1157	许可证服务器上运行的版本早于 Citrix Broker 服务的版本，因此不兼容。请升级您的许可证服务器，或在 XenDesktop 配置中指定具有正确版本的许可证服务器位置。

事件 ID	描述
1158	Citrix Broker 服务检测到您已超出此版本在此站点许可证服务器上可用的许可证数量。许可证服务器已授予您透支许可证。
1159	Citrix Broker 服务拒绝了桌面连接，因为此站点已超出最大安装许可证数量。此版本已安装三个许可证，但此版本允许的最大许可证数量为两个。请从许可证服务器中删除相关许可证以符合许可证限制。
1160	Citrix Broker 服务在管理许可证时遇到内部错误。请确保许可证服务器正常运行，并且 XenDesktop 配置中标识许可证服务器的详细信息正确无误。重新启动 Citrix Broker 服务也可能解决此问题。如果此问题仍然存在，请重新安装 Citrix XenDesktop Controller。请参阅 Citrix 知识库文章 CTX126990。
1161	初始化许可时出错。检查许可证服务器连接。
1162	停止许可时出错。检查许可证服务器连接。
1163	无可用连接许可证。要解决此问题，请通过关闭不需要的会话来释放许可证，或添加更多许可证。
1164	签出连接许可证时出错。检查许可证服务器连接。
1165	签入连接许可证时出错。检查许可证服务器连接。
1166	检查许可证可用性时出错。检查许可证服务器连接。
1167	无法启动许可。请检查许可证服务器连接。
1168	读取许可用户通知设置时出错。请检查许可证服务器连接。

事件 ID	描述
1169	此控制器已进入开箱即用许可证缓存模式，因为在许可证服务器上未找到合适的许可证。此控制器停止提供桌面和应用程序会话前，您还有 2 小时。
1170	Citrix Broker Service 已成功在许可证服务器上检测到合适的许可证。此控制器不再处于开箱即用许可证缓存模式。
1171	未指定许可证服务器。在指定有效的许可证服务器之前，Citrix Broker Service 无法向用户提供桌面和应用程序。您可以在 Citrix Studio 中或使用 Citrix PowerShell SDK cmdlet Set-ConfigSite 指定许可证服务器。
1172	检查许可证服务器适用性时出错。Citrix Broker Service 在检查计算机是否适合用作许可证服务器时收到意外响应。请检查控制器是否可以联系到该计算机，以及该计算机上的任何防火墙是否允许来自控制器的连接。如果计算机上安装了许可证服务器，请检查其是否已正确配置和运行。
1173	此 XenDesktop 站点在许可证服务器上没有所需的启动许可证。请使用许可证管理控制台将相关许可证添加到许可证服务器。
1174	此 XenDesktop 站点配置的产品版本不支持应用程序；应用程序资源将不可用。
1176	配置的产品版本不支持多会话计算机。注册被拒绝。
1177	配置的产品版本不支持单会话计算机。注册被拒绝。
1178	配置的产品版本不支持 RemotePC。注册被拒绝。
1179	配置的产品版本不支持预配到云系统中的计算机。注册被拒绝。

事件 ID	描述
1180	此 XenDesktop 站点配置的产品版本不支持单会话（工作站操作系统）计算机上的应用程序。应用程序资源启动被拒绝。
1181	此 XenDesktop 站点配置的产品版本不支持多会话（服务器操作系统）计算机上的应用程序。应用程序资源启动被拒绝。
1182	此 XenDesktop 站点配置的产品版本不支持单会话（工作站操作系统）计算机上的桌面。桌面资源启动被拒绝。
1183	此 XenDesktop 站点配置的产品版本不支持多会话（服务器操作系统）计算机上的桌面。桌面资源启动被拒绝。
1196	由于许可证服务器上所有可用许可证已耗尽，此控制器已进入许可证突发模式。请添加更多许可证以解决此问题。在此控制器停止提供桌面和应用程序会话之前，您还有 2 小时。
1197	Citrix Broker Service 现在将停止提供桌面和应用程序会话。由于许可证服务器上的许可证不足，此控制器不再处于或无法进入许可证突发模式。请使用许可证管理控制台将相关许可证添加到许可证服务器。
1198	Citrix Broker Service 正在成功从许可证服务器使用许可证。服务器上有足够的许可证来满足当前需求。此控制器不再处于因许可证耗尽而导致的许可证突发模式。
1199	Citrix Broker Service 现在将停止提供桌面和应用程序会话。由于许可证服务器上未安装任何许可证，此控制器不再处于或无法进入许可证缓存模式。请使用许可证管理控制台将相关许可证添加到许可证服务器。
1205	您的软件维护已过期。您的 Citrix 环境目前不受支持。请检查您的许可证服务器以查找过期许

事件 ID	描述
	可证并将其删除。在用户开始收到警告消息之前，有 30 天的许可证缓存模式。
1206	许可证证书哈希无效。您的 Citrix 许可证证书哈希无效。
1300	Citrix Broker Service 现在将停止提供桌面和应用程序会话。许可证服务器的系统时钟存在问题。
1301	许可证服务器的系统时钟问题已得到纠正。Citrix Broker Service 现在将恢复正常运行。
1302	此控制器再次未能签入或签出连接许可证。以前检测到的故障仍然存在。为避免过多的事件日志记录，服务将抑制相关消息（事件 ID 1163、1164、1165），直到问题解决。许可尝试将继续。
1303	此控制器不再抑制相关消息（事件 ID 1163、1164、1165）。
1304	Citrix Broker Service 已成功联系 LAS。
1305	Citrix Broker Service 无法联系 LAS。请确保 LAS 正常运行，并且 XenDesktop 配置中标识 LAS 的详细信息正确无误。

更多信息

有关检查站点的 LAS 状态或验证站点是否处于许可证缓存模式的信息，请参阅：

- 如何检查站点的 LAS 状态？
- 如何验证站点是否处于许可证缓存模式？

有关命令的详细信息，请参阅：

- Get-BrokerController
- Get-ConfigSite

Citrix Virtual Apps and Desktops™ 遥测数据元素

代理

用法

标头

键	描述	示例
版本	指示遥测事件的版本。	1
id	指示使用事件的唯一标识符。	d4ce7919-5d80-44de-a8fa-102923fe0ead
类型	指示 Citrix Analytic Service 用于识别云使用事件的事件类型。	SendBrokerTelemetryData
st	指示事件在 Broker 中生成时的时间戳。	2011-08-12T20:17:46.384Z
生产	标识使用事件的源产品和部署。	XenDesktop.Broker (云) OnPrem.Broker (OnPrem)
prodVer	指示 Citrix DaaS/ Citrix Virtual Apps and Desktops 产品版本。	7.25.0.0

负载

字段	描述	示例
TotalPublishedApps	指示已发布的应用程序总数。	10
TotalPublishedDesktops	表示已发布的桌面总数。	10
VDAs.Total	表示 VDA 的总数。	10

字段	描述	示例
VDAs.OSTypes	表示按操作系统类型（如 Windows、Linux 和 Mac）划分的 VDA 总数。	10
VDAs.OSVersions	表示按操作系统版本（如 Windows 10、11、2022、2019）划分的总数。	10
VDAs.HostingLocations.Azure	表示每个受支持的托管位置（如 Azure、AWS、GCP、Nutanix、VMWare、XenServer 和 HyperV）的 VDA 数量。	10
VDAs.HostingLocations.AWS		
VDAs.HostingLocations.Nutanix		
VDAs.HostingLocations.VMWare		
VDAs.HostingLocations.XenServer		
VDAs.HostingLocations.HyperV		
VDAs.ProvisionedMethod.MCS	指示通过 Machine Creation Service (MCS) 预配的计算机数量。	10
VDAs.ProvisionedMethod.ManualOr3P	指示手动或通过第三方预配的计算机数量。	10
VDAs.SessionSupport.StaticSingle	指示静态分配的单会话计算机数量。	10
VDAs.SessionSupport.DynamicSingle	指示动态分配的单会话计算机数量。	10
VDAs.SessionSupport.Multi	指示多会话计算机的总数量。	10
VDAs.RemotePCAccess.Windows	指示按操作系统类型（Windows、Mac、Linux）	10

字段	描述	示例
VDAs.RemotePCAccess.Linux	划分的远程电脑访问计算机数量。	
VDAs.RemotePCAccess.MacOS		
VDAs.ActiveSessionRecordingAgents	指示具有活动会话录制代理的 VDA 数量。	5
VDAs.Subscriptions	表示 VDA 的公有云订阅数量。	2
VDAs.LocationTypes	表示 VDA 的位置类型数量。	2
AutoScale.DGWithAutoscaleEnabled	表示启用了 **Autoscale** 的交付组数量。	2
AutoScale.TotalMachinesCtrlByAutoscale	表示由 autoscale 控制的计算机数量。	5
AutoScale.VerticalAutoscaleEnabledByDGandSite	表示按 DG 和站点启用了 **Vertical Autoscale** 的计算机数量。	2
AutoScale.TaggedBasedAutoscaledDG	表示基于标签的自动缩放交付组数量。	2
DeliveryGroup.TotalRebootSchedulesEnabled	表示启用了 **重新启动计划** 的交付组数量。	2
DeliveryGroup.Total	指示交付组的总数。	10
Policy.TotalPolicySets	指示策略集的数量。	3
Policy.TotalPolicies	指示组策略的数量。	2
Policy.TotalPolicySettings	指示组设置的数量。	2
PublishedPackageApps.AppVSingleAdmin	指示在 AppV 单管理员模式下发布的打包应用程序总数。	2

字段	描述	示例
PublishedPackageApps.AppVDualAdmin	指示在 AppV 双管理员模式下发布的打包应用程序总数。	2
PublishedPackageApps.Msix	指示在 MSIX 模式下发布的打包应用程序总数。	2
PublishedPackageApps.AppAttach	指示在 AppAttach 模式下发布的打包应用程序总数。	2
PublishedPackageApps.FlexApp	指示在 FlexApp 模式下发布的打包应用程序的总数。	2

会话

标头

字段	描述	示例
版本	指示许可证使用事件的版本。	1
id	指示使用事件的唯一标识符。	d4ce7919-5d80-44de-a8fa-102923fe0ead
类型	指示 Citrix Analytic Service 用于识别云使用事件的事件类型。	Cloud.Licensing
st	指示事件在 Broker 中生成时的时间戳。	2011-08-12T20:17:46.384Z
生产	标识使用事件的源产品和部署。	XenDesktop.Broker (云) OnPrem.Broker (OnPrem)
prodVer	指示 Citrix DaaS 或 Citrix Virtual Apps	7.25.0.0

字段	描述	示例
	and Desktops 产品版本。	
用户	标识用于唯一标识启动会话的用户的用户 ID。**该值已打乱。**	fullName: C648FE671A44B3F7 **（始终混淆）** samName:C758LH671A44B3F7 **（始终混淆）** upn: C7948FE671A44B3F7 **（始终混淆）** userLicenseId:C265FE671A44B3F7 **（始终混淆）** userSid: C097FE671A44B3F7 **（始终混淆）**
租户 -> ID	指示 Citrix Cloud™ 帐户的客户 ID。对于本地部署，此字段不适用且没有值。	joj1mh0598tj 代码
设备 到 设备 ID	指示设备 ID，用于唯一标识启动会话的设备。	AE18C4D5
dvc 映射到 dvcName	指示设备的友好名称。**该值已加扰。**	C758LH671A44B3F7 **（始终加扰）**

负载

字段	描述	示例
appProtectionKeyLoggingRequired	指示会话是否在启用键盘记录保护的情况下启动。	否
appProtectionScreenCaptureRequired	指示会话是否在启用屏幕捕获保护的情况下启动。	否
cspTenantCustomerId	指示 CSP 租户的 Citrix Cloud 帐户的客户 ID。对于本地部署，此字段不适用且没有值。	6c2vtxgxyftt 代码
isAnonymousUser	指示是否启动了未经身份验证的会话。	否
licenseActivityTimeStamp	指示生成有效负载的时间戳。	2011-08-12T20:17:46.384Z
licenseActivityType	指示许可事件类型。此字段指示许可事件类型是用于分配还是释放操作。	连接
licenseModel	指示部署的许可模型。	用户设备
productEdition	指示部署的产品版本。	高级版
productId	指示部署中产品的产品 ID。	CAVDS
协议	表示用于启动会话的协议。	HDX™
sessionKey	表示会话的唯一标识符。	uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2

字段	描述	示例
sessionSupport	表示会话支持类型。	SingleSession
sessionType	表示会话类型。	应用程序
版本	表示有效负载版本。	1.3
workerSid	表示用于会话的 VDA 的唯一标识符。**该值已加扰。**	1E5LH671A44B3F7**（始终加扰）**
isWindows365	表示会话是否为 Windows 365 启动。	是
entitlementType	指示客户的许可证授权类型。	生产
siteId	指示站点的唯一标识符。	a35647d0-901c-4477-87e0-dcd781d455f4
desktopGroupId	指示桌面或交付组的唯一标识符。	e9d859dc-1bfc-4b3e-bad3-41806bb4e694
clientType	指示 Citrix Workspace™ 应用程序类型。	视窗
clientVersion	指示 Citrix Workspace 应用程序版本。	23.5.1.83
workerCloudType	指示用于 VDA 预配的公共云类型。	艾滋尔
enabledFeatures	指示为会话启用的功能。例如，在启用了 `AppProtectionScreenCaptureRequired` 和 `SessionRecording`	66

字段	描述	示例
	的会话中，此字段的值为 66。	
launchRequestSource	记录用于请求启动的产品。它可以是本地 StoreFront™ 或云 StoreFront。	0 (StoreFront or 3P) 1 (工作区)
isEvents	指示 {{page.lic}} 中的关键故障。	无法创建 ST 数据库。
heartBeatTime	指示许可证服务器到 CIS 或 Citrix Analytic Service 的心跳时间。	1689058813
vdaTelemetry	指示为应用程序分层、用户个性化层、用户配置文件管理、Workspace Environment Management™ 和 HDX 功能捕获的负载。	vdaTelemetry SessionTelemetry CPM_feature: 32 HDX1: 66 HDX2: 0 MachineTelemetry AL_productVersion: 23.12.0.1001 UPL_isEnabled: 1 CPM_版本: 22.3.4000 wem_enableMethod: 1 wem_agentVersion: 2402.1

工作室

用法

标头

字段	描述	示例
版本	指示许可证使用事件的版本。	1
id	指示使用事件的唯一标识符。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
类型	指示 Citrix Analytic Service 用于识别云使用情况事件的事件类型	Studio.Usage
st	指示在 Studio 中生成事件的时间戳。	2024-03-22T01:32:23.4056195Z
生产	标识使用情况事件的源产品和部署。	XenDesktop.Studio
prodVer	指示 Citrix DaaS/Citrix Virtual Apps and Desktops 产品版本	7.42.0.0

负载

字段	描述	示例
AdminLoginList	指示唯一管理员 SamAccountName 的列表。**该值已加扰。**	{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}**(始终加扰)**
TotalApiRequests	指示编排服务的 API 请求。	{TotalApiRequests: 1000}
BackupCount	指示由 Studio 管理员操作的备份数量。	{BackupCount: 200}
RestoreCount	指示由 Studio 管理员操作的还原数量。	{RestoreCount: 20}

导览器

使用情况报告

标头

字段	描述	示例
版本	指示许可证使用情况事件的版本。	1
id	指示使用情况事件的唯一标识符。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
类型	指示 Citrix Analytic Service 用于识别云使用情况事件的事件类型。	遥测
st	指示事件在 Studio 中生成时的时间戳。	2024-03-22T01:32:23.4056195Z
生产	标识使用情况事件的源产品和部署。	XenApp.Monitor
prodVer	指示 Director 产品版本。	7.42.0.0
dvcName	服务器名称	C758LH671A44B3F7

负载

字段	描述	示例
AdminLoginCount	这是有效负载的一部分，提供管理员登录的计数。	类型: AdminLogin 统计 0: 1 1: 7
FeatureUsageCount	有效负载的这一部分包含 Director 中使用的大型关键功能的计数。	类型: 功能使用统计信息 0: 15

字段	描述	示例
		1: 20 5: 10
OdataUsageCount	此有效负载部分包含 Odata API 使用计数	类型: OData_v3 统计信息 0: 1 2: 7 5: 9 类型: OData_v4 统计信息 0: 1 2: 8 6: 7
AppUsage	指示已发布应用程序的每周使用情况指标。	类型: AppUsage 标头: applicationName,processName,totalDurationInMinutes 期间: 01/05/24-07/05/24 值: [Calc_AWTSVDA-1907R,calc.exe,0.13, Notepad_AWTSVDA-1907R,notepad.exe,4]

字段	描述	示例
UniqueAppUsers	指示已发布应用程序的每月唯一用户数以及应用程序启动总数。	类型: UniqueAppUsers 标头: applicationName,totalLaunches,totalUniqueUsers 期间: 04/24 值: [Calc_AWTSVDA-1907R,100,10, Notepad_AWTSVDA-1907R,200,20]
DesktopUsage	指示已发布的桌面的每周使用情况指标。	类型: DesktopUsage 标题: desktopGroupName,sessionSupport,totalDurationInMinutes 期间: 01/05/24-07/05/24 值: [RdsDesktopAndAppGroup,1,10]
UniqueDesktopUsers	指示已发布的桌面在一个月内的唯一用户数和总启动次数。	类型: UniqueDesktopUsers 标题: desktopGroupName,totalLaunches,totalUniqueUsers 期间: 04/24

字段	描述	示例
		值: [RdsDesktopAndAppGroup,10,5]
AvgLogonDuration	指示平均登录持续时间。	类型: AvgLogonDuration 标头: totalUserLogons, avgLogonDurationInSeconds 期间: 01/05/24-07/05/24 值: [200,4]
CostSaved	指示客户在一个月内节省的成本。	类型: CostSaved 标头: 虚拟机监控程序,节省的成本,货币 期间: 04/24 值: [1,221.02,1 2,301.02,2]

Citrix Workspace 应用遥测

用法

标头

字段	描述	示例
版本	正在发送的有效负载版本	1.0

字段	描述	示例
id	事件标识符	d4ce7919-5d80-44de-a8fa-102923fe0ead
类型	遥测事件类型	配置
st	指示事件生成的时间	2011-08-12T20:17:46.384Z
生产	生成事件的产品名称	OnPrem.StoreFront
prodVer	生成事件的 CWA 版本	3.30.0.0

负载

字段	描述	示例
设备 ID	指示一个匿名设备 ID，用于唯一标识启动会话的设备。	AE18C4D5
客户端设备 GUID	指示一个匿名设备 GUID，用于唯一标识启动会话的设备。	123e4567-e89b-12d3-a456-426614174000
国家/地区代码	用户登录 CWA 的国家/地区	GB
时区	最终用户的本地时区	America/New_York

Storefront 配置

用法

标头

字段	描述	示例
版本	指示许可证使用事件的版本	1.0
id	指示使用事件的唯一标识符	d4ce7919-5d80-44de-a8fa-102923fe0ead
类型	指示 CAS 用于识别云使用事件的事件类型	配置

字段	描述	示例
st	指示事件在 StoreFront 中生成时的时间戳	2011-08-12T20:17:46.384Z
生产	标识使用事件的原始产品和部署	OnPrem.StoreFront
prodVer	指示 StoreFront 版本（内部）	3.30.0.0

负载

字段	描述	示例
serverName	指示 StoreFront 运行所在服务的主机名	店面-01.店面.本地
deploymentId	指示 StoreFront 部署的唯一标识符	f47ac10b-58cc-4372-a567-0e02b2c3d479
installedWithCVAD	指示 StoreFront 是否与 CVAD 一同安装	否
cpuCores	指示 CPU 核心总数	4
cpuModel	指示运行 StoreFront 的 CPU	第12代 英特尔(R) 酷睿(TM) i7-1255U 1.70 GHz
ramGb	指示 RAM 总量（GB）	16
numServersInGroup	指示服务器组中的服务器数量	3
商店	指示 StoreFront 商店配置 JSON blob。Store 对象的数组。**某些值已打乱**	示例
rfWebSites	指示 StoreFront RFWeb 配置 JSON blob。RFWeb 配置对象的数组	示例
网关	指示网关配置对象作为 JSON blob。网关对象的数组	示例

字段	描述	示例
authServices	指示身份验证服务配置对象作为 JSON blob。身份验证服务对象的数组	示例
IsPiiScrambled	是	

字段 STORES 的示例

```
[{

            "BaseUrl": "baseUrl",

            "StorePath": "/",

            "EnabledFeatures": 21 bit bitmap,

            "ResourceTypeFilteringEnabled": "disabled|
Citrix.MPS.Application;Citrix.MPS.Desktop",

            "DefaultRfWebSite": "/Citrix/StoreWeb",

            "GatewaysUsed": [

                "gatewayId"

            ],

            "VdaLogonDataProvider": "",

            "ResourceFeeds": [

                {

                    "FeedName": "<resourceFeedName>|scrambled",

                    "Type": "CVAD",

                    "LoadBalancingEnabled": true,

                }
```

```
            ],
            "AdvancedAggregation": {
                "Enabled": true,
                "GroupingCount": 1,
                "ControllersPushIdenticalResources": true,
                "LoadBalanced": true,
                "AnyPrimaryFarms": true,
                "AnyBackupFarms": true,
            }
}]
```

如果未找到任何商店，它将是一个空数组 。

字段 RFWEBSITES 的示例

```
[{
    "SiteId": "siteId",
    "BaseUrl": "baseUrl",
    "StorePath": "storePath",
    "UiExperienced": 0,
    "EnabledFeatures": 9 bit,
    "AuthMethodsEnabled": [
        "ad"
    ],
    "CanUsersDownloadApps": {
```

```
        "Enabled": true,
        "Windows": "exe",
        "MacOS": "dmg"
    },
    "WorkspaceControl": {
        "Enabled": true,
        "LogoffAction": 0,
        "AutoReconnectAtLogon": true,
        "ShowReconnectButton": true,
        "ShowDisconnectButton": true
    },
    "MultiClickTimeout": 1,
    "UiViews": [
        "apps",
        "desktops"
    ],
    "DefaultTab": 0,
}]
```

如果未找到任何 rfWebSites，它将是一个空数组 。

字段 GATEWAYS 的示例

```
[{

            "GatewayId": "gatewayId",

            "IsCloudGateway": true,

            "LoadBalancingSTAEnabled": true,

            "SessionReliabilityEnabled": true,

            "RequestTicketsFromTwoSTA": true,

            "Version": "1234",

            "LogonType": "domain",

            "SmartCardFallbackEnabled": true

}]
```

如果未找到任何网关，它将是一个空数组 。

字段 AUTHSERVICES 的示例

```
[{

    "SiteId": "SiteId",

    "Store": "StoreAuth",

    "AuthMethodsEnabled": [

        "ad"

    ],

    "PasswordChangeWhenExpired": 0,

    "PasswordRemindersForm": 1,

    "DelegateCredentialValidationToCitrix": true,
```

```
    "ValidatePasswordsOnDeliveryControllers": true

}]
```

如果未找到任何身份验证服务，它将是一个空数组 。

店面登录

用法

标头

字段	描述	示例
版本	指示许可证使用事件的版本	1.0
id	指示使用事件的唯一标识符	d4ce7919-5d80-44de-a8fa-102923fe0ead
类型	指示 CAS 用于识别云使用事件的事件类型	登录
st	指示在 Broker 中生成事件的时间戳	2011-08-12T20:17:46.384Z
生产	标识使用事件的原始产品和部署	OnPrem.StoreFront
prodVer	StoreFront 版本（内部）	3.30.0.0

负载

字段	描述	示例
用户	发起启动的用户。**该值已混淆**	fullName: C648FE671A44B3F7 **（始终混淆）** samName:C758LH671A44B3F7 **（始终混淆）**

字段	描述	示例
		upn: C7948FE671A44B3F7 **（始终混淆）** userLicenseId:C265FE671A44B3F7 **（始终混淆）** userSid: C097FE671A44B3F7 **（始终混淆）**
serverName	指示 StoreFront 运行所在服务的主机名	店面-01.店面.本地
loginMethodRfWeb	指示用户从 RFWeb 登录 StoreFront 所使用的方法	0
loginMethodAuth	指示用户从 Auth 服务登录 StoreFront 所使用的方法	0
网关 URL	指示登录期间使用的 Netscaler Gateway	NetScaler-网关.com
enabledFeatures	指示已启用功能的位掩码	12
userAgent	指示用于登录的客户端的 UserAgent	CitrixReceiver/22.11.0.19 Linux/5.17.15 X1Class CWACapable CWA/22.11.0.19
baseUrl	指示用户登录到的应用商店	storefront-dev.storefront.dev
storePath	指示用户登录到的应用商店	/Citirx/StoreWeb

字段	描述	示例
apiUsed	指示客户端是否正在使用 Store 或 PNAgent API	0
deviceId	指示用于登录 StoreFront 的设备。**该值已加扰**	张三
transactionId	指示在单个事务期间发送/生成的事务 ID	773aba9e-5b91-4ef9-8782-c4afb75698e7

委派管理

用法

标头

键	描述	示例
版本	指示许可证使用事件的版本。	1
id	指示使用事件的唯一标识符。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
类型	指示 Citrix Analytic Service 用于识别云使用事件的事件类型。	DelegatedAdmin.Usage
st	指示在委派管理员中生成事件的时间戳。	2024-03-22T01:32:23.4056195Z
生产	标识使用事件的源产品和部署。	XenDesktop.DelegatedAdmin (云)
		OnPrem.DelegatedAdmin (OnPrem)
prodVer	指示 Citrix DaaS 或 Citrix Virtual Apps and Desktops 产品版本。	7.42.0.0

负载

键	描述	示例
TotalCustomScopes	指示自定义作用域的总数。	2
TotalCustomRoles	指示自定义角色的总数。	4

混淆许可遥测数据

考虑到许可遥测中发送信息的敏感性，Citrix 为您提供了混淆数据的选项。

下表列出了可以混淆的数据：

字段	描述	示例
用户	标识用户 ID，以唯一标识启动会话的用户。	• fullName: `C648FE671A44B3F7` • samName: `C758LH671A44B3F7` • upn： `C7948FE671A44B3F7` • userLicenseId: `C265FE671A44B3F7` • userSid: `C097FE671A44B3F7`
dvc 映射到 dvcName	指示设备的友好名称。	`C758LH671A44B3F7`
workerSid	指示用于会话的 VDA 的唯一标识符。	`1E5LH671A44B3F7`

字段	描述	示例
AdminLoginList	指示唯一管理员 SamAccountName 的列表	`{AdminLoginList: [UFMJ+JvXOTHO9mQD sOweiw= =]}`
商店	指示 StoreFront 商店配置 JSON blob。一个商店对象数组。**某些值已打乱**	示例
deviceId	指示用于登录 StoreFront 的设备。	张三

要在 Delivery Controller 上启用或禁用加扰，请运行以下 PowerShell 命令。

> **注意：**
>
> 对于 Citrix Service Provider™ (CSP) 客户，混淆始终处于禁用状态。CSP 客户无法使用 PowerShell 命令启用混淆。

1. 从 Delivery Controller 主机打开 PowerShell 窗口。
2. 运行命令 `asnp citrix` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行以下命令以启用或禁用加扰：

   默认情况下，该值为 `1` 或 `true`，这会启用许可证遥测数据的加扰。

   要禁用：

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $false
   ```

   禁用加扰后，可以使用以下命令启用它：

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $true
   ```

许可常见问题解答

注意：

- 有关与 COVID-19 大流行相关的业务连续性资源，请参阅 CTX27055。
- 有关维护业务连续性的一般信息，请参阅 业务连续性 — 按需。
- 有关当前 Citrix 许可证服务器的更多信息，请参阅 许可。

Citrix® 许可

什么是许可证激活服务?

许可证激活服务 (LAS) 是一种现代化的云端许可解决方案，适用于本地 Citrix 许可证服务器。它提供了传统基于文件的许可方法的简化替代方案。

您无需手动上传许可证文件，而是可以将许可证服务器连接到 Citrix Cloud™ 进行在线激活。您的权利将自动交付到许可证服务器，从而无需进行许可证文件生命周期管理。

对于无法连接到云的许可证服务器，LAS 还提供了离线激活选项，确保了各种网络环境的灵活性。此服务引入了一种无缝且现代的方法来管理您的 Citrix 产品许可证。

有关更多信息，请参阅 许可证激活服务。

如何获取我的许可证文件?

我们通过电子邮件发送许可证访问代码。有三种方法可以使用许可证访问代码生成许可证文件：

- 从 `citrix.com` 上的 MyAccount 页面中的 **管理许可证**。有关更多信息，请参阅 在 citrix.com 上管理许可证。
- Web Studio 用于分配您的购买，许可证文件会自动安装在您的 Citrix 许可证服务器上。
- Citrix 许可证服务器中的 Citrix Licensing Manager 用于分配您的购买并安装您的许可证文件。有关更多信息，请参阅 安装许可证。

如何在我的帐户中分配许可证?

请参阅分配许可证。

如何将已分配的许可证添加到许可证服务器?

请参阅修改许可证。

Citrix 许可使用哪些 TCP 端口?

- 许可证服务器端口号为 27000。
- 供应商守护程序端口号为 7279。
- 许可 Web 服务端口为 8083。

什么是 Citrix 许可证服务器?

Citrix 许可证服务器是一个允许在网络上共享许可证的系统。有关详细信息，请参阅许可操作概述。

我可以虚拟化或群集 Citrix 许可证服务器吗?

可以。您可以虚拟化或群集 Citrix 许可证服务器。有关详细信息，请参阅群集许可证服务器。

如果我虚拟化 Citrix 许可证服务器，我能获得哪些好处?

虚拟化 Citrix 许可证服务器提供了一个冗余解决方案。该解决方案允许在多个物理服务器之间移动，而无需停机。

如果我虚拟化 Citrix 许可证服务器，是否有任何限制需要考虑?

否。

Citrix 许可证服务器是否管理我的 Citrix Virtual Apps and Desktops™ 部署的所有许可证?

Citrix 许可证服务器管理您为 Citrix Virtual Apps™ 和 Desktop 收到的所有许可证，但用于 Citrix Gateway 的 Premium Edition 许可证除外。那些安全导向的网络设备所需的内置于网络设备中的许可证服务器管理这些许可证。

什么是 Citrix 许可管理器?

Citrix Licensing Manager 允许从您安装了 Citrix Licensing Manager 的许可证服务器下载和分配许可证文件。Citrix Licensing Manager 是推荐的许可证服务器管理方法，它支持以下功能：

- 将许可证服务器通过短代码注册到 Citrix Cloud，并轻松移除注册。
- 配置用户和组帐户。
- 使用控制板显示已安装、正在使用、已过期和可用的许可证，以及 Customer Success Services 日期。
- 导出许可证使用数据，用于报告。
- 配置历史使用数据保留期。默认数据保留期为 180 天。
- 简化在许可证服务器上安装许可证文件，使用许可证访问代码或下载的文件。
- 启用和禁用许可证突发模式。
- 配置客户体验改善计划 (CEIP) 和 Call Home。

- 自动或手动检查 Customer Success Services 续订许可证，并在找到时通知您或安装许可证。
- 通知您许可证服务器状态 - 缺少启动许可证、时间问题、上传程序故障。
- 修改这些端口：
  - 许可证服务器（默认 27000）
  - 供应商守护程序（默认 7279）
  - 许可 Web 服务（默认 8083）

有关详细信息，请参阅 Citrix Licensing Manager。

Citrix 许可证管理控制台在哪里?

许可证管理控制台不再受支持，已从许可证服务器版本 11.16.6 中移除。我们建议您使用 Citrix Licensing Manager。

如果许可证服务器与 Studio 位于同一域或受信任域中，则可以使用 Studio 管理和跟踪许可。

有关详细信息，请参阅 Citrix Licensing Manager。

许可证分配期限是多久?

许可证分配期限是指 Citrix Virtual Apps and Desktops 许可证分配给用户或设备的期限。默认许可证分配期限为 90 天。

我如何知道我的组织购买了多少许可证?

所有购买的许可证都可以在 `<https://www.citrix.com>` 上的“**我的帐户**”页面中的安全“**管理许可证**”工具箱中随时（24x7）查看和访问。

我如何知道任何时候有多少许可证正在使用?

Citrix Licensing Manager 和 Studio 提供实时许可证使用情况的详细信息。

许可证服务器灾难恢复和维护

有关许可证服务器的灾难恢复和维护信息，请参阅 Citrix 许可文档中的灾难恢复和维护。

Citrix 虚拟应用和桌面许可

Citrix Virtual Apps and Desktops 如何获得许可?

思杰虚拟应用和桌面许可提供用户/设备和并发许可模式。

用户/设备：

灵活的用户/设备模型与以下各项保持一致：

- 企业范围的桌面使用。
- 基础 Microsoft 桌面虚拟化许可。
- 对于只需要偶尔访问其虚拟桌面和应用程序的客户，采用并发许可。

用户/设备许可允许用户从无限数量的设备访问其虚拟桌面和应用程序。设备许可允许无限数量的用户从单个设备访问其虚拟桌面和应用程序。这种方法为您提供了最大的灵活性，并改善了与 Microsoft 桌面虚拟化许可的一致性。

> **重要提示：**
>
> 您无法手动将许可证分配给用户或设备。许可证服务器或云服务会分配许可证。对于用户/设备许可，一旦分配了许可证，除非在 90 天不活动后，否则无法将其分配给其他用户。
>
> **并发：**
>
> 并发许可证允许任何用户和任何设备连接到无限数量的虚拟应用程序和桌面。许可证仅在活动会话期间占用。如果会话断开连接或终止，许可证将返回到池中。

有关用户/设备许可的更多信息，请参阅用户/设备许可证；有关并发许可证的更多信息，请参阅并发许可证。

是否可以在购买许可证之前试用 Citrix Virtual Apps and Desktops?

可以。您可以下载 Citrix Virtual Apps and Desktops 软件并以试用模式运行。试用模式允许您在本地使用 Citrix Virtual Apps and Desktops 30 天，支持 10 个连接，无需许可证。有关详细信息，请参阅评估许可证。

Citrix Cloud 的 Citrix DaaS™（以前称为 Citrix Virtual Apps and Desktops 服务）经批准后可提供试用服务。请咨询您的 Citrix 代表以了解更多详细信息。

Citrix 如何定义 Citrix Virtual Apps and Desktops 的并发性?

Citrix Virtual Apps and Desktops 并发模型允许任何用户和任何设备连接到无限数量的虚拟应用程序和桌面。许可证仅在活动会话期间占用。如果会话断开连接或终止，许可证将退回池中以供重新发放。有关详细信息，请参阅并发许可证。

我可以在一个通用许可证服务器上部署多个版本的 Citrix Virtual Apps and Desktops 许可证?

可以。许可证服务器同时管理 Citrix Virtual Apps 和 Citrix Virtual Apps and Desktops 的许可证。我们建议您安装最新版本的许可证服务器。如果您不确定您的许可证服务器版本是否为最新版本，请通过将您的版本与 Citrix 下载站点 上的版本号进行比较来验证它。

单个站点可以使用 Citrix Virtual Apps 和 Citrix Virtual Apps and Desktops 许可证?

根据版本不同，单个 Citrix Virtual Apps 或 Citrix Virtual Apps and Desktops 站点可以支持两种许可模型 - 用户/设备或并发。单个 Citrix Virtual Apps 或 Citrix Virtual Apps and Desktops 站点只能支持一个版本。有关详细信息，请参阅多类型许可。

支持多类型许可的最低版本是 XenApp 和 XenDesktop 7.15 长期服务版本 (LTSR) 以及 Citrix Virtual Apps and Desktops 7 1808。

如果我的许可证服务器上安装了 Citrix Virtual Apps and Desktops 用户/设备或 Citrix Virtual Apps and Desktops 并发许可证，我可以选择 Citrix Virtual Apps 并发作为产品模型?

如果您将 Citrix Virtual Apps 作为 Citrix Virtual Apps and Desktops 高级版或尊享版的功能使用，则其许可模型与 Citrix Virtual Apps and Desktops 的高级版或尊享版相同。如果您已购买 Citrix Virtual Apps and Desktops，即使您计划仅使用 Citrix Virtual Apps 功能，也应将许可配置为该产品。仅当您的许可证服务器上安装了 Citrix Virtual Apps 并发独立许可证时，才应选择此产品作为产品模型。

每个 Citrix Virtual Apps 和 Citrix Virtual Apps and Desktops 版本包含哪些产品组件?

有关按版本划分的完整功能矩阵，请参阅Citrix Virtual Apps and Desktops 功能。

如何根据 Citrix Virtual Apps and Desktops 最终用户许可协议许可 Citrix Virtual Desktops™ 环境?

为了根据 Citrix Virtual Apps and Desktops EULA 部署用户/设备或并发许可模型下的 Citrix Virtual Apps and Desktops，请将许可证文件应用到您的许可证服务器。许可证服务器随后控制并监视许可证合规性。我们建议您根据所购买的产品配置您的产品。例如，如果您购买了 Citrix Virtual Apps and Desktops Premium 但只想使用 Citrix Virtual Apps 功能，请将产品配置为 Citrix Virtual Apps and Desktops 以符合合规性。有关详细信息，请参阅产品许可证合规性中心。

如何根据 Citrix Virtual Apps 最终用户许可协议许可 Citrix Virtual Apps 环境?

为了根据 Citrix Virtual Apps EULA 部署并发许可模型下的 Citrix Virtual Apps，请将许可证文件应用到您的许可证服务器。许可证服务器随后控制并监视许可证合规性。

Citrix Virtual Apps and Desktops 服务选项：长期服务版本 (LTSR) 或当前版本 (CR) 是否有许可要求?

Citrix Virtual Apps and Desktops 服务选项（例如长期服务版本）是客户成功服务计划的一项权益。您必须拥有有效的客户成功服务才能享受 LTSR 的权益。有关详细信息，请参阅[Citrix Virtual Apps、Citrix Virtual Apps and Desktops 和 XenServer 服务选项。

远程浏览器隔离 (RBI) 服务池化小时数如何工作?

当您购买至少 25 个服务用户时，您将获得 5000 小时的服务使用权，这些小时数在所有用户之间共享。后续购买的用户权限不会增加池化小时数权益。要增加服务小时数权益，请购买附加包。

我可以使用远程电脑访问和 CCU 许可证吗?

是的。

有关远程电脑访问的信息，请参阅远程电脑访问。

当我的 Citrix 环境的软件维护过期时会发生什么?

当您的软件维护 (SWM) 或订阅过期时，对软件升级和技术支持的访问将暂停。此外，根据您的许可证类型和产品版本，最终用户和管理员将收到特定的警告通知，指示环境不受支持。

这些通知仅在服务器上的所有许可证都已过期时才会触发。

最终用户体验

用户在启动会话后将收到一条警告消息。该消息指出：

```
Citrix Virtual Apps and Desktops warning: Your corporate Citrix
environment is currently unsupported. Please contact your IT department to
resolve.
```

管理员体验

管理员将在 Citrix Studio 控制台中看到警告警报，提醒他们即将到期或已到期。

按许可证类型划分的到期行为

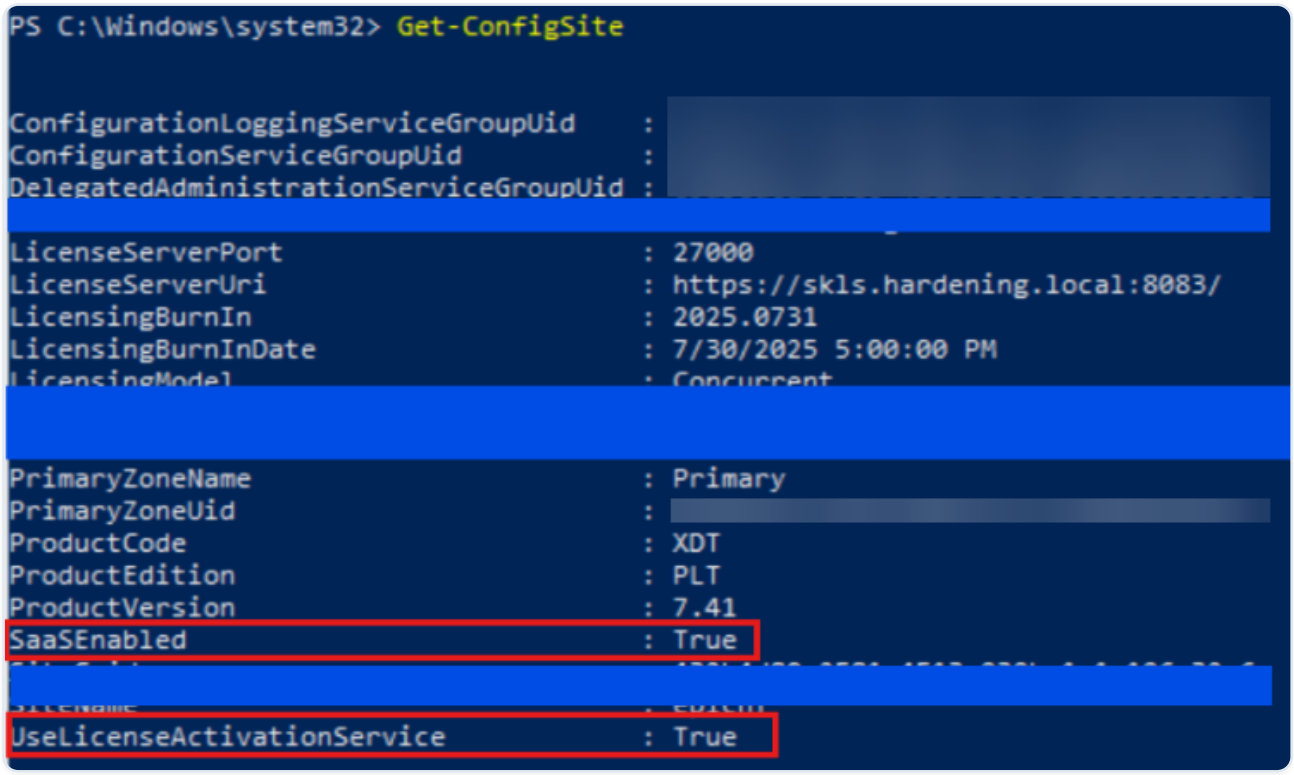
这些消息的显示时间取决于许可证类型和安装的 Citrix Virtual Apps and Desktops 版本。

本地订阅许可证

- 最终用户警告：订阅到期后，在宽限期内显示。
- 管理员警告：在订阅到期前 30 天在 Studio 中显示。
- 支持的版本：
  - 当前版本：Citrix Virtual Apps and Desktops 2411 及更高版本。
  - LTSR：2203 CU6、2402 CU1 及更高版本的 LTSR 版本

如何检查站点的 LAS 状态?

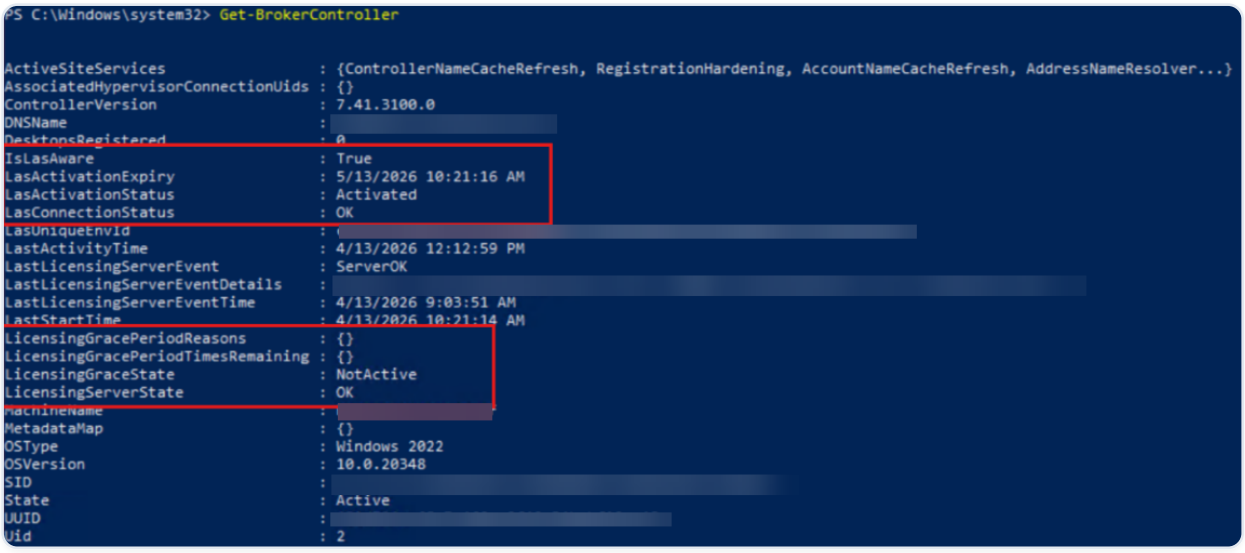
运行 `Get-configsite` 以检查 LAS 激活状态和 SaaS 位状态。



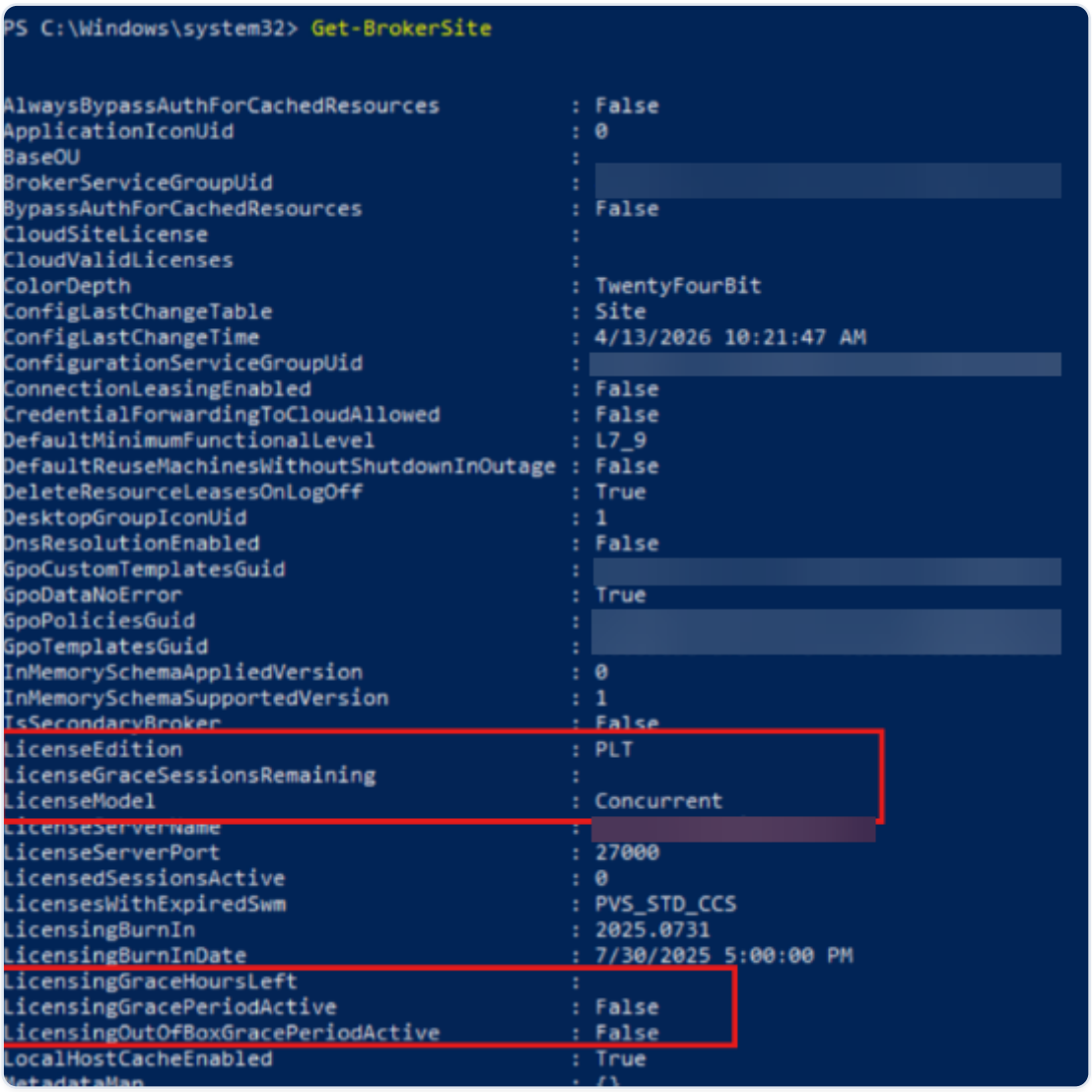
如何验证站点是否处于许可证缓存模式?

运行 `Get-Brokercontroller` 和 `Get-brokersite` 以获取有关缓存模式和剩余时间的详细信息。

- `Get-Brokercontroller` 输出：



- `Get-brokersite` 输出：



有关这些命令的详细信息，请参阅：

- Get-BrokerController
- Get-ConfigSite

有关 Delivery Controller 事件查看器日志中与许可相关的信息，请参阅 与许可事件相关的事件查看器日志。

用户或设备许可证

思杰如何在用户/设备许可模型中向用户分配许可证?

在用户/设备许可模型中，许可证服务器将许可证分配给唯一的用户 ID。它允许该单个用户从无限数量的设备进行无限连接。如果用户连接到桌面或设备，则该用户需要一个分配给该用户的许可证才能访问虚拟桌面或应用程序。许可证服务器或云服务分配许可证。您无法手动分配这些许可证。许可证分配给用户，而不是共享设备。一旦分配了许可证，在 90 天不活动之后才能将其分配给其他用户。有关详细信息，请参阅 用户/设备许可证。

思杰如何在用户/设备许可模型中定义许可设备?

许可设备需要唯一的端点设备 ID。在用户/设备模型下，设备是指您授权任何个人用于访问 Citrix Virtual Apps and Desktops 实例的任何设备。对于共享设备，单个 Citrix Virtual Apps and Desktops 用户/设备许可证可以支持共享该设备的多个用户。例如，共享设备可以是教室工作站或医院中的临床工作站。

我能否将我的思杰虚拟桌面标准版并发许可证转换为用户/设备模型?

您无法将思杰虚拟桌面标准版并发许可证转换为思杰虚拟桌面标准版用户/设备许可证。同样，您无法将思杰虚拟桌面标准版用户/设备许可证转换为思杰虚拟桌面标准版并发许可证。

如果您拥有 Citrix Virtual Desktops 标准版并发许可证，并且希望采用用户/设备许可模式，请升级到 Citrix Virtual Apps and Desktops 高级版或高级版。

从	到标准并发	到标准用户/设备	到高级用户/设备	到高级用户/设备
Citrix Virtual Desktops 标准版并发许可证	N/A	不允许并发到用户/设备的转换	您无法转换许可模式，但可以升级到 Citrix Virtual Apps and Desktops 高级版或高级版。	您无法转换许可模式，但可以升级到 Citrix Virtual Apps and Desktops 高级版或高级版。
Citrix 虚拟桌面标准版用户/设备许可证	不允许用户/设备到并发的转换	N/A	N/A	N/A

并发许可与用户/设备许可有何不同?

并发许可基于并发设备连接。并发许可证仅在设备建立活动连接时才被使用。连接结束后，并发许可证将返回许可证池以供立即使用。我们建议将此许可模式用于偶尔使用的情况。用户/设备许可证在一段时间内租用，在租约到期之前，其他用户无法使用。

在用户/设备模式下，我们能否在同一企业中同时为用户和设备分配许可证?

是的。两种类型可以同时存在于同一企业中。许可证服务器根据使用情况，将许可证最佳地分配给用户或设备。您无法手动分配这些许可证。

我如何决定要许可多少用户或设备?

评估用例要求以确定适当的许可证数量。用户/设备许可允许从无限数量的设备无限制地访问无限数量的虚拟桌面和虚拟应用程序。并发许可允许从单个设备无限制地访问无限数量的虚拟桌面和虚拟应用程序，该设备可供无限数量的用户使用。请考虑以下公式：

```
(Number of total users) – (number of users that only access exclusively

 with shared devices) + (number shared devices) = total number

 of licenses to buy.



For example, there are 1000 total users at the hospital. If 700 of them
access only

Citrix Virtual Desktops from 300 shared devices in the hospital, the
number of

licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

在用户/设备模型下，一个获得许可的用户最多可以使用多少设备连接到我的环境?

每个获得许可的用户都有权使用无限数量的连接设备或离线设备。

在用户/设备模型下，最多有多少用户可以访问一个获得许可的设备?

每个获得许可的设备可以为组织内的无限数量用户提供服务。

在用户/设备模型下，一个获得许可的用户在任何给定时间最多可以使用多少虚拟桌面或 RBI Web 应用程序?

每个获得许可的用户可以连接到无限数量的虚拟桌面或 Web 应用程序。

我是否可以购买 Citrix Virtual Apps and Desktops 许可证，以增加现有 Citrix Virtual Apps and Desktops 环境中获得许可的用户/设备的数量?

是的。您可以购买 Citrix Virtual Apps and Desktops 许可证，以增加现有 Citrix Virtual Apps and Desktops 环境中获得许可的用户/设备的数量。

如何释放授权的用户/设备许可证?

要释放授权用户/设备的分配，请根据 EULA 条款使用 `udadmin` 实用程序。许可证服务器随后会将许可证分配给下一个合适的用户/设备。有关详细信息，请参阅显示或释放用户或设备的许可证。

如果我超出了购买的用户/设备许可证数量，会发生什么?

用户/设备许可证包含 10% 的透支额度，该额度在生成许可证时已包含在内。透支额度也包含在已安装的许可证数量中。如果使用高峰超过了包括透支额度在内的已安装数量，则会拒绝更多用户的访问。购买并部署新许可证以允许更多用户访问。

如果所有许可证（包括许可证透支）都在使用中，则许可证突发模式允许无限连接到产品。许可证突发模式让您有时间确定为什么超出了最大许可证数量，并购买更多许可证，而不会中断您的用户。此期限持续到 15 天过去或您安装更多零售许可证（以先发生者为准）。有关详细信息，请参阅许可证突发模式。

Director 显示许可证缓存模式状态。有关详细信息，请参阅Director 控制板上的面板。

许可用户在任何给定时间可以使用的虚拟应用程序的最大数量是多少?

每个许可用户可以连接到无限数量的虚拟应用程序。

如果许可用户离开我的组织，会发生什么?

当现有许可用户离开您的组织时，您可以在不通知 Citrix 的情况下释放该离开用户的许可证。使用 `udadmin` 实用程序释放许可证。如果您不释放许可证，许可证服务器会在 90 天不活动后自动释放任何许可证。此信息受 EULA 中规定的条款约束。

如果许可用户长期缺席，会发生什么?

如果现有许可用户长期缺席，您可以在不通知 Citrix 的情况下释放许可证，以便将其重新分配。使用 `udadmin` 实用程序释放许可证。

如果我的组织中更换了许可设备，会发生什么?

如果您更换现有许可设备，您可以在不通知 Citrix 的情况下释放许可证，以便将其重新分配。使用 `udadmin` 实用程序释放许可证。

如果许可设备长时间停用，会发生什么?

当现有许可设备长时间停用时，您可以在不通知 Citrix 的情况下释放许可证，以便将其重新分配。使用 `udadmin` 实用程序释放许可证。如果您不释放许可证，许可证服务器会在 90 天不活动后自动释放任何许可证。此信息受 EULA 中规定的条款约束。

在将许可证分配给设备或用户后，我可以将用户许可证切换为设备许可证，反之亦然吗?

是的。此更改是自动发生的。许可证服务器根据使用模式将许可证分配给用户或设备。如果使用模式发生变化，许可证服务器可能会根据新的使用情况切换分配。许可证服务器始终以对客户最经济的方式分配许可证。此外，许可证服务器会监控许可证，以识别 90 天分配期后的**未使用**许可证。您可以将 90 天分配期后识别为未使用的许可证重新分配给其他用户或设备。

并发许可证

在并发模型下，Citrix Virtual Apps and Desktops 许可用户在任何给定时间可以使用的虚拟桌面最大数量是多少?

一个端点可以服务多个用户，并允许无限连接。

我可以将以前版本的 Citrix Virtual Apps and Desktops 的并发许可证以及新的用户/设备或并发许可证部署到单个许可证服务器吗?

是的。您可以继续使用相同的许可证服务器来支持用户/设备或并发许可部署。

我可以将并发许可证和用户/设备或并发许可证部署到单个许可证服务器?

是的。您可以继续使用相同的许可证服务器来支持并发以及用户/设备或并发许可部署。

Citrix Virtual Apps and Desktops Advanced 和 Premium 版本是否包含 Citrix Virtual Apps 并发许可证?

Citrix 虚拟应用和桌面 高级版和尊享版用户/设备许可证仅出于兼容性目的包含并发 Citrix 虚拟应用许可证。这些并发许可证仅适用于与用户/设备许可证不兼容的早期产品版本。用户/设备许可证中包含的并发兼容性许可证仅允许与这些版本一起使用 - XenApp 6.5 之前的版本和 XenDesktop 5.0 服务包 1 之前的版本。

如果我超出了购买的并发许可证数量，会发生什么?

如果所有许可证都在使用中，许可证突发模式将允许对产品进行无限连接。许可证突发模式让您有时间确定超出最大许可证数量的原因，并在不中断用户的情况下购买更多许可证。此期限持续到 15 天过去或您安装更多零售许可证（以先发生者为准）。有关详细信息，请参阅许可证突发模式。

Director 显示宽限期状态。有关详细信息，请参阅Director 控制板上的面板。

透支许可证

如何获取透支许可证?

支持用户/设备、用户或设备许可证模式的产品（Citrix Cloud 除外）包含许可证透支功能，使您能够使用有限数量的额外许可证来防止拒绝访问。我们提供任何透支功能是为了方便，而不是作为许可证权利。并发许可证和服务器许可证不包含透支。任何使用的透支许可证必须在首次使用后 30 天内购买，但使用不限于 30 天。Citrix 保留在新产品版本中删除任何透支功能的权利。有关详细信息，请参阅许可证透支。

如何识别许可证透支?

您可以在 Citrix Licensing Manager 中查看使用情况信息，包括透支许可证的数量。Studio 也包含透支使用情况信息。

透支许可证被使用后会发生什么?

系统会从您已安装的许可证中分配一个许可证，以启用对 Citrix Virtual Apps and Desktops 环境的访问。此透支许可证提供与您其他许可证相同的访问权限和功能。

当我的透支许可证被使用时，我能收到警报吗?

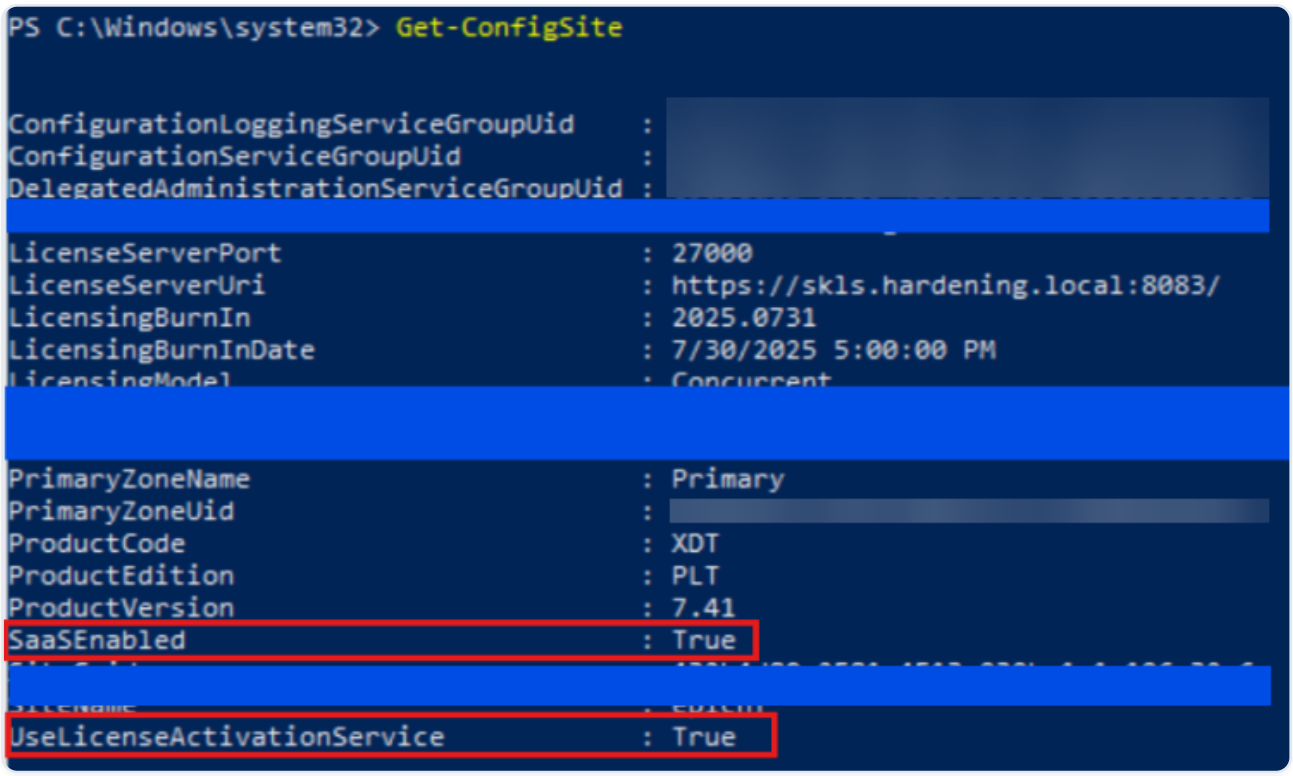
目前，当透支许可证被使用时，没有提供特定的警报。

透支许可证可以使用多长时间?

请在首次使用后的 30 天内购买任何已使用的透支许可证。

如何检查站点的 LAS 状态?

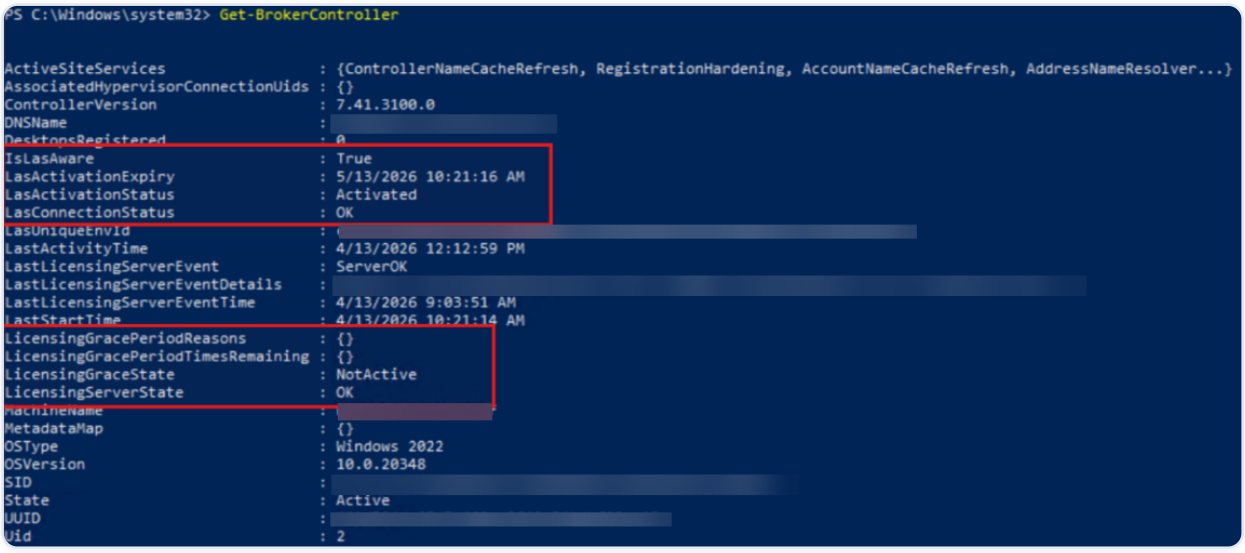
运行 `Get-configsite` 以检查 LAS 激活状态和 SaaS 位状态。



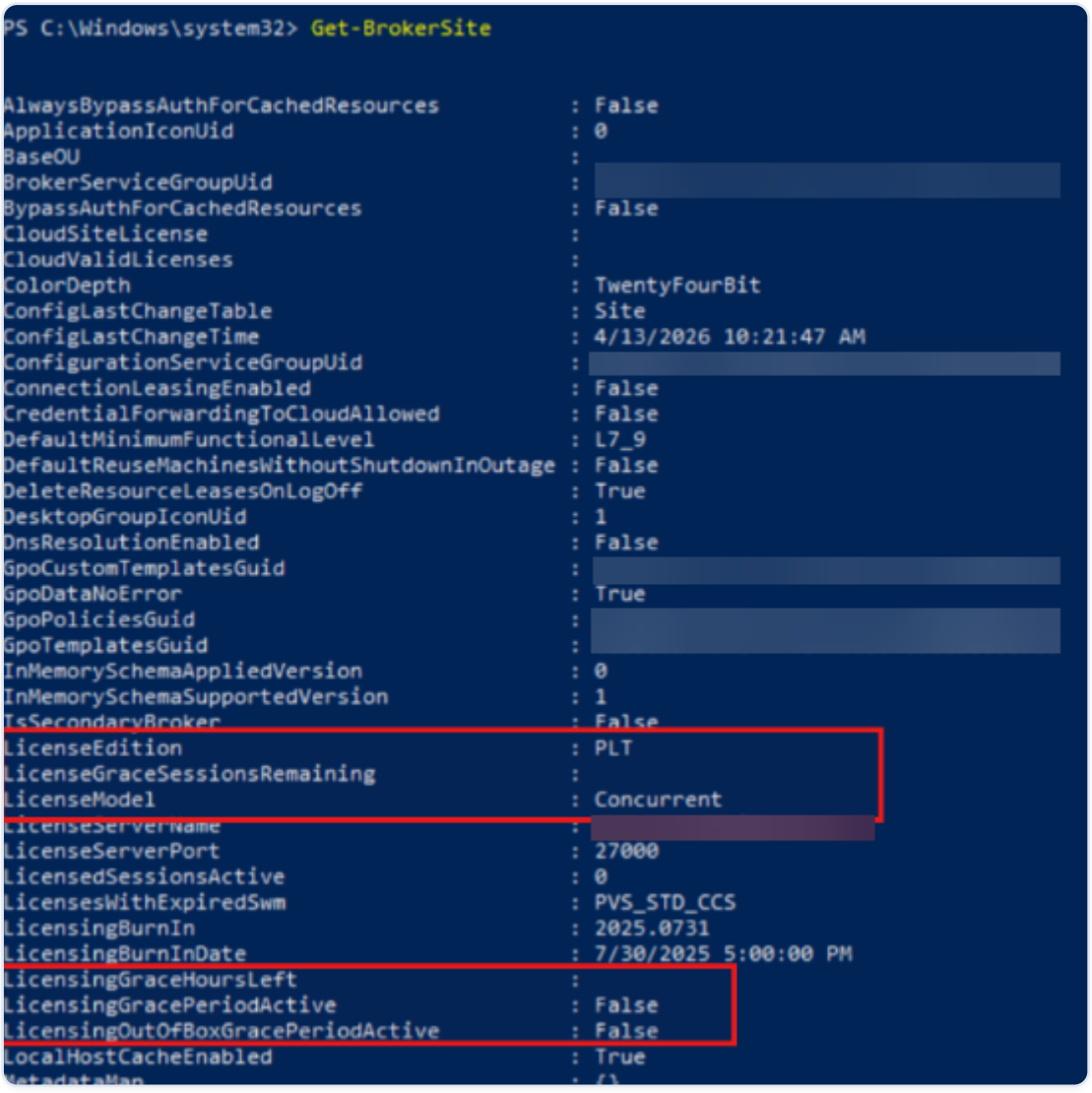
如何验证站点是否处于紧急许可证缓存模式?

运行 `Get-Brokercontroller` 和 `Get-brokersite` 以获取有关紧急缓存模式和剩余时间的详细信息。

- `Get-Brokercontroller` 输出：



- `Get-brokersite` 输出：



有关这些命令的详细信息，请参阅：

- Get-BrokerController

- Get-ConfigSite

有关交付控制器事件查看器日志中与许可相关的信息，请参阅与许可事件相关的事件查看器日志。

其他特定于产品的许可信息

- Citrix 应用交付控制器
- 思杰云
- 思杰端点管理
- 思杰网关
- XenServer
- Citrix 许可

本地主机缓存

为确保 Citrix Virtual Apps and Desktops 站点数据库始终可用，Citrix 建议从容错 SQL Server 部署开始，遵循 Microsoft 的高可用性最佳实践。（有关支持的 SQL Server 高可用性功能，请参阅数据库。）但是，网络问题和中断可能导致用户无法连接到其应用程序或桌面。

本地主机缓存功能允许站点中的连接代理操作在发生中断时继续进行。当 Delivery Controller™ 与站点数据库之间的连接在本地 Citrix® 环境中失败时，就会发生中断。当站点数据库在 90 秒内无法访问时，本地主机缓存将启用。

自 XenApp and XenDesktop 7.16 起，连接租用功能（早期版本中的前身高可用性功能）已从产品中移除，不再可用。

数据内容

本地主机缓存包含以下信息，这些信息是主数据库中信息的子集：

- 被授予站点发布的资源权限的用户和组的身份。
- 当前正在使用或最近使用过站点发布的资源的用户身份。
- 站点中配置的 VDA 计算机（包括远程 PC 访问计算机）的身份。
- 正在主动用于连接到已发布资源的客户端 Citrix Receiver™ 计算机的身份（名称和 IP 地址）。

它还包含在主数据库不可用时建立的当前活动连接的信息：

- Citrix Receiver 执行的任何客户端计算机端点分析的结果。
- 与站点相关的基础结构计算机（例如 NetScaler Gateway 和 StoreFront™ 服务器）的身份。

- 用户最近活动的日期、时间和类型。

工作原理

下图说明了正常运行期间本地主机缓存组件和通信路径。



正常运行期间

- 控制器上的*主代理* (Citrix Broker Service) 接受来自 StoreFront 的连接请求。代理与站点数据库通信，以将用户连接到已向控制器注册的 VDA。
- Citrix Config Synchronizer Service (CSS) 大约每 5 分钟检查一次代理，查看是否进行了任何更改。这些更改可以是管理员发起的（例如更改交付组属性），也可以是系统操作（例如计算机分配）。
- 如果自上次检查以来发生了配置更改，CSS 会将信息同步（复制）到 Controller 上的辅助代理。(辅助代理也称为高可用性服务。)

  将复制所有配置数据，而不仅仅是自上次检查以来发生更改的项目。CSS 将配置数据导入到 Controller 上的 Microsoft SQL Server Express LocalDB 数据库中。此数据库称为本地主机缓存数据库。CSS 确保本地主机缓存数据库中的信息与站点数据库中的信息匹配。每次同步时都会重新创建本地主机缓存数据库。

  安装 Controller 时，会自动安装 Microsoft SQL Server Express LocalDB（由本地主机缓存数据库使用）。（从命令行安装 Controller 时，可以禁止安装此项。）本地主机缓存数据库不能在 Controller 之间共享。您无需备份本地主机缓存数据库。每次检测到配置更改时，都会重新创建该数据库。
- 如果自上次检查以来未发生任何更改，则不会复制任何数据。

下图说明了如果主代理与站点数据库失去联系（中断开始）时通信路径的变化。



中断期间

中断开始时：

- 辅助代理开始侦听和处理连接请求。
- 中断开始时，辅助代理没有当前的 VDA 注册数据，但是当 VDA 与其通信时，会触发注册过程。在此过程中，辅助代理还会获取有关该 VDA 的当前会话信息。

- 当辅助代理正在处理连接时，代理主体会继续监视连接。连接恢复后，代理主体会指示辅助代理停止侦听连接信息，并且代理主体会恢复代理操作。VDA 下次与代理主体通信时，会触发注册过程。辅助代理会删除上次中断中剩余的任何 VDA 注册。当 CSS 得知部署中发生了配置更改时，它会恢复同步信息。

万一在同步期间发生中断，则会丢弃当前导入，并使用上次已知的配置。

事件日志 提供有关同步和中断的信息。

在中断模式下运行没有时间限制。

正常模式和中断模式之间的转换不会影响现有会话。它仅影响新会话的启动。

您也可以有意地触发中断。有关这样做的原因和方法，请参阅强制中断。

具有多个 Controller 的站点

除其他任务外，CSS 会定期向辅助代理提供有关区域中所有 Controller 的信息。（如果您的部署不包含多个区域，则此操作会影响站点中的所有 Controller。）有了这些信息，每个辅助代理都会了解区域中其他 Controller 上运行的所有对等辅助代理。

辅助代理通过单独的通道相互通信。这些代理使用其运行所在计算机的 FQDN 名称的字母顺序列表来确定（选举）哪个辅助代理将在发生中断时代理区域中的操作。中断期间，所有 VDA 都向选定的辅助代理注册。区域中未选定的辅助代理会主动拒绝传入连接和 VDA 注册请求。

如果选定的辅助代理在中断期间发生故障，则会选举另一个辅助代理接管，并且 VDA 会向新选定的辅助代理注册。

中断期间，如果 Controller 重新启动：

- 如果该 Controller 不是选定的代理，则重新启动没有影响。
- 如果该 Controller 是选定的代理，则会选举另一个 Controller，导致 VDA 注册。重新启动的 Controller 通电后，它会自动接管代理，这会导致 VDA 再次注册。在这种情况下，注册期间的性能可能会受到影响。

如果在正常操作期间关闭 Controller，然后在中断期间将其打开，则如果该 Controller 被选为代理，则无法在该 Controller 上使用本地主机缓存。

事件日志提供了有关选举的信息。

中断期间不可用的功能以及其他差异

在中断模式下运行没有时间限制。但是，Citrix 建议尽快恢复连接。

中断期间：

- 您无法使用 Studio。
- 您对 PowerShell SDK 的访问权限有限。
    - 您必须首先：
        - 添加注册表项 `EnableCssTestMode`，其值为 1：`New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
        - 使用端口 89：`Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
    - 运行这些命令后，您可以访问：
        - 所有 `Get-Broker*` cmdlet。
- 无法从主机服务获取管理程序凭据。所有计算机都处于未知电源状态，并且无法发出任何电源操作。但是，主机上已开机的虚拟机可用于连接请求。
- 只有在正常运行期间进行分配的计算机才能使用。在中断期间无法进行新的分配。
- 无法自动注册和配置远程电脑访问计算机。但是，在正常运行期间注册和配置的计算机是可用的。
- 如果资源位于不同的区域，服务器托管的应用程序和桌面用户使用的会话数可能超过其配置的会话限制。
- 用户只能从包含当前活动/选定辅助代理的区域中的已注册 VDA 启动应用程序和桌面。在中断期间，不支持跨区域启动（从一个区域的辅助代理到另一个区域的 VDA）。
- 如果在交付组中 VDA 的计划重启开始之前发生站点数据库中断，则重启将在中断结束时开始。这可能会导致意外结果。有关详细信息，请参阅因数据库中断而延迟的计划重启。
- 无法配置区域首选项。如果已配置，则在会话启动时不考虑首选项。
- 会话启动不支持使用标签指定区域的标签限制。当配置此类标签限制并启用 StoreFront 商店的高级运行状况检查选项时，会话可能会间歇性地启动失败。

应用程序和桌面支持

LHC 支持以下类型的 VDA 和交付模型：

VDA 类型	交付模型	LHC 事件期间的 VDA 可用性
多会话操作系统	应用程序和桌面	始终可用。
单会话操作系统静态（已分配）	桌面	始终可用。
电源管理的单会话操作系统随机（池化）	桌面	默认情况下不可用。默认情况下，所有针对池化交付组中电源管理的 VDA 的会话启动尝试都将失败。您可以使它们在 LHC 事件期间可用于新连接。有关详细信息，请参阅使用 Web Studio 启用 和 使用 PowerShell 启用。 **重要提示：** 启用对电源管理的单会话池化计算机的访问可能会导致先前用户会话中的数据和更改出现在后续会话中。

注意：

在池式交付组中启用对电源管理的桌面 VDA 的访问不会影响配置的 `ShutdownDesktopsAfterUse` 属性在正常操作期间的工作方式。在 LHC 期间启用对这些桌面的访问后，VDA 不会在 LHC 事件完成后自动重新启动。池式交付组中电源管理的桌面 VDA 可以保留以前会话的数据，直到 VDA 重新启动。VDA 重新启动可能发生在用户在非 LHC 操作期间注销 VDA 时，或者管理员重新启动 VDA 时。

使用 Web Studio 为电源管理的单会话操作系统池式 VDA 启用 LHC

使用 Web Studio，您可以按交付组使这些计算机在 LHC 事件期间可用于新连接：

- 要在创建交付组期间启用此功能，请参阅 创建交付组。
- 要为现有交付组启用此功能，请参阅管理交付组。

> **注意：**
>
> 此设置仅在 Web Studio 中适用于提供电源管理的 VDA 的池式桌面交付组。

使用 PowerShell 为电源管理的单会话操作系统池化 VDA 启用 LHC

要为特定交付组中的 VDA 启用 LHC，请按照以下步骤操作：

1. 通过运行此命令在站点级别启用此功能：

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. 通过运行此命令并指定交付组名称来为交付组启用 LHC：

   ```
   Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
   ```

要更改新创建的、具有电源管理型 VDA 的池化交付组的默认 LHC 可用性，请运行以下命令：

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

RAM 大小注意事项

LocalDB 服务大约可以使用 1.2 GB RAM（数据库缓存最多 1 GB，运行 SQL Server Express LocalDB 额外 200 MB）。如果中断持续时间较长且发生大量登录（例如，12 小时内有 1 万用户），则辅助代理最多可以使用 1 GB RAM。这些内存要求是控制器正常 RAM 要求之外的，因此您可能需要增加 RAM 总容量。

如果将 SQL Server Express 安装用于站点数据库，则服务器将有两个 sqlserver.exe 进程。

CPU 核心和套接字配置注意事项

控制器的 CPU 配置，特别是 SQL Server Express LocalDB 可用的核心数量，直接影响本地主机缓存性能，甚至比内存分配影响更大。此 CPU 开销仅在数据库无法访问且辅助代理处于活动状态的中断期间观察到。

虽然 LocalDB 可以使用多个核心（最多 4 个），但它仅限于单个套接字。添加更多套接字不会提高性能（例如，4 个套接字，每个套接字 1 个核心）。相反，Citrix 建议使用多个套接字和多个核心。在 Citrix 测试中，2x3（2 个套接字，3 个核心）配置比 4x1 和 6x1 配置提供更好的性能。

存储注意事项

在中断期间，随着用户访问资源，LocalDB 会增长。例如，在以每秒 10 次登录运行的登录/注销测试期间，数据库每 2-3 分钟增长 1 MB。当正常操作恢复时，本地数据库会重新创建并释放空间。但是，安装 LocalDB 的驱动器上必须有足够的空间，以允许数据库在中断期间增长。本地主机缓存在中断期间还会产生更多 I/O：大约每秒 3 MB 的写入，以及数十万次读取。

性能注意事项

在中断期间，一个辅助代理处理所有连接，因此在正常操作期间在多个控制器之间进行负载平衡的站点（或区域）中，选定的辅助代理可能需要在中断期间处理比平时更多的请求。因此，CPU 需求会更高。站点（区域）中的每个辅助代理都必须能够处理本地主机缓存数据库和所有受影响的 VDA 施加的额外负载，因为在中断期间选定的辅助代理可能会更改。

VDI 限制：

- 在单区域 VDI 部署中，中断期间可有效处理多达 10,000 个 VDA。
- 在多区域 VDI 部署中，在中断期间，每个区域最多可有效处理 10,000 个 VDA，站点中最多可处理 40,000 个 VDA。例如，在中断期间，以下每个站点都可以得到有效处理：
  - 一个包含四个区域的站点，每个区域包含 10,000 个 VDA。
  - 一个包含七个区域的站点，其中一个区域包含 10,000 个 VDA，另外六个区域每个包含 5,000 个 VDA。

在中断期间，站点内的负载管理可能会受到影响。负载评估器（尤其是会话计数规则）可能会超出限制。

在所有 VDA 向辅助代理注册期间，该服务可能没有关于当前会话的完整信息。因此，在此间隔期间的用户连接请求可能会导致启动新会话，即使可以重新连接到现有会话。此间隔（即“新”辅助代理在重新注册期间从所有 VDA 获取会话信息的时间）是不可避免的。中断开始时已连接的会话在转换间隔期间不受影响，但新会话和会话重新连接可能会受到影响。

每当 VDA 必须注册时，就会出现此间隔：

- 中断开始：从主代理迁移到辅助代理时。
- 中断期间辅助代理故障：从发生故障的辅助代理迁移到新选出的辅助代理时。
- 从中断中恢复：当正常操作恢复且主代理恢复控制时。

您可以通过降低 Citrix Broker Protocol 的 `HeartbeatPeriodMs` 注册表值来缩短间隔（默认值 = 600000 毫秒，即 10 分钟）。此心跳值是 VDA 用于 ping 的间隔的两倍，因此默认值会导致每 5 分钟 ping 一次。

例如，以下命令将心跳更改为五分钟（300000 毫秒），这将导致每 2.5 分钟 ping 一次：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name
HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

更改心跳值时请务必小心。增加频率会导致控制器在正常模式和中断模式下负载增加。

无论 VDA 注册速度多快，都无法完全消除此间隔。

辅助代理之间同步所需的时间会随着对象数量（例如 VDA、应用程序、组）的增加而增加。例如，同步 5000 个 VDA 可能需要 10 分钟或更长时间才能完成。

与 XenApp 6.x 版本的差异

尽管此本地主机缓存实现与 XenApp 6.x 及更早的 XenApp 版本中的本地主机缓存功能同名，但它具有显著改进。此实现更强大且不易损坏。维护要求降至最低，例如，无需定期执行 `dsmaint` 命令。此本地主机缓存从技术上讲是完全不同的实现。

管理本地主机缓存

为使本地主机缓存正常工作，每个控制器上的 PowerShell 执行策略必须设置为 RemoteSigned、Unrestricted 或 Bypass。

SQL Server Express 本地数据库

当您安装控制器或从早于 7.9 的版本升级控制器时，本地主机缓存使用的 Microsoft SQL Server Express LocalDB 软件会自动安装。只有辅助代理与此数据库通信。您不能使用 PowerShell cmdlet 更改此数据库的任何内容。LocalDB 不能在控制器之间共享。

无论是否启用本地主机缓存，都会安装 SQL Server Express LocalDB 数据库软件。

为防止其安装，请使用 `XenDesktopServerSetup.exe` 命令安装或升级控制器，并包含 `/exclude "Local Host Cache Storage (LocalDB)"` 选项。但是，请记住，如果没有此数据库，本地主机缓存功能将无法工作，并且您不能将其他数据库与辅助代理一起使用。

此 LocalDB 数据库的安装对您是否安装 SQL Server Express 作为站点数据库没有影响。

有关用较新版本替换早期 SQL Server Express LocalDB 版本的信息，请参阅 替换 SQL Server Express LocalDB。

产品安装和升级后的默认设置

在全新安装 Citrix Virtual Apps and Desktops（最低版本 7.16）期间，本地主机缓存已启用。

升级到版本 7.16 或更高版本后，如果整个部署中的 VDA 少于 10,000 个，则启用本地主机缓存。

启用和禁用本地主机缓存

- 要启用本地主机缓存，请输入：

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  要确定本地主机缓存是否已启用，请输入 `Get-BrokerSite`。检查 `LocalHostCacheEnabled` 属性是否为 `True`。

- 要禁用本地主机缓存，请输入：

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

请记住：自 XenApp 和 XenDesktop 7.16 起，连接租用（在版本 7.6 中引入，早于本地主机缓存的功能）已从产品中移除，不再可用。

验证本地主机缓存是否正常工作

要验证本地主机缓存是否已正确设置并正常工作：

- 确保同步导入成功完成。检查事件日志。
- 确保已在每个 Delivery Controller 上创建 SQL Server Express LocalDB 数据库。这确认了辅助代理可以在需要时接管。
  - 在 Delivery Controller 服务器上，浏览到 `C:\Windows\ServiceProfiles\NetworkService`。
  - 验证 `HaDatabaseName.mdf` 和 `HaDatabaseName_log.ldf` 已创建。
- 在 Delivery Controller 上强制中断。验证本地主机缓存正常工作后，请记住将所有 Controller 恢复到正常模式。这大约需要 15 分钟。

事件日志

事件日志指示同步和中断发生的时间。在事件查看器日志中，中断模式称为 *HA 模式*.*

配置同步器服务：

在正常操作期间，当 CSS 使用本地主机缓存代理将配置数据导入本地主机缓存数据库时，可能会发生以下事件。

- 503：Citrix 配置同步服务收到更新的配置。此事件表示同步过程的开始。
- 504：Citrix 配置同步服务导入了更新的配置。配置导入成功完成。

- 505：Citrix 配置同步服务导入失败。配置导入未成功完成。如果存在以前成功的配置，则在发生中断时将使用该配置。但是，它将与当前配置不同步。如果没有可用的以前配置，则服务在中断期间无法参与会话代理。在这种情况下，请参阅故障排除部分，并联系 Citrix 支持。
- 507：Citrix 配置同步服务放弃了导入，因为系统处于中断模式，并且正在使用本地主机缓存代理进行代理。服务收到了新配置，但由于发生中断而放弃了导入。这是预期行为。
- 510: 未从主配置服务接收到配置服务配置数据。
- 517: 与主代理通信时出现问题。
- 518: 配置同步脚本已中止，因为辅助代理（高可用性服务）未运行。

高可用性服务：

此服务也称为本地主机缓存代理。

- 3502: 发生中断，本地主机缓存代理正在执行代理操作。
- 3503: 中断已解决，正常操作已恢复。
- 3504: 指示哪个本地主机缓存代理被选中，以及参与选举的其他本地主机缓存代理。
- 3507: 每 2 分钟提供一次本地主机缓存的状态更新，指示本地主机缓存模式在选定的代理上处于活动状态。包含中断摘要，包括中断持续时间、VDA 注册和会话信息。
- 3508: 宣布本地主机缓存不再在选定的代理上处于活动状态，并且正常操作已恢复。包含中断摘要，包括中断持续时间、在本地主机缓存事件期间注册的计算机数量以及在 LHC 事件期间成功启动的数量。
- 3509: 通知本地主机缓存在未选定的代理上处于活动状态。每 2 分钟包含一次中断持续时间，并指示选定的代理。
- 3510: 宣布本地主机缓存不再在未选定的代理上处于活动状态。包含中断持续时间并指示选定的代理。

强制中断

您可能希望故意强制中断。

- 如果您的网络反复出现故障。强制中断直到网络问题解决，可以防止在正常模式和中断模式之间持续转换（以及由此导致的频繁 VDA 注册风暴）。
- 测试灾难恢复计划。
- 帮助确保本地主机缓存正常工作。
- 在更换或维护站点数据库服务器时。

要强制中断，请编辑包含 Delivery Controller 的每台服务器的注册表。在 `HKLM\Software\Citrix\DesktopServer\LHC` 中，创建 `OutageModeForced` 并将其设置为 `REG_DWORD` 到 `1`。此设置指示本地主机缓存代理进入中断模式，无论数据库状态如何。将值设置为 `0` 会使本地主机缓存代理退出中断模式。

要验证事件，请监视 `C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService` 中的 `Current_HighAvailabilityService` 日志文件。

故障排除

当同步导入到本地主机缓存数据库失败并发布 505 事件时，可以使用多种故障排除工具。

CDF 跟踪： 包含 `ConfigSyncServer` 和 `BrokerLHC` 模块的选项。这些选项以及其他代理模块可能会识别出问题。

报告： 如果同步导入失败，您可以生成一份报告。此报告会在导致错误的那个对象处停止。此报告功能会影响同步速度，因此 Citrix 建议在不使用时禁用它。

要启用并生成 CSS 跟踪报告，请输入以下命令：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTML 报告发布在 `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htm`。

生成报告后，输入以下命令以禁用报告功能：

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

导出代理配置： 提供用于调试目的的精确配置。

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

例如，`Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`。

本地主机缓存 PowerShell 命令

您可以使用 PowerShell 命令在 Delivery Controller 上管理本地主机缓存 (LHC)。

PowerShell 模块位于 Delivery Controller 上的以下位置：

`C:\Program Files\Citrix\Broker\Service\ControlScripts`

> **重要提示：**
>
> 仅在 Delivery Controller 上运行此模块。

导入 PowerShell 模块

要导入模块，请在 Delivery Controller 上运行以下命令。

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

用于管理 LHC 的 PowerShell 命令

以下命令可帮助您在 Delivery Controller 上激活和管理 LHC 模式。

命令	功能
`Enable-LhcForcedOutageMode`	将 Broker 置于 LHC 模式。ConfigSync Service 必须已成功创建 LHC 数据库文件，以便 `Enable-LhcForcedOutageMode` 正常运行。此 cmdlet 仅在其运行的 Delivery Controller 上强制启用 LHC。要使 LHC 处于活动状态，必须在区域内的所有 Delivery Controller 上运行此命令。
`Disable-LhcForcedOutageMode`	使 Broker 退出 LHC 模式。此 cmdlet 仅在其运行的 Delivery Controller 上禁用 LHC 模式。必须在区域内的所有 Delivery Controller 上运行 `Disable-LhcForcedOutageMode`。
`Set-LhcConfigSyncIntervalOverride`	设置 Citrix Config Synchronizer Service (CSS) 检查站点内配置更改的间隔。时间间隔范围为 60 秒（一分钟）到 3600 秒（一小时）。此设置仅适用于其运行所在的 Delivery Controller。为了在所有 Delivery Controller 之间保持一致性，请考虑在每个 Delivery Controller 上运行此 cmdlet。例如：`Set-LhcConfigSyncIntervalOverride -Seconds 1200`

命令	功能
`Clear-LhcConfigSyncIntervalOverride`	将 Citrix Config Synchronizer Service (CSS) 检查站点内配置更改的间隔设置为默认值 300 秒（五分钟）。此设置仅适用于其运行所在的 Delivery Controller。为了在所有 Delivery Controller 之间保持一致性，请考虑在每个 Delivery Controller 上运行此 cmdlet。
`Enable-LhcHighAvailabilitySDK`	启用对其运行所在的 Delivery Controller 中所有 `Get-Broker*` cmdlet 的访问。
`Disable-LhcHighAvailabilitySDK`	禁用对其运行所在的 Delivery Controller 中 Broker cmdlet 的访问。

注意：

- 在 Delivery Controller 上运行 `Get-Broker*` cmdlet 时，请使用端口 89。例如：
  - `Get-BrokerMachine -AdminAddress localhost:89`
- 当不在 LHC 模式下时，Delivery Controller 上的 LHC Broker 仅保留配置信息。
- 在 LHC 模式期间，当选的 Delivery Controller 上的 LHC Broker 包含以下信息：
  - 资源状态
  - 会话详细信息
  - VDA 注册
  - 配置信息

在搜索 > 默认视图中监视和管理计算机和会话

注意：

从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web

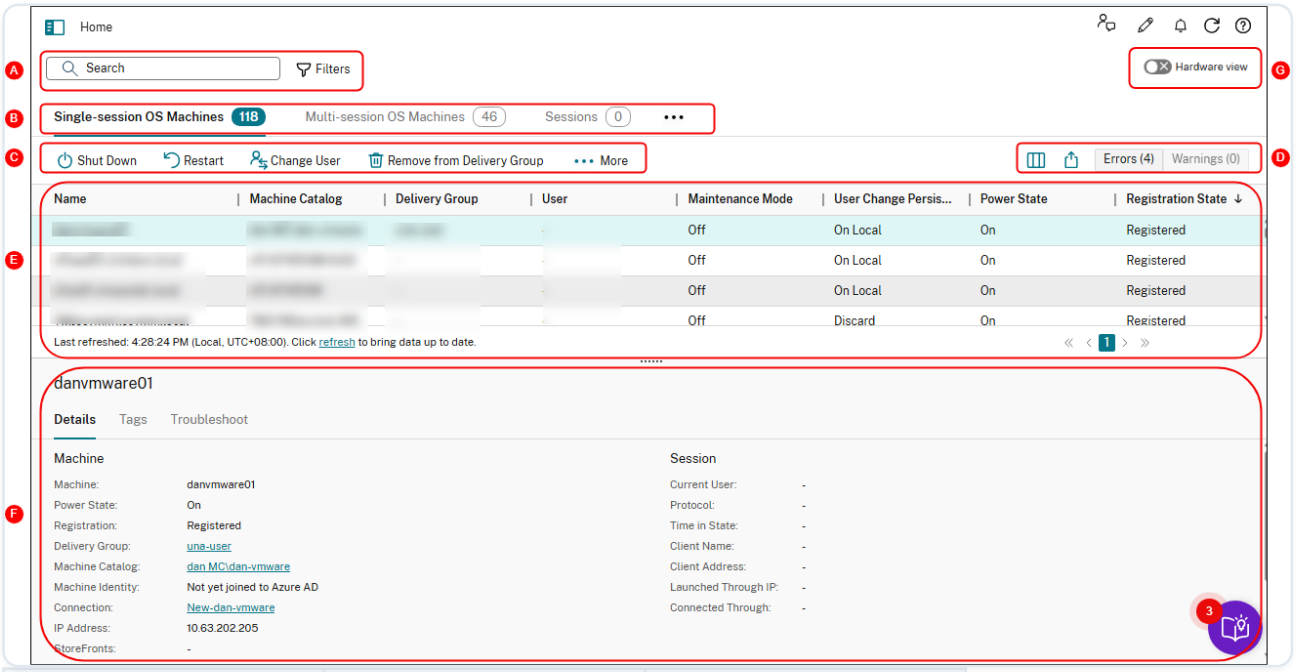
> Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

> 本文指导您如何在 **搜索** 节点中使用默认视图监视和管理计算机和会话。它包括以下主题：

- 了解默认视图
- 搜索计算机和会话
- 自定义要显示的列
- 管理计算机和会话
- 将计算机或会话数据导出到 CSV 文件

了解默认视图

“**搜索**”节点中的默认视图提供了一个集中位置，用于监视和管理计算机和用户会话。



标注	区域	描述
A	搜索栏	提供快速搜索和基于过滤器的搜索，允许您定义复杂的搜索条件。有关详细信息，请参阅搜索实例。
B	类型选项卡	显示选项卡以按类型列出计算机或列出所

标注	区域	描述
		有会话。实例计数显示在选项卡名称中。
C	实例级操作	显示可对*选定实例*（计算机或会话）执行的操作。有关详细信息，请参阅计算机操作和会话操作。
D	列表级操作	显示您可以对当前*列表*执行的操作： • **导出**图标：将主视图中显示的实例列表导出到 CSV 文件。 • **要显示的列**图标：自定义列表的主视图。 • **错误** 标签：启用此标签可在主视图中仅显示具有错误的未注册计算机。要查看问题详细信息，请转到**详细信息**窗格中的**故障排除**选项卡。 • **警告** 标签：启用此标签可在主视图中仅显示具有警告的未注册计算机。要查看问题详细信息，请转到**详细信息**窗

标注	区域	描述
		格中的**故障排除**选项卡。
E	主视图	显示实例及其属性。您可以通过选择**列显示**图标来自定义主视图。有关可用列的更多信息，请参阅计算机列和会话列。
F	详细信息窗格	显示以下详细信息: • 所选实例（计算机或会话）的详细信息 • 应用于所选计算机的标签 • 所选计算机的错误或警告详细信息，包括问题、可能的原因和建议的解决方案
G	切换到硬件视图	单击可从默认视图切换到硬件视图。

搜索实例

使用搜索功能查找特定的计算机和会话：

- 使用筛选器搜索
- 保存当前筛选器集以进行快速搜索
- 在搜索栏中固定筛选字段
- 使用快速搜索框进行搜索
- 增强搜索的技巧

使用筛选器进行搜索

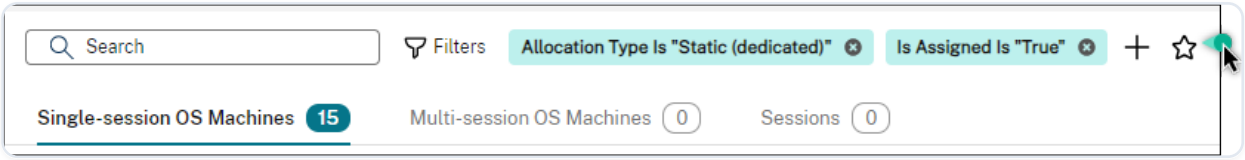
例如，要查找所有*静态*且*已分配给用户*的单会话操作系统计算机，请执行以下步骤：

1. 在**单会话操作系统计算机**选项卡上，单击**筛选器**图标。此时将显示“筛选器”面板。
2. 添加必要的筛选条件。

3. 如果要搜索返回与所有筛选条件匹配的结果，请选择**匹配所有**（AND 运算符）。如果要搜索返回与任何筛选条件匹配的结果，请选择**匹配任意**（OR 运算符）。
4. 单击**应用**。

   筛选后的列表显示所有静态且已分配给用户的单会话操作系统计算机。



保存当前筛选器集以进行快速搜索

例如，要保存静态且已分配给用户的单会话操作系统计算机的筛选器集以供将来使用，请执行以下步骤：

1. 执行基于筛选器的搜索后，单击搜索栏中的**星形**图标，如上图所示。
2. 在显示的页面上，为此筛选器集输入一个名称（例如，*静态和已分配的计算机*）。
3. 单击 **保存**。

   单击搜索框时，保存的筛选器集将显示在搜索历史记录列表中。

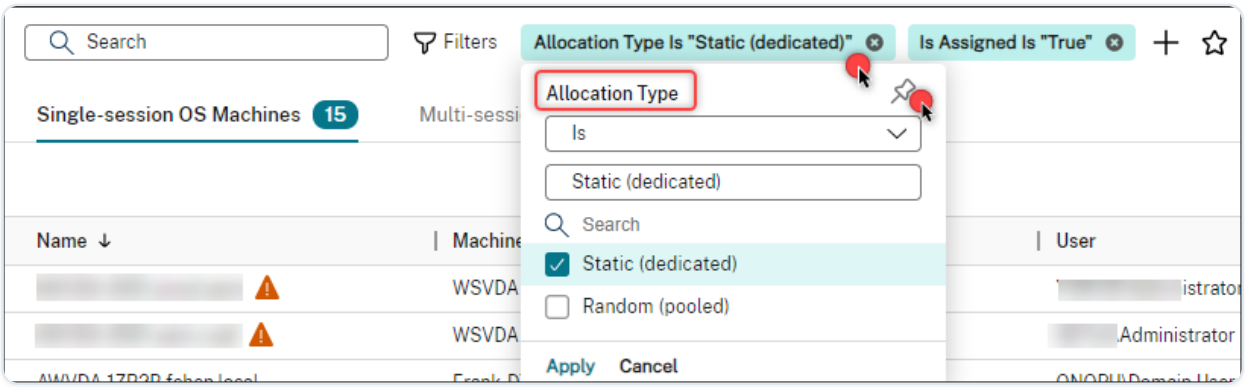
> **注意：**
>
> 筛选器集按用户帐户保存。要管理已保存的筛选器集，请选择**管理**。

在搜索栏中固定筛选字段

将常用筛选器*字段*固定到搜索栏中以便于访问。例如，执行基于筛选器的搜索后，您希望将**分配类型**固定到搜索栏中。请按照以下步骤操作：

1. 单击搜索栏中的*筛选器设置*。

2. 在出现的面板中，单击**固定**图标以将筛选器字段（例如，*分配类型*）固定到搜索栏中。



使用快速搜索框进行搜索

快速搜索框提供了一种便捷方式，可用于基于名称相关属性或已保存的筛选器集搜索实例。详细步骤如下：

1. 单击搜索框。您最近的搜索和已保存的筛选器集将显示在下拉列表中。您可以单击以前的搜索或筛选器集进行快速搜索。
2. 要开始新搜索，请从以下选项中输入完整或部分名称：
   - 计算机名称或 DNS 名称
   - 计算机目录名称
   - 交付组名称
   - 会话用户名
   - 会话客户端名称
   - 托管会话的虚拟机的友好名称，由其管理程序使用
   - 托管服务器名称

增强搜索的技巧

使用搜索功能时，请考虑以下提示：

- 在“**搜索**”节点上，选择任意列以对项目进行排序。
- 要显示更多可在其中搜索和排序的特性，请选择“**要显示的列**”或单击任意列并选择“**要显示的列**”。在“**要显示的列**”窗口中，选中要显示的项目旁边的复选框，然后选择“**保存**”以退出。

> **注意：**
>
> 降低性能的列标有“**降低性能**”标签。

- 要查找连接到计算机的用户设备，请使用“**客户端 (IP)**”和“**是**”，然后输入设备 IP 地址。
- 要查找活动会话，请使用“**会话状态**”、“**是**”和“**已连接**”。
- 要列出交付组中的所有计算机，请在左侧窗格中选择“**交付组**”。选择该组，然后从操作栏或上下文菜单中选择“**查看计算机**”。
- 要通过特定属性快速缩小 MCS 预配的计算机范围，请使用 硬件视图 中提供的“**搜索**”栏。

执行排序操作时，请牢记以下注意事项：

- 只要项目数不超过 5,000，您就可以单击任意列对其进行排序。当数量超过 5,000 时，您只能按名称或当前用户进行排序（具体取决于您所在的选项卡）。要启用排序，请使用筛选器将项目数减少到 5,000 或更少。
- 当项目数量大于 500 但不超过 5,000 时：
  - 我们会在本地缓存所有数据以提高排序性能。在“**单会话操作系统计算机**”和“**多会话操作系统计算机**”选项卡上，首次单击列（除“**名称**”列之外的任何列）进行排序时，我们会缓存数据。在“**会话**”选项卡上，首次单击列（除“**当前用户**”列之外的任何列）进行排序时，我们会缓存数据。因此，排序完成所需的时间会更长。为了获得更快的性能，请按名称或当前用户排序，或使用筛选器减少项目数量。
  - 表下方的以下消息表示数据已缓存：上次刷新时间：`<the time when you refreshed the table>`。在这种情况下，排序操作基于以前加载的项目。这些项目可能不是最新的。要更新它们，请单击刷新图标。

自定义要显示的列

创建个性化的主视图以显示对日常操作至关重要的属性和状态。详细步骤如下：

1. 在“**搜索**”节点中，根据需要选择“**多会话操作系统计算机**”、“**单会话操作系统计算机**”或“**会话**”选项卡。
2. 单击操作栏中的“**要显示的列**”图标并选择列。

   有关可用列及其说明的更多信息，请参阅计算机列和会话列。

选择列时，您会看到标有“**性能下降**”标签的列。选择这些列可能会降低控制台的性能。请记住以下注意事项：

- 完成自定义后，表格会刷新以显示您选择的列。它们的存在可能会导致您刷新表格时出现延迟。
- 刷新浏览器或从控制台注销然后重新登录后，会出现一条消息，询问是否保留这些列。如果您选择保留它们，则为了获得最佳控制台性能，您将受限于每分钟刷新表格的次数不能超过一次。如需更频繁地刷新，请删除任何会降低性能的列。

管理计算机和会话

使用“搜索”节点中的操作来排查计算机和会话问题或处理用户请求。

须知

您可以在不同级别管理计算机：

- 在单个计算机级别。使用**搜索**节点定位目标计算机并执行操作。
- 在计算机目录级别，例如更改目录的主映像、从目录中删除计算机以及向目录中添加计算机。有关详细信息，请参阅管理计算机目录。
- 在交付组级别，例如为组中的计算机启用或禁用维护模式。有关详细信息，请参阅管理交付组。

除了单个会话级别，您还可以在交付组级别管理会话，例如为交付组配置会话预启动和会话保留。有关详细信息，请参阅管理交付组。

对计算机或会话执行操作

要在单个实例级别管理计算机或会话，请按照以下步骤操作：

1. 在**搜索**节点中，选择**多会话操作系统计算机**、**单会话操作系统计算机**或**会话**选项卡。
2. 根据需要选择一个或多个实例。
3. 根据您在这些实例中遇到的问题或用户请求，从操作栏或右键单击菜单中选择一个操作。

   有关可用操作及其说明的更多信息，请参阅计算机操作和会话操作。

> **注意：**
>
> 如果您选择两个或更多实例，则仅显示适用于所有实例的操作。

将计算机或会话数据导出到 CSV 文件

将选项卡上显示的实例（计算机或会话）列表（最多 30,000 个项目）导出到 CSV 文件。详细步骤如下：

1. 在“**搜索**”节点中，根据需要选择“**多会话操作系统计算机**”、“**单会话操作系统计算机**”或“**会话**”选项卡。
2. 在右上角点击“**导出**”图标。
3. 在出现的对话框中，点击“**继续**”。

   导出可能需要几分钟才能完成。您可以在浏览器的默认下载文件夹中找到该文件。

注意：

在“**搜索**”节点的每个选项卡上，当有导出正在进行时，您无法执行另一次导出。

计算机操作和列

本文列出了机器操作和列及其说明，供您参考。

操作

查看您可以对机器执行的操作及其说明。

操作	说明	适用于
从交付组中删除	从交付组中删除计算机。	单会话和多会话
添加到交付组	将计算机添加到交付组。	单会话和多会话
查看会话	查看计算机上运行的会话	单会话和多会话
管理标签	为计算机添加和管理标签。有关标签典型用例的详细信息，请参阅标签。	单会话和多会话
启用维护模式	在应用修补程序或进行故障排除之前，将计算机置于维护模式。 此模式可防止新连接连接到该计算机。用户可以连接到该计算机上的现有会话，但无法在该计算机上启动新会话。	单会话和多会话
禁用维护模式	禁用计算机的维护模式。	单会话和多会话
升级 VDA	升级计算机的 VDA。	满足特定要求的单会话或多会话操作系统计算机：了解更多。
注销	强制注销计算机	单会话和多会话

操作	说明	适用于
删除	从计算机目录中删除 VM，同时使其在虚拟机管理程序或云服务上保持不变。	单会话和多会话
更改用户	将计算机分配给特定用户。	单会话 *静态* 计算机。
启动	启动计算机。	单会话和多会话
关机	关闭计算机。	单会话和多会话
重新启动	重新启动计算机	单会话和多会话
挂起	将机器置于休眠或挂起状态。挂起机器时，Delivery Controller 会将机器的内存内容存储到文件中，然后关闭机器。	单会话操作系统计算机
恢复	恢复已挂起的机器。恢复已挂起的机器时，Delivery Controller 会启动机器并将其恢复到以前的状态。	单会话操作系统计算机
强制重新启动	强制重新启动计算机。	单会话操作系统计算机
强制关机	强制关闭计算机。	单会话操作系统计算机

列

按类型查看所有计算机列及其说明：

- 计算机
- 计算机详细信息
- 应用程序
- 托管
- 连接
- 注册
- 会话详细信息
- 会话

计算机

“**计算机**”类别中的列。

列	描述	适用于
名称	计算机的 DNS 主机名。	单会话和多会话
计算机目录	计算机所属目录的名称。	单会话和多会话
交付组	计算机所属的交付组的名称。	单会话和多会话
用户显示名称	与计算机关联的用户的全名（通常采用 `Firstname Lastname` 形式）。关联用户是共享计算机的当前用户和专用计算机的指定用户。	单会话和多会话
用户	与计算机关联的用户的用户名（采用“domain\user”形式）。关联用户是共享计算机的当前用户和专用计算机的指定用户。	单会话和多会话
用户主体名称	与计算机关联的用户的用户主体名称（采用“user@domain”形式）。关联用户是共享计算机的当前用户和专用计算机的指定用户。	单会话和多会话
桌面显示名称	最初用于启动会话的计算机的已发布名称。这是在 Citrix Workspace™ app 或	仅限单会话

列	描述	适用于
	StoreFront 上显示的名称。	
	注意： 要更改桌面的显示，您需要 **执行计算机更新** 权限，因为更改显示名称涉及更新计算机属性。	
桌面状况	计算机的未决桌面状况列表。可能的值：Unknown、CPU、ICALatency 和 UPMLogonTime。	单会话和多会话
分配类型	计算机的分配类型：**永久**，当永久分配给用户时；**随机**，当随机分配时。	单会话和多会话
维护模式	指示计算机是否处于维护模式。	单会话和多会话
Windows 连接设置	Windows 报告的登录模式。	仅限多会话
	可能的值：LogonEnabled、Draining、DrainingUntilRestart 和 LogonDisabled。	
是否已分配	指示是否已将专用桌面分配给用户或客户端（名称/地址）。用户可以显式分配，也可以通过首次使用计算机时分配。	单会话和多会话
是否为物理机	指示机器是否为物理机。`True` 表示机器是物理机，这意味着	单会话和多会话

列	描述	适用于	
	它不受 Delivery Controller 的电源管理。`False` 表示不是物理机。		
预配类型	计算机的预配方式。可能的值： • 手动：未使用 PVS 或 MCS 预配。 • PVS: 使用 PVS 预配（物理机、刀片服务器和虚拟机） • MCS: 使用 MCS 预配（仅限虚拟机）	单会话和多会话	
计划的重新启动	计算机的任何计划重新启动操作的状态。可能的值： • 无：未计划重新启动。 • 待处理：等待重新启动，但可供使用。 • 正在排空: 等待重启，并且不可用于新会话。但是，仍然允许重新连接到现有连接。	单会话和多会话	

列	描述	适用于
	• 进行中: 正在主动执行计划的重启。 • 自然: 自然重启正在进行中。计算机正在等待重启。	
区域	计算机所在的区域名称。	单会话和多会话
状态	与计算机关联的桌面的总体状态，源自各种特定状态，例如会话状态、注册状态和电源状态。	单会话和多会话
	可能的状态：关机、未注册、可用、已断开连接、正在使用和正在准备。	
标签	与计算机关联的标签列表。	单会话和多会话
VDA 升级	VDA 软件包升级操作的计算机状态。	单会话和多会话
	可能的值：MissingUpgradeType、UpgradeScheduled、UpgradeAvailable、UpToDate 和 Unknown。	

列	描述	适用于
可挂起	指示计算机是否支持电源操作（挂起和恢复）。	单会话和多会话
负载评估器索引	机器的整体有效负载指数（百分比）。有关详细信息，请参阅CTX202150。	仅限多会话
负载索引	当前负载索引。有关详细信息，请参阅 了解更多。	仅限多会话
排空状态	指示计算机是否正在排空，以及在计算机上的所有会话结束后是否将关闭。仅对电源管理的、多会话计算机显示 True。 **注意：** 如果计算机处于维护模式，则不会关机。它只会在退出维护模式后关机。	仅限多会话

计算机详细信息

计算机详细信息类别中的列。

列	说明	适用于
代理版本	计算机上安装的 Citrix Virtual Delivery Agent (VDA) 的版本。	单会话和多会话
IP 地址	计算机的 IP 地址。	单会话和多会话
是否已分配	指示是否已将专用桌面分配给用户或客户端（名称/地址）。用户可以显式分配，也	单会话和多会话

列	说明	适用于
	可以在首次使用计算机时分配。	
操作系统类型	计算机上运行的操作系统类型。	仅限单会话

应用程序

应用程序类别中的列。

列	描述	适用于
正在使用的应用程序	机器上正在使用的应用程序列表（显示为浏览器名称）。	单会话和多会话
已发布的应用程序	机器发布的应用程序列表（显示为浏览器名称）。	单会话和多会话

连接

连接类别中的列。

列	描述	适用于
客户端 (IP)	连接到机器的客户端的 IP 地址。	仅限单会话
客户端	连接到机器的客户端的主机名。	仅限单会话
插件版本	连接客户端上的 Citrix Workspace 应用程序版本。	仅限单会话
连接方式	传入连接的主机名，通常是网关、路由器或客户端。	仅限单会话
连接方式 (IP)	传入连接的 IP 地址，通常是网关、路由器或客户端。	仅限单会话
连接类型	会话使用的协议。可能的值：HDX、RDP 和 Console。注意：对于 XenDesktop® 5	仅限单会话

列	描述	适用于
	VDA 上的控制台会话，此字段留空。	
上次连接时间 (UTC)	上次检测到的连接尝试（无论是失败还是成功）的时间。	单会话和多会话
上次连接用户	上次尝试连接到此计算机的用户的 SAM 名称（格式为“DOMAIN\user”）。如果 SAM 名称不可用，则使用 SID。	单会话和多会话
Secure ICA® 活动	指示 SecureICA 是否在当前会话中处于活动状态。对于多会话计算机，始终为空。	单会话和多会话

托管

托管类别中的列。

列	描述	适用于
VM	运行会话的托管计算机的友好名称，由其管理程序使用。它不一定与计算机的 DNS 或 AD 名称匹配。	单会话和多会话
托管服务器名称	如果受管理，则为托管计算机的管理程序 DNS 名称。	单会话和多会话
连接	分配给托管会话的计算机的主机连接名称。	单会话和多会话
待定更新	指示托管计算机的 VM 映像是否已过期，以及是否应在计算机下次重新启动时更新为新映像。	单会话和多会话

列	描述	适用于
用户更改持久性	用户更改的处理方式，指示更改是否持久： • OnLocal: 持久。用户更改将本地保存。 丢弃：非持久性。用户更改将被丢弃。	单会话和多会话
待处理电源操作	指示该计算机是否有任何待处理的电源操作。	单会话和多会话
电源状态	计算机的电源状态。可能的值：未管理、未知、不可用、关机、开机、已挂起、正在开机、正在关机、正在挂起和正在恢复。	单会话和多会话
使用后将关机	仅适用于采用电源管理的单会话计算机。指示计算机是否已受污染，以及是否将在所有会话结束后关机。 **注意：** 如果计算机处于维护模式，则不会关机。只有在退出维护模式后才会关机。	仅限单会话

注册

注册类别中的列。

列	描述	适用于
上次注册失败	计算机上次与代理注销的原因。 可能的值包括：AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure,	单会话和多会话

列	描述	适用于
	SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError, and BrokerRegistrationLimitReached。	
上次注册失败时间 (UTC)	计算机上次注销的时间。	单会话和多会话
注册状态	计算机的注册状态。可能的值：Unregistered、Initializing、Registered 和 AgentError。	单会话和多会话
故障状态	计算机当前任何故障状态的摘要状态。可能的值： • 无：无故障。计算机运行正常。 • FailedToStart：计算机上次开机操作失败。 • StuckOnBoot：计算机开机后未能启动。	单会话和多会话
	未注册。计算机未在预期时间内注册，或其注册已被拒绝。	
	最大容量。计算机报告其已达到最大容量。	

会话详细信息

会话详细信息类别中的列。

列	描述	适用于
启动来源	用于启动当前代理会话的 StoreFront 服务器的主机名。对于多会话计算机，此值始终为 null。	单会话和多会话
启动来源 (IP)	用于启动当前代理会话的 StoreFront 服务器的 IP 地址。对于多会话计算机，此值始终为 null。	单会话和多会话
会话更改时间 (UTC)	当前会话上次状态更改的时间。	仅限单会话
SmartAccess 筛选器	当前会话的 Smart Access 标签。对于多会话计算机始终为 null。	单会话和多会话

会话

会话类别中的列。

列	说明	适用于
会话状态	当前会话的状态。可能的值：Other、PreparingSession、Connected、Active、Disconnected、Reconnecting、NonBrokeredSession 和 Unknown。	仅限单会话
当前用户	当前会话用户的名称（格式为“DOMAIN\user”）。	仅限单会话
开始时间 (UTC)	当前会话的开始时间。	仅限单会话
会话计数	计算机上的会话数量。	仅限多会话

会话操作和列

本文列出了机器操作和列及其说明，供您参考。

操作

查看可对会话执行的操作及其说明。

操作	描述	适用于以下会话
注销	将用户从会话注销。	单会话操作系统计算机或多会话操作系统计算机
发送消息	向会话用户发送消息。	单会话操作系统计算机或多会话操作系统计算机
查看计算机	查看会话的托管计算机。	单会话操作系统计算机或多会话操作系统计算机
断开连接	断开会话连接。如果会话断开连接，它仍处于活动状态，其应用程序将继续运行，但用户设备不再与 Delivery Controller 通信。	单会话操作系统计算机或多会话操作系统计算机
关闭计算机	关闭与会话关联的计算机。	单会话操作系统计算机
重新启动计算机	重新启动与会话关联的计算机。	单会话操作系统计算机

列

查看会话列及其说明。

列	描述
当前用户	用户的名称；用户的用户主体名称 (UPN)。
名称	托管会话的计算机的 DNS 主机名。
交付组	包含会话托管计算机的交付组的名称。

列	描述
计算机目录	包含会话托管计算机的计算机目录的名称。
代理版本	托管会话的计算机上安装的 Citrix Virtual Delivery Agent (VDA) 版本。
正在使用的应用程序	会话中正在使用的应用程序列表，按其管理名称标识。
自主代理	这是否是通过直接连接建立的 HDX™ 会话，而无需通过代理。
代理时间 (UTC)	会话被代理的时间。
代理用户名	代理用户的名称。
客户端 (IP)	连接到会话的客户端的 IP 地址。
客户端	连接到会话的客户端的主机名。
插件版本	连接到会话的客户端上运行的 Citrix Workspace™ 应用程序的版本。
连接方式	传入连接的主机名，通常是网关、路由器或客户端。
连接方式 (IP)	传入连接的 IP 地址，通常是网关、路由器或客户端。
分配类型	会话是共享还是专用。
隐藏	会话是否对用户隐藏且不应重新连接。
VM	托管会话的虚拟机的友好名称，由其管理程序使用。它不

列	描述
	一定与计算机的 DNS 名称或 AD 名称匹配。
托管服务器名称	托管会话主机的管理程序的 DNS 名称。
连接	分配给托管会话的计算机的主机连接名称。
待定更新	托管计算机的虚拟机映像是否已过期，并将在计算机下次重新启动时更新为新映像。
维护模式	托管会话的计算机是否处于维护模式。
IP 地址	托管会话的计算机的 IP 地址。
是否为物理机	托管会话的计算机是物理机还是非物理机。`True` 表示该计算机是物理机，这意味着它不受 Delivery Controllers 的电源管理。`False` 表示非物理机。
启动来源	用于启动会话的 StoreFront™ 服务器的主机名。如果会话是通过 Workspace 启动的，则为空白。
启动来源 (IP)	用于启动会话的 StoreFront 服务器的 IP 地址。如果会话是通过 Workspace 启动的，则为空白。
操作系统类型	托管会话的操作系统的标识字符串。
用户更改持久性	用户更改的处理方式，指示更改是否持久：

列	描述
	• OnLocal: 持久。用户更改将本地保存。 丢弃：非持久性。用户更改将被丢弃。
连接类型	会话使用的协议，例如 HDX、RDP 或 Console。 **注意：** 对于 XenDesktop® 5 VDA 上的控制台会话，此字段为空白。
预配类型	托管会话的计算机的预配方式: • 手动：未使用 PVS 或 MCS 预配。 • PVS: 由 PVS 预配（物理机、刀片服务器和虚拟机）。 • MCS: 由 MCS 预配（仅限虚拟机）。
Secure ICA® 活动	SecureICA 是否在会话上处于活动状态。
会话状态	会话状态。可能的值：Connected、Active 或 Disconnected。对于功能级别低于 L7 的计算机上的会话，可能会出现其他状态，例如 PreparingSession、Reconnecting、NonBrokeredSession、Other 和 Unknown。
会话更改时间	会话最近一次状态更改的时间。

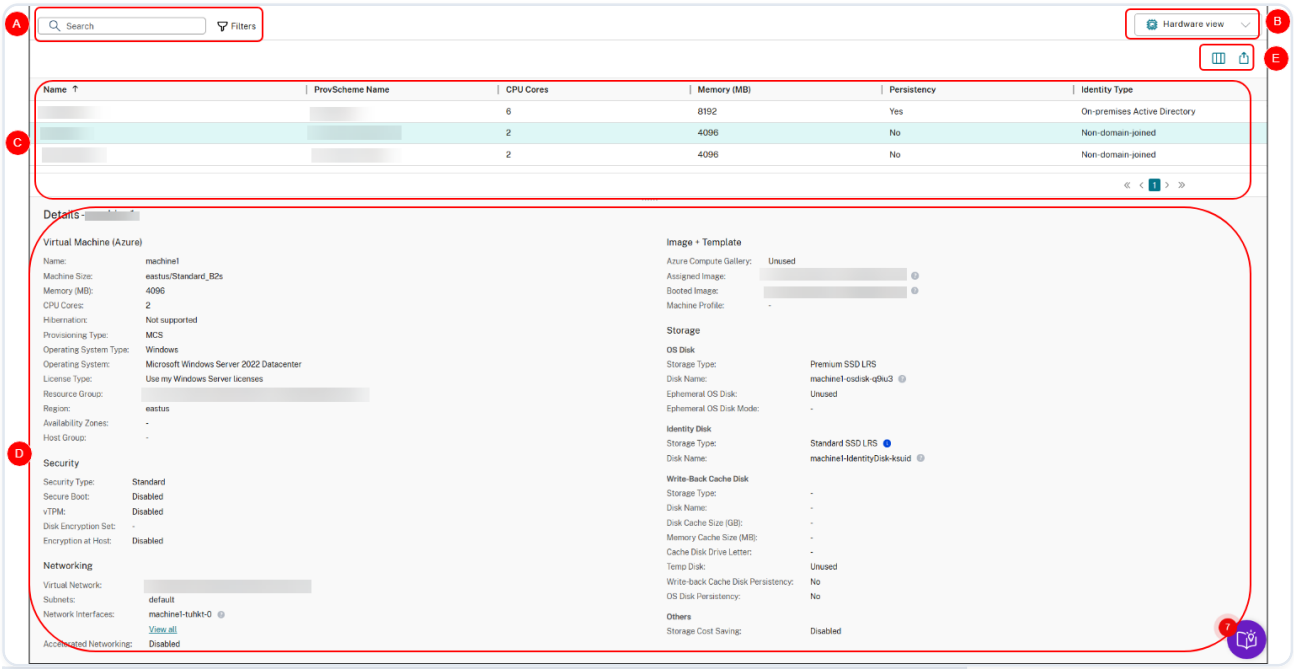
列	描述
应用程序状态	会话中应用程序的状态。可能的值：PreLogon、PreLaunched、Active、Desktop、Lingering 和 NoApps。
会话支持	托管会话的计算机是支持多会话还是单会话。
区域	托管会话的计算机所在区域的名称。
SmartAccess 筛选器	会话的智能访问标签。
开始时间 (UTC)	会话启动时间。
状态	计算机的摘要状态。可能的值：未注册、已断开连接或正在使用。
处于此状态的时间 (UTC)	会话处于当前状态的时长。
交付控制器™	会话托管计算机注册到的控制器的 DNS 主机名。
用户显示名称	用户的全名。
桌面显示名称	最初用于启动会话的计算机的已发布名称。这是在 Citrix Workspace 应用程序或 StoreFront 上显示的名称。对于应用程序会话，它是启动到会话中的第一个应用程序的名称，即使该应用程序后来已结束。即使资源后来被重命名或删除，该名称也保持不变。

监控 搜索 > 硬件视图 中的 MCS 预配的计算机

本文指导您如何在 **搜索** 节点中使用 **硬件视图** 查看 MCS 预配的计算机及其属性。

了解硬件视图

“**搜索**”节点中的“硬件视图”显示您的 MCS 预配计算机及其关键属性，包括计算机安全设置、网络详细信息、映像和计算机配置文件详细信息。



标注	区域	说明	
A	搜索栏	提供快速搜索和基于筛选器的搜索，允许您定义复杂的搜索条件。有关详细信息，请参阅 搜索计算机。**提示：** 使用筛选器可根据特定属性快速缩小计算机范围。例如，结合 **待处理映像更新 = 是** 和 **身份类型 = ActiveDirectory** 以查看所有待处理映像更新的 Active Directory 计算机。	
B	切换到默认视图	从硬件视图切换到默认视图。	

标注	区域	说明
C	主视图	显示您的 MCS 预配计算机及其关键属性。您可以通过选择“**要显示的列**”图标来自定义视图。有关可用列的更多信息，请参阅计算机列。
D	详细信息窗格	显示所选计算机的详细信息。
E	列表级操作	显示您可以对整个显示列表执行的操作： • **导出**图标：将主视图中显示的计算机列表导出到 CSV 文件。 • **要显示的列**图标：自定义列表的主视图。

参考：计算机列

此表列出了硬件视图中的所有列及其说明。

列	描述
名称	计算机的 DNS 主机名。
预配方案名称	用于预配计算机的预配方案的名称。
CPU 核心数	分配给计算机的 CPU 核心数。
内存 (MB)	分配给计算机的内存量 (MB)。
持久性	指示计算机的磁盘和数据是否在重新启动后仍然保留。

列	描述
身份类型	计算机的身份类型。
待处理的映像更新	指示计算机的 VM 映像是否已过时，以及是否应在计算机下次重新启动时更新为新映像。
上次启动时间 (UTC)	计算机上次启动的日期和时间 (UTC)。
使用 WBC	指示计算机是否配置了 WBC（也称为 MCSIO）。
WBC 磁盘大小 (GB)	计算机的 MCSIO 磁盘缓存大小。
WBC 内存大小 (MB)	计算机的 MCSIO 内存缓存大小。
身份提供程序	计算机的身份提供程序。
激活类型	仅适用于 Windows VDA。计算机的 Windows 许可证激活类型。值包括：不支持的 VDA、密钥管理服务、多重激活密钥和无效。

管理安全密钥

重要提示：

- 您必须将此功能与 StoreFront™ 1912 LTSR CU2 或更高版本结合使用。
- Secure XML 功能仅在 Citrix ADC 和 Citrix Gateway 12.1 及更高版本上受支持。

注意：

从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

> 此功能允许您仅授权经批准的 StoreFront 和 Citrix Gateway 计算机与 Delivery Controller 通信。启用此功能后，不包含密钥的任何请求都将被阻止。使用此功能可增加一层额外的安全性，以防范源自内部网络的攻击。

使用此功能的通用工作流程如下：

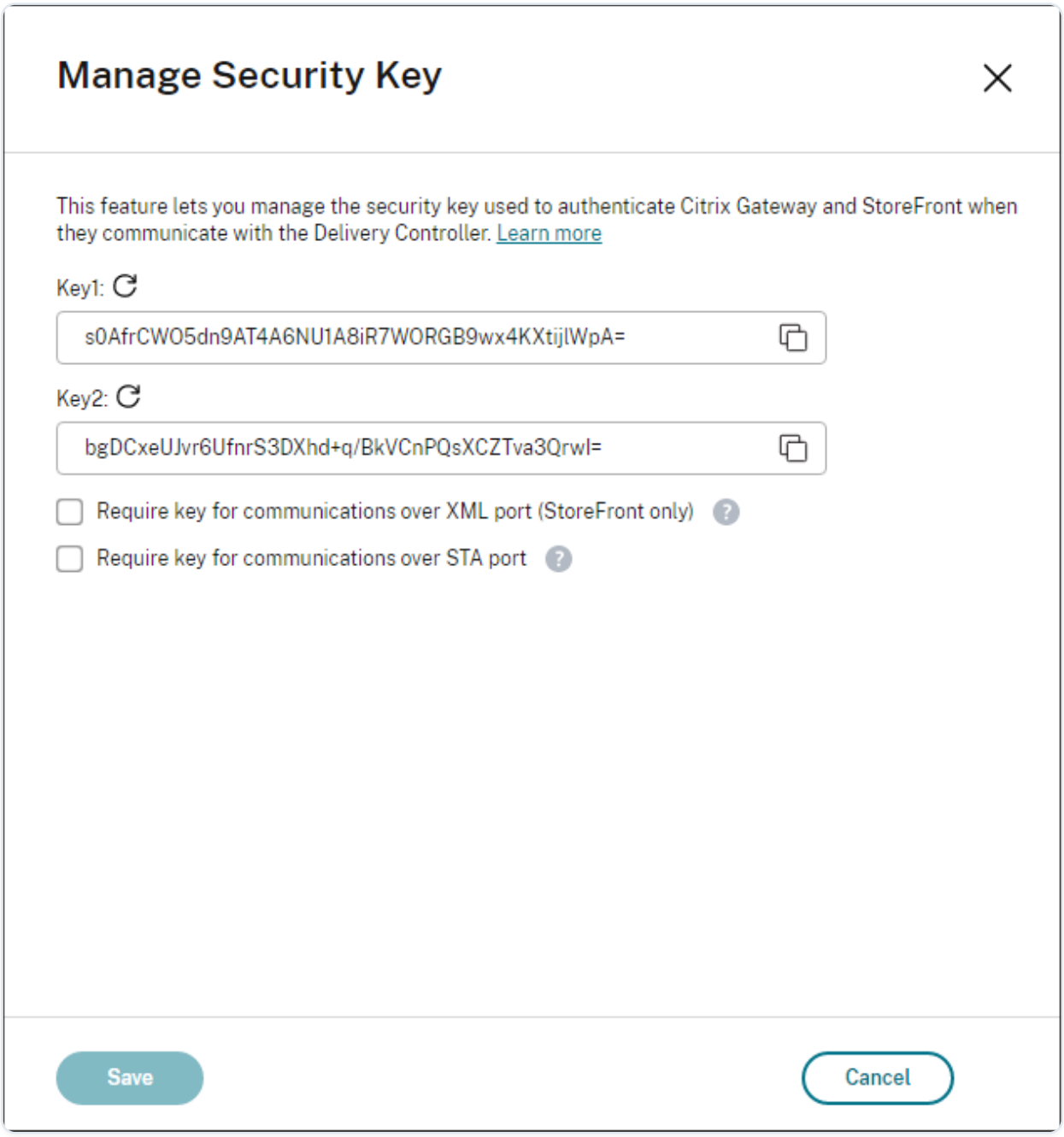
1. 启用 Web Studio 以显示功能设置。
2. 配置站点的设置。
3. 配置 StoreFront 的设置。
4. 配置 Citrix ADC 的设置。

配置站点的设置

您可以使用 Web Studio 或 PowerShell 为您的站点配置安全密钥设置。

使用 Web Studio

1. 登录 Web Studio，在左侧窗格中选择**设置**。
2. 找到 **Manage security key** 磁贴，然后单击 **Edit**。将显示 **Manage Security Key** 页面。



3. 单击刷新图标以生成密钥。

重要提示：

- 有两个可用的密钥。您可以对通过 XML 和 STA 端口进行的通信使用相同密钥或不同密钥。我们建议您一次只使用一个密钥。未使用的密钥仅用于密钥轮换。
- 请勿单击刷新图标来更新已在使用的密钥。否则，服务将中断。

4. 选择通信需要密钥的位置：

- **要求通过 XML 端口进行通信时使用密钥（仅限 StoreFront）**。如果选中此选项，则要求使用密钥对通过 XML 端口进行的通信进行身份验证。StoreFront 通过此端口与 Citrix Cloud 通信。有关更改 XML 端口的信息，请参阅知识中心文章 CTX127945。
- **要求通过 STA 端口进行通信时使用密钥**。如果选中此选项，则要求使用密钥对通过 STA 端口进行的通信进行身份验证。Citrix Gateway 和 StoreFront 通过此端口与 Citrix Cloud 通信。有关更改 STA 端口的信息，请参阅知识中心文章 CTX101988。

5. 单击 **Save** 以应用更改并关闭窗口。

使用 PowerShell

以下是与 Web Studio 操作等效的 PowerShell 步骤。

1. 运行 Citrix 虚拟应用和桌面™ 远程 PowerShell SDK。
2. 在命令窗口中，运行以下命令：
   - `Add-PSSnapIn Citrix*`
3. 运行以下命令以生成密钥并设置 Key1：
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. 运行以下命令以生成密钥并设置 Key2：
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. 运行以下一个或两个命令以启用密钥用于身份验证通信：
   - 要通过 XML 端口验证通信：
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - 要通过 STA 端口验证通信：
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

有关指导和语法，请参阅 PowerShell 命令帮助。

配置 StoreFront 的设置

完成站点的配置后，您需要使用 PowerShell 为 StoreFront 配置相关设置。

在 StoreFront 服务器上，运行以下 PowerShell 命令：

要配置用于通过 XML 端口进行通信的密钥，请使用命令。例如：

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

为以下参数输入相应的值：

- `Path to store`
- `Resource feed name`
- `secret`

要配置通过 STA 端口进行通信的密钥，请使用 `New-STFSecureTicketAuthority` 和 `Set-STFRoamingGateway` 命令。例如：

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

为以下参数输入相应的值：

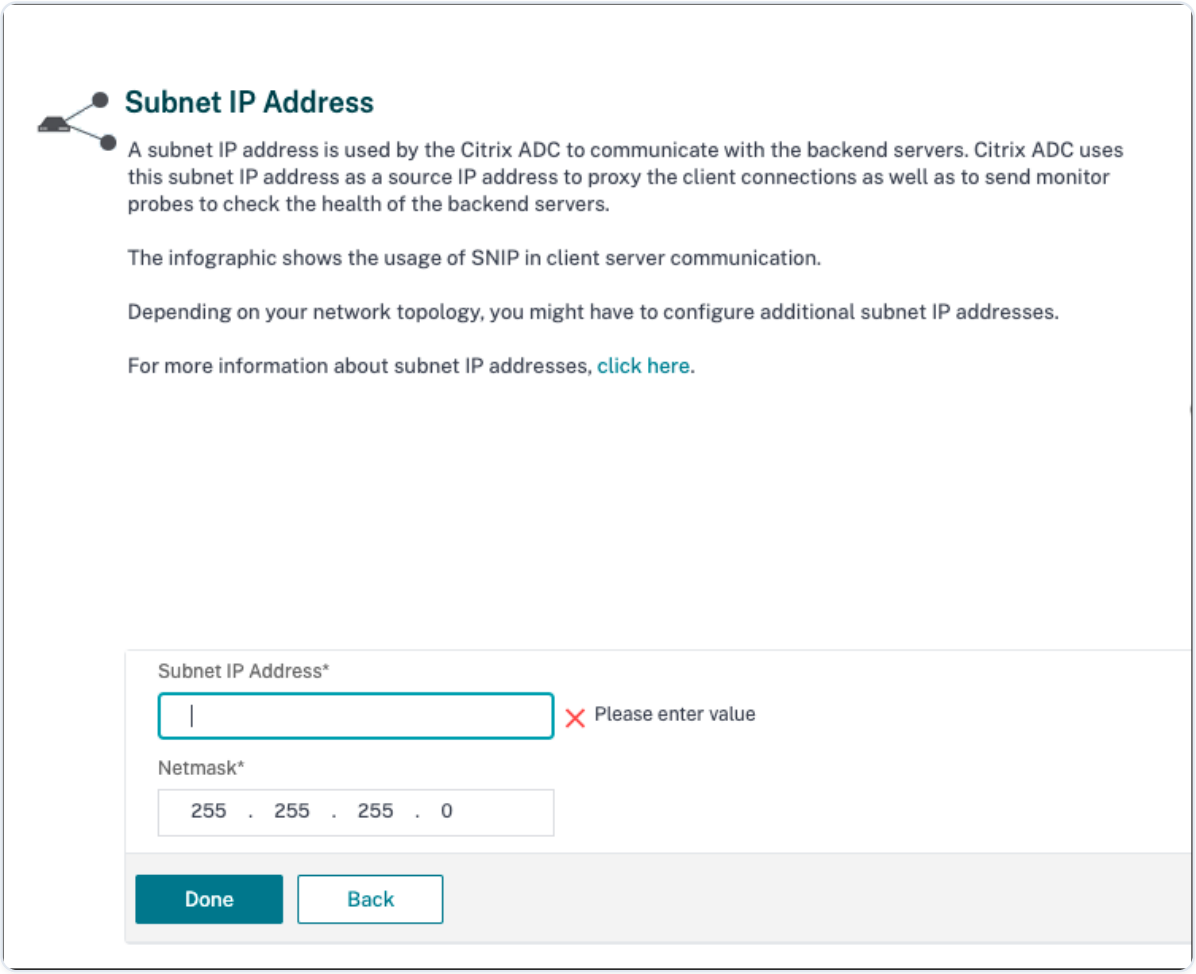
- `Gateway name`
- `STA URL`
- `Secret`

有关指导和语法，请参阅 PowerShell 命令帮助。

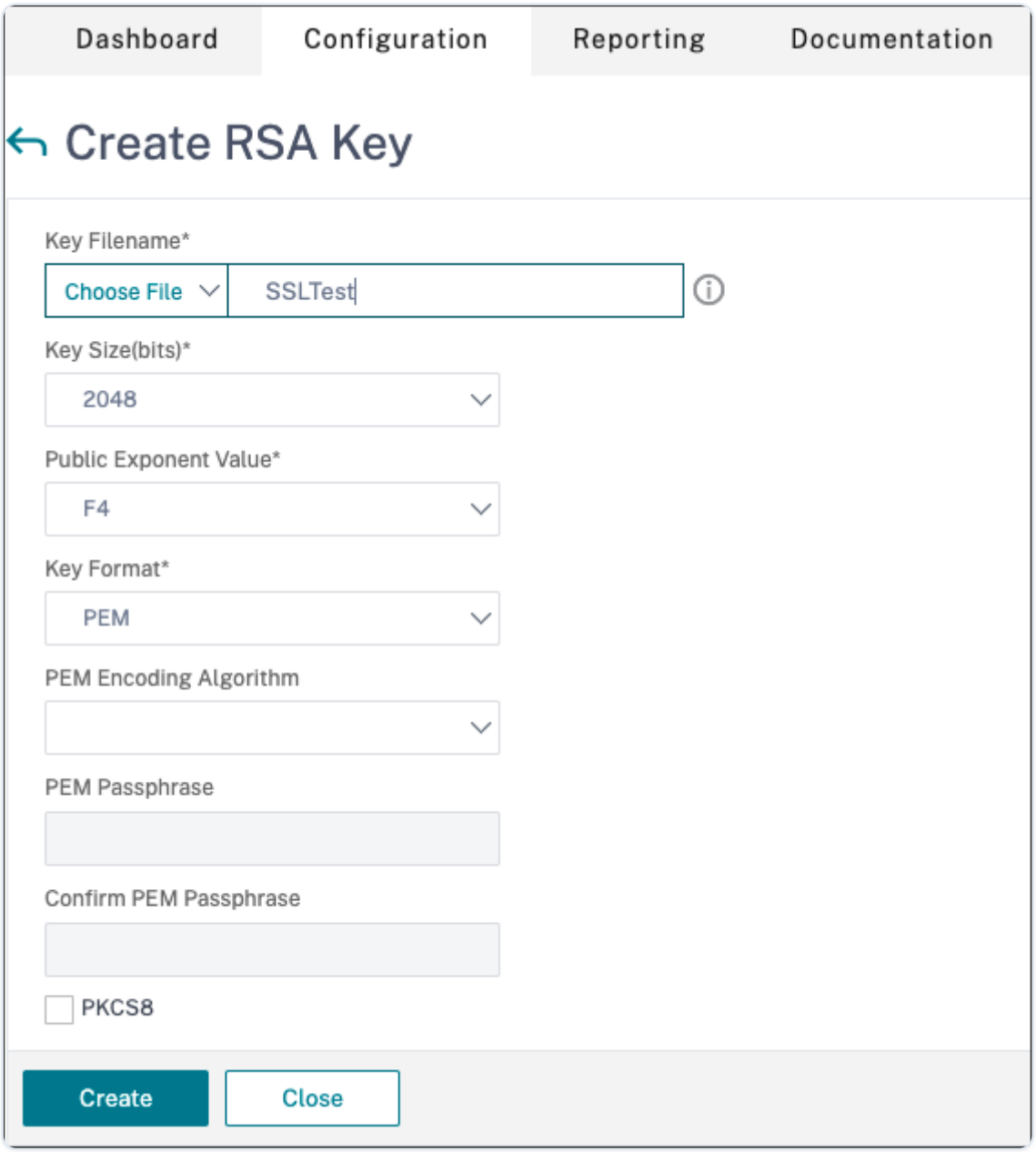
配置 Citrix ADC 的设置

> **注意：**
>
> 除非您使用 Citrix ADC 作为网关，否则无需为 Citrix ADC 配置此功能。如果您使用 Citrix ADC，请按照以下步骤操作：

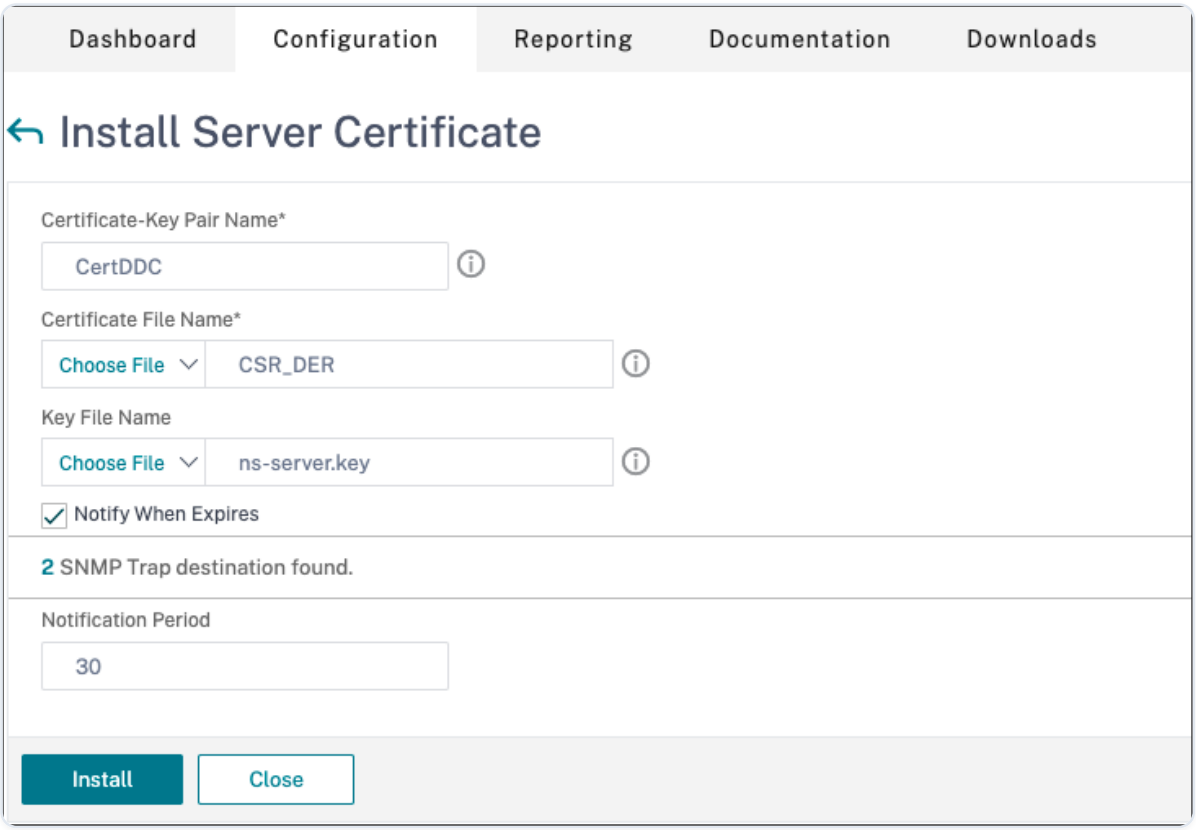
1. 确保已完成以下先决条件配置：
   - 已配置以下 Citrix ADC 相关 IP 地址。
     - 用于访问 Citrix ADC 控制台的 Citrix ADC 管理 IP (NSIP) 地址。有关详细信息，请参阅配置 NSIP 地址。
     - 子网 IP (SNIP) 地址，用于启用 Citrix ADC 设备与后端服务器之间的通信。有关详细信息，请参阅 配置子网 IP 地址。
     - Citrix Gateway 虚拟 IP 地址和负载均衡器虚拟 IP 地址，用于登录 ADC 设备以启动会话。有关详细信息，请参阅 创建虚拟服务器。



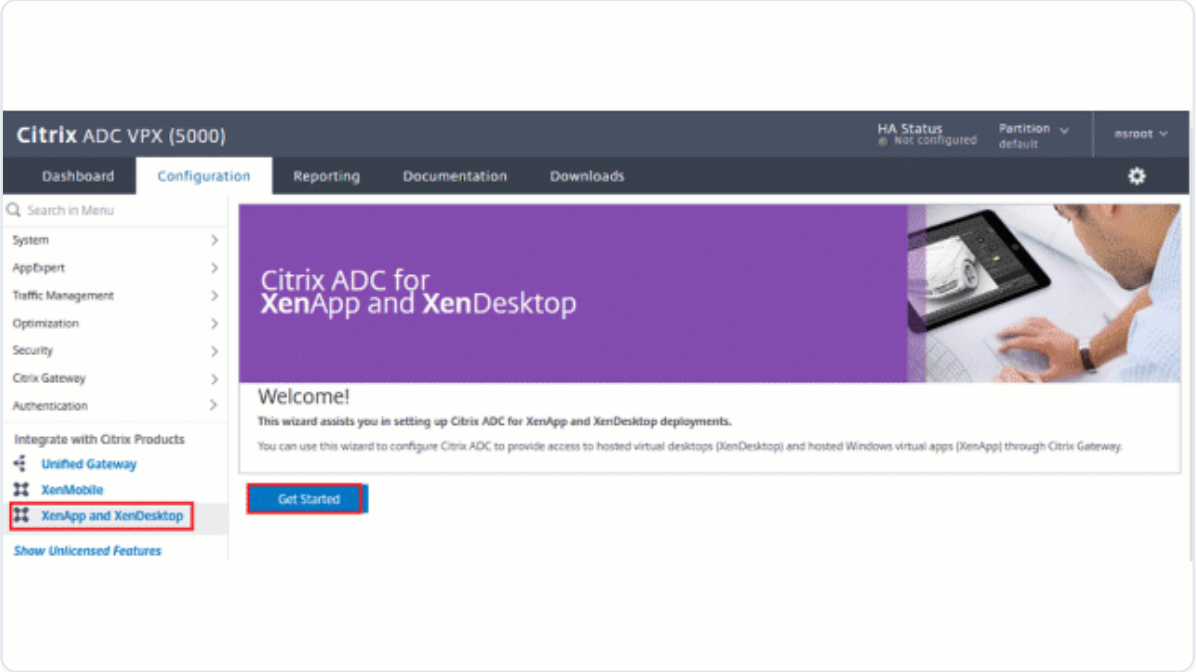
- Citrix ADC 设备中所需的模式和功能已启用。
  - 要启用这些模式，请在 Citrix ADC GUI 中转到 **System > Settings > Configure Mode**。
  - 要启用这些功能，请在 Citrix ADC GUI 中转到 **System > Settings > Configure Basic Features**。
- 证书相关配置已完成。
  - 证书签名请求 (CSR) 已创建。有关详细信息，请参阅 创建证书。



◦ 服务器证书、CA 证书和根证书已安装。有关详细信息，请参阅 安装、链接和更新。



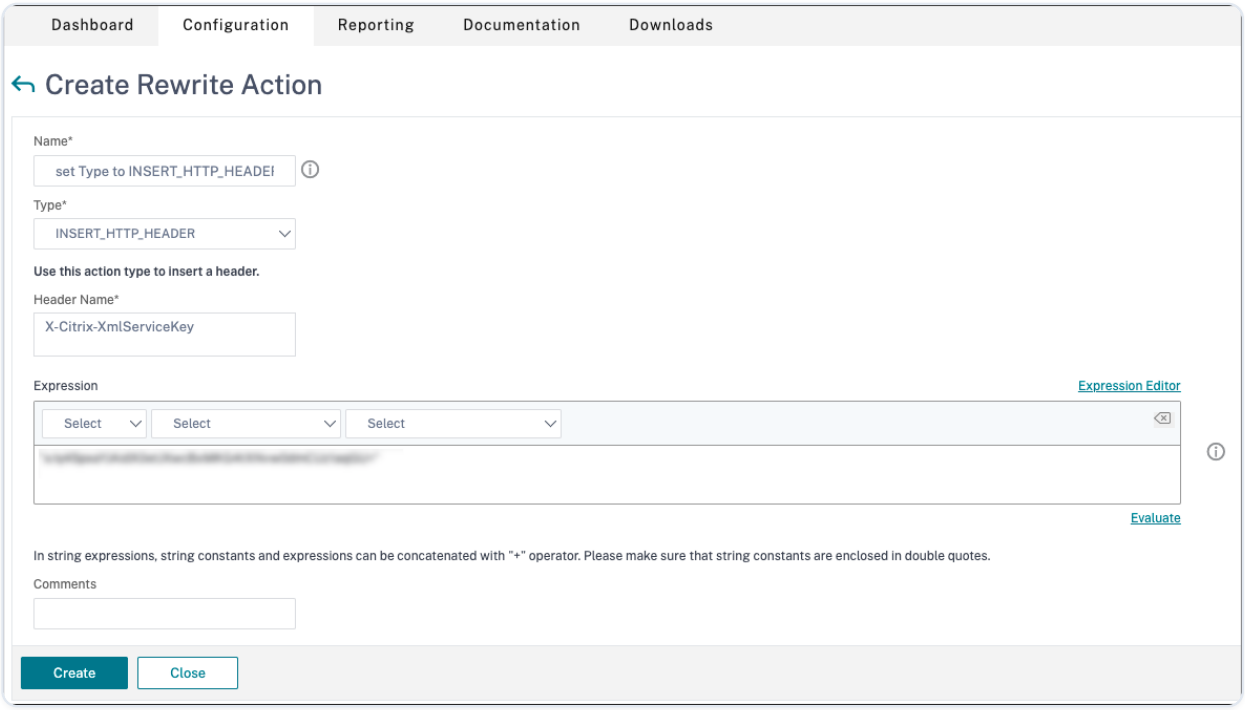
- 已为 Citrix Virtual Desktops 创建 Citrix Gateway。通过单击**测试 STA 连接**按钮测试连接，以确认虚拟服务器在线。有关详细信息，请参阅(/zh-cn/citrix-adc/current-release/solutions/deploy-xa-xd.html)。



2. 添加重写操作。有关详细信息，请参阅 配置重写操作。

   a. 请转到 **AppExpert > Rewrite > Actions**。

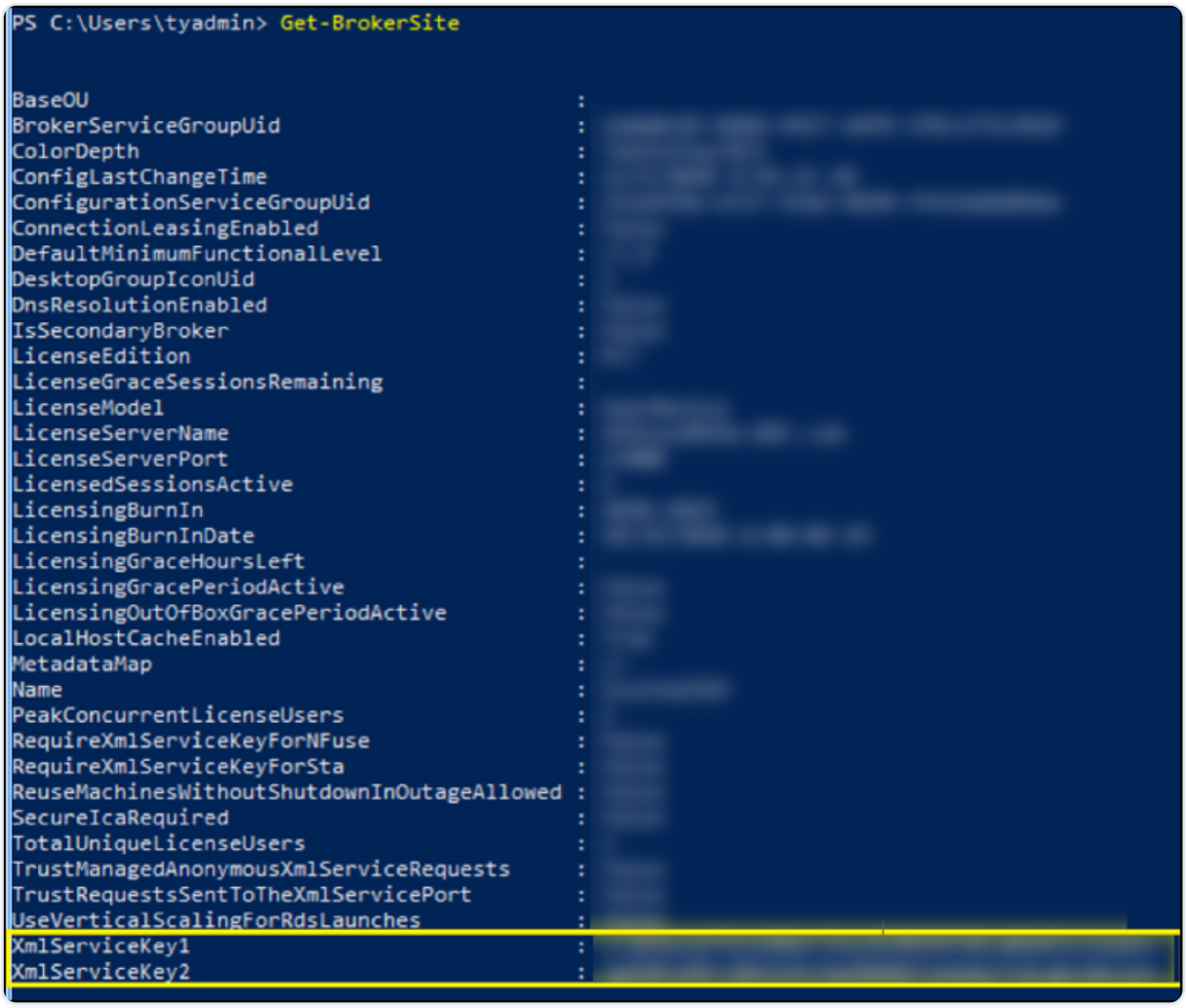
b. 单击 **添加** 以添加新的重写操作。您可以将操作命名为“set Type to INSERT_HTTP_HEADER”。



a. 在 **类型** 中，选择 **INSERT_HTTP_HEADER**。

b. 在 **标头名称** 中，输入 X-Citrix-XmlServiceKey。

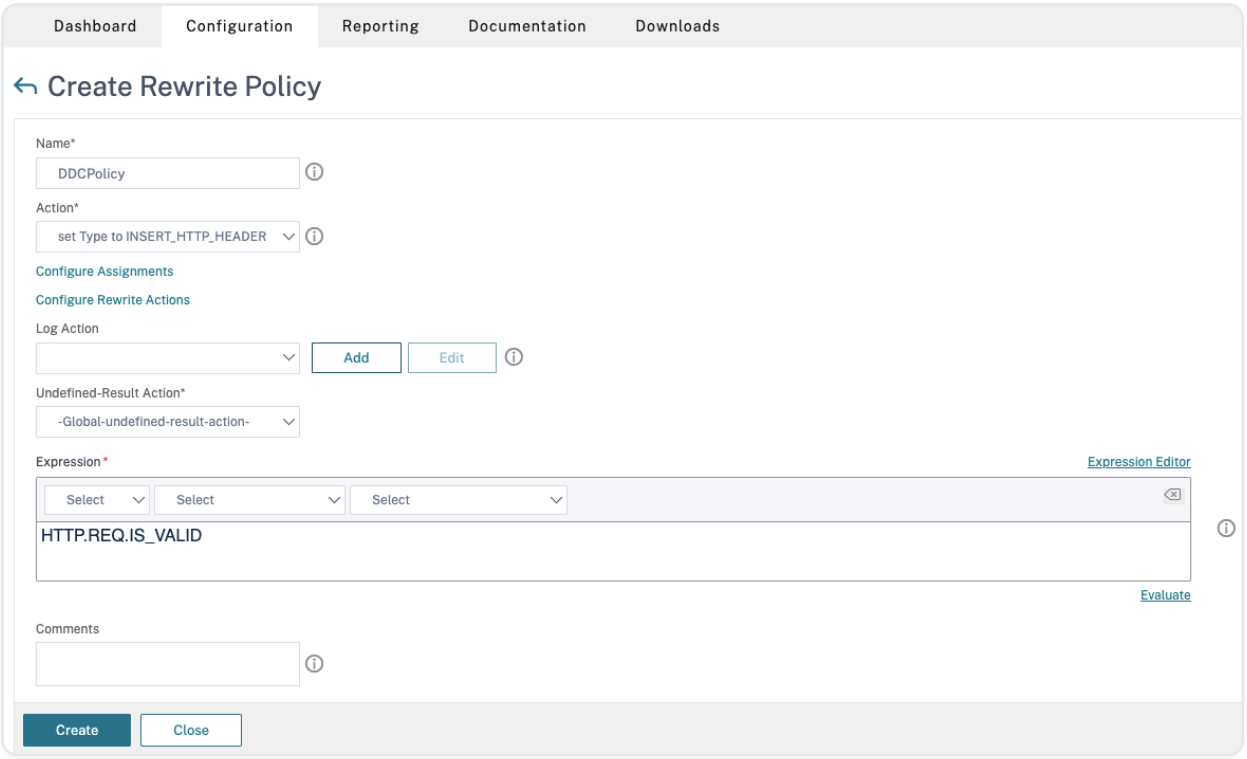
c. 在 **表达式** 中，添加 `<XmlServiceKey1 value>` 并带引号。您可以从您的 Desktop Delivery Controller™ 配置中复制 XmlServiceKey1 值。



3. 添加重写策略。有关详细信息，请参阅配置重写策略。

   a. 请转到 **AppExpert > Rewrite > Policies**。

   b. 单击 **添加** 以添加新策略。



a. 在 **操作** 中，选择上一步中创建的操作。

b. 在 **表达式** 中，添加 HTTP.REQ.IS_VALID。

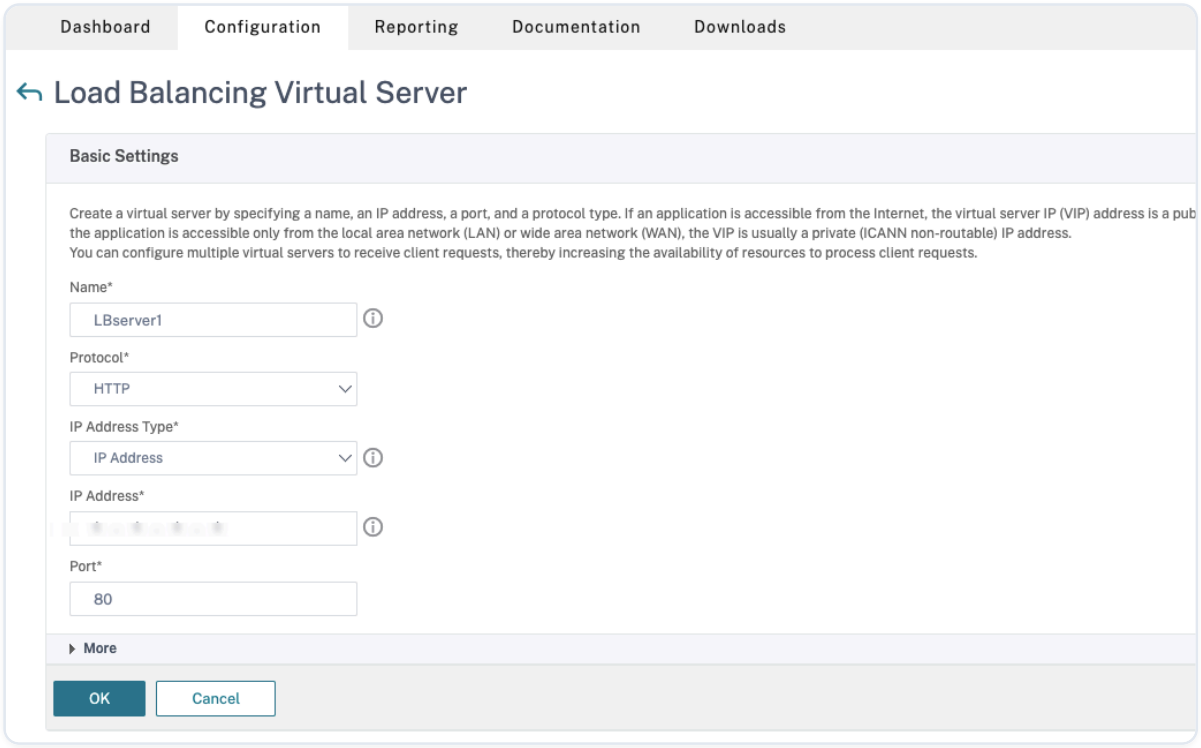
c. 单击 **确定**。

4. 设置负载平衡。您必须为每个 STA 服务器配置一个负载平衡虚拟服务器。否则会话将无法启动。

   有关详细信息，请参阅设置基本负载平衡。

   a. 创建负载平衡虚拟服务器。

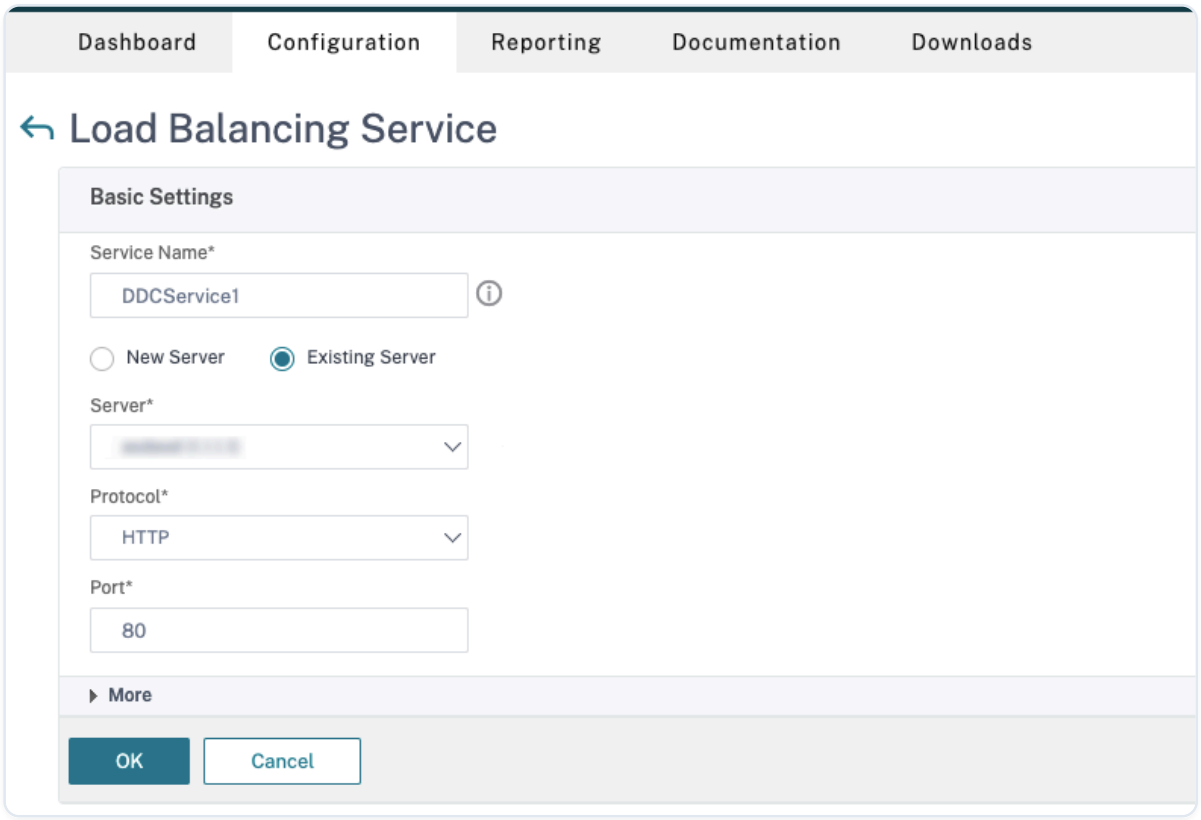
      - 转到 **流量管理 > 负载平衡 > 服务器**。
      - 在 **虚拟服务器** 页面中，单击 **添加**。



- 在 **协议** 中，选择 **HTTP**。
- 添加负载平衡虚拟 IP 地址，并在 **端口** 中选择 **80**。
- 单击 **确定**。

b. 创建负载平衡服务。

- 转到 **流量管理 > 负载平衡 > 服务**。



- 在 **现有服务器** 中，选择上一步中创建的虚拟服务器。
- 在 **协议** 中，选择 **HTTP**，并在 **端口** 中选择 **80**。
- 单击 **确定**，然后单击 **完成**。

c. 将服务绑定到虚拟服务器。

- 选择之前创建的虚拟服务器，然后单击**编辑**。
- 在“**服务和服务组**”中，单击“**无负载平衡虚拟服务器服务绑定**”。

绑定服务到虚拟服务器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/adc-bind-service-to-lbvserver.png)

- 在**服务绑定**中，选择之前创建的服务。
- 单击“**绑定**”。

d. 将之前创建的重写策略绑定到虚拟服务器。

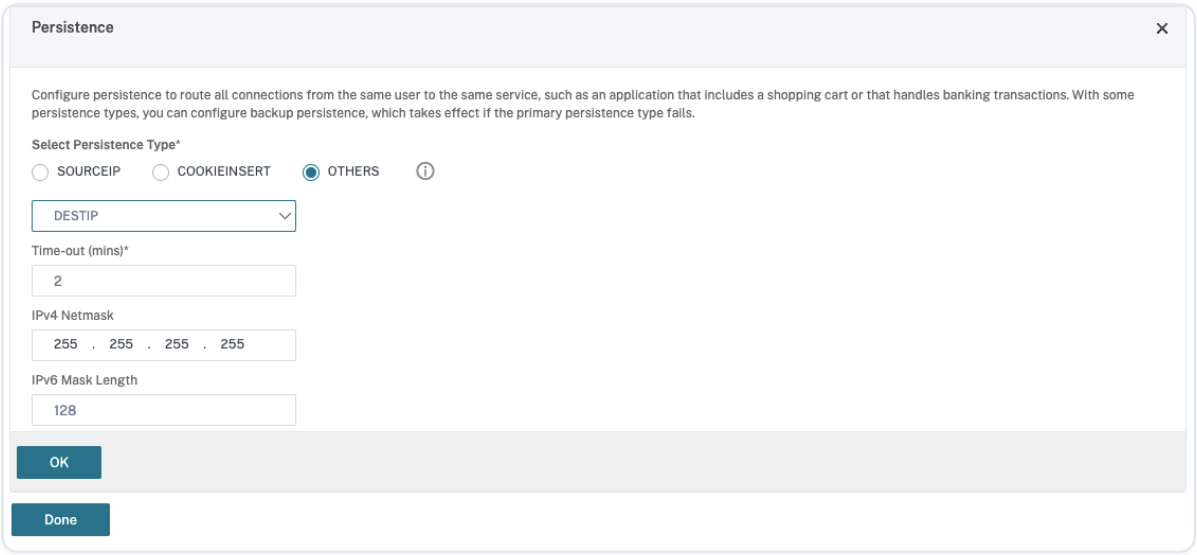
- 选择之前创建的虚拟服务器，然后单击**编辑**。
- 在“**高级设置**”中，单击“**策略**”，然后在“**策略**”部分单击“**+**”。

绑定重写策略(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/adc-bind-rewrite-policy.png)

- 在“**选择策略**”中，选择“**重写**”，并在“**选择类型**”中，选择“**请求**”。
- 单击“**继续**”。
- 在“**选择策略**”中，选择之前创建的重写策略。
- 单击“**绑定**”。
- 点击 **完成**。

e. 如有必要，为虚拟服务器设置持久性。

- 选择之前创建的虚拟服务器，然后单击**编辑**。
- 在**高级设置**中，单击**持久性**。



- 选择持久性类型为**其他**。
- 选择 **DESTIP** 以根据虚拟服务器选择的服务 IP 地址（目标 IP 地址）创建持久性会话
- 在 **IPv4 子网掩码**中，添加与 DDC 相同的网络掩码。
- 单击 **确定**。

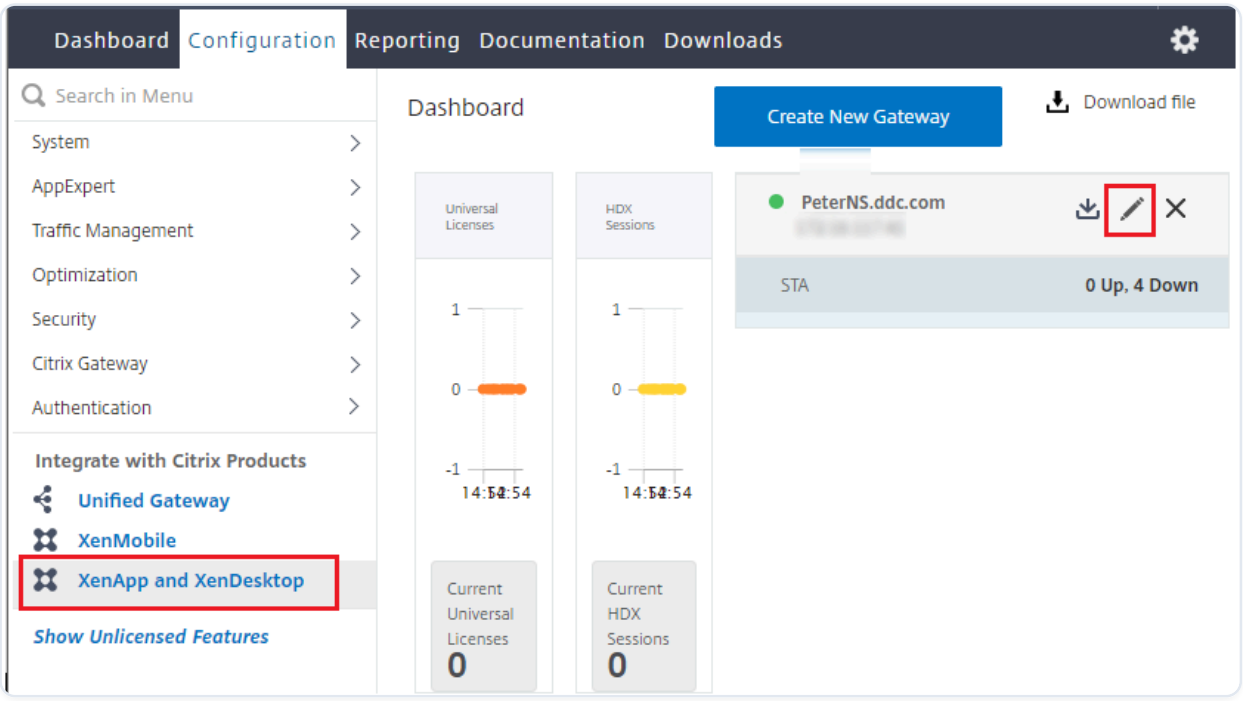
f. 对其他虚拟服务器也重复这些步骤。

如果 Citrix ADC 设备已配置 Citrix Virtual Desktops™，则进行配置更改

如果您已使用 Citrix Virtual Desktops 配置了 Citrix ADC 设备，则要使用安全 XML 功能，必须进行以下配置更改。

- 在会话启动之前，更改网关的**安全票证颁发机构 URL**，以使用负载平衡虚拟服务器的 FQDN。
- 确保 `TrustRequestsSentToTheXmlServicePort` 参数设置为 False。默认情况下，`TrustRequestsSentToTheXmlServicePort` 参数设置为 False。但是，如果客户已为 Citrix Virtual Desktops 配置了 Citrix ADC，则 `TrustRequestsSentToTheXmlServicePort` 设置为 True。

1. 在 Citrix ADC GUI 中，转到**配置 > 与 Citrix 产品集成**，然后单击 **XenApp and XenDesktop®**。
2. 选择网关实例，然后单击编辑图标。



3. 在 StoreFront 窗格中，单击编辑图标。

   编辑 StoreFront 详细信息(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/edit-storefront-details.png)

4. 添加 **安全票证颁发机构 URL**。

   - 如果启用了安全 XML 功能，则 STA URL 必须是负载平衡服务的 URL。
   - 如果安全 XML 功能已禁用，则 STA URL 必须是 STA 的 URL（DDC 的地址），并且 DDC 上的 `TrustRequestsSentToTheXmlServicePort` 参数必须设置为 True。

   添加 STA URL(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/add-sta-urls.png)

会话弹性设置

保持会话活动对于提供最佳用户体验至关重要。由于网络不可靠、网络延迟高度可变以及无线设备的范围限制而失去连接，可能导致用户沮丧。在设备之间快速切换并在每次登录时访问相同的应用程序，对于许多移动工作人员（例如医护人员）来说是优先事项。

本文介绍的功能可优化会话的可靠性，减少不便、停机时间和生产力损失；使用这些功能，移动用户可以在设备之间快速轻松地漫游。

会话可靠性

当网络连接中断时，会话可靠性会保持会话处于活动状态并显示在用户屏幕上。用户将继续看到他们正在使用的应用程序，直到网络连接恢复。

此功能对于使用无线连接的移动用户特别有用。例如，使用无线连接的用户进入铁路隧道并暂时失去连接。通常，会话会断开连接并从用户屏幕上消失，用户必须重新连接到断开的会话。借助会话可靠性，会话在计算机上保持活动状态。为了指示连接丢失，用户的显示屏会冻结，光标会变成旋转的沙漏，直到隧道另一侧的连接恢复。用户在中断期间可以继续访问显示屏，并在网络连接恢复时恢复与应用程序的交互。会话可靠性会在不提示重新身份验证的情况下重新连接用户。

Citrix Workspace™ 应用程序用户无法覆盖控制器设置。

您可以将会话可靠性与传输层安全性 (TLS) 结合使用。TLS 仅加密在用户设备和 Citrix Gateway 之间发送的数据。

使用以下策略设置启用和配置会话可靠性：

- “会话可靠性连接”策略设置允许或阻止会话可靠性。
- “会话可靠性超时”策略设置默认为 180 秒（即三分钟）。尽管您可以延长会话可靠性保持会话打开的时间，但此功能旨在方便用户。因此，它不会提示用户重新进行身份验证。随着您延长会话保持打开的时间，用户可能会分心并离开用户设备的可能性会增加。这些操作可能会使会话可供未经授权的用户访问。
- 传入的会话可靠性连接使用端口 2598，除非您在“会话可靠性端口号”策略设置中更改端口号。
- 为防止用户在不重新进行身份验证的情况下重新连接到中断的会话，请使用自动客户端重新连接功能。您可以配置“自动客户端重新连接身份验证”策略设置，以在用户重新连接到中断的会话时提示他们重新进行身份验证。

如果您同时使用会话可靠性和自动客户端重新连接，这两个功能将按顺序工作。会话可靠性会在您在“会话可靠性超时”策略设置中指定的时间量后关闭或断开用户会话。之后，“自动客户端重新连接”策略设置生效，尝试将用户重新连接到断开的会话。

客户端自动重新连接

借助自动客户端重新连接功能，Citrix Workspace 应用程序可以检测 ICA® 会话的意外断开连接，并自动将用户重新连接到受影响的会话。在服务器上启用此功能后，用户无需手动重新连接即可继续工作。

对于应用程序会话，Citrix Workspace 应用程序会尝试重新连接到会话，直到成功重新连接或用户取消重新连接尝试。

对于桌面会话，Citrix Workspace 应用程序会尝试在指定的时间段内重新连接到会话，除非重新连接成功或用户取消重新连接尝试。默认情况下，此时间段为五分钟。要更改此时间段，请在用户设备上编辑以下注册表设置（其中 `seconds` 是不再尝试重新连接会话的秒数）。

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

使用以下策略设置启用和配置自动客户端重新连接：

- **自动客户端重新连接：** 在连接中断后，启用或禁用 Citrix Workspace 应用程序的自动重新连接。
- **自动客户端重新连接身份验证：** 启用或禁用自动重新连接后对用户身份验证的要求。
- **自动客户端重新连接日志记录：** 启用或禁用事件日志中重新连接事件的日志记录。默认情况下，日志记录处于禁用状态。启用后，服务器的系统日志会捕获有关成功和失败的自动重新连接事件的信息。每个服务器都在其自己的系统日志中存储有关重新连接事件的信息。站点不提供所有服务器的重新连接事件的组合日志。

> **注意：**
>
> 无需重新身份验证的自动客户端重新连接仅支持密码身份验证。如果您使用联合身份验证服务或智能卡身份验证，则不支持无需重新身份验证的自动客户端重新连接。在这种情况下，用户将被重定向到登录屏幕。

> 自动客户端重新连接包含一个基于加密用户凭据的身份验证机制。当用户首次登录时，服务器会加密并将用户凭据存储在内存中。服务器还会创建并向 Citrix Workspace 应用程序发送一个包含加密密钥的 Cookie。Citrix Workspace 应用程序将密钥提交给服务器以进行重新连接。服务器解密凭据并将其提交给 Windows 登录以进行身份验证。当 Cookie 过期时，用户必须重新进行身份验证才能重新连接到会话。

如果您启用了自动客户端重新连接身份验证设置，则不使用 Cookie。相反，当 Citrix Workspace 应用程序尝试自动重新连接时，会向用户显示一个请求凭据的对话框。

为了最大限度地保护用户凭据和会话，请对客户端和站点之间的所有通信使用加密。

通过使用 icaclient.adm 文件，在适用于 Windows 的 Citrix Workspace 应用程序上禁用自动客户端重新连接。有关详细信息，请参阅适用于 Windows 版本的 Citrix Workspace 应用程序文档。

连接设置也会影响自动客户端重新连接：

- 默认情况下，如前所述，通过站点级别的策略设置启用自动客户端重新连接。不需要用户重新身份验证。但是，如果服务器的 ICA TCP 连接配置为在通信链接中断时重置会话，则不会发生自动重新连接。自动客户端重新连接仅在服务器在连接中断或超时时断开会话的情况下才有效。在

此上下文中，ICA TCP 连接是指用于 TCP/IP 网络上会话的服务器虚拟端口（而不是实际网络连接）。

- 默认情况下，服务器上的 ICA TCP 连接设置为断开具有中断或超时连接的会话。断开的会话在系统内存中保持完整，并可供 Citrix Workspace 应用程序重新连接。
- 连接可以配置为重置或注销具有中断或超时连接的会话。当会话被重置时，尝试重新连接会启动一个新会话。应用程序将重新启动，而不是将用户恢复到正在使用的应用程序中的相同位置。
- 如果服务器配置为重置会话，则自动客户端重新连接会创建一个新会话。此过程要求用户输入其凭据才能登录到服务器。
- 如果 Citrix Workspace 应用程序或插件提交了不正确的身份验证信息，自动重新连接可能会失败，这可能发生在攻击期间，或者服务器确定自检测到断开连接以来已过去太长时间。

ICA 保持活动

启用 ICA 保持活动功能可防止断开的连接被终止。启用后，如果服务器检测到没有活动，此功能可防止远程桌面服务断开该会话。没有活动的示例包括没有时钟变化、没有鼠标移动、没有屏幕更新。服务器每隔几秒发送一次保持活动数据包，以检测会话是否处于活动状态。如果会话不再处于活动状态，服务器会将该会话标记为已断开连接。

> **重要提示：**
>
> ICA 保持活动仅在您不使用会话可靠性时才有效。会话可靠性有其自己的机制来防止断开的连接被终止。仅为不使用会话可靠性的连接配置 ICA 保持活动。

> ICA 保持活动设置会覆盖在 Windows 组策略中配置的保持活动设置。

使用以下策略设置启用和配置 ICA 保持活动：

- **ICA 保持活动超时：** 指定用于发送 ICA 保持活动消息的时间间隔（1-3600 秒）。如果您希望网络监控软件在断开连接不频繁的环境中关闭非活动连接，并且允许用户重新连接到会话不是问题，请勿配置此选项。

  默认间隔为 60 秒：ICA 保持活动数据包每 60 秒发送到用户设备。如果用户设备在 60 秒内没有响应，ICA 会话的状态将变为已断开连接。
- **ICA 保持活动：** 发送或阻止发送 ICA 保持活动消息。

工作区控制

工作区控制允许桌面和应用程序随用户从一个设备移动到另一个设备。这种漫游能力使用户只需登录即可从任何地方访问所有桌面或打开的应用程序，而无需在每个设备上重新启动桌面或应用程序。例如，工作区控制可以帮助医院中的医护人员，他们需要在不同工作站之间快速移动，并在每次登录时访问同一组应用程序。如果您配置工作区控制选项以允许此操作，这些工作人员可以从一个客户端设备断开多个应用程序，然后重新连接以在不同的客户端设备上打开相同的应用程序。

工作区控制影响以下活动：

- **登录：** 默认情况下，工作区控制允许用户在登录时自动重新连接到所有正在运行的桌面和应用程序，从而无需手动重新打开它们。通过工作区控制，用户可以打开已断开连接的桌面或应用程序，以及在另一个客户端设备上处于活动状态的任何桌面或应用程序。从桌面或应用程序断开连接会使其在服务器上继续运行。如果您有漫游用户，他们必须在一个客户端设备上保持某些桌面或应用程序运行，同时在另一个客户端设备上重新连接到其桌面或应用程序的子集，您可以配置登录重新连接行为，使其仅打开用户之前断开连接的桌面或应用程序。
- **重新连接：** 登录到服务器后，用户可以随时通过单击“重新连接”来重新连接到其所有桌面或应用程序。默认情况下，“重新连接”会打开已断开连接的桌面或应用程序，以及当前在另一个客户端设备上运行的任何桌面或应用程序。您可以配置“重新连接”以仅打开用户之前断开连接的那些桌面或应用程序。
- **注销：** 对于通过 StoreFront™ 打开桌面或应用程序的用户，您可以配置“**注销**”命令，以将用户从 StoreFront 和所有活动会话中注销，或者仅从 StoreFront 中注销。
- **断开连接：** 用户可以一次性断开所有正在运行的桌面和应用程序的连接，而无需单独断开每个连接。

工作区控制仅适用于通过 Citrix StoreFront 连接访问桌面和应用程序的 Citrix Workspace 应用程序用户。默认情况下，虚拟桌面会话的工作区控制处于禁用状态，但对托管应用程序启用。已发布的桌面与这些桌面中运行的任何已发布的应用程序之间默认不发生会话共享。

当用户移动到新的客户端设备时，用户策略、客户端驱动器映射和打印机配置会相应地更改。策略和映射根据用户登录会话的客户端设备应用。例如，医护人员从急诊室的设备注销，然后登录到 X 射线实验室的工作站。适用于 X 射线实验室会话的策略、打印机映射和客户端驱动器映射会在会话启动时生效。

您可以自定义用户更改位置时向其显示的打印机。您还可以控制用户是否可以打印到本地打印机、用户远程连接时消耗的带宽量以及其打印体验的其他方面。

有关为用户启用和配置工作区控制的信息，请参阅 StoreFront 文档。

会话漫游

> **注意：**
>
> 以下信息指导您使用 PowerShell 配置会话漫游。您可以改用 Web Studio。有关详细信息，请参阅管理交付组。

> 默认情况下，会话会随用户在客户端设备之间漫游。当用户启动会话然后移动到另一台设备时，将使用相同的会话，并且应用程序在两台设备上都可用。无论设备如何或是否存在当前会话，应用程序都会随之移动。通常，分配给应用程序的打印机和其他资源也会随之移动。

虽然此默认行为提供了许多优点，但在所有情况下可能并不理想。您可以使用 PowerShell SDK 阻止会话漫游。

示例 1：一名医务人员正在使用两台设备，在一台台式电脑上填写保险表格，并在平板电脑上查看患者信息。

- 如果启用了会话漫游，两个应用程序都会显示在两台设备上（在一台设备上启动的应用程序在所有正在使用的设备上都可见）。这可能不符合安全要求。
- 如果禁用了会话漫游，患者记录不会显示在台式电脑上，并且保险表格不会显示在平板电脑上。

示例 2：一位生产经理在他的办公室电脑上启动了一个应用程序。设备名称和位置决定了该会话可用的打印机和其他资源。当天晚些时候，他去隔壁大楼的办公室开会，会议需要使用打印机。

- 当启用会话漫游时，生产经理可能无法访问会议室附近的打印机，因为他之前在办公室启动的应用程序导致分配了该位置附近的打印机和其他资源。
- 当禁用会话漫游时，当他登录到另一台机器（使用相同的凭据）时，会启动一个新会话，并且附近的打印机和资源将可用。

配置会话漫游

要配置会话漫游，请使用以下授权策略规则 cmdlet 和“SessionReconnection”属性。可选地，您还可以指定“LeasingBehavior”属性。

对于桌面会话：

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

对于应用程序会话：

`Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed`

其中 `value` 可以是以下之一：

- **始终：** 会话始终漫游，无论客户端设备以及会话是连接还是断开。这是默认值。
- **仅断开连接：** 仅重新连接到已断开连接的会话；否则，启动新会话。（会话可以通过先断开连接，或使用 Workspace Control 显式漫游，在客户端设备之间漫游。）永远不会使用来自其他客户端设备的活动连接会话。而是启动一个新会话。
- **仅限相同端点：** 用户为其使用的每个客户端设备获取一个唯一的会话。这会完全禁用漫游。用户只能重新连接到会话中以前使用过的同一设备。

下面介绍了“LeasingBehavior”属性。

其他设置的影响：

禁用会话漫游受交付组中应用程序属性中的应用程序限制**每个用户只允许一个应用程序实例**的影响。

- 如果禁用会话漫游，则禁用“只允许一个实例...”应用程序限制。
- 如果启用“只允许一个实例...”应用程序限制，则不要配置允许在新设备上创建新会话的两个值中的任何一个。

登录间隔

如果包含桌面 VDA 的虚拟机在登录过程完成之前关闭，您可以为该过程分配更多时间。7.6 及更高版本的默认值为 180 秒（7.0-7.5 版本的默认值为 90 秒）。

在计算机上（或在计算机目录中使用的主映像上），设置以下注册表项：

项：`HKLM\SOFTWARE\Citrix\PortICA`

- 值: `AutoLogonTimeout`
- 类型: `DWORD`
- 指定一个十进制时间（以秒为单位），范围为 0-3600。

如果您更改了主映像，请更新目录。

此设置仅适用于具有桌面 VDA 的虚拟机。Microsoft 控制具有服务器 VDA 的计算机上的登录超时。

设置

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

使用 Web Studio 管理身份验证、域设置、个人首选项以及其他站点级配置。

管理身份验证

默认情况下，用户使用其域用户名和密码登录 Web Studio。您还可以为用户选择其他身份验证方法，例如智能卡身份验证或集成 Windows 身份验证。

使用 Studio 进行管理

要为用户选择身份验证方法，请执行以下步骤：

1. 登录 Web Studio 并在左侧窗格中选择**设置**。
2. 找到**身份验证**磁贴，然后单击**编辑**以选择一个选项：

   - **域凭据**
   - **域凭据或集成 Windows 身份验证**

     启用集成 Windows 身份验证后，用户可以使用其 Windows 凭据 (Kerberos/NTLM) 或客户端证书访问 Web Studio。

     当 Web Studio 和 Delivery Controller™ 安装在不同的计算机上时，为了使集成 Windows 身份验证正常工作，请启用“允许跨源访问”并将 Web Studio 服务器的 URL 添加到允许列表中。

     > **重要提示**
     >
     > 当 Web Studio 配置为 Delivery Controller 的代理时，集成 Windows 身份验证不起作用。

- **智能卡身份验证**
- **域凭据或智能卡身份验证**

  启用智能卡身份验证需要额外配置。有关详细信息，请参阅为 Web Studio 设置智能卡身份验证。

使用 PowerShell 脚本进行管理

身份验证方法在 Delivery Controller 数据库中配置。您可以使用以下 PowerShell 脚本设置身份验证方法：

1. 通过在 Delivery Controller 上运行以下命令获取当前站点 ID：

   ```
   Get-ConfigSite | Select SiteGuid
   ```

2. 通过运行以下脚本设置身份验证方法：

```
# Generate a new bearer token

$bearerData = New-TrustBearerToken

# Define the Delivery Controller DNS name and Site ID

$ddc = "ddc.dc.com" # replace this with the Delivery Controller's DNS
name

$siteid = "c68a8f89-42af-4bea-a6e9-c8c936353f49" # replace this with
the site ID you get from step #1

# Define the URL and headers

$url = "https://$ddc/citrix/orchestration/api/CitrixOnPremises/Sites/
$siteid/Settings"

$headers = @{

"Content-Type" = "application/json"

"Authorization" = "Bearer $($bearerData.Token)"

}

# Define the JSON body
```

```
$body = @{

SupportedAuthenticators = "BasicAndSmartCard" # replace this with a
required authentication method: "Basic" for "Domain credentials";
"BasicAndIntegratedWindowsAuthentication" for "Domain credentials or
integrated Windows authentication"; "BasicAndSmartCard" for "Domain
credentials or smart card authentication"; "SmartCard" for "Smart card
authentication"

} | ConvertTo-Json -Depth 10

# Send the PATCH request

Invoke-RestMethod -Uri $url -Method Patch -Headers $headers -Body $body
```

为集成 Windows 身份验证配置浏览器

如果您使用**域凭据或集成 Windows 身份验证**启用*集成 Windows 身份验证*，则用户下次登录时将自动登录。如果用户无法自动登录，请按照以下步骤配置 Web 浏览器以允许集成 Windows 身份验证。

对于谷歌浏览器：

1. 从“控制面板”中，选择**Internet 选项**。
2. 选择**高级**选项卡。
3. 选择**启用集成 Windows 身份验证**。
4. 选择**安全**选项卡。
5. 选择**本地 Intranet > 站点 > 高级**。
6. 在**将此网站添加到区域**框中：
   - 如果 Web Studio 和 Delivery Controller 位于同一服务器上，请键入运行 Web Studio 的主机的 URL。
   - 如果不是，请键入通配符域。例如：如果 Delivery Controller 位于 `ddc.domain.com`，请键入 `*.domain.com`。
7. 单击 **添加 > 关闭**

对于火狐浏览器：

1. 在浏览器中，在 URL 框中键入 `about:config`。

2. 在“**搜索**”框中，键入 `network negotiate`。
3. 右键单击 **network.negotiate-auth.trusted-uris**，然后选择“**修改**”。
4. 在“**输入字符串值**”框中：
   - 如果 Web Studio 和 Delivery Controller 位于同一服务器上，请添加一个逗号分隔的 URL 和/或别名列表，这些 URL 和/或别名引用托管 Web Studio 的服务器名称。
   - 如果不是，请按此方式添加 URL。例如：如果 Delivery Controller 位于 `ddc.domain.com`，请键入 `*.domain.com`。

配置浏览器后，您可以在登录页面上单击“**Windows 集成登录**”以重试。

当 Web Studio 和 Delivery Controller 安装在不同的计算机上时，要使集成 Windows 身份验证正常工作，您需要启用“**允许跨域访问**”。

请按照以下步骤启用“**允许跨域访问**”：

1. 选中“**允许跨域访问**”复选框。
2. 将 Web Studio 服务器的 URL 添加到允许列表中。
3. 在“**输入 URL**”字段中，输入 URL。如有必要，单击“**添加**”以添加更多。

> **注意**
>
> - URL 必须遵循正确的格式：`<scheme>://<hostname>`。确保它不包含任何路径或尾随斜杠。
> - 支持 IP 地址和 FQDN。添加 URL 时，请确保它与您访问 Web Studio 的方式相对应。例如，如果使用 IP 地址访问 Web Studio，请将基于 IP 地址的 URL 添加到列表中。
> - 如果使用非默认端口，请务必包含端口号。

4. 如有必要，单击 **添加** 以添加更多。
5. 完成后，单击 **完成** 以保存并退出。

为 Studio 登录页面设置默认域名

要使用域名自动填充 Studio 登录页面上的 **域** 字段，请按照以下步骤操作：

1. 登录 Web Studio 并在左侧窗格中选择 **设置**。
2. 在 **配置域名** 磁贴上，根据需要键入域名。

3. 单击**应用**。

   当管理员访问 Studio 登录页面时，*域* 字段会自动填充您设置的域名。

配置域排除列表

通过将无法访问或不必要的域添加到 **设置 > 站点设置** 中的域排除列表来提高域查找性能。Web Studio 会自动跳过所有域和 OU 查找中的排除域，从而使域查找响应更快。

为了加快域查询速度，请将无法访问或不需要的域添加到排除列表。Web Studio 随后会自动跳过所有域和 OU 查找中的这些域。

要将域添加到排除列表，请按照以下步骤操作：

1. 登录 Web Studio 并在左侧窗格中选择 **设置**。
2. 在 **站点设置** 下，找到 **将域添加到排除列表**。
3. 启用 **启用域排除**。
4. 选择 **添加域**，在 **域名** 字段中输入域名，然后选择 **确认**。对要排除的每个域重复此操作。
5. 选择“**保存**”。

节标题下方的状态指示器显示当前已排除的域数量。

> **注意：**
>
> - 排除列表中的域名必须是唯一的，并遵循有效的域名格式。
> - 若要暂时禁用所有排除项而不从列表中删除域，请关闭 **启用域排除**。
> - 如果您在 **位置（域）** 下拉列表中搜索已排除的域，**Web Studio** 会通知您该域已被排除，并提供指向此页面的链接，以便您查看或删除它。

在 Studio 中管理个人首选项

使用 **设置** 节点下的 **我的首选项** 选项卡来管理您在 Studio 中的个人视图和交互首选项。这些设置仅适用于您的帐户，不影响其他管理员。可用选项包括：

- **日期和时间**：设置您的默认时区、日期格式和时间格式。这些设置在整个 Studio 中用于时间相关的显示，例如计划重新启动和自动缩放。
- **文件夹视图**：选择在 **计算机目录**、**交付组** 和 **应用程序** 节点中显示或隐藏文件夹视图。
- **搜索中的选项卡顺序**：自定义**搜索**节点中的选项卡顺序。

要在 Studio 中设置您的首选视图，请按照以下步骤操作：

1. 在 Studio 中，转到 **设置 > 我的首选项**。
2. 单击**编辑**。
3. 在 **日期和时间** 磁贴中，配置以下格式设置：
   - **日期格式**：选择如何显示日期（例如，yyyy/MM/dd）。要使用与您为 Studio 选择的语言关联的日期格式，请选择 **匹配控制台语言**。
   - **时间格式**：选择 12 小时制（例如，09:00 PM）或 24 小时制（例如，21:00）。要使用与您为 Studio 选择的语言关联的时间格式，请选择 **匹配控制台语言**。
   - **时区**： 选择您的首选时区。要使用计算机的时区，请选择**匹配控制台语言**。

     > **注意：**
     >
     > - 要使用计算机的日期、时间或时区区域设置，请选择**匹配控制台语言**。
     > - 在 Studio 中，您可以将鼠标悬停在任何显示的时间上，以查看其在本地时区中的等效时间。
4. 在**文件夹视图**磁贴中，选择是在**计算机目录**、**交付组**和**应用程序**节点中显示还是隐藏文件夹视图。
5. 在**搜索中的选项卡顺序**磁贴中，拖动并重新排序**搜索**节点中的选项卡。
6. 单击**应用**以立即保存并应用更改。

启用 DNS 解析

要在 ICA® 文件中显示 DNS 名称而不是 IP 地址，请按照以下步骤操作：

1. 登录 Web Studio 并在左侧窗格中选择**设置**。
2. 启用**启用 DNS 解析**设置。

设置 Studio 控制台的非活动超时

您可以设置非活动持续时间，超过该持续时间后，管理员将自动从 Studio 控制台注销。

1. 登录 Web Studio 并在左侧窗格中选择**设置**。
2. 键入一个持续时间，范围为 10 分钟到 24 小时。
3. 要应用此设置，请刷新页面或注销然后重新登录。

集中管理站点

此功能允许您使用一个 Web Studio 控制台管理多个 Citrix Virtual Apps and Desktops 站点。有关详细信息，请参阅启用多站点管理。

在 Studio 登录页面上设置自定义通知

要设置登录页面通知，请执行以下步骤：

1. 登录 Web Studio 并在左侧窗格中选择**设置**。
2. 找到**登录页面通知**磁贴，然后选中**在登录页面上显示通知**复选框。
3. 单击**编辑**以打开**登录页面通知**页面，并根据需要键入登录页面通知。
4. 单击 **保存**。

在 Studio 登录页面上显示活动 DDC 的 FQDN

要在 Studio 登录页面上显示当前会话使用的 DDC 的 FQDN，请执行以下步骤：

1. 登录 Web Studio 并在左侧窗格中选择**设置**。
2. 启用**显示连接的 Delivery Controller**。

配置日志服务器

配置 AOT（始终开启跟踪）日志服务器并定义日志记录范围。**Director** 连接到日志服务器以检索日志，用于监视和故障排除。

要配置日志服务器并定义日志记录范围，请执行以下步骤：

1. 登录 **Web Studio** 并在左侧窗格中选择**设置**。
2. 如果未配置日志服务器，请在**日志服务器**磁贴中单击**添加**。
3. 在出现的**日志服务器**页面上，选择**启用日志转发到日志服务器**。
4. 选择哪些组件将日志转发到日志服务器：
   - **包括 Delivery Controller：** 将所有 Delivery Controller 的日志转发到日志服务器。
   - **选择交付组：** 将特定交付组中的 VDA 的日志转发到日志服务器。默认情况下，选择**所有交付组**，这将转发所有交付组中 VDA 的日志。要仅转发特定交付组中 VDA 的日志，请选择**选择特定交付组**，然后选择要包括的组。
5. 输入日志服务器生成的 **Authkey**。**Director** 使用此密钥访问日志服务器。
6. 单击**保存**以应用配置。

要更新日志服务器或修改日志记录范围，请在**设置 > 日志服务器**磁贴中单击**编辑**。

配置 Microsoft Entra 单点登录 (SSO)

设置 Microsoft Entra 单点登录 (SSO)。配置 SSO 后，用户可以使用其 Microsoft Entra ID 凭据在已加入 Microsoft Entra 或已加入 Microsoft Entra 混合的会话主机上登录其虚拟应用程序和桌面。

> **注意：**
>
> Microsoft Entra SSO 目前仅支持已加入 Microsoft Entra 混合的会话主机。

开始之前

在配置 SSO 之前：

- 注册所需的资源应用程序。
- 在您的 Microsoft Entra 租户中创建客户端应用程序。

有关要求的更多信息，请参阅 Microsoft Entra 单点登录。

工作流程

1. 登录到 **Web Studio** 并在左侧窗格中选择**设置**。
2. 在 **Microsoft Entra 单一登录 (SSO)** 磁贴中单击**配置**。将显示配置页面。
3. 在 **应用程序（客户端）ID** 中，输入有效的 GUID。 示例：`12345678-1234-1234-1234-123456789abc`
4. 在 **重定向 URI（回复 URL）** 中，输入有效的重定向 URI。 示例：`https://ctx-ws-assets.cloud.com/assets/workspace/html/static/aad_sso_msal_redirect.html`
5. 在 **身份验证 URL** 中，输入身份验证终结点。 示例：`https://login.microsoftonline.com`
6. 在 **资源应用程序 ID URI** 中，选择以下选项之一：
   - **商业、政府**或**日本**。资源应用程序 ID URI 会自动填充 Citrix 提供的值。
   - **自定义**。输入您的自定义应用程序 ID URI。
7. 选择“**保存**”。

保存配置后，将为您的站点启用 Microsoft Entra 单一登录 (SSO)。

标签

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的相应文章。

简介

标签是用于标识项目（例如计算机、应用程序、桌面、交付组、应用程序组和策略）的字符串。创建标签并将其添加到项目后，您可以自定义某些操作，使其仅应用于具有指定标签的项目。

- 自定义 Web Studio 中的搜索显示。

  例如，要仅显示已针对测试人员优化的应用程序，请创建一个名为“test”的标签，然后将其添加（应用）到这些应用程序。现在，您可以使用“test”标签筛选 Web Studio 搜索。

- 从应用程序组发布应用程序或从交付组发布特定桌面时，仅考虑所选交付组中的一部分计算机。这称为*标签限制*。

  通过标签限制，您可以将现有计算机用于多个发布任务，从而节省部署和管理更多计算机的成本。标签限制可以看作是对交付组中的计算机进行细分（或分区）。其功能与 XenApp 7.x 之前的版本中的辅助角色组类似，但并不完全相同。

  使用带有标签限制的应用程序组或桌面有助于隔离和排查交付组中一部分计算机的问题。

- 为交付组中的一部分计算机安排定期重新启动。

  对计算机使用标签限制可让您使用新的 PowerShell cmdlet 为交付组中的一部分计算机配置多个重新启动计划。有关示例和详细信息，请参阅 管理交付组。

- 自定义 Citrix 策略的应用程序（分配），使其应用于交付组、交付组类型或具有（或不具有）指定标签的 OU 中的一部分计算机。

  例如，如果您只想将 Citrix 策略应用于功能更强大的工作站，请为这些计算机添加一个名为“high power”的标签。然后，在“创建策略”向导的 **“分配策略”** 页面上，选择该标签和 **“启用”** 复选框。您还可以向交付组添加标签，然后将 Citrix 策略应用于该组。有关详细信息，请参阅 创建策略。

您可以将标签应用于：

- 计算机
- 应用程序
- 计算机目录（仅限 PowerShell；请参阅 计算机目录上的标签）
- 交付组
- 应用程序组

在 Web Studio 中创建或编辑以下内容时，可以配置标签限制：

- 共享交付组中的桌面
- 应用程序组

> **重要提示：**
>
> 标签可以显式应用于计算机，也可以显式应用于计算机目录或交付组级别。当标签应用于计算机目录或交付组级别时，该目录或交付组中的所有计算机都会隐式继承该标签。这些继承的标签无法在计算机级别删除。要移除标签效果，必须从计算机目录或交付组级别移除该标签。

桌面或应用程序组的标签限制

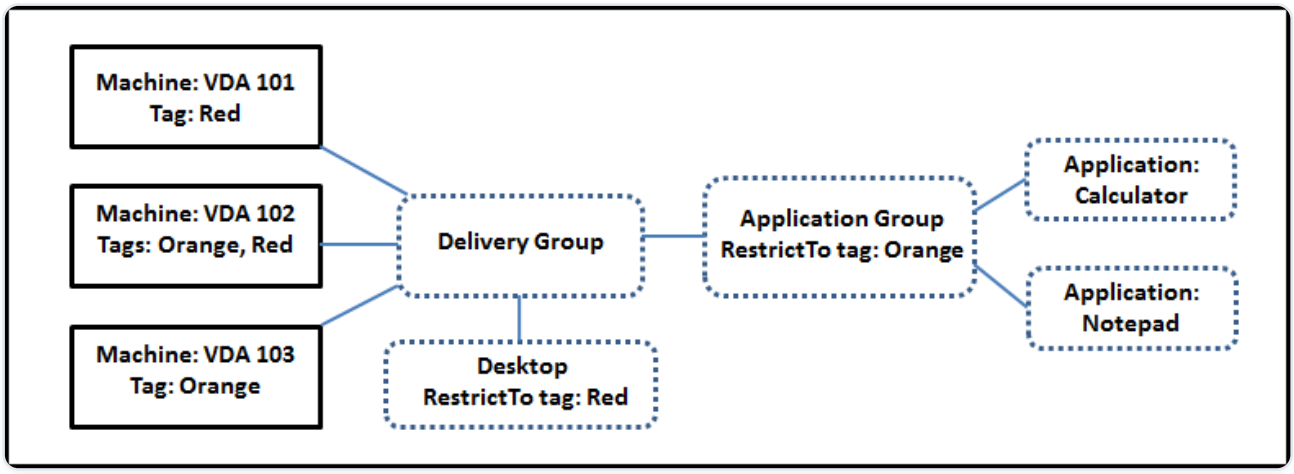
标签限制涉及以下几个步骤：

- 创建标签，然后将其添加（应用）到计算机。
- 创建或编辑具有标签限制的组（换句话说，“将启动限制为具有标签 x 的计算机”）。

标签限制扩展了代理的计算机选择过程。代理从关联的交付组中选择一台计算机，选择过程受访问策略、配置的用户列表、区域首选项和启动就绪状态以及标签限制（如果存在）的约束。对于应用程序，代理会按优先级顺序回退到其他交付组，并对每个考虑的交付组应用相同的计算机选择规则。

示例 1：简单布局

本示例介绍了一种简单布局，该布局使用标签限制来限制哪些计算机可用于某些桌面和应用程序启动。该站点有一个共享交付组、一个已发布的桌面和一个配置了两个应用程序的应用程序组。



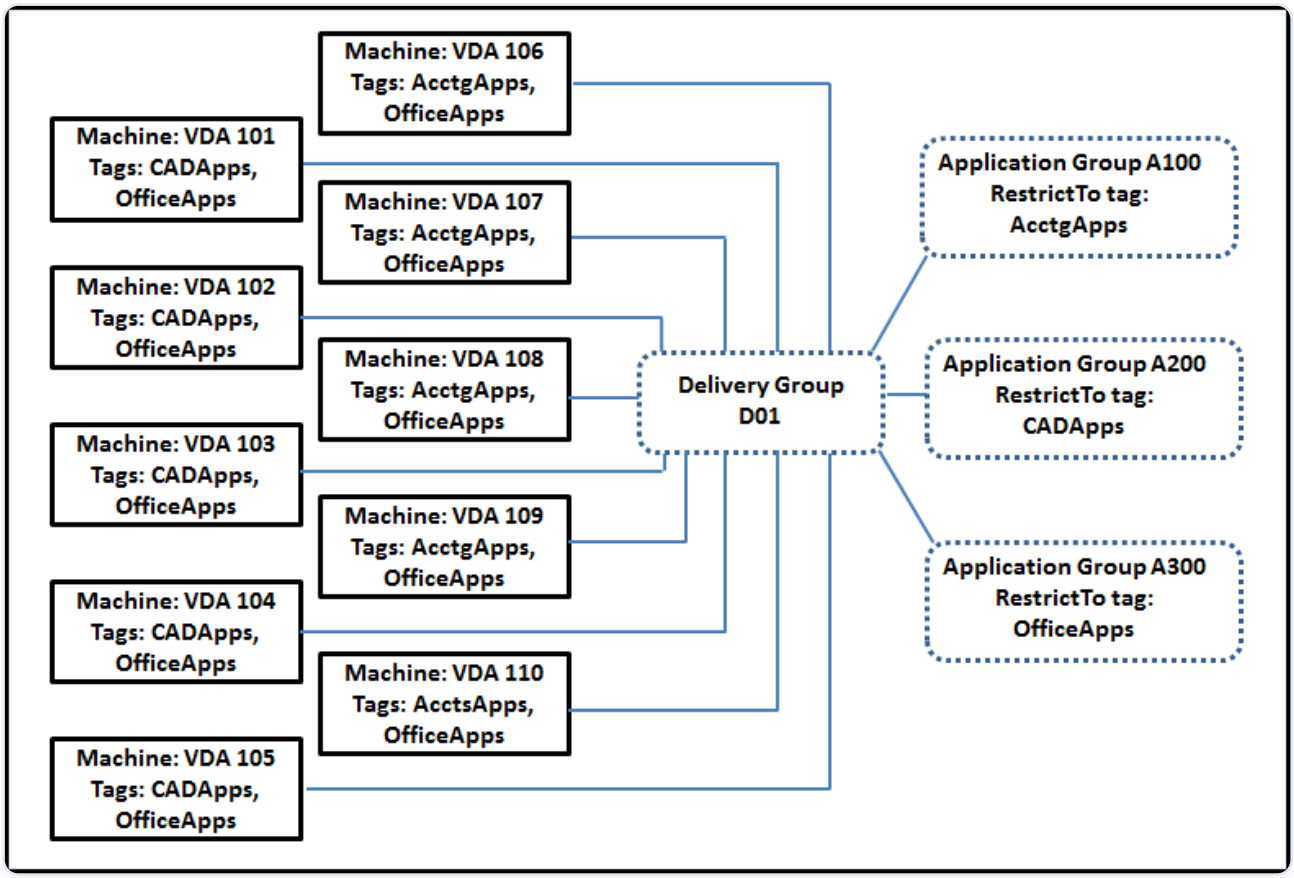
- 已将标记添加到三台计算机（VDA 101–103）中的每一台。
- 共享交付组中的桌面是使用名为“Red”的标签限制创建的。桌面只能在该交付组中具有“Red”标签的计算机上启动：VDA 101 和 102。
- 应用程序组是使用“Orange”标签限制创建的，因此其每个应用程序（计算器和记事本）只能在该交付组中具有“Orange”标签的计算机上启动：VDA 102 和 103。

计算机 VDA 102 具有两个标签（Red 和 Orange），因此可以考虑用于启动应用程序和桌面。

示例 2：更复杂的布局

本示例包含多个使用标签限制创建的应用程序组。这样，与仅使用交付组相比，可以使用更少的计算机交付更多的应用程序。

如何配置示例 2 显示了在此示例中用于创建和应用标签，然后配置标签限制的步骤。



此示例使用 10 台计算机 (VDA 101–110)、一个交付组 (D01) 和三个应用程序组 (A100、A200、A300)。通过对每台计算机应用标签，然后在创建每个应用程序组时指定标签限制，可以实现以下目的：

- 组中的会计用户可以在五台计算机 (VDA 101–105) 上访问他们所需的应用程序
- 组中的 CAD 设计人员可以在五台计算机 (VDA 106-110) 上访问他们所需的应用程序
- 组中需要 Office 应用程序的用户可以在 10 台计算机 (VDA 101–110) 上访问 Office 应用程序

仅使用 10 台计算机，且只有一个交付组。如果仅使用交付组（不使用应用程序组），则需要两倍的计算机，因为一台计算机只能属于一个交付组。

管理标签和标签限制

通过 Web Studio 中的**管理标签**操作，可以对选定项目创建、添加（应用）、编辑和删除标签。

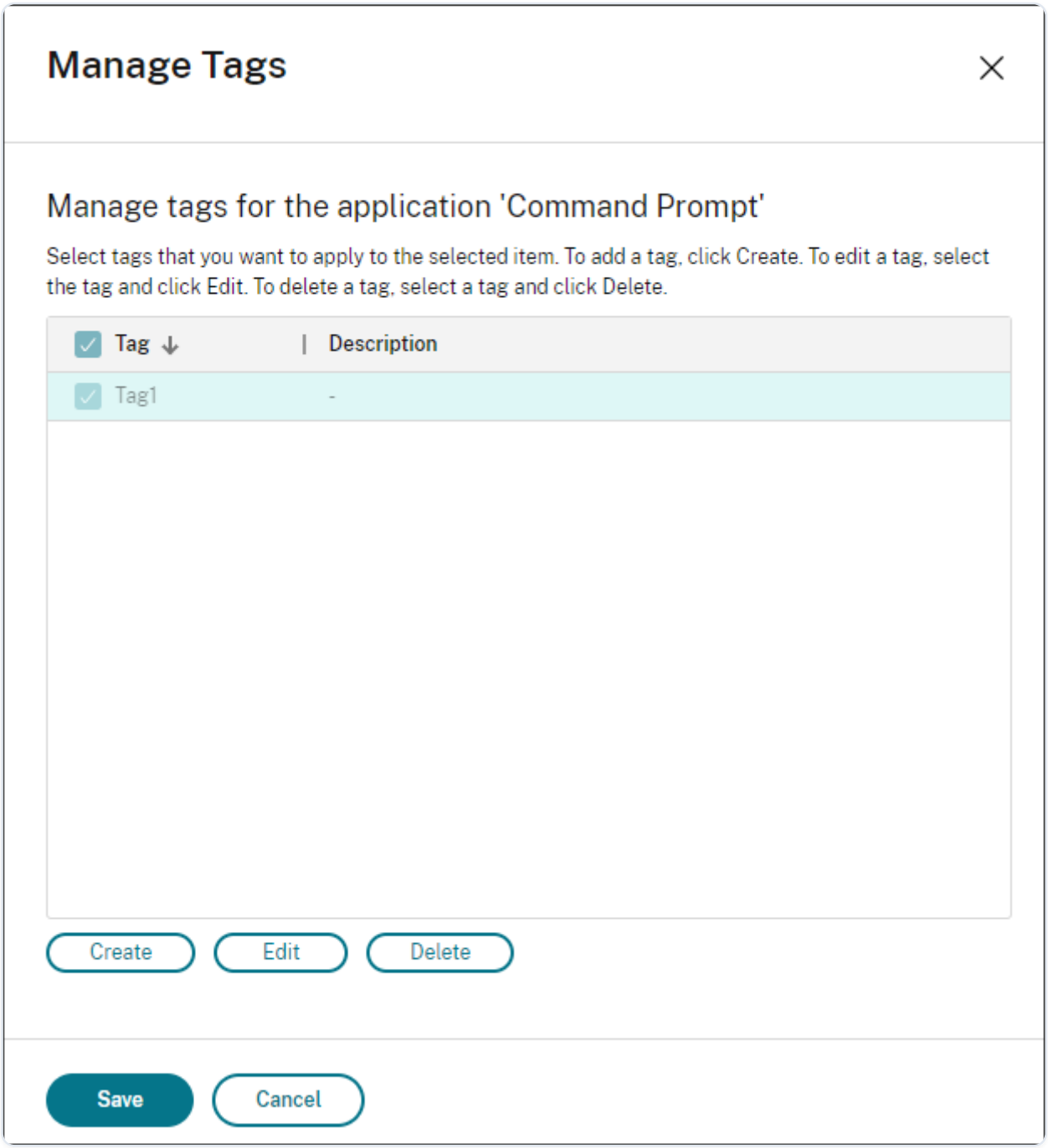
（例外：用于策略分配的标签通过 Web Studio 中的**管理标签**操作创建、编辑和删除。但是，标签是在创建策略时应用（分配）的。有关详细信息，请参阅创建策略。）

在交付组中创建或编辑桌面以及创建和编辑应用程序组时，将配置标签限制。

在 Web Studio 中使用“管理标签”对话框

在 Web Studio 中，选择要应用标签的项目（一台或多台计算机、应用程序、桌面、交付组或应用程序组），然后在操作栏中选择**管理标签**。该对话框列出了站点中已创建的所有标签，而不仅仅是您选择的项目所使用的标签。

- 包含复选标记的复选框表示该标签已添加到所选项目。（在下面的屏幕截图中，所选计算机已应用名为“Tag1”的标签。）
- 如果您选择了多个项目，则包含连字符的复选框表示部分（但并非所有）选定项目已添加该标签。



以下操作可从**管理标签**对话框中获取。请务必查看使用标签时的注意事项。

- **创建标签：**

  点击“**创建**”。输入名称和描述。标签名称必须唯一且不区分大小写。然后点击“**确定**”。（创建标签不会自动将其应用于您选择的任何项目。使用复选框应用标签。）

- **添加（应用）一个或多个标签：**

  选中标签名称旁边的复选框。如果您选择了多个项目，并且标签旁边的复选框包含连字符（表示部分而非全部选定项目已应用该标签），则将其更改为复选标记会影响所有选定的计算机。

  如果您尝试将标签添加到一个或多个计算机，并且该标签在应用程序组中用作限制，则会收到警告，指出此操作可能导致这些计算机可用于启动。如果这是您的意图，请继续。

- **删除一个或多个标签：**

  清除标签名称旁边的复选框。如果您选择了多个项目，并且标签旁边的复选框包含连字符（表示部分而非全部选定项目已应用该标签），则清除该复选框会从所有选定的计算机中删除该标签。

  如果您尝试从将某个标签用作限制的计算机中删除该标签，则会收到警告，指出此操作可能会影响哪些计算机被考虑用于启动。如果这是您的意图，请继续。

- **编辑标签：**

  选择一个标签，然后点击“**编辑**”。输入新名称、新描述或两者。您一次只能编辑一个标签。

- **删除一个或多个标签：**

  选择标签，然后点击“**删除**”。“删除标签”对话框会显示当前有多少项目正在使用所选标签（例如“2 台计算机”）。点击一个项目以显示更多信息。例如，点击“2 台计算机”项目会显示已应用该标签的两台计算机的名称。确认是否要删除这些标签。

  您不能使用 Web Studio 删除用作限制的标签。首先，编辑应用程序组并删除标签限制或选择其他标签。

在“**管理标签**”对话框中完成后，点击“**保存**”。

要查看计算机是否已应用任何标签：在左侧窗格中选择“**交付组**”。在中间窗格中选择一个交付组，然后在操作栏中选择“**查看计算机**”。在中间窗格中选择一台计算机，然后在“**详细信息**”窗格中选择“**标签**”选项卡。

管理标签限制

配置标签限制是一个多步骤过程：首先创建标签并将其添加/应用到计算机。然后，将限制添加到应用程序组或桌面。

- **创建并应用标签：**

创建标签，然后使用前面描述的“**管理标签**”操作将其添加（应用）到受标签限制影响的计算机。

- **将标签限制添加到应用程序组：**

  创建或编辑应用程序组。在“**交付组**”页面上，选择“**将启动限制到具有该标签的计算机**”，然后从列表中选择该标签。

- **更改或删除应用程序组上的标签限制：**

  编辑组。在“**交付组**”页面上，可以从列表中选择其他标签，也可以通过清除“**将启动限制到具有该标签的计算机**”来完全删除标签限制。

- **将标签限制添加到桌面：**

  创建或编辑交付组。在“**桌面**”页面上，单击“**添加**”或“**编辑**”。在“添加桌面”对话框中，选择“**将启动限制到具有该标签的计算机**”，然后从菜单中选择该标签。

- **更改或删除交付组上的标签限制：**

  编辑组。在“桌面”页面上，单击“**编辑**”。在对话框中，可以从列表中选择其他标签，也可以通过清除“**将启动限制到具有该标签的计算机**”来完全删除标签限制。

使用标签时的注意事项

应用于项目的标签可以用于不同的目的，因此请记住，添加、删除和移除标签可能会产生意外影响。您可以使用标签在 Web Studio 搜索字段中对计算机显示进行排序。在配置应用程序组或桌面时，可以将同一标签用作限制。该标签将启动考虑范围限制为仅包含指定交付组中具有该标签的计算机。

当您尝试将标签添加到计算机，而该标签已配置为桌面或应用程序组的标签限制时，将显示警告。添加该标签可能会使计算机可用于启动其他应用程序或桌面。如果这是您的预期，请继续。如果不是，您可以取消操作。

例如，假设您创建了一个具有“Red”标签限制的应用程序组。稍后，您在该应用程序组使用的相同交付组中添加了其他几台计算机。如果您随后尝试将“Red”标签添加到这些计算机，Web Studio 将显示类似以下内容的消息：“标签‘Red’用作以下应用程序组的限制。添加此标签可能会使选定的计算机可用于在此应用程序组中启动应用程序。”然后，您可以确认或取消将该标签添加到这些额外的计算机。

同样，如果应用程序组使用标签来限制启动，Web Studio 会警告您，在编辑组以将其作为限制删除之前，您无法删除该标签。（如果允许您删除用作应用程序组中限制的标签，则可能会导致允许应用程序在与该应用程序组关联的交付组中的所有计算机上启动。）如果标签用作桌面启动的限制，则同样禁止删除该标签。在您编辑交付组中的应用程序组或桌面以删除该标签限制后，即可删除该标签。

并非所有计算机都可能具有相同的应用程序集。一个用户可以属于多个应用程序组，每个组都有不同的标签限制以及来自交付组的不同或重叠的计算机集。下表列出了如何确定计算机注意事项。

当应用程序已添加到	所选交付组中的这些计算机被视为可用于启动
一个没有标签限制的应用程序组	任何计算机。
一个具有标签限制 A 的应用程序组	已应用标签 A 的计算机。
两个应用程序组，一个具有标签限制 A，另一个具有标签限制 B	具有标签 A 和标签 B 的计算机。如果没有可用，则为具有标签 A 或标签 B 的计算机。
两个应用程序组，一个具有标签限制 A，另一个没有标签限制	具有标签 A 的计算机。如果没有可用，则为任何计算机。

如果您在计算机重新启动计划中使用了标签限制，则您所做的任何影响标签应用或限制的更改都会影响下一个计算机重新启动周期。它不会影响在进行更改时正在进行的任何重新启动周期。

如何配置示例 2

以下序列展示了创建和应用标签，然后为第二个示例中所示的应用程序组配置标签限制的步骤。

VDA 和应用程序已安装在计算机上，并且已创建交付组。

创建标签并将其应用于计算机：

1. 在 Web Studio 中，选择交付组 D01，然后在操作栏中选择 **View Machines**。
2. 选择计算机 VDA 101–105，然后在操作栏中选择 **Manage Tags**。
3. 在“管理标签”对话框中，单击 **Create**，然后创建名为 `CADApps` 的标签。单击 **OK**。
4. 再次单击 **Create**，然后创建名为 OfficeApps 的标签。单击 **OK**。
5. 在 **Manage Tags** 对话框中，通过启用每个标签名称（`CADApps` 和 `OfficeApps`）旁边的复选框，将新创建的标签添加（应用）到选定的计算机。完成后，关闭对话框。
6. 选择交付组 D01，在操作栏中选择 **View Machines**。
7. 选择计算机 VDA 106–110，然后在操作栏中选择 **Manage Tags**。
8. 在 **Manage Tags** 对话框中，单击 **Create**。创建名为 `AcctgApps` 的标签。单击 **OK**。
9. 通过单击每个标签名称旁边的复选框，将新创建的 `AcctgApps` 标签和 `OfficeApps` 标签应用于选定的计算机，然后关闭对话框。

创建具有标签限制的应用程序组。

1. 在 Web Studio 中，在左侧窗格中选择 **Applications**，选择 **Application Groups** 选项卡，然后在操作栏中选择 **Create Application Group**。“创建应用程序组”向导启动。
2. 在向导的 **Delivery Groups** 页面上，选择交付组 D01。选择 **Restrict launches to machines with tag**，然后从列表中选择 `AcctgApps` 标签。
3. 完成向导，指定会计用户和会计应用程序。（添加应用程序时，选择**从“开始”菜单**源，该源会在具有 `AcctgApps` 标记的计算机上搜索应用程序。）在**摘要**页面上，将组命名为 `A100`。
4. 重复上述步骤以创建应用程序组 `A200`，指定具有 `CADApps` 标记的计算机以及相应的用户和应用程序。
5. 重复步骤以创建应用程序组 `A300`，指定具有 `OfficeApps` 标记的计算机以及相应的用户和应用程序。

计算机目录上的标记

您可以在计算机目录上使用标记。创建标记然后将其应用于目录的总体顺序与前面所述相同。但是，仅通过 PowerShell 界面支持将标记应用于目录。您不能使用 Web Studio 将标记应用于目录或从目录中删除标记。Web Studio 中的目录显示不指示是否应用了标记。

摘要：您可以使用 Web Studio 或 PowerShell 创建或删除用于目录的标记。使用 PowerShell 将标记应用于目录。

以下是一些将标记与目录结合使用的示例：

- 交付组包含来自多个目录的计算机，但您希望某个操作（例如重新启动计划）仅影响特定目录中的计算机。将标记应用于该目录即可实现此目的。
- 在应用程序组中，您希望将应用程序会话限制为特定目录中的计算机。将标记应用于该目录即可实现此目的。

受影响的 PowerShell cmdlet：

- 您可以将目录对象传递给 `Add-BrokerTag` 和 `Remove-BrokerTag` 等 cmdlet。
- `Get-BrokerTagUsage` 显示有多少个目录包含标记。
- `Get-BrokerCatalog` 具有一个名为 `Tags` 的属性。

例如，以下 cmdlet 将名为 `fy2018` 的标记添加到名为 `acctg` 的目录中：`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`。（该标记之前已使用 Web Studio 或 PowerShell 创建。）

有关更多指导和语法，请参阅 PowerShell cmdlet 帮助。

自动标签

使用自动标签，您可以定义规则以自动添加和删除计算机、应用程序组、应用程序、桌面组或桌面上的标签。如果标签不符合定义的规则，它们也会被自动删除。此增强功能消除了维护定期运行以优化环境的不同脚本的需要。

用例

通过自动标记，您可以实施与您的业务驱动因素相关的规则，例如降低成本、优化基础架构和推动消费。以下是一些用例：

- **回收未使用的 VDI** - 将超过预配置天数未使用的专用工作负载释放到可用池中。
- **清除应用程序冗余** - 通过识别超过预配置天数未使用的应用程序来减少应用程序冗余。
- **功能级别低于 X 的交付组** - 查找功能级别低于特定级别的交付组。
- **不活跃用户** - 回收超过预配置天数未登录的用户的资源。

> **注意：**
>
> 如果用户在 30 天后登录一台超过 30 天未使用的计算机，则下次运行时将从该计算机中删除附加到该计算机的标签。

PowerShell 命令

您可以使用 PowerShell 命令创建自动标签。创建自动标签规则后，它会以 3600 秒的频率进行评估。有关详细信息，请参阅 New-BrokerAutoTagRule。

`New-BrokerAutoTagRule` 的参数包括：

- 名称：规则的通用名称
- 对象类型：计算机
- 规则文本：定义规则的筛选器。
- 标签 Uid：您要关联的标签 ID。

示例

1. 要标记超过 30 天未使用的专用 VDI：

```
New-BrokerAutoTagRule -Name ‘UnusedVdi’ -ObjectType ‘Machine’ -RuleText
“-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne
```

```
`"InUse`" -and ( LastConnectionTime -lt '-30' -or LastConnectionTime
-eq `$null ) }" -TagUid 123
```

规则配置完成后，带有标签 **unused-VDI** 的计算机将被释放。

2. 标记功能级别低于 X 的交付组（使用 **L7_20** 作为阈值功能级别）：

```
New-BrokerAutoTagRule -Name 'LowFL' -ObjectType 'DesktopGroup'
-RuleText " -Filter { MinimumFunctionalLevel -lt 'L7_20' } " -TagUid
143
```

3. 标记未发布到文件夹中的用户可见应用程序：

```
New-BrokerAutoTagRule -Name 'NoFolder' -ObjectType 'Application'
-RuleText "-Enabled $true -Filter { ClientFolder -eq $null } " -TagUid
153`
```

更多信息

博客文章：如何将桌面分配给特定服务器。

在任务中心监控和管理任务

任务中心提供 Citrix Virtual Apps and Desktops™ 中计划和重复任务的集中视图。您可以在 Studio 中实时跟踪任务状态并从一个位置管理任务。

> **注意：**
>
> 在此版本中，任务中心支持 Machine Creation Services (MCS) 任务。对其他任务类型的支持将在未来版本中推出。

访问任务中心

1. 打开 Studio 控制台。
2. 在右上角，选择**日历**图标。

   任务中心面板打开，显示任务活动。

查看和管理任务

在任务中心，您可以：

- 使用搜索栏搜索和筛选任务。
- 跟踪实时任务状态。
- 对任务执行操作，例如取消或重新运行。

每个任务条目都显示以下详细信息：

字段	描述
状态	任务的当前状态：成功、已取消、正在进行或失败
任务目标	任务适用的资源
任务类型	操作类型（例如，操作系统磁盘重置、VM 备份）
描述	操作摘要
任务 ID	用于跟踪的唯一标识符

支持的任务类型

- 硬件更新
- 操作系统磁盘重置

用户配置文件

默认情况下，在安装 Virtual Delivery Agent 时，Citrix Profile Management 会在主映像上静默安装，但您不必将 Profile Management 用作配置文件解决方案。

为了满足用户不同的需求，您可以使用 Citrix Virtual Apps and Desktops™ 策略将不同的配置文件行为应用于每个交付组中的计算机。例如，一个交付组可能需要 Citrix 强制配置文件（其模板存储在一个网络位置），而另一个交付组可能需要存储在另一个位置并包含多个重定向文件夹的 Citrix 漫游配置文件。

- 如果组织中的其他管理员负责 Citrix Virtual Apps and Desktops™ 策略，请与他们协作，确保他们在所有交付组中设置任何与配置文件相关的策略。

- Profile Management 策略还可以在组策略、Profile Management .ini 文件中以及在各个虚拟机本地进行设置。定义配置文件行为的这些多种方式按以下顺序读取：

  a. 组策略（.adm 或 .admx 文件）

  b. 策略节点中的 Citrix Virtual Apps and Desktops 策略

  c. 用户连接到的虚拟机上的本地策略

  d. 配置文件管理 .ini 文件

  例如，如果您在组策略和策略节点中配置相同的策略，系统将读取组策略中的策略设置并忽略 Citrix Virtual Apps and Desktops 策略设置。

无论您选择哪种配置文件解决方案，Director 管理员都可以访问诊断信息并对用户配置文件进行故障排除。有关详细信息，请参阅 Director 文档。

自动配置

桌面类型会根据 Virtual Delivery Agent 安装自动检测，并且除了您在 Studio 中所做的配置选择之外，还会相应地设置 Profile Management 默认值。

Profile Management 调整的策略显示在下表中。任何非默认策略设置都将保留，并且不会被此功能覆盖。有关每个策略的信息，请查阅 Profile Management 文档。创建配置文件的计算机类型会影响调整的策略。主要因素是计算机是持久的还是预配的，以及它们是多用户共享还是专用于单个用户。

持久系统具有某种类型的本地存储，其内容在系统关闭时预计会持久存在。持久系统可能会采用 SAN 等存储技术来模拟本地磁盘。相比之下，预配系统是“即时”从基本磁盘和某种身份磁盘创建的。本地存储通常由 RAM 磁盘或网络磁盘模拟，后者通常由具有高速链路的 SAN 提供。预配技术通常是 Citrix Provisioning 或 Machine Creation Services™（或第三方等效产品）。有时，预配系统具有持久本地存储。这些系统被归类为持久系统。

这两个因素共同定义了以下计算机类型：

- **持久且专用**。示例包括使用 Machine Creation Services 创建的具有静态分配和持久本地存储的单会话操作系统计算机、物理工作站和笔记本电脑。
- **持久且共享**。示例包括使用 Machine Creation Services 创建的多会话操作系统计算机和 Citrix Virtual Apps 服务器。
- **预配且专用**。示例包括使用 Citrix Provisioning Service（在 Citrix Virtual Desktops™ 中）创建的具有静态分配但没有持久存储的单会话操作系统计算机。
- **预配且共享**。示例包括使用 Citrix Provisioning™ Service（在 Citrix Virtual Desktops 中）创建的具有随机分配的单会话操作系统计算机和 Citrix Virtual Apps 服务器。

以下配置文件管理策略设置是针对不同计算机类型的建议准则。它们在大多数情况下都适用，但您可能需要根据部署要求进行调整。

重要提示：

注销时删除本地缓存的配置文件、**配置文件流技术**和**始终缓存**由自动配置功能强制执行。请手动调整其他策略。

持久性计算机

策略	持久且专用	持久且共享
在注销时删除本地缓存的配置文件	已禁用	启用
配置文件流技术	已禁用	启用
始终缓存	已启用（注 1）	已禁用（注 2）
活动回写	已禁用	已禁用（注 3）
处理本地管理员的登录	启用	已禁用（注 4）

预配的计算机

策略	预配和专用	预配和共享
在注销时删除本地缓存的配置文件	已禁用（注 5）	启用
配置文件流技术	启用	启用
始终缓存	已禁用（注 6）	已禁用
活动回写	启用	启用
处理本地管理员的登录	启用	已启用（注 7）

1. 由于此计算机类型已禁用**配置文件流**，因此**始终缓存**设置始终被忽略。

2. 禁用**始终缓存**。但是，您可以通过启用此策略并使用它来定义文件大小限制（以 MB 为单位），确保在登录后尽快将大文件加载到配置文件中。任何达到或超过此大小的文件都将尽快在本地缓存。
3. 禁用**活动回写**，除非是为了保存漫游于 Citrix Virtual Apps 服务器之间的用户配置文件中的更改。在这种情况下，请启用此策略。
4. 禁用**处理本地管理员登录**，托管共享桌面除外。在这种情况下，请启用此策略。
5. 禁用**注销时删除本地缓存的配置文件**。此设置会保留本地缓存的配置文件。由于计算机在注销时会重置但会分配给单个用户，因此如果配置文件已缓存，登录速度会更快。
6. 禁用**始终缓存**。但是，您可以通过启用此策略并使用它来定义文件大小限制（以 MB 为单位），确保在登录后尽快将大文件加载到配置文件中。任何达到或超过此大小的文件都将尽快在本地缓存。
7. 启用**处理本地管理员登录**，漫游于 Citrix Virtual Apps and Desktops 服务器之间的用户配置文件除外。在这种情况下，请禁用此策略。

文件夹重定向

文件夹重定向允许您将用户数据存储在配置文件存储位置以外的网络共享上。文件夹重定向可减小配置文件大小并缩短加载时间，但可能会影响网络带宽。文件夹重定向不要求使用 Citrix 用户配置文件。您可以选择自行管理用户配置文件，并仍然重定向文件夹。

在 Studio 中使用 Citrix 策略配置文件夹重定向。

- 确保用于存储重定向文件夹内容的网络位置可用并具有正确的权限。将验证位置属性。
- 重定向文件夹在网络上设置，其内容在用户登录时从用户的虚拟桌面填充。

仅使用 Citrix 策略或 Active Directory 组策略对象配置文件夹重定向，不要同时使用两者。同时使用两种策略引擎配置文件夹重定向可能会导致不可预测的行为。

高级文件夹重定向

在具有多个操作系统 (OS) 的部署中，您可能希望用户的部分配置文件由每个 OS 共享。配置文件的其余部分不共享，仅由一个 OS 使用。为了确保跨 OS 的一致用户体验，您需要为每个 OS 提供不同的配置，即高级文件夹重定向。例如，在两个 OS 上运行的应用程序的不同版本可能需要读取或编辑共享文件，因此您决定将其重定向到两个版本都可以访问的单个网络位置。或者，由于两个 OS 中 **“开始”菜单** 文件夹的内容结构不同，您决定只重定向一个文件夹，而不是两个。此方法将每个 OS 上的 **“开始”菜单** 文件夹及其内容分开，从而确保用户获得一致的体验。

如果您的部署需要高级文件夹重定向，则必须了解用户配置文件数据的结构，并确定其中哪些部分可以在 OS 之间共享。除非正确使用文件夹重定向，否则可能会导致不可预测的行为。

若要在高级部署中重定向文件夹：

- 为每个 OS 使用单独的交付组。
- 了解您的虚拟应用程序（包括虚拟桌面上的应用程序）存储用户数据和设置的位置，并了解数据的结构。
- 对于可以安全漫游的共享配置文件数据（因为它在每个 OS 中结构相同），请在每个交付组中重定向包含文件夹。
- 对于无法漫游的非共享配置文件数据，请仅在其中一个桌面组中重定向包含文件夹，通常是使用最频繁的 OS 或数据最相关的 OS。或者，对于无法在 OS 之间漫游的非共享数据，请将两个系统上的包含文件夹重定向到单独的网络位置。

高级部署示例

该部署包含在 Windows 10 桌面上运行的应用程序（包括 Microsoft Outlook 和 Internet Explorer 的版本）以及由 Windows Server 2019 交付的应用程序（包括 Outlook 和 Internet Explorer 的其他版本）。您已经为这两个 OS 设置了两个交付组。用户希望在这两个应用程序的两个版本中访问相同的 **“联系人”** 和 **“收藏夹”** 集。

重要提示： 以下决定和建议适用于所描述的 OS 和部署。在您的组织中，您选择重定向的文件夹以及是否决定共享它们取决于您特定部署的各种独特因素。

- 使用应用于交付组的策略，您可以选择以下文件夹进行重定向。

文件夹	在 WINDOWS 10 中重定向？	在 WINDOWS SERVER 2019 中重定向？
我的文档	是	是
应用程序数据	否	否
联系人	是	是
桌面	是	否
下载	否	否
收藏夹	是	是
链接	是	否
我的音乐	是	是

文件夹	在 WINDOWS 10 中重定向？	在 WINDOWS SERVER 2019 中重定向？
我的图片	是	是
我的视频	是	是
搜索	是	否
保存的游戏	否	否
开始菜单	是	否

- 对于共享的重定向文件夹：
  - 在分析了不同版本的 Outlook 和 Internet Explorer 保存的数据结构后，您决定可以安全地共享“**联系人**”和“**收藏夹**”文件夹。
  - 您知道“**我的文档**”、“**我的音乐**”、“**我的图片**”和“**我的视频**”文件夹的结构在所有操作系统中都是标准的。因此，可以安全地将这些文件夹存储在每个交付组的相同网络位置。
- 对于非共享的重定向文件夹：
  - 您不会在 Windows Server 交付组中重定向“桌面”、“链接”、“搜索”或“**开始菜单**”文件夹，因为这些文件夹中的数据在两个操作系统中的组织方式不同。因此，无法共享。
  - 为确保此非共享数据的可预测行为，您仅在 Windows 10 交付组中重定向它。用户在日常工作中更频繁地使用 Windows 10。用户仅偶尔访问 Windows Server 交付的应用程序。此外，在这种情况下，非共享数据与桌面环境而非应用程序环境更相关。例如，桌面快捷方式存储在 **Desktop** 文件夹中，如果它们源自 Windows 10 计算机而不是 Windows Server 计算机，则可能很有用。
- 对于未重定向的文件夹：
  - 您不希望用用户下载的文件使服务器变得混乱，因此选择不重定向“下载”文件夹
  - 来自单个应用程序的数据可能会导致兼容性和性能问题，因此您决定不重定向“应用程序数据”文件夹

有关文件夹重定向的更多信息，请参阅 文件夹重定向、脱机文件和漫游用户配置文件概述。

文件夹重定向和排除项

在 Citrix Profile Management 中（但不在 Studio 中），一项性能增强功能允许您使用排除项阻止处理文件夹。如果使用此功能，请勿排除任何重定向的文件夹。文件夹重定向和排除功能协同工作。

确保不排除任何重定向的文件夹，可让 Profile Management 将它们移回配置文件文件夹结构中，并在您以后决定不重定向它们时保留数据完整性。有关排除项的更多信息，请参阅 包含和排除项目。

VDA 注册

简介

> **注意：**
>
> 在本地环境中，VDA 向 Delivery Controller 注册。在 Citrix Cloud 服务环境中，VDA 向 Cloud Connector 注册。在混合环境中，一些 VDA 向 Delivery Controller 注册，而另一些则向 Cloud Connector 注册。

> VDA 必须先向站点中的一个或多个 Controller 或 Cloud Connector 注册（建立通信），然后才能使用。VDA 通过检查名为 `ListofDDCs` 的列表来查找 Controller 或 Connector。VDA 上的 `ListOfDDCs` 包含将该 VDA 指向站点上的 Controller 或 Cloud Connector 的 DNS 条目。为了实现负载平衡，VDA 会自动将连接分布到列表中的所有 Controller 或 Cloud Connector。

为什么 VDA 注册如此重要？

- 从安全角度来看，注册是一项敏感操作。您正在 Controller 或 Cloud Connector 与 VDA 之间建立连接。对于此类敏感操作，如果一切不完美，则预期行为是拒绝连接。您实际上正在建立两个独立的通信通道：VDA 到 Controller 或 Cloud Connector，以及 Controller 或 Cloud Connector 到 VDA。连接使用 Kerberos，因此时间同步和域成员资格问题是不可原谅的。Kerberos 使用服务主体名称 (SPN)，因此您不能使用负载平衡的 IP\\主机名。
- 如果 VDA 没有准确且最新的 Controller 或 Cloud Connector 信息（在您添加和删除 Controller 或 Cloud Connector 时），VDA 可能会拒绝由未列出的 Controller 或 Cloud Connector 代理的会话启动。无效条目可能会延迟虚拟桌面系统软件的启动。VDA 不会接受来自未知且不受信任的 Controller 或 Cloud Connector 的连接。

除了 `ListofDDCs` 之外，`ListOfSIDs`（安全 ID）还指示 `ListofDDCs` 中哪些计算机是受信任的。`ListofSIDs` 可用于减少 Active Directory 上的负载，或避免来自受损 DNS 服务器的潜在安全威胁。有关详细信息，请参阅 ListOfSIDs。

如果 `ListofDDCs` 指定了多个 Controller 或 Cloud Connector，VDA 会尝试以随机顺序连接它们。在本地部署中，`ListofDDCs` 还可以包含 Controller 组。VDA 会尝试连接组中的每个 Controller，然后才会转到 `ListofDDCs` 中的其他条目。

Citrix Virtual Apps and Desktops™ 在 VDA 安装期间会自动测试与已配置的 Controller 或 Cloud Connector 的连接。如果无法访问 Controller 或 Cloud Connector，则会显示错误。如果您忽略了无法联系 Controller 或 Cloud Connector 的警告（或者在 VDA 安装期间未指定 Controller 或 Cloud Connector 地址），则会显示消息提醒您。

配置 Controller 或 Cloud Connector 地址的方法

管理员选择 VDA 首次注册（初始注册）时要使用的配置方法。在初始注册期间，会在 VDA 上创建一个持久缓存。在后续注册期间，除非检测到配置更改，否则 VDA 会从此本地缓存中检索 Controller 或 Cloud Connector 列表。

在后续注册期间检索该列表的最简单方法是使用自动更新功能。自动更新默认启用。有关详细信息，请参阅自动更新。

有多种方法可以在 VDA 上配置 Controller 或 Cloud Connector 地址。

- 基于策略（LGPO 或 GPO）
- 基于注册表（手动、组策略首选项 (GPP)、在 VDA 安装期间指定）
- 基于 Active Directory OU（旧版 OU 发现）
- 基于 MCS (personality.ini)

在安装 VDA 时，您可以指定初始注册方法。（如果禁用自动更新，则在 VDA 安装期间选择的方法将用于后续注册。）

下图显示了 VDA 安装向导的**交付控制器**页面。

VDA 安装向导中的交付控制器页面(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/vda-install-controllers-all.png)

基于策略 (LGPO\\GPO)

Citrix® 建议使用 GPO 进行初始 VDA 注册。它具有最高优先级。（尽管自动更新被列为最高优先级，但自动更新仅在初始注册后使用。）基于策略的注册提供了使用组策略进行配置的集中化优势。

要指定此方法，请完成以下两个步骤：

- 在 VDA 安装向导的**交付控制器**页面上，选择**稍后执行 (高级)**。即使您在 VDA 安装期间未指定控制器地址，向导也会多次提醒您指定控制器地址。（VDA 注册非常重要。）

- 通过 Citrix 策略使用 `Virtual Delivery Agent Settings > Controllers` 设置启用或禁用基于策略的 VDA 注册。（如果安全性是您的首要任务，请使用 `Virtual Delivery Agent Settings > Controller SIDs` 设置。）

此设置存储在 `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)` 下。

基于注册表

要指定此方法，请完成以下步骤之一：

- 在 VDA 安装向导的**交付控制器**页面上，选择**手动执行**。然后，输入已安装控制器的 FQDN，然后单击**添加**。如果您安装了更多控制器，请添加它们的地址。
- 对于命令行 VDA 安装，请使用 /controllers 选项并指定已安装的控制器或云连接器的 FQDN。

此信息存储在注册表项 `HKLM\Software\Citrix\VirtualDesktopAgent` 或 `HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent` 下的注册表值 `ListOfDDCs` 中。

您也可以手动配置此注册表项或使用组策略首选项 (GPP)。此方法可能优于基于策略的方法（例如，如果您希望对不同的控制器或云连接器进行条件处理，例如：对于以 XDW-001- 开头的计算机名称，使用 XDC-001）。

更新 `ListOfDDCs` 注册表项，其中列出了站点中所有控制器或云连接器的 FQDN。（此项等同于 Active Directory 站点 OU。）

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

如果 `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent` 注册表位置同时包含 `ListOfDDCs` 和 `FarmGUID` 键，则使用 `ListOfDDCs` 进行控制器或云连接器发现。如果在 VDA 安装期间指定了站点 OU，则存在 `FarmGUID`。（这可能用于旧版部署。）

（可选）更新 `ListOfSIDs` 注册表项（有关详细信息，请参阅 ListOfSIDs：

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)`

请记住：如果您还通过 Citrix 策略启用了基于策略的 VDA 注册，该策略会覆盖您在 VDA 安装期间指定的设置，因为它是一种优先级更高的方法。

基于 Active Directory OU（旧版）

此方法主要用于向后兼容，不建议使用。如果您仍在使用此方法，Citrix 建议更改为其他方法。

要指定此方法，请完成以下两个步骤：

- 在 VDA 安装向导的“**交付控制器**”页面上，选择“**从 Active Directory 中选择位置**”。
- 使用 `Set-ADControllerDiscovery.ps1` 脚本（在每个控制器上均可用）。此外，在每个 VDA 上配置 `FarmGuid` 注册表项以指向正确的 OU。此设置可以使用组策略进行配置。

基于 MCS

如果您使用 MCS 预配 VM，MCS 会设置控制器或云连接器列表。此功能与自动更新配合使用。创建目录时，MCS 会在初始预配期间将控制器或云连接器列表注入到 `Personality.ini` 文件中。自动更新会使列表保持最新。

要指定此方法，请在 VDA 安装向导的“**交付控制器**”页面上，选择“**让 Machine Creation Services™ 完成此操作**”。

审查和建议

最佳实践：

- 使用组策略注册方法进行初始注册。
- 使用自动更新（默认启用）以使您的控制器列表保持最新。
- 在多区域部署中，使用组策略进行初始配置（至少包含两个控制器或云连接器）。将 VDA 指向其区域本地的控制器或云连接器。使用自动更新使其保持最新。自动更新会自动优化卫星区域中 VDA 的 `ListofDDCs`。
- 在 `ListOfDDCs` 注册表项上列出多个控制器，以空格分隔，以防止在控制器不可用时出现注册问题。例如：

```
DDC7x.xd.local DDC7xHA.xd.local



32-bit: HKEY_LOCAL_MACHINE
\Software\Citrix\VirtualDesktopAgent\ListOfDDCs



HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs
(REG_SZ)
```

- 确保 `ListofDDCs` 下列出的所有值都映射到有效的完全限定域名，以防止启动注册延迟。

自动更新

自动更新（在 XenApp 和 XenDesktop 7.6 中引入）默认启用。它是使 VDA 注册保持最新状态的最有效方法。尽管不用于初始注册，但自动更新软件会在初始注册发生时将 `ListofDDCs` 下载并存储在 VDA 上的持久缓存中。此过程针对每个 VDA 执行。缓存还包含计算机策略信息，这可确保策略设置在重新启动后仍保留。

使用 MCS 或 Citrix Provisioning™ 预配计算机时支持自动更新，但 Citrix Provisioning 服务器端缓存除外。服务器端缓存不是常见方案，因为自动更新缓存没有持久存储。

要指定此方法：

- 通过包含设置 `Virtual Delivery Agent Settings > Enable auto update of Controllers` 的 Citrix 策略启用或禁用自动更新。此设置默认启用。

工作原理：

- 每次 VDA 重新注册（例如，在计算机重新启动后），缓存都会更新。每个控制器或云连接器还会每 90 分钟检查一次站点数据库。如果自上次检查以来添加或删除了控制器或云连接器，或者发生了影响 VDA 注册的策略更改，则控制器或云连接器会向其注册的 VDA 发送更新列表，并且缓存会更新。VDA 接受其最近缓存列表中的所有控制器或云连接器的连接。
- 如果 VDA 收到的列表中不包含其注册的控制器或云连接器（换句话说，该控制器或云连接器已从站点中删除），则 VDA 会重新注册，从 `ListofDDCs` 中的控制器或云连接器中进行选择。

示例：

- 一个部署有三个控制器：A、B 和 C。一个 VDA 注册到控制器 B（在 VDA 安装期间指定）。
- 稍后，将两个控制器（D 和 E）添加到站点。在 90 分钟内，VDA 会收到更新列表，然后接受来自控制器 A、B、C、D 和 E 的连接。（在 VDA 重新启动之前，负载不会平均分配到所有控制器。）
- 再后来，控制器 B 被移动到另一个站点。在 90 分钟内，原始站点中的 VDA 会收到更新列表，因为自上次检查以来控制器已发生更改。最初注册到控制器 B 的 VDA（该控制器已不在列表中）会重新注册，从当前列表中的控制器（A、C、D 和 E）中进行选择。

在多区域部署中，卫星区域中的自动更新会首先自动缓存所有本地控制器。主区域中的所有控制器都缓存在备份组中。如果卫星区域中没有可用的本地控制器，则会尝试向主区域中的控制器注册。

如以下示例所示，缓存文件包含主机名和安全 ID 列表 (`ListofSIDs`)。VDA 不查询 SID，因此减少了 Active Directory 负载。

VDA 注册缓存文件示例图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/vda-registration-cache-file.png)

您可以使用 WMI 调用检索缓存文件。但是，它存储在只有 SYSTEM 帐户才能读取的位置。

> **重要提示：**
>
> 此信息仅供参考。请勿修改此文件。对此文件或文件夹的任何修改都将导致不受支持的配置。

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class
"Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

如果出于安全原因（与减少 Active Directory 负载不同）需要手动配置 `ListofSIDs`，则无法使用自动更新功能。有关详细信息，请参阅 ListOfSIDs。

自动更新优先级的例外

尽管自动更新通常在所有 VDA 注册方法中具有最高优先级并会覆盖其他方法的设置，但存在一个例外。缓存中的 `NonAutoListOfDDCs` 元素指定了初始 VDA 配置方法。自动更新会监视此信息。如果初始注册方法发生更改，注册过程将跳过自动更新，并使用下一个最高优先级的配置方法。当您将 VDA 移动到另一个站点时（例如，在灾难恢复期间），此过程会很有帮助。

配置注意事项

查看常见的 VDA 注册配置。

<iframe src="https://www.youtube.com/embed/MgGMZp4SnZgEq9ieibQc9j" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
查看 VDA 注册步骤。

<iframe src="https://www.youtube.com/embed/iwsbajSVY5QvoUTh6m7AjG" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
配置可能影响 VDA 注册的项目时，请考虑以下事项。

控制器或 Cloud Connector 地址

无论您使用哪种方法指定控制器或 Cloud Connector，Citrix 都建议使用 FQDN 地址。IP 地址不被视为受信任的配置，因为 IP 比 DNS 记录更容易受到攻击。如果您手动填充 `ListofSIDs`，则可以在 `ListofDDCs` 中使用 IP。但是，仍然建议使用 FQDN。

负载平衡

如前所述，VDA 会自动将连接分配到 `ListofDDCs` 中的所有控制器或 Cloud Connector。故障转移和负载平衡功能内置于 Citrix 代理协议 (CBP) 中。如果在配置中指定了多个控制器或 Cloud

Connector，则注册会在需要时自动在它们之间进行故障转移。通过自动更新，所有 VDA 都会自动进行自动故障转移。

出于安全原因，您不能使用网络负载均衡器，例如 Citrix ADC。VDA 注册使用 Kerberos 相互身份验证，其中客户端 (VDA) 必须向服务 (控制器) 证明其身份。但是，控制器或 Cloud Connector 必须向 VDA 证明其身份。这意味着 VDA 和控制器或 Cloud Connector 同时充当服务器和客户端。如本文开头所述，存在两个通信通道：VDA 到控制器/Cloud Connector，以及控制器/Cloud Connector 到 VDA。

此过程中的一个组件称为服务主体名称 (SPN)，它作为属性存储在 Active Directory 计算机对象中。当 VDA 连接到 Controller 或 Cloud Connector 时，它必须指定要与谁通信。此地址是 SPN。如果您使用负载均衡 IP，相互 Kerberos 身份验证会正确识别该 IP 不属于预期的 Controller 或 Cloud Connector。

有关详细信息，请参阅：

- Kerberos 简介
- 使用 Kerberos 的相互身份验证

自动更新取代 CNAME

自动更新功能取代了 XenApp 和 XenDesktop 7.x 之前版本中的 CNAME (DNS 别名) 功能。从 XenApp 和 XenDesktop 7 开始，CNAME 功能已禁用。请使用自动更新而不是 CNAME。（如果您必须使用 CNAME，请参阅 CTX137960。为了使 DNS 别名一致地工作，请勿同时使用自动更新和 CNAME。）

控制器/云连接器组

在某些情况下，您可能希望以组的形式处理 Controller 或 Cloud Connector，其中一个组是首选组，另一个组在所有 Controller/Cloud Connector 都失败时用于故障转移。请记住，Controller 或 Cloud Connector 是从列表中随机选择的，因此分组有助于强制优先使用。

这些组旨在用于单个站点内（而非多个站点）。

使用括号指定 Controller/Cloud Connector 组。例如，对于四个 Controller（两个主用和两个备用），分组可能是：

```
(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)
```

在此示例中，第一个组中的 Controller（001 和 002）将首先处理。如果两者都失败，第二个组中的 Controller（003 和 004）将处理。

对于 XenDesktop 7.0 或更高版本，您需要执行一个额外的步骤才能使用 **注册组** 功能。您需要从 Studio **禁止“启用 Controller 自动更新”**策略。

ListOfSIDs

VDA 可以联系以进行注册的 Controller 列表是 `ListofDDCs`。VDA 还必须知道要信任哪些 Controller，因为 VDA 不会自动信任 `ListofDDCs` 中的 Controller。`ListofSIDs`（安全 ID）标识受信任的 Controller。VDA 仅尝试向受信任的 Controller 注册。

在大多数环境中，`ListofSIDs` 是从 `ListofDDCs` 自动生成的。您可以使用 CDF 跟踪来读取 `ListofSIDs`。

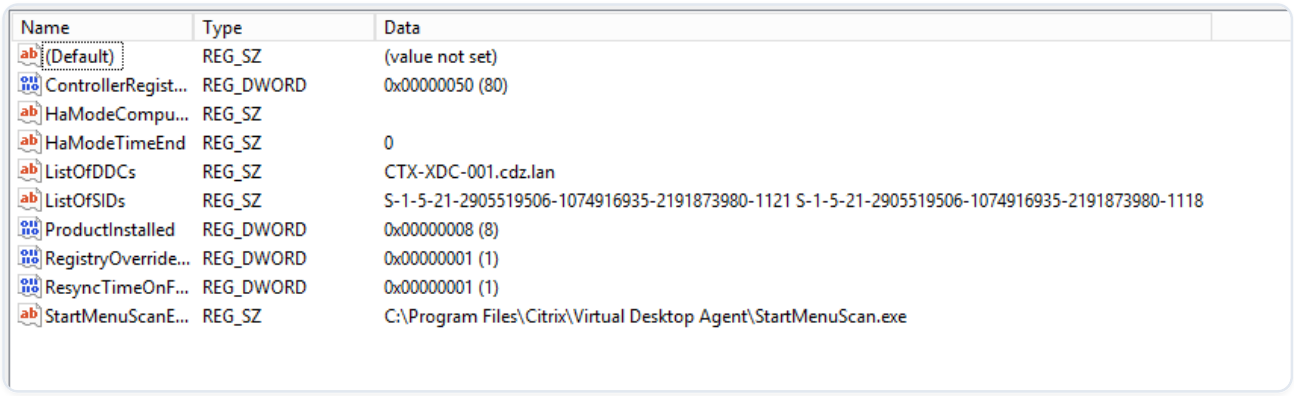
通常，无需手动修改 `ListofSIDs`。有几个例外。前两个例外不再有效，因为有更新的技术可用。

- **控制器角色分离：** 在 XenApp 和 XenDesktop 7.7 引入区域之前，当仅使用一部分控制器进行注册时，`ListofSIDs` 是手动配置的。例如，如果您使用 XDC-001 和 XDC-002 作为 XML 代理，使用 XDC-003 和 XDC-004 进行 VDA 注册，则您需要在 `ListofSIDs` 中指定所有控制器，并在 `ListofDDCs` 中指定 XDC-003 和 XDC-004。这不是典型或推荐的配置。请勿在新环境中使用此配置。请改用区域。
- **减少 Active Directory 负载：** 在 XenApp 和 XenDesktop 7.6 引入自动更新功能之前，`ListofSIDs` 用于减少域控制器上的负载。通过预填充 `ListofSIDs`，可以跳过从 DNS 名称到 SID 的解析。但是，自动更新功能消除了此工作的需要，因为此持久缓存包含 SID。Citrix 建议保持启用自动更新功能。
- **安全性：** 在某些高度安全的环境中，会手动配置受信任控制器的 SID，以避免受损 DNS 服务器可能带来的安全威胁。但是，如果这样做，您还必须禁用自动更新功能。否则，将使用持久缓存中的配置。

因此，除非有特殊原因，否则请勿修改 `ListofSIDs`。

如果必须修改 `ListofSIDs`，请在 `HKLM\Software\Citrix\VirtualDesktopAgent` 下创建名为 `ListOfSIDs (REG_SZ)` 的注册表项。该值是受信任 SID 的列表，如果有多个，请用空格分隔。

在以下示例中，一个控制器用于 VDA 注册 (`ListofDDCs`)，但两个控制器用于代理 (List OfSIDs)。



Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

VDA 注册期间的控制器搜索

当 VDA 尝试注册时，Broker Agent 首先在本地域中执行 DNS 查找，以确保可以访问指定的控制器。

如果初始查找未找到控制器，Broker Agent 可以启动 AD 中的回退自上而下查询。该查询会搜索所有域，并频繁重复。如果控制器地址无效（例如，管理员在安装 VDA 时输入了不正确的 FQDN），则该查询的活动可能会导致域控制器上出现分布式拒绝服务 (DDoS) 情况。

以下注册表项控制 Broker Agent 在初始搜索期间无法找到控制器时是否使用回退自上而下查询。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- 名称: `DisableDdcWildcardNameLookup`
- 类型: `DWORD`
- 值：`0`（默认）或任何非零值

当设置为 `0` 时，将启用回退搜索。如果控制器的初始搜索失败，则会启动回退自上而下搜索。这是默认行为。但是，如果设置为任何非零值，则会禁用回退搜索。如果控制器的初始搜索失败，Broker Agent 将停止查找。

使用只读域控制器进行 VDA 注册期间的 LDAP 绑定序列

当 VDA 向只读域控制器 (RODC) 注册时，Broker Agent 必须选择要忽略的轻型目录访问协议 (LDAP) 绑定。为了进行此选择，Broker Agent 需要一个合适的注册表项。

如果未提供注册表项，或注册表项字段为空，则 VDA 与 RODC 的注册将花费更长时间，因为它需要通过原始 LDAP 绑定序列。

为了修改 LDAP 绑定序列，已将注册表项 `ListofIgnoredBindings` 添加到 `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`。使用

`ListofIgnoredBindings` 可以根据需要修改 LDAP 绑定序列，从而加快 VDA 与 RODC 的注册速度。

- 名称: `ListofIgnoredBindings`
- 类型: `REG_SZ`
- 值: `DefaultPath`, `DomainPath`, `PDCPath`

该值是绑定路径选项的列表，每个选项之间用逗号分隔。注册表项会忽略它不识别为有效的值。

解决 VDA 注册问题

如前所述，VDA 必须向 Delivery Controller 或 Cloud Connector 注册，才能在启动代理会话时被考虑。未注册的 VDA 可能会导致原本可用的资源利用不足。VDA 未注册的原因有很多，其中许多问题管理员都可以进行故障排除。Studio 在目录创建向导中以及创建交付组后提供故障排除信息。

- **在计算机目录创建期间识别问题：** 在目录创建向导中，添加现有计算机后，计算机帐户名称列表会指示每台计算机是否适合添加到目录。将鼠标悬停在每台计算机旁边的图标上，可显示有关该计算机的信息性消息。

  如果消息识别出有问题的计算机，您可以删除该计算机（使用**删除**按钮），或添加该计算机。例如，如果消息指示未获取有关计算机的信息（可能是因为它从未注册），您仍然可以选择添加该计算机。

  目录的功能级别控制目录中计算机可用的产品功能。使用新产品版本中引入的功能可能需要新的 VDA。设置功能级别可使该版本中引入的所有功能（以及更高版本中引入的功能，如果功能级别未更改）可用于目录中的计算机。但是，该目录中 VDA 版本较早的计算机将无法注册。
- **创建交付组后识别问题：** 创建交付组后，Studio 会显示与该组关联的计算机的详细信息。

  交付组的详细信息窗格会指示必须注册但未注册的计算机数量。换句话说，可能有一台或多台计算机已开机且未处于维护模式，但当前未向 Controller 注册。查看“未注册但必须注册”的计算机时，请查看详细信息窗格中的**故障排除**选项卡，以了解可能的原因和建议的纠正措施。

有关 VDA 注册故障排除的更多信息

- 有关功能级别的更多信息，请参阅VDA 版本和功能级别。
- 有关 VDA 注册故障排除的更多信息，请参阅 CTX136668。
- 您还可以使用 Citrix Scout 运行状况检查来排查 VDA 注册和会话启动问题。有关详细信息，请参阅关于运行状况检查。

虚拟 IP 和虚拟环回

重要提示：

- Windows 10 企业多会话版不支持远程桌面 IP 虚拟化（虚拟 IP），我们也不支持在 Windows 10 企业多会话版上使用远程桌面 IP 虚拟化或虚拟环回。
- 云托管计算机不支持远程桌面 IP 虚拟化（虚拟 IP）。 有关详细信息，请参阅 Microsoft 文档。

Windows Server 2016、Windows Server 2019 和 Windows Server 2022 计算机支持远程桌面 IP 虚拟化和虚拟环回功能。这些功能不适用于 Windows 桌面操作系统计算机。

Microsoft 远程桌面 IP 虚拟化地址功能为每个会话的已发布应用程序提供唯一的动态分配 IP 地址。借助 Citrix 虚拟环回功能，您可以配置依赖于与 localhost（默认为 127.0.0.1）通信的应用程序，以使用 localhost 范围 (127.*) 中的唯一虚拟环回地址。

某些应用程序（例如 CRM 和计算机电话集成 (CTI)）使用 IP 地址进行寻址、许可、标识或需要唯一 IP 地址或环回地址的其他目的。其他应用程序可能绑定到静态端口，因此在多用户环境中启动应用程序的其他实例的尝试会失败，因为该端口正在使用中。为了使此类应用程序在 Citrix Virtual Apps™ 环境中正常运行，每个设备都需要一个唯一的 IP 地址。

远程桌面 IP 虚拟化和虚拟环回是相互独立的功能。您可以单独使用其中一个，也可以同时使用两者。

管理员操作概要：

- 要使用 Microsoft 远程桌面 IP 虚拟化，请在 Windows 服务器上启用并配置它。（不需要 Citrix® 策略设置。）
- 要使用 Citrix 虚拟环回，请在 Citrix 策略中配置两个设置。

远程桌面 IP 虚拟化（虚拟 IP）

在 Windows 服务器上启用并配置远程桌面 IP 虚拟化后，在会话中运行的每个已配置应用程序都将显示为具有唯一地址。用户访问 Citrix Virtual Apps 服务器上的这些应用程序的方式与访问任何其他已发布应用程序的方式相同。在以下任一情况下，进程都需要远程桌面 IP 虚拟化：

- 进程使用硬编码的 TCP 端口号
- 进程使用 Windows 套接字并且需要唯一的 IP 地址或指定的 TCP 端口号

要确定应用程序是否需要使用远程桌面 IP 虚拟化地址：

1. 从 Microsoft 获取 **TCPView** 工具。此工具列出了所有绑定特定 IP 地址和端口的应用程序。有关 TCPView 的更多信息，请参阅 Microsoft 文档。
2. 禁用**解析 IP 地址**功能，以便您看到的是地址而不是主机名。
3. 启动应用程序并使用 **TCPView** 查看应用程序打开了哪些 IP 地址和端口，以及哪些进程名称正在打开这些端口。
4. 配置打开服务器 IP 地址 0.0.0.0 或 127.0.0.1 的任何进程。
5. 为确保应用程序不会在不同端口上打开相同的 IP 地址，请启动应用程序的另一个实例。

Microsoft 远程桌面 (RD) IP 虚拟化工作原理

- 必须在 Microsoft 服务器上启用虚拟 IP 寻址。

  例如，在 Windows Server 2016 环境中，从服务器管理器中，展开**远程桌面服务 > RD 会话主机连接**以启用 RD IP 虚拟化功能，并配置设置以使用动态主机配置协议 (DHCP) 服务器按会话或按程序动态分配 IP 地址。有关配置远程桌面 IP 虚拟化的更多信息，请参阅 Microsoft 文档。
- 启用此功能后，在会话启动时，服务器会从 DHCP 服务器请求动态分配的 IP 地址。
- “**RD IP 虚拟化**”功能为远程桌面连接按会话或按程序分配 IP 地址。如果您为多个程序分配 IP 地址，它们将共享一个按会话的 IP 地址。
- 为会话分配地址后，每当进行以下调用时，会话都会使用虚拟地址而不是系统的主要 IP 地址：`bind`、`closesocket`、`connect`、`WSAConnect`、`WSAAccept`、`getpeername`、`getsockname`、`sendto`、`WSASendTo`、`WSASocketW`、`gethostbyaddr`、`getnameinfo`、`getaddrinfo`。

在远程桌面会话托管配置中使用 Microsoft IP 虚拟化功能时，应用程序通过在应用程序和 Winsock 函数调用之间插入“筛选器”组件来绑定到特定的 IP 地址。然后，应用程序只会看到要使用的正确 IP 地址。应用程序尝试侦听 TCP 或 UDP 通信的任何尝试都会自动绑定到其分配的虚拟 IP 地址（或环回地址）。应用程序打开的任何源连接都源自绑定到该应用程序的 IP 地址。

在返回地址的函数中（例如 `GetAddrInfo()`，由 Windows 策略控制），如果请求本地主机 IP 地址，远程桌面 IP 虚拟化会查看返回的 IP 地址并将其更改为会话的远程桌面 IP 虚拟化地址。尝试通过此类名称函数获取本地服务器 IP 地址的应用程序只会看到分配给该会话的唯一远程桌面 IP 虚拟化地址。此 IP 地址通常用于后续的套接字调用，例如绑定或连接。有关 Windows 策略的更多信息，请参阅 Windows Server 中的 RDS IP 虚拟化。

通常，应用程序会请求绑定到端口以侦听地址 0.0.0.0。当应用程序执行此操作并使用静态端口时，您无法启动该应用程序的多个实例。远程桌面 IP 虚拟化地址功能也会在这些调用类型中查找

0.0.0.0。它会将调用更改为侦听特定的远程桌面 IP 虚拟化地址，这使得多个应用程序可以在同一台计算机上的同一端口上侦听，因为它们都在不同的地址上侦听。仅当调用处于 ICA 会话中且启用了远程桌面 IP 虚拟化地址功能时，才会更改调用。例如，如果应用程序的两个实例在不同的会话中运行，都尝试绑定到所有接口 (0.0.0.0) 和特定端口（例如 9000），它们将绑定到 VIPAddress1:9000 和 VIPAddress2:9000，并且不会发生冲突。

虚拟环回

启用“**Citrix 远程桌面 IP 虚拟化环回策略**”设置允许每个会话拥有自己的环回地址进行通信。当应用程序在 Winsock 调用中使用 localhost 地址（默认 = 127.0.0.1）时，虚拟环回功能会简单地将 127.0.0.1 替换为 127.X.X.X，其中 X.X.X 表示会话 ID + 1。例如，会话 ID 为 7 时，地址为 127.0.0.8。在会话 ID 超过第四个八位字节（超过 255）的极少数情况下，地址会滚动到下一个八位字节 (127.0.1.0)，最大值为 127.255.255.255。

在以下任一情况下，进程都需要虚拟回送：

- 进程使用 Windows 套接字回送 (localhost) 地址 (127.0.0.1)
- 进程使用硬编码的 TCP 端口号

对于使用回送地址进行进程间通信的应用程序，请使用虚拟回送策略设置。无需额外配置。虚拟回送不依赖于虚拟 IP，因此您无需配置 Microsoft 服务器。

- 虚拟 IP 回送支持。启用后，此策略设置允许每个会话拥有自己的虚拟回送地址。此设置默认禁用。此功能仅适用于通过“虚拟 IP 虚拟回送程序列表”策略设置指定的应用程序。
- 虚拟 IP 虚拟回送程序列表。此策略设置指定使用虚拟 IP 回送功能的应用程序。此设置仅在启用“虚拟 IP 回送支持”策略设置时适用。
- 虚拟 IP 环回端口排除。当应用程序在此设置中指定的端口上调用环回地址时，虚拟环回不会将调用更改为会话特定的环回地址。

相关功能

您可以使用以下注册表设置来确保虚拟环回优先于虚拟 IP。此功能称为首选环回。但是，请谨慎操作：

- 仅当同时启用虚拟 IP 和虚拟环回时才使用首选环回。否则，可能会出现意外结果。
- 错误地编辑注册表可能会导致严重问题，甚至可能需要重新安装操作系统。Citrix 无法保证因不正确使用注册表编辑器而导致的问题能够得到解决。请自行承担使用注册表编辑器的风险。在编辑注册表之前，请务必备份注册表。

在应用程序所在的服务器上运行 regedit。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`
- 名称: PreferLoopback, 类型: REG_DWORD, 数据: 1
- 名称: PreferLoopbackProcesses, 类型: REG_MULTI_SZ, 数据: \<进程列表\>

区域

> **注意：**
>
> 从版本 2511 开始，Citrix Web Studio（基于 Web）是 Citrix Virtual Apps and Desktops™ 的唯一管理控制台。Citrix Studio（基于 MMC）已从安装程序中删除。本文仅适用于 Web Studio。有关 Citrix Studio 的信息，请参阅 Citrix Virtual Apps and Desktops 7 2212 或更早版本中的等效文章。

跨越通过 WAN 连接的广泛分散位置的部署可能会面临网络延迟和可靠性方面的挑战。有两种选项可以缓解这些挑战：

- 部署多个站点，每个站点都有自己的 SQL Server 站点数据库。

  此选项建议用于大型企业部署。多个站点是单独管理的，每个站点都需要自己的 SQL Server 站点数据库。每个站点都是一个独立的 Citrix Virtual Apps™ 部署。
- 在单个站点中配置多个区域。

  配置区域可以帮助远程区域的用户连接到资源，而无需强制其连接遍历 WAN 的大部分。使用区域可以从单个 Web Studio 控制台、Citrix Director 和站点数据库进行有效的站点管理。这节省了在远程位置部署、配备人员、许可和运营包含单独数据库的更多站点的成本。

  区域在各种规模的部署中都很有用。您可以使用区域使应用程序和桌面更靠近最终用户，从而提高性能。一个区域可以本地安装一个或多个控制器以实现冗余和弹性，但这不是必需的。

  站点中配置的控制器数量可能会影响某些操作的性能，例如向站点本身添加新控制器。为避免这种情况，我们建议您将 Citrix Virtual Apps 或 Citrix Virtual Desktops™ 站点中的区域数量限制为不超过 50 个。

  当您的区域网络延迟超过 250 毫秒 RTT 时，我们建议您部署多个站点而不是区域。

在本文中，“本地”一词指正在讨论的区域。例如，“VDA 向本地控制器注册”表示 VDA 向 VDA 所在区域中的控制器注册。

此版本中的区域与 XenApp 6.5 及更早版本中的区域相似，但并不完全相同。例如，在此区域实现中，没有数据收集器。站点中的所有控制器都与主区域中的一个站点数据库通信。此外，此版本中的故障转移和首选区域的工作方式也不同。

区域类型

一个站点始终有一个主区域。它还可以选择有一个或多个卫星区域。卫星区域可用于灾难恢复、地理上遥远的数据中心、分支机构、云或云中的可用区。

主区域：

主区域的默认名称为“Primary”。此区域包含 SQL Server 站点数据库（如果使用，还包含高可用性 SQL 服务器）、Web Studio、Director、Citrix StoreFront™、Citrix 许可证服务器和 Citrix Gateway。始终将站点数据库保留在主区域中。

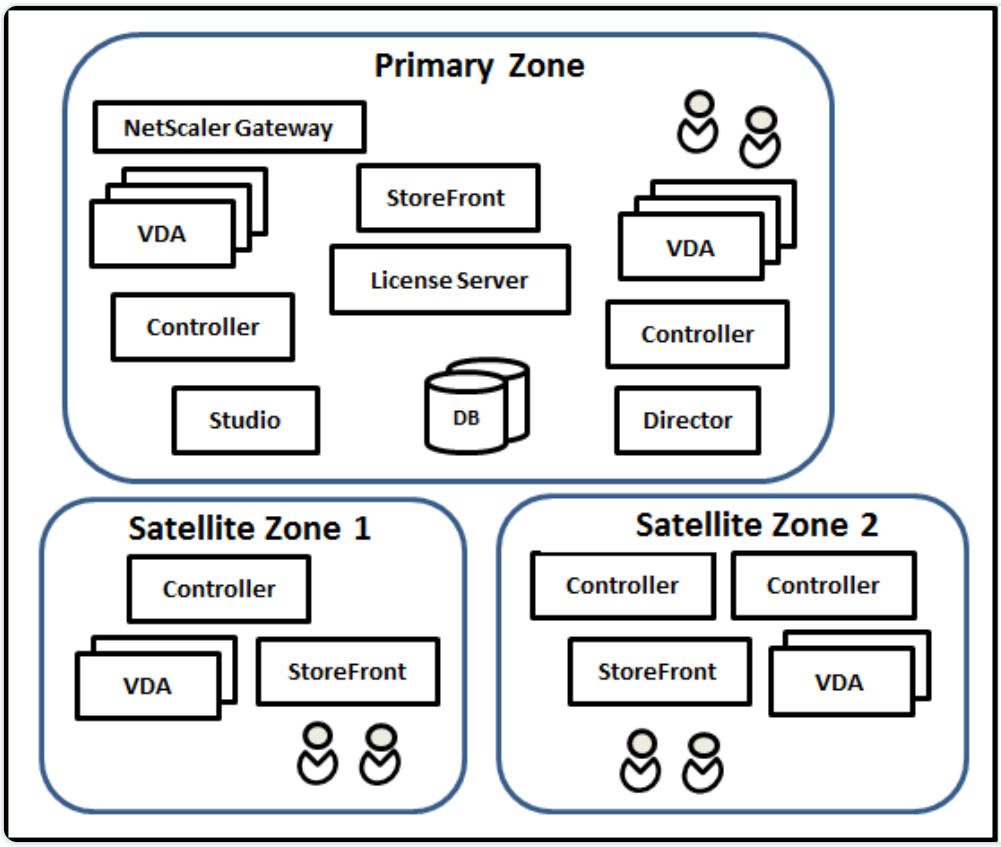
主区域应至少有两个控制器以实现冗余。主区域可以包含与数据库和基础架构紧密耦合的应用程序的 VDA。

卫星区域：

卫星区域包含一个或多个 VDA、控制器、StoreFront 服务器和 Citrix Gateway 服务器。在正常操作下，卫星区域中的控制器直接与主区域中的数据库通信。

卫星区域，特别是大型卫星区域，可能还包含一个用于为该区域预配和存储计算机的管理程序。配置卫星区域时，可以将其与管理程序或其他服务连接相关联。（请确保使用该连接的所有目录都位于同一区域中。）

站点可以根据您的独特需求和环境拥有不同配置的卫星区域。下图说明了主区域和卫星区域的示例。



在插图中：

- **主区域：** 包含两个控制器、Web Studio、Director、StoreFront、许可证服务器和站点数据库（以及高可用性 SQL Server 部署）。主区域还包含多个 VDA 和一个 Citrix Gateway。
- **卫星区域 1：带控制器的 VDA：** 卫星区域 1 包含一个控制器、VDA 和一个 StoreFront 服务器。此卫星区域中的 VDA 向本地控制器注册。本地控制器与主区域中的站点数据库和许可证服务器通信。

  如果 WAN 发生故障，本地主机缓存功能允许卫星区域中的控制器继续代理与该区域中 VDA 的连接。这种部署在工作人员使用本地 StoreFront 站点和本地控制器访问其本地资源的办公室中可能很有效。
- **卫星区域 2：带冗余控制器的 VDA：** 卫星区域 2 包含两个控制器、VDA 和一个 StoreFront 服务器。这是最具弹性的区域类型，可防止 WAN 和其中一个本地控制器同时发生故障。

VDA 注册位置和控制器故障转移位置

在包含主区域和卫星区域且 VDA 最低版本为 7.7 的站点中：

- 主区域中的 VDA 向主区域中的控制器注册。主区域中的 VDA 绝不会尝试向卫星区域中的控制器注册。
- 卫星区域中的 VDA 尽可能向本地控制器注册。（这被认为是首选控制器。）如果没有可用的本地控制器（例如，因为它们无法接受更多 VDA 注册或它们已发生故障），VDA 将尝试向主区域

中的控制器注册。在这种情况下，即使卫星区域中的控制器再次可用，VDA 仍会注册在主区域中。卫星区域中的 VDA 绝不会尝试向另一个卫星区域中的控制器注册。

- 当为 VDA 发现 Controller 启用自动更新，并且在 VDA 安装期间指定 Controller 地址列表时，将从该列表中随机选择一个 Controller 进行初始注册（无论 Controller 位于哪个区域）。在该 VDA 所在的计算机重新启动后，VDA 将开始优先注册其本地区域中的 Controller。
- 如果卫星区域中的 Controller 发生故障，它将尽可能故障转移到另一个本地 Controller。如果没有可用的本地 Controller，它将故障转移到主区域中的 Controller。
- 如果您将 Controller 移入或移出某个区域，并且启用了自动更新，则两个区域中的 VDA 都会收到更新的列表，指示哪些 Controller 是本地的，哪些在主区域中，以便它们知道可以向谁注册并接受来自谁的连接。
- 如果将目录移动到另一个区域，则该目录中的 VDA 将重新注册到您移动目录的区域中的 Controller。（将目录移动到另一个区域时，请确保此区域与具有关联主机连接的区域连接良好。如果带宽有限或延迟较高，请将主机连接移动到包含关联计算机目录的同一区域。）

如果主区域中的所有 Controller 都发生故障：

- Web Studio 无法连接到站点。
- 无法连接到主区域中的 VDA。
- 站点性能会下降，直到主区域中的 Controller 可用为止。

对于包含早于 7.7 版本的 VDA 的站点：

- 卫星区域中的 VDA 接受来自其本地区域和主区域中的 Controller 的请求。（最低版本为 7.7 的 VDA 可以接受来自其他卫星区域的 Controller 请求。）
- 卫星区域中的 VDA 随机注册到主区域或本地区域中的 Controller。（最低版本为 7.7 的 VDA 优先选择本地区域。）

区域首选项

要使用区域首选项功能，您必须使用最低 StoreFront 3.7 和 Citrix Gateway 11.0-65.x。

在多区域站点中，区域首选项功能为管理员提供了更大的灵活性，可以控制使用哪个 VDA 启动应用程序或桌面。

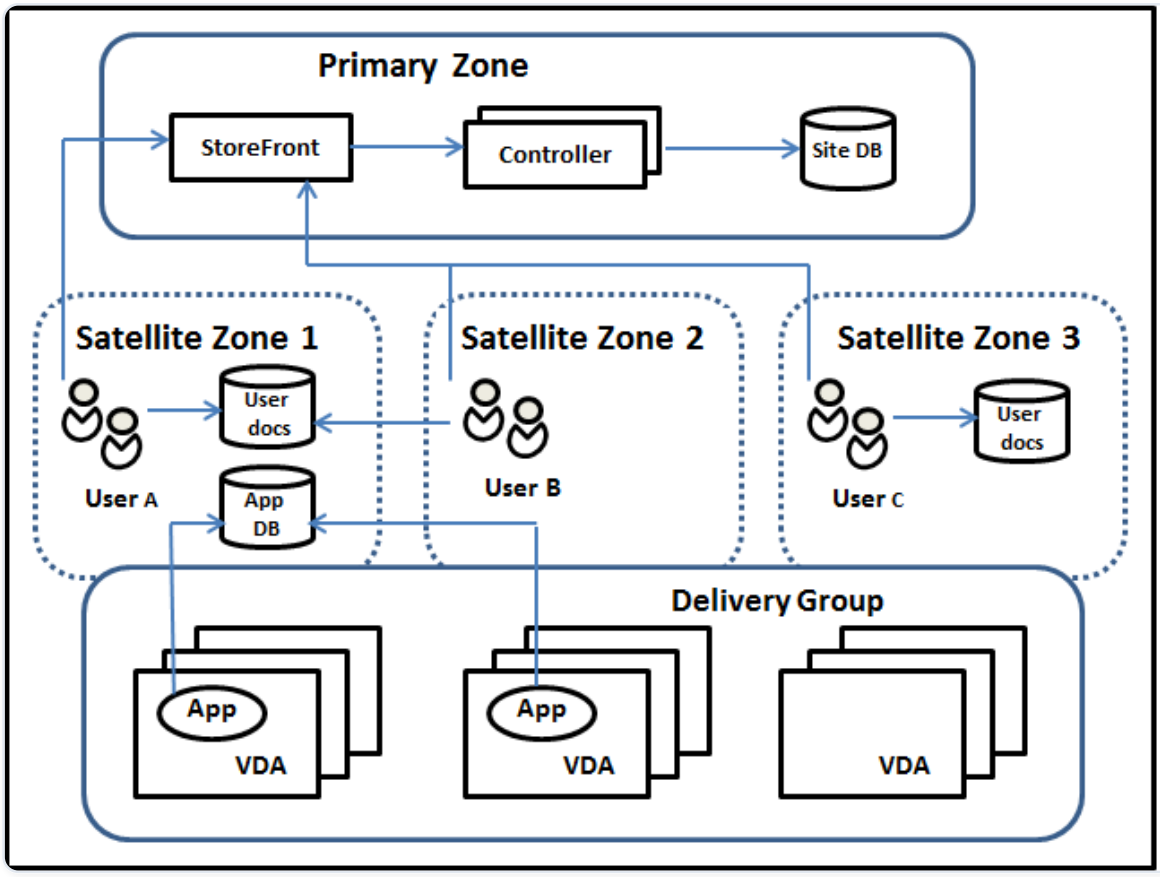
区域首选项的工作原理

区域首选项有三种形式。您可能希望在特定区域中使用 VDA，具体取决于：

- 应用程序数据存储的位置。这称为应用程序主目录。
- 用户主数据的位置，例如配置文件或主共享。这称为用户主目录。

- 用户的当前位置（Citrix Workspace™ 应用程序运行的位置）。这称为用户位置。

下图显示了一个多区域配置示例。



在此示例中，VDA 分布在三个卫星区域中，但它们都位于同一个交付组中。因此，代理可能会选择使用哪个 VDA 来处理用户启动请求。此示例表明用户可以在多个位置运行其 Citrix Workspace 应用程序端点：

- 用户 A 正在卫星区域 1 中使用运行 Citrix Workspace 应用程序的设备。
- 用户 B 正在卫星区域 2 中使用设备。
- 用户的文档可以存储在各个位置。
  - 用户 A 和 B 使用基于卫星区域 1 的共享。
  - 用户 C 使用来自卫星区域 C 的共享。
  - 其中一个已发布的应用程序使用位于卫星区域 1 中的数据库。

通过为用户或应用程序配置主区域，可以将用户或应用程序与区域关联。然后，Delivery Controller™ 中的代理会使用这些关联来帮助选择在资源可用时启动会话的区域。您可以：

- 通过将用户添加到区域来配置用户的主区域。
- 通过编辑应用程序属性来配置应用程序的主区域。

用户或应用程序一次只能有一个主区域。（当由于用户组成员身份而出现多个区域成员身份时，用户可能会出现例外情况；请参阅“其他注意事项”部分。但是，即使在这种情况下，代理也只使用一个主区域。）

尽管可以为用户和应用程序配置区域首选项，但代理仅为一次启动选择一个首选区域。选择首选区域的默认优先级顺序是应用程序主区域 \> 用户主区域 \> 用户位置。您可以限制此顺序；请参阅自定义区域首选项。当用户启动应用程序时：

- 如果该应用程序具有配置的区域关联（应用程序主区域），则首选区域是该应用程序的主区域。
- 如果应用程序没有配置区域关联，但用户有配置区域关联（用户主区域），则首选区域是该用户的主区域。
- 如果应用程序和用户都没有配置区域关联，则首选区域是用户运行 Citrix Workspace 应用程序实例的区域（用户位置）。如果未定义该区域，则使用随机 VDA 和区域选择。负载平衡应用于首选区域中的所有 VDA。如果没有首选区域，则负载平衡应用于交付组中的所有 VDA。

调整区域首选项

当您为用户或应用程序配置（或删除）主区域时，您还可以进一步限制区域首选项的使用方式。

- **强制使用用户主区域：** 在交付组中，您可以指定会话在用户的主区域（如果已配置）中启动，如果主区域没有可用资源，则不进行故障转移到其他区域。当您必须避免在区域之间复制大型配置文件或数据文件的风险时，此限制很有用。换句话说，您宁愿拒绝会话启动，也不愿在不同区域中启动会话。
- **强制使用应用程序主区域：** 同样，当您为应用程序配置主区域时，您可以指示该应用程序只能在该区域中启动，如果应用程序的主区域中没有可用资源，则不会故障转移到其他区域。
- **无应用程序主区域，并忽略已配置的用户主区域：** 如果您未指定应用程序的主区域，您还可以指示在启动该应用程序时，不考虑任何已配置的用户区域。例如，您可能更希望用户使用用户位置区域首选项在其设备附近的 VDA 上运行应用程序，即使某些用户可能具有不同的主区域。

首选区域如何影响会话使用

当用户启动应用程序或桌面时，代理程序更倾向于使用首选区域，而不是使用现有会话。

如果启动应用程序或桌面的用户已经有一个适合所启动资源的会话（例如，可以用于应用程序的会话共享，或者已经运行所启动资源的会话），但该会话正在用户/应用程序首选区域之外的区域中的 VDA 上运行，则系统可能会创建一个新会话。这满足了在正确区域中启动（如果它有可用容量）的要求，优先于重新连接到用户会话要求中不太首选区域的会话。

为防止无法再访问的孤立会话，即使现有断开连接的会话位于非首选区域，也允许重新连接到这些会话。

满足启动需求的会话的理想顺序是：

1. 重新连接到首选区域中的现有会话。
2. 重新连接到首选区域之外的区域中现有的已断开连接的会话。
3. 在首选区域中启动新会话。
4. 重新连接到首选区域之外的区域中已连接的现有会话。
5. 在首选区域之外的区域中启动新会话。

其他区域首选项注意事项

- 如果您为用户组（例如安全组）配置了主区域，则该组的用户（通过直接或间接成员身份）将与指定区域关联。但是，用户可以是多个安全组的成员，因此可能通过其他组成员身份配置了不同的主区域。在这种情况下，确定该用户的主区域可能会不明确。

如果用户配置了并非通过组成员身份获得的主区域，则该区域将用于区域首选项。通过组成员身份获得的任何区域关联都将被忽略。

如果用户仅通过组成员身份获得了多个不同的区域关联，则代理会随机选择其中一个区域。一旦代理做出此选择，该区域将用于后续的会话启动，直到用户的组成员身份发生变化。

- 用户位置区域首选项要求 Citrix Gateway 通过其连接的端点设备检测 Citrix Workspace 应用程序。Citrix Gateway 必须配置为将 IP 地址范围与特定区域关联，并且发现的区域身份必须通过 StoreFront 传递给 Controller。

有关区域首选项的更多信息，请参阅区域首选项内部机制。

注意事项、要求和最佳实践

- 您可以将以下项目放置在区域中：Controller、计算机目录、主机连接、用户和应用程序。如果目录使用主机连接，请确保目录和连接位于同一区域中。（但是，如果存在低延迟、高带宽连接，它们可以位于不同的区域中。）
- 当您将项目放置在卫星区域中时，它会影响站点与这些项目以及与它们相关的其他对象进行交互的方式。
    - 当 Controller 放置在卫星区域中时，假定这些计算机与同一区域中的管理程序和 VDA 具有良好的（本地）连接。然后，该卫星区域中的 Controller 将优先于主区域中的 Controller 用于处理这些管理程序和 VDA 计算机。
    - 当管理程序连接放置在卫星区域中时，假定通过该管理程序连接管理的所有管理程序也驻留在该卫星区域中。然后，该卫星区域中的 Controller 将优先于主区域中的 Controller 用于与该管理程序连接进行通信。

  - 当计算机目录放置在卫星区域中时，假定该目录中的所有 VDA 计算机都位于卫星区域中。在每个 VDA 首次注册后，Controller 列表自动更新机制激活后，本地 Controller 将优先于主区域中的 Controller 用于尝试向站点注册。
  - Citrix Gateway 实例也可以与区域关联。这是作为 StoreFront 最佳 HDX™ 路由配置的一部分完成的，而不是像此处描述的其他元素那样作为站点配置的一部分完成的。当 Citrix Gateway 与某个区域关联时，在连接到该区域中的 VDA 计算机时，将优先使用该 Citrix Gateway。

- 创建生产站点，然后创建第一个目录和交付组时，所有项目都位于主区域中 – 必须先完成初始设置，然后才能创建卫星区域。（如果创建空站点，则主区域最初将只包含一个控制器。您可以在创建目录和交付组之前或之后创建卫星区域。）
- 创建包含一个或多个项目的第一个卫星区域时，站点中的所有其他项目都保留在主区域中。
- 主区域默认命名为“Primary”；您可以更改该名称。尽管 Web Studio 会指示哪个区域是主区域，但最佳做法是为主区域使用一个易于识别的名称。您可以重新分配主区域（即将另一个区域设为主区域），但它应始终包含站点数据库和任何高可用性服务器。
- 始终将站点数据库保留在主区域中。
- 创建区域后，您可以稍后将项目从一个区域移动到另一个区域。这种灵活性使您能够分离最适合在近距离运行的项目。例如，将目录移动到与创建目录中计算机的连接（主机）不同的区域可能会影响性能。在区域之间移动项目之前，请考虑潜在的意外影响。将目录及其使用的主机连接保留在同一区域中，或保留在连接良好（例如，通过低延迟和高带宽网络）的区域中。
- 为获得最佳性能，请仅在主区域中安装 Web Studio 和 Director。您可以从卫星区域访问 Web Studio 和 Director（例如，包含控制器的卫星区域，以便在主区域无法访问时用作故障转移），因为它们是 Web 应用程序。
- 理想情况下，卫星区域中的 Citrix Gateway 用于从其他区域或外部位置进入该区域的用户连接，尽管您也可以将其用于区域内的连接。
- 请记住：要使用区域首选项功能，您必须至少使用 StoreFront 3.7 和 Citrix Gateway 11.0-65.x。

连接质量限制

卫星区域中的控制器直接与站点数据库执行 SQL 交互。这会对卫星区域与包含站点数据库的主区域之间的链接质量施加一些限制。具体限制与部署在卫星区域中的 VDA 数量以及这些 VDA 上的用户会话数量有关。因此，只有少量 VDA 和会话的卫星区域可以比具有大量 VDA 和会话的卫星区域使用质量较差的数据库连接。

有关详细信息，请参阅延迟和 SQL 阻塞查询改进。

延迟对代理性能的影响

尽管区域允许用户使用更高延迟的链接（前提是有本地代理），但额外的延迟不可避免地会影响最终用户体验。对于用户所做的大多数工作，他们会遇到由卫星区域中的控制器与站点数据库之间的往返通信导致的缓慢。

对于启动应用程序，在会话代理过程识别要发送会话启动请求的合适 VDA 时，会发生额外的延迟。

创建和管理区域

完全管理员可以执行所有区域创建和管理任务。但是，您也可以创建自定义角色，允许您创建、编辑或删除区域。在区域之间移动项目不需要区域相关权限（区域读取权限除外）；但是，您必须具有要移动项目的编辑权限。例如，要将目录从一个区域移动到另一个区域，您必须具有该目录的编辑权限。有关详细信息，请参阅委派管理。

如果您使用 Citrix Provisioning™： Citrix Provisioning 控制台不识别区域，因此我们建议使用 Web Studio 为卫星区域创建目录。在 Web Studio 中创建目录，指定正确的卫星区域。然后使用 Citrix Provisioning 控制台在该目录中预配计算机。（如果您使用 Citrix Provisioning 向导创建目录，则该目录将放置在主区域中。您必须稍后使用 Web Studio 将其移动到卫星区域。）

创建区域

1. 登录 Web Studio。
2. 在左侧窗格中选择**区域**。
3. 在操作栏中选择**创建区域**。
4. 输入区域名称和描述（可选）。名称在站点中必须是唯一的。
5. 选择要放置在新区域中的项目。您可以筛选或搜索可供选择的项目列表。您也可以创建空区域；只需不选择任何项目即可。
6. 单击 **保存**。

作为此方法的替代方法，您可以在 Web Studio 中选择一个或多个项目，然后在操作栏中选择**创建区域**。

更改区域名称或描述

1. 登录 Web Studio。
2. 在左侧窗格中选择**区域**。
3. 在中间窗格中选择一个区域，然后在操作栏中选择“**编辑区域**”。
4. 更改区域名称、描述或两者。如果更改主区域的名称，请确保该区域仍易于识别为主区域。
5. 单击**保存**或**应用**。

将项目从一个区域移动到另一个区域

1. 登录到 Web Studio。
2. 在左侧窗格中选择“**区域**”。
3. 在中间窗格中选择一个区域，然后选择一个或多个项目。
4. 将项目拖动到目标区域，或者在操作栏中选择“**移动项目**”，然后指定要将它们移动到哪个区域。

确认消息会列出您选择的项目，并询问您是否确定要移动所有这些项目。

请记住：当目录使用到管理程序或其他服务的主机连接时，请将目录和连接都放在同一个区域中。否则，性能可能会受到影响。如果您移动其中一个，也要移动另一个。

删除区域

区域必须为空才能删除。您不能删除主区域。

1. 登录到 Web Studio。
2. 在左侧窗格中选择“**区域**”。
3. 在中间窗格中选择一个区域。
4. 从操作栏中选择“**删除区域**”。如果区域不为空（包含项目），系统会要求您选择要将这些项目移动到的区域。
5. 确认删除。

为用户添加主区域

为用户配置主区域也称为 *将用户添加到区域*。

1. 登录到 Web Studio。
2. 在左侧窗格中选择“**区域**”，然后在中间窗格中选择一个区域。
3. 在操作栏中选择 **将用户添加到区域**。
4. 在 **将用户添加到区域** 对话框中，单击 **添加**，然后选择要添加到区域的用户和用户组。如果您指定的用户已拥有主区域，则会显示一条消息，提供两个选项：**是** = 仅添加您指定的没有主区域的用户；**否** = 返回用户选择对话框。
5. 单击**确定**。

对于配置了主区域的用户，您可以要求会话仅从其主区域启动：

1. 创建或编辑交付组。
2. 在**用户**页面上，选择**要求会话在用户的主区域中启动（如果已配置）**复选框。

该交付组中用户启动的所有会话必须从该用户主区域中的计算机启动。如果交付组中的用户没有配置主区域，则此设置无效。

删除用户的主区域

此过程也称为从区域中删除用户。

1. 登录 Web Studio。
2. 在左侧窗格中选择 **区域**，然后在中间窗格中选择一个区域。
3. 在操作栏中选择 **从区域中删除用户**。
4. 在 **将用户添加到区域** 对话框中，单击 **删除**，然后选择要从区域中删除的用户和组。此操作仅从区域中删除用户；这些用户仍保留在其所属的交付组和应用程序组中。
5. 在出现提示时确认删除。

管理应用程序的主区域

为应用程序配置主区域也称为将应用程序添加到区域。默认情况下，在多区域环境中，应用程序没有主区域。

应用程序的主区域在应用程序的属性中指定。您可以在将应用程序添加到组时或之后配置应用程序属性。

- 在 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/delivery-groups-create.html)、(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/install-configure/application-groups-create.html) 或 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/manage-deployment/applications-manage.html#add-applications) 时，在向导的 **应用程序** 页面上选择 **属性**。
- 要在添加应用程序后更改其属性，请在左侧窗格中选择 **应用程序**。选择一个应用程序，然后在操作栏中选择 **编辑应用程序属性**。

在应用程序属性/设置的 **区域** 页面上：

- 如果您希望应用程序具有主区域：
  - 选择 **使用选定的区域进行决定** 单选按钮，然后选择该区域。
  - 如果您希望应用程序仅从选定区域启动（而不是从任何其他区域启动），请选中区域选择下方的复选框。
- 如果您不希望应用程序具有主区域：
  - 选择 **不配置主区域** 单选按钮。

- 如果您不希望代理在启动此应用程序时考虑任何已配置的用户区域，请选中单选按钮下方的复选框。在这种情况下，应用程序或用户主区域都不会用于确定此应用程序的启动位置。

其他涉及指定区域的操作

创建至少一个卫星区域后，您可以在添加主机连接或创建目录时指定一个区域。

通常，主区域是默认区域。使用 Machine Creation Services™ 创建目录时，将自动选择为主机连接配置的区域。

如果站点不包含卫星区域，则假定为主区域，并且不会显示区域选择框。

从缓存中移除代理用户

有些情况下，管理员无法从缓存中移除代理用户，或者有时在运行 `Get-BrokerUser` 时，用户显示了 AD 中不正确的 SID。

当用户从 AD 中删除并重新创建，但代理缓存仍保留以前的用户 SID 时，就会发生这种情况。

要解决此问题，请执行以下操作：

1. 从 Active Directory 中移除用户。
2. 对每个已移除的帐户运行 `Get-BrokerUser`。未在任何地方引用的帐户不会返回任何结果。对于已引用的用户，运行 `Get-BrokerUser` 后会获得一个值。现在，您必须找出用户被分配到哪些资源，并手动从这些资源中移除用户。

   例如：

   - 查找用户是否已分配给应用程序：`Get-BrokerApplication`
   - 查找用户是否已分配给应用程序组：`Get-BrokerApplicationGroup`
   - 查找用户是否已分配给访问策略：`Get-BrokerAccessPolicyRule`
   - 查找用户是否已分配给应用程序授权策略：`Get-BrokerAppEntitlementPolicyRule`
   - 查找用户是否已分配给桌面授权策略：`Get-BrokerEntitlementPolicyRule`
   - 查找用户是否已分配给桌面组会话保留：`Get-BrokerSessionLinger`
   - 查找用户是否正在 VDA 上运行任何会话：`Get-BrokerSession`
   - 查找用户是否已分配给合并组中的资源：`Get-BrokerMergedResource`
   - 查找用户是否已分配给资源组：`Get-BrokerMergeGroup`
   - 查找用户是否有排队的命令：`Get-BrokerMachineCommand`

- 查找用户是否已分配到专用桌面：`Get-BrokerMachineV2`
- 查找用户是否已分配到区域首选项：`Get-BrokerUserZonePreference`

3. 手动将用户从资源中移除。
4. 运行 `Get-BrokerUser` 命令以确认用户已从所有资源中移除。
5. 用户从所有资源中移除后，运行以下命令以将用户从缓存中移除。

```
Update-BrokerNameCache -Users -Purge -UnusedFor 0
```

思杰虚拟桌面助手应用程序

Citrix Virtual Desktop Assistant 应用程序是一个 GUI 工具，旨在帮助最终用户优化其在 CPU、内存、网络、HDX™ 和其他性能因素方面的会话。它提供简单便捷的体验，通常只需单击一下即可显著提高会话性能或进行故障排除。

会话目前可在以下方面进行优化：

- 系统资源：CPU 和内存优化。
- 网络：网络状态检查和个性化建议。
- 应用程序：显示无响应的应用程序并提供终止它们的选项。
- 存储：清理临时文件并识别大于 100 MB 的文件，以便直接从用户界面删除。
- 硬件诊断和故障排除：
  - 音频诊断和故障排除。
  - 摄像头设备测试。
  - 键盘诊断
  - USB 诊断

  如果 VDA 出现问题，您还可以使用 Always On Tracing (AOT) 功能。

安装和执行

对于工作站和服务器 VDA： Citrix Virtual Desktop Assistant 应用程序默认下载并以最小操作模式运行。安装后，重新启动 VDA 以在系统托盘中显示 Citrix Virtual Desktop Assistant 应用程序图标。然后，单击系统托盘中的 Citrix Virtual Desktop Assistant 应用程序图标以启动图形用户界面 (GUI)。

您可以通过 Citrix Virtual Desktop Assistant Studio 策略设置禁用该应用程序。禁用后，系统托盘中的图标将被移除，用户无法启动该应用程序。为此，请执行以下操作：

1. 在 Studio 中，转到**策略**。
2. 右键单击 Assistant 应用程序，选择**编辑设置**，然后单击**已禁用**。

日志文件

Citrix Virtual Desktop Assistant 应用程序的日志文件存储在 `USERPROFILE%\AppData\Local\Temp\citrix\AssistantApp\ctxasst.log` 中。使用日志文件进行故障排除。

您可以手动附加这些日志并将其通过电子邮件发送到 `CitrixVDAssistantFeedback@citrix.com`，以帮助我们改进 Citrix Virtual Desktop Assistant 应用程序。

探索用户界面

该应用程序会自动检测您操作系统的语言变体，并以该语言显示应用程序。

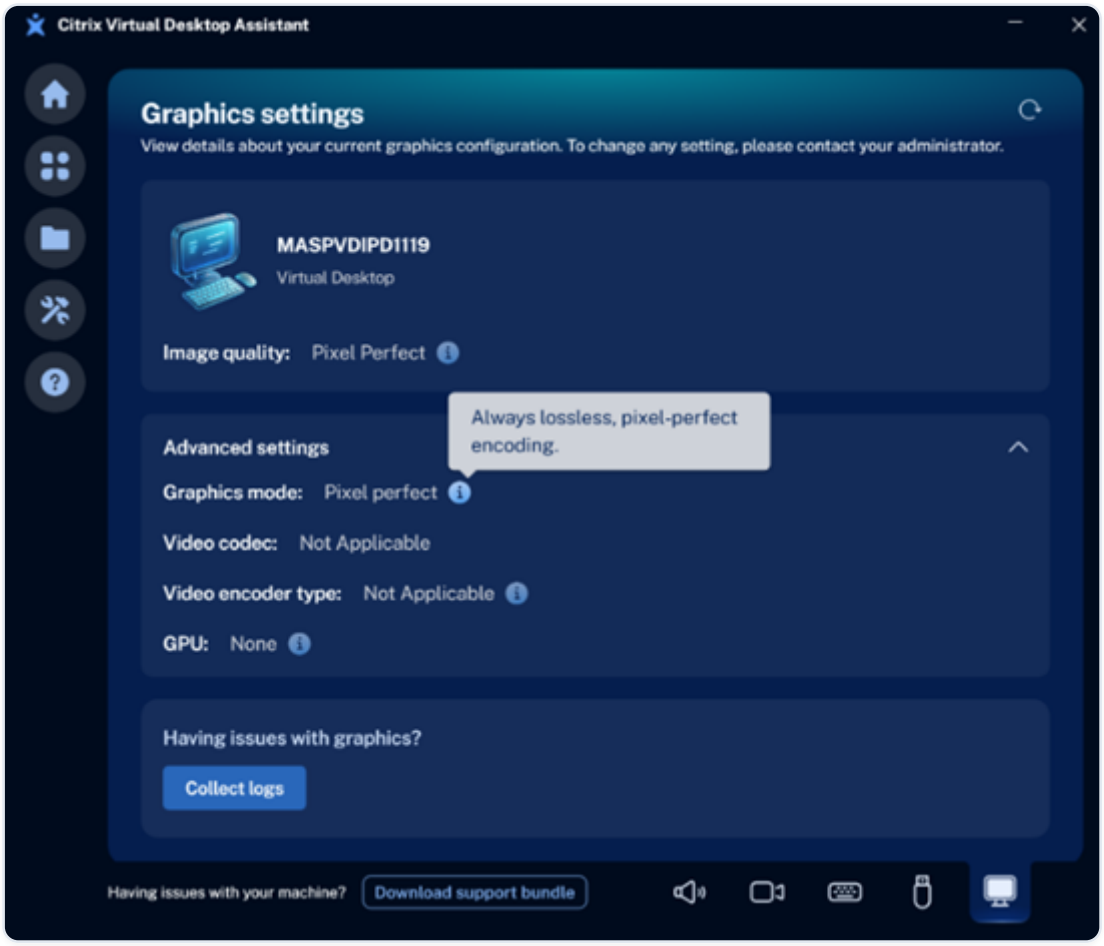
该应用程序有三个主要页面，可通过左侧窗格访问：

- 主页
- 应用程序
- 文件
- 工具
- 关于

摄像头、声音、键盘和 USB 设置位于右下角。

图形页面

Citrix Virtual Desktop Assistant 应用程序的图形页面可帮助您查看当前虚拟投递代理 (VDA) 会话的 HDX 图形配置详细信息。



- **图像质量：** 显示会话的当前 HDX 图像质量设置。
- **高级设置：** 单击可展开并查看其他图形详细信息，包括：
  - **图形模式：** 活动的 HDX 图形渲染模式。
  - **视频编解码器：** 显示视频编解码器是已禁用、对全屏处于活动状态，还是仅对正在主动更改的屏幕区域处于活动状态。
  - **视频编码器类型：** 当前使用的硬件或软件编码器。
  - **GPU：** 会话使用的 GPU 模型。

将鼠标悬停在每个设置旁边的信息图标上，以了解有关该值的更多信息。

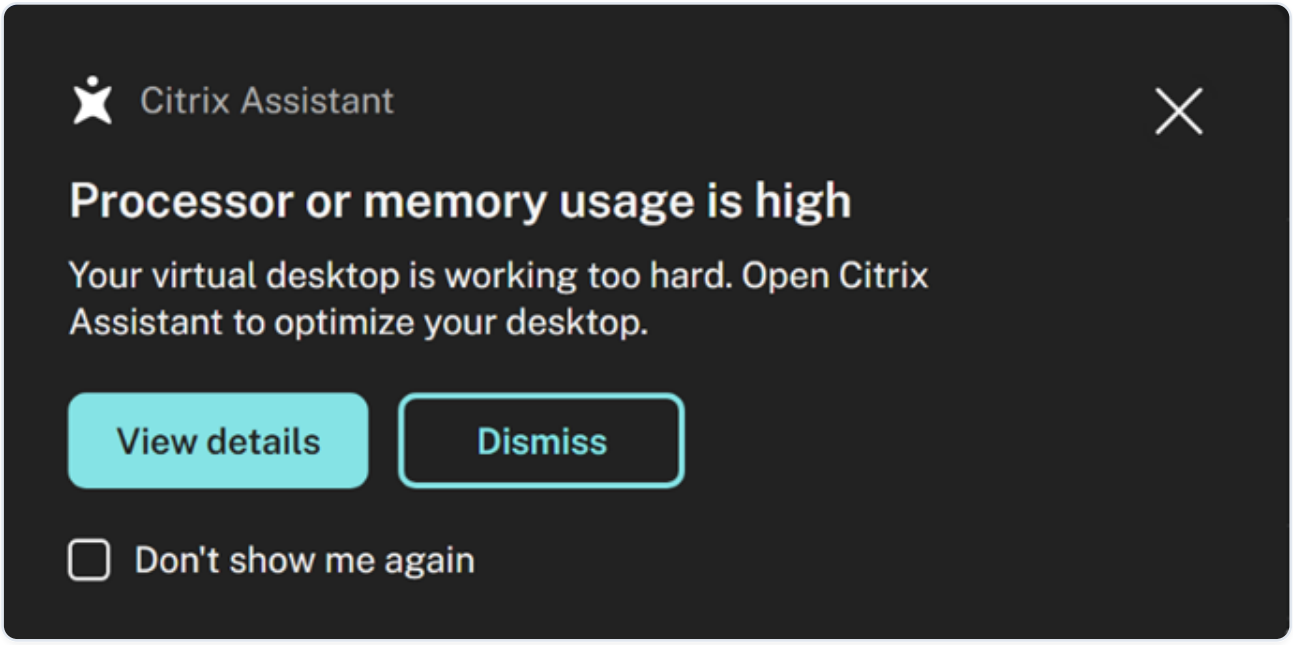
要解决 VDA 会话中的图形问题，请单击**收集日志**并将导出的日志文件共享给您的 IT 管理员。

要刷新图形数据，请单击右上角的**刷新**图标。

> **注意：**
>
> “图形”页面仅在 Citrix Virtual Desktop 会话中可用。它不会显示在物理计算机上。

主动通知

Citrix Virtual Desktop Assistant 应用程序现在会在您的会话持续高负载或配置文件存储空间不足时主动通知您，以便您可以在性能受到影响之前采取措施。



在以下情况下，屏幕右下角会显示通知弹出窗口：

- **CPU 或内存使用率高：** CPU 或内存使用率已超过 70% 达 30 秒或更长时间。
- **高配置文件存储使用率：**您的容器配置文件存储已达到或超过 70% 的容量。

通知弹出窗口提供以下选项：

- **查看详细信息：**打开 Citrix Virtual Desktop Assistant 应用程序并导航到相关页面。
- **关闭：**关闭通知。通知可能会在冷却期后再次出现。
- **不再显示：**选中此复选框可永久禁用主动通知。此设置在会话之间保持不变。

> **注意：**
>
> 存储通知仅适用于具有容器类型用户配置文件（CitrixContainer 或 FSLogix）的用户。
>
> 通知每小时显示不超过一次，以避免在持续工作负载期间重复中断。

> **在选择“不再显示”后重新启用通知：**

右键单击系统托盘中的 Citrix Virtual Desktop Assistant 图标，然后单击“启用通知”。

> **注意：**
>
> 系统托盘中的“启用通知”选项仅在管理员策略允许通知且用户之前已选择“不再显示”时可用。

DDC 对主动通知的策略控制

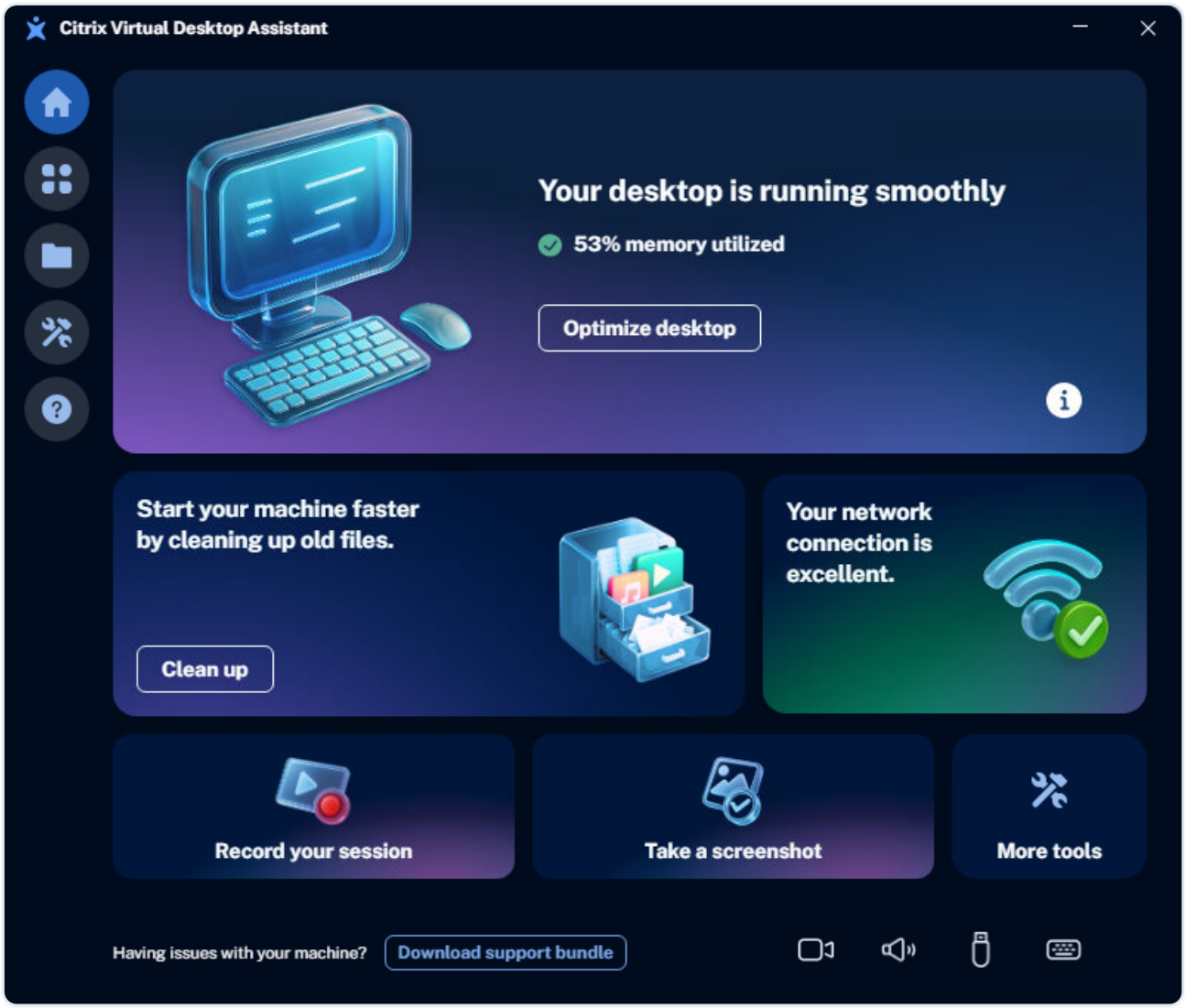
您可以通过 **AssistantApp** 类别下的 **EnableAssistantAppNotificationDialog** Studio 策略设置禁用主动通知。

1. 在 Studio 中，转到“策略”。
2. 在 AssistantApp 类别下搜索或找到 EnableAssistantAppNotificationDialog 设置。
3. 右键单击该设置，选择“**编辑设置**”，然后单击“**已禁用**”。

> **注意：**
>
> 这是一项计算机级策略。默认值为“已启用”。

主页

主页提供以下功能：



- *优化桌面*：优化功能通过在高 CPU 使用率期间调整资源密集型应用程序的 CPU 优先级来增强整体系统性能。它还会从非活动应用程序中回收内存，以确保高效利用系统资源。单击**优化桌面**后，您可能会注意到系统性能有所提高，并且通过内存回收优化的应用程序也会得到改善。
- *网络状态*：此磁贴显示 VDA 网络连接状态。网络连接结果根据带宽和延迟数据显示。连接状态分为优秀、一般或差。如果状态为一般或差，单击**我能做什么？**将提供改进建议。

> **注意：**
>
> 当连接状况不佳时，清理文件的选项不可用。

- *清理*：此选项提供有关您的用户配置文件的信息，并帮助清理临时文件或大文件（大于 100 MB）。此操作可以显著缩短计算机的登录时间。临时文件包括崩溃转储报告、应用程序缓存和导致配置文件臃肿的隐藏文件。您还可以访问左侧窗格中的“文件”页面来清理文件。有关详细信息，请参阅文件页面。

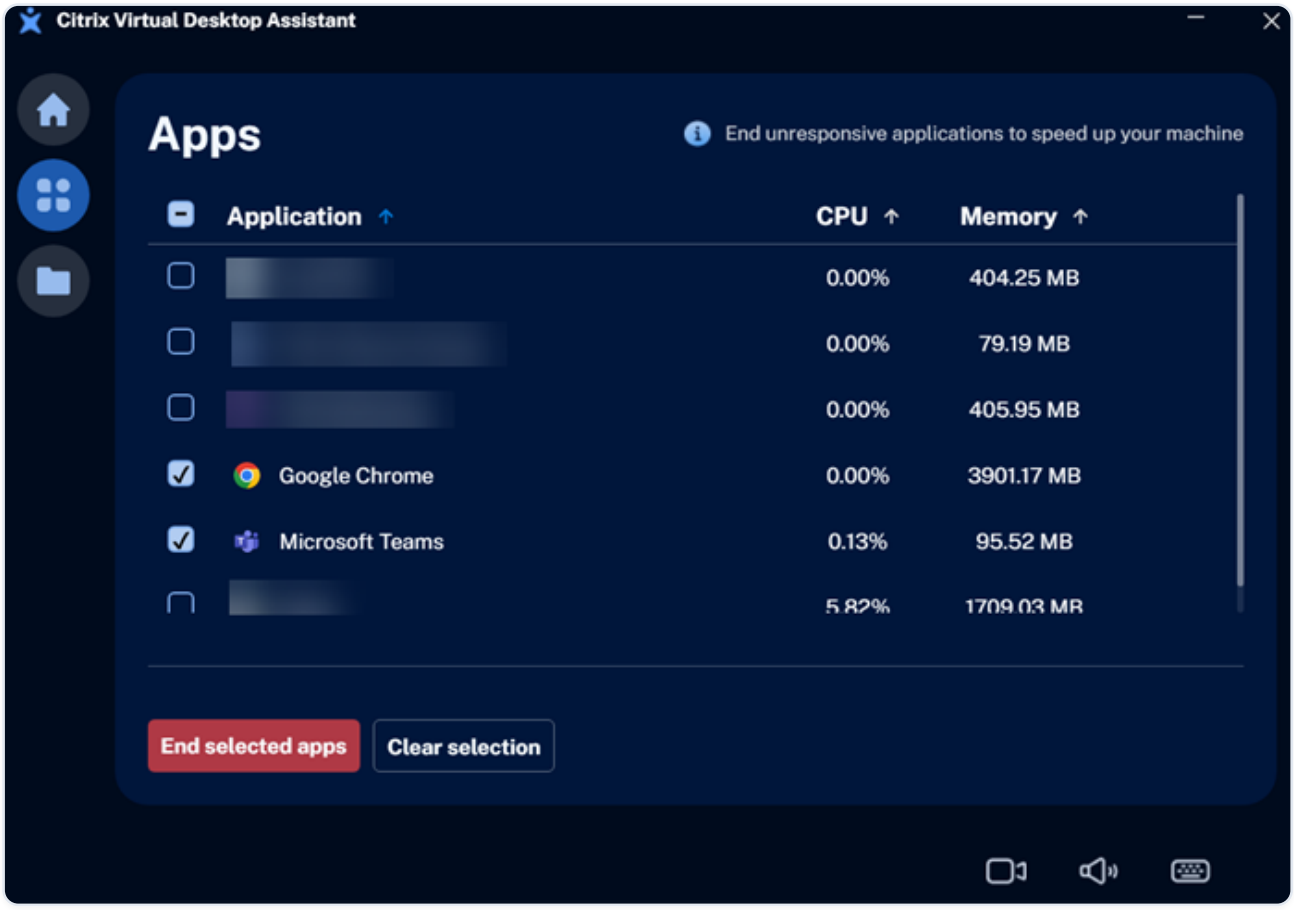
- *录制会话*：此选项可帮助您将活动虚拟桌面会话录制为 MP4 视频剪辑，以便进行故障排除、协作和会话审查。有关信息，请参阅工具页面。
- *截取屏幕截图*：此选项可帮助您捕获整个会话，包括 Windows 截图工具可能遗漏或变黑的区域。有关信息，请参阅工具页面。
- *更多工具*：此选项将带您进入**工具**页面，您可以在其中获得各种工具来增强您的虚拟桌面体验。有关信息，请参阅工具页面。

应用程序页面

应用程序页面显示 VDA 会话中所有无响应的应用程序以及终止它们的选项。您可以从此界面终止单个或多个应用程序。如果应用程序在优化列表中，您还会看到应用程序名称旁边的**已优化**标签。



- 终止单个应用程序：您可以将鼠标悬停在应用程序行上以显示**结束**按钮，或者选中复选框并单击**结束选定的应用程序**。出现提示时确认操作。
- 终止多个应用程序：一次选择多个应用程序，然后单击**结束选定的应用程序**。出现提示时确认操作。

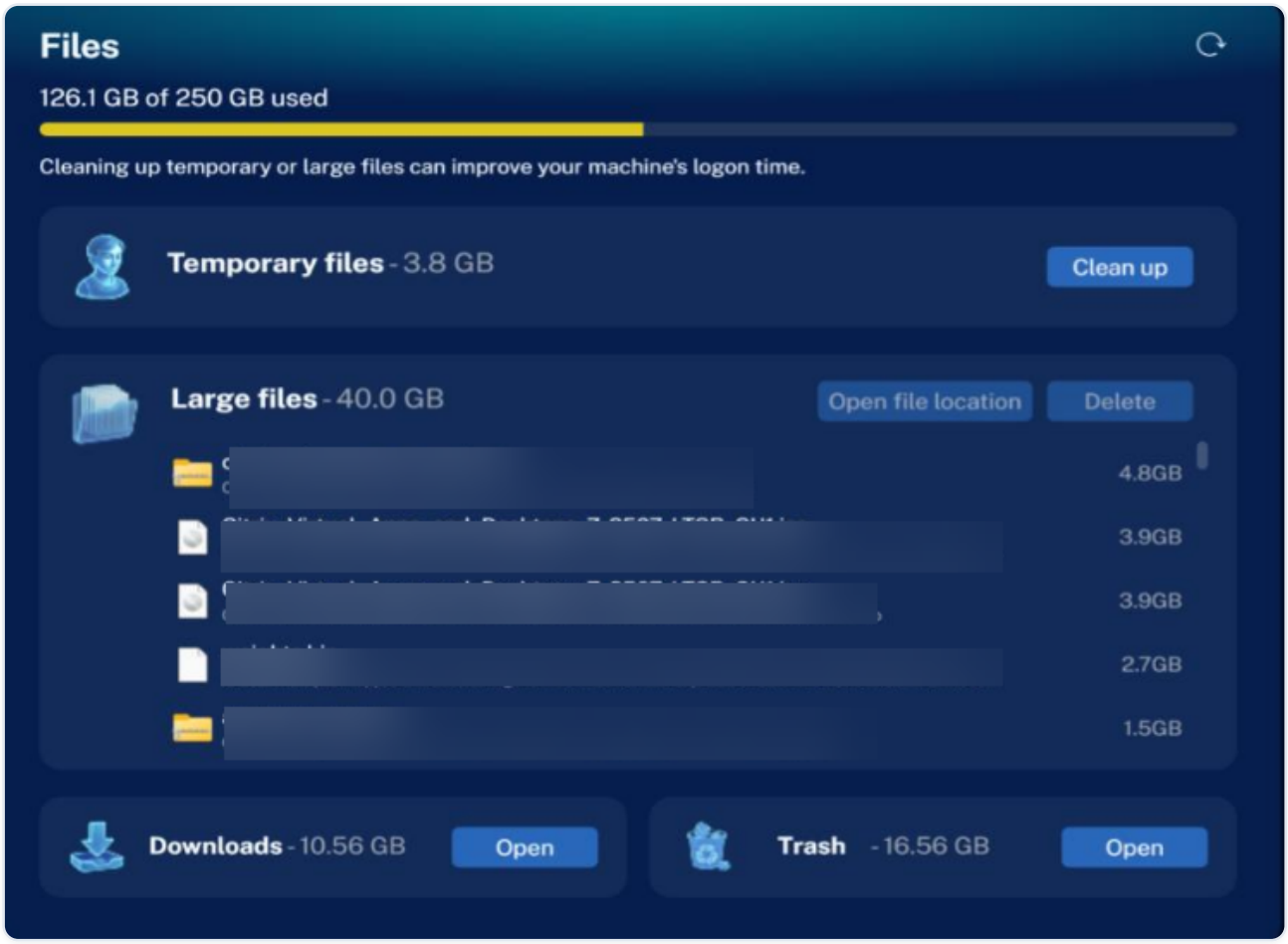


文件页面

文件页面提供有关您的用户配置文件的信息，并帮助清理临时文件或大文件（大于 100 MB）。此操作可以显著缩短您计算机的登录时间。临时文件包括崩溃转储报告、应用程序缓存以及导致配置文件臃肿的隐藏文件。

- 临时文件：单击**清理**以清理临时文件。
- 大文件：您可以单击**删除**以删除大文件，或单击**打开文件位置**以转到其位置，然后决定采取适当的操作。您可以使用 **Ctrl** 键同时选择多个文件。
- 下载和垃圾箱文件夹：单击**打开**以转到其位置，然后决定采取适当的操作。

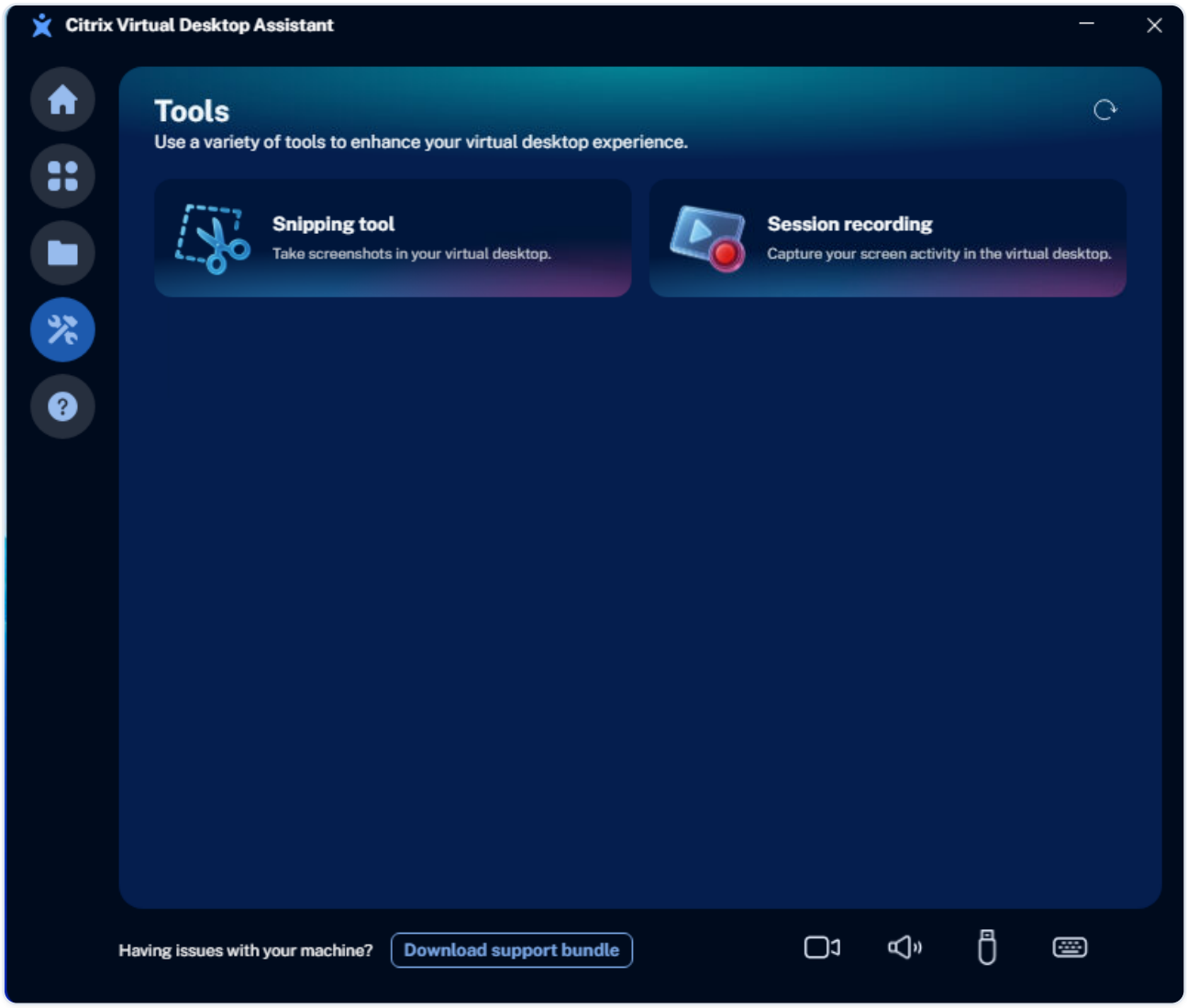
对于容器类型配置文件，您还可以查看容量使用情况。



要重新计算**文件**页面上的数据，请单击应用程序右上角的**刷新**图标。

工具页面

工具页面显示以下工具，以增强您的虚拟桌面体验。



- 截图工具：Citrix 截图工具允许用户在其 Citrix Virtual Apps and Desktops 会话中无缝捕获覆盖和重定向内容的屏幕截图。这包括优化的媒体，例如浏览器内容重定向 (BCR)、Microsoft Teams 优化以及其他统一通信平台。有关详细信息，请参阅Citrix 截图工具文档

  要捕获会话内屏幕截图：

  a. 点击**截图工具**。

  b. 点击**新建**以开始新的截图并选择要捕获的区域。

  c. 捕获截图后，将截图保存为 `.PNG` 或 `.BMP` 文件格式的文件，或保存到剪贴板。

  > **注意：**
  >
  > - 默认情况下，截图工具可以捕获 VDA 会话的用户定义区域。或者，截图工具还可以用于捕获整个屏幕的完整会话内屏幕截图（单屏幕），或在多屏幕使用时捕获（所有屏幕）。

> ◦ 截图工具还可以用于延迟截图。使用延迟按钮选择所需的延迟时间。设置的延迟时间结束后，将进行屏幕截图。

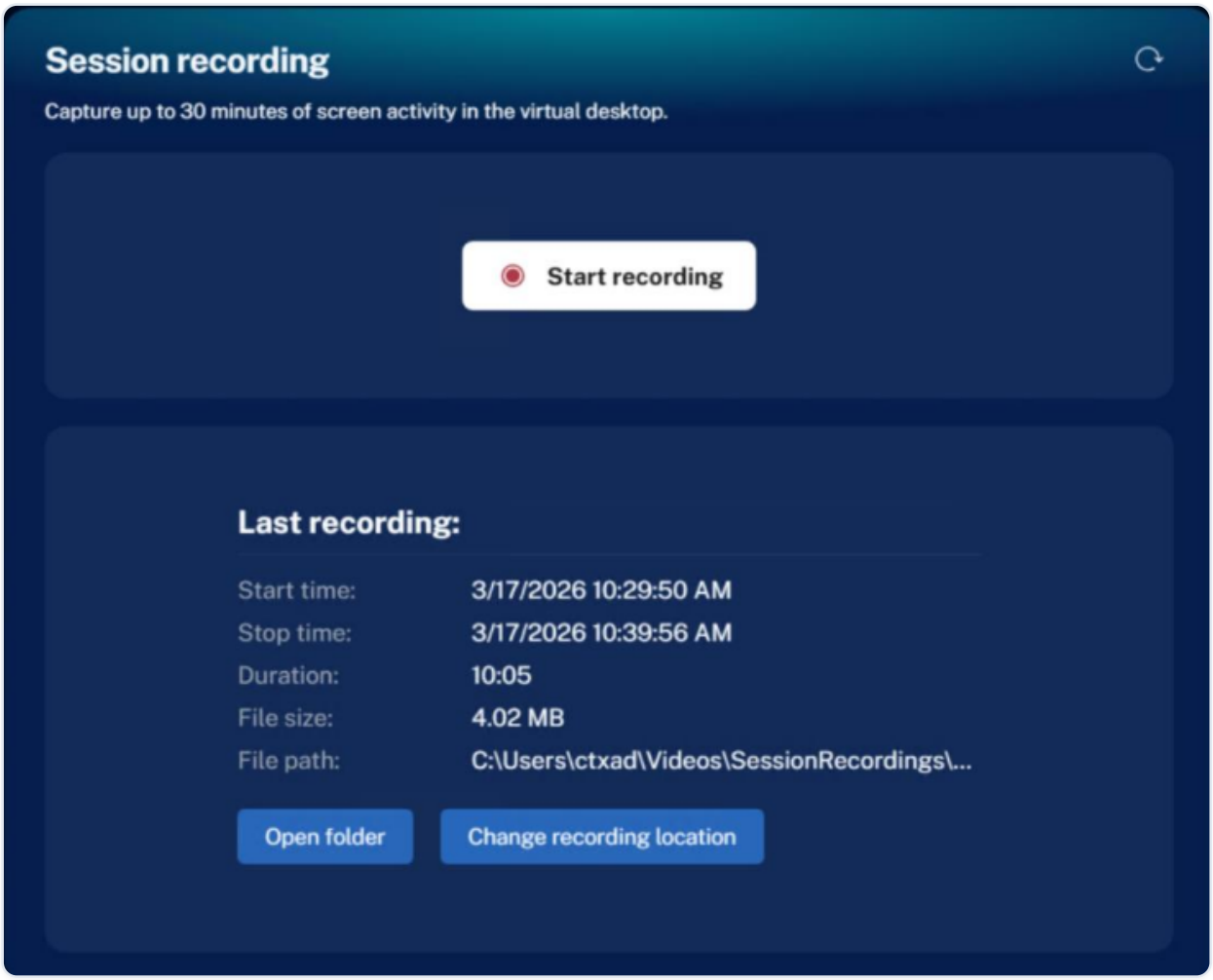
> 如果未捕获叠加内容，请检查以下各项：

- 确认 Web Studio 中已启用**屏幕截图重定向内容**策略。
- 确保 VDA 和 Citrix Workspace App 版本满足最低要求。
  - VDA: 2607 LTSR 或更高版本
  - 适用于 Windows 的 Citrix Workspace App (CWA): 2607 LTSR 或更高版本
  - 支持的客户端: 仅限 Windows
- 检查 App Protection 是否正在阻止屏幕截图功能。

- 会话录制: 将您的活动虚拟桌面会话录制为 MP4 视频剪辑，用于故障排除、协作和会话审查。

  在**会话录制**页面上，您可以使用以下选项管理捕获：

  - **开始录制**: 开始捕获当前桌面会话。将显示录制指示器以确认录制正在进行中。
  - **停止录制**：结束捕获并自动将视频保存为 MP4 文件。



会话录制页面提供以下选项来管理捕获的内容：

- **打开文件夹**：打开配置的目录，其中存储了录制的 MP4 文件。默认情况下，录制内容保存到：`%userprofile%\Videos\SessionRecordings`。
- **更改录制位置**：允许您修改会话录制的存储路径。支持的位置包括：
  - 本地存储：虚拟机本地驱动器上的文件夹。
  - 网络路径：可访问的映射网络驱动器或 UNC 路径（例如，`\\Server\Share\Recordings`），前提是您具有写入权限。

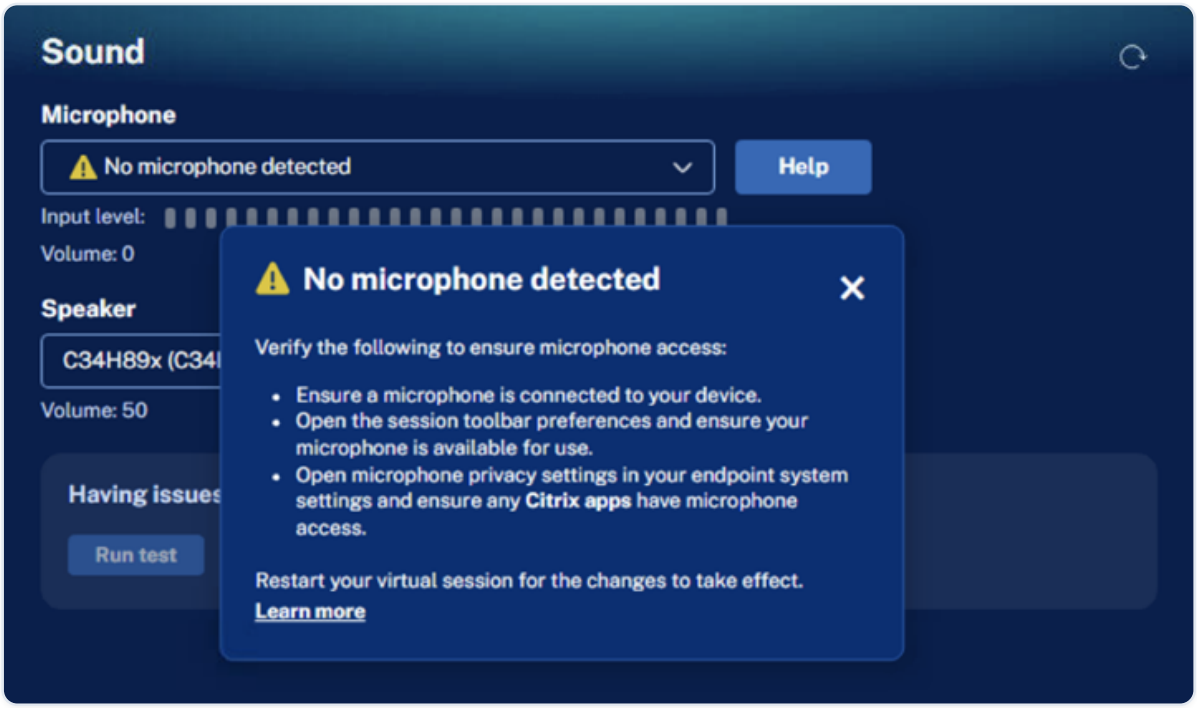
声音页面

Citrix Virtual Desktop Assistant 应用程序的声音页面有助于诊断和排查 VDA 会话中的音频设置问题。

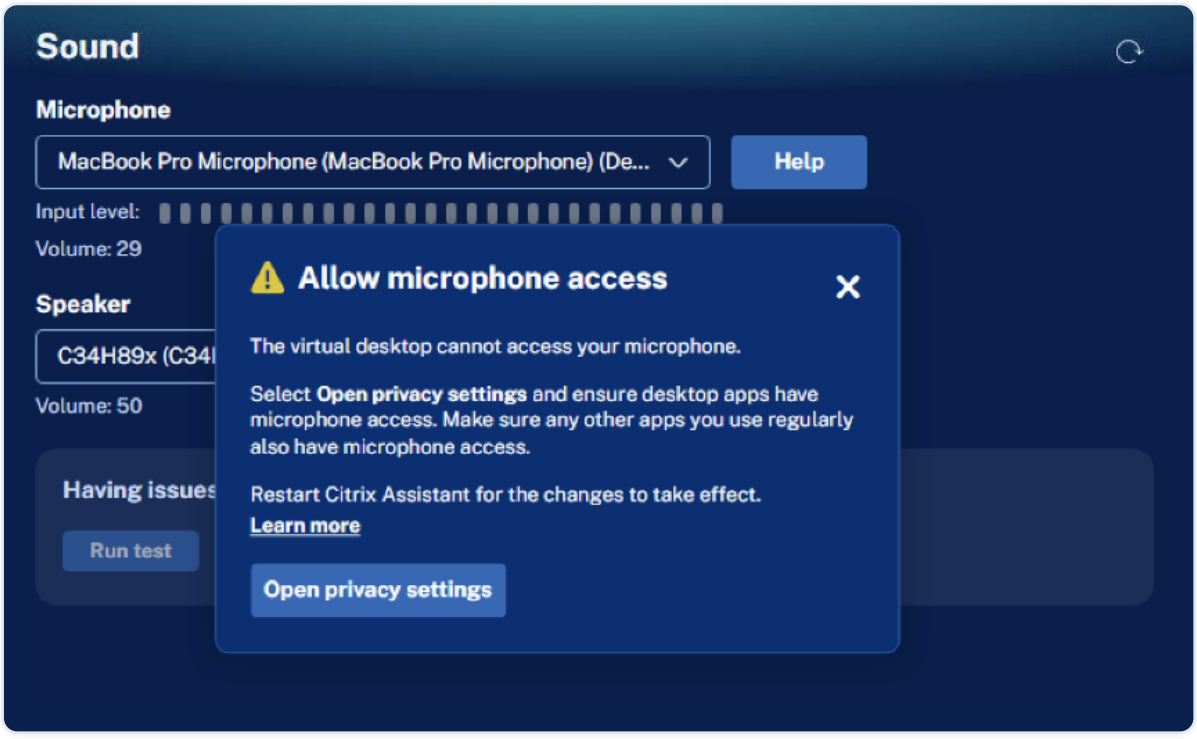
- 如果连接了多个音频设备，您可以从下拉列表中选择麦克风和扬声器。

  如果 Citrix Virtual Desktop Assistant 无法使用您的麦克风，您可能会看到以下警告消息之一：

- **未检测到麦克风**：这很可能是由于 Citrix Workspace 应用程序的麦克风隐私设置被禁用所致。请检查您的麦克风隐私设置，并按照对话框中显示的提示为 Citrix Workspace 应用程序启用访问权限。

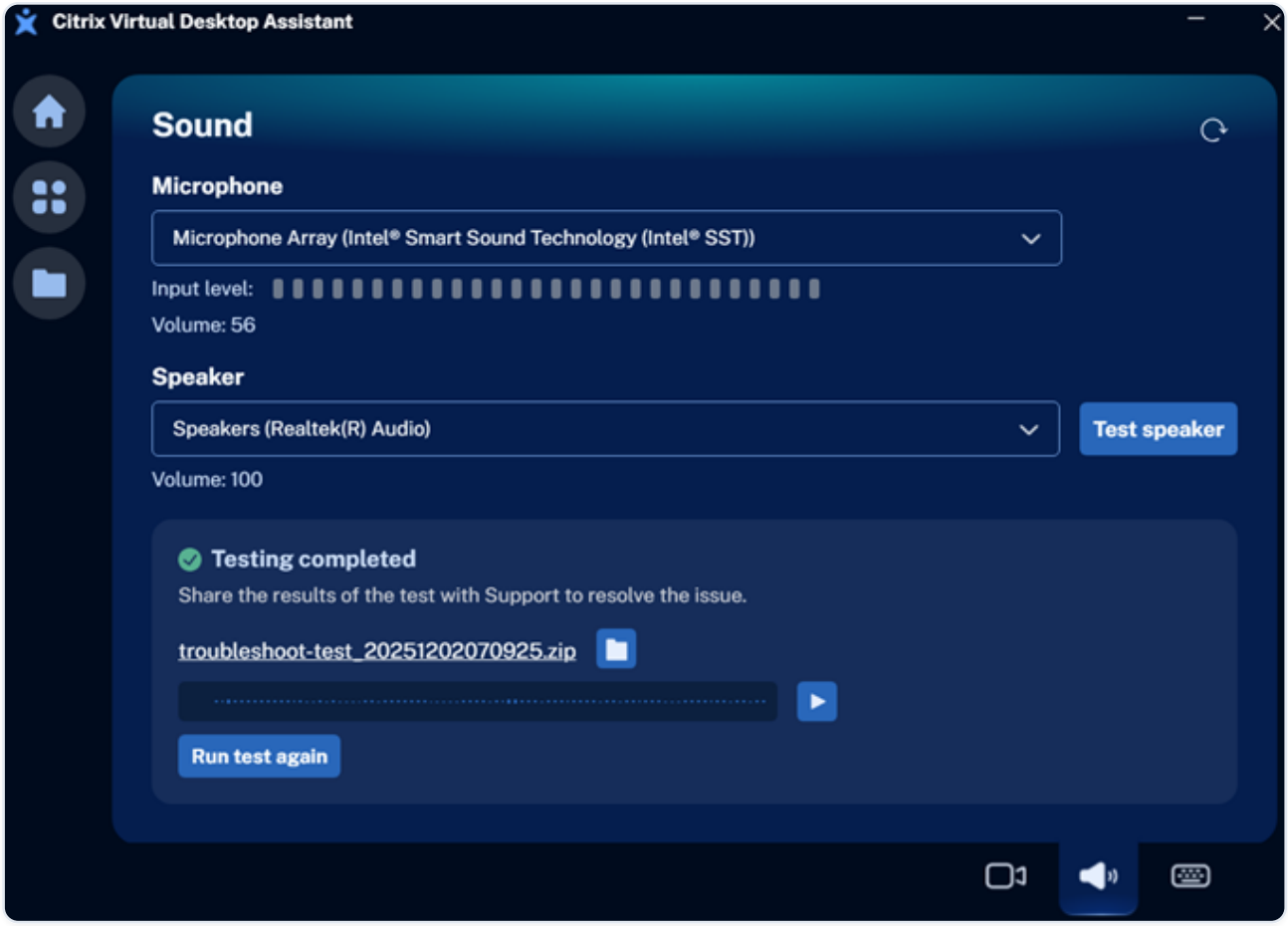


- **允许麦克风访问**：当 Citrix Virtual Desktop Assistant 在当前 Citrix 虚拟桌面中没有麦克风访问权限时，会发生这种情况。按照对话框中显示的提示解决此问题。



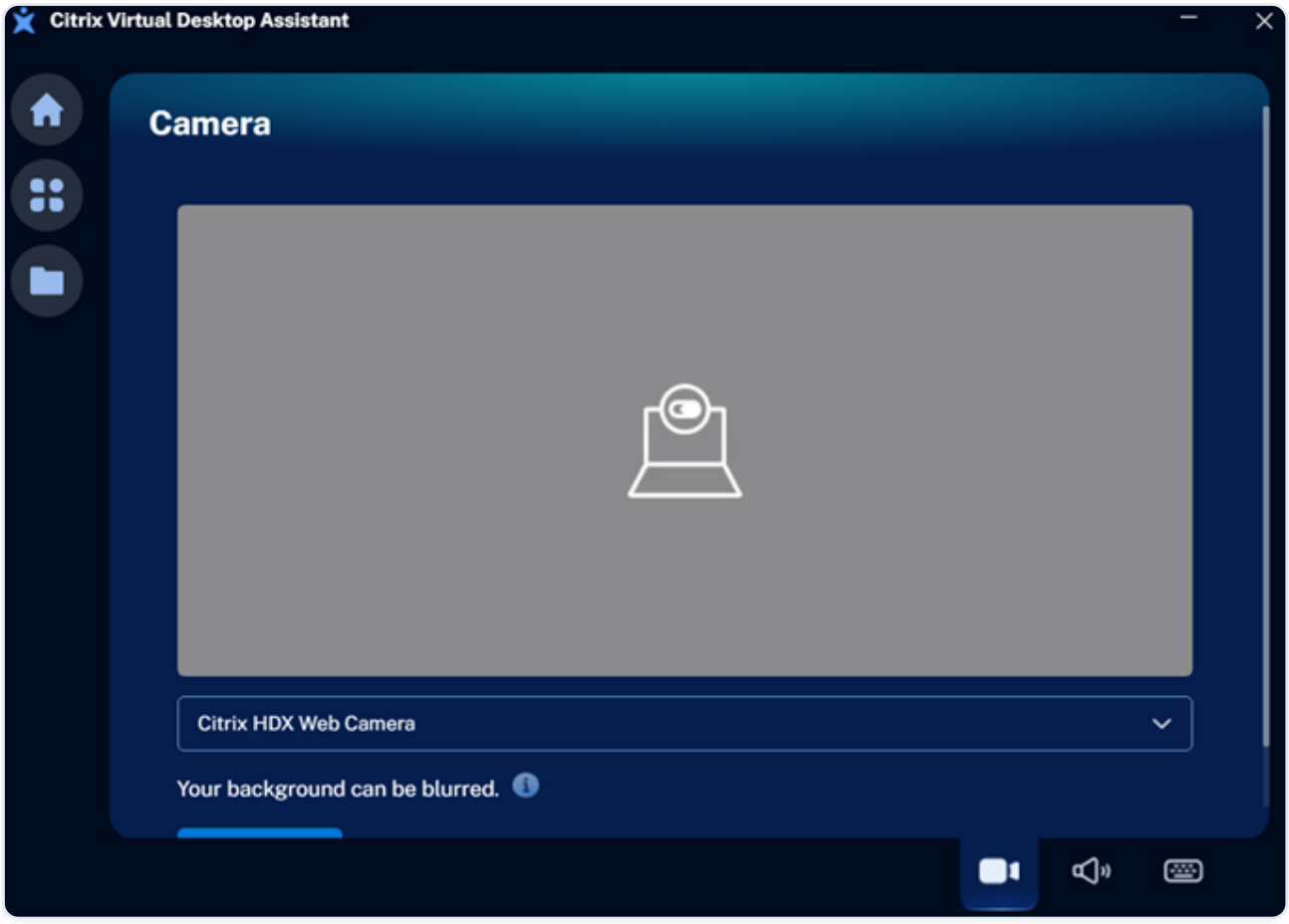
- 单击“**测试扬声器**”以通过播放演示音频来测试所选扬声器设备。

- 在 VDA 会话中排查音频设备问题时，单击“**运行测试**”，然后应用程序会录制声音输入。此录音随后会导出为 zip 文件。您可以将 zip 文件共享给您的 IT 或 Citrix 管理员团队以获得帮助。您还可以重播音频以验证声音播放。



摄像头页面

Citrix Virtual Desktop Assistant 应用程序的摄像头页面有助于在 VDA 会话中配置视频设置。



- 如果连接了多个摄像头，您可以从下拉列表中选择一个摄像头。

> **注意：**
>
> 如果只显示“**Citrix HDX Web Camera**”，并且您在 CWA 客户端上连接了多个摄像头设备，请重新启动 VDA 计算机以查看所有连接的摄像头设备列表。请务必在安装 Citrix Virtual Desktop Assistant 应用程序后才重新启动。

- 您可以模糊背景。要模糊背景，请导航到“**Citrix Workspace™ app > Preferences > Default webcam > Enable background blur**”。
- 要调整摄像头设置，请单击“**重试摄像头**”。但是，请确保摄像头未被其他视频会议工具使用。

键盘页面

“**键盘**”页面在一个视图中显示本地设备键盘布局、虚拟桌面键盘布局、同步设置和键盘快捷方式设置。您可以从 Citrix Workspace 应用程序 (CWA) 首选项工具栏更新这些设置，更改会反映在 Assistant 应用程序中。

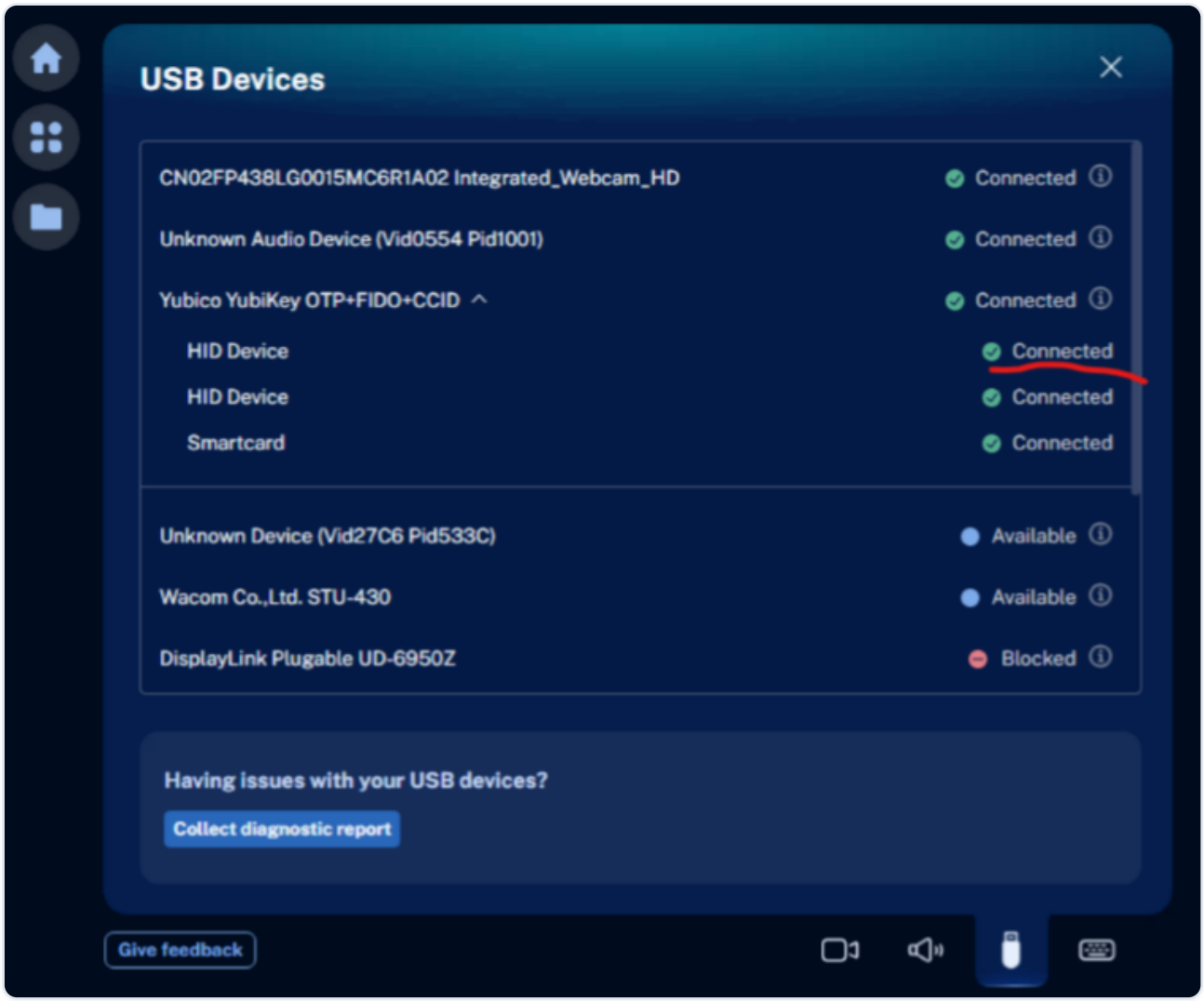
要在 VDA 会话中排查键盘或 IME 问题，请单击页面底部的“**收集诊断报告**”。



> **注意：**
>
> 悬停在信息图标上，了解键盘设置值。

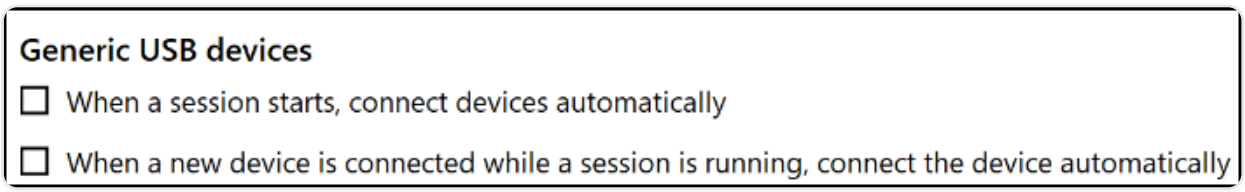
USB 页面

USB 页面可让您查看 USB 设备。



如果您在 Citrix Assistant 中未看到 USB 屏幕，请确保满足以下条件：

- 您的 Citrix Workspace 应用程序 (CWA) 版本为 2511 或更高版本。
- USB 重定向策略 已禁用。
- 您的“首选项”工具栏中已选中以下复选框。



USB 设备可以有五种不同的状态值：

- **已连接**：这些设备已成功重定向，使用虚拟通道，并且可在客户端和 VDA 上使用。
- **已连接（带信息）**：这些 USB 设备已成功重定向，可在 VDA 上使用。您可以通过从 Citrix Workspace 应用程序 (CWA) 工具栏访问**设备**工具栏来禁用它们。
- **缺少驱动程序**：这些设备需要在 VDA 上安装驱动程序，但目前缺少该驱动程序。

- **已阻止**：这些设备已被管理员通过设备规则阻止。要使用这些设备，请联系您的管理员。
- **可用**：从**设备**工具栏启用这些设备。启用后，它们将连接并可在 VDA 上使用。

为了排查 VDA 会话中的 USB 问题，请单击页面底部的“**收集诊断报告**”。

AOT 日志

如果您的管理员已设置“始终开启跟踪 (AOT)”功能，并且您的 VDA 遇到问题，请单击“**下载支持包**”以导出您的会话日志并与您的管理员共享。日志还会捕获您的 Citrix 软件版本，供管理员或支持人员根据版本隔离问题。

Citrix Assistant 应用程序 AOT(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/assistant-aot-log.png)

关于页面

在左侧窗格中，右键单击“**关于**”图标以打开“**关于**”页面。

Citrix Assistant 应用程序 AOT(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/assistant-app-about-page_1.png)

Citrix Virtual Desktop Assistant 应用程序的版本信息和第三方许可证条目显示在“**关于**”页面上。

您还可以下载支持文件，并随 Citrix Virtual Desktop Assistant 日志一起发送反馈。

Citrix Assistant 应用程序 AOT(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/assistant-send-feedback-page.png)

限制

- **临时文件清理限制**：只读、已损坏或正在使用的临时文件无法清理。
- **大文件渲染时间**：“**大文件**”部分可能需要很长时间才能显示文件。我们正在努力减少这些文件的列出时间。
- **录制位置限制**：会话录制存储路径目前仅支持英文字符。

监控

管理员和技术支持人员可以使用各种功能和工具监控 Citrix Virtual Apps and Desktops™ 站点。使用这些工具，您可以监控：

- 用户会话和会话使用情况
- 登录性能
- 连接和计算机，包括故障
- 负载评估
- 历史趋势
- 基础结构

思杰监控台

Director 是一款实时 Web 工具，可用于监控和故障排除，并为最终用户执行支持任务。

有关详细信息，请参阅 Director 文章。

配置日志记录

配置日志记录允许管理员跟踪对站点的管理更改。配置日志记录可以帮助管理员在进行配置更改后诊断和排除问题，协助变更管理和跟踪配置，并报告管理活动。

您可以从 Studio 查看和生成有关已记录信息的报告。您还可以在 Director 中使用趋势视图查看已记录的项目，以提供配置更改通知。此功能对于无法访问 Studio 的管理员非常有用。

趋势视图提供了一段时间内配置更改的历史数据，以便管理员可以评估对站点进行了哪些更改、何时进行的以及由谁进行的，从而找出问题的根源。此视图将配置信息分为三类：

- 连接故障
- 失败的单会话计算机
- 失败的多会话计算机

有关如何启用和配置配置日志记录的详细信息，请参阅配置日志记录。 Director文章介绍了如何从该工具查看日志信息。

事件日志

Citrix Virtual Apps and Desktops™ 中的服务会记录发生的事件。事件日志用于监视和排查操作问题。

有关详细信息，请参阅事件日志。各个功能文章也可能包含事件信息。

配置日志记录

配置日志记录是一项功能，可将站点配置更改和管理活动捕获到数据库中。此功能默认启用。您可以使用记录的内容来：

- 在配置更改后诊断和解决问题。日志提供了一个跟踪线索。
- 协助变更管理并跟踪配置。
- 报告管理活动。

您可以从 Citrix Studio 设置配置日志记录首选项、显示配置日志以及生成 HTML 和 CSV 报告。您可以按日期范围和全文搜索结果筛选配置日志显示。强制日志记录（启用时）会阻止进行配置更改，除非这些更改可以被记录。获得适当权限后，您可以从配置日志中删除条目。您不能使用配置日志记录功能编辑日志内容。

配置日志记录使用 PowerShell SDK 和配置日志记录服务。配置日志记录服务在站点中的每个控制器上运行。如果一个控制器发生故障，另一个控制器上的服务会自动处理日志记录请求。

默认情况下，配置日志记录功能处于启用状态，并使用在创建站点时创建的数据库（站点配置数据库）。您可以为数据库指定不同的位置。配置日志记录数据库支持与站点配置数据库相同的高可用性功能。

对配置日志记录的访问通过委派管理进行控制，具有“编辑日志记录首选项”和“查看配置日志”权限。

配置日志在创建时即已本地化。例如，以英语创建的日志将以英语读取，无论读者的区域设置如何。

记录了什么

从 Studio、Director 和 PowerShell 脚本启动的配置更改和管理活动都会被记录。记录的配置更改示例包括处理（创建、编辑、删除、分配）：

- 计算机目录
- 交付组（包括更改电源管理设置）
- 管理员角色和范围

- 主机资源和连接
- 通过 Studio 的 Citrix 策略

记录的管理更改示例包括：

- 虚拟机或用户桌面的电源管理
- Studio 或 Director 向用户发送消息

以下操作不会被记录：

- 自主操作，例如池管理虚拟机的电源开启。
- 通过组策略管理控制台 (GPMC) 实现的策略操作；使用 Microsoft 工具查看这些操作的日志。
- 通过注册表、直接访问数据库或来自 Studio、Director 或 PowerShell 以外的源进行的更改。
- 部署初始化时，当第一个配置日志记录服务实例向配置服务注册时，配置日志记录才可用。因此，配置的早期阶段不会被记录（例如，获取和应用数据库架构时，初始化管理程序时）。

管理配置日志记录

默认情况下，配置日志记录使用创建站点时创建的数据库（也称为站点配置数据库）。Citrix 建议您将配置日志记录数据库（和监视数据库）放置在单独的位置，原因如下：

- 配置日志记录数据库的备份策略可能与站点配置数据库的备份策略不同。
- 为配置日志记录（和监视服务）收集的数据量可能会对站点配置数据库的可用空间产生不利影响。
- 它将三个数据库的单点故障分离开来。

不支持配置日志记录的产品版本在 Studio 中没有“日志记录”节点。

启用和禁用配置日志记录以及强制日志记录

默认情况下，配置日志记录处于启用状态，强制日志记录处于禁用状态。

1. 登录 Web Studio 并在左侧窗格中选择 **日志记录**。
2. 在操作栏中选择 **首选项**。配置日志记录对话框包含数据库信息，并指示配置日志记录和强制日志记录是启用还是禁用。
3. 选择所需操作：

   要启用配置日志记录，请选择 **启用**。这是默认设置。如果无法写入数据库，则日志记录信息将被丢弃，但操作会继续。

要禁用配置日志记录，请选择 **禁用**。如果以前启用了日志记录，则现有日志仍可通过 PowerShell SDK 读取。

要启用强制日志记录，请选择 **当数据库不可用时阻止更改站点配置**。除非可以将配置更改或通常记录的管理活动写入配置日志记录数据库，否则不允许进行此类更改或活动。仅当启用配置日志记录时（即选择 **启用** 时），才能启用强制日志记录。如果配置日志记录服务失败且未使用高可用性，则假定为强制日志记录。在这种情况下，通常会记录的操作将不会执行。

要禁用强制日志记录，请选择 **当数据库不可用时允许更改站点配置**。即使无法访问配置日志记录数据库，也允许进行配置更改和管理活动。这是默认设置。

更改配置日志记录数据库位置

当强制日志记录启用时，您无法更改数据库位置，因为位置更改包括一个无法记录的短暂断开连接间隔。

1. 使用受支持的 SQL Server 版本创建数据库服务器。
2. 登录 Web Studio 并在左侧窗格中选择 **日志记录**。
3. 在操作栏中选择 **首选项**。
4. 在“日志记录首选项”对话框中，选择 **更改日志记录数据库**。
5. 在“更改日志记录数据库”对话框中，指定包含新数据库服务器的服务器位置。有关有效格式，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/technical-overview/databases.html#database-address-formats)。
6. 要允许 Studio 创建数据库，请单击 **确定**。出现提示时，单击 **确定**，数据库将自动创建。Studio 尝试使用当前 Studio 用户的凭据访问数据库。如果失败，系统会提示您输入数据库用户的凭据。然后，Studio 会将数据库架构上传到数据库。（凭据仅在数据库创建期间保留。）
7. 要手动创建数据库，请单击**生成数据库脚本**。生成的脚本包含手动创建数据库的说明。在上传架构之前，请确保数据库为空，并且至少有一个用户有权访问和更改数据库。

以前数据库中的配置日志记录数据不会导入到新数据库。检索日志时，无法从两个数据库聚合日志。新配置日志记录数据库中的第一个日志条目指示发生了数据库更改，但它不标识以前的数据库。

查看配置日志内容

要查看配置日志内容，请在左侧窗格中选择**日志记录**，然后选择**事件**选项卡。

默认情况下，事件日志按管理员名称列出。您可以根据需要执行以下任务：

- **查看日志详细信息。** 高级操作会导致一个或多个服务和 SDK 调用，这些是低级操作。当您在上部窗格中选择高级操作时，下部窗格会显示低级操作。
- **排序显示。** 通过单击列标题对显示进行排序。
- **筛选日志。** 通过设置筛选条件（例如日期间隔或自定义周期）或在搜索框中输入完整或部分主任务名称来优化显示。使用搜索后要返回标准显示，请清除搜索框中的文本。
- **导出日志。** 将选定日志或所有日志导出到 CSV 文件，以进行存档或进一步分析。
- **自定义列。** 通过添加非默认列（例如客户端 IP 和标签）来根据您的需要调整显示。
- **管理标签。** 添加、编辑和删除事件日志的标签，以增强日志组织和跟踪。

显示特性：

- 如果操作在完成之前失败，则日志操作可能未在数据库中完成。例如，开始记录没有相应的停止记录。在这种情况下，日志会指示信息缺失。当您根据时间范围显示日志时，如果数据符合条件，则会显示不完整的日志。

  例如，如果您请求过去五天的日志，并且过去五天内开始但没有结束时间的日志也会被包括在内。
- 当使用调用 PowerShell cmdlet 的脚本时，如果您创建低级操作而未指定父高级操作，则配置日志记录会创建一个替代高级操作。

生成报告

您可以生成包含配置日志数据的 CSV 和 HTML 报告。

- CSV 报告包含指定时间间隔内的所有日志记录数据。数据库中的分层数据被展平为单个 CSV 表。数据在文件中没有优先级。不使用任何格式，也不假定人类可读性。该文件（名为 MyReport）以通用可消费格式包含数据。CSV 文件通常用于存档数据或作为 Microsoft Excel 等报告或数据操作工具的数据源。
- HTML 报告以人类可读的形式提供指定时间间隔内的日志记录数据。它提供了一个结构化、可导航的视图，用于查看更改。HTML 报告包含两个文件，分别名为 Summary 和 Details。Summary 列出高级操作：每个操作发生的时间、执行者和结果。单击每个操作旁边的**详细信息**链接会将您带到 Details 文件中的低级操作，其中提供了更多信息。

要生成配置日志报告，请在 Studio 导航窗格中选择**日志记录**，然后在操作栏中选择**创建自定义报告**。

- 选择报告的日期范围。
- 选择报告格式：CSV、HTML 或两者。

- 浏览到要保存报告的位置。

删除配置日志内容

要删除配置日志，您必须具有特定的委派管理和 SQL Server 数据库权限。

- **委派管理：** 您必须具有允许读取部署配置的委派管理角色。完全管理员角色具有此权限。自定义角色必须在“其他权限”类别中选择“只读”或“管理”。

  要在删除配置日志数据之前创建备份，自定义角色还必须在“日志记录权限”类别中选择“只读”或“管理”。

- **SQL Server 数据库：** 您必须具有有权从数据库中删除记录的 SQL Server 登录名。有两种方法可以执行此操作：

  - 使用具有 sysadmin 服务器角色的 SQL Server 数据库登录名，该角色允许您在数据库服务器上执行任何活动。或者，`serveradmin` 或 `setupadmin` 服务器角色允许您执行删除操作。
  - 如果您的部署需要更高的安全性，请使用映射到有权从数据库中删除记录的数据库用户的非 sysadmin 数据库登录名。

    a. 在 SQL Server Management Studio 中，创建一个服务器角色不是“sysadmin”的 SQL Server 登录名。

    b. 将登录名映射到数据库中的用户。SQL Server 会自动在数据库中创建一个与登录名同名的用户。

    c. 在“数据库角色成员身份”中，为数据库用户指定至少一个角色成员：`ConfigurationLoggingSchema_ROLE` 或 `dbowner`。

    有关详细信息，请参阅 SQL Server Management Studio 文档。

要删除配置日志：

1. 登录 Web Studio 并在左侧窗格中选择“**日志记录**”。
2. 在操作栏中选择“**删除日志**”。
3. 系统会询问您是否要在删除日志之前创建日志备份。如果您选择创建备份，请浏览到保存备份存档的位置。备份将创建为 CSV 文件。

配置日志清除后，日志删除是发布到空日志的第一项活动。该条目提供有关谁在何时删除了日志的详细信息。

查看 API 和 PowerShell 日志

要监视当前会话期间发出的 API 请求，请单击“**API**”选项卡。退出 Web Studio 后，API 日志将被清除。

要查看与您当天执行的 UI 操作对应的 PowerShell 命令，请单击“**PowerShell**”选项卡。

将元数据与配置日志关联

您可以通过将一个名为 `MetadataMap` 的 `name-value` 对与日志记录关联，从而将元数据附加到配置日志。

> **注意：**
>
> - 您只能将元数据附加到高级操作对象。
> - 元数据在执行时与现有记录关联。

设置元数据

运行 PowerShell 命令 `Set-LogHighLevelOperationMetadata` 以将日志记录与 `MetadataMap` 关联。 `Set-LogHighLevelOperationMetadata` 接受以下参数：

- **Id**：高级操作的 ID。
- **InputObject**：您向其添加元数据的高级操作。这是 `Id` 参数的替代方法，其中高级操作对象或对象列表传递给 PowerShell 命令。
- **Name**：要添加的元数据的属性名称。该属性对于指定的高级操作必须是唯一的。该属性不能包含以下任何字符：()\/;:#.*?=<>|'"。
- **Value**：属性的值。
- **Map**：属性的（名称、值）对字典。这是使用 `-Name` 和 `-Value` 参数设置元数据的替代方法。

例如，要将元数据附加到所有 Id 为 40 的高级日志记录，请运行以下 PowerShell 命令：

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata -Name A -Value B
```

要将元数据附加到用户为 `abc@example.com` 的高级记录，请运行以下 PowerShell 命令：

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-
LogHighLevelOperationMetadata -Name C -Value D
```

使用元数据检索

运行以下 PowerShell 命令以使用关联的元数据检索日志记录：

- 按键和值搜索：

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- 按值搜索任意键：

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- 按键搜索任意值：

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

移除元数据

运行 PowerShell 命令 `Remove-LogHighLevelOperationMetadata` 以移除关联的元数据。`Remove-LogHighLevelOperationMetadata` 接受以下参数：

- **Id**：高级操作的 ID。
- **InputObject**：您添加元数据的高级操作。这是 `Id`` 参数的替代方法，其中高级操作对象或对象列表将传递给 PowerShell 命令。
- **Name**：要移除的元数据的属性名称。设置为 $null 以移除指定对象的所有元数据。
- **Map**：属性的（名称、值）对字典。这可以是哈希表（使用 @{"name1" = "val1"; "name2" = "val2"} 创建）或字符串字典（使用 new-object "System.Collections.Generic.Dictionary" 创建）。名称与映射中的键匹配的属性将被移除。

最佳实践

1. **首先使用直接参数**。将已知操作与相应的参数匹配：`-User`、`-OperationType`、`-TargetType`、`-Source` 或 `-IsSuccessful`。
2. **始终包含时间范围**。`-StartTime` 和 `-EndTime` 是任何查询最有效的首个筛选器。
3. **从高级别深入到低级别**。调查特定操作时，首先检索高级别操作，然后将其 ID 与 `-HighLevelOperationId` 结合使用。
4. **将导出范围限定在感兴趣的时期**。使用 `-StartDateRange` 和 `-EndDateRange` 定位相关时间窗口。
5. **当不需要显示名称时，对导出使用 `-RawReport`**。这可以减少处理时间和输出大小。

事件日志

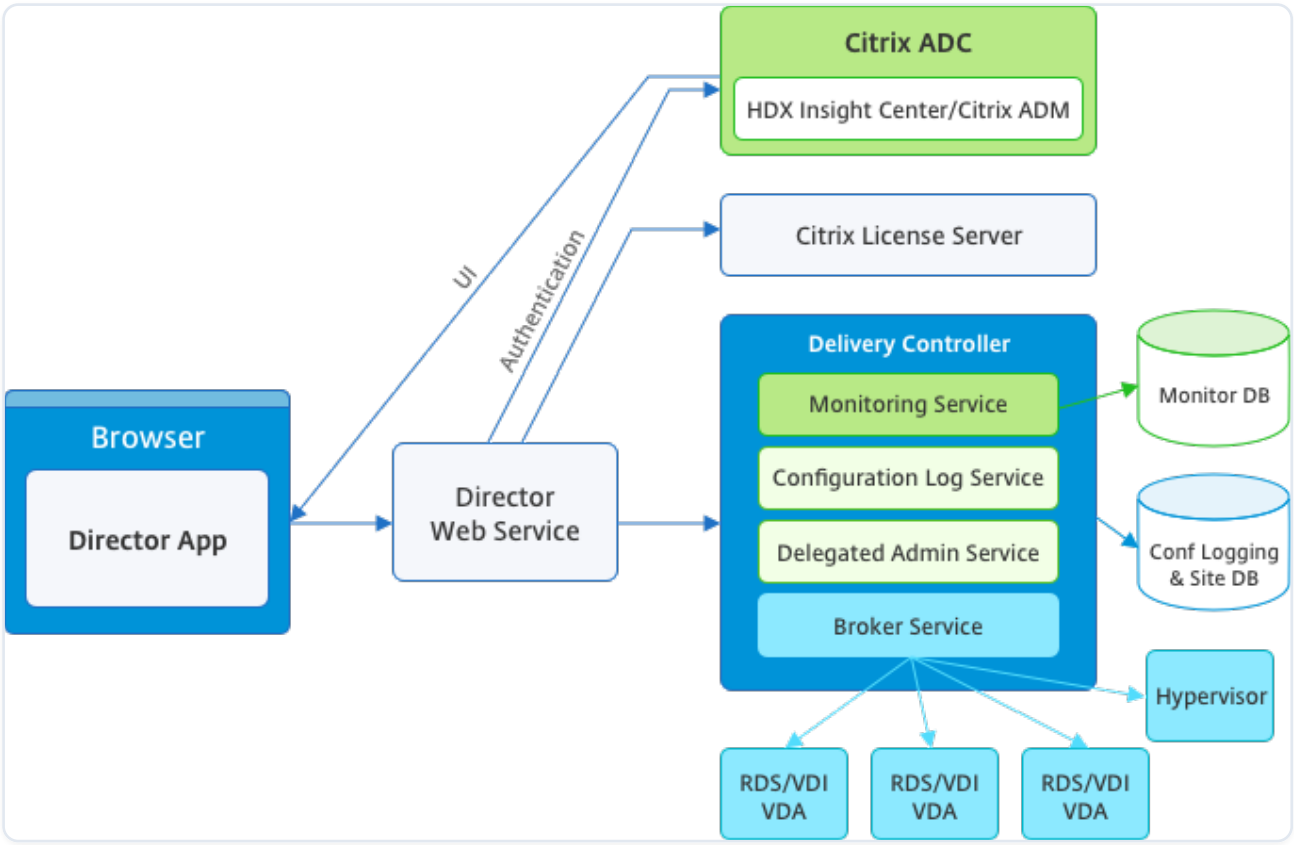
以下文章列出并描述了 Citrix Virtual Apps and Desktops 中服务可以记录的事件。

此信息并非详尽无遗。读者应查阅各个功能文章以获取更多事件信息。

- Citrix Broker 服务事件
- Citrix FMA 服务 SDK 事件
- Citrix Configuration 服务事件
- Citrix 委派管理服务事件

导向器

Director 是一个用于 Citrix Virtual Apps and Desktops 的监控和故障排除控制台。



Director 可以访问：

- 来自 Broker Agent 的实时数据，使用与 Analytics、Performance Manager 和 Network Inspector 集成的统一控制台。以下分析由 Citrix ADM 提供支持，用于识别您的 Citrix Virtual Apps™ 或 Desktops 环境中由于网络造成的瓶颈：
  - 用于健康状况和容量保障的性能管理
  - 历史趋势和网络分析
- 存储在 Monitor 数据库中的历史数据，用于访问 Configuration Logging 数据库。
- 来自 Citrix Gateway 的 ICA® 数据，使用 Citrix ADM。
  - 深入了解 Citrix Virtual Apps 或 Desktops 的虚拟应用程序、桌面和用户的最终用户体验。
  - 将网络数据与应用程序数据和实时指标关联起来，以实现有效的故障排除。
  - 与 Citrix Virtual Desktop 7 Director 监控工具集成。

Director 使用故障排除控制板，提供 Citrix Virtual Apps 或 Desktops 站点的实时和历史健康状况监控。此功能允许您实时查看故障，从而更好地了解最终用户的体验。

有关 Director 功能与 Delivery Controller (DC)、VDA 和任何其他相关组件兼容性的更多信息，请参阅 功能兼容性矩阵。

> **注意：**

> 随着 Meltdown 和 Spectre 推测执行侧信道漏洞的披露，Citrix 建议您安装相关的缓解补丁。这些补丁可能会影响 SQL Server 性能。有关更多信息，请参阅 Microsoft 支持文章：保护 SQL Server 免受 Spectre 和 Meltdown 侧信道漏洞攻击。Citrix 建议您在生产环境中推出补丁之前，测试规模并规划工作负载。

> Director 默认作为网站安装在 Delivery Controller 上。有关先决条件和其他详细信息，请参阅本版本的系统要求文档。有关 Director 安装和配置的具体信息，请参阅安装和配置 Director。

登录 Director

Director 网站位于 https 或 `http://<Server FQDN>/Director`。

如果多站点部署中的某个站点出现故障，则在尝试连接到该故障站点时，登录时间会稍长一些。

将 Director 与 PIV 智能卡身份验证结合使用

Director 现在支持基于个人身份验证 (PIV) 的智能卡身份验证登录。此功能对于使用基于智能卡的身份验证进行访问控制的组织和政府机构非常有用。 智能卡身份验证需要在 Director 服务器和 Active Directory 中进行特定配置。配置步骤详见配置 PIV 智能卡身份验证。

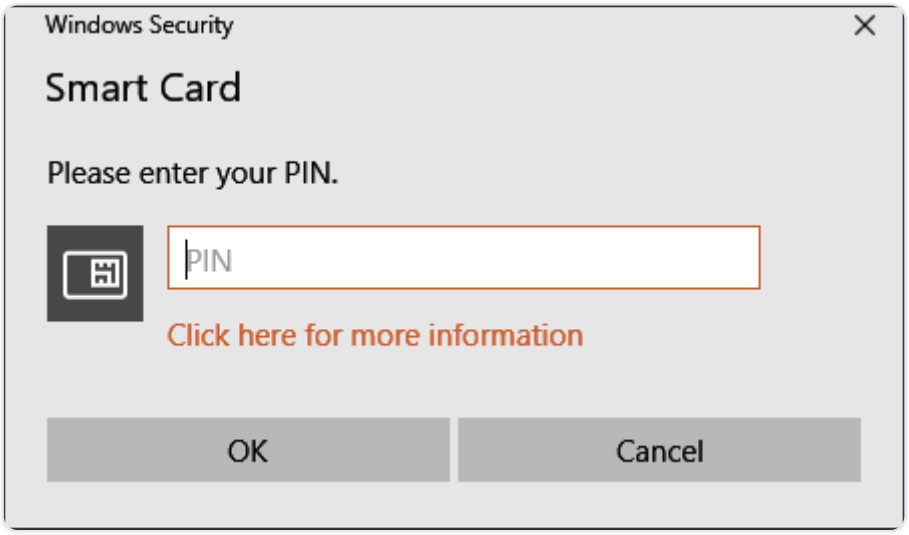
> **注意：**

> 智能卡身份验证仅支持来自同一 Active Directory 域的用户。

> 完成所需配置后，您可以使用智能卡登录 Director：

1. 将智能卡插入智能卡读卡器。
2. 打开浏览器并访问 Director URL，`https://<directorfqdn>/Director`。
3. 从显示的列表中选择一个有效的用户证书。

4. 输入您的智能卡令牌。



5. 身份验证成功后，您无需在 Director 登录页面上输入额外凭据即可访问 Director。

将 Director 与集成 Windows 身份验证结合使用

通过集成 Windows 身份验证 (IWA)，加入域的用户可以直接访问 Director，而无需在 Director 登录页面上重新输入其凭据。使用集成 Windows 身份验证和 Director 的先决条件是：

- 在托管 Director 的 IIS 网站上启用集成 Windows 身份验证。安装 Director 时，会启用匿名身份验证和表单身份验证。为了支持集成 Windows 身份验证和 Director，请禁用匿名身份验证并启用 Windows 身份验证。对于非域用户的身份验证，表单身份验证必须保持启用状态。

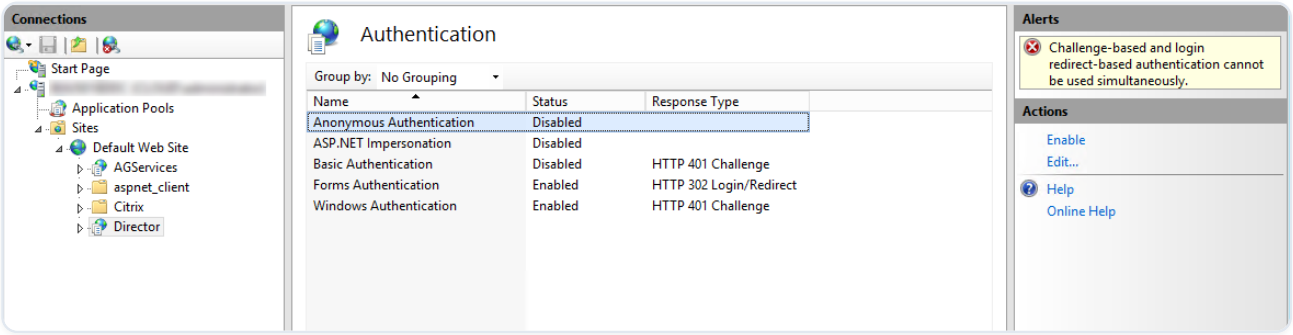
  a. 启动 IIS 管理器。

  b. 转至 **站点** \> **Default Web Site** \> **Director**。

  c. 选择**身份验证**。

  d. 右键单击**匿名身份验证**，然后选择**禁用**。

  e. 右键单击**Windows 身份验证**，然后选择**启用**。



- 为 Director 计算机配置 Active Directory 委派权限。仅当 Director 和 Delivery Controller™ 安装在不同的计算机上时才需要进行配置。

a. 在 Active Directory 计算机上，打开 Active Directory 管理控制台。
b. 在 Active Directory 管理控制台中，导航到 **域名** \> **计算机**。选择 Director 计算机。
c. 右键单击并选择**属性**。
d. 在“属性”中，选择**委派**选项卡。
e. 选择选项**信任此计算机以委派给任何服务（仅限 Kerberos）**。

- 用于访问 Director 的浏览器必须支持集成 Windows 身份验证。Firefox 和 Chrome 中可能需要额外的配置步骤。有关详细信息，请参阅浏览器文档。
- 监控服务必须运行 Microsoft .NET Framework 4.5.1 或 Director 系统要求中列出的更高版本。有关详细信息，请参阅系统要求。

当用户从 Director 注销或会话超时时，将显示登录页面。在登录页面上，用户可以将身份验证类型设置为**自动登录**或**用户凭据**。

界面视图

Director 提供针对特定管理员量身定制的不同界面视图。产品权限决定了显示的内容和可用的命令。

例如，技术支持管理员会看到一个针对技术支持任务量身定制的界面。Director 允许技术支持管理员搜索报告问题的用户，并显示与该用户相关的活动。例如，用户应用程序和进程的状态。他们可以通过执行以下操作快速解决问题：结束无响应的应用程序或进程、在用户计算机上执行影子操作、重新启动计算机或重置用户配置文件。

相比之下，完全管理员可以查看和管理整个站点，并可以对多个用户和计算机执行命令。仪表板提供了部署关键方面的概述，例如会话状态、用户登录和站点基础结构。信息每分钟更新一次。如果出现问题，会自动显示有关已发生的故障数量和类型的详细信息。

有关 Director 中各种角色及其权限的详细信息，请参阅委派管理和 Director

Pendo 收集使用情况数据

Director 安装后，Director 服务开始使用 Pendo 收集使用情况数据。将收集有关趋势页面使用情况和 OData API 调用分析的统计信息。分析收集符合Citrix 隐私策略。安装 Director 时，默认启用数据收集。

要选择退出 Pendo 数据收集，请编辑安装 Director 的计算机上的注册表项。如果注册表项不存在，请创建并将其设置为所需值。更改注册表项值后，刷新 Director 实例。

注意：不正确使用注册表编辑器可能会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证可以解决因不正确使用注册表编辑器而导致的问题。使用注册表编辑器风险自负。Citrix 建议您在更改 Windows 注册表之前对其进行备份。

位置：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名称：DisableGoogleAnalytics

> **注意：**
>
> 以前，Director 服务使用 Google Analytics 收集数据。现在，Pendo 使用相同的注册表项。
>
> 值：0 = 启用（默认），1 = 禁用

您可以使用以下 PowerShell cmdlet 禁用 Pendo 的数据收集功能：

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

新功能指南

Director 具有产品内指南，该指南使用 Pendo 深入了解 Director 当前版本中发布的新功能。快速概述与适当的产品内消息相结合，可帮助您了解产品中的新增功能。

要选择退出此功能，请按照以下说明在安装 Director 的计算机上编辑注册表项。如果注册表项不存在，请创建并将其设置为所需值。更改注册表项值后，刷新 Director 实例。

> **注意：**
>
> 不正确地使用注册表编辑器会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。Citrix 建议您在更改 Windows 注册表之前对其进行备份。

> 位置：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名称：DisableGuidedHelp

值：0 = 启用（默认），1 = 禁用

您可以使用以下 PowerShell cmdlet 禁用产品内指南：

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

参考文章

- 通过 Citrix Director 缩短 MTTR
- Citrix Director - 使用 PowerShell 管理和配置警报和通知
- Citrix Virtual Apps and Desktops 开发人员文档

相关产品中的新增功能

- 思杰 DaaS
- StoreFront
- 安全私有访问
- Citrix 企业浏览器
- Citrix 工作区
- 预配

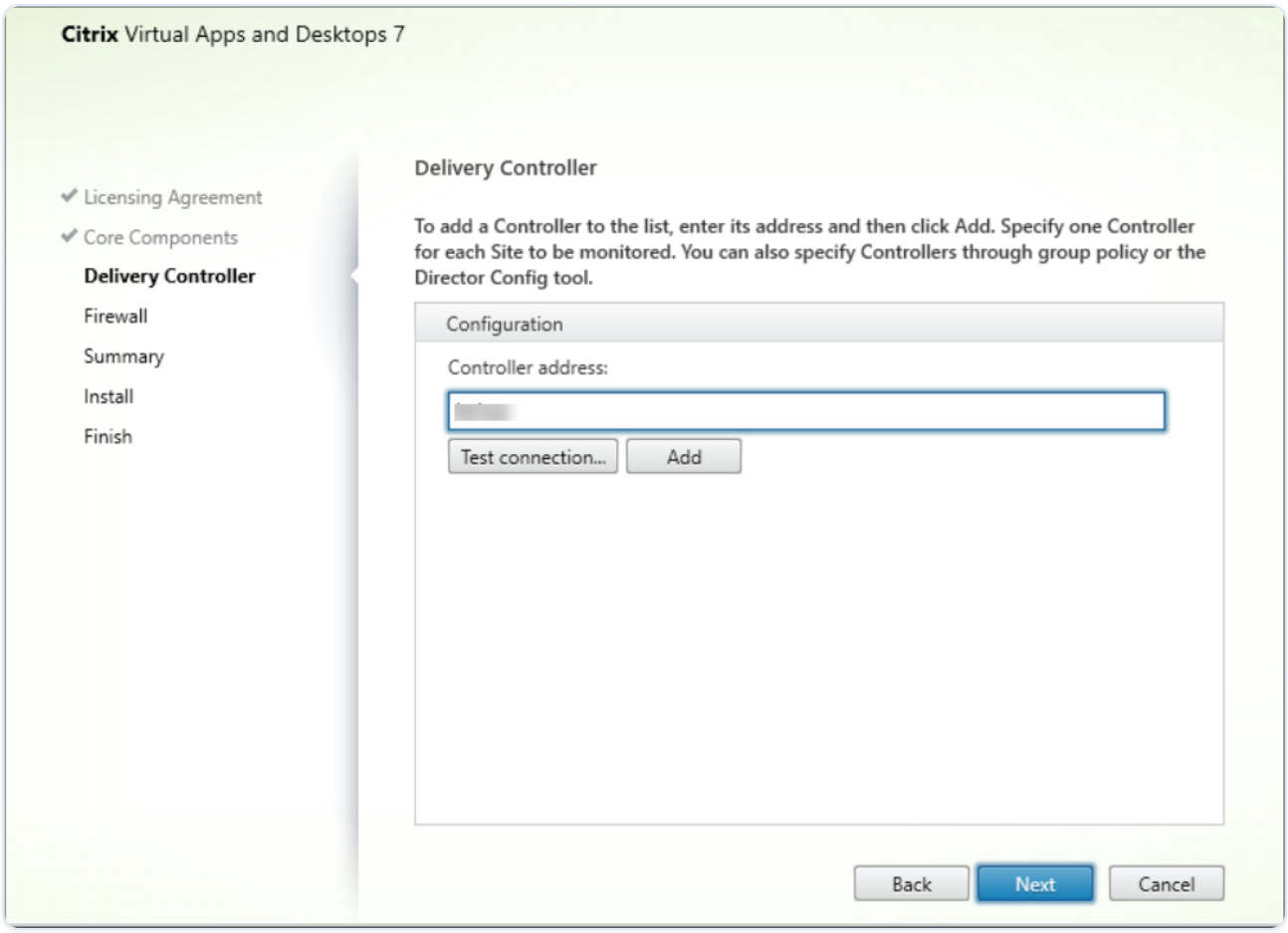
安装和配置

安装 Director

使用适用于 Citrix Virtual Apps and Desktops 的完整产品 ISO 安装程序安装 Director，该安装程序会检查必备条件、安装所有缺失的组件、设置 Director 网站并执行基本配置。有关必备条件和其他详细信息，请参阅此版本的系统要求文档。此版本的 Director 不兼容早于 6.5 的 Virtual Apps 部署或早于 7 的 Virtual Desktops 部署。 ISO 安装程序提供的默认配置可处理典型部署。如果安装期间

未包含 Director，请使用 ISO 安装程序添加 Director。要添加任何其他组件，请重新运行 ISO 安装程序并选择要安装的组件。有关使用 ISO 安装程序的信息，请参阅安装文档中的安装核心组件。Citrix 建议您仅使用完整产品 ISO 安装程序进行安装，而不要使用 .MSI 文件。

当 Director 安装在 Controller 上时，它会自动将 localhost 配置为服务器地址，并且 Director 默认与本地 Controller 通信。要将 Director 安装在远离 Controller 的专用服务器上，系统会提示您输入 Controller 的 FQDN 或 IP 地址。



注意：

单击**添加**以添加要监视的 Controller。

Director 默认与指定的 Controller 通信。为您监控的每个站点仅指定一个 Controller 地址。如果您指定的 Controller 出现故障，Director 会自动发现同一站点中的所有其他 Controller 并回退到这些其他 Controller。

注意：

> Director 不会在 Controller 之间进行负载平衡。

> 为保护浏览器与 Web 服务器之间的通信安全，Citrix® 建议您在托管 Director 的 IIS 网站上实施 TLS。有关说明，请参阅 Microsoft IIS 文档。启用 TLS 不需要 Director 配置。

部署和配置 Director

当 Director 用于包含多个站点的环境中时，请务必同步安装了 Controller、Director 和其他核心组件的所有服务器上的系统时钟。否则，这些站点可能无法在 Director 中正确显示。

> **重要提示：**

> 为保护通过网络以纯文本形式发送的用户名和密码的安全，请仅允许使用 HTTPS 连接 Director，而不要使用 HTTP。某些工具能够读取 HTTP（未加密）网络数据包中的纯文本用户名和密码，这可能会给用户带来潜在的安全风险。

配置权限

要登录 Director，具有 Director 权限的管理员必须是 Active Directory 域用户，并且必须具有以下权限：

- 在所有要搜索的 Active Directory 林中具有读取权限（请参阅高级配置）。
- 已配置的委派管理员角色（请参阅委派管理和 Director）。
- 要对用户进行影子操作，必须使用 Microsoft 组策略为 Windows 远程协助配置管理员。此外：
  - 安装 VDA 时，请确保在所有用户设备上启用 Windows 远程协助功能（默认选中）。
  - 在服务器上安装 Director 时，请确保已安装 Windows 远程协助（默认选中）。但是，它在服务器上默认是禁用的。Director 无需启用此功能即可向最终用户提供帮助。Citrix 建议禁用此功能以提高服务器安全性。
  - 要使管理员能够启动 Windows 远程协助，请使用适用于远程协助的相应 Microsoft 组策略设置授予他们所需的权限。有关信息，请参阅 CTX239706: 如何在最新 Director 版本中配置影子功能。

Citrix uberAgent® 与 Director 集成

Citrix uberAgent 现已默认包含在 Citrix Virtual Apps and Desktops™ 安装中，提供增强的监控功能并与 Citrix Director 无缝集成。管理员可以在 Virtual Delivery Agent 设置期间的**可选软件**屏幕上取消选择它，从而将其从安装中排除。

有关将 uberAgent 作为 Citrix Virtual Apps and Desktops 安装的一部分进行安装的更多信息，请参阅 uberAgent 文档。

主要功能：

本地应用程序使用情况监控：借助 Citrix uberAgent，您可以监控在虚拟桌面会话中启动的应用程序（也称为本地应用程序）的使用情况，并且通过 Director 集成，数据可直接在 Director 控制板上获取（需要白金版许可证）。

配置 Citrix uberAgent 与 Director 的集成

安装 Citrix uberAgent 后，在 Citrix Web Studio™ 中配置以下策略，以将 uberAgent 与 Director 完全集成和使用：

- **启用 uberAgent 数据收集策略**：启用后，uberAgent 提供应用程序使用情况和性能、系统运行状况、网络指标和安全分析的见解。此策略默认禁用。
- **使用 uberAgent 数据策略增强 Director**：此策略启用 Director 与 uberAgent 的集成。它允许 Director 处理 uberAgent 提供的数据，以增强监控功能，包括监控本地应用程序使用情况。此策略默认启用。

配置后，数据将在 Citrix Director 的 应用程序使用情况监控 部分中可用。

> **注意：**
>
> uberAgent 有关本地应用程序使用情况的数据至少需要一天才能在 Director 中聚合和显示。

高级配置

Director 可以支持跨林配置的多林环境，其中用户、交付控制器 (DC)、VDA 和 Director 位于不同的林中。这需要正确设置林之间的信任关系和配置设置。

多林环境中的推荐配置

推荐配置要求在林之间创建具有域范围身份验证的出站和入站林信任关系。

来自 Director 的信任关系使您能够排查位于不同林中的用户会话、VDA 和交付控制器中的问题。

Director 支持多林所需的高级配置通过在 Internet Information Services (IIS) 管理器中定义的设置进行控制。

> **重要提示：**

> 在 IIS 中更改设置时，Director 服务会自动重启并注销用户。

> 要使用 IIS 配置高级设置，请执行以下操作：

1. 打开 Internet Information Services (IIS) 管理器控制台。
2. 在默认网站下，转到 Director 网站。
3. 双击**应用程序设置**。
4. 双击某个设置以对其进行编辑。
5. 单击**添加**以添加新设置。

Director 使用 Active Directory 搜索用户并查找更多用户和计算机信息。默认情况下，Director 搜索以下域或林：

- 管理员帐户是成员。
- Director Web 服务器是成员（如果不同）。

Director 尝试使用 Active Directory 全局编录在林级别执行搜索。如果您没有在林级别搜索的权限，则只搜索域。

从其他 Active Directory 域或林搜索或查找数据需要您明确设置要搜索的域或林。在 IIS 管理器中，为 Director 网站配置以下应用程序设置：

```
Connector.ActiveDirectory.Domains = (user),(server)
```

值属性 user 和 server 分别表示 Director 用户（管理员）和 Director 服务器的域。

要启用从额外域或林进行的搜索，请将域的名称添加到列表中，如以下示例所示：

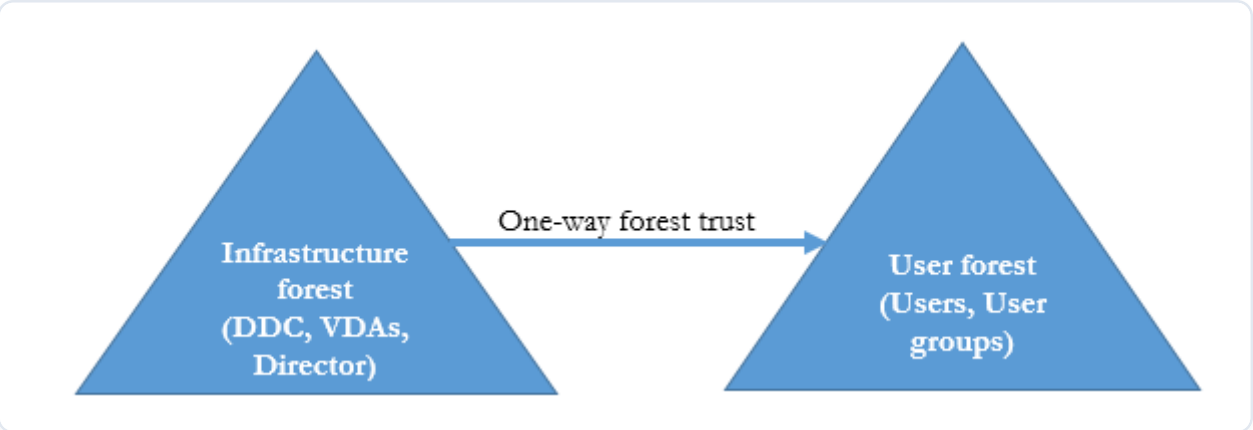
```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

对于列表中的每个域，Director 都会尝试在林级别执行搜索。如果您没有在林级别搜索的权限，则只搜索域。

域本地组配置

大多数 Citrix 服务提供商 (CSP) 具有类似的环境设置，包括基础结构林中的 VDA、DC 和 Director。用户或用户组记录属于客户林。从基础结构林到客户林存在单向出站信任。

CSP 管理员通常在基础结构林中创建域本地组，并将客户林中的用户或用户组添加到此域本地组中。



Director 可以支持此类多林设置，并监视使用域本地组配置的用户的会话。

1. 在 IIS 管理器中，将以下应用程序设置添加到 Director 网站：

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true



   DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
   ```

   \<domain1\>\<domain2\> 是域本地组所在的林的名称。

2. 在 Web Studio 中将域本地组分配给交付组。
3. 重新启动 IIS 并再次登录 Director，以使更改生效。现在，Director 可以监视并显示这些用户的会话。

向 Director 添加站点

如果 Director 已安装，请将其配置为与多个站点配合使用。要进行配置，请在每个 Director 服务器上使用 IIS 管理器控制台更新应用程序设置中的服务器地址列表。

将每个站点的 Controller 地址添加到以下设置中：

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAController 和 SiteBController 是来自两个不同站点的 Delivery Controller 的地址。

禁用活动管理器中正在运行的应用程序的可见性

默认情况下，Director 中的活动管理器会显示用户会话的所有正在运行的应用程序列表。所有有权访问 Director 中活动管理器功能的管理员都可以查看此信息。对于委派管理员角色，这包括完全管理员、交付组管理员和技术支持管理员。

为了保护用户及其正在运行的应用程序的隐私，您可以禁用**应用程序**选项卡以列出正在运行的应用程序。

> **警告：**
>
> 不正确地编辑注册表可能导致严重问题，可能需要重新安装操作系统。Citrix® 不保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。编辑注册表之前，请务必备份注册表。

1. 在 VDA 上，修改 `HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed` 处的注册表项。默认情况下，该项设置为 1。将值更改为 0，这意味着不会从 VDA 收集信息，因此不会在活动管理器中显示。
2. 在安装了 Director 的服务器上，修改控制正在运行的应用程序可见性的设置。默认情况下，该值为“true”，允许在“应用程序”选项卡中显示正在运行的应用程序。将值更改为“false”以禁用可见性。此选项仅影响 Director 中的活动管理器，而不影响 VDA。 修改以下设置的值：UI.TaskManager.EnableApplications = false

> **重要提示：**
>
> 要禁用正在运行的应用程序的视图，请同时进行这两项更改，以确保数据不会显示在活动管理器中。

配置 PIV 智能卡身份验证

本文列出了在 Director 服务器和 Active Directory 中启用智能卡身份验证功能所需的配置。

> **注意：**

> 智能卡身份验证仅支持来自同一 Active Directory 域的用户。

Director 服务器配置

在 Director 服务器上执行以下配置步骤：

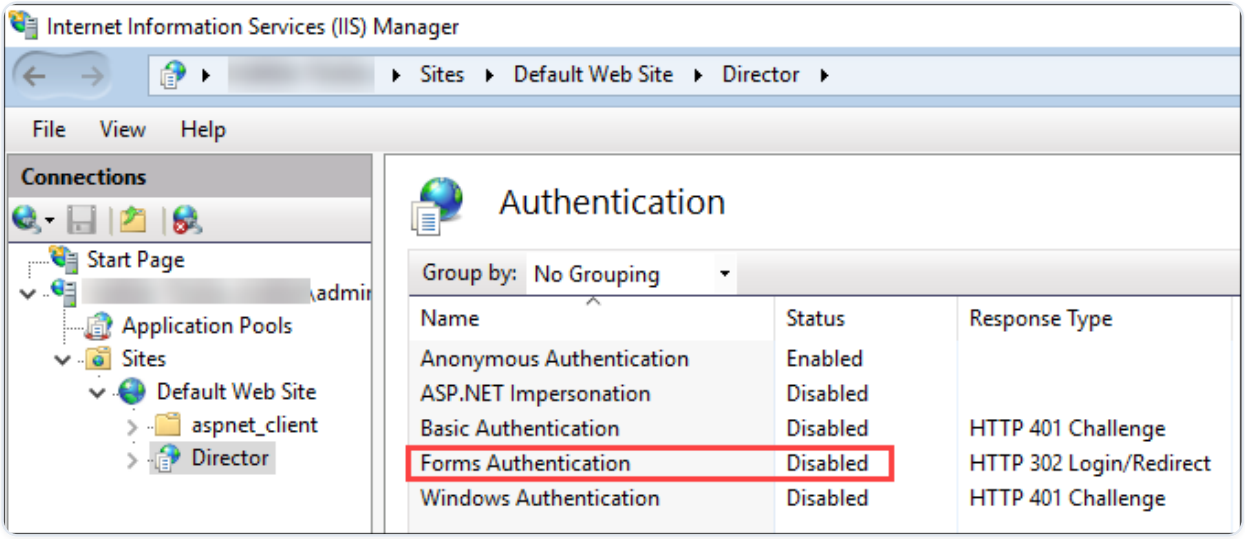
1. 安装并启用客户端证书映射身份验证。请遵循 Microsoft 文档 客户端证书映射身份验证 中的 **使用 Active Directory 进行客户端证书映射身份验证** 说明。
2. 在 Director 站点上禁用表单身份验证。

   启动 IIS 管理器。

   转到 **站点** \> **默认网站** \> **Director**。

   选择 **身份验证**。

   右键单击 **表单身份验证**，然后选择 **禁用**。



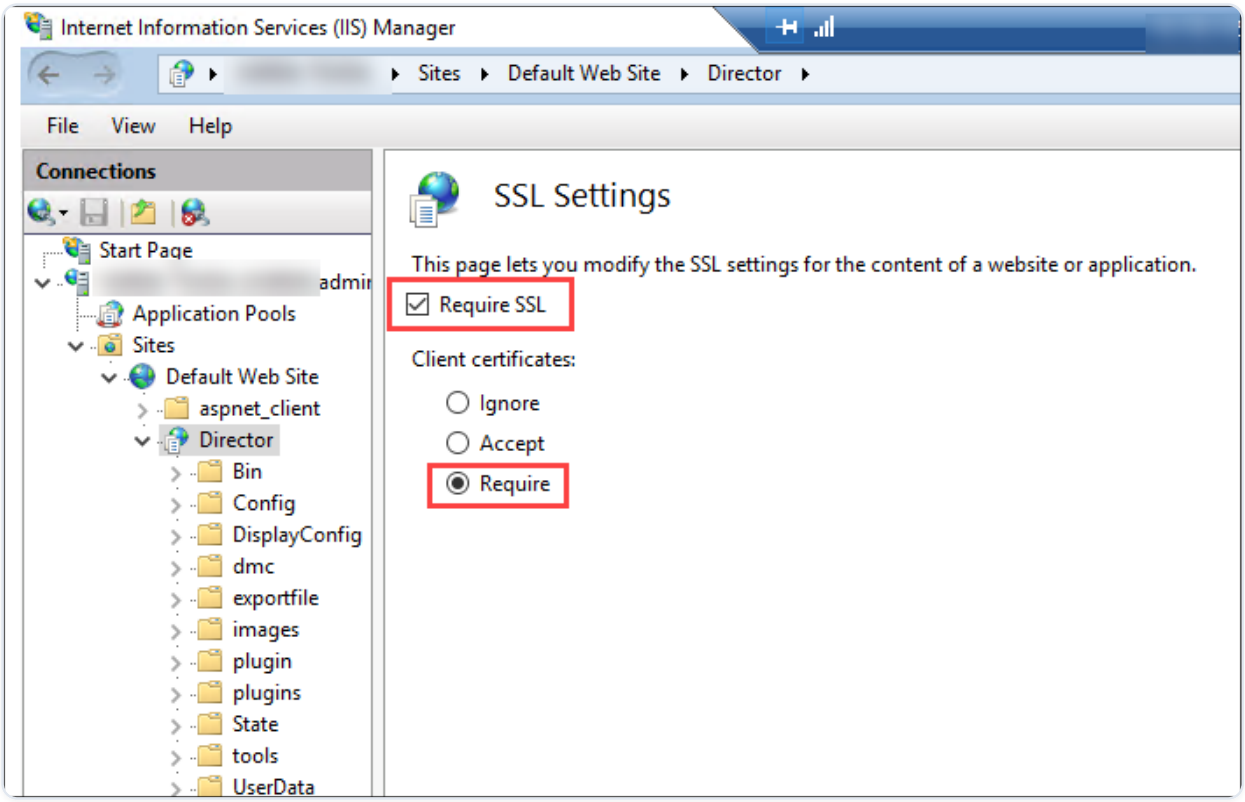
3. 为客户端证书身份验证配置 Director URL，使用更安全的 HTTPS 协议（而不是 HTTP）。

   a. 启动 IIS 管理器。

   b. 转到 **站点** \> **默认网站** \> **Director**。

   c. 选择 **SSL 设置**。

   d. 选择 **要求 SSL** 和 **客户端证书** \> **要求**。



4. 更新 web.config。使用文本编辑器打开 web.config 文件（位于 `c:\inetpub\wwwroot\Director` 中）。

在 `<system.webServer>` 父元素下，将以下代码片段添加为第一个子元素：

```
&lt;defaultDocument>

   &lt;files>

       &lt;add value="LogOn.aspx"/>

   &lt;/files>

&lt;/defaultDocument>
```

活动目录配置

默认情况下，Director 应用程序使用 **应用程序池** 标识属性运行。智能卡身份验证需要委派，为此，Director 应用程序标识必须在服务主机上具有可信计算基 (TCB) 权限。

Citrix 建议您为应用程序池标识创建单独的服务帐户。根据 Microsoft MSDN 文章 Protocol Transition with Constrained Delegation Technical Supplement 中的说明创建服务帐户并分配 TCB 权限。

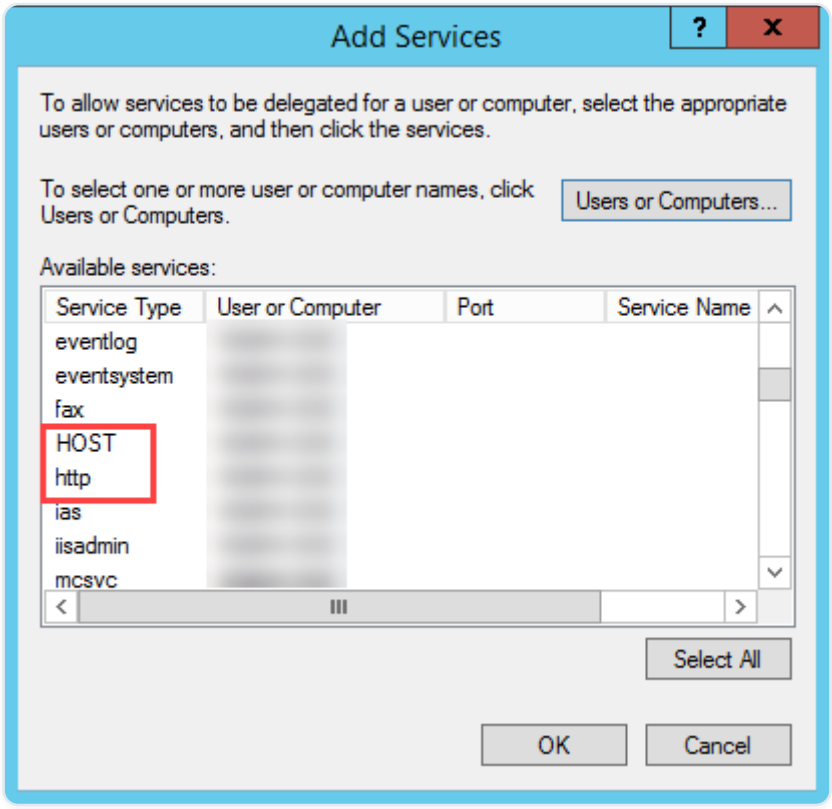
将新创建的服务帐户分配给 Director 应用程序池。下图显示了示例服务帐户“Domain Pool”的属性对话框。

为此帐户配置以下服务：

- 交付控制器™: HOST, HTTP
- 控制台：HOST, HTTP
- 活动目录：GC, LDAP

要配置，

1. 在用户帐户属性对话框中，单击“**添加**”。
2. 在“**添加服务**”对话框中，单击“用户”或“计算机”。
3. 选择 Delivery Controller 主机名。
4. 从“**可用服务**”列表中，选择 HOST 和 HTTP **服务类型**。



同样，为 **Director** 和 **Active Directory** 主机添加服务类型。

创建服务主体名称记录

您必须为每个 Director 服务器以及用于访问 Director 服务器池的负载均衡虚拟 IP (VIP) 创建一个服务帐户。您必须创建服务主体名称 (SPN) 记录，以配置对新创建的服务帐户的委派。

- 使用以下命令为 Director 服务器创建 SPN 记录：

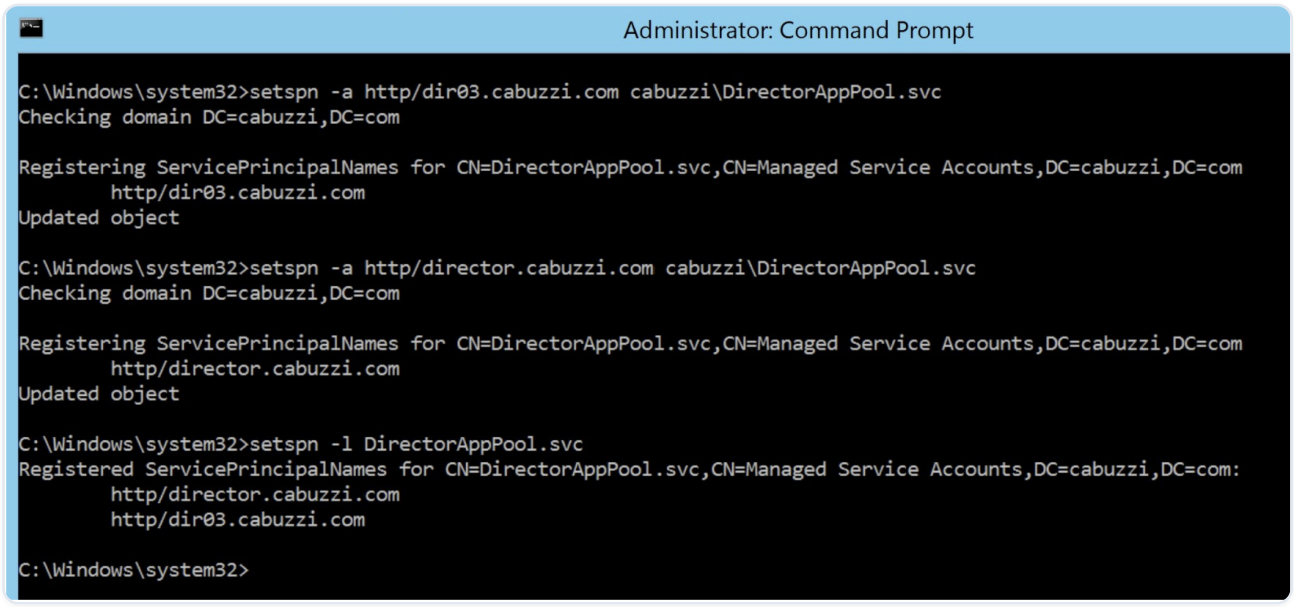
```
setspn -a http/<directorServer>.<domain_fqdn>
<domain>\<DirectorAppPoolServiceAcct>
```

- 使用以下命令为负载均衡 VIP 创建 SPN 记录：

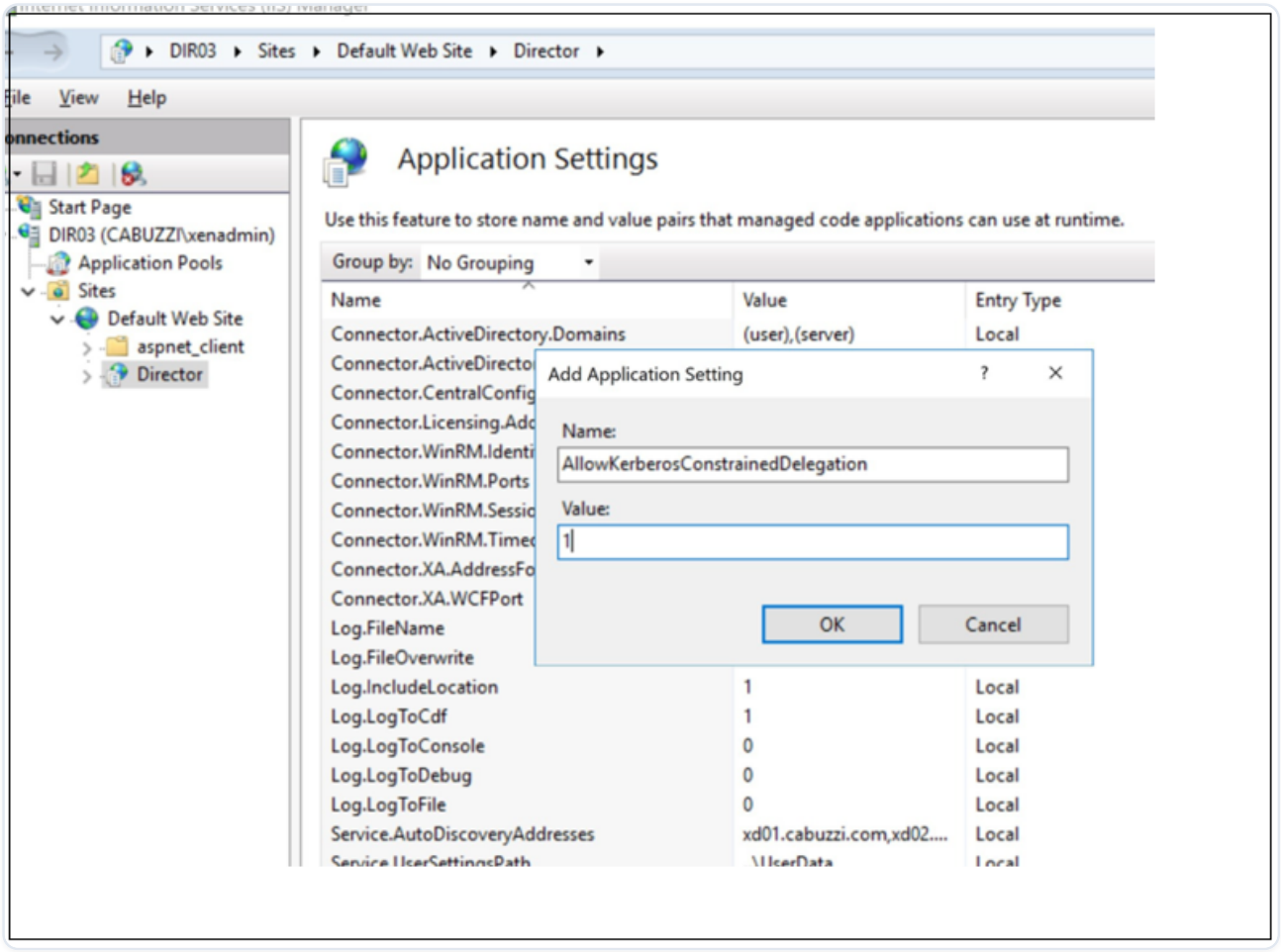
```
setspn -S http/<DirectorFQDN> <domain>\<DirectorAppPoolServiceAcct>
```

- 使用以下命令查看或测试创建的 SPN：

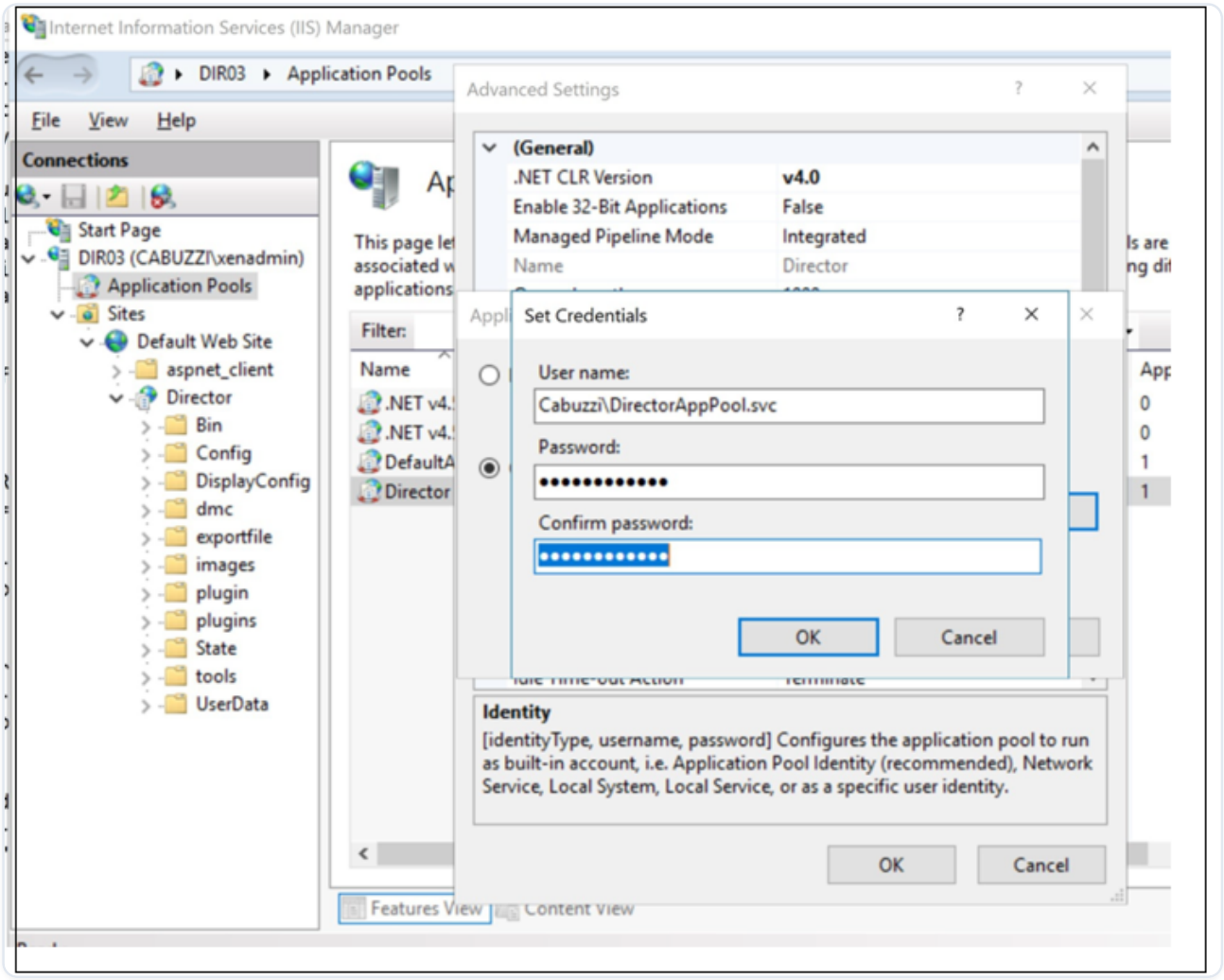
```
setspn –l <DirectorAppPoolServiceAcct>
```



- 在左侧窗格中选择 Director 虚拟目录，然后双击“**应用程序设置**”。在“应用程序设置”窗口中，单击“**添加**”并确保 **AllowKerberosConstrainedDelegation** 设置为 1。



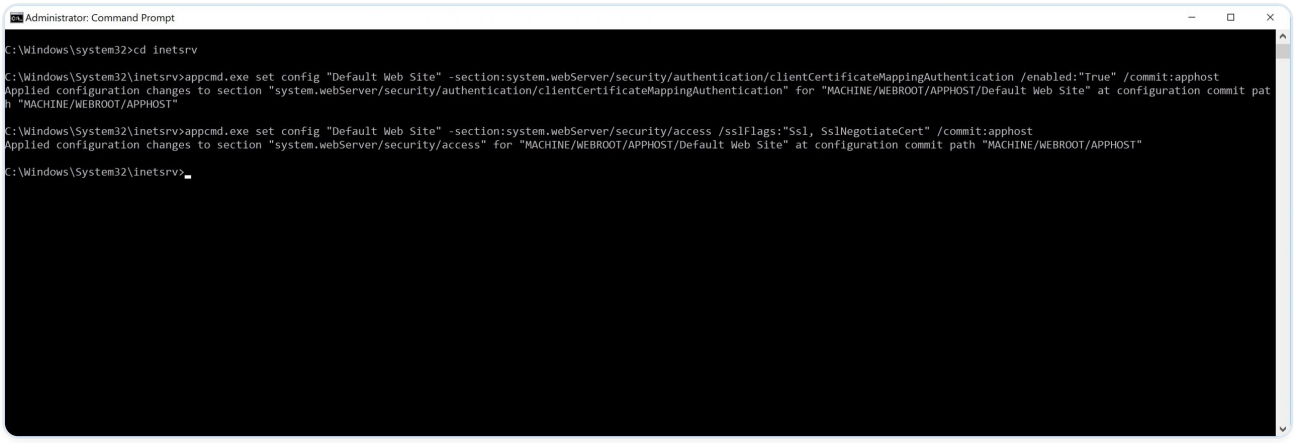
- 在左侧窗格中选择“**应用程序池**”，然后右键单击 Director 应用程序池并选择“**高级设置**”。
- 选择 **Identity**，单击省略号 (“…”) 以输入服务帐户域\登录名和密码凭据。关闭 IIS 控制台。



- 从提升的命令提示符，将目录更改为 C:\Windows\System32\inetsrv 并输入以下命令：

```
   appcmd.exe set config “Default Web Site” -section:system.webServer/
security/authentication/clientCertificateMappingAuthentication /
enabled:”True” /commit:apphost
```

```
    appcmd.exe set config “Default Web Site” -section:system.webServer/
security/access /sslFlags:”Ssl, SslNegotiateCert” /commit:apphost
```



Firefox 浏览器配置

要使用 Firefox 浏览器，请安装以下位置提供的 PIV 驱动程序：OpenSC 0.17.0。有关安装和配置说明，请参阅在 Firefox 中逐步安装 OpenSC PKCS#11 模块。 有关 Director 中智能卡身份验证功能的使用信息，请参阅 Director 文章中的将 Director 与基于 PIV 的智能卡身份验证结合使用部分。

配置网络分析

> **注意：**

> 此功能的可用性取决于您的组织许可证和管理员权限。

> Director 与 Citrix ADM 集成，以提供网络分析和性能管理：

- 网络分析使用 Citrix ADM 中的 HDX™ Insight 报告来提供网络的应用程序和桌面上下文视图。借助此功能，Director 可提供部署中 ICA 流量的高级分析。
- 性能管理提供历史数据保留和趋势报告。通过数据历史保留与实时评估，您可以创建趋势报告，包括容量和运行状况趋势。

在 Director 中启用此功能后，HDX Insight 报告会为 Director 提供更多信息：

- “趋势”页面中的“网络”选项卡显示整个部署中应用程序、桌面和用户的延迟和带宽影响。
- “用户详细信息”页面显示特定用户会话的延迟和带宽信息。

限制：

- 在“趋势”视图中，不收集早于 7 的 VDA 的 HDX 连接登录数据。对于较早的 VDA，图表数据显示为 0。

要启用网络分析，必须在 Director 中安装和配置 Citrix ADM。Director 需要 Citrix ADM 版本 11.1 Build 49.16 或更高版本。MAS 是在 XenServer 上运行的虚拟设备。通过网络分析，Director 可以通信并收集与您的部署相关的信息。

有关详细信息，请参阅 Citrix ADM 文档。

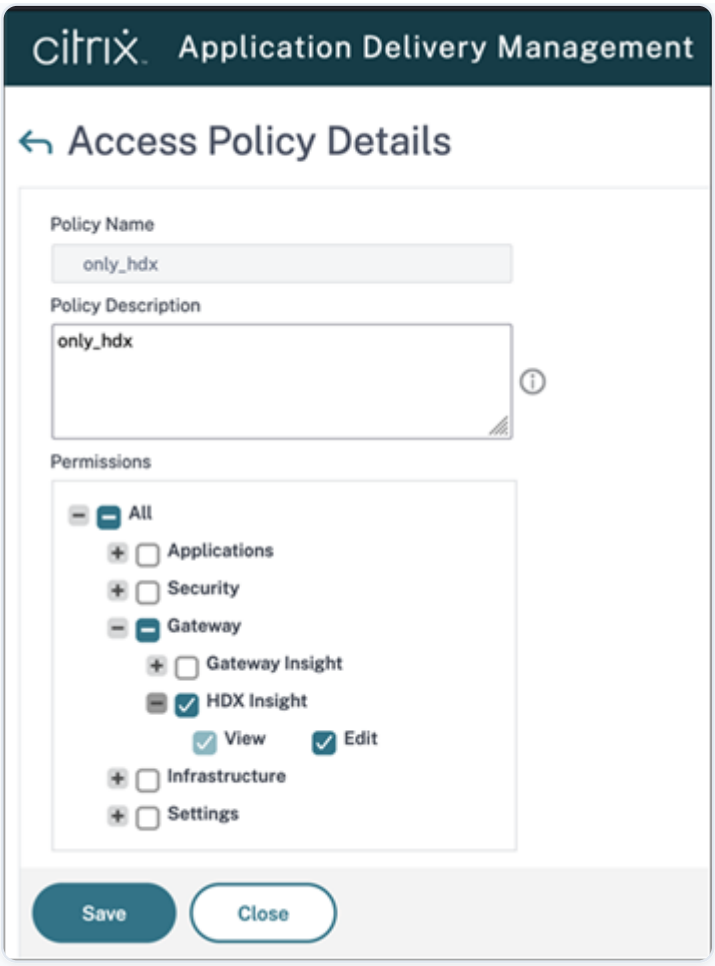
注意：

Citrix NetScaler Insight Center 已于 15 May 2018 达到其维护终止日期。请参阅 Citrix 产品矩阵。将 Director 与 Citrix ADM 集成以进行网络分析。要将 NetScaler Insight Center 迁移到 Citrix ADM，请参阅 从 NetScaler Insight Center 迁移到 Citrix ADM。

1. 在安装 Director 的服务器上，在 `C:\inetpub\wwwroot\Director\tools` 中找到 DirectorConfig 命令行工具，然后从命令提示符处使用参数 /configNetscaler 运行它。
2. 出现提示时，输入 Citrix ADM 计算机名称（FQDN 或 IP 地址）、用户名、密码、HTTPS 连接类型（优先于 HTTP），然后选择 Citrix ADM 集成。
3. 要验证更改，请注销并重新登录。

注意：

出于安全原因，建议为 ADM 与 Director 的集成创建一个自定义角色，该角色仅具有访问 HDX Insight 的足够权限。



有关详细信息，请参阅配置访问策略。

委派管理和 Director

委派管理使用三个概念：管理员、角色和作用域。权限基于管理员的角色和该角色的作用域。例如，管理员可能被分配了帮助台管理员角色，其作用域仅涉及一个站点的最终用户。

有关创建委派管理员的信息，请参阅主要委派管理 文章。

管理权限决定了向管理员呈现的 Director 界面以及他们可以执行的任务。权限决定：

- 管理员可以访问的视图，统称为一个视图。
- 管理员可以查看和交互的桌面、计算机和会话。
- 管理员可以执行的命令，例如影子跟进用户会话或启用维护模式。

内置角色和权限还决定了管理员如何使用 Director：

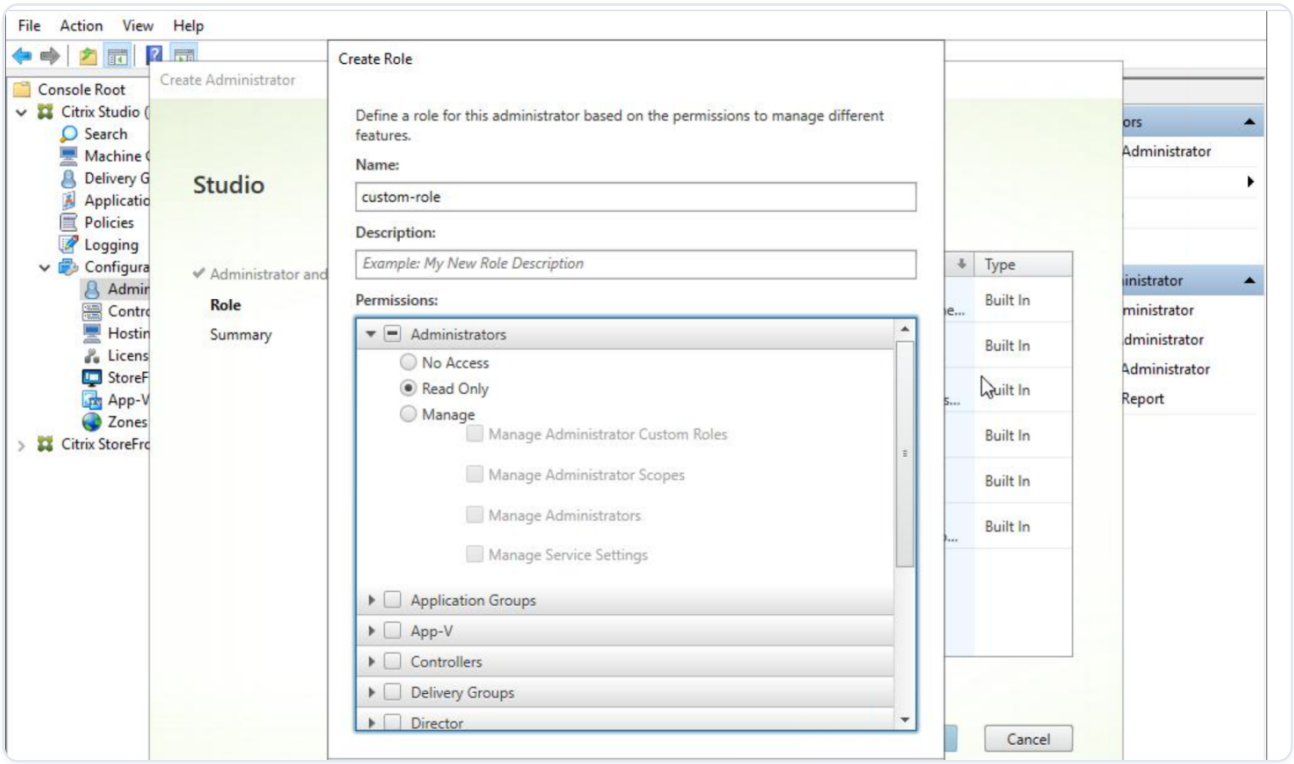
管理员角色	DIRECTOR 中的权限
完全管理员	完全访问所有视图，并可以执行所有命令，包括影子跟进用户会话、启用维护模式和导出趋势数据。
交付组管理员	完全访问所有视图并可以执行所有命令，包括影子用户会话、电源管理和会话管理、启用维护模式以及导出趋势数据。
只读管理员	可以访问所有视图并查看指定范围内的所有对象和全局信息。可以从 HDX™ 通道下载报告，并可以使用“趋势”视图中的“导出”选项导出趋势数据。无法执行任何其他命令或更改视图中的任何内容。
帮助台管理员	只能访问“帮助台”和“用户详细信息”视图，并且只能查看管理员被委派管理的对象。可以影子用户会话并为该用户执行命令。可以执行维护模式操作。可以对单会话操作系统计算机使用电源控制选项。无法访问“控制板”、“趋势”、“警报”或“筛选器”视图。无法对多会话操作系统计算机使用电源控制选项。
计算机目录管理员	只能访问“计算机详细信息”页面（基于计算机的搜索）。
主机管理员	无权访问。Director 不支持此管理员，也无法查看数据。

为 Director 管理员配置自定义角色

在 Studio 中，您还可以配置 Director 专用的自定义角色，以更密切地匹配您的组织要求并更灵活地委派权限。例如，您可以限制内置的帮助台管理员角色，使该管理员无法注销会话。

如果您创建具有 Director 权限的自定义角色，则还必须为该角色授予其他通用权限：

- Delivery Controller™ 登录 Director 的权限 - 至少在管理员节点中具有只读访问权限
- 交付组权限，用于在 Director 中查看与这些交付组相关的数据 - 至少只读访问权限

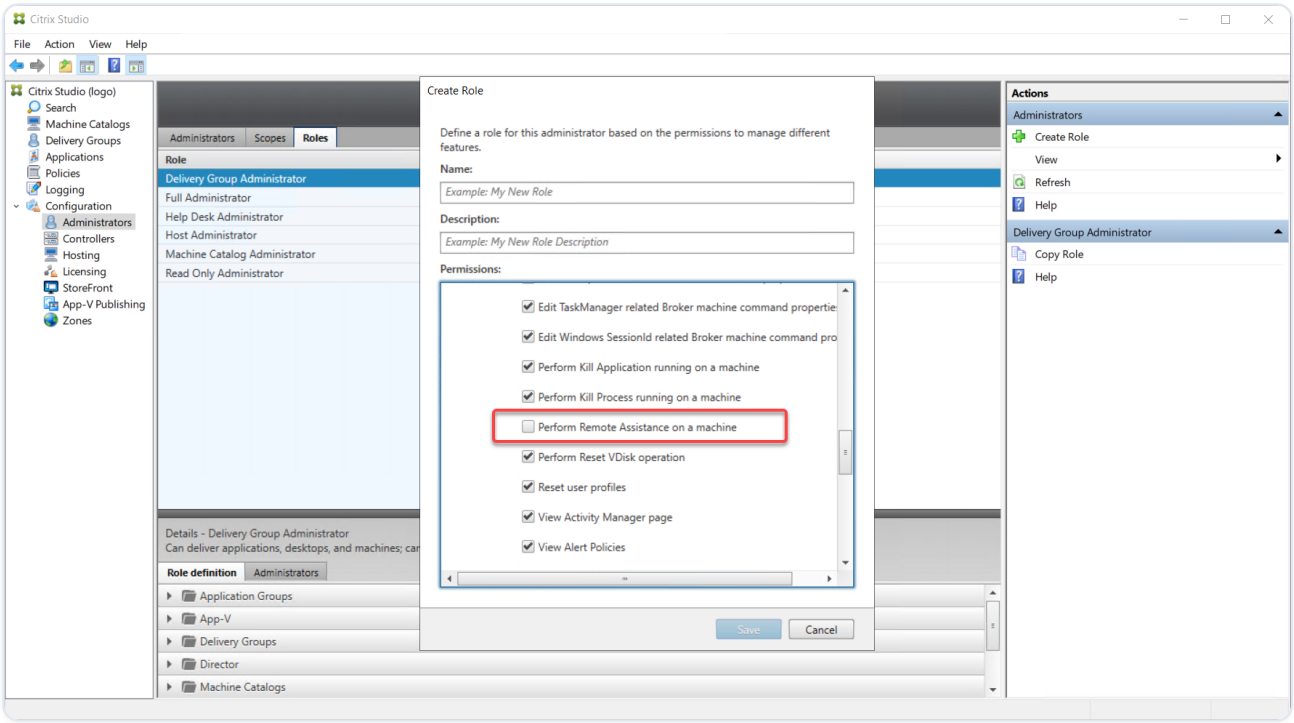


此外，您还可以通过复制现有角色并为不同视图添加额外权限来创建自定义角色。例如，您可以复制“帮助台”角色并添加查看“控制板”或“筛选器”页面的权限。

选择自定义角色的 Director 权限，其中包括：

- 执行终止在计算机上运行的应用程序
- 执行终止在计算机上运行的进程
- 执行对计算机的远程协助
- 重置用户配置文件
- 查看客户端详细信息页面
- 查看仪表板页面
- 查看筛选器页面
- 查看计算机详细信息页面
- 查看趋势页面
- 查看用户详细信息页面

在此示例中，影子会话（执行对计算机的远程协助）已关闭。



某个权限可能依赖于其他权限才能在 UI 上适用。例如，选择“**执行终止在计算机上运行的应用程序**”权限仅在角色具有权限的那些面板中启用“**结束应用程序**”功能。您可以选择以下面板权限：

- 查看筛选器页面
- 查看用户详细信息页面
- 查看计算机详细信息页面
- 查看客户端详细信息页面

此外，从其他组件的权限列表中，请考虑交付组的以下权限：

- 使用交付组成员身份启用/禁用计算机的维护模式。
- 使用交付组成员身份对 Windows 桌面计算机执行电源操作。
- 使用交付组成员身份对计算机执行会话管理。

保护 Director 部署

本文重点介绍在部署和配置 Director 时可能影响系统安全的方面。

Director 通信

在生产环境中，使用 HTTPS 协议保护 Director 与服务器之间传输的数据。HTTPS 使用传输层安全 (TLS) 协议提供强大的数据加密。

> **注意：**

- Citrix® 强烈建议您将 Director 控制台的访问权限限制在内部网络中。
- Citrix 强烈建议您不要在生产环境中启用对 Director 的不安全连接。
- 使用 TLS 1.2 或更高版本。请勿使用旧版 TLS 或 SSL。

要保护用户 Web 浏览器与 Director 之间的通信，请参阅 在 Web Studio 和 Director 上启用 TLS

要保护 Director 与 Citrix Virtual Apps and Desktops 服务器之间的通信（用于监视和报告），请参阅保护本地 Monitor OData API 访问。

要保护 Director 与 Citrix ADC 之间的通信（用于 Citrix Insight），当您 配置网络分析 时，请选择 HTTPS 连接类型。

配置 微软互联网信息服务 (IIS)

您可以使用受限的 IIS 配置来配置 Director。

应用程序池回收限制

Director 使用名为 **Director** 的应用程序池。您可以为该应用程序池设置以下应用程序池回收限制：

- 虚拟内存限制：4,294,967,295
- 私有内存限制：StoreFront™ 服务器的物理内存大小
- 请求限制：4,000,000,000

文件名扩展名

在安装过程中，Director 配置请求筛选以仅允许以下扩展名：

- .
- .aspx 文件
- .css 文件
- .eot 文件
- .html 文件
- .ico 文件
- .js
- .png 文件
- .服务

- .svg 文件
- .gif 文件
- 点json
- 点woff
- 点woff2
- 点ttf

HTTP 谓词

在安装过程中，Director 会配置请求筛选以仅允许以下谓词：

- GET
- POST
- HEAD

IIS 功能

Director 不需要以下 IIS 组件：

- ISAPI 扩展
- CGI 程序
- FastCGI 程序

您可以删除这些组件。

.NET 信任级别

Director 要求将 **.NET 信任级别**设置为**完全信任**。请勿将 .NET 信任级别设置为任何其他值。

配置用户权限

安装 Director 后，其应用程序池将获得以下权限：

- **作为服务登录**的登录权限
- **调整进程的内存配额、生成安全审核**和**替换进程级别令牌**的权限

上述权限和特权是创建应用程序池时的正常安装行为。

您无需更改这些用户权限。Director 不使用这些特权，并且它们会自动禁用。

Director 安全隔离

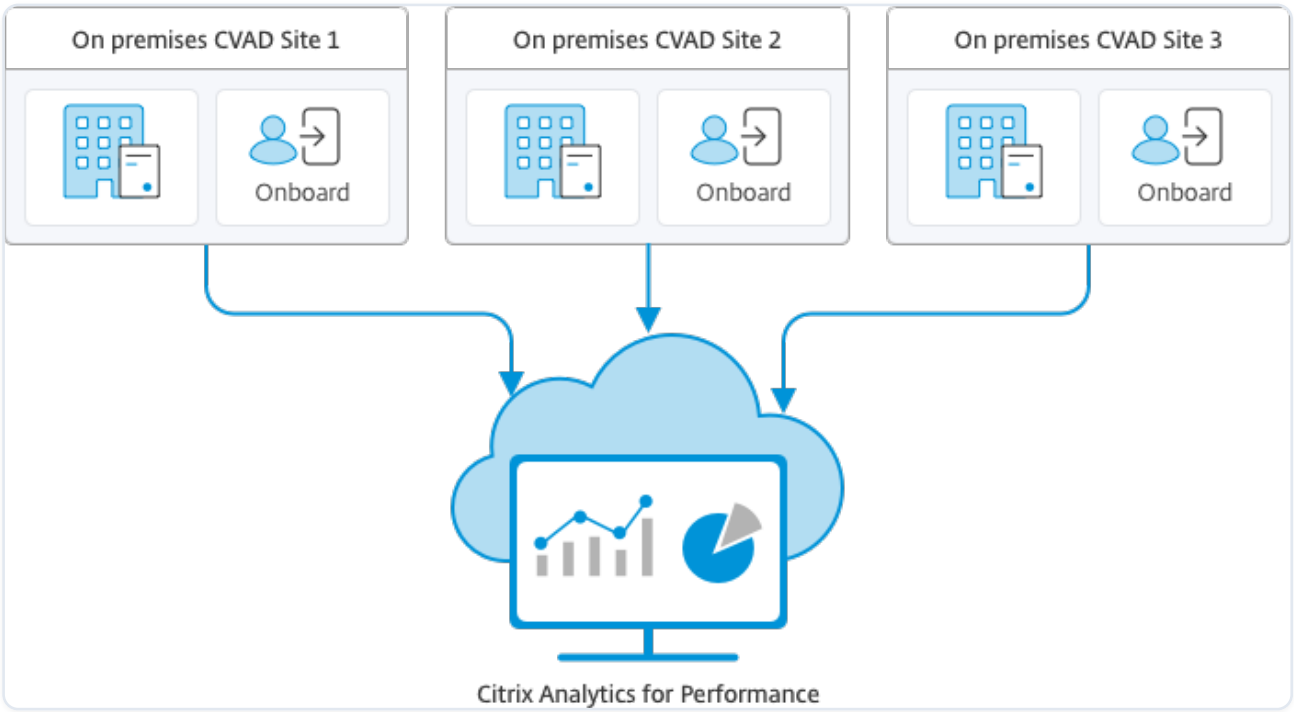
您可以在与 Director 相同的 Web 域（域名和端口）中部署任何 Web 应用程序。但是，这些 Web 应用程序中的任何安全风险都可能降低 Director 部署的安全性。如果需要更高程度的安全隔离，Citrix 建议您将 Director 部署在单独的 Web 域中。

使用 Citrix Analytics for Performance™ 配置本地站点

Citrix Analytics for Performance（性能分析）是 Citrix Analytics Cloud Service 提供的综合性能监控解决方案。性能分析提供基于性能指标的高级洞察和分析。性能分析可帮助您监控和查看组织中一个或多个 Citrix Virtual Apps and Desktops™ 站点的使用情况和性能指标。

有关性能分析的更多信息，请参阅性能分析文章。

您可以将站点的性能数据发送到 Citrix Cloud™ 上的 Citrix Analytics for Performance，以利用其高级性能分析功能。要查看和使用性能分析，您必须首先在 **Director** 的“**分析**”选项卡中，使用 Citrix Analytics for Performance 配置本地站点。



性能分析以安全的方式访问数据，并且不会将任何数据从 Citrix Cloud 传输到本地环境。

先决条件

要从 Director 配置 Citrix Analytics for Performance，无需安装任何新组件。请确保满足以下要求：

- 您的 Delivery Controller 和 Director 版本为 1912 CU2 或更高版本。有关详细信息，请参阅功能兼容性矩阵。

注意：

- 如果 Delivery Controller 运行的 Microsoft .NET Framework 版本低于 4.8，则使用 Director 中的 Citrix Analytics for Performance 配置本地站点可能会失败。作为一种解决方法，请将 Delivery Controller 中的 .NET Framework 升级到版本 4.8。LCM-9255。
- 当您使用 Director 中的 Citrix Analytics for Performance 配置运行 Citrix Virtual Apps and Desktops 2012 版的本地站点时，配置可能会在几个小时后或在 Delivery Controller 中重新启动 Citrix Monitor Service 后失败。“分析”选项卡在这种情况下会显示“未连接”状态。作为一种解决方法，请在 Delivery Controller 的注册表中创建一个 Encryption 文件夹，位置：HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor，文件夹名称：Encryption。确保 CitrixMonitor 帐户对 Encryption 文件夹具有完全控制访问权限。重新启动 Citrix Monitor Service。DIR-14324。

- 只有完全管理员才能访问“**分析**”选项卡以执行此配置。
- 为了让性能分析访问性能指标，所有 Delivery Controller 以及安装了 Director 的计算机都必须具有出站 Internet 访问权限。具体而言，请确保可以访问以下 URL：
  - Citrix 密钥注册：`https://*.citrixnetworkapi.net/`
  - 思杰云：`https://*.citrixworkspacesapi.net/`
  - 思杰分析：`https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` 如果交付控制器和 Director 计算机位于内网中，并且出站互联网访问通过代理服务器，请确保以下事项：
- 代理服务器必须允许上述 URL 列表。
- 在 Director web.config 和 citrix.monitor.exe.config 文件中添加以下配置。请确保将此配置添加到 **configuration** 标签内：

```
&lt;system.net>

    &lt;defaultProxy>

        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>
```

```
&lt;/system.net>
```

- Director web.config 位于安装 Director 的计算机上的 `C:\inetpub\wwwroot\Director\web.config`。
- citrix.monitor.exe.config 位于安装交付控制器的计算机上的 `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config`。

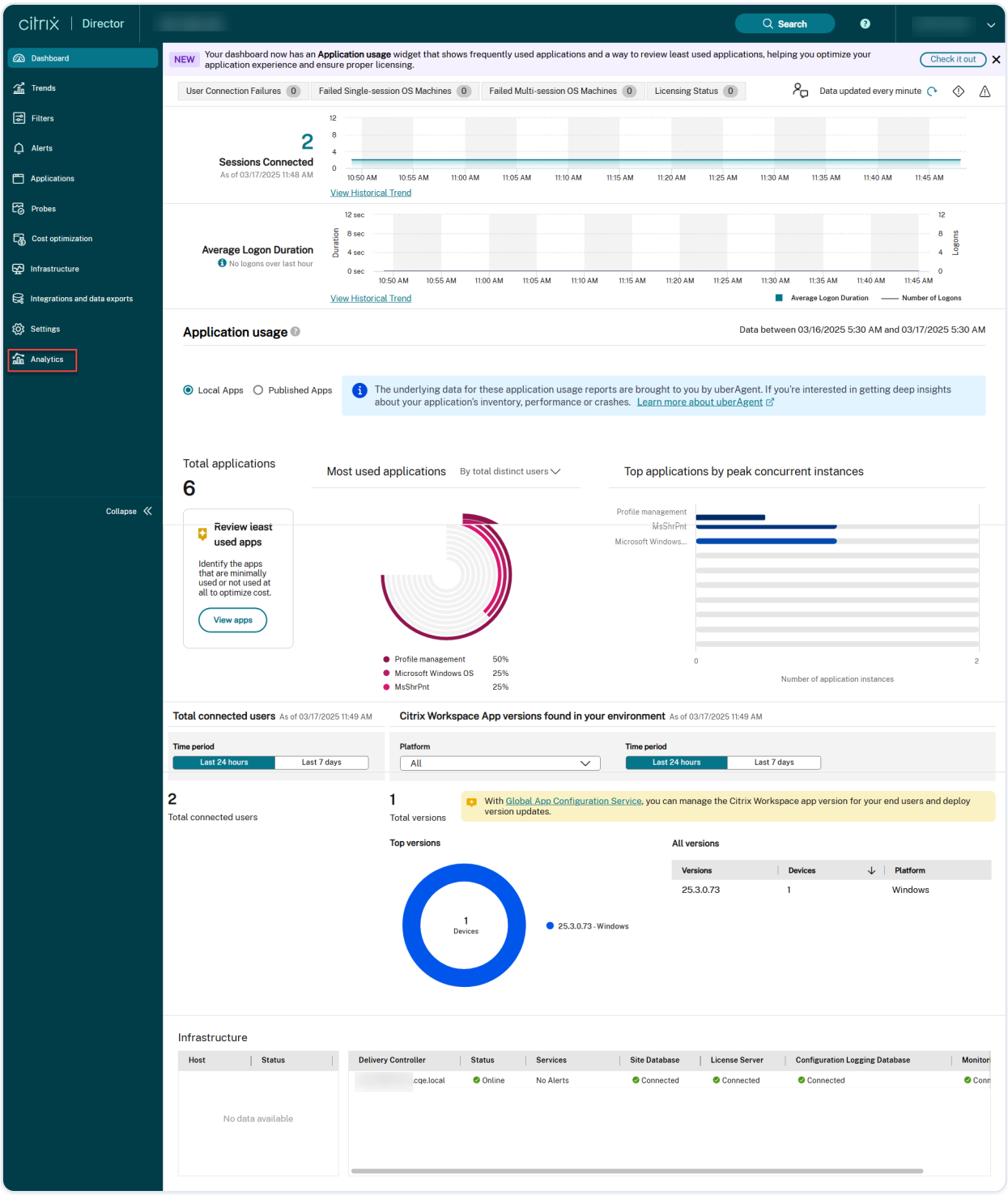
此设置由 Microsoft 在 IIS 上提供。有关详细信息，请参阅 `https://docs.microsoft.com/zh-cn/dotnet/framework/network-programming/proxy-configuration`。 配置文件中的 **defaultproxy** 字段控制 Director 和 Monitor Service 的出站访问。与 Performance Analytics 的配置和通信要求将 **defaultproxy** 字段设置为 **true**。生效的策略可能会将此字段设置为 false。在这种情况下，您必须手动将该字段设置为 true。在进行更改之前，请备份配置文件。重新启动 Delivery Controller™ 上的 Monitoring 服务以使更改生效。

- 您拥有 Citrix Analytics for Performance 的有效 Citrix Cloud 授权。
- 您的 Citrix Cloud 帐户是具有产品注册体验权限的管理员帐户。有关管理员权限的详细信息，请参阅修改管理员权限。

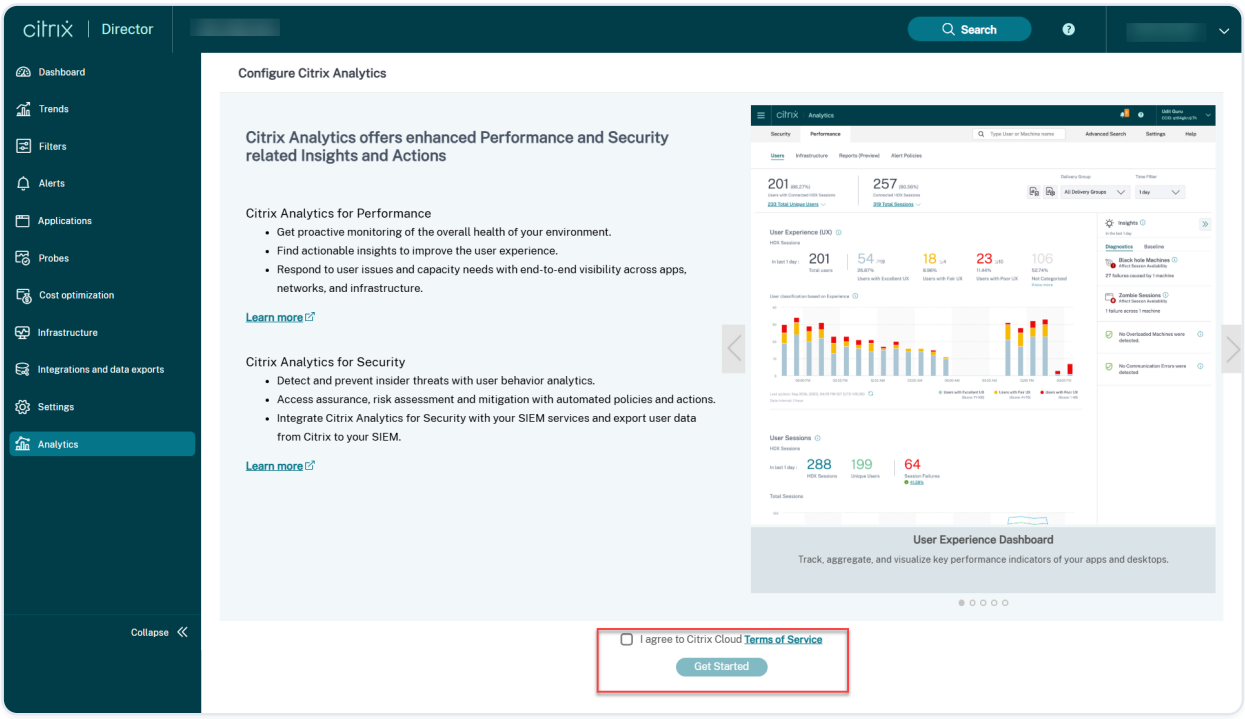
配置步骤

验证先决条件后，请执行以下操作：

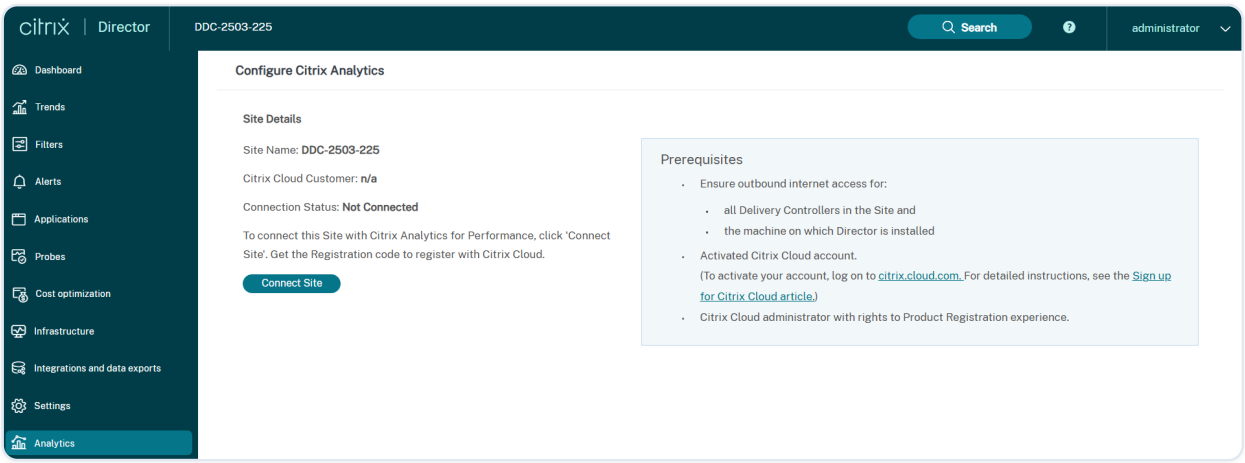
1. 以完全管理员身份登录 Director，然后选择要使用 Performance Analytics 配置的站点。Director 仪表板页面随即显示。



2. 单击“**Analytics**”选项卡。“**配置 Citrix Analytics**”页面随即显示。



3. 查看步骤，选择服务条款，然后单击“**开始使用**”。“**站点详细信息**”页面随即显示。



4. 查看先决条件并确保满足这些条件。查看站点详细信息。
5. 单击“**连接站点**”以开始配置过程。

   将生成一个唯一的 8 位注册码，用于将此站点注册到 Citrix Cloud。

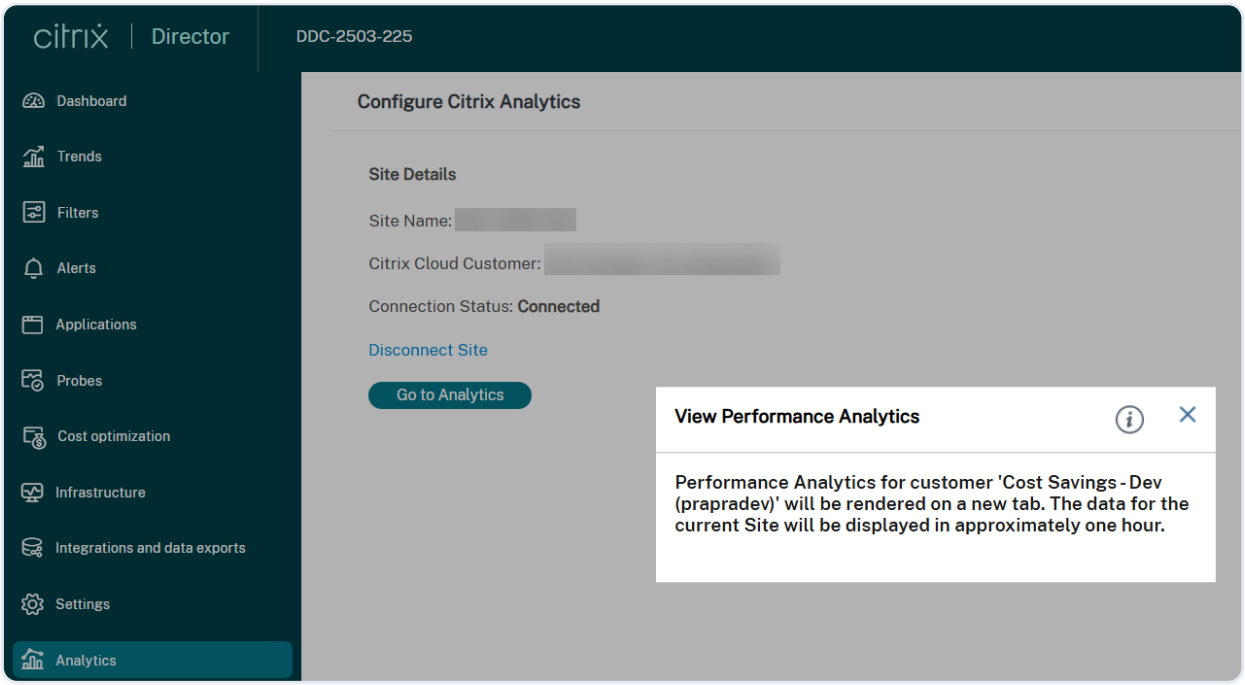
   

6. 单击**复制代码**以复制代码，然后单击**在 Citrix Cloud 上注册**。您将被重定向到 Citrix Cloud 中的注册 URL。
7. 使用您的 Citrix Cloud 凭据登录并选择您的客户。
8. 在 Citrix Cloud 的“产品注册”页面中粘贴复制的注册码。单击“**继续**”进行注册。查看注册详细信息，然后单击“**注册**”。

您的本地站点注册到 Citrix Cloud。

9. 在 **Director** 中，单击“**Analytics**”选项卡上的“**转到 Analytics**”。



Performance Analytics 在浏览器的新选项卡中打开。

如果您的 Citrix Cloud 会话已过期，您可能会被重定向到 Citrix.com 或 My Citrix 帐户登录页面。

10. 要向 Performance Analytics 注册多个站点，请对 Director 中的每个站点重复前面的配置步骤。所有已配置站点的指标都显示在 Performance Analytics 控制板上。

    如果每个站点运行多个 Director 实例，请从任意一个 Director 实例进行配置。连接到该站点的所有其他 Director 实例将在配置过程后的下一次刷新时更新。

11. 要将您的站点与 Citrix Cloud 断开连接，请单击“**断开站点连接**”。此选项将删除现有配置。

> **注意：**
>
> 首次配置站点时，来自站点的事件可能需要一些时间（大约一小时）才能处理；这会导致 Performance Analytics 控制板上指标的显示延迟。此后，事件会定期刷新。
>
> 断开连接后，旧帐户的数据传输会持续一段时间，直到新帐户的事件传输完毕。数据传输停止后大约一小时内，与旧帐户相关的分析仍显示在 Performance Analytics 控制板上。
>
> Citrix Analytics 服务授权到期后，最多需要一天时间才能停止向 Performance Analytics 发送站点指标。

Director 独立版本，适用于 LTSR 部署

Director 独立版本现已适用于 LTSR 部署，它提供了一个选项，可在 Citrix® 环境中访问最新的 Director 功能，以增强对兼容 LTSR 环境的故障排除和监视。此功能允许您在 2402 LTSR 部署上使用最新的 Director 版本。此外，它还提供对 LTSR 发布后发布的功能的访问，而不会影响应用程序交付基础结构。

独立安装程序包含 Monitor 服务、Director 服务和 Monitor 管理单元的最新 .msi。使用这些新的 .msi 文件，您可以使用当前版本功能升级 2402 LTSR CU1。

有关 2402 LTSR 版本之后当前版本中包含的 Director 功能的信息，请参阅以下内容：

- Citrix 虚拟应用和桌面 2407 版本
- Citrix 虚拟应用和桌面 2411 版本

要了解有关 Director 特定功能以及 VDA 最低版本的更多信息，请参阅 Director 版本矩阵。

优势

- **访问新功能**：访问 2402 LTSR 发布后发布的 Director 功能，包括 Citrix Virtual Apps and Desktops™ 2407 和 2411 累积版本 (CR) 中的功能。
- **有针对性的升级**：仅升级 Director 和监视服务组件，而不会影响 LTSR 基础结构的其他部分。
- **LTSR 兼容性**：在维护 LTSR 环境的同时，受益于最新的 Director 增强功能。
- **回滚选项**：如果需要，您可以灵活地回滚到以前的 Director 版本。

主要注意事项

升级后的 Director 组件与 LTSR 兼容，但不在 LTSR 核心组件支持范围内。但是，LTSR 基础结构的其他部分保留其现有支持。

先决条件

1. 从 Citrix 下载 页面下载 `Director2411.zip` 文件。
2. 解压缩安装程序文件，可以找到以下安装程序：
    - DesktopDirector.msi
    - Monitor_PowerShellSnapIn.msi
    - Monitor_Service_x64.msi
3. 确保您使用的是 Citrix Virtual Apps and Desktops™ 2402 LTSR 或 2402 LTSR CU1 站点。

高级概述

要将 Citrix Virtual Apps and Desktops 2402 LTSR CU1 站点升级到最新版本的最新功能，请按照以下步骤操作：

1. **备份数据库**：在升级之前，请务必备份监控数据库。此过程至关重要，因为升级过程也会更新数据库。
2. **升级您的站点**：继续升级您的站点，以整合当前版本的新功能。
3. **回滚选项**：如果您决定不继续使用升级后的站点，可以使用回滚步骤恢复到以前的站点。

升级步骤

1. 备份监控数据库。
2. 从 Citrix 下载 页面下载 `Director2411.zip` 文件。
3. 解压缩安装程序文件，可以找到以下安装程序：
   - DesktopDirector.msi
   - Monitor_PowerShellSnapIn.msi
   - Monitor_Service_x64.msi
4. 导航到 .msi 文件所在的位置。
5. 使用命令行安装 Monitor 服务：

   ```
   msiexec /i Monitor_service_x64 REINSTALLMODE=amus /l*v <logfile path and name>
   ```

6. 按照屏幕上的说明完成向导。
7. 使用命令行安装 Director 服务：

   ```
   msiexec /i DesktopDirector /l*v <logfile path and name>
   ```

8. 按照屏幕上的说明完成向导。
9. 使用命令行运行以下命令。

   ```
   DirectorConfig.exe /UPGRADE
   ```

10. 使用命令行安装 Monitor 管理单元

```
msiexec /i Monitor_PowershellSnapin_x64.msi
```

11. 所有 .msi 安装完成后，导航到 Program Files 中的 Monitor 服务并运行命令：

```
Citrix.Monitor.exe /upgrade /enablefeatures
```

12. 打开 Citrix Site Manager 并选择 **Automatic Site Upgrade** 选项，然后完成升级工作流。
13. 登录 Director 以验证新功能是否可用。

回滚步骤

1. 确保备份监控数据库。
2. 下载并运行名为 dbollback.zip 的数据库回滚脚本。
3. 从控制面板卸载以下内容：
   - 选择 **Citrix Monitor Service PowerShell Snap-in- x64** 并单击 **卸载**。
   - 选择 **Citrix Monitor Service - x64** 并单击 **卸载**。
   - 选择 **Citrix Director** 并单击 **卸载**。
4. 从您已有的备份中恢复监控数据库。有关详细信息，请参阅知识共享文章 CTX135207。
5. 使用 Citrix Virtual Apps and Desktops 安装程序重新安装 Delivery Controller 和 Director。有关详细信息，请参阅 install core components

   或者，

您还可以使用以下命令重新安装组件：

```
XenDesktopServerSetup.exe /components controller,director /
configure_firewall /quiet
```

1. 安装完成后，选中“**打开 Citrix Site Manager**”复选框。
2. 执行站点升级（如果 Citrix Site Manager 中有建议）。

支持和合规性

支持

- Director 的累积版本 (CR) 与 LTSR 兼容，但不符合 LTSR 规范。
- 升级后，所有所需的支持票证和错误修复都将添加到 Director 的以下累积版本 (CR) 中。

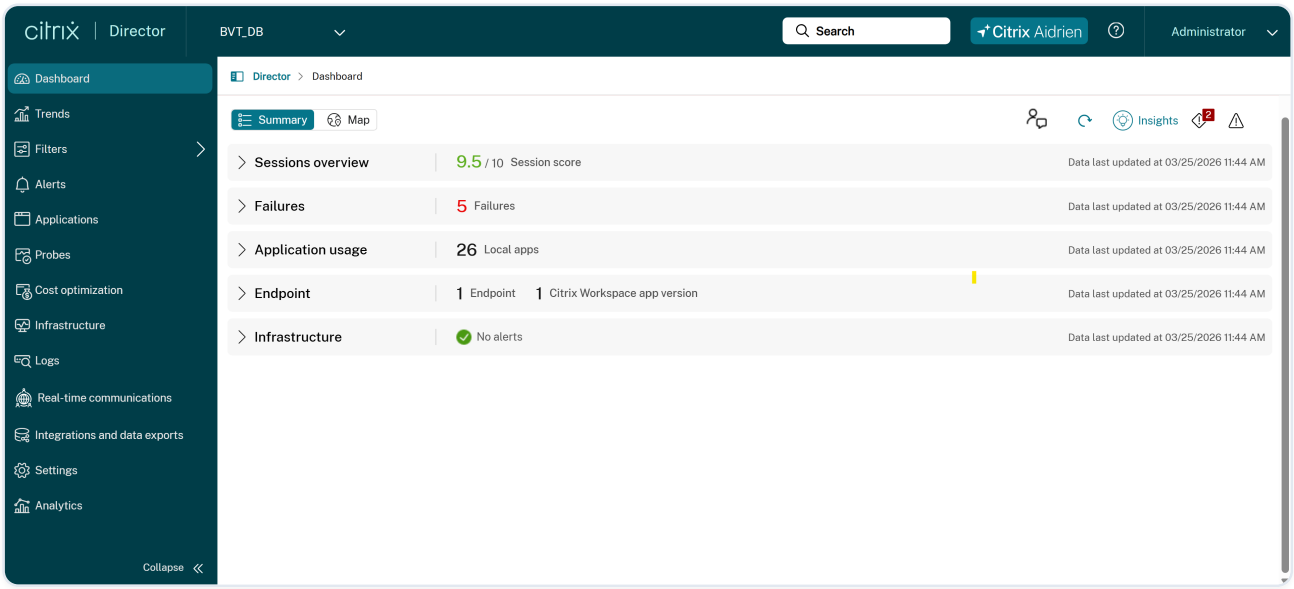
- 包含更改或修复的 CR 将在以下累积更新 (CU) 中提供。

508/WCAG 2.1

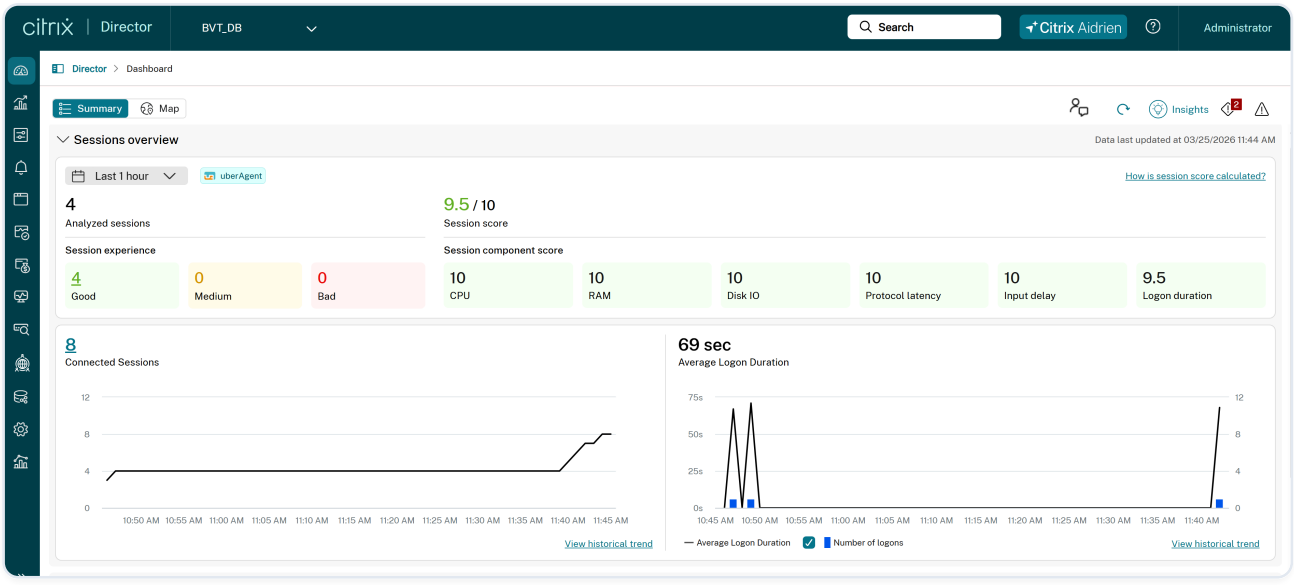
- 对于有 508/WCAG 2.1 合规性要求的客户，建议继续使用所有核心组件的 LTSR 版本。

站点分析

使用 Director，您可以监控部署的运行状况。您可以通过在所有已加入的站点中搜索用户、端点或计算机来排查性能问题。



在拥有完整管理员权限的情况下，当您打开 Director 时，仪表板提供了一个集中位置来监控站点的运行状况和使用情况。



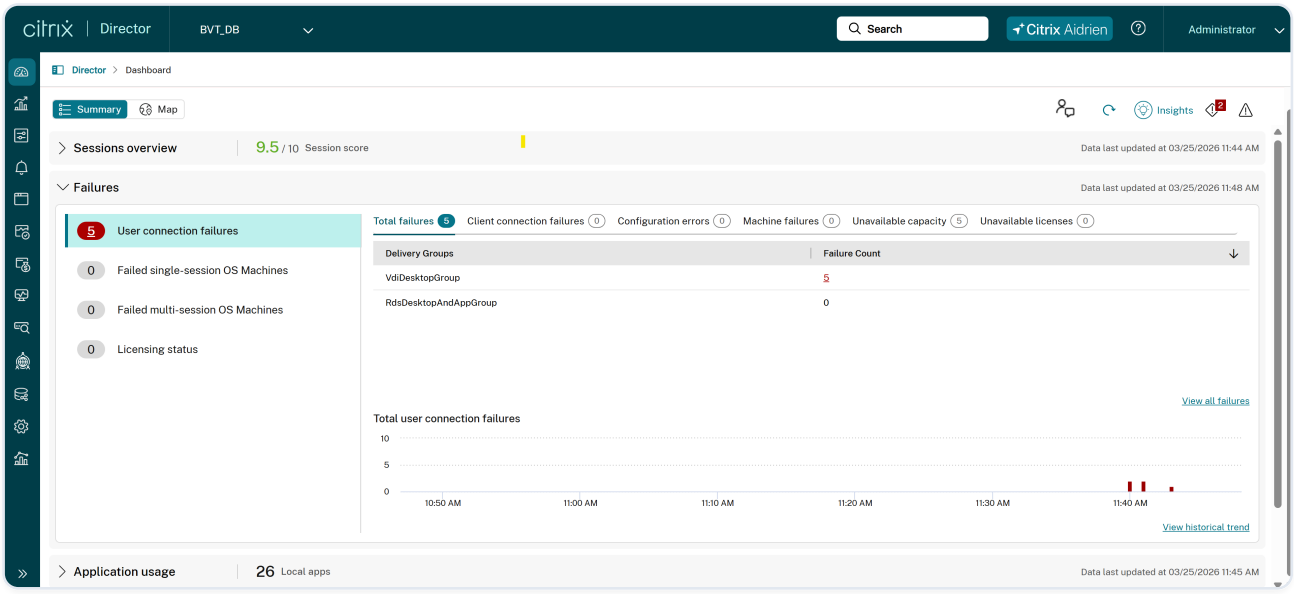
如果当前没有故障，并且在过去 60 分钟内没有发生故障，则面板将保持折叠状态。当出现故障时，特定的故障面板会自动显示。

> **注意：**
>
> 根据您组织的许可证和您的管理员权限，某些选项或功能可能不可用。

Director 仪表板上的面板

用户连接故障

过去 60 分钟内的连接故障。单击总数旁边的类别以查看该类型故障的指标。在相邻的表中，该数字按交付组细分。连接故障包括因达到应用程序限制而导致的故障。有关应用程序限制的更多信息，请参阅应用程序。



失败的单会话操作系统计算机或失败的多会话操作系统计算机

过去 60 分钟内的总故障，按交付组细分。故障按类型细分，包括启动失败、启动卡住和未注册。对于多会话操作系统计算机，故障还包括达到最大负载的计算机。

许可状态

许可证服务器警报显示许可证服务器发送的警报以及解决警报所需的操作。需要许可证服务器版本 11.12.1 或更高版本。交付控制器警报显示控制器所见的许可状态详细信息，并由控制器发送。需要 XenApp 7.6 或 XenDesktop 7.6 或更高版本的控制器。您可以在 Studio 中设置警报阈值。在 **Delivery Controllers** > **Details** > **Product Editions** > **PLT** 中显示的许可状态表示 **Premium** 而不是 **Platinum**。

宽限状态

Director 显示以下宽限状态之一。此信息从交付控制器获取。

1. **未激活：** 未处于任何类型的许可证缓存模式。适用正常的许可限制。
2. **紧急宽限期：** 在许可证服务器无法访问或在代理连接时无法获取许可证信息时生效。用户不受影响。Director 中显示的错误在许可证服务器可访问之前无法消除。
3. **宽限期已过期：** 紧急许可证缓存模式已过期。

有关详细信息，请参阅许可证透支和许可证突发模式。

已连接会话

过去 60 分钟内所有交付组的已连接会话。

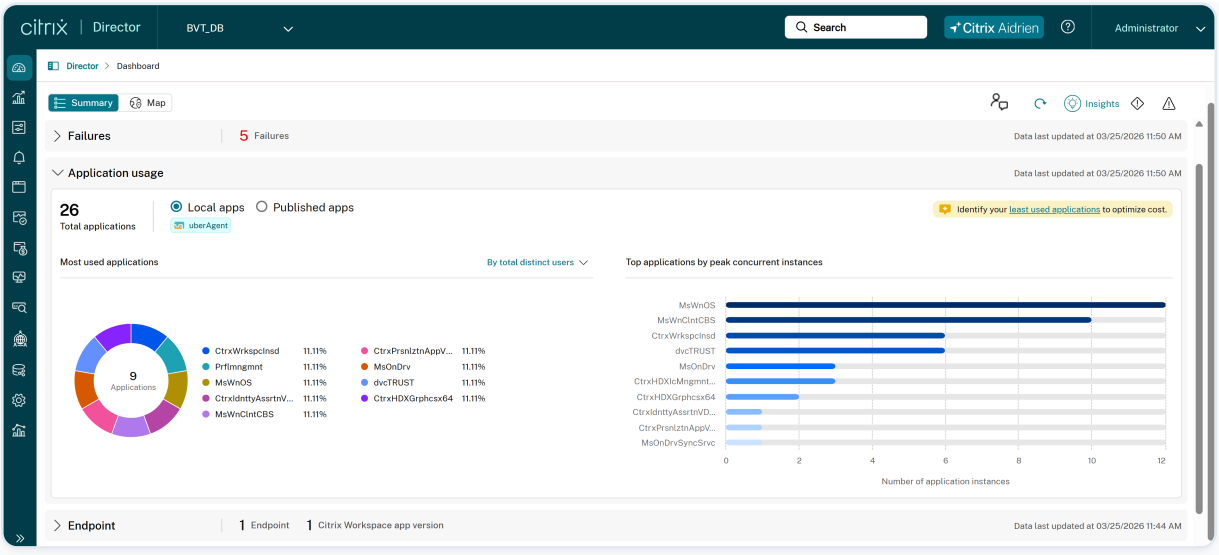
平均登录持续时间

过去 60 分钟的登录数据。左侧的大数字是该小时内的平均登录持续时间。早于 XenDesktop 7.0 的 VDA 的登录数据不包含在此平均值中。有关详细信息，请参阅诊断用户登录问题。

基础结构

列出站点的基础结构 - 主机和控制器。对于来自 XenServer 或 VMware 的基础结构，您可以查看性能警报。例如，您可以配置 XenCenter 以在托管服务器或虚拟机上的 CPU、网络 I/O 或磁盘 I/O 使用率超过指定阈值时生成性能警报。默认情况下，警报重复间隔为 60 分钟，但您也可以配置此项。有关详细信息，请参阅XenServer 产品文档中的 XenCenter 性能警报部分。

> **注意：**
>
> 如果特定指标没有显示图标，则表示您使用的主机类型不支持此指标。例如，System Center Virtual Machine Manager (SCVMM) 主机、AWS 和 CloudStack 不提供运行状况信息。



继续使用以下选项（在以下各节中进行了说明）排查问题：

- 控制用户计算机电源
- 阻止连接到计算机

已连接用户总数

显示在过去 24 小时或 7 天内至少进行过一次连接的用户数量。此面板可帮助管理员向其高管展示采用趋势。

在您的环境中找到的 Citrix Workspace™ 应用程序版本

概述了整个组织中使用的 Citrix Workspace 应用程序版本。它通过显示有多少设备正在使用不同版本来帮助统一版本。默认情况下，将显示所有操作系统平台的 Citrix Workspace 应用程序版本数据。您可以通过从“**平台”下拉列表**中选择相应的操作系统来查看特定操作系统平台的版本数据。

监视会话

如果会话断开连接，它仍然处于活动状态，其应用程序会继续运行，但用户设备不再与服务器通信。

操作	描述
查看用户当前连接的计算机或会话	在“活动管理器”和“用户详细信息”视图中，查看用户当前连接的计算机或会话以及该用户有权访问的所有计算机和会话的列表。要访问此列表，请单击用户标题栏中的会话切换器图标。有关详细信息，请参阅恢复会话。
查看所有交付组中连接会话的总数	在仪表板的“**已连接会话**”窗格中，查看过去 60 分钟内所有交付组的已连接会话总数。然后单击大的总数，这将打开“筛选器”视图，您可以在其中根据选定的交付组和范围以及跨交付组的使用情况显示图形会话数据。
结束空闲会话	“会话筛选器”视图显示与所有活动会话相关的数据。根据关联用户、交付组、会话状态和大于阈值时间段的空闲时间筛选会话。从筛选列表中，选择要注销或断开连接的会话。有关详细信息，请参阅排查应用程序问题。
查看更长时间段的数据	在“趋势”视图中，选择“**会话**”选项卡以深入查看更长时间段内（即早于过去 60 分钟的会话总数）已连接和已断开连接会话的更具体使用数据。要查看此信息，请单击“**查看历史趋势**”。

注意：

如果用户设备运行的是旧版 Virtual Delivery Agent (VDA)，例如版本 7 之前的 VDA 或 Linux VDA，Director 无法显示有关会话的完整信息。相反，它会显示一条消息，指出信息不可用。

桌面分配规则限制： Web Studio 允许将多个桌面分配规则 (DAR) 分配给交付组中不同用户或用户组的单个 VDA。StoreFront™ 会根据登录用户的 DAR 显示分配的桌面以及相应的**显示名称**。但是，Director 不支持 DAR，并且无论登录用户是谁，都使用交付组名称显示分配的桌面。因此，您无法在 Director 中将特定桌面映射到计算机。 您可以使用以下 PowerShell 命令将 StoreFront 中显示的分配桌面映射到 Director 中显示的交付组名称：

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq
"\&lt;Name on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property
Name, Uid
```

会话传输协议

在“**会话详细信息**”面板中查看当前会话的 HDX 连接类型所使用的传输协议。此信息适用于在 VDA 7.13 或更高版本上启动的会话。

- 对于 **HDX™** 连接类型，
  - 如果 HDX 连接使用 EDT，则协议显示为 **UDP**。
  - 如果 HDX 连接使用 TCP，则协议显示为 **TCP**。
- 对于 **RDP** 连接类型，协议显示为 **n/a**。

配置自适应传输后，会话传输协议会根据网络状况在 EDT（通过 UDP）和 TCP 之间动态切换。如果无法使用 EDT 建立 HDX 会话，则会回退到 TCP 协议。

有关自适应传输配置的更多信息，请参阅自适应传输。

导出报告

您可以导出趋势数据以生成常规使用情况和容量管理报告。导出支持 PDF、Excel 和 CSV 报告格式。PDF 和 Excel 格式的报告包含以图表和表格形式表示的趋势。CSV 格式的报告包含可用于生成视图或存档的表格数据。

要导出报告：

1. 转到“**趋势**”选项卡。
2. 设置筛选条件和时间段，然后单击“**应用**”。趋势图和表格将填充数据。
3. 单击**导出**并输入报告的名称和格式。

Director 根据您选择的筛选条件生成报告。如果更改筛选条件，请在单击**导出**之前单击**应用**。

> **注意：**
>
> 导出大量数据会导致 Director 服务器、交付控制器和 SQL 服务器上的内存和 CPU 消耗显著增加。为实现最佳导出性能，支持的并发导出操作数量和可导出的数据量已设置为默认限制。

支持的导出限制

导出的 PDF 和 Excel 报告包含所选筛选条件的完整图表。但是，所有报告格式中的表格数据都会在超出表中行数或记录数的默认限制后被截断。支持的默认记录数是根据报告格式定义的。

您可以通过在 Internet Information Services (IIS) 中配置 Director 应用程序设置来更改默认限制。

报告格式	默认支持的记录数	DIRECTOR 应用程序设置中的字段	支持的最大记录数
PDF	500	UI.ExportPdfDrilldownLimit	5000
艾赛尔	100,000	UI.ExportExcelDrilldownLimit	100,000
CSV	100,000（在**会话**选项卡中为 10,000,000）	UI.ExportCsvDrilldownLimit	100,000

要更改可导出记录数的限制：

1. 打开 IIS 管理器控制台。
2. 在默认网站下，转到 Director 网站。
3. 双击“**应用程序设置**”。
4. 根据需要编辑或添加字段 UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit 或 UI.ExportCsvDrilldownLimit 的设置。

在“应用程序设置”中添加这些字段值会覆盖默认值。

> **警告：**
>
> 将字段值设置为大于支持的最大记录数可能会影响导出性能，并且不受支持。

错误处理

本节提供有关处理在导出操作期间可能遇到的错误的信息。

- “**Director 已超时**”

此错误可能是由于网络问题或 Director 服务器或 Monitor Service 上的资源使用率过高造成的。

默认超时持续时间为 100 秒。要增加 Director Service 的超时持续时间，请在 Internet Information Services (IIS) 的 Director 应用程序设置中设置 **Connector.DataServiceContext.Timeout 字段**的值：

1. 打开 IIS 管理器控制台。
2. 导航到默认网站下的 Director 网站。
3. 双击**应用程序设置**。
4. 编辑值 **Connector.DataServiceContext.Timeout**。

- “**Monitor 已超时**”

此错误可能是由于网络问题、Monitor Service 资源使用率过高或 SQL 服务器资源使用率过高导致的。

要增加 Monitor Service 的超时持续时间，请在 Delivery Controller 上运行以下 PowerShell 命令：

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds &lt;timeout value>
```

- **最大并发导出或预览操作正在进行**

Director 支持一个导出或预览实例。如果出现**最大并发导出或预览操作正在进行**错误，请稍后重试下一个导出操作。

可以增加并发导出或预览操作的数量，但这可能会影响 Director 的性能，并且不受支持：

1. 打开 IIS 管理器控制台。
2. 导航到默认网站下的 Director 网站。
3. 双击**应用程序设置**。
4. 编辑值 **UI.ConcurrentExportLimit**。

- **Director 中磁盘空间不足**

每个导出操作在 Windows Temp 文件夹中最多需要 2 GB 硬盘空间。在 Director 服务器上清理空间或添加更多硬盘空间后，重试导出。

Monitor 热修复程序

要查看安装在特定计算机 VDA（物理或虚拟机）上的热修复程序，请选择**计算机详细信息**视图。

控制用户计算机电源状态

要控制在 Director 中选择的计算机的状态，请使用电源控制选项。这些选项适用于单会话操作系统计算机，但可能不适用于多会话操作系统计算机。

注意：

此功能不适用于物理计算机或使用远程电脑访问的计算机。

命令	功能
重新启动	执行 VM 的有序（软）关机，并在重新启动 VM 之前单独停止所有正在运行的进程。例如，选择在 Director 中显示为“启动失败”的计算机，然后使用此命令重新启动它们。
强制重新启动	重新启动 VM，而不首先执行任何关机过程。此命令的工作方式与拔下物理服务器电源，然后再插上电源并重新打开电源相同。
关机	执行 VM 的有序（软）关机。所有正在运行的进程都将单独停止。

命令	功能
强制关机	在不首先执行任何关机程序的情况下关闭 VM。此命令的工作方式与拔下物理服务器电源相同。它可能无法始终关闭所有正在运行的进程，并且如果以这种方式关闭 VM，则存在数据丢失的风险。
挂起	挂起正在运行的 VM 的当前状态，并将该状态存储在默认存储库中的文件中。此选项允许您关闭 VM 的主机服务器，稍后，在重新启动它之后，恢复 VM，使其返回到原始运行状态。
恢复	恢复已挂起的 VM 并将其还原到其原始运行状态。
启动	在 VM 关闭时启动它（也称为冷启动）。

如果电源控制操作失败，请将鼠标悬停在警报上，将显示一个弹出消息，其中包含有关故障的详细信息。

阻止连接到计算机

使用维护模式暂时阻止新连接，同时由相应的管理员对映像执行维护任务。

在计算机上启用维护模式后，在您禁用它之前，不允许建立任何新连接。如果用户当前已登录，则维护模式将在所有用户注销后立即生效。对于未注销的用户，请发送消息通知他们计算机将在特定时间关闭，并使用电源控件强制关闭计算机。

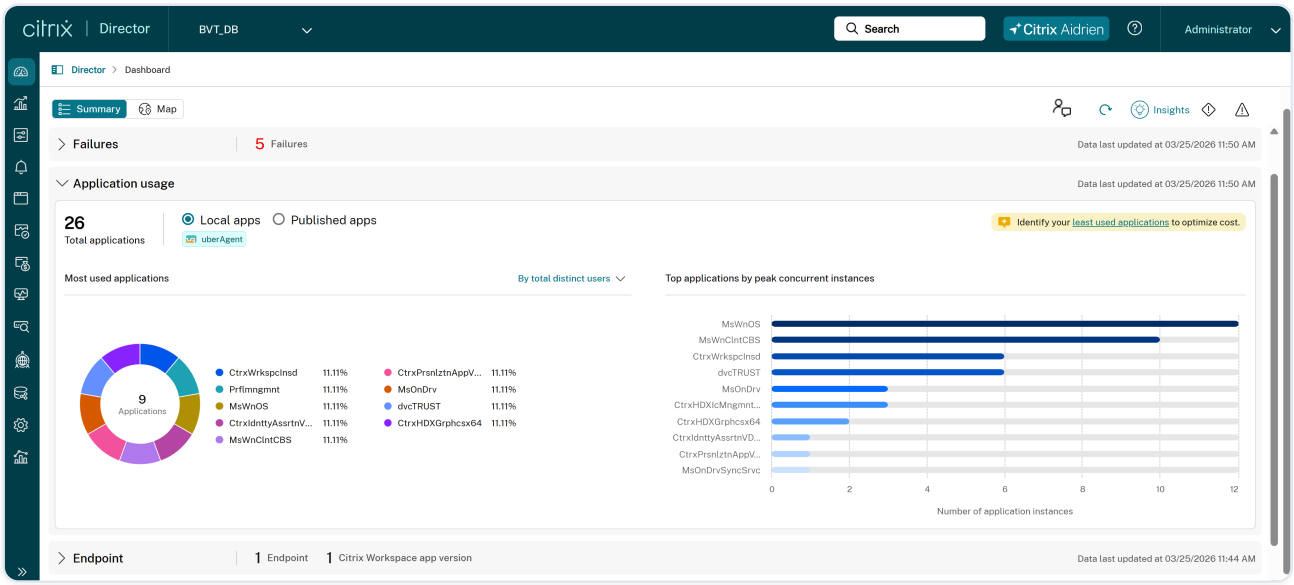
1. 选择计算机，例如从“用户详细信息”视图中选择，或在“筛选器”视图中选择一组计算机。
2. 选择**维护模式**，然后打开该选项。

如果用户尝试连接处于维护模式的已分配桌面，则会显示一条消息，指示该桌面不可用。在您禁用维护模式之前，无法建立任何新连接。

应用程序分析

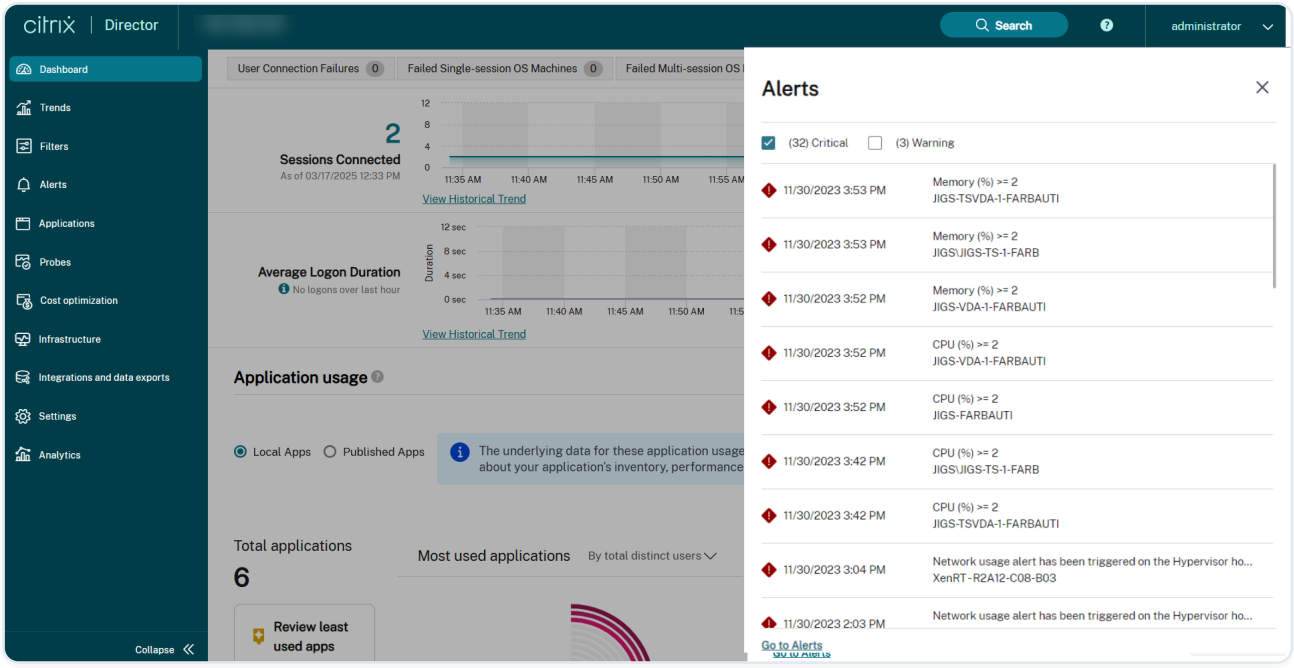
“**应用程序**”选项卡以单一的整合视图显示基于应用程序的分析，以帮助高效地分析和管理应用程序性能。您可以深入了解站点上发布的所有应用程序的运行状况和使用情况信息。它显示了诸如探测结

果、每个应用程序的实例数以及与已发布应用程序相关的故障和错误等指标。有关详细信息，请参阅“**应用程序故障排除**”中的应用程序分析部分。



警报和通知

警报在 Director 的仪表板和其他高级视图中显示，并带有警告和严重警报符号。警报适用于 **Premium** 许可站点。警报每分钟自动更新；您也可以按需更新警报。

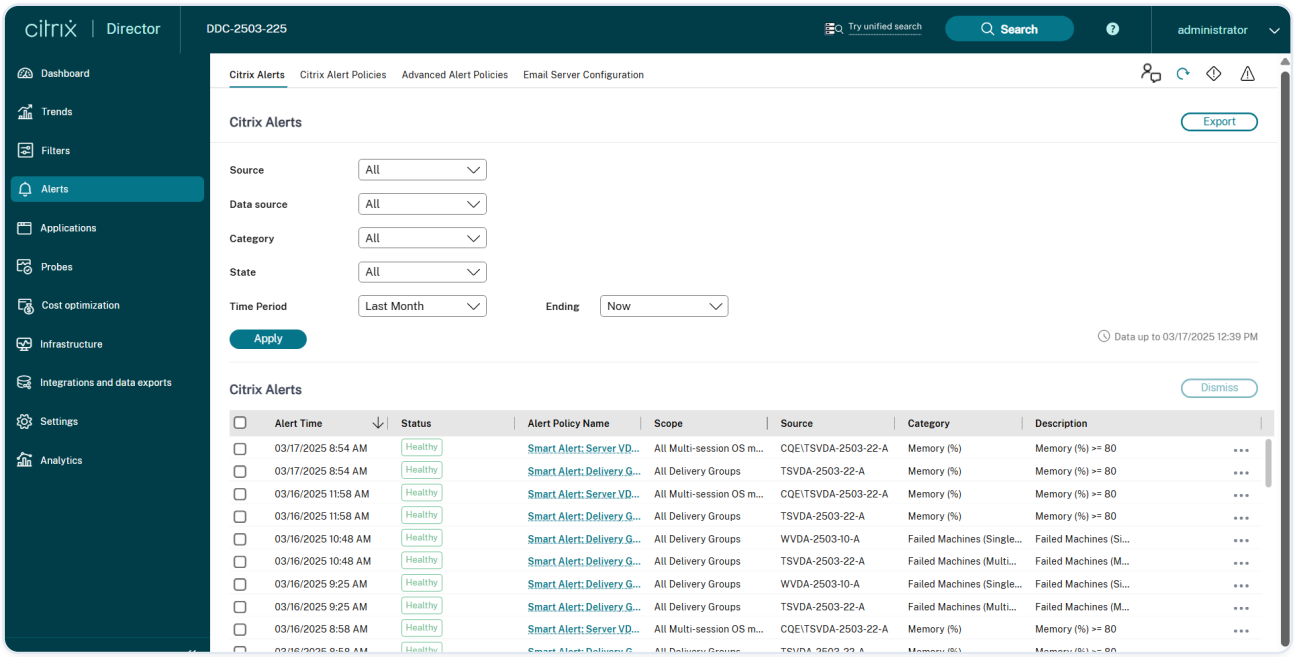


警告警报（琥珀色三角形）表示某个条件的警告阈值已达到或超出。

严重警报（红色圆形）表示某个条件的严重阈值已达到或超出。

您可以通过从侧边栏中选择警报、单击侧边栏底部的“**转到警报**”链接或从 Director 页面顶部选择“**警报**”来查看有关警报的更详细信息。

在“警报”视图中，您可以筛选和导出警报。例如，过去一个月内特定交付组的失败多会话操作系统计算机，或特定用户的所有警报。有关详细信息，请参阅导出报告。



Citrix® 警报

Citrix 警报是 Director 中监视的源自 Citrix 组件的警报。您可以在 Director 的“**警报**”\>“**Citrix 警报策略**”中配置 Citrix 警报。作为配置的一部分，您可以设置当警报超出您设置的阈值时，通过电子邮件向个人和组发送通知。有关设置 Citrix 警报的更多信息，请参阅创建警报策略。

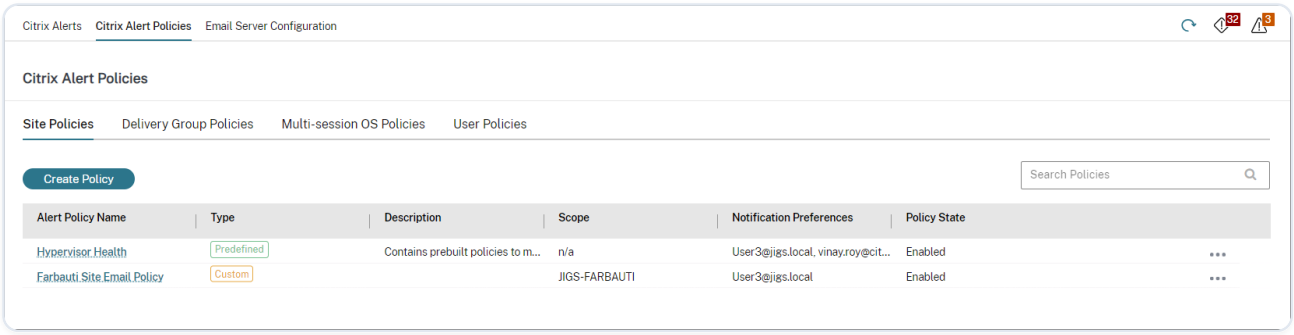
> **注意：**
>
> 确保您的防火墙、代理或 Microsoft Exchange Server 不会阻止电子邮件警报。

智能警报策略

一组具有预定义阈值值的内置警报策略可用于交付组和多会话操作系统 VDA 范围。此功能需要 Delivery Controller 7.18 或更高版本。您可以在“**警报**”\>“**Citrix 警报策略**”中修改内置警报策略的阈值参数。 当您的站点中定义了至少一个警报目标（交付组或多会话操作系统 VDA）时，将创建这些策略。此外，这些内置警报会自动添加到新的交付组或多会话操作系统 VDA。

如果您升级 Director 和您的站点，则会沿用您以前的 Director 实例中的警报策略。仅当 Monitor 数据库中不存在相应的警报规则时，才会创建内置警报策略。

有关内置警报策略的阈值，请参阅警报策略条件部分。



高级警报策略

Director 的主动通知和警报功能已增强，包含一个名为“**高级警报策略**”的新警报框架。借助此功能，您可以通过为每个元素或条件添加精细详细信息来创建警报，从而增强对警报范围的控制。目前，这些策略包括成本节约和基础架构的警报。

随着高级警报策略（一种数据源驱动的警报）的引入，您可以使用多条件范围筛选。

此功能可帮助您减少过多的警报，这可能会导致在处理重要问题时响应能力或效率降低。此策略有助于衡量警报策略的有效性以及管理员的参与度。

您可以从“**警报**”>“**高级警报策略**”>“**创建策略**”部分创建高级警报策略。

您可以选择以下数据源之一：

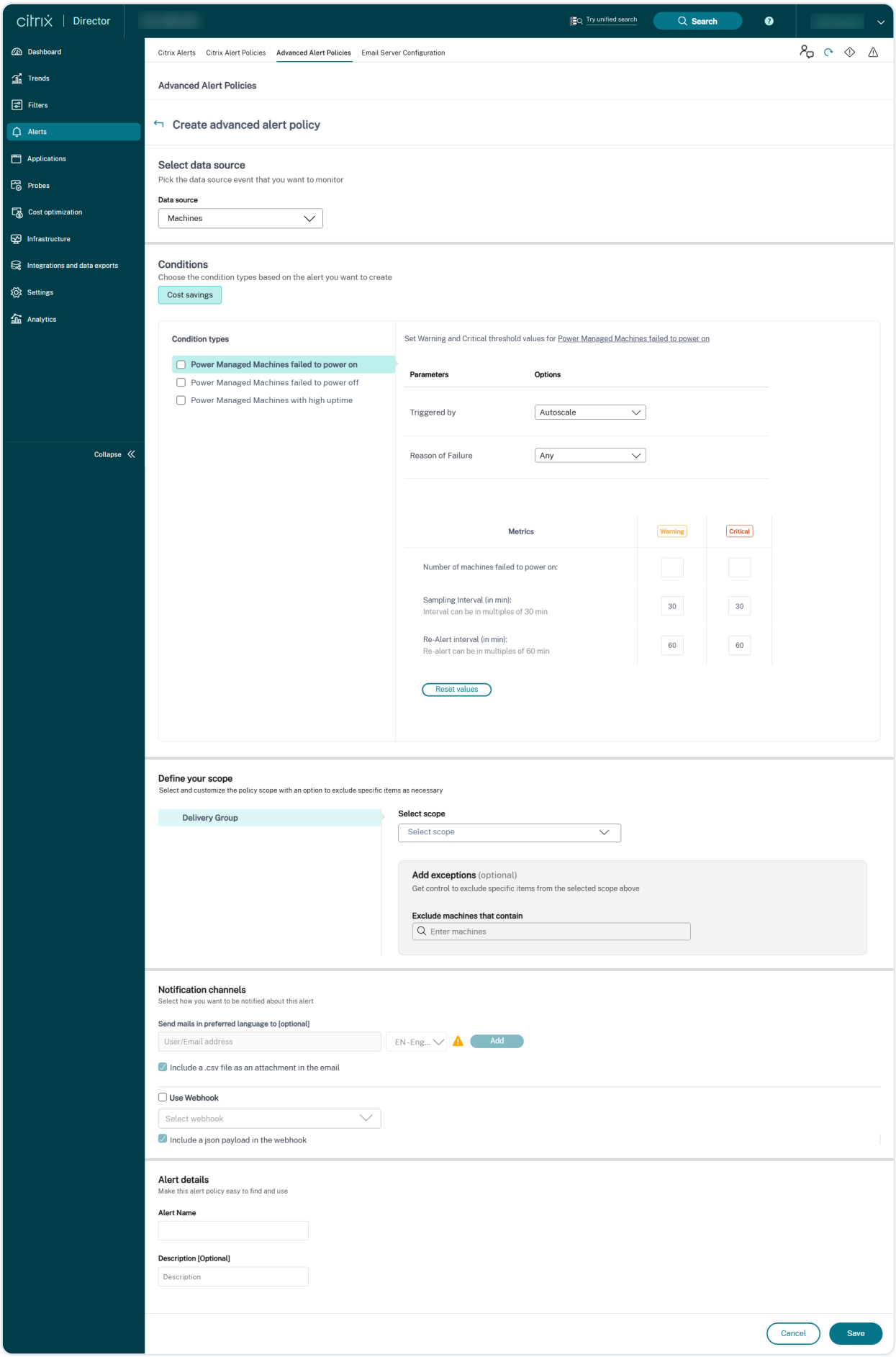
- 计算机
- 预配服务
- StoreFront™
- 交付控制器™

成本节约警报

您可以创建成本节约警报，以帮助您优化成本。目前，您可以为计算机创建警报。

要在计算机上创建警报，请执行以下操作：

1. 单击“**警报**”选项卡 >“**高级警报策略**”。将显示“**高级警报策略**”页面。
2. 单击“**创建策略**”。此时将显示“**创建高级警报策略**”部分。
3. 从“数据源”下拉列表中选择“**计算机**”。此时将显示“成本节约”条件和相应的条件类型。


citrix | Director
Try unified search
Search
Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and data exports
Settings
Analytics
Collapse
Citrix Alerts
Citrix Alert Policies
Advanced Alert Policies
Email Server Configuration
Advanced Alert Policies
Create advanced alert policy
Select data source
Pick the data source event that you want to monitor
Data source
Machines
Conditions
Choose the condition types based on the alert you want to create
Cost savings
Condition types
Power Managed Machines failed to power on
Power Managed Machines failed to power off
Power Managed Machines with high uptime
Set Warning and Critical threshold values for Power Managed Machines failed to power on
Parameters
Options
Triggered by
Autoscale
Reason of Failure
Any
Metrics
Warning
Critical
Number of machines failed to power on:
Sampling Interval (in min):
Interval can be in multiples of 30 min
30
30
Re-Alert interval (in min):
Re-alert can be in multiples of 60 min
60
60
Reset values
Define your scope
Select and customize the policy scope with an option to exclude specific items as necessary
Delivery Group
Select scope
Select scope
Add exceptions (optional)
Get control to exclude specific items from the selected scope above
Exclude machines that contain
Enter machines
Notification channels
Select how you want to be notified about this alert
Send mails in preferred language to [optional]
User/Email address
EN - Eng...
Add
Include a .csv file as an attachment in the email
Use Webhook
Select webhook
Include a json payload in the webhook
Alert details
Make this alert policy easy to find and use
Alert Name
Description [Optional]
Description
Cancel
Save

4. 根据需要选择以下条件类型：
    - 电源管理的计算机未能开机
    - 电源管理的计算机未能关机
    - 具有高运行时间的电源管理计算机
5. 为每个选定的条件选择特定的参数和相应的选项。
6. 为选定的条件类型设置警告和严重指标：
    - 对于具有高运行时间的电源管理计算机：
        - 超出运行时间阈值的机器数量
        - 重新警报间隔（分钟）最短为 60 分钟
    - 对于未能开机的电源管理计算机和未能关机的电源管理计算机：
        - 超出运行时间阈值的机器数量
        - 采样间隔（分钟），间隔可以是 30 分钟的倍数
        - 重新警报间隔（分钟），重新警报可以是 60 分钟的倍数
7. 根据需要为选定的警报安排重新警报间隔。
8. 定义警报的范围。
9. 设置通知渠道。这可以是电子邮件或 Webhook。

    a. 您可以选择以下复选框：

    - 在 Webhook 中包含 JSON 有效负载作为附件
    - 在电子邮件中包含 CSV 文件作为附件

    有关详细信息，请参阅警报内容增强功能。
10. 输入**警报详细信息**，例如**警报名称**和**描述**（可选）。
11. 单击**保存**。警报已创建。

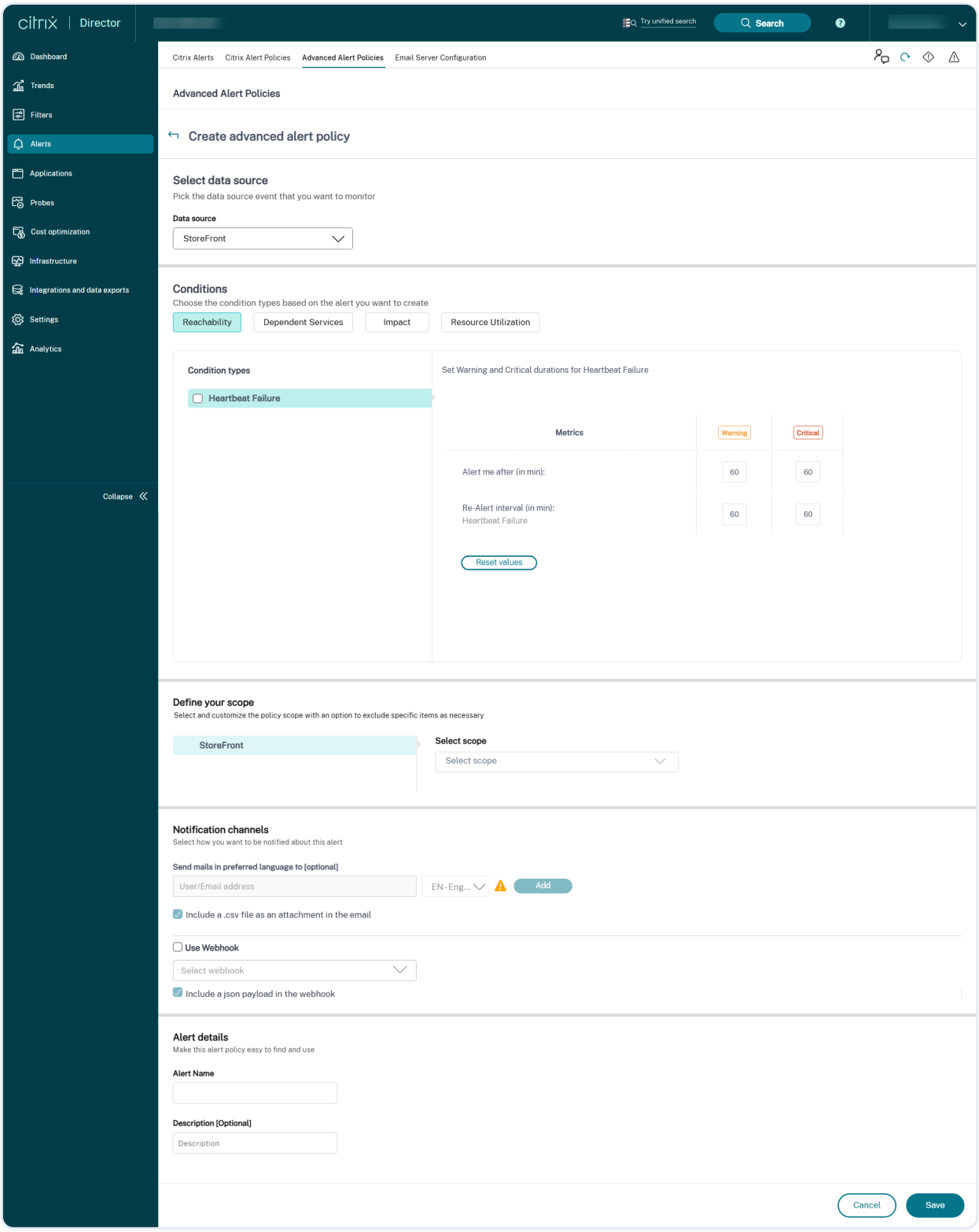
基础结构监控警报

您可以创建警报来监控以下受支持的 Citrix Virtual Apps and Desktops™ 组件的运行状况：

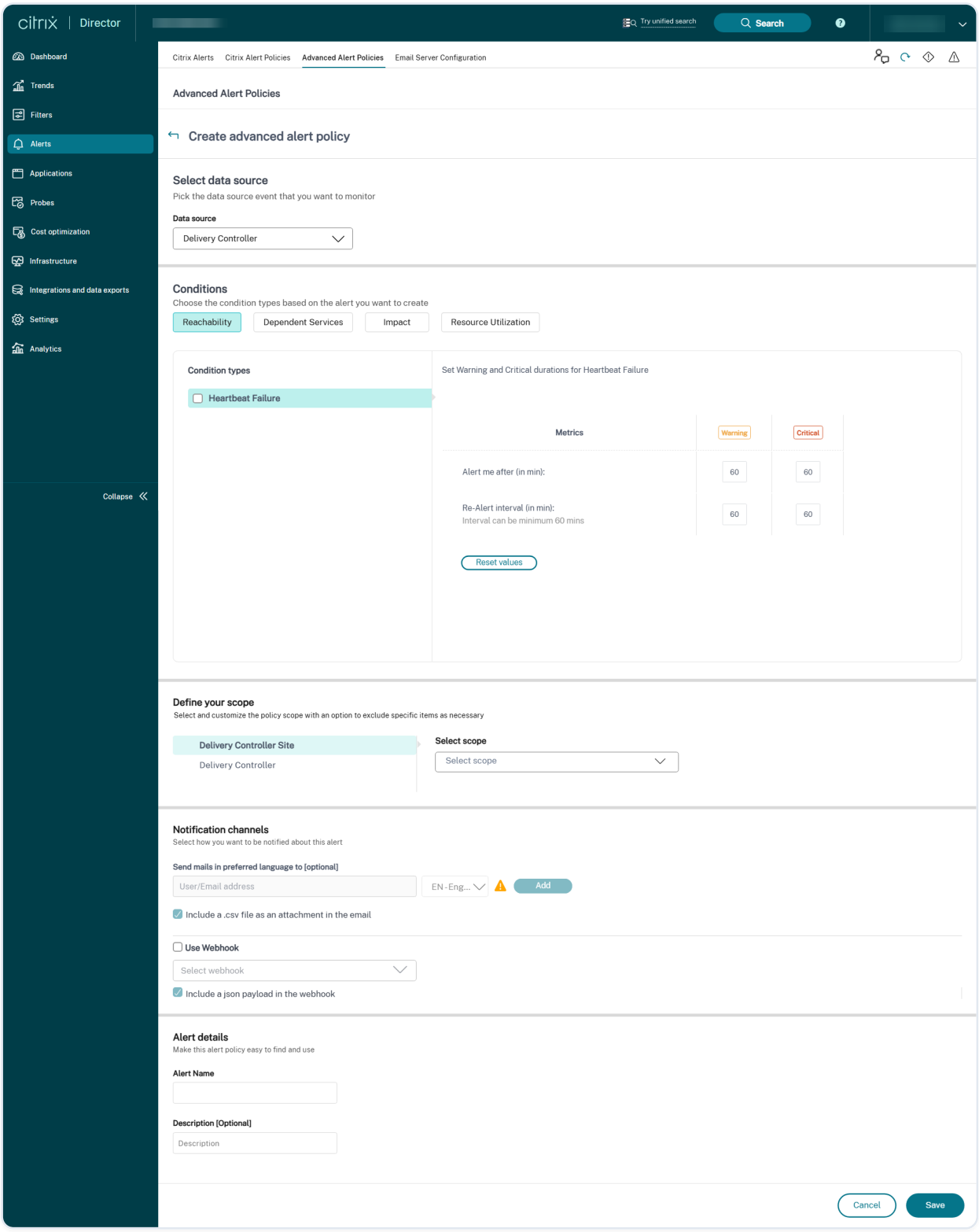
- 预配服务

- StoreFront


citrix | Director
Try unified search
Search
Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and data exports
Settings
Analytics
Collapse
Citrix Alerts
Citrix Alert Policies
Advanced Alert Policies
Email Server Configuration
Advanced Alert Policies
Create advanced alert policy
Select data source
Pick the data source event that you want to monitor
Data source
StoreFront
Conditions
Choose the condition types based on the alert you want to create
Reachability
Dependent Services
Impact
Resource Utilization
Condition types
Heartbeat Failure
Set Warning and Critical durations for Heartbeat Failure
Metrics
Warning
Critical
Alert me after (in min):
60
60
Re-Alert interval (in min):
Heartbeat Failure
60
60
Reset values
Define your scope
Select and customize the policy scope with an option to exclude specific items as necessary
StoreFront
Select scope
Select scope
Notification channels
Select how you want to be notified about this alert
Send mails in preferred language to [optional]
User/Email address
EN - Eng...
Add
Include a .csv file as an attachment in the email
Use Webhook
Select webhook
Include a json payload in the webhook
Alert details
Make this alert policy easy to find and use
Alert Name
Description [Optional]
Description
Cancel
Save

- 交付控制器



完成 基础结构监控 设置后，您可以使用 Director 中提供的运行状况数据为任何所需组件配置警报。管理员可以设置条件、范围和通知媒介，以通过电子邮件或通过 Webhook 的 JSON 有效负载接收重要警报。对于 Provisioning Service 和 Delivery Controller，您可以将警报范围选择为站点级别或单个服务器级别。例如，对于 Provisioning Service，如果选择“所有 Provisioning Service”，则即使站点有两台服务器，您也只会收到整个站点的单个警报。这被视为站点级警报。触发的警报也可在“**Citrix 警报**”部分中进行分析和管理。

作为新引入的基础结构策略的一部分，警报条件分为以下四个部分：

- 可访问性
- 相关服务
- 影响
- 资源利用率

可以根据您的组织优先级，将每个类别中的条件设置为**严重**和**警告**级别。您还可以为这些警报安排重新警报间隔。

您可以从“**警报**”>“**Citrix 警报策略**”部分创建基础结构策略。您可以选择所需的类别，然后选择策略所需的条件。有关如何创建策略的更多信息，请参阅创建警报策略。创建策略后，您可以在 Citrix 警报页面上编辑、删除或禁用该策略。

有关每个类别和组件中支持的条件的更多详细信息，请参阅以下内容：

- Provisioning Service 运行状况指标
- StoreFront 运行状况指标
- Delivery Controller 运行状况指标

以下数据将作为警报通过电子邮件或在 Citrix 警报页面上接收：

字段	描述
客户 ID	站点的客户 ID。
警报级别	可能的值为“严重”和“警告”。
目标	触发警报的计算机名称。
时间	触发警报的时间。
范围	策略的范围。
策略	策略的名称。
描述	触发警报的问题描述。

定义策略范围

您可以定义警报的范围并添加例外。警报仅针对选定范围生成，使用添加例外排除的子范围不包括在警报生成中。此功能可帮助您在精细级别创建警报。

您可以通过电子邮件或 Webhook URL 创建通知。您还可以选择接收警报的首选语言。您还可以选择通过电子邮件以 .CSV 文件附件形式或通过 Webhook URL 以 JSON 有效负载形式接收警报参数。附件包含所需参数的详细信息。有关详细信息，请参阅警报内容增强功能。

以下数据将作为警报通过电子邮件或在 **Citrix Alerts** 页面上接收：

字段	描述
客户 ID	站点的客户 ID。
警报级别	此值是为每个警报条件设置的预定义值。可能的值为“严重”和“警告”。
条件	此值是创建策略时设置的条件。例如，未注册计算机的数量等于或多于 20 台。
目标	触发警报的交付组或站点的名称。
站点	站点的名称。
范围	策略的范围。此值也包括子范围。
策略	策略的名称。
描述	触发警报的问题描述。

如何使用 PowerShell 脚本创建高级警报策略?

用于创建警报策略的 PowerShell 脚本：

```
asnp Citrix.Monitor.*

# Add Parameters

$timeSpan = New-TimeSpan -Seconds 30

$alertThreshold = 1

$alarmThreshold = 2

# Add Target UID's

$targetIds = @()
```

```
$targetIds += "e9a211b4-a1f3-4f74-b6c7-85225902e997"

# Add email addresses

$emailaddress = @()

$emailaddress += "loki@abc.com"

# Create new policy

$policy = New-MonitorNotificationPolicy -Name
"FailedMachinePercentageAlertCreationViaPowershell" -Description "Policy
created to test urm" -Enabled $true
```

将以下行替换为 FAILEDMACHINEPERCENTAGE 的正确条件

```
Add-MonitorNotificationPolicyCondition -Uid $policy.Uid -ConditionType
FailedMachinePercentage -AlertThreshold $alertThreshold -AlarmThreshold
$alarmThreshold -AlertRenotification $timeSpan -AlarmRenotification
$timeSpan

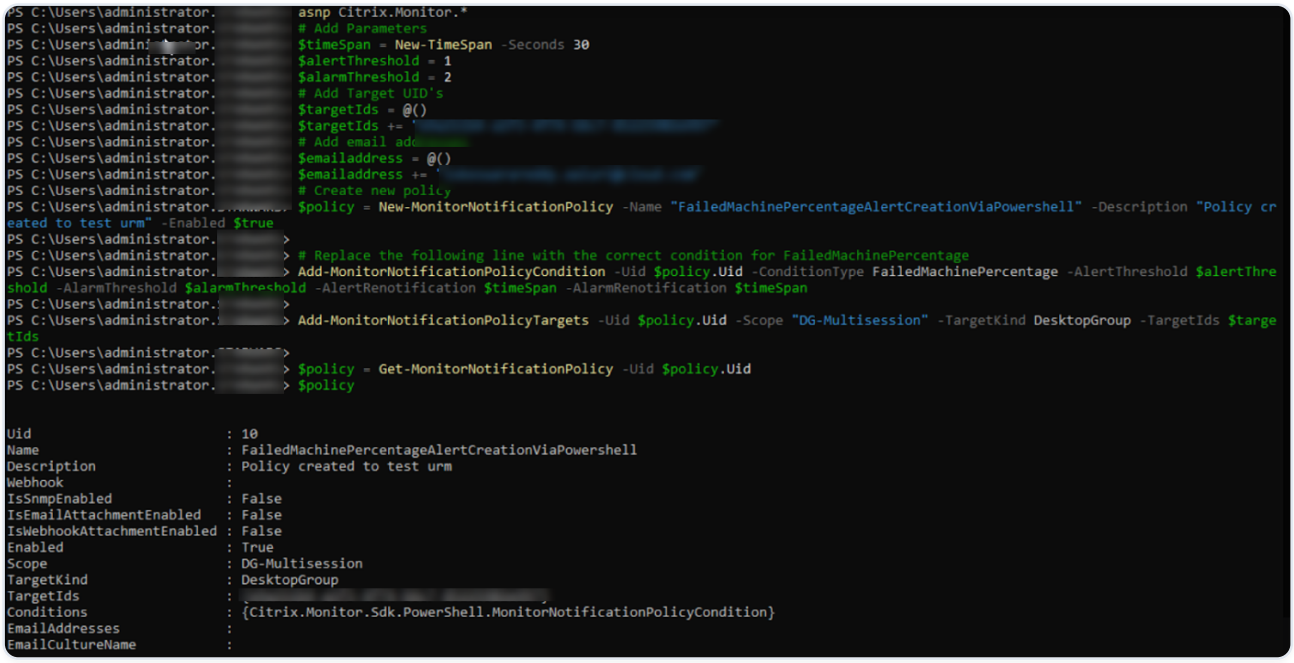


Add-MonitorNotificationPolicyTargets -Uid $policy.Uid -Scope "DG-
Multisession" -TargetKind DesktopGroup -TargetIds $targetIds



$policy = Get-MonitorNotificationPolicy -Uid $policy.Uid

$policy
```



从上图中，您可以看到策略已创建，并且 Uid 为 10。

将电子邮件添加到配置

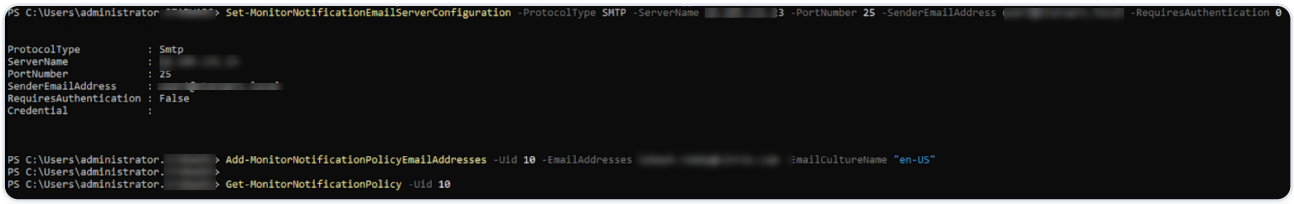
```
Set-MonitorNotificationEmailServerConfiguration -ProtocolType SMTP
-ServerName NameOfTheSMTPServerOrIPAddress -PortNumber 80
-SenderEmailAddress loki@abc.com -RequiresAuthentication 0
```

将电子邮件添加到策略

```
Add-MonitorNotificationPolicyEmailAddresses -Uid $policy.Uid
-EmailAddresses $emailaddress -EmailCultureName "en-US"
```

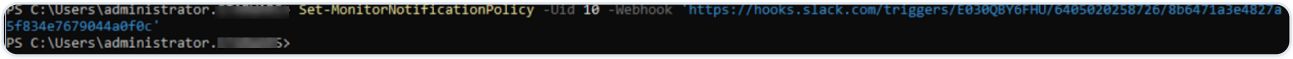
添加电子邮件的示例脚本：

```
Add-MonitorNotificationPolicyEmailAddresses -Uid 10 -EmailAddresses
$emailaddress -EmailCultureName "en-US"
```



将 WEBHOOK URL 添加到策略

```
Set-MonitorNotificationPolicy –Uid $polcy.Uid –Webhook 'URL'
```

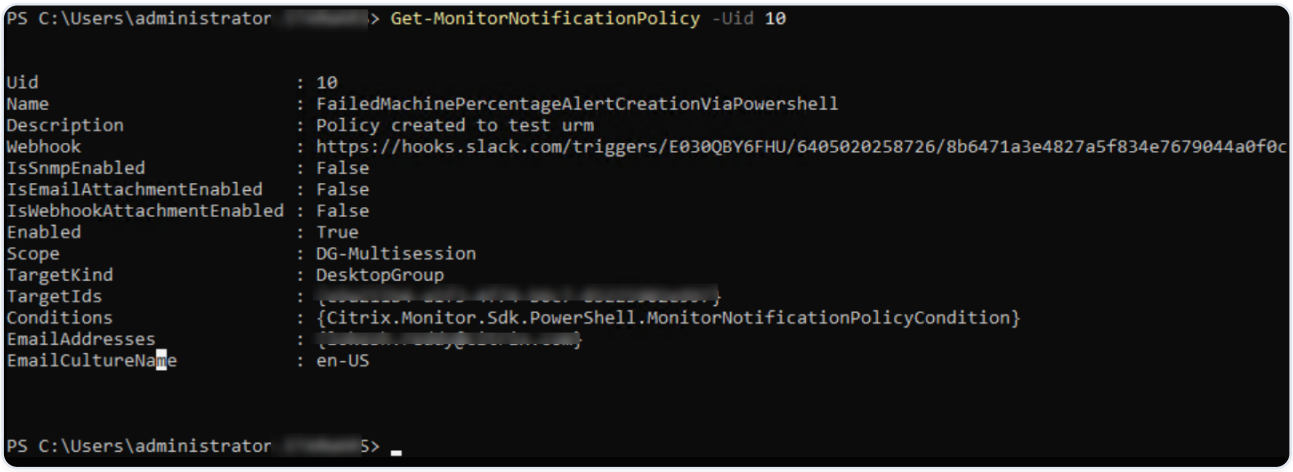


添加 Webhook URL 的示例脚本：

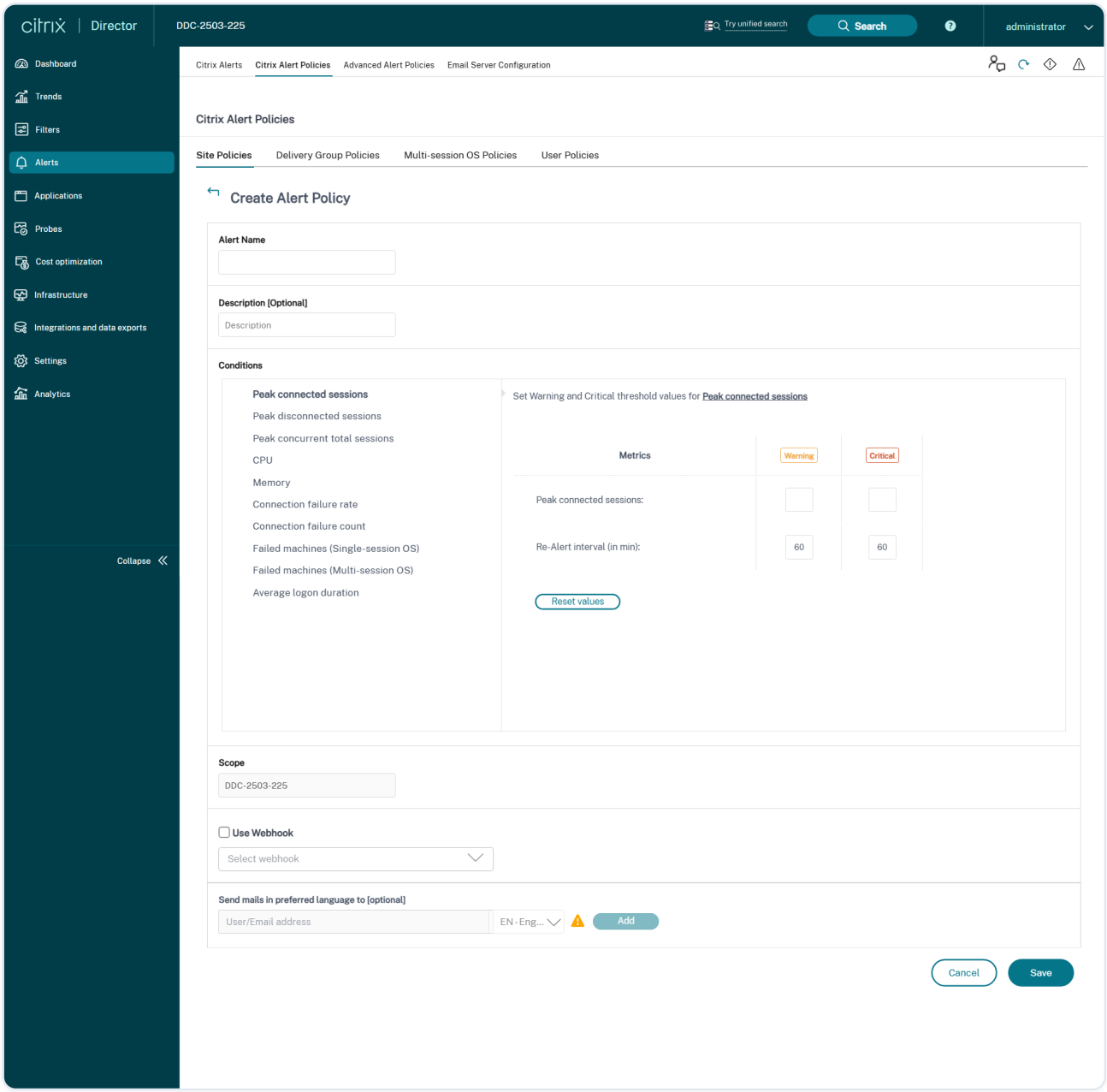
```
Set-MonitorNotificationPolicy –Uid 10  –Webhook  'https://hooks.slack.com/
triggers/E030QBY6FHU/6405020258726/8b6471a3e4827a5f834e7679022a1f1c'
```

获取已创建策略详细信息

```
Get-MonitorNotificationPolicy -Uid 10
```



创建警报策略



例如，要创建警报策略以在满足特定会话计数条件时生成警报，请执行以下操作：

1. 转到**警报** > **Citrix 警报策略**，然后选择（例如）多会话操作系统策略。
2. 单击**创建**。
3. 命名并描述策略，然后设置触发警报必须满足的条件。例如，为峰值连接会话、峰值断开连接会话和峰值并发总会话指定警告和严重计数。警告值不得大于严重值。有关详细信息，请参阅警报策略条件。
4. 设置重新警报间隔。如果警报条件仍然满足，警报将在此时间间隔再次触发，并且，如果警报策略中已设置，则会生成电子邮件通知。已解除的警报不会在重新警报间隔生成电子邮件通知。
5. 设置范围。例如，为特定的交付组设置。

6. 在“通知首选项”中，指定当警报触发时必须通过电子邮件通知谁。您必须在**电子邮件服务器配置**选项卡上指定电子邮件服务器，才能在“警报策略”中设置电子邮件通知首选项。

   a. 您还可以通过 .CSV 附件或 json 有效负载接收警报内容。为此，请选中以下复选框：

      - **在 Webhook 中包含 JSON 有效负载作为附件**
      - **在电子邮件中包含 CSV 文件作为附件**

   > **注意：**
   >
   > 目前，通过 .CSV 附件和 json 有效负载选项接收警报内容仅适用于少数警报。有关详细信息，请参阅警报内容增强功能

7. 单击 **保存**。

创建在“范围”中定义了 20 个或更多交付组的策略可能需要大约 30 秒才能完成配置。在此期间会显示一个旋转图标。

为多达 20 个唯一交付组（总共 1000 个交付组目标）创建 50 个以上的策略可能会导致响应时间增加（超过 5 秒）。

将包含活动会话的计算机从一个交付组移动到另一个交付组可能会触发使用计算机参数定义的错误交付组警报。

> **注意：**
>
> 删除警报策略后，策略生成的警报通知可能需要长达 30 分钟才能停止。

警报内容的增强功能

Director 的警报功能已增强，可包含 CSV 附件和 JSON 有效负载。通过此增强功能，您可以通过电子邮件以 CSV 附件形式或在存在 Webhook 时以 JSON 有效负载形式获取警报详细信息。使用此 CSV 附件或 JSON 有效负载，您可以接收详细级别的丰富内容，从而有助于快速识别和解决问题。

目前，此增强功能仅适用于以下警报：

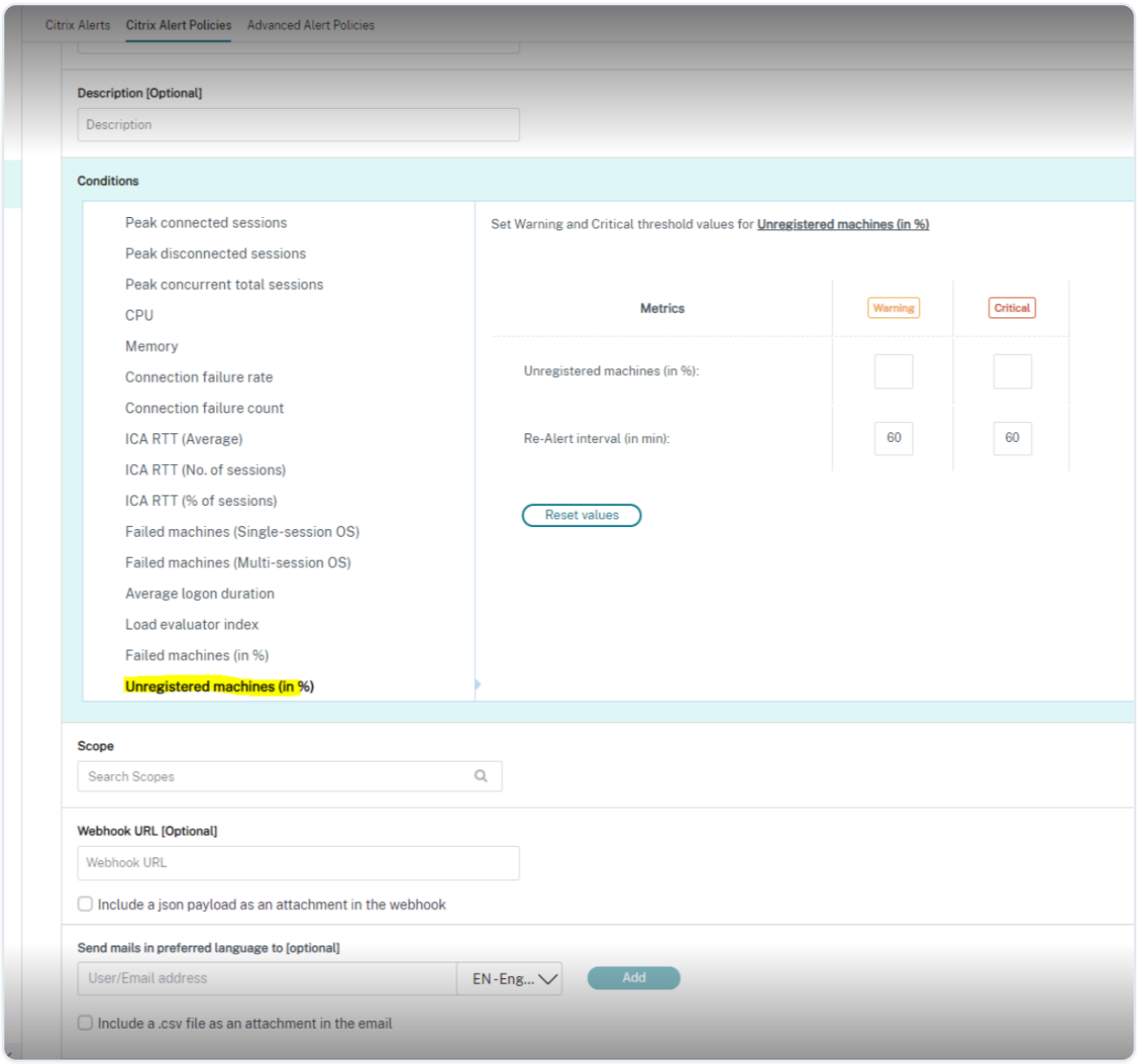
- 计算机正常运行时间
- 失败的开机操作
- 失败的关机操作

- 未注册的计算机 (%)

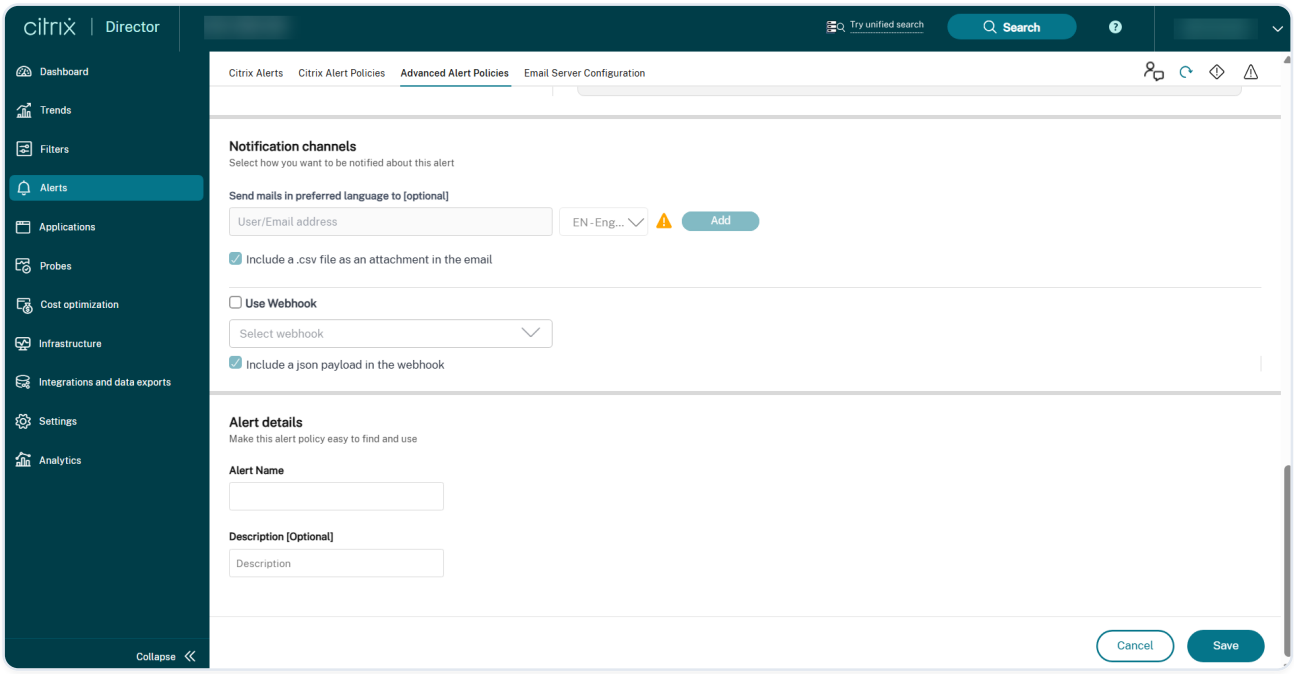
要使用此功能，请导航到警报并选择以下复选框：

- **在 Webhook 中包含 JSON 有效负载作为附件**
- **在电子邮件中包含 CSV 文件作为附件**

以下是来自 **Citrix 警报策略** 部分的屏幕截图：



以下是来自 **高级警报策略** 部分的屏幕截图：



CSV 附件

下表提供了所有受支持警报的 .CSV 附件的列：

列	适用警报
计算机名称、IP 地址和交付组名称	计算机正常运行时间、关机失败操作和开机失败操作以及未注册计算机 (%)
当前注册状态、失败日期、故障状态和生命周期状态	未注册计算机 (%)
上次电源操作失败原因、上次电源操作触发者、上次电源操作类型和上次电源操作完成日期	失败的关机操作和失败的开机操作
电源状态、开机日期和总运行时间（分钟）	计算机正常运行时间

WEBHOOK 有效负载

未注册计算机百分比警报

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Unregistered machines (in %)\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
```

```
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"CurrentRegistrationState\":\"Unregistered\",
\"FailureDate\":\"<Date of Failure>\",\"FaultState\":\"<Fault State of the
Machine>\",\"LifecycleState\":\"<Lifecycle state of the Machine>\"},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"CurrentRegistrationState\":\"Unregistered\",\"FailureDate\":\"<Date of
Failure>\",\"FaultState\":\"<Fault State of the Machine>\",
\"LifecycleState\":\"<Lifecycle state of the Machine>\"}]}"

}
```

失败的开机操作警报

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOn Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of the
DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"
```

```
}
```

失败的关机操作警报

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOff Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IPV4 Address of the Machine>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IPV4 Address of the Machine>\",\"DeliveryGroupName\":
\"<Name of the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"

}
```

计算机运行时间警报

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Machine Uptime Alert\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
```

```
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"PowerState\":\"<On/Off>\",\"PoweredOnDate\":
\"2024-05-15T15:04:27.723\",\"TotalUptimeInMinutes\":180},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",\"PowerState\":
\"<ON/OFF>\",\"PoweredOnDate\":\"2024-05-15T15:04:27.723\",
\"TotalUptimeInMinutes\":\"<Uptime Duration>\"}]}"

}
```

警报策略条件

下面列出了警报类别、建议的缓解警报措施以及（如果已定义）内置策略条件。内置警报策略的警报和重新警报间隔为 60 分钟。

峰值连接会话

- 检查 Director 会话趋势视图以查看峰值连接会话。
- 检查以确保有足够的容量来适应会话负载。
- 如果需要，添加新计算机

峰值断开连接会话

- 检查 Director 会话趋势视图以查看峰值断开连接会话。
- 检查以确保有足够的容量来容纳会话负载。
- 如有需要，添加新计算机。
- 如有需要，注销断开连接的会话。

并发会话总数峰值

- 检查 Director 中的 Director 会话趋势视图以查看峰值并发会话。
- 检查以确保有足够的容量来容纳会话负载。
- 如有需要，添加新计算机。
- 如有需要，注销断开连接的会话。

CPU

CPU 使用率百分比表示 VDA 上的整体 CPU 消耗，包括进程的 CPU 消耗。您可以从相应 VDA 的**计算机详细信息**页面获取有关单个进程的 CPU 利用率的更多见解。

- 转到**计算机详细信息 > 查看历史利用率 > 前 10 个进程**，识别消耗 CPU 的进程。确保已启用进程监视策略以启动进程级别资源使用情况统计信息的收集。
- 如有必要，结束进程。
- 结束进程会导致未保存的数据丢失。
- 如果一切按预期运行，将来请添加额外的 CPU 资源。

> **注意：**
>
> 默认情况下，**启用资源监视**策略设置允许用于监视具有 VDA 的计算机上的 CPU 和内存性能计数器。如果此策略设置被禁用，则不会触发具有 CPU 和内存条件的警报。有关详细信息，请参阅监视策略设置
>
> **智能策略条件：**
>
> - **范围：**交付组，多会话操作系统范围
> - **阈值：**警告 - 80%，严重 - 90%

内存

内存使用百分比指示 VDA 上的总体内存消耗，包括进程的内存消耗。您可以从相应 VDA 的“**计算机详细信息**”页面更深入地了解单个进程的内存使用情况。

- 转到**计算机详细信息 > 查看历史利用率 > 前 10 个进程**，识别占用内存的进程。确保已启用进程监视策略以启动进程级别资源使用情况统计信息的收集。
- 如有必要，结束该进程。
- 结束进程会导致未保存的数据丢失。
- 如果一切按预期运行，将来请添加额外的内存。

> **注意：**

> 默认情况下，**启用资源监视**策略设置允许用于监视具有 VDA 的计算机上的 CPU 和内存性能计数器。如果此策略设置被禁用，则不会触发具有 CPU 和内存条件的警报。有关详细信息，请参阅监视策略设置

> **智能策略条件：**

- **范围：**交付组，多会话操作系统范围
- **阈值：** 警告 - 80%，严重 - 90%

连接失败率

过去一小时内连接失败的百分比。

- 根据尝试连接总数中的失败总数计算。
- 检查 Director 连接失败趋势视图以查看从配置日志记录的事件。
- 确定应用程序或桌面是否可访问。

连接失败计数

过去一小时内连接失败的数量。

- 检查 Director 连接失败趋势视图以查看从配置日志记录的事件。
- 确定应用程序或桌面是否可访问。

ICA® RTT（平均）

平均 ICA 往返时间。

- 检查 Citrix ADM 以获取 ICA RTT 的细分，从而确定根本原因。有关详细信息，请参阅 Citrix ADM 文档。
- 如果 Citrix ADM 不可用，请检查 Director 用户详细信息视图中的 ICA RTT 和延迟，并确定是网络问题还是应用程序或桌面问题。

ICA RTT（会话数）

超过阈值 ICA 往返时间的会话数。

- 检查 Citrix ADM 以获取 ICA RTT 较高的会话数。有关详细信息，请参阅 Citrix ADM 文档。
- 如果 Citrix ADM 不可用，请与网络团队协作以确定根本原因。

智能策略条件：

- **范围：**交付组，多会话操作系统范围

- **阈值：**警告 - 5 个或更多会话的 300 毫秒，严重 - 10 个或更多会话的 400 毫秒

ICA RTT（会话百分比）

超过平均 ICA 往返时间的会话百分比。

- 检查 Citrix ADM 中 ICA RTT 较高的会话数。有关详细信息，请参阅 Citrix ADM 文档。
- 如果 Citrix ADM 不可用，请与网络团队协作以确定根本原因。

ICA RTT（用户）

应用于指定用户启动的会话的 ICA 往返时间。如果至少一个会话中的 ICA RTT 大于阈值，则会触发警报。

失败的计算机（单会话操作系统）

失败的单会话操作系统计算机数量。失败可能由于各种原因而发生，如 Director 控制板和筛选器视图中所示。

- 运行 Citrix Scout 诊断以确定根本原因。

  智能策略条件：

  - **范围：** 交付组、多会话操作系统范围
  - **阈值：**警告 - 1，严重 - 2

失败的计算机（多会话操作系统）

失败的多会话操作系统计算机数量。失败可能由于各种原因而发生，如 Director 控制板和筛选器视图中所示。

- 运行 Citrix Scout 诊断以确定根本原因。

  智能策略条件：

  - **范围：** 交付组、多会话操作系统范围
  - **阈值：**警告 - 1，严重 - 2

失败的计算机（百分比）

交付组中失败的单会话和多会话操作系统计算机的百分比，根据失败计算机的数量计算。此警报条件允许您将警报阈值配置为交付组中失败计算机的百分比，并且每 30 秒计算一次。 失败可能由于各种原因而发生，如 Director 控制板和筛选器视图中所示。运行 Citrix Scout 诊断以确定根本原因。有关详细信息，请参阅 解决用户问题。

开机操作失败和关机操作失败

交付组中失败的开机操作数和失败的关机操作数，根据未能开机或关机的 **电源管理计算机** 数量计算。此警报条件允许您将警报阈值配置为交付组中未能开机或关机的 **电源管理计算机** 数量，并且每 30 分钟计算一次。

管理员可以在高级警报策略中为这些警报配置以下参数：

- 触发者：是什么触发了电源操作
- 失败原因：操作失败的原因
- 阈值：触发策略的电源操作失败的计算机数量阈值
- 采样间隔：检查失败电源操作的间隔
- 重新警报间隔：警报必须重新发送的时间间隔

失败可能由于各种原因而发生，如 Director 控制板和筛选器视图中所示。运行 Citrix Scout 诊断以确定根本原因。有关详细信息，请参阅 解决用户问题。

未注册的计算机（百分比）

当计算机因重新启动而变得不稳定，或者交付控制器与虚拟机之间存在通信问题时，该计算机被视为未注册。**未注册计算机（百分比）** 是交付组中未注册的单会话和多会话操作系统计算机的百分比，根据未注册计算机的数量计算。此警报条件允许您将警告和严重阈值配置为交付组中未注册计算机的百分比。您可以设置重新警报的间隔。您还可以添加电子邮件，以便在满足 **未注册计算机（百分比）** 的条件时收到通知。当超出严重或警告阈值时，会生成警报和电子邮件。您可以在 **Citrix 警报** 下查看警报。您可以按 **未注册计算机（百分比）** 类别以及所需的状态和时间进行筛选。

如果存在电子邮件，您还可以通过 CSV 附件接收警报详细信息；如果存在 Webhook，则可以通过 JSON 有效负载接收警报详细信息。

> **注意：**
>
> 严重值必须大于警告值。

> **策略条件：**

- **范围**：单会话操作系统和多会话操作系统交付组
- **阈值**：警告和严重

计算机正常运行时间警报

交付组中的计算机正常运行时间是根据交付组中已开机计算机每天、每周或每月的小时数计算的。此警报条件允许您将警报阈值配置为交付组中计算机的开机小时数。在以下情况下，计算机正常运行时间警报的工作方式如下：

- 每天小时数 - 您可以指定计算机每天开机的小时数，并每 30 分钟计算一次。您可以设置的每天最大小时数为 24 小时。
- 每周小时数 - 您可以指定一台机器每周开启的小时数，该数值每六小时计算一次。您可以设置的每周最大小时数为 168 小时。
- 每月小时数 - 您可以指定一台机器每月开启的小时数，该数值每天计算一次。每月最大小时数为 720 小时。 您可以设置的最小重新警报间隔值为 60 分钟。您可以在“警告和严重警报”部分输入超出机器正常运行时间阈值的机器数量。您还可以为任何机器添加例外。

例如，如果为此警报添加了五个交付组，并且在第一个交付组和第四个交付组中，机器数量超过了警告或严重阈值，则警报将分别为第一个交付组和第四个交付组触发。

此警报可帮助管理员分析计算机的正常运行时间，并根据此分析帮助管理员优化成本。如果存在电子邮件，您还可以通过 CSV 附件接收警报详细信息；如果存在 Webhook，则可以通过 JSON 有效负载接收警报详细信息。

平均登录持续时间

过去一小时内发生的登录的平均登录持续时间。

- 检查 Director 控制板以获取有关登录持续时间的最新指标。在短时间内登录的许多用户可能会增加登录持续时间。
- 检查登录的基线和细分以缩小原因范围。有关详细信息，请参阅 诊断用户登录问题

  智能策略条件：

  - **范围：** 交付组，多会话操作系统范围
  - **阈值：** 警告 - 45 秒，严重 - 60 秒

登录持续时间（用户）

过去一小时内指定用户的登录持续时间。

负载评估器指数

过去 5 分钟内负载评估器指数的值。

- 检查 Director 中可能具有峰值负载（最大负载）的多会话操作系统计算机。查看“控制板”（故障）和“趋势负载评估程序索引”报告。

智能策略条件：

- **范围：** 交付组，多会话操作系统范围
- **阈值：** 警告 - 80%，严重 - 90%

使用 Webhook 配置警报策略

除了电子邮件通知之外，您还可以使用 Webhook 配置警报策略。

注意： 此功能需要 Delivery Controller 7.11 或更高版本。

您可以使用 PowerShell cmdlet 配置带有 HTTP 回调或 HTTP POST 的警报策略。它们已扩展为支持 Webhook。

有关创建新的 Octoblu 工作流和获取相应 Webhook URL 的信息，请参阅 Octoblu Developer Hub。

要为新的警报策略或现有策略配置 Webhook URL，请使用以下 PowerShell cmdlet。

创建包含 Webhook URL 的新警报策略：

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -Description
<Policy description> -Enabled $true -Webhook <Webhook URL>
```

将 Webhook URL 添加到现有警报策略：

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

有关 PowerShell 命令的帮助，请使用 PowerShell 帮助，例如：

```
Get-Help  <Set-MonitorNotificationPolicy>
```

警报策略生成的通知会通过对 Webhook URL 的 POST 调用触发 Webhook。POST 消息包含 JSON 格式的通知信息：

```
{"NotificationId" : \<Notification Id\>,



"Target" : \<Notification Target Id\>,
```

```
"Condition" : \<Condition that was violated\>,

"Value" : \<Threshold value for the Condition\>,

"Timestamp": \<Time in UTC when notification was generated\>,

"PolicyName": \<Name of the Alert policy\>,

"Description": \<Description of the Alert policy\>,

"Scope" : \<Scope of the Alert policy\>,

"NotificationState": \<Notification state critical, warning, healthy or
dismissed\>,

"Site" : \<Site name\>}
```

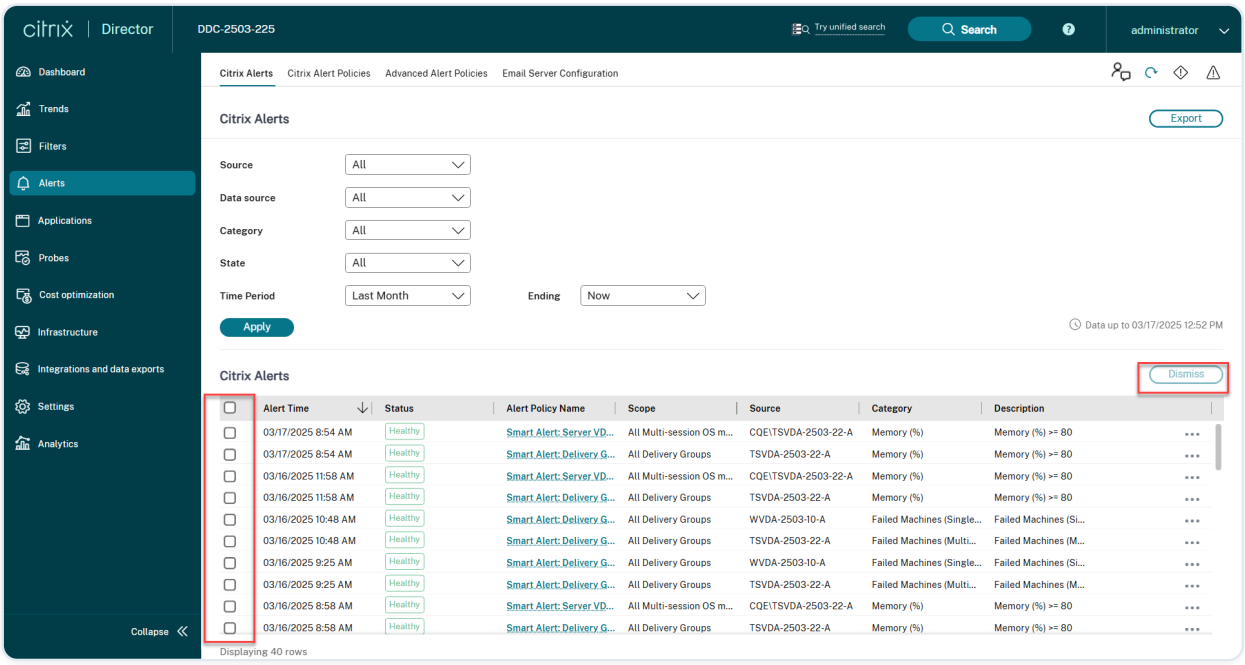
批量解除警报

此功能优化了管理员的警报管理流程，提供了灵活性并减少了警报疲劳。管理员可以根据时间、类型或类别批量解除警报，从而简化了维护期间或处理虚拟机管理程序及其他环境时的警报管理。

批量解除警报有助于管理员高效管理其工作负载，并防止他们被大量警报淹没。

批量解除警报的步骤

1. 导航到“**警报**”>“**Citrix 警报**”选项卡。将显示警报。



2. 从“**源**”、“**类别**”、“**状态**”或“**时间段**”中选择一个选项以筛选要解除的警报。将显示特定警报。
3. 选择特定警报旁边的复选框，或选择顶部的复选框以选择所有警报。
4. 单击“**解除**”。将显示一条通知以确认解除警报。
5. 单击“**是**”。选定的警报将标记为“*已解除*”，并且警报状态将相应更新。

使用 PowerShell SDK 配置 Webhook

使用 PowerShell SDK 的 Webhook 配置功能允许管理员创建、修改、删除和列出 Webhook 配置文件。此功能通过允许指定标头、身份验证类型、内容类型、有效负载和 Webhook URL，为配置 Webhook 提供了灵活性。

> **注意：**

> 支持的有效负载格式是文本，最终用户必须在其 Webhook 中启用文本。

> 最新的有效负载格式为：

```
{"text": "This is a message from a Webex incoming webhook."}
```

创建 Webhook

您可以使用以下 PowerShell 示例命令创建 Webhook 配置文件：

创建不带授权标头的 Webhook：

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$payloads = '{ "text": "$PAYLOAD" }'


$url = "<Fill this field with the required URL>"


Add-MonitorWebhookProfile -Name "profile_slack" -Description "webhook
profile for slack" -Url $url -Headers $headers -PayloadFormat $payloads
```

创建带授权标头的 Webhook：

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")

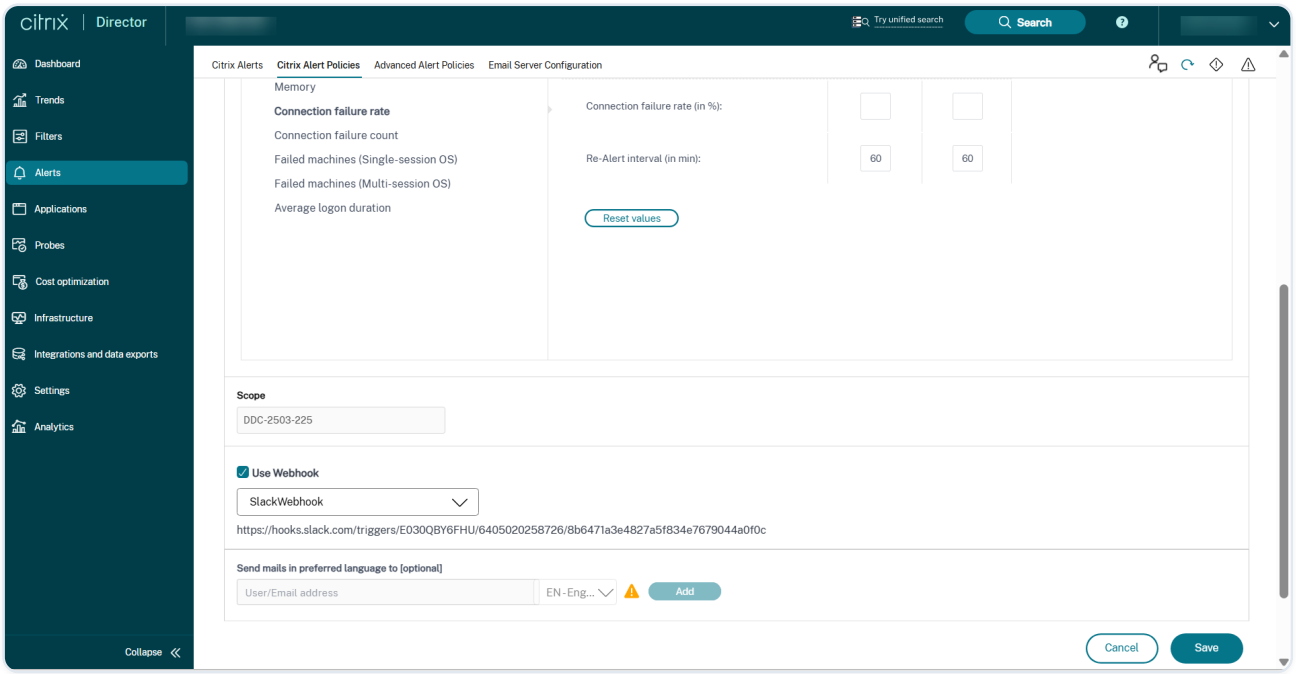

$headers.Add("Authorization", "Basic <Fill this field with the
authorization token>")


$payloads = '{ "text": "$PAYLOAD" }'


$url = "<Fill this field with the required URL>"
```

```
Add-MonitorWebhookProfile -Name "profile_azure" -Description "webhook
profile for azure function with Authentication" -Url $url -Headers
$headers -PayloadFormat $payloads
```

创建配置文件后，您可以在数据库中进行检查。此外，您还可以在“**Citrix 警报**”页面中找到新创建的 Webhook 配置文件。



更新 Webhook 配置文件

您可以使用以下 PowerShell 示例命令更新 Webhook 配置文件：

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$payloads = '{ "text": "$PAYLOAD" }'


$url =  "<Fill this field with the required URL>"
```

```
Set-MonitorWebhookProfile -Uid 1  -Name "profile_slack_citrix"
-Description "webhook profile for citrix slack" -Url $url -Headers
$headers -PayloadFormat $payloads
```

获取所有 Webhook 配置文件列表

您可以使用以下 PowerShell 示例命令获取所有可用的 Webhook 配置文件列表：

```
Get-MonitorWebhookProfile



Get-MonitorWebhookProfile -Name 'profile_msteams'



Get-MonitorWebhookProfile -Uid 1
```

删除 Webhook 配置文件

您可以使用以下 PowerShell 示例命令删除 Webhook 配置文件：

```
Remove-MonitorWebhookProfile -Uid 1
```

注意：

如果 Webhook 配置文件已映射到任何策略，则无法将其删除。作为一种解决方法，您必须首先从策略中删除 Webhook 映射。

使用 Webhook 配置文件创建策略

您可以使用以下 PowerShell 示例命令创建包含 Webhook 配置文件的策略：

```
New-MonitorNotificationPolicy -Name "Policy1" -Description "Policy
Description" -Enabled $true -WebhookProfileId 1
```

使用 Webhook 配置文件更新策略

您可以使用以下 PowerShell 示例命令更新包含 Webhook 配置文件的策略：

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 1
```

从策略中删除 Webhook 映射

您可以使用以下 PowerShell 示例命令从策略中删除 Webhook 配置文件：

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 0
```

测试 Webhook 配置文件

您可以使用以下 PowerShell 示例命令测试 Webhook 配置文件：

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$headers.Add("Authorization", "Basic <Fill this with authorization
token>")

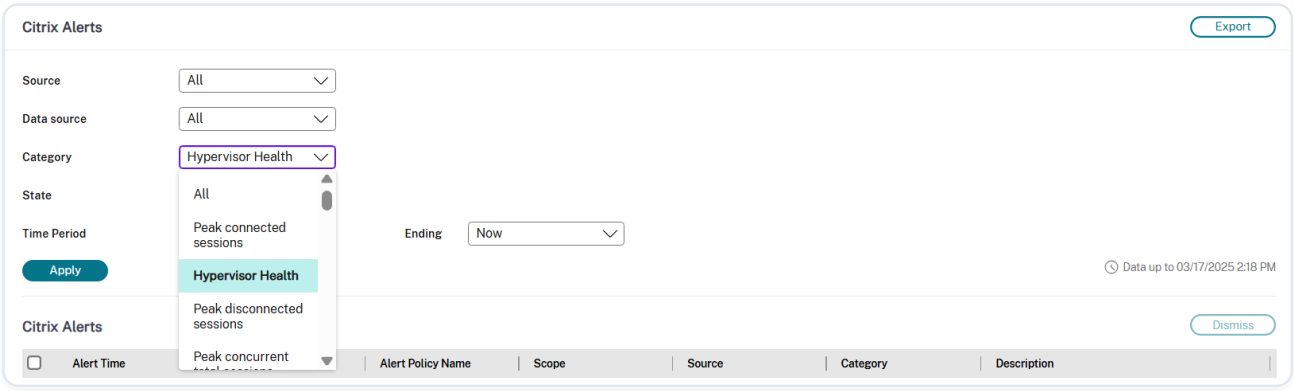

$payloads = '{ "text": "$PAYLOAD" }'


$url ="<Fill this field with the required URL>"


Test-MonitorWebhookProfile -Url $url -Headers $headers -PayloadFormat
$payloads
```

管理程序警报监控

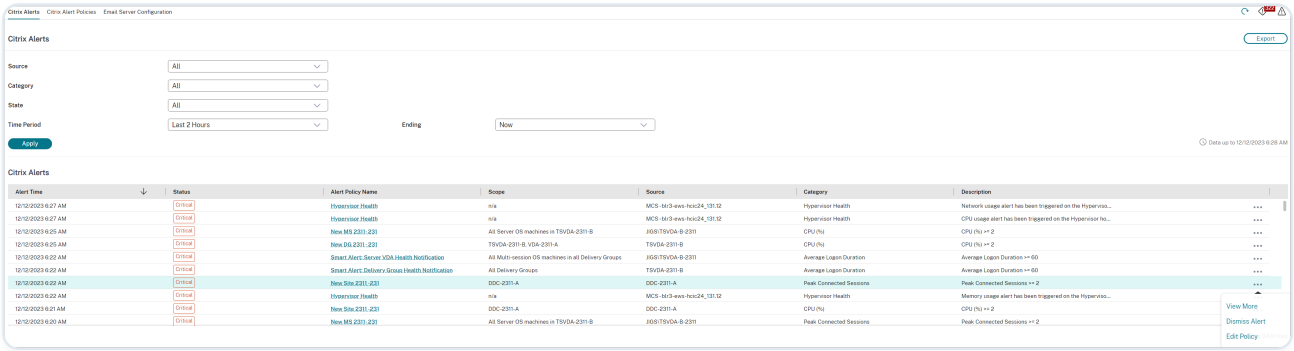
Director 显示警报以监视管理程序运行状况。来自 XenServer® 和 VMware vSphere 的警报有助于监视管理程序参数和状态。还会监视与管理程序的连接状态，以便在群集或主机池重新启动或不可用时提供警报。



要接收管理程序警报，请确保在 Web Studio 中创建了托管连接。有关详细信息，请参阅连接和资源。仅监视这些连接以获取管理程序警报。

达到或超出阈值后，将显示这些警报。管理程序警报可以是：

- 严重—已达到或超过管理程序警报策略的严重阈值
- 警告—已达到或超过管理程序警报策略的警告阈值
- 已解除—警报不再显示为活动警报



此功能需要 Delivery Controller 7 1811 或更高版本。如果您使用的是旧版 Director，但站点版本为 7 1811 或更高版本，则仅显示管理程序警报计数。要查看警报，必须升级 Director。

下表描述了管理程序警报的各种参数和状态。

警报	支持的管理程序	触发条件	条件	配置
CPU 使用率	Xen 服务器, 威睿 vSphere	管理程序	达到或超出 CPU 使用率警报阈值	警报阈值必须在管理程序中配置。
内存使用情况	Xen 服务器, 威睿 vSphere	管理程序	内存使用情况警报阈值已达到或超出	警报阈值必须在管理程序中配置。

警报	支持的管理程序	触发条件	条件	配置
网络使用情况	Xen 服务器, 威睿 vSphere	管理程序	网络使用情况警报阈值已达到或超出	警报阈值必须在管理程序中配置。
磁盘使用情况	威睿 vSphere	管理程序	磁盘使用情况警报阈值已达到或超出	警报阈值必须在管理程序中配置。
主机连接或电源状态	威睿 vSphere	管理程序	管理程序主机已重新启动或不可用	警报在 VMware vSphere 中预先构建。无需额外配置。
管理程序连接不可用	Xen 服务器, 威睿 vSphere	交付控制器	与管理程序（池或群集）的连接已丢失、已断电或已重新启动。只要连接不可用，此警报就会每小时生成一次。	警报已与 Delivery Controller 预先构建。无需额外配置。

注意：

有关配置警报的更多信息，请参阅 Citrix XenCenter 警报 或查看 VMware vCenter 警报文档。

电子邮件通知首选项可以在 **Citrix Alerts Policy > Site Policy > Hypervisor Health** 下配置。Hypervisor 警报策略的阈值条件只能从 hypervisor 配置、编辑、禁用或删除，而不能从 Director 配置、编辑、禁用或删除。但是，可以在 Director 中修改电子邮件首选项和关闭警报。如果您的角色不涉及基础结构监视，则可以禁用警报。

重要提示：

- Hypervisor 触发的警报会在 Director 中获取并显示。但是，Hypervisor 警报生命周期/状态的更改不会反映在 Director 中。

- 在 Hypervisor 控制台中处于正常、已关闭或已禁用状态的警报会继续显示在 Director 中，并且必须明确关闭。
- 在 Director 中关闭的警报不会在 Hypervisor 控制台中自动关闭。

改进了纵向和横向负载平衡警报的处理

以前，当您将 `UseVerticalScalingForRdsLaunches` 设置为 true 并在 Studio 中配置了“最大会话数”策略时，计算机将进入“最大容量”状态。Director 会针对“最大容量”触发警报，无论该限制是由于纵向还是横向负载平衡而达到。在遇到特定错误（例如“达到最大负载”）时，无法区分纵向和横向负载平衡。这会导致在纵向扩展场景中针对预期行为发出不必要的警报，浪费您的时间并造成混淆。

现在，当纵向负载平衡处于活动状态并且计算机达到其会话限制时，它会进入新状态：“纵向扩展的最大容量”。Director 不再为此新状态生成警报。警报仅在横向扩展场景中针对“最大容量”触发。您可以在“筛选器”和“自定义报告”页面中查看新状态，从而更容易区分预期条件和异常条件。此增强功能可帮助您避免不必要的警报并专注于实际问题，从而简化监视和故障排除。当您使用 Set-BrokerSite 配置 `UseVerticalScalingForRdsLaunches` 并在 Studio 中设置“最大会话数”策略时，此功能适用。

应用程序使用情况监控

Citrix Director 可帮助您监控以下内容的使用情况：

- 在虚拟桌面会话中启动的应用程序（也称为本地应用程序）
- 直接从 Citrix Workspace™ 应用程序会话启动的应用程序（也称为已发布的应用程序）

应用程序使用情况报告可让您了解使用最多、最少和未使用的应用程序。使用最多的应用程序显示在控制板上，并包含精选图表。这些图表可帮助 IT 管理员或应用程序管理员深入了解哪些应用程序使用频繁以及其使用程度。

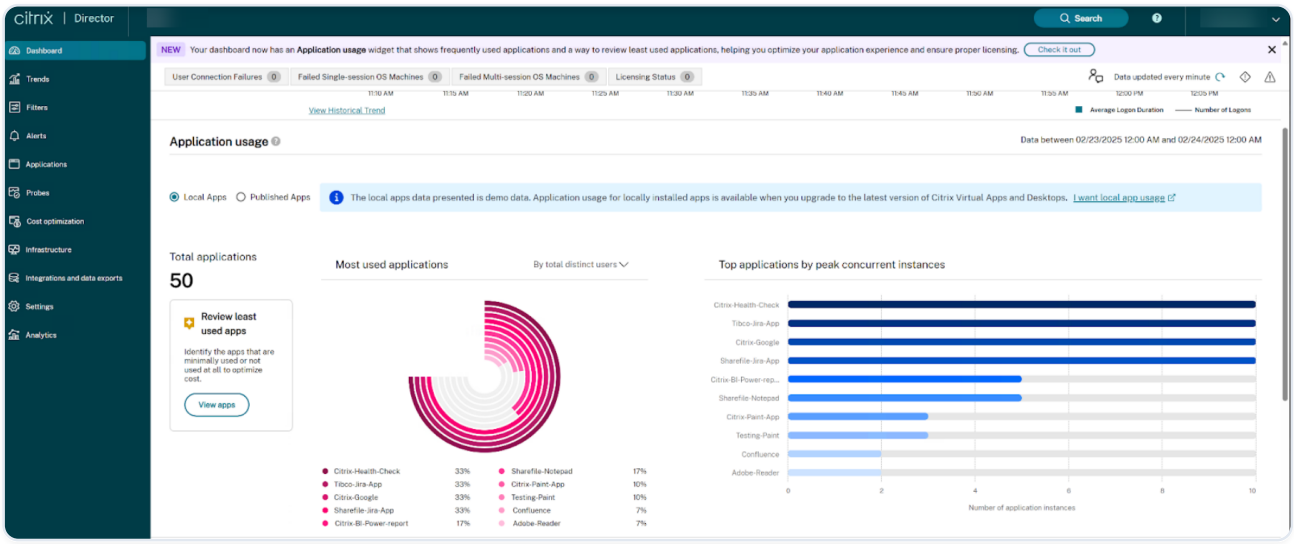
注意：

- 此功能仅适用于白金许可站点。
- uberAgent 必须与 Director 集成才能监控本地应用程序的使用情况。有关详细信息，请参阅 Citrix uberAgent 与 Director 集成。
- 如果您的环境同时以已发布的应用程序和桌面内已安装的应用程序（本地应用程序）的形式交付同一应用程序，您可能会在已发布的应用程序和本地应用程序报告中看到该应用程序。

> 借助此功能，管理员可以查看哪些本地和已发布的应用程序使用最多。利用这些数据，管理员可以深入了解使用程度。管理员可以通过以下数据点分析过去 24 小时内热门应用程序的详细信息：

- 应用程序总数 - 标识企业站点中所有用户正在使用的应用程序总数。
- 按不同用户总数计算的使用最多的应用程序 - 标识按唯一用户总数计算的前 10 个应用程序。
- 按应用程序启动总数计算的使用最多的应用程序 - 标识按应用程序启动总数计算的前 10 个应用程序。
- 峰值并发应用程序实例数 - 标识按每个应用程序使用情况的最高并发实例数计算的前 10 个应用程序。此信息为您提供了所列应用程序的最大需求。

此图表位于“控制板”页面的底部。但是，您可以单击屏幕顶部的 **Check it out** 直接访问该图表。



您还可以单击 **View all app usage** 查看单个应用程序的详细信息。此链接将打开 **Trends** > **Capacity Management** > **Hosted Application Usage** 页面。

该图表提供了应用程序使用情况的可视化表示。此外，当您将鼠标悬停在图表上时，您会获得所选数据点的相应绝对计数。当您单击图表上的任何数据点时，将打开 **Trends** > **Capacity Management** > **Hosted Application Usage** 页面，并选中特定的应用程序名称。此数据旨在表示与企业系统中所有应用程序的比较值。数据点的绝对值也在此悬停中单独提及。

使用最少和未使用的应用程序报告

在大型 Citrix Virtual Apps and Desktops™ 环境中，通常会有许多未充分利用的应用程序。为了优化您的环境，**应用程序**页面现在提供额外的指标，以帮助您了解组织内的应用程序使用模式，并做出数据驱动的决策，以改进资源分配和节省成本。

主要功能

- **详细使用信息：**查看独立用户（最近 30 天）、总启动次数、并发实例峰值以及每个应用程序随时间变化的独立用户趋势图。
- **数据焦点：**分析过去 7 天、30 天或 90 天的应用程序使用模式，以评估应用程序的必要性。建议查看 90 天的数据，因为它提供了季度数据，让您可以观察应用程序使用情况是波动还是保持一致。X 轴上的日期有助于将组织事件与使用趋势关联起来，以确定下降是否在预期之中。这些数据使管理员能够通过消除不必要的应用程序来维护高效的环境。
- **优化：**识别已发布的应用程序总数、使用最少的应用程序和未使用的应用程序，以优化您的 Citrix 部署。
- **可操作数据：**做出数据驱动的决策，辅助应用程序管理，以优化资源分配和许可证管理。
- **导出数据：**以 PDF 或 CSV 格式导出数据以进行进一步分析。您还可以使用 Power BI 集成或通过应用程序使用情况进行 ODATA 查询来导出数据。

要求

- Delivery Controllers 版本 7.16 或更高版本
- VDA 版本 7.15 或更高版本

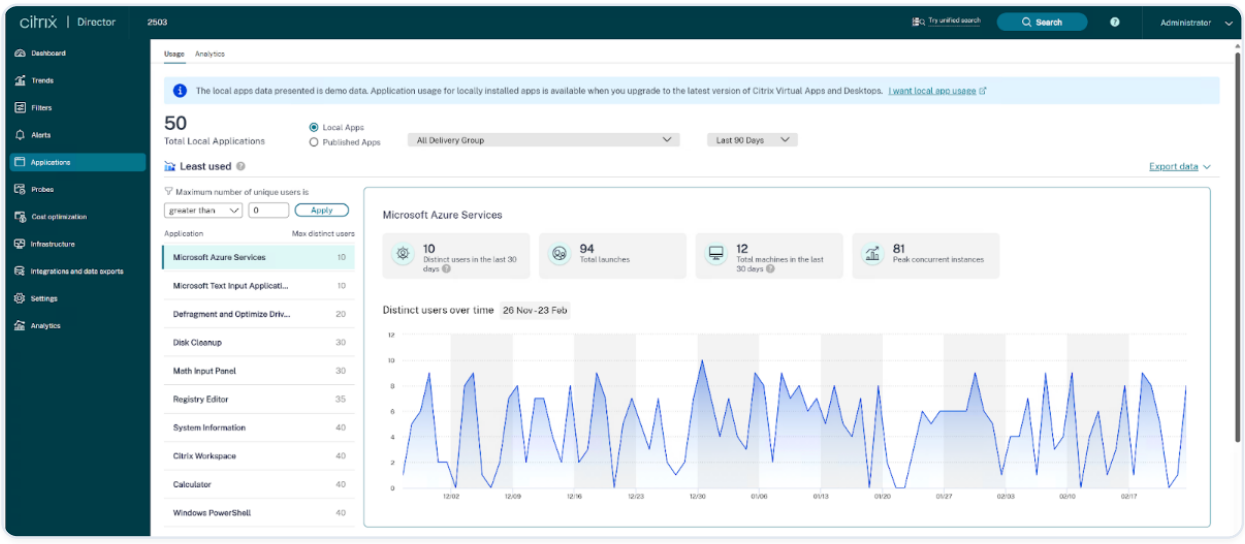
查看应用程序使用详情

1. 在控制板上的**查看使用最少的应用程序**部分中，单击**查看应用程序**链接。

   或者，

   单击**应用程序**选项卡。将显示以下页面：

   选择**本地应用程序**选项时：



   选择**已发布的应用程序**选项时：

应用程序选项卡(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-app-analytics-published.png)

2. 选择所需的交付组。
3. 选择所需的时间段。（注意：为获得最佳分析效果，默认值为最近 90 天。）

   显示以下信息：

   - **本地和已发布的应用程序总数：**显示本地和已发布的应用程序总数。
   - **使用最少：**显示在选定时间内唯一用户最少的应用程序。计算方法如下：

     a. **每日用户数：**每天统计每个应用程序的唯一用户数。

     b. **每日峰值使用量：**识别每个应用程序的最高每日用户数。

     c. **最高总使用量：**确定在选定时间范围内每个应用程序的最高用户数。

     d. **升序：**应用程序根据其最高总用户数按升序排列，从用户数最少的应用程序开始。

     > **注意：**
     >
     > 建议选择最近 90 天作为分析周期。此时间范围提供了一个季度的数据，并能全面了解应用程序的使用模式。但是，也可以选择按七天和一个月进行筛选。

   - **未使用：**列出过去 90 天内未启动过一次的应用程序。提供了交付这些应用程序的交付组、应用程序版本及其上次使用的确切时间戳。此信息有助于管理员在从虚拟桌面中删除应用程序之前做出明智的决定。

     应用程序选项卡 - 未使用(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-app-analytics-not-used.png)

4. 从**使用最少**类别中选择一个应用程序以查看详细使用信息，包括：

   - **过去 30 天内的独立用户：**显示在过去 30 天内访问该应用程序的独立用户数。如果您筛选七天，此指标将显示所选应用程序在这七天内的独立用户数。

   > **注意：**
   >
   > 即使您选择 90 天，此指标仍仅显示过去 30 天的数据。

   - **总启动次数：** 显示应用程序启动的次数。

- **过去 30 天内的计算机总数**：显示过去 30 天内安装的计算机数量。此指标仅在您查看本地应用程序详细信息时显示。
- **并发实例峰值：** 显示同时运行的实例的最高数量。
- **趋势图：** 查看显示所选应用程序随时间变化的独立用户数量的趋势图。单击**查看详细信息**可在**容量管理 > 托管应用程序使用情况**部分查看更多信息。

趋势图的使用

趋势图说明了使用模式，有助于识别所选时间段内的趋势以及低使用率或高使用率时期。X 轴表示天数，Y 轴表示随时间变化的独立用户数量。通过分析这些指标和使用模式图，管理员可以自信地优化其 Citrix Virtual Apps and Desktops™ 环境。

您可以通过以下方式使用趋势图：

- **将鼠标悬停在数据点上：** 查看所选时间段内的独立用户数量。
- **查看趋势：** 识别使用模式并确定应用程序使用情况是持续的还是只是暂时的峰值。此图表有助于管理员监控员工活动并识别潜在问题或改进领域。例如，如果员工休假，该期间可能没有应用程序使用情况。一旦员工返回，应用程序使用情况就会增加。该时间段的默认筛选器是 90 天，这有助于管理员进行这些计算。
- **查看详细信息：** 查看日期和相应的独立用户数量。
- **筛选选项：** 选择不同的“时间段”筛选选项以查看相应数据。

筛选数据以排查故障

当您单击仪表板上的数字或从“筛选器”菜单中选择预定义筛选器时，“筛选器”视图将打开以显示基于所选计算机或故障类型的数据。

预定义筛选器无法编辑，但您可以将预定义筛选器另存为自定义筛选器，然后对其进行修改。此外，您还可以创建跨所有交付组的计算机、连接、会话和应用程序实例的自定义筛选视图。

1. 选择一个视图：
    - **计算机**。选择单会话操作系统计算机或多会话操作系统计算机。这些视图显示已配置的计算机数量。多会话操作系统计算机选项卡还包括负载评估器索引，该索引指示性能计数器的分布以及将鼠标悬停在链接上时会话计数的工具提示。
    - **会话**。按不同的时间段筛选会话，包括最近 60 分钟、最近 24 小时、最近 7 天或自定义时间段。您还可以从“会话”视图中查看会话计数。使用空闲时间测量值来识别空闲时间超过阈值时间段的会话。单击**关联用户**可为该用户打开“活动管理器”。单击**端点**名称可为该端点打开“活动管理器”。单击**查看详细信息**可分别打开**用户详细信息**或**端点详细信息**页面。有关详细信息，请参阅用户详细信息。

- **连接**。按不同的时间段筛选连接，包括最近 60 分钟、最近 24 小时、最近 7 天或自定义时间段。
- **应用程序实例**。按不同的时间段筛选应用程序实例，包括最近 60 分钟、最近 24 小时、最近 7 天或自定义时间段。此视图显示服务器和单会话操作系统 VDA 上所有应用程序实例的属性。多会话操作系统 VDA 上的应用程序实例提供会话空闲时间测量值。

> **注意：**
>
> 如果您在安装了 Windows 10 1809 计算机的 VDA 上启动了桌面会话，Director 中的“活动管理器”有时可能会将 Microsoft Edge 和 Office 显示为正在主动运行的应用程序，而实际上它们仅在后台运行。

2. 对于**筛选依据**，选择条件。
3. 根据需要，使用每个视图的附加选项卡来完成筛选。
4. 根据需要选择额外的列，以进一步排查故障。
5. 保存并命名您的筛选器。
6. 要从多个 Director 服务器访问筛选器，请将筛选器存储在可从这些服务器访问的共享文件夹中：
   - 共享文件夹必须对 Director 服务器上的帐户具有修改权限。
   - 必须将 Director 服务器配置为访问共享文件夹。要进行配置，请运行 **IIS 管理器**。在**站点 > 默认网站 > Director > 应用程序设置**中，修改 **Service.UserSettingsPath** 设置以反映共享文件夹的 UNC 路径。
7. 要稍后打开筛选器，请从**筛选器**菜单中选择筛选器类型（计算机、会话、连接或应用程序实例），然后选择已保存的筛选器。
8. 单击**导出**可将数据导出为 CSV 格式文件。最多可导出 100,000 条记录的数据。此功能在 Delivery Controller™ 1808 版及更高版本中可用。
9. 如果需要，对于**计算机**或**连接**视图，请对筛选列表中选择的所有计算机使用电源控制。对于“会话”视图，请使用会话控制或发送消息选项。
10. 如果需要，您可以使用多个操作。您会看到操作进度的进度条。此外，操作完成后会收到一条消息。
11. 在“**计算机**”和“**连接**”视图中，单击发生故障的计算机或连接的“**故障原因**”以获取故障的详细说明以及建议的故障排除操作。计算机和连接故障的故障原因以及建议的操作可在Citrix Director 故障原因和故障排除中找到。

12. 在“**计算机**”视图中，单击计算机名称链接以转到相应的“**计算机详细信息**”页面。此页面显示计算机的详细信息，提供电源控制，并显示 CPU、内存、磁盘监视和 GPU 监视图表。此外，单击“**查看历史利用率**”以查看计算机的资源利用率趋势。有关详细信息，请参阅对计算机进行故障排除。
13. 在“**应用程序实例**”视图中，根据大于阈值时间段的“**空闲时间**”进行排序或筛选。选择要结束的空闲应用程序实例。注销或断开应用程序实例会结束同一会话中的所有活动应用程序实例。有关详细信息，请参阅对应用程序进行故障排除。如果 Director、交付控制器和 VDA 的版本为 7.13 或更高版本，则可以使用“应用程序实例”筛选页面和“会话”筛选页面中的空闲时间度量。

注意：

Web Studio 允许将多个桌面分配规则 (DAR) 分配给交付组中单个 VDA 的不同用户或用户组。StoreFront™ 根据登录用户的 DAR 显示具有相应显示名称的已分配桌面。但是，Director 不支持 DAR，并且无论登录用户是谁，都使用交付组名称显示已分配的桌面。因此，您无法在 Director 中将特定桌面映射到计算机。要将 StoreFront 中显示的已分配桌面映射到 Director 中显示的交付组名称，请使用以下 PowerShell 命令：

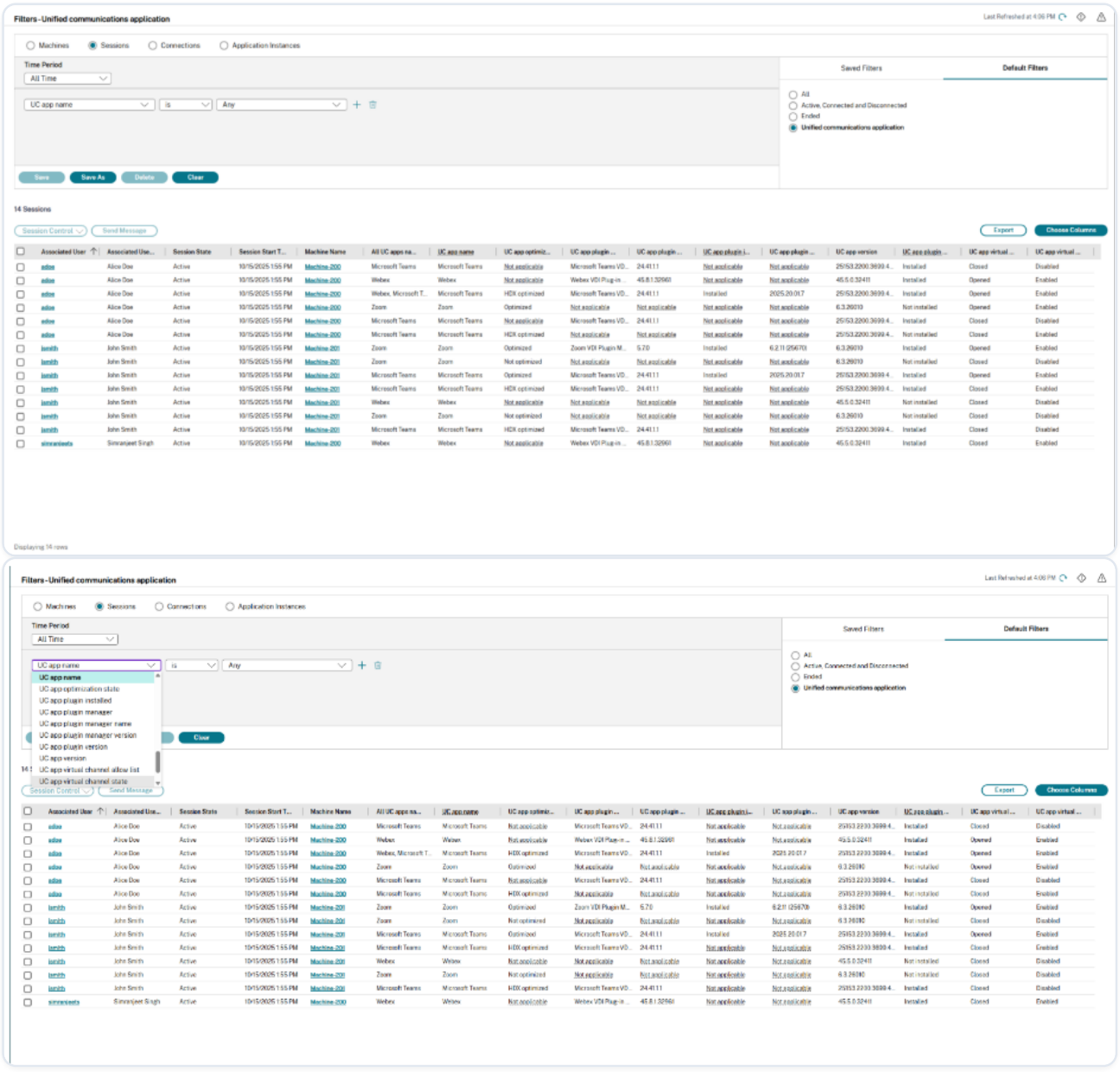
```
Get-BrokerDesktopGroup | Where-Object { $_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $_.PublishedName -eq "<Name on
StoreFront>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

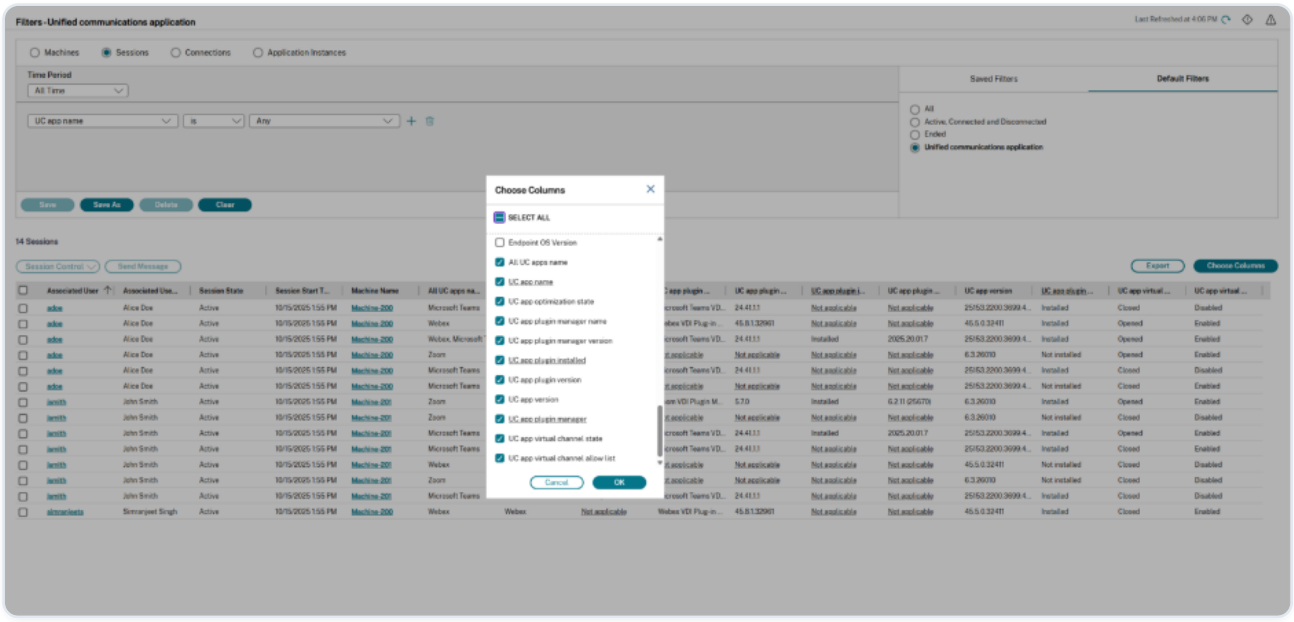
统一通信应用程序指标

“会话”视图现在包含几个新的显示列，这些列提供了用户会话中统一通信 (UC) 应用程序使用情况的详细见解。这些指标可在筛选器中使用，以优化会话列表，也可以通过“**选择列**”选项选择在主会话表视图中显示。

- **所有 UC 应用程序名称（仅限列）：** 包含同时在会话中运行的所有多个 UC 应用程序的数据列表。这是一个显示列，而不是筛选选项。
- **UC 应用程序名称：** 特定统一通信应用程序的名称（例如，Microsoft Teams、Webex、Zoom）。
- **UC 应用程序优化状态：** 会话中 UC 应用程序的优化状态（例如，已优化、HDX 优化、未优化、不适用）。
- **UC 应用程序插件管理器名称：** 用于 UC 应用程序的插件管理器名称。
- **UC 应用程序插件管理器版本：** 正在使用的插件管理器版本。
- **UC 应用程序插件已安装：** 指示 UC 应用程序是否已安装或未安装必要的应用程序插件。

- **UC 应用程序插件版本：** 特定 UC 应用程序插件的版本。
- **UC 应用程序版本：** 统一通信应用程序的总体版本。
- **UC 应用程序插件管理器：** 指示 UC 应用程序所需的应用程序插件管理器是否已安装在端点上。
- **UC 应用程序虚拟通道状态：** 为 UC 应用程序建立的虚拟通道的状态（例如，已打开、已关闭）。
- **UC 应用程序虚拟通道允许列表：** 指示应用程序的虚拟通道是否在允许列表中。





监视站点的历史趋势

“趋势”视图访问每个站点的以下参数的历史趋势信息：

- 会话
- 连接失败
- 计算机故障
- 登录性能
- 负载评估
- 容量管理
- 计算机使用情况
- 资源利用率
- 每个站点的网络分析。

要查找此信息，请单击“**趋势**”菜单。

放大钻取功能允许您通过放大某个时间段（单击图表中的数据点）并向下钻取以查看与趋势相关的详细信息来浏览趋势图表。此功能使您能够更好地了解受影响的人员或内容的详细信息。

要更改每个图表的默认范围，请对数据应用不同的筛选器。

选择您需要历史趋势信息的时间段。时间段的可用性取决于您的 Director 部署，具体如下：

- 最长可达去年（365天）的趋势报告可在高级版许可站点中获取。
- 最长可达上个月（31天）的趋势报告可在增强版许可站点中获取。

- 最长可达最近7天的趋势报告可在非高级版和非增强版许可站点中获取。

注意：

- 在所有 Director 部署中，当时间段设置为上个月（**截至当前**）或更短时，会话、故障和登录性能趋势信息以图表形式提供。对于选择为具有自定义结束日期的上个月或去年的时间段，趋势信息以图表形式提供，而非表格形式。
- Monitor Service 的清理保留值控制趋势数据的可用性。默认值可在数据粒度和保留中获取。高级版许可站点的客户可以将其清理保留更改为所需的保留天数。
- IIS Manager 中的以下参数控制可供选择的自定义结束日期范围。但是，所选日期的数据可用性取决于正在测量的特定指标的清理保留设置。

参数	默认值
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

可用趋势

查看会话趋势： 在**会话**选项卡中，选择交付组和时间段，以查看有关并发会话计数的更详细信息。

会话自动重新连接列显示会话中自动重新连接的次数。当会话可靠性或客户端自动重新连接策略生效时，将启用自动重新连接。当端点上发生网络中断时，以下策略将生效：

- 会话可靠性生效（默认情况下为 3 分钟），在此期间，Citrix Receiver™ 或 Citrix Workspace™ 应用程序会尝试连接到 VDA。
- 客户端自动重新连接在 3 到 5 分钟内生效，在此期间，客户端会尝试连接到 VDA。

两次重新连接都会被捕获并显示给用户。重新连接发生后，此信息最多可能需要 5 分钟才能显示在 Director UI 上。

自动重新连接信息可帮助您查看和排查存在中断的网络连接。它还可以分析具有无缝体验的网络。您可以查看在筛选器中选择的特定交付组或时间段的重新连接次数。向下钻取可提供其他信息，例如会话可靠性或客户端自动重新连接、时间戳、端点 IP 以及安装了 Workspace 应用程序的计算机的端点名称。

默认情况下，日志按事件时间戳降序排序。此功能适用于适用于 Windows 的 Citrix Workspace 应用程序、适用于 Mac 的 Citrix Workspace 应用程序、适用于 Windows 的 Citrix Receiver 和适用于 Mac 的 Citrix Receiver。此功能需要 Delivery Controller™ 7 1906 或更高版本以及 VDA 1906 或更高版本。

有关会话重新连接的详细信息，请参阅会话。

有关策略的详细信息，请参阅客户端自动重新连接策略设置和会话可靠性策略设置。

有时，自动重新连接数据可能不会在 Director 中显示，原因如下：

- Workspace 应用程序未将自动重新连接数据发送到 VDA。
- VDA 未将数据发送到监视服务。
- Delivery Controller 会丢弃 VDA 有效负载，因为它们可能没有相应的会话。

> **注意：**
>
> 有时，如果设置了某些 Citrix Gateway 策略，则可能无法正确获取客户端 IP 地址。

> **查看连接失败趋势：** 在“失败”选项卡中，选择连接、计算机类型、失败类型、交付组和时间段，以查看包含有关站点中用户连接失败的更详细信息的图表。

查看计算机故障趋势： 在**单会话操作系统计算机故障**选项卡或多会话操作系统计算机选项卡中，选择故障类型、交付组和时间段，以查看包含站点中计算机故障详细信息的图表。

查看登录和重新连接性能趋势： 在登录和重新连接性能选项卡中，选择交付组和时间段，以查看包含站点中用户登录和重新连接持续时间详细信息的图表。此视图可帮助您了解登录或重新连接的数量以及整体性能。

图表包括：

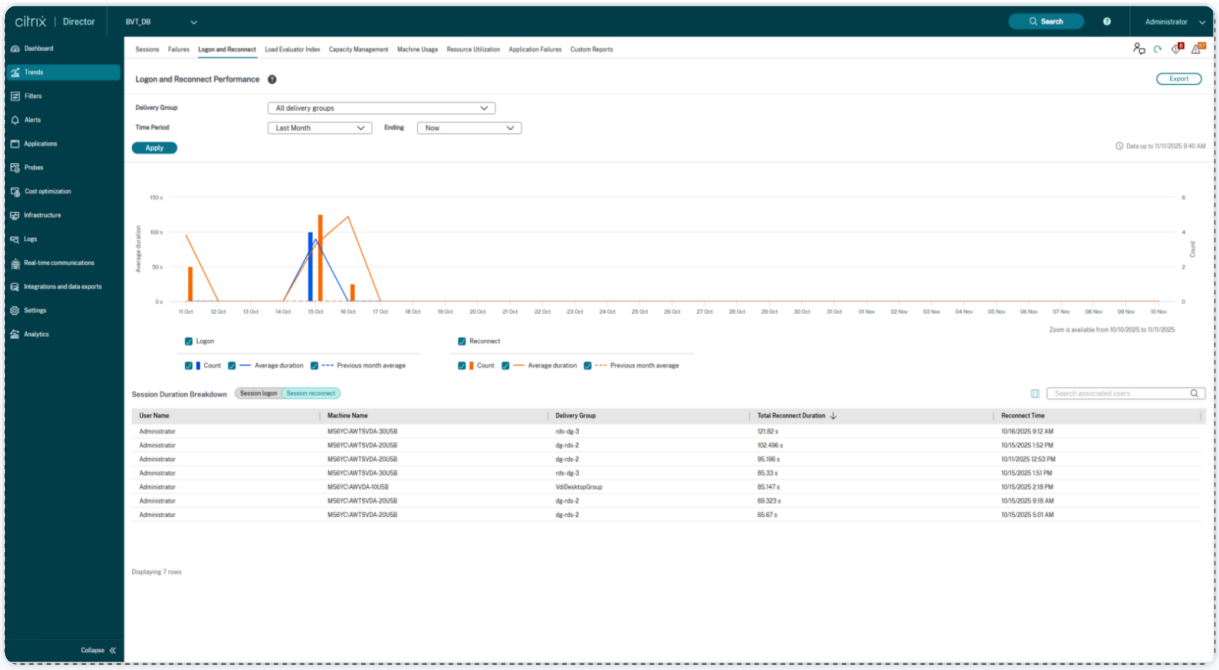
- **登录事件、登录持续时间和阶段**（例如代理、交互式会话等），提供启动新会话时的用户体验洞察。
- **重新连接事件和重新连接持续时间**，提供从断开连接的会话重新连接时的用户体验洞察。

使用图例根据正在分析的趋势选择所需的指标。

- 计数
- 平均持续时间
- 上一个（时间范围）平均值

图表下方的表格按用户会话或连接显示**会话登录**和**会话重新连接**详细信息。您可以使用表格上方的选择在指标之间切换，选择要显示的列，按任意列排序，并将报告导出为 PDF、Excel 或 CSV 格式。

> **注意：**
>
> 会话重新连接持续时间在 **Director 和 VDA 2511 CR 或更高版本**上受支持。



查看负载评估趋势： 在**负载评估器索引**选项卡中，查看包含多会话操作系统计算机之间负载分布详细信息的图表。此图表的筛选选项包括交付组或交付组中的多会话操作系统计算机、多会话操作系统计算机（仅当选择了交付组中的多会话操作系统计算机时可用）以及范围。

查看托管应用程序使用情况： 此功能的可用性取决于您的组织许可证。 在**容量管理**选项卡中，选择**托管应用程序使用情况**选项卡。选择交付组和时间段，以查看显示并发使用峰值的图表以及显示基于应用程序使用情况的表格。在“基于应用程序的使用情况”表格中，您可以选择特定的应用程序以查看详细信息以及正在使用或已使用该应用程序的用户列表。

查看单会话和多会话操作系统使用情况：“趋势”视图按站点和交付组显示单会话操作系统的使用情况。当您选择**站点**时，使用情况按交付组显示。当您选择交付组时，使用情况按用户显示。“趋势”视图还按站点、交付组和计算机显示多会话操作系统的使用情况。当您选择**站点**时，使用情况按交付组显示。当您选择交付组时，使用情况按计算机和用户显示。当选择计算机时，使用情况按用户显示。

查看虚拟机使用情况：在计算机使用情况选项卡中，选择**单会话操作系统计算机或多会话操作系统计算机**以实时查看您的 VM 使用情况，从而能够快速评估站点的容量需求。 单会话操作系统可用性 - 按整个站点或特定交付组的可用性显示单会话操作系统计算机 (VDI) 的当前状态。 多会话操作系统可用性 - 按整个站点或特定交付组的可用性显示多会话操作系统计算机的当前状态。

您可以单击显示的横幅上的以下链接，以通过**成本优化**更好地了解计算机使用情况：

- 预计节省 - 此链接将您定向到**成本优化**页面上的**预计节省**部分，其中显示了所有交付组的详细信息。
- 节省报告 - 此链接将您定向到**成本优化**页面上的**节省报告**部分，其中显示了所有交付组的详细信息。

> **注意：**

> 可用计数器中显示的计算机数量包括处于维护模式的计算机。

> **查看资源利用率：在资源利用率**选项卡中，选择**单会话操作系统计算机或多会话操作系统计算机**以深入了解每台 VDI 计算机的 CPU 和内存使用情况以及 IOPS 和磁盘延迟的历史趋势数据，从而更好地进行容量规划。 此功能需要 Delivery Controller 和 VDA **版本 7.11** 或更高版本。 图表显示了平均 CPU、平均内存、平均 IOPS、磁盘延迟和并发会话峰值的数据。您可以深入到计算机，查看占用 CPU 的前 10 个进程的数据和图表。

按交付组和时间段进行筛选。CPU、内存使用情况和并发会话峰值图表可用于过去 2 小时、24 小时、7 天、月和年。平均 IOPS 和磁盘延迟图表可用于过去 24 小时、月和年。您可以单击横幅上的**查看**链接，以通过成本优化更好地了解计算机使用情况。此链接会将您带到**成本优化**页面中的**工作负载调整**选项卡，其中显示了从**资源利用率**选项卡中选择的交付组的详细信息。

> **注意：**

- 必须将监视策略设置**启用进程监视**设置为**允许**，才能在历史计算机利用率页面上的“前 10 个进程”表中收集和显示数据。默认情况下，此策略设置为**禁止**。默认情况下会收集所有资源利用率数据。可以使用**启用资源监视**策略设置禁用此功能。图表下方的表格显示了每台计算机的资源利用率数据。有关详细信息，请参阅监视策略设置。
- 平均 IOPS 显示每日平均值。峰值 IOPS 计算为所选时间范围内 IOPS 平均值的最高值。（IOPS 平均值是 VDA 上每小时收集的 IOPS 的每小时平均值）。
- 计算机深入分析列出了平均 CPU 或平均内存使用率超过 1% 的进程，这可能意味着有时列出的进程少于 10 个。

查看网络分析数据：此功能的可用性取决于您组织的许可证和您的管理员权限。此功能需要 Delivery Controller **版本 7.11** 或更高版本。

在**网络**选项卡中，监视您的网络分析，该分析提供了网络的上下文用户、应用程序和桌面视图。借助此功能，Director 通过 Citrix ADM 中的 HDX Insight 报告提供部署中 ICA 流量的高级分析。有关详细信息，请参阅配置网络分析

查看应用程序故障： 应用程序故障选项卡显示与 VDA 上已发布的应用程序相关的故障。

此功能需要 Delivery Controller 和 VDA **版本 7.15** 或更高版本。支持运行 Windows Vista 及更高版本的单会话操作系统 VDA，以及运行 Windows Server 2008 及更高版本的多会话操作系统 VDA。有关详细信息，请参阅历史应用程序故障监视。

默认情况下，仅显示来自多会话操作系统 VDA 的应用程序故障。您可以使用监视策略设置应用程序故障的监视。有关详细信息，请参阅监视策略设置。

查看探测结果：“**探测结果**”选项卡显示在“配置”页面中已配置探测的应用程序和桌面的探测结果。此处记录了发生故障的启动阶段。

有关详细信息，请参阅应用程序和桌面探测。

创建自定义报告：“自定义报告”选项卡提供了一个用户界面，用于生成包含监控数据库中实时和历史数据的自定义报告，并以表格形式显示。

此功能需要 Delivery Controllers **7.12 版**或更高版本。

从以前保存的自定义报告查询列表中，您可以单击“**运行并下载**”以 CSV 格式导出报告，单击“**复制 OData**”以复制并共享相应的 OData 查询，或者单击“**编辑**”以编辑查询。 您可以基于计算机、连接、会话或应用程序实例创建自定义报告查询。根据计算机、交付组或时间段等字段指定筛选条件。指

定自定义报告中所需的其他列。预览显示报告数据的示例。保存自定义报告查询会将其添加到已保存查询列表中。

您可以基于复制的 OData 查询创建自定义报告查询。为此，请选择 OData 查询选项并粘贴复制的 OData 查询。您可以保存生成的查询以供以后执行。

> **注意：**
>
> 使用 OData 查询生成的预览和导出报告中的列名未本地化，而是以英文显示。

> 图表上的标记图标指示该特定时间范围内的重要事件或操作。将鼠标悬停在标记上并单击以列出事件或操作。

> **注意：**
>
> - 对于早于 7 的 VDA，不收集 HDX™ 连接登录数据。对于较早的 VDA，图表数据显示为 0。
> - 在 Citrix Studio 中删除的交付组在 Director 趋势筛选器中仍可供选择，直到与其相关的数据被清除。选择已删除的交付组会显示可用数据的图表，直到保留期结束。但是，表格不显示数据。
> - 将包含活动会话的计算机从一个交付组移动到另一个交付组，会导致新交付组的“**资源利用率和负载评估器索引**”表格显示从旧交付组和新交付组整合的指标。

监控 Autoscale 管理的计算机

Autoscale 是一项电源管理功能，可对交付组中所有已注册的多会话和单会话操作系统计算机进行主动电源管理。您可以在 Web Studio 中为选定的交付组配置 Autoscale。有关详细信息，请参阅 Autoscale。 您可以使用 Director 监控已启用 Autoscale 的计算机的关键指标。

计算机使用情况

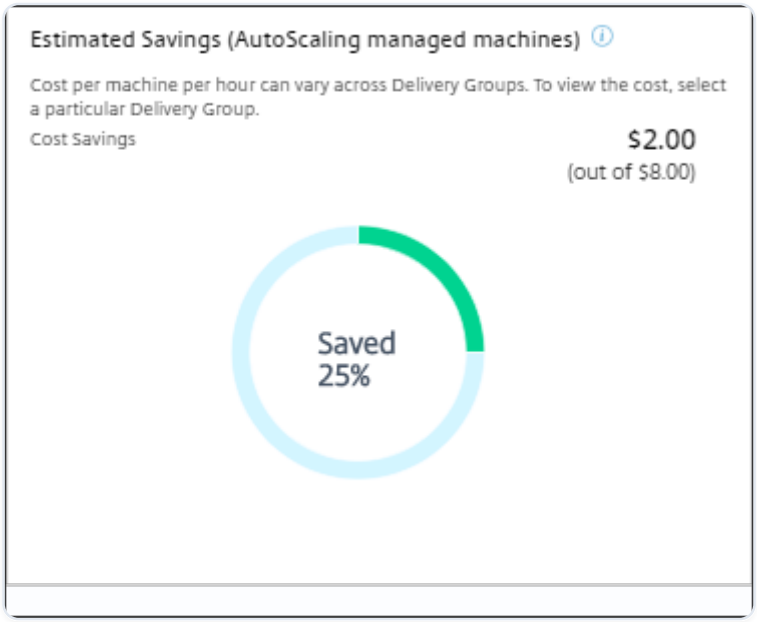
计算机使用情况页面显示在选定交付组和时间段内已开机的已启用 Autoscale 的多会话和单会话操作系统计算机的总数。此指标表示交付组中计算机的实际使用情况。 在**单会话操作系统计算机**或**多会话操作系统计算机**选项卡中，选择交付组和时间段。

图表绘制以下指标：

- **已开机计算机** - 已开机的已启用 Autoscale 的计算机数量
- **已注册计算机** - 已注册的多会话或单会话操作系统计算机的数量
- **维护模式下的计算机** - 已启用维护模式的多会话或单会话操作系统计算机的数量

预估节省

计算机使用情况页面还显示通过在选定交付组中启用 Autoscale 所实现的预估成本节省。



预估节省是根据在**编辑交付组** > **Autoscale**中配置的每台计算机每小时节省的百分比（以美元计）计算的。有关配置每台计算机节省的详细信息，请参阅 Autoscale。

当您选择所有交付组时，将显示所有交付组的预估节省平均值。

预估节省可帮助管理员整合现有基础结构并规划容量，以实现最大程度的节省和利用率。

计算机和会话的警报通知

Director 控制板显示可进一步深入查看的警报通知。警报详细信息显示在**警报**页面上。

- 要在交付组中创建警报策略，请转至 **警报** > **Citrix 警报策略** > **交付组策略**。
- 在此处，您可以设置以下警告和严重阈值：
  - 失败的计算机（单会话操作系统）和失败的计算机（多会话操作系统），
  - 交付组中的峰值连接会话、峰值断开连接会话和峰值并发总会话。
- 当交付组中的相应指标达到阈值时，将生成警报。

有关警报策略条件和创建新警报策略的更多详细信息，请参阅警报和通知。

计算机状态

- **筛选器** > **计算机** 以表格格式显示所有计算机的电源状态。您可以按特定交付组进行筛选。
- **筛选器** > **会话** 按计算机名称显示筛选器，以查看关联的会话及其实时状态。
- 在 **趋势** > **会话** 中，选择您的交付组和时间段，以查看会话及其关联指标的趋势。

有关详细信息，请参阅筛选数据以排查故障。

负载评估趋势

“**趋势** > **负载评估器索引**”页面显示一个图表，其中包含有关在多会话操作系统计算机之间分配的负载的详细信息。此图表的筛选选项包括交付组或交付组中的多会话操作系统计算机、多会话操作系统计算机（仅当选择了交付组中的多会话操作系统计算机时才可用）以及范围。负载评估器索引以总 CPU、内存、磁盘或会话的百分比形式显示，并与上一个间隔中连接的用户数进行比较。

实时通信仪表板

用于监视和故障排除的 Microsoft 呼叫质量仪表板

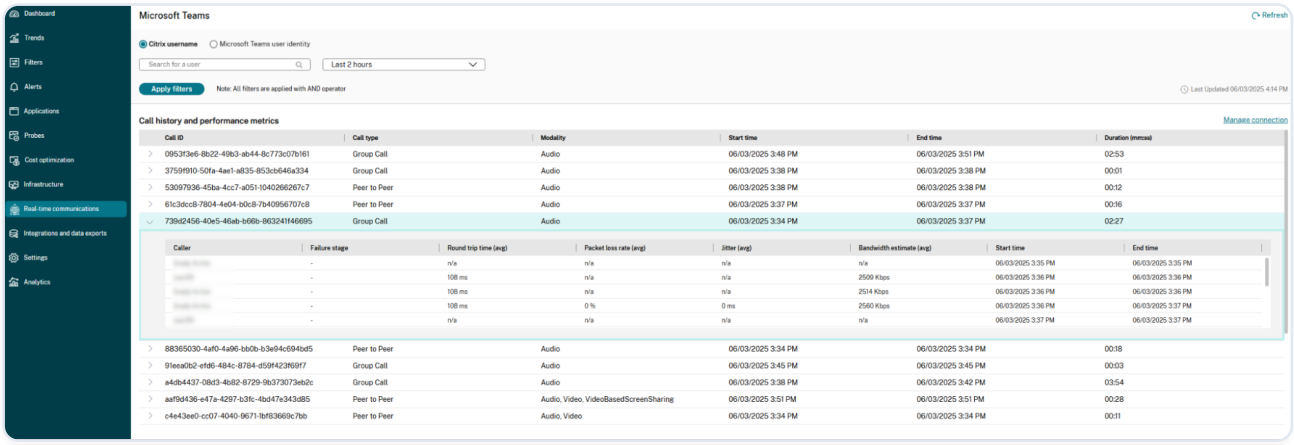
此功能通过使用 Microsoft Graph API 集成为管理员提供 Microsoft Teams 呼叫性能的统一视图，从而增强了 Citrix Director。它支持聚合监视和故障排除，通过简化 Citrix 中 Microsoft Teams 的 IT 运营来改善用户体验。

仪表板显示每个参与者会话的呼叫详细信息和质量指标。您可以区分常规呼叫、视频会议和其他协作会话。

微软团队

Citrix Director 中的 Microsoft Teams 控制板提供了跨用户的 Microsoft Teams 通话可见性，以及参与者详细信息和指示通话性能的指标。该控制板提供了以下功能：

- 评估 Microsoft Teams 使用情况摘要
- 筛选并查看所选持续时间的 Microsoft Teams 通话详细信息
- 使用性能指标评估单个通话



先决条件

将 Microsoft Graph 应用程序编程接口 (API) 添加到 Citrix Director 中的允许列表：

- 为了 Director 访问通话记录，请确保在所有安装了 Director 的计算机上都可进行出站互联网访问。具体来说，请确保 `<https://graph.microsoft.com>` URL 可访问
- 如果您使用代理服务器，请确保 Microsoft Graph API : `<https://graph.microsoft.com>` URL 可访问。

入门

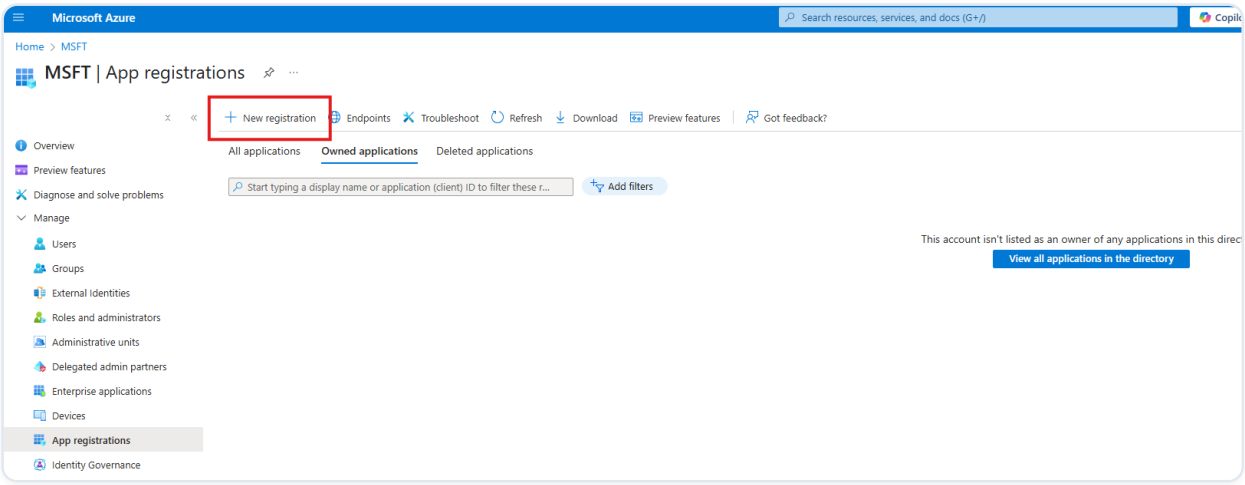
连接到 Microsoft Graph API

Microsoft 通话详细信息是从 Microsoft Graph API 中获取的。为了让 Citrix Director 访问该 API，需要在 Microsoft Entra ID 中创建一个具有所需权限的应用程序。Graph API URL 也需要添加到 Director 的允许列表中。

执行以下步骤以完成连接：

步骤 1：在 Microsoft Entra ID 中注册应用程序

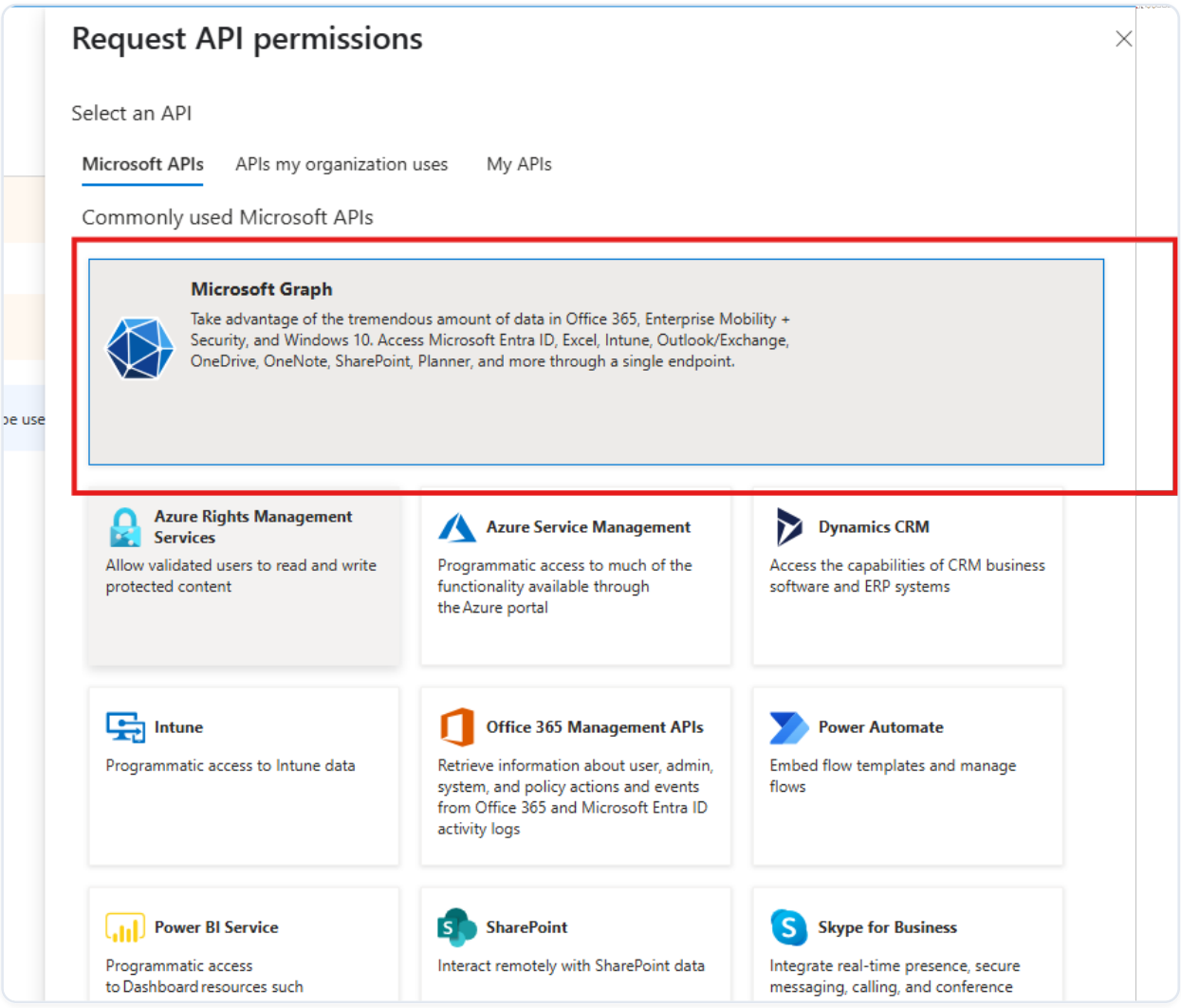
1. 在 Microsoft Entra ID 中导航到 **应用注册** -> **新注册**。



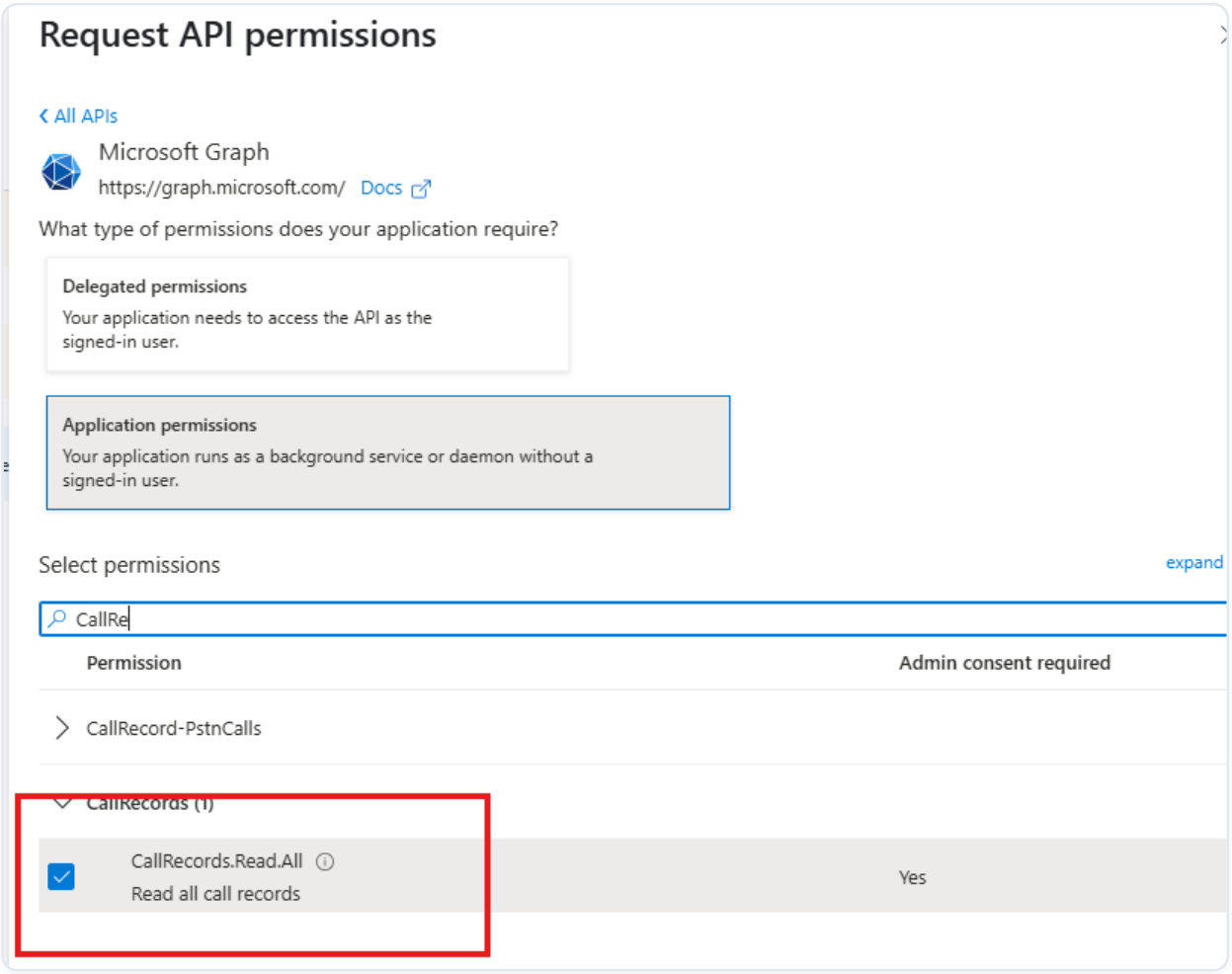
2. 执行应用程序注册所需的步骤。
3. 注册后，复制应用程序的客户端 ID 和租户 ID。

步骤 2：在 Microsoft Entra ID 中添加 Microsoft Graph 权限

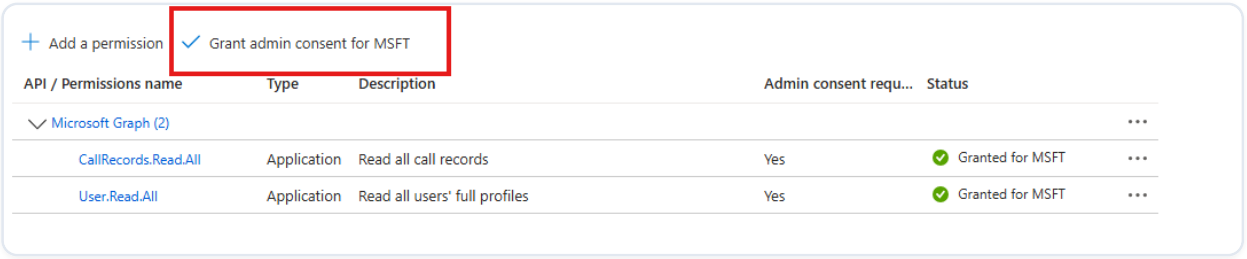
1. 导航到 **API 权限** -> **添加权限**。
2. 选择 **Microsoft Graph**，然后选择 **应用程序权限**。



3. 添加 **CallRecords.Read.All** 和 **User.Read.All** 的权限

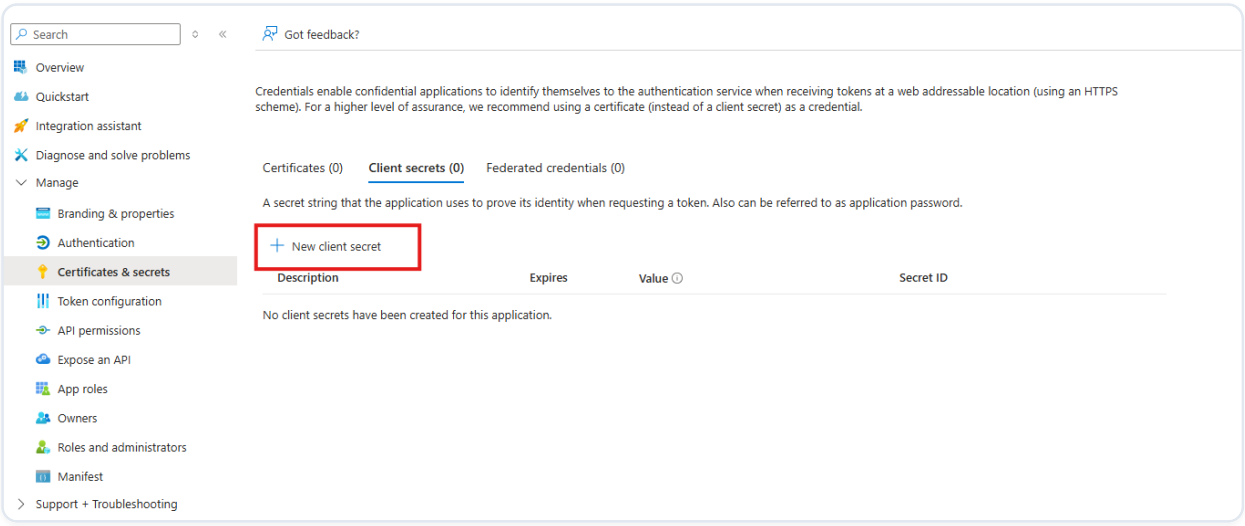


4. 单击 **为 MSFT 授予管理员同意**。此操作需要 Entra ID 全局管理员。



步骤 3：创建客户端密钥

1. 在 Microsoft Entra ID 中，导航到 **证书和密钥** -> **客户端密钥** -> **新建客户端密钥**。您也可以重复使用现有密钥。

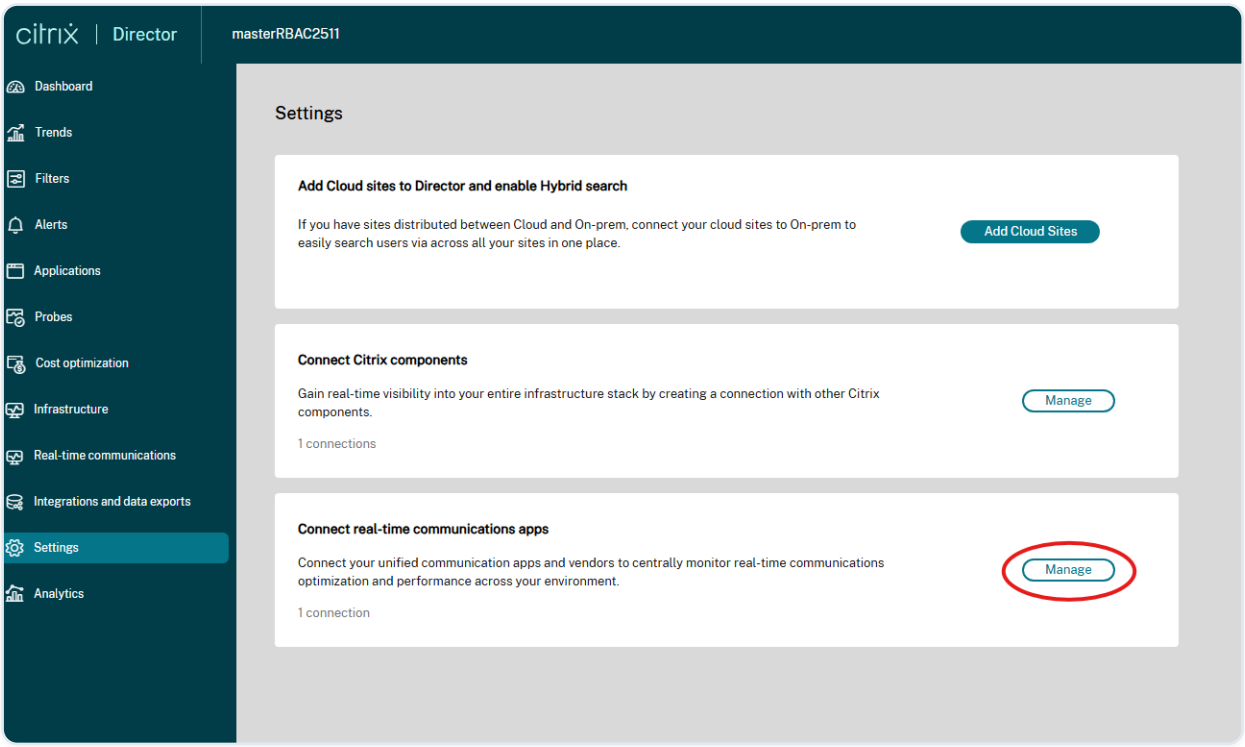


2. 为密钥提供名称和过期日期。确保在密钥过期前续订，以保持连接。
3. 复制客户端密钥以在 Director UI 中使用。

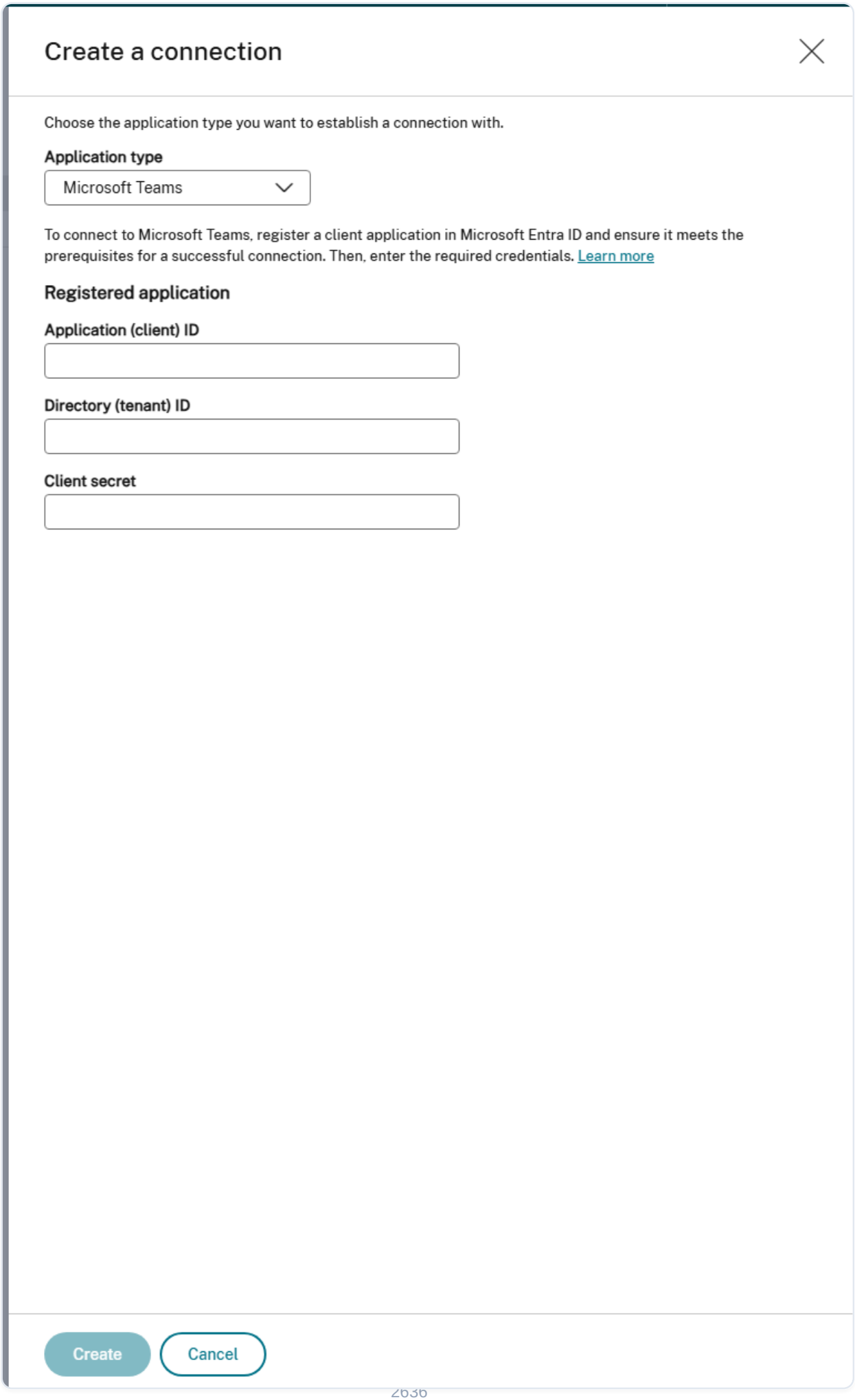
如果遇到任何问题，请参阅官方 Azure 文档 以获取更多信息。

步骤 4：在 Director 上完成连接

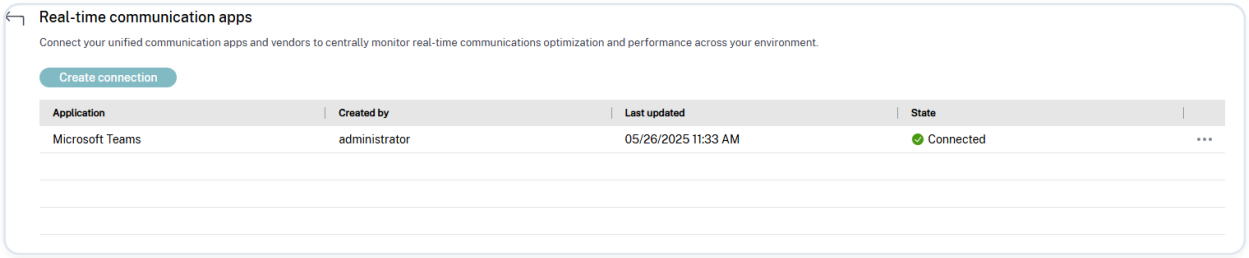
1. 在 Director 中，导航到**设置** -> **连接实时通信应用程序**。



2. 单击**创建连接**，然后输入从应用程序注册中复制的应用程序 ID、目录 ID 和客户端密钥。


Create a connection
Choose the application type you want to establish a connection with.
Application type
Microsoft Teams
To connect to Microsoft Teams, register a client application in Microsoft Entra ID and ensure it meets the prerequisites for a successful connection. Then, enter the required credentials. Learn more
Registered application
Application (client) ID
Directory (tenant) ID
Client secret
Create
Cancel

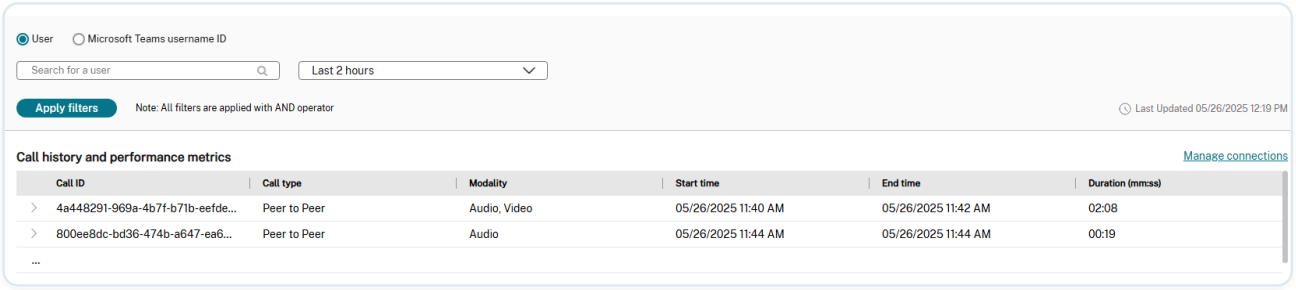
如果提供了有效的凭据和获取呼叫详细信息的权限，则连接将成功建立。



3. 通过单击行末尾的省略号，可以**编辑**和**删除**连接。

Microsoft Teams 控制板

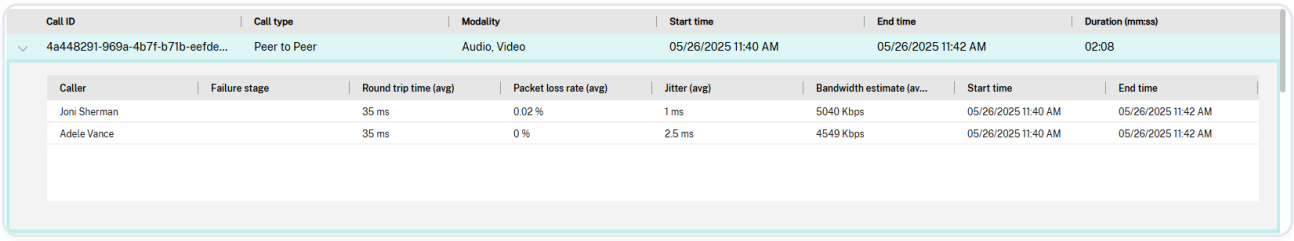
导航到 Director UI 中的**实时通信**选项卡。Microsoft Teams 控制板将填充从已建立的 Microsoft Graph 连接收集的数据。呼叫结束后大约 15 分钟即可获得呼叫详细信息。



表视图提供所有呼叫的以下详细信息。

列名称	描述
呼叫 ID	每个呼叫的唯一标识符。
呼叫类型	指示呼叫是点对点呼叫还是群组呼叫。
模式	指示呼叫期间使用的模式，例如音频、视频或屏幕共享。
开始时间	呼叫开始的日期和时间。
结束时间	呼叫结束的日期和时间。
持续时间 (mm: ss)	呼叫持续时间（分钟和秒）。

单击表中的单个呼叫可查看每个用户的故障和性能详细信息。



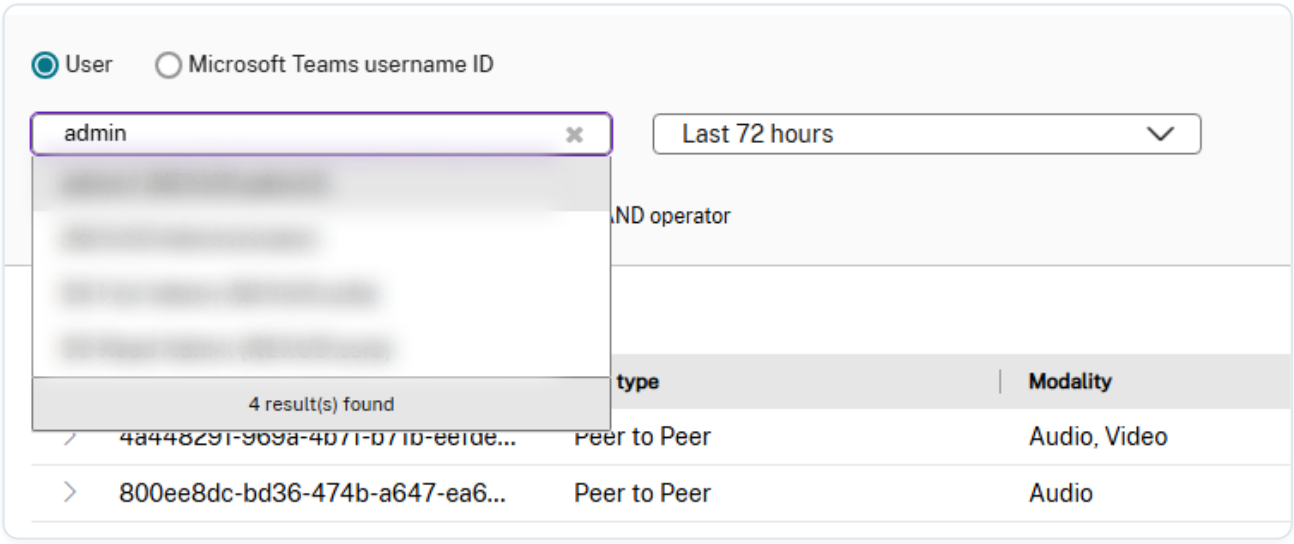
在群组呼叫中，当用户断开连接并重新加入时，这被视为一个单独的会话。此考量有助于识别特定问题，例如连接到特定网络时延迟较高。

呼叫详细信息表中的每一行都包含以下信息：

列名称	描述
开始时间	呼叫或参与者会话开始的日期和时间。
往返时间（平均）	数据包的平均往返时间。
数据包丢失率（平均）	通话期间丢失的数据包的平均百分比。
抖动（平均）	接收到的数据包延迟的平均变化。
故障阶段	指示呼叫失败发生的阶段，例如在设置期间或通话过程中。
结束时间	呼叫或参与者会话结束的日期和时间。
呼叫者	通话中参与者的姓名。
带宽估算（平均）	通话期间使用的估计平均带宽。

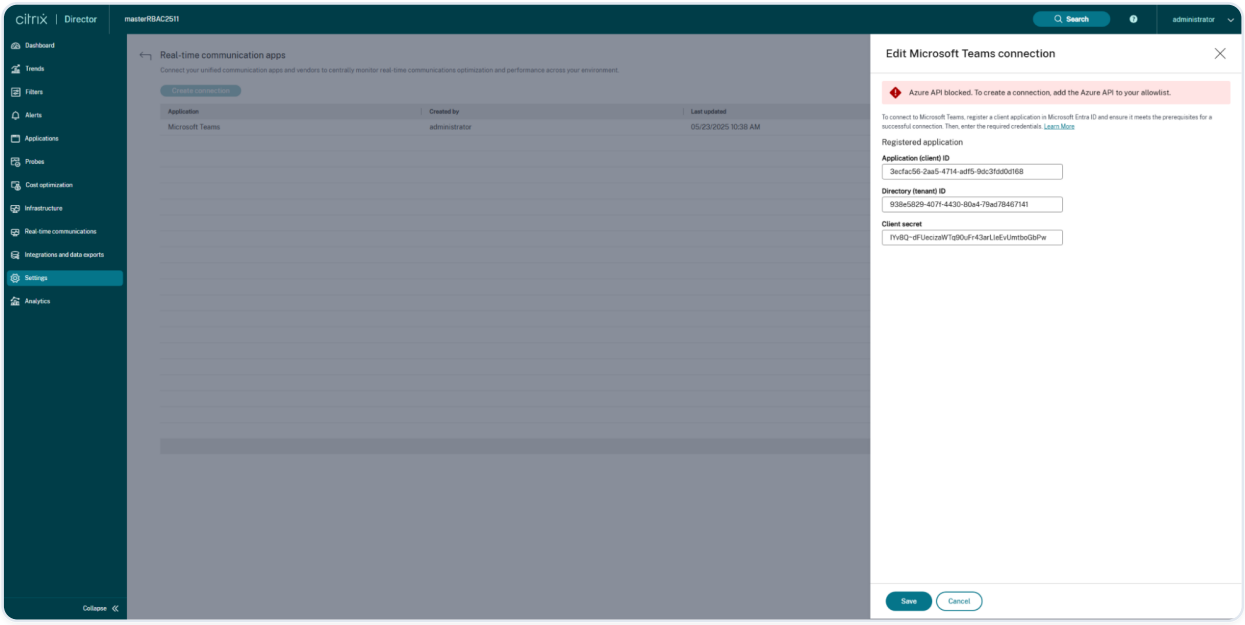
您可以通过两种方式筛选用户：按 Citrix 用户名或按 Microsoft Teams 用户名。您可以使用页面顶部的单选按钮在这两个选项之间切换。

- Citrix 用户名：当您开始键入用户名时，系统会建议匹配的用户。然后，您可以选择特定帐户以查看详细信息。
- Microsoft Teams 用户名：如果与 Microsoft Teams 帐户关联的电子邮件或用户主体名称 (UPN) 与 Citrix 帐户 ID 不同，请使用此选项。使用此方法时，您必须输入完整且有效的电子邮件地址。



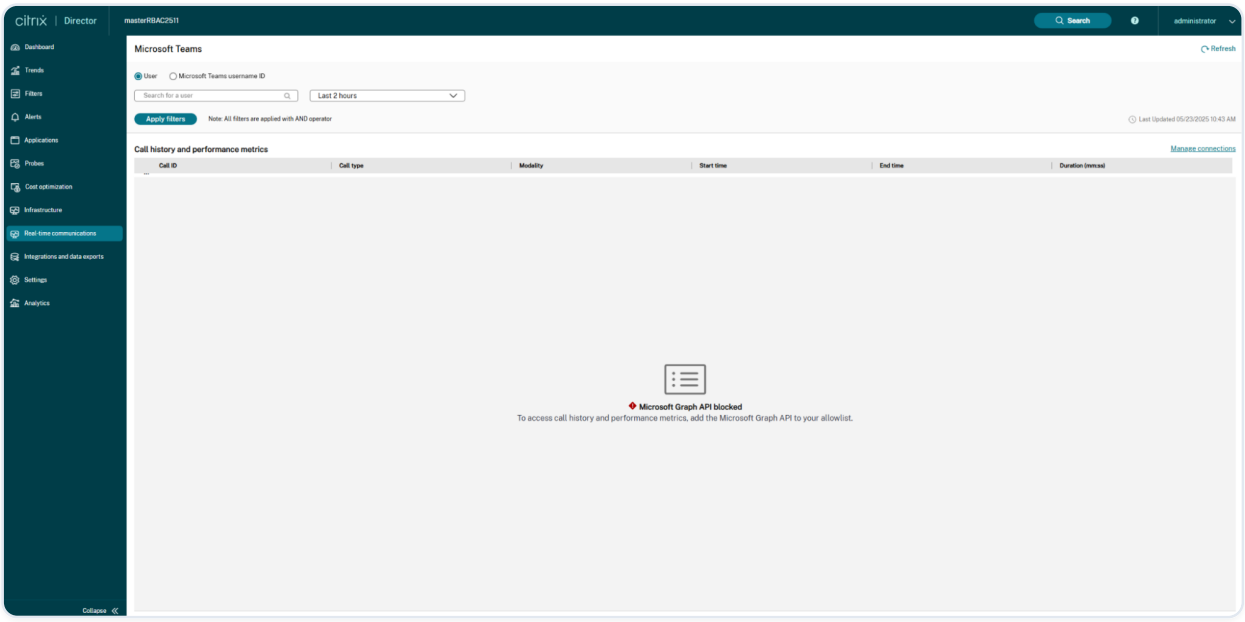
故障排除

- 为什么载入失败并出现错误“Azure API 被阻止。要创建连接，请将 Azure API 添加到您的允许列表”？



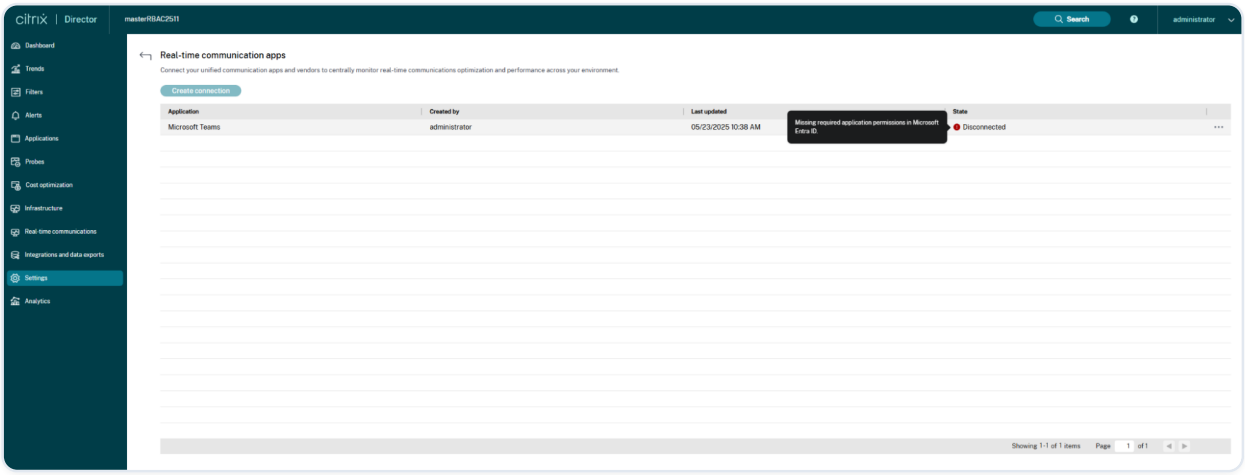
解决方案：确保您已遵循先决条件并将 Microsoft Graph API 终结点添加到您的允许列表。

- 为什么查看通话时会看到错误“Microsoft Graph API 被阻止”？



解决方案：确保您已遵循先决条件并将 Microsoft Graph API 终结点添加到您的允许列表。

- 为什么“连接”屏幕显示“Microsoft Entra ID 中缺少所需的应用程序权限”？



解决方案：验证应用程序权限 **CallRecords.Read.All** 和 **User.Read.All** 已分配给 Entra ID 应用程序。

故障排除部署

作为技术支持管理员，您可以搜索报告问题的用户，并显示与该用户关联的会话或应用程序的详细信息。同样，搜索报告问题的计算机或端点。通过监控相关指标并执行适当操作来快速解决问题。

可用操作包括：

- 结束无响应的应用程序或进程
- 影子操作用户的计算机
- 注销无响应的会话
- 重新启动计算机

- 将计算机置于维护模式
- 重置用户配置文件

应用程序故障排除

实时应用程序监控

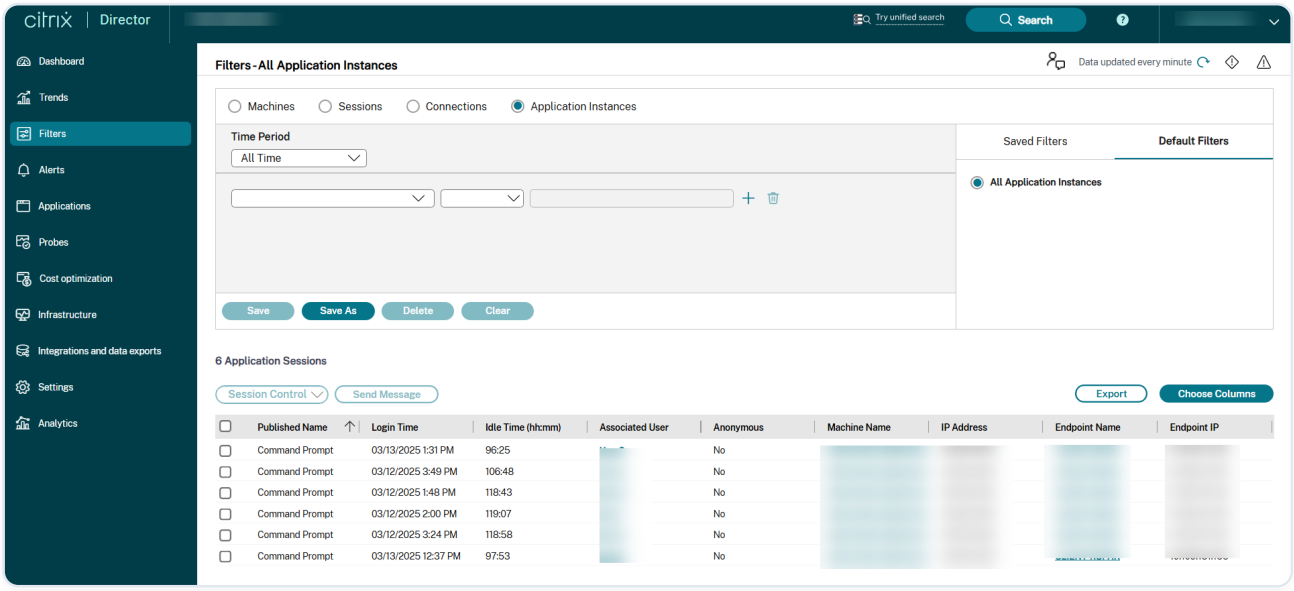
您可以使用空闲时间指标来识别超出特定时间限制的空闲实例，从而对应用程序和会话进行故障排除。

基于应用程序故障排除的典型用例是在医疗保健领域，员工共享应用程序许可证。在这种情况下，您必须终止空闲会话和应用程序实例，以清除 Citrix Virtual Apps and Desktops™ 环境，重新配置性能不佳的服务器，或维护和升级应用程序。

“**应用程序实例**”筛选页面列出了服务器和单会话操作系统 VDA 上的所有应用程序实例。对于多会话操作系统 VDA 上空闲至少 10 分钟的应用程序实例，将显示相关的空闲时间测量值。

> **注意：**
>
> 应用程序实例指标适用于所有许可证版本的站点。

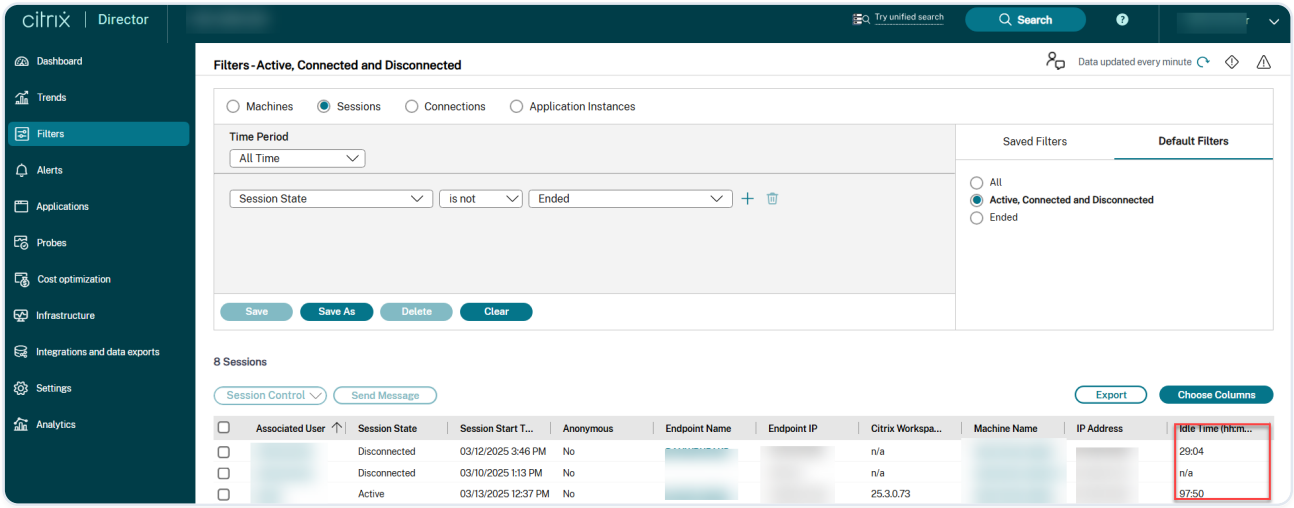
使用此信息识别超出特定时间段的空闲应用程序实例，并酌情注销或断开连接。为此，请选择 **Filters \> Application Instances**，然后选择一个预保存的筛选器或选择 **All Application Instances** 并创建您自己的筛选器。



筛选器示例如下。在“**筛选依据**”条件中，选择“**已发布名称**”（应用程序的）和“**空闲时间**”。然后，将“**空闲时间**”设置为“**大于或等于**”特定时间限制，并保存筛选器以供重复使用。从筛选列表中，选择应用程序实例。选择发送消息的选项，或从“**会话控制**”下拉列表中选择“**注销**”或“**断开连接**”以终止实例。

> **注意：**
>
> 注销或断开应用程序实例会注销或断开当前会话，从而终止属于同一会话的所有应用程序实例。

> 您可以使用会话状态和会话空闲时间指标，从“**会话**”筛选页面识别空闲会话。按“**空闲时间**”列排序或定义筛选器以识别超出特定时间限制的空闲会话。对于多会话操作系统 VDA 上空闲至少 10 分钟的会话，将列出空闲时间。



当会话或应用程序实例出现以下情况时，“**空闲时间**”显示为“**N/A**”

- 空闲时间未超过 10 分钟，
- 在单会话操作系统 VDA 上启动，或
- 在运行版本 7.12 或更早版本的 VDA 上启动。

历史应用程序故障监控

“**趋势**” -\> “**应用程序故障**”选项卡显示与 VDA 上已发布的应用程序相关的故障。

对于高级版和高级许可站点，应用程序故障趋势可用于过去 2 小时、24 小时、7 天和一个月。对于其他许可证类型，它们可用于过去 2 小时、24 小时和 7 天。将源为“应用程序错误”的应用程序故障记录到事件查看器中进行监控。单击“**导出**”以生成 CSV、Excel 或 PDF 格式的报告

应用程序故障监控的清理保留设置 GroomApplicationErrorsRetentionDays 和 GroomApplicationFaultsRetentionDays 默认设置为一天，适用于高级版和非高级版许可站点。您可以使用 PowerShell 命令更改此设置：

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```

应用程序故障趋势图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir_application_faults.png)

故障根据其严重性显示为“**应用程序故障**”或“**应用程序错误**”。“应用程序故障”选项卡显示与功能或数据丢失相关的故障。“应用程序错误”表示不立即相关的问题；它们表示可能导致未来问题的状况。

您可以根据“**已发布的应用程序名称**”、“**进程名称**”或“**交付组**”以及“**时间段**”筛选故障。该表显示故障或错误代码以及故障的简要说明。详细故障说明以工具提示形式显示。

> **注意：**
>
> 当无法派生相应的应用程序名称时，已发布的应用程序名称将显示为“未知”。这通常发生在启动的应用程序在桌面会话中失败，或者由于依赖的可执行文件导致未处理的异常而失败时。

> 默认情况下，仅监控托管在多会话操作系统 VDA 上的应用程序故障。您可以通过监控组策略修改监控设置：启用应用程序故障监控、启用单会话操作系统 VDA 上的应用程序故障监控以及从故障监控中排除的应用程序列表。有关详细信息，请参阅监控策略设置中的应用程序故障监控策略。

“**趋势**”**\>“应用程序探测结果”**页面显示站点中过去 24 小时和 7 天内运行的应用程序探测结果。有关如何配置应用程序探测的更多详细信息，请参阅应用程序探测。

排查计算机问题

> **注意：**
>
> **Citrix Health Assistant** 是一款用于排查未注册 VDA 中配置问题的工具。该工具可自动执行多项健康检查，以识别 VDA 注册失败以及会话启动和时区重定向配置中问题的可能根本原因。知识中心文章 Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch 包含 **Citrix Health Assistant** 工具的下载和使用说明。

> Director 控制台中的“**筛选器 > 计算机**”视图显示站点中配置的计算机。“多会话操作系统计算机”选项卡包含负载评估器索引，该索引指示性能计数器的分布，以及将鼠标悬停在链接上时会话计数的工具提示。

单击故障计算机的“**失败原因**”列，可获取故障的详细描述以及建议的故障排除操作。计算机和连接故障的失败原因和建议操作可在 Citrix Director 失败原因和故障排除 中找到。

单击计算机名称链接可转到“**计算机详细信息**”页面。

“计算机详细信息”页面列出了计算机详细信息、基础结构详细信息以及应用于计算机的热修复程序详细信息。

先决条件

- uberAgent 必须安装在 VDA 上
- **Windows VDA 版本**：2511 或更高版本

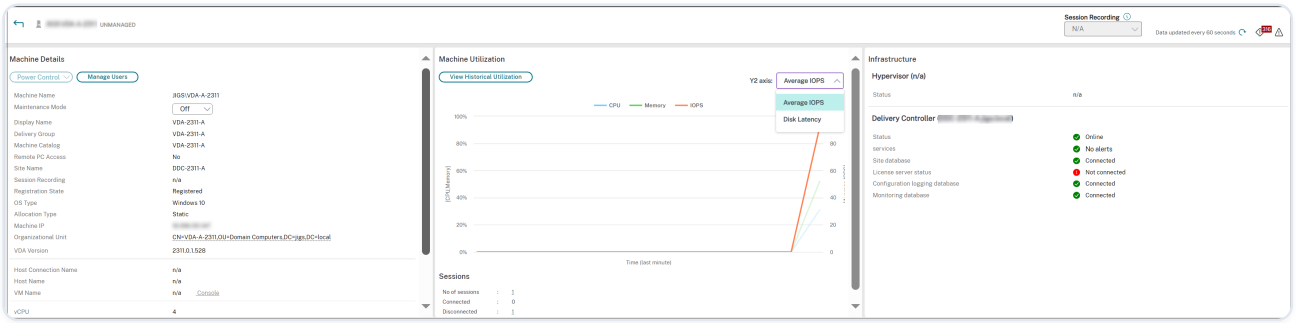
指标

指标	描述
平均 CPU 使用率 (%)	
平均 RAM 使用率 (%)	
平均磁盘 IOPS	
平均磁盘延迟 (ms)	
平均 GPU 使用率 (%)	
平均网络利用率 (%)	
平均负载指数	
平均磁盘使用率 (%)	
平均配置文件磁盘使用率 (%)	
平均 CPU 空闲率 (%)	
平均页面文件使用率 (%)	
平均 CPU 相对频率 (%)	

基于计算机的实时资源利用率

“**计算机利用率**”面板显示了 CPU 和内存的实时利用率图表。此外，对于 Delivery Controllers 和 VDA 版本为 **7.14** 或更高版本的站点，还提供磁盘和 GPU 监控图表。

磁盘监控图表、平均 IOPS 和磁盘延迟是重要的性能测量指标，可帮助您监控和排查与 VDA 磁盘相关的问题。平均 IOPS 图表显示了磁盘的平均读写次数。选择**磁盘延迟**可查看数据请求与数据从磁盘返回之间的延迟图表，以毫秒为单位。



GPU 利用率

选择**GPU 利用率**可查看 GPU、GPU 内存以及编码器和解码器的利用率百分比，以排查多会话和单会话操作系统 VDA 上的 GPU 相关问题。

支持的 GPU 版本：

- 运行显示驱动程序版本 369.17 或更高版本的 NVIDIA Tesla M60 GPU。有关详细信息，请参阅 NVIDIA vGPU Software。
- AMD Radeon Instinct MI25 GPU 和 AMD EPYC 7V12(Rome) CPU。有关详细信息，请参阅 AMD Drivers and Support。

驱动程序：

必须在 VDA 上安装相应的驱动程序或扩展。

- 对于 NVIDIA GPU，请手动或通过扩展安装 GRID 驱动程序。有关详细信息，请参阅 NVIDIA vGPU Software。
  - 对于 NVIDIA，仅支持 GRID 驱动程序。CUDA 驱动程序不适用于 NVadsA10 v5 系列，并且不受支持。
  - 有关通过扩展在基于 Azure 的计算机上安装 NVIDIA Grid GPU 驱动程序的示例过程，请参阅 NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines。
  - 有关手动安装 NVIDIA Grid GPU 驱动程序的示例过程，请参阅 Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines。

- 对于 AMD GPU，请手动或通过扩展安装 AMD 图形驱动程序。有关详细信息，请参阅 AMD Drivers and Support。
  - 有关通过扩展在基于 Azure 的计算机上安装 AMD GPU 驱动程序的示例过程，请参阅 AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines。
  - 有关在 Azure 计算机上手动安装 AMD GPU 驱动程序的示例过程，请参阅 Install AMD GPU drivers on N-series VMs running Windows。

使用说明：

- GPU 利用率图表仅适用于运行 64 位 Windows 的 VDA。
- VDA 必须启用 HDX 3D Pro 才能提供 GPU 加速。有关详细信息，请参阅 GPU acceleration for Windows Single-session OS 和 GPU acceleration for Windows Multi-session OS。
- 当 VDA 访问多个 GPU 时，利用率图表会显示从各个 GPU 收集的 GPU 指标的平均值。GPU 指标是针对整个 VDA 收集的，而不是针对单个进程收集的。
- 对于 AMD，编码器和解码器使用情况不支持单独显示。任何使用 GPU 的编码/解码工作负载都将报告为 GPU 使用率上的常规 3D 负载。
- 确保在安装过程中安装 NVIDIA WMI。此窗口仅在手动安装期间可用。
- 如果已安装驱动程序但 Director 未检测到 GPU
  - 检查任务管理器。如果驱动程序安装正确，GPU 必须显示在任务管理器中。
  - 检查计算机是否已注册。有时，计算机可能需要一些时间才能被检测为联机。
- 如果 Director 中未显示 GPU 使用情况活动，请确保您正在运行的工作负载正在使用 GPU。对于图形工作负载，可以在“设置”>“系统”>“显示”>“图形设置”>“选择要设置首选项的应用程序”中启用此功能。请务必开启“高性能”。有时，当此设置基于其他设置设为系统默认值或省电模式时，Windows 默认使用 CPU 处理图形工作负载。
- 数据每分钟更新一次，数据可视化在选择**GPU 利用率**后一分钟内开始。

基于计算机的历史资源利用率

在**计算机利用率**面板中，单击**查看历史利用率**以查看所选计算机上的资源历史使用情况。 利用率图表包括 CPU、内存、并发会话峰值、平均 IOPS 和磁盘延迟的关键性能计数器。

> **注意：**
>
> 必须将监视策略设置**启用进程监视**设置为“允许”才能在“历史计算机利用率”页面上的“前 10 个进程”表中收集和显示数据。默认情况下禁止收集。

CPU 和内存利用率、平均 IOPS 和磁盘延迟数据默认情况下会收集。您可以使用**启用资源监视**策略设置禁用收集。



1. 在**计算机详细信息**视图的**计算机利用率**面板中，选择**查看历史利用率**。
2. 在**历史计算机利用率**页面中，将**时间段**设置为查看过去 2 小时、24 小时、7 天、月或年的使用情况。

> **注意：**
>
> 平均 IOPS 和磁盘延迟使用情况数据仅适用于截至目前的过去 24 小时、月和年。不支持自定义结束时间。

3. 单击**应用**并选择所需的图表。
4. 将鼠标悬停在图表的不同部分上，以查看所选时间段的更多信息。



例如，如果选择**过去 2 小时**，则基线时间段是所选时间范围之前的 2 小时。查看过去 2 小时和基线时间的 CPU、内存和会话趋势。如果选择**上个月**，则基线时间段是前一个月。选择查看上个月和基线时间的平均 IOPS 和磁盘延迟。

1. 单击 **导出** 以导出所选时间段的资源利用率数据。有关详细信息，请参阅 Monitor Deployments 中的 导出报告 部分。
2. 在图表下方，该表列出了基于 CPU 或内存利用率排名前 10 位的进程。您可以按任意列进行排序，这些列显示了所选时间范围内的应用程序名称、用户名、会话 ID、平均 CPU、峰值 CPU、平均内存和峰值内存。IOPS 和磁盘延迟列无法排序。

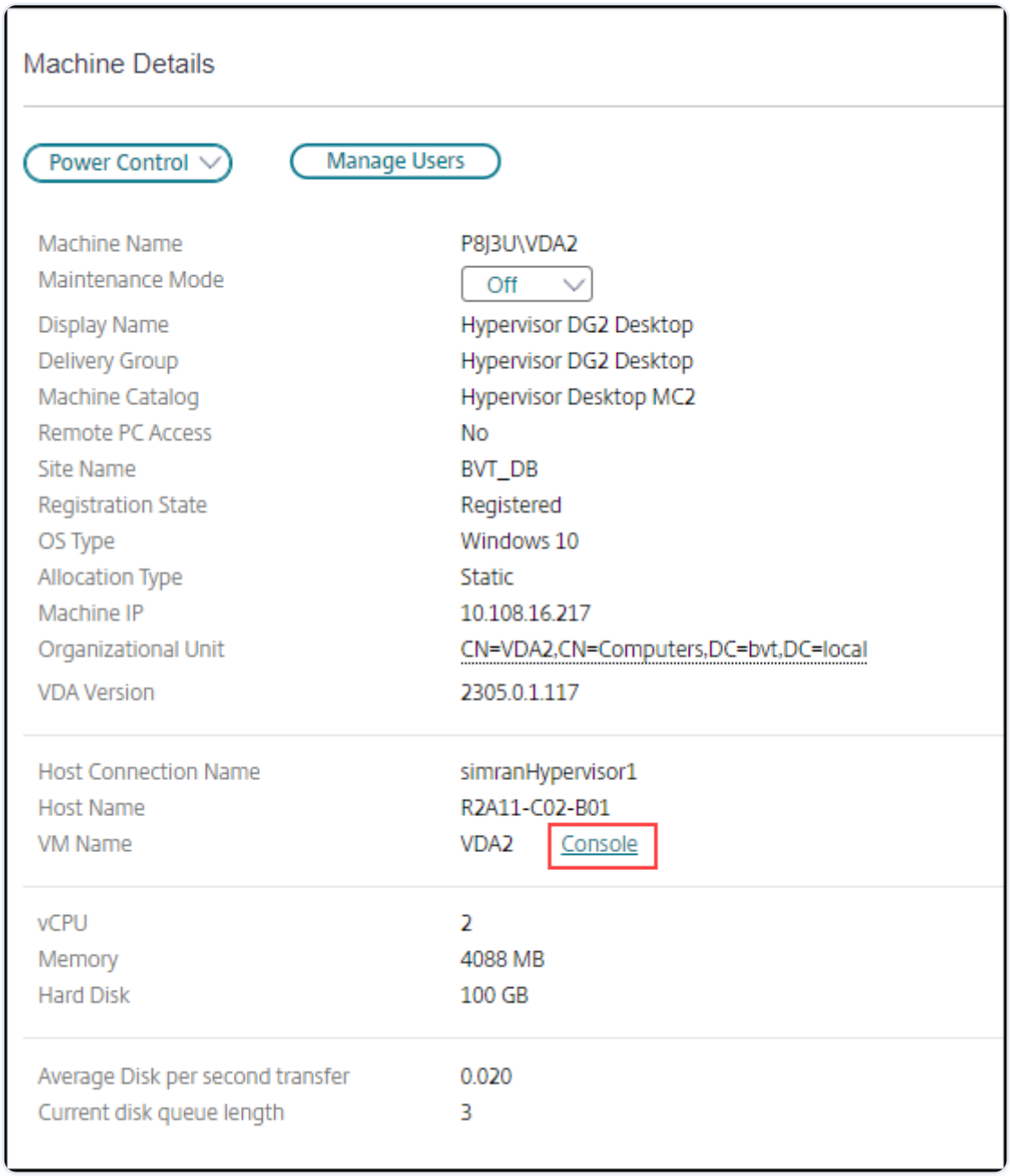
   > **注意：**
   >
   > 系统进程的会话 ID 显示为“0000”。

3. 要查看特定进程的资源消耗历史趋势，请深入查看排名前 10 位的任意进程。

计算机控制台访问

您可以直接从 Director 访问托管在 XenServer 7.3 及更高版本上的单会话和多会话操作系统计算机的控制台。这样，您无需 XenCenter 即可对 XenServer 托管的 VDA 进行故障排除。要使用此功能，需要满足以下条件：

- 需要 7.16 或更高版本的 Delivery Controller。
- 托管计算机的 XenServer 必须是 7.3 或更高版本，并且必须可从 Director UI 访问。



要对计算机进行故障排除，请单击相应的“计算机详细信息”面板中的 **控制台** 链接。在您提供的主机凭据通过身份验证后，计算机控制台将使用基于 Web 的 VNC 客户端 noVNC 在单独的选项卡中打开。现在，您可以访问控制台的键盘和鼠标。

注意：

- Internet Explorer 11 不支持此功能。
- 如果计算机控制台上的鼠标指针未对齐，请参阅 CTX230727 以了解解决此问题的步骤。
- Director 在新选项卡中启动控制台访问，请确保您的浏览器设置允许弹出窗口。
- 出于安全原因，Citrix® 建议您在浏览器上安装 SSL 证书。

检查具有近期电源操作的计算机

您现在可以检查具有成功和失败电源操作状态的计算机。此功能可帮助您分析以下内容：

- 导致用户问题的开机失败
- 增加成本的关机失败

注意：

数据仅适用于电源管理的计算机。对于此功能受支持之前执行的电源操作，数据不可用。

您可以通过以下方式查看计算机的电源操作状态：

从“**筛选器**”->“**计算机**”选项卡。在这种情况下，默认情况下会显示“**电源操作时间**”和“**电源操作结果**”列。您还可以选择要显示的列。

从**成本优化**选项卡。在这种情况下，默认筛选器是**电源操作触发者**设置为 *Autoscale*™，**电源操作结果**设置为*失败*。

借助此功能，您可以查看电源操作控制的详细信息。例如，您可以查看谁触发了操作、哪个操作更改了电源状态、失败原因以及操作完成时间。您还可以导出这些详细信息。

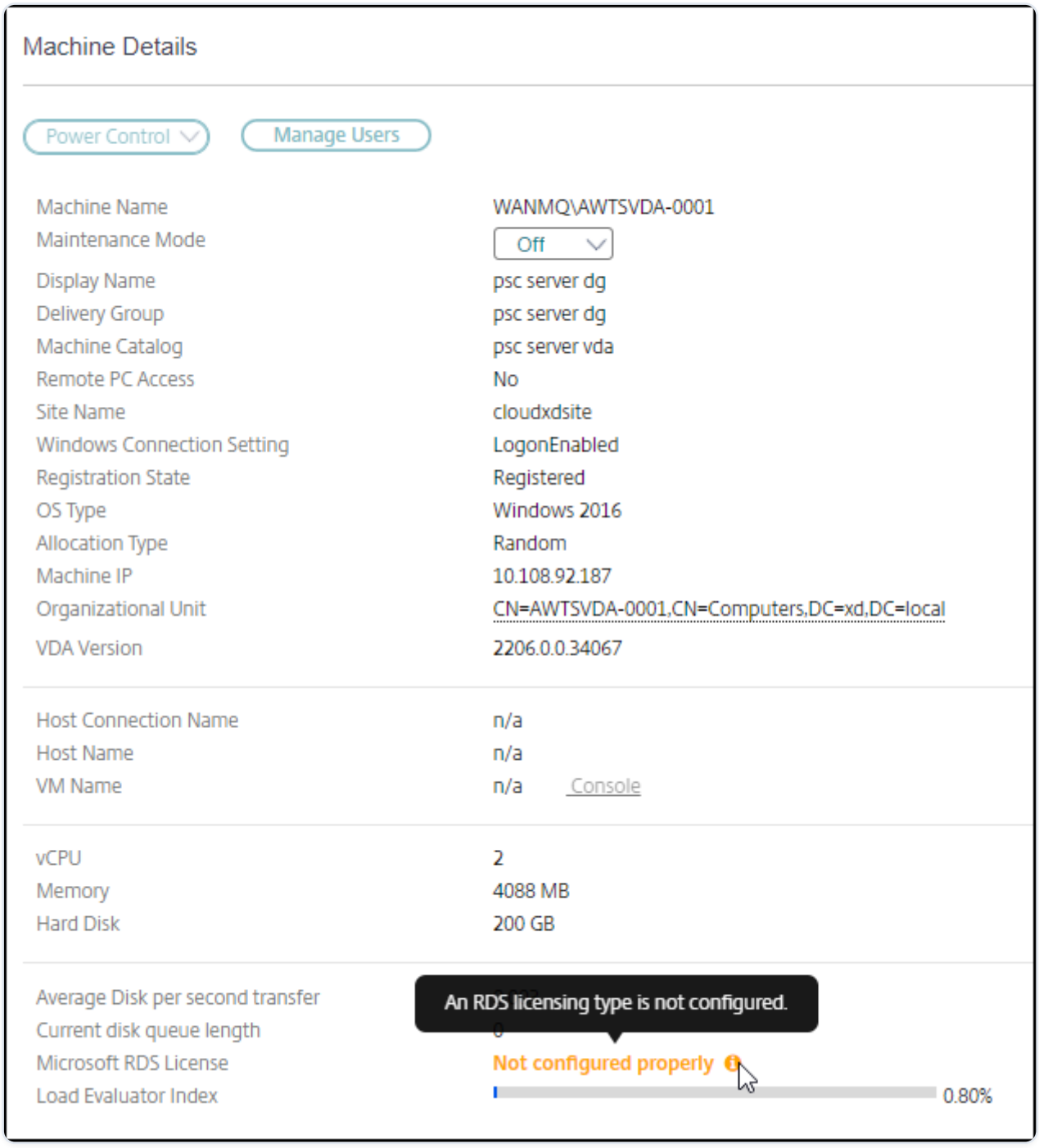
添加了以下筛选器以查看电源操作状态：

筛选器	描述
电源操作结果	显示电源操作的结果。可能的筛选值是成功和失败。
电源操作触发者	显示触发电源操作的人员或内容。可能的筛选器值如下： • 自动缩放 - 当以下情况触发电源操作时，将显示此值 • 当管理员关闭 VM 以将 VM 的 OS 磁盘清理回其初始状态时

筛选器	描述
	• 当虚拟机根据设置的策略关闭或挂起时
	• 当虚拟机根据池大小或缓冲区大小配置可用时
	• 管理员 - 当电源操作由管理员触发时，将显示此值。可能的示例是管理员请求关闭、打开、挂起、恢复、重新启动或重启虚拟机。
	• 用户 - 当电源操作由用户触发时，将显示此值。示例是用户重置、打开或恢复虚拟机上的工作。
	• 其他 - 当电源操作由计划和未知原因触发时，将显示此值。
上次电源操作	显示计算机上发生的精确电源操作，例如开机、关机、关闭、重新启动、重置、恢复
电源操作时间	电源操作完成的时间。可能的筛选值包括上一分钟、过去 5 分钟、过去 30 分钟、上一小时、今天、过去 24 小时和昨天。
电源操作失败原因	显示失败原因。可能的筛选值包括管理程序报告的故障、管理程序速率限制超出、未知错误和无。如果操作成功，则显示“无”。

Microsoft RDS 许可证运行状况

您可以在多会话操作系统计算机的“**计算机详细信息**”页面和“**用户详细信息**”页面中的“**计算机详细信息**”面板中查看 Microsoft RDS 许可证的状态。



将显示以下消息之一：

- 许可证可用
- 未正确配置（警告）
- 许可证错误（错误）
- VDA 版本不兼容（错误）

> **注意：**

处于宽限期且具有有效许可证的计算机的 Microsoft RDS 许可证运行状况状态以绿色显示“**许可证可用**”消息。请在许可证过期前续订。

对于警告和错误消息，将鼠标悬停在信息图标上可查看下表中提供的其他信息。

消息类型	DIRECTOR 中的消息
错误	适用于 VDA 7.16 及更高版本。
错误	不允许新的 RDS 连接。
错误	Microsoft RDS 许可证已超出其宽限期。
错误	未为所需的操作系统级别配置具有“按设备客户端访问”许可类型的许可证服务器。
错误	配置的许可证服务器与具有“按设备客户端访问”许可类型的 RDS 主机操作系统级别不兼容。
警告	个人终端服务器在 Citrix Virtual Apps and Desktops™ 部署中不是有效的 RDS 许可类型。
警告	用于管理的远程桌面在 Citrix Virtual Apps and Desktops™ 部署中不是有效的许可类型。
警告	未配置 RDS 许可类型。
警告	域控制器或许可证服务器在使用“按用户客户端访问”RDS 许可类型时无法访问。
警告	使用“按设备客户端访问”许可类型时，由于所需操作系统级别的许可证服务器无法访问，因此无法确定客户端设备许可证。

注意：

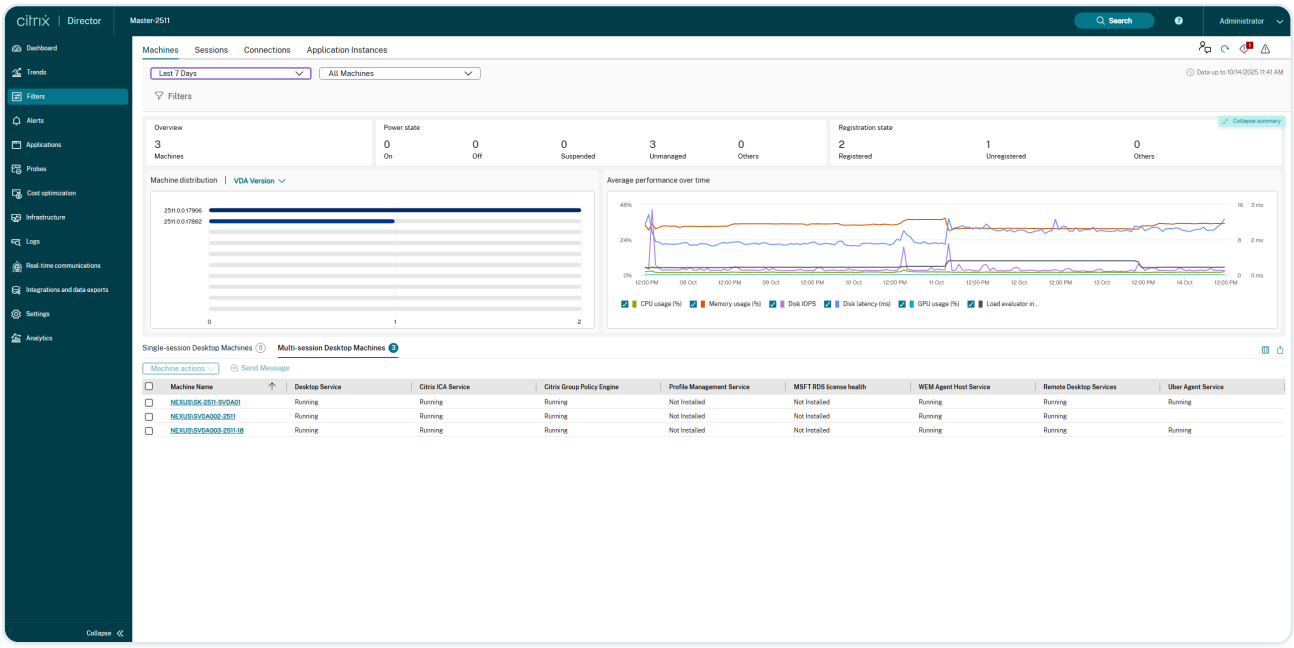
此功能仅适用于 Microsoft RDS CAL（客户端访问许可证）。

通过 UberAgent Lite 的 VDA 健康监控指标

1. 简介：新增功能?

为了更深入地了解 Virtual Delivery Agent (VDA) 计算机的运行状况和性能，我们引入了多项关键增强功能：

- **新可视化效果：**
  a. 已添加一个摘要面板，其中包含三个类别：**概述、电源状态**和**注册状态**。
  b. 已添加两个新图表（**计算机分布**和**随时间变化的平均性能**），以提供计算机状态和历史趋势的即时图形视图。
- **增强的表格数据： 单会话**和**多会话桌面**计算机表现在包含关键 VDA 服务的详细状态列，有助于快速查明计算机运行状况问题的根本原因。
- **新的时间范围筛选器：** 已添加两个新的时间范围筛选器 - “过去 2 小时”和“过去 7 天”，以支持历史趋势。

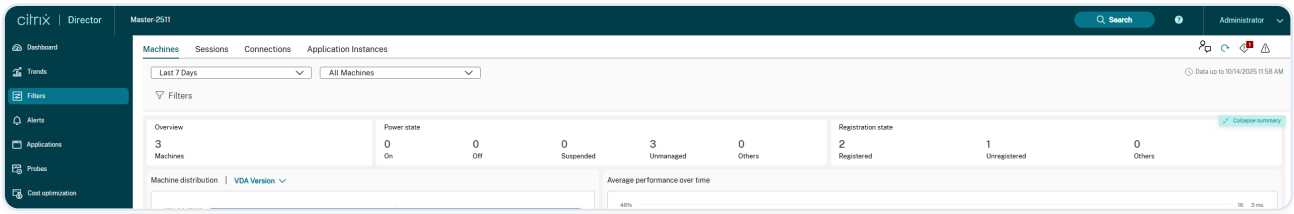


2. 了解新可视化效果

2.1. 摘要面板

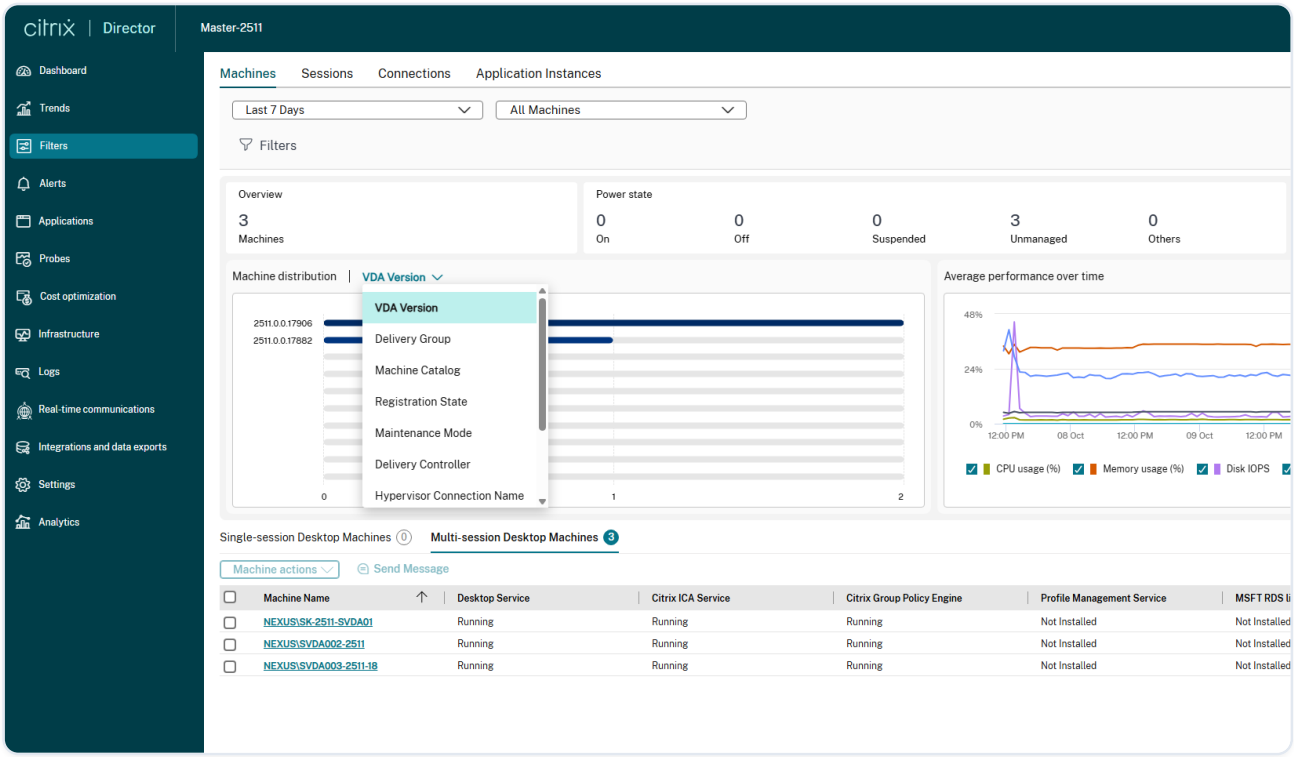
- **概述：** 显示关联的 VDA（计算机）总数。
- **电源状态：** 显示基于其电源状态（开机、关机、挂起、未管理和其他）的计算机数量。
- **注册状态：** 显示基于其注册状态（已注册、未注册和其他）的计算机数量。

此摘要可折叠，可帮助管理员根据上述分类采取必要的措施，例如打开处于关机状态的计算机或识别处于未注册状态的计算机。

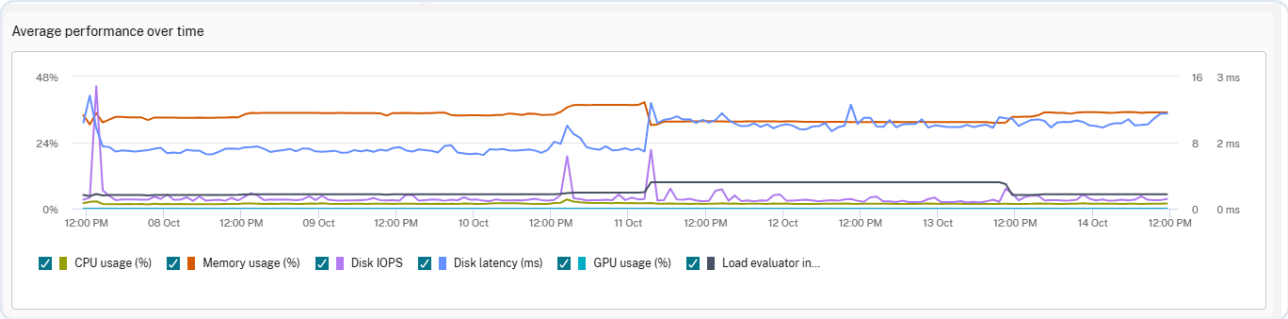


2.2. 计算机分布

- **目的：** 此条形图提供了当前筛选集中包含的 VDA 计算机的快速可视化细分。默认筛选器设置为 VDA 版本。但是，用户可以使用交付组、计算机目录、注册状态、维护模式、交付控制器、虚拟机管理程序连接名称、故障类型、故障原因和电源状态进行筛选。
- **实用性：** 这使管理员能够根据筛选条件获取 VDA 的整体概览。例如，VDA 版本上的计算机分布有助于管理员快速识别是否有很大一部分 VDA 正在运行较旧或非标准的 VDA 版本，这可能是故障排除或升级规划的先决条件。



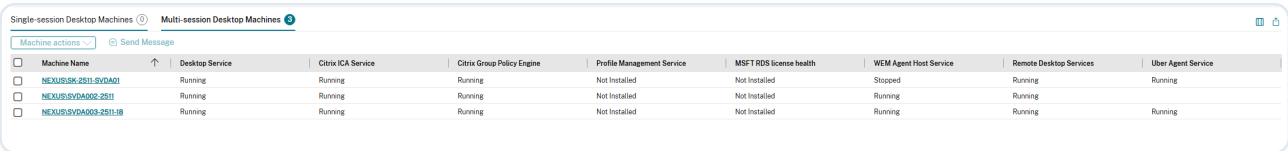
2.3. 随时间变化的平均性能



- **目的：** 此时间序列图表跟踪所选时间范围（例如，过去 24 小时）内的关键性能指标。
- **跟踪的关键指标：**
  - **CPU 使用率 (%)：** CPU 的平均使用百分比。
  - **内存使用率 (%)：** RAM 的平均使用百分比。
  - **磁盘 IOPS：** 每秒输入/输出操作的平均数量。
  - **磁盘延迟 (ms)：** 磁盘 I/O 请求的平均时间延迟（以毫秒为单位）。
  - **GPU 使用率 (%)：** GPU 的平均使用百分比（如果适用）。
  - **负载评估器 (%)：** VDA 计算机上的计算负载指数百分比。
- **实用性：** 允许进行历史趋势分析，有助于发现性能下降、资源争用以及何时出现峰值负载。

3. 增强的表格数据

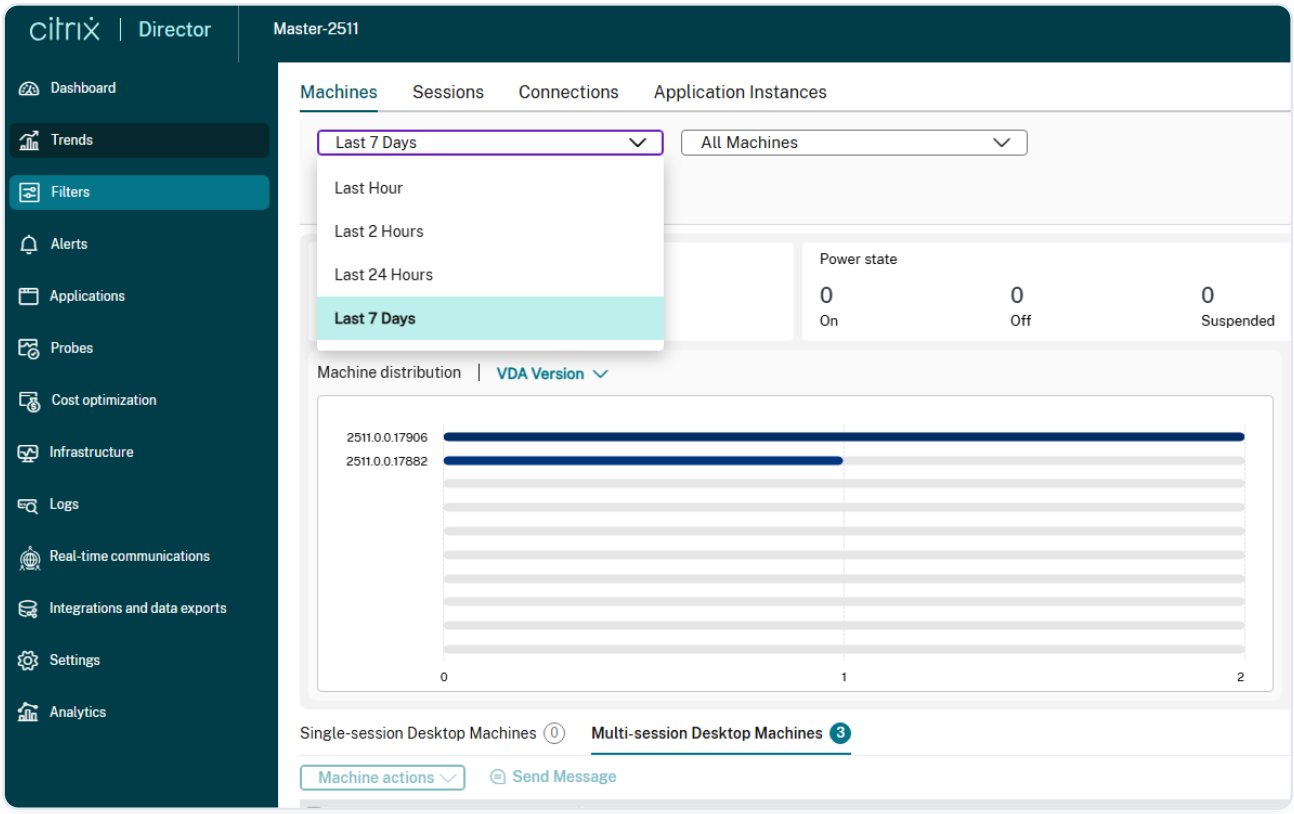
单会话/多会话表：新的列定义



列名称	描述	可能的值
桌面服务	负责管理桌面会话的主服务的运行状况（例如，CtxSvcHost）。	正在运行、已停止、未安装、已暂停、启动挂起、停止挂起、继续挂起、暂停挂起、未知
Citrix ICA 服务	负责处理用户会话的独立计算架构 (ICA) 协议的核心服务的运行状况。	正在运行、已停止、未安装、已暂停、启动挂起、停止挂起、继续挂起、暂停挂起、未知

列名称	描述	可能的值
Citrix 组策略引擎	负责处理和应用 Citrix 特定策略的服务的运行状况。	正在运行、已停止、未安装、已暂停、启动挂起、停止挂起、继续挂起、暂停挂起、未知
配置文件管理服务	Citrix Profile Management 的运行状况，用于管理 Citrix 虚拟环境中的用户配置文件。	正在运行、已停止、未安装、已暂停、启动挂起、停止挂起、继续挂起、暂停挂起、未知
MSFT RDS 许可证运行状况	指示 Microsoft 远程桌面服务 (RDS) 许可证检查的状态。	正在运行、已停止、未安装、已暂停、启动挂起、停止挂起、继续挂起、暂停挂起、未知
WEM 代理主机服务	Workspace Environment Management (WEM) 代理的运行状况，负责优化和配置。	正在运行、已停止、未安装、已暂停、启动挂起、停止挂起、继续挂起、暂停挂起、未知
远程桌面服务	底层 Microsoft 远程桌面服务的运行状况（单会话和多会话主机功能均需要）。	正在运行、已停止、未安装、已暂停、启动挂起、停止挂起、继续挂起、暂停挂起、未知
Uber Agent 服务	第三方监控代理服务的运行状况（如果适用且已安装）。	正在运行、已停止、未安装、已暂停、启动挂起、停止挂起、继续挂起、暂停挂起、未知

4. 支持新的时间范围筛选器



1. **最近 2 小时**

   - **目的：** 提供过去 120 分钟内 VDA 资源利用率的高粒度即时视图。
   - **实用性：** 此短时间范围非常适合实时故障排除。使用它来查明资源峰值（例如高 CPU 或低磁盘 IOPS）发生的确切时间，并将其与最近的用户活动或管理操作关联起来。

2. 最近 7 天

   - **目的：** 显示过去一周的资源使用情况和性能趋势。
   - **实用性：** 这是每周性能审查的标准筛选器。它可帮助管理员识别重复出现的性能问题，例如持续对 VDA 资源造成压力的特定日期或高峰时段（例如周一上午登录），从而实现主动容量规划和优化。

VDA 运行状况监视指标：支持的平台和版本

VDA 列	视窗	MAC	林纳克斯
桌面服务	2511 或以上	2511 或以上	2511 或以上
Citrix ICA 服务	2511 或以上	2511 或以上	2511 或以上
Citrix 组策略引擎	2511 或以上	2511 或以上	2511 或以上

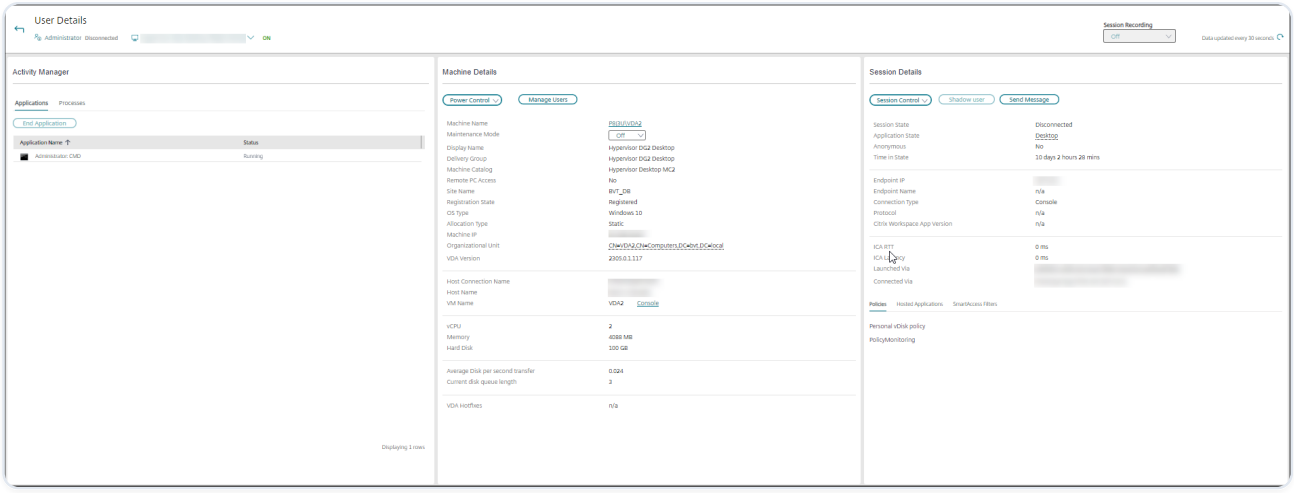
VDA 列	视窗	MAC	林纳克斯
配置文件管理服务	2511 或以上	2511 或以上	2511 或以上
MSFT RDS 许可证运行状况	2511 或以上	2511 或以上	2511 或以上
WEM 代理主机服务	2511 或以上	2511 或以上	2511 或以上
远程桌面服务	2511 或以上	2511 或以上	2511 或以上
Uber Agent 服务	2511 或以上	2511 或以上	2511 或以上

解决用户问题

使用 Director 的“**帮助台**”视图（“**活动管理器**”页面）查看有关用户或会话的信息：

用户详细信息(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-user-details-summary.png)

从活动管理器中单击用户的“**查看详细信息**”将打开“**用户详细信息**”页面。 从活动管理器中单击端点的“**查看详细信息**”将打开“**端点详细信息**”页面。



会话选择器

如果用户已启动多个会话，会话选择器有助于选择一个会话。

会话选择器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-session-selector.png)

选择一个会话以查看详细信息。

- 检查有关会话、用户登录体验、会话启动、连接和应用程序的详细信息。
- 您可以远程协助用户的计算机。

- 录制 ICA® 会话。

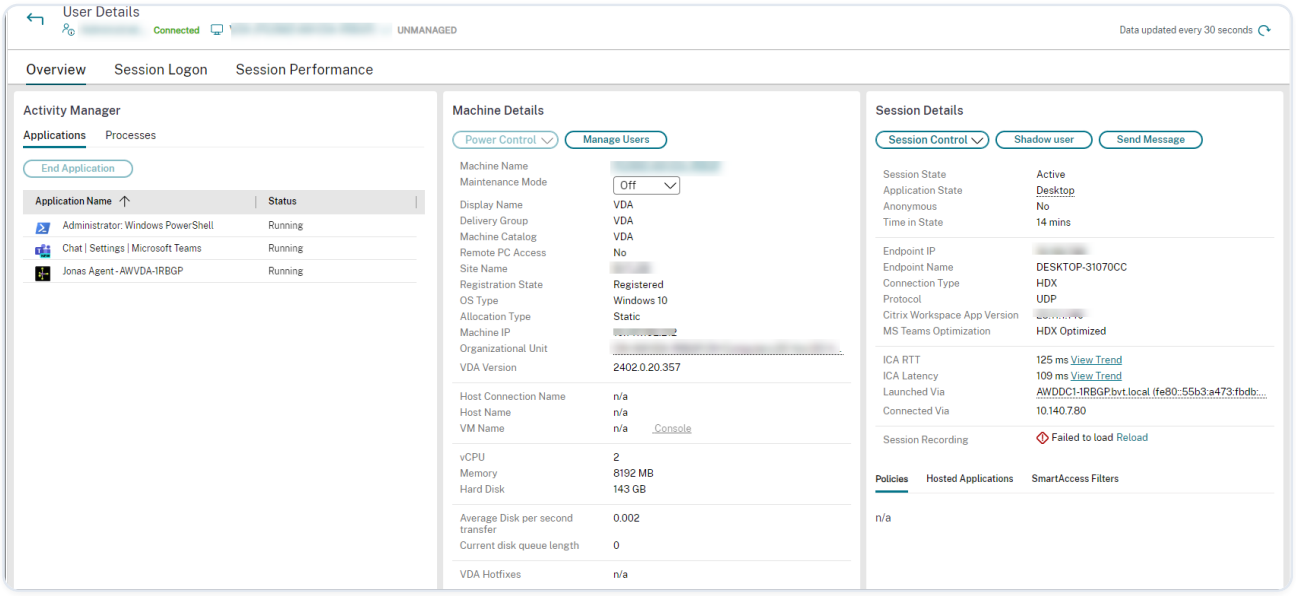
Microsoft Teams 优化状态

Director 在“**用户详细信息**”页面 > “**会话详细信息**”面板 > “**MS Teams 优化**”字段中显示 HDX™ 会话的 Microsoft Teams 优化状态。Microsoft Teams 的优化对于更好的用户体验（例如清晰的音频和视频）至关重要。Microsoft Teams 优化状态的可见性有助于减少解决工单所需的时间，并帮助管理员在故障排除期间识别重要指标。

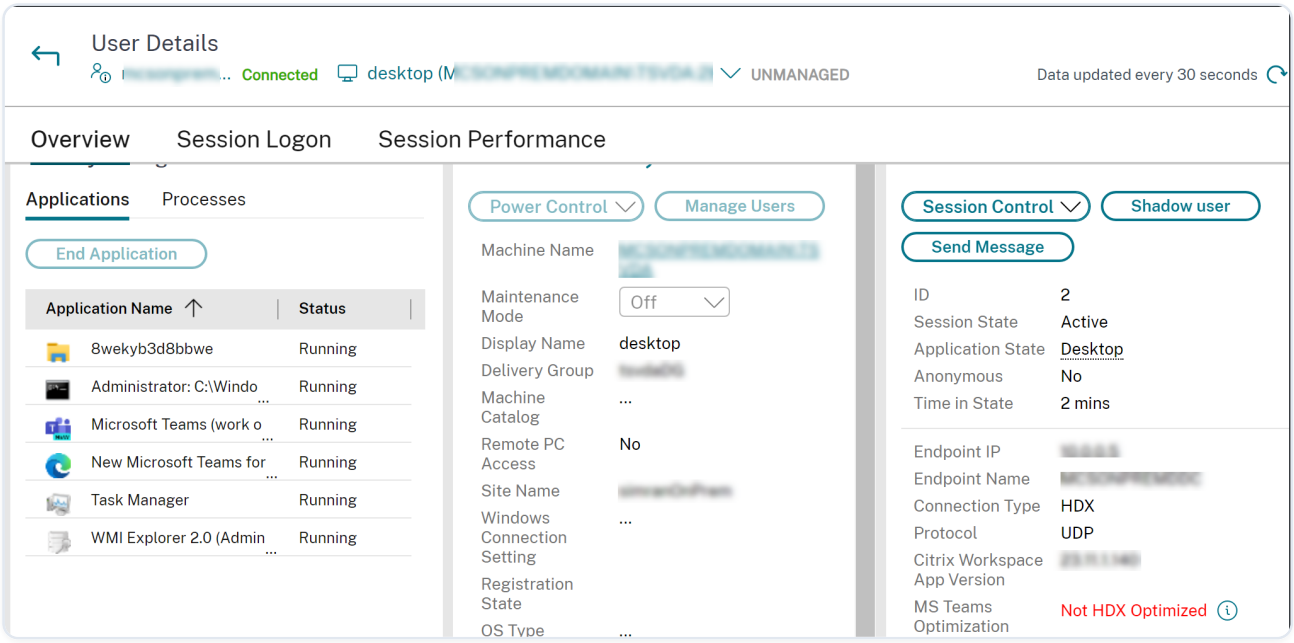
> **注意：**
>
> Citrix Director 支持 Microsoft Teams 2.1 版或更早版本。

> 先决条件：

- VDA 运行版本 2311 及更高版本。
- 支持的 Citrix Workspace 应用程序版本列在 Microsoft Teams 优化 中。
- Microsoft Teams 作为已发布的应用程序或在已发布的桌面中运行。
- Citrix HDX HTML5 视频重定向服务等关键服务正在运行。



如果 Microsoft Teams 未优化，工具提示会提供一个链接，指向 HDX 的外部故障排除实时文章，其中包含优化 Microsoft Teams 的技巧。HDX 优化故障排除。



故障排除技巧

使用下表中的建议操作对问题进行故障排除，如果需要，将问题上报给相应的管理员。

用户问题	建议
登录时间过长或间歇性/反复失败	诊断用户登录问题
会话启动时间过长或间歇性/反复失败	诊断会话启动问题
会话响应缓慢或无响应	诊断会话性能问题
应用程序运行缓慢或无响应	解决应用程序故障
连接失败	恢复桌面连接
会话运行缓慢或无响应	恢复会话
录制会话	录制会话
视频运行缓慢或质量不佳	运行 HDX 通道系统报告

注意：

为确保计算机未处于维护模式，请从“用户详细信息”视图中查看“计算机详细信息”面板。

会话登录

“**用户详细信息**”视图 > “**会话登录**”选项卡显示会话登录过程的全面视图。此选项卡显示总登录持续时间、客户端和控制器持续时间以及 VDA 持续时间。“**会话登录**”选项卡包含“登录持续时间阶段”图表，其中绘制了各个登录阶段。使用此数据可排查用户登录问题。有关详细信息，请参阅诊断用户登录问题。

会话性能

“**会话性能**”选项卡具有增强的故障排除工作流，首先能够关联实时指标以识别用户会话中的问题。“**会话拓扑**”面板提供连接的 HDX 会话的会话内路径的可视化表示。“**性能指标**”面板提供会话指标的趋势，例如 ICARTT、ICA 延迟、每秒帧数、可用输出带宽和已用输出带宽，有助于指示这些指标随时间的变化情况。有关详细信息，请参阅诊断会话性能问题。

搜索技巧

当您在搜索字段中键入用户名时，Director 会在 Active Directory 中搜索配置为支持 Director 的所有站点中的用户。

当您在搜索字段中键入多用户计算机名称时，Director 会显示指定计算机的“计算机详细信息”。

当您在搜索字段中键入端点名称时，Director 会使用连接到特定端点的未经身份验证（匿名）和已通过身份验证的会话。此搜索可用于排查未经身份验证的会话。请确保端点名称是唯一的，以便能够排查未经身份验证的会话。

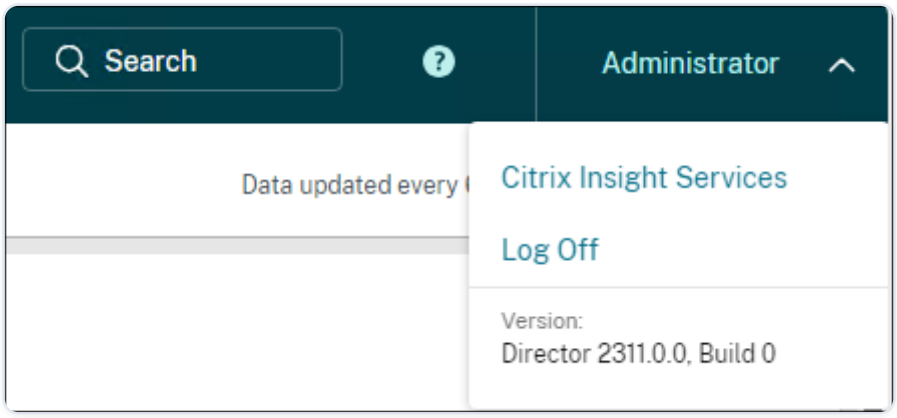
搜索结果还包括当前未使用或未分配给计算机的用户。

- 搜索不区分大小写。
- 部分输入会生成可能的匹配项列表。
- 在您键入由空格分隔的两部分名称的几个字母后，结果将包含两个字符串的匹配项。两部分名称的示例包括用户名、姓氏和名字，或显示名称。例如，如果您键入 jo rob，结果可能包括“John Robertson”或“Robert Jones”等字符串。

要返回登录页面，请单击 **Director 徽标**。

访问 Citrix 洞察服务

您可以从 Director 中的“**用户**”下拉列表中访问 Citrix Insight Services (CIS)，以获取额外的诊断见解。CIS 中可用的数据来自包括 Call Home 和 Citrix Scout 在内的源。



将故障排除信息上传到 Citrix 技术支持

从单个 Delivery Controller™ 或 VDA 运行 Citrix Scout 以捕获关键数据点和 Citrix Diagnostics Facility (CDF) 跟踪，从而对选定的计算机进行故障排除。Scout 提供了将数据安全上传到 CIS 平台的功能，以协助 Citrix 技术支持进行故障排除。Citrix 技术支持使用 CIS 平台来缩短解决客户报告问题所需的时间。

Scout 随 Citrix Virtual Apps and Desktops™ 组件一起安装。根据 Windows 版本，当您安装或升级到 Citrix Virtual Apps and Desktops 时，Scout 会显示在“**Windows 开始**”菜单或“开始”屏幕中。

要启动 Scout，请从“开始”菜单或“开始”屏幕中选择“**Citrix \> Citrix Scout**”。

有关使用和配置 Scout 的信息以及常见问题解答，请参阅 CTX130147。

诊断会话启动问题

除了 诊断用户登录问题 部分中提到的登录过程阶段之外，Director 还会显示会话启动持续时间。在“**用户详细信息**”页面和“**计算机详细信息**”页面上，这分为 Workspace App 会话启动持续时间和 VDA 会话启动持续时间。这两个持续时间还包含各个阶段，其启动持续时间也会显示。此数据可帮助您了解和排查会话启动持续时间过长的问题。此外，会话启动中涉及的每个阶段的时间持续时间有助于排查与各个阶段相关的问题。例如，如果驱动器映射时间过长，您可以检查 GPO 或脚本中是否正确映射了所有有效驱动器。此功能适用于 Delivery Controller 7 1906 及更高版本以及 VDA 1903 及更高版本。

先决条件

确保满足以下先决条件，才能显示会话启动持续时间数据：

- Delivery Controller™ 7 1906 或更高版本。
- VDA 1903 或更高版本。
- Citrix End User Experience Monitoring (EUEM) 服务必须在 VDA 上运行。

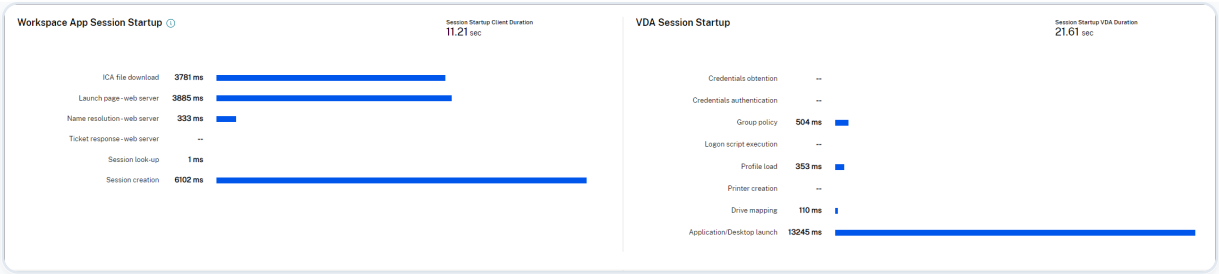
限制

当 Director 显示会话启动持续时间数据时，适用以下限制。

- 会话启动持续时间仅适用于 HDX™ 会话。
- 对于从 iOS 和 Android 操作系统启动的会话，仅提供 VDA 启动持续时间。
- ICA® 文件下载持续时间 (IFDCD) 仅在从浏览器启动时检测到 Workspace App 时可用。
- 对于从 Mac OS 启动的会话，IFDCD 仅适用于 Workspace App 1902 或更高版本。
- 对于从 Windows OS 启动的会话，IFDCD 适用于 Workspace app 1902 及更高版本。对于早期版本，IFDCD 仅显示从浏览器启动且检测到 Workspace app 的应用程序启动。

注意：

- 如果满足先决条件后会话启动持续时间显示仍有问题，请按照 CTX130320 中所述查看 Director 服务器和 VDA 日志。 对于共享会话（在同一会话中启动多个应用程序），Workspace App 启动指标将显示最新连接或最新应用程序启动的数据。
- VDA 会话启动中的某些指标不适用于重新连接。在这种情况下，将显示一条消息。



Workspace App 会话启动阶段

会话启动客户端持续时间 (SSCD)

当此指标较高时，表示存在导致启动时间过长的客户端问题。查看后续指标以确定问题的可能根本原因。SSCD 尽可能接近请求（鼠标单击）的时间开始。它在客户端设备和 VDA 之间的 ICA 连接建立时结束。在共享会话的情况下，此持续时间会短得多，因为创建新服务器连接所需的大部分设置成本都不会产生。在下一级别，有几个详细指标可用。

ICA 文件下载持续时间

这是客户端从服务器下载 ICA 文件所需的时间。整个过程如下：

1. 用户在 Workspace 应用程序中单击资源（应用程序或桌面）。

2. 用户的请求通过 Citrix Gateway（如果已配置）发送到 StoreFront™，StoreFront™ 将请求发送到 Delivery Controller。
3. Delivery Controller 查找请求的可用计算机，并将计算机信息和其他详细信息发送到 StoreFront。此外，StoreFront 从安全票证颁发机构请求并接收一次性票证。
4. StoreFront 生成 ICA 文件并通过 Citrix Gateway（如果已配置）将其发送给用户。

IFDCD 表示完成整个过程（步骤 1-4）所需的时间。当客户端收到 ICA 文件时，IFDCD 持续时间停止计数。

LPWD 是此过程的 StoreFront 组件。

如果 IFDCD 较高（但 LPWD 正常），则启动的服务器端处理成功，但客户端设备和 StoreFront 之间存在通信问题。这通常是由于两台计算机之间的网络问题造成的。因此，您可以首先排查潜在的网络问题。

启动页面 WEB 服务器持续时间 (LPWD)

这是在 StoreFront 上处理启动页面 (launch.aspx) 所需的时间。如果 LPWD 较高，则 StoreFront 上可能存在瓶颈。

可能的原因包括：

- StoreFront 上的负载过高。尝试通过检查 Internet Information Services (IIS) 日志和监控工具、任务管理器、性能监视器等来确定速度变慢的原因。
- StoreFront 在与其他组件（例如 Delivery Controller）通信时遇到问题。检查 StoreFront 和 Delivery Controller 之间的网络连接是否缓慢，或者某些 Delivery Controller 是否已关闭或过载。

名称解析 WEB 服务器持续时间 (NRWD)

这是 Delivery Controller 将已发布的应用程序/桌面名称解析为 VDA 计算机 IP 地址所需的时间。

当此指标较高时，表示 Delivery Controller 解析已发布的应用程序名称到 IP 地址所需的时间较长。

可能的原因包括客户端问题、Delivery Controller 问题（例如 Delivery Controller 过载）或它们之间的网络链接问题。

票证响应 WEB 服务器持续时间 (TRWD)

此持续时间表示从安全票证颁发机构 (STA) 服务器或 Delivery Controller 获取票证（如有必要）所需的时间。当此持续时间较高时，表示 STA 服务器或 Delivery Controller 过载。

会话查找客户端持续时间 (SLCD)

此持续时间表示查询每个会话以托管请求的已发布应用程序所需的时间。在客户端执行检查以确定现有会话是否可以处理应用程序启动请求。所使用的方法取决于会话是新建的还是共享的。

会话创建客户端持续时间 (SCCD)

此持续时间表示从 wfica32.exe（或类似的等效文件）启动到建立连接所需的时间。

VDA 会话启动阶段

会话启动 VDA 持续时间 (SSVD)

此持续时间是高级别的服务器端连接启动指标，它包含 VDA 执行整个启动操作所需的时间。当此指标较高时，表示存在 VDA 问题导致会话启动时间增加。这包括 VDA 执行整个启动操作所花费的时间。

凭据获取 VDA 持续时间 (COVD)

VDA 获取用户凭据所需的时间。

如果用户未能及时提供凭据，此持续时间可能会人为增加。因此，它不包含在 VDA 启动持续时间中。此时间仅在以下情况下可能很重要：使用手动登录且显示服务器端凭据对话框（或者在登录开始前显示法律声明）。

凭据身份验证 VDA 持续时间 (CAVD)

这是 VDA 根据身份验证提供程序验证用户凭据所需的时间。它们可以是 Kerberos、Active Directory 或安全支持提供程序接口 (SSPI)。

组策略 VDA 持续时间 (GPVD)

此持续时间是登录期间应用组策略对象所需的时间。

登录脚本执行 VDA 持续时间 (LSVD)

这是 VDA 运行用户登录脚本所需的时间。

考虑使用户或组的登录脚本异步化。考虑优化任何应用程序兼容性脚本或改用环境变量。

配置文件加载 VDA 持续时间 (PLVD)

这是 VDA 加载用户配置文件所需的时间。

如果此持续时间较长，请考虑您的用户配置文件配置。漫游配置文件的大小和位置会导致会话启动缓慢。当用户登录到启用了终端服务漫游配置文件和主文件夹的会话时，漫游配置文件内容和对该文件夹的访问会在登录期间进行映射。这会占用额外的资源。有时，这会消耗大量的 CPU 使用率。考虑使用带有重定向个人文件夹的 **Terminal Services 主**文件夹来缓解此问题。通常，请考虑使用 Citrix Profile Management 在 Citrix 环境中管理用户配置文件。如果您正在使用 Citrix Profile

Management 并且登录时间较长，请检查您的防病毒软件是否正在阻止 Citrix Profile Management 工具。

打印机创建 VDA 持续时间 (PCVD)

这是 VDA 同步映射用户客户端打印机所需的时间。如果配置设置为异步执行打印机创建，则不会为 PCVD 记录该值，因为它不影响会话启动的完成。

映射打印机所花费的时间过长通常是打印机自动创建策略设置的结果。用户客户端设备上本地添加的打印机数量以及您的打印配置会直接影响会话启动时间。会话启动时，Citrix Virtual Apps and Desktops™ 必须在客户端设备上创建每个本地映射的打印机。考虑重新配置打印策略，以减少创建的打印机数量，尤其是在用户拥有许多本地打印机时。为此，请在 Delivery Controller 和 Citrix Virtual Apps and Desktops 中编辑打印机自动创建策略。

驱动器映射 VDA 持续时间 (DMVD)

这是 VDA 映射用户客户端驱动器、设备和端口所花费的时间。

确保您的基本策略包含禁用未使用的虚拟通道的设置。例如，音频或 COM 端口映射，以优化 ICA 协议并提高整体会话性能。

应用程序/桌面启动 VDA 持续时间 (ALVD/DLVD)

此阶段是 Userinit 和 Shell 持续时间的组合。当用户登录到 Windows 计算机时，winlogon 会运行 userinit.exe。Userinit.exe 运行登录脚本，重新建立网络连接，然后启动 Explorer.exe。Userinit 表示从 userinit.exe 启动到虚拟桌面或应用程序用户界面启动之间的时间。Shell 持续时间是指从用户界面初始化到用户获得键盘和鼠标控制之间的时间。

会话创建 VDA 持续时间 (SCVD)

此时间包括 VDA 上会话创建时间中的任何杂项延迟。

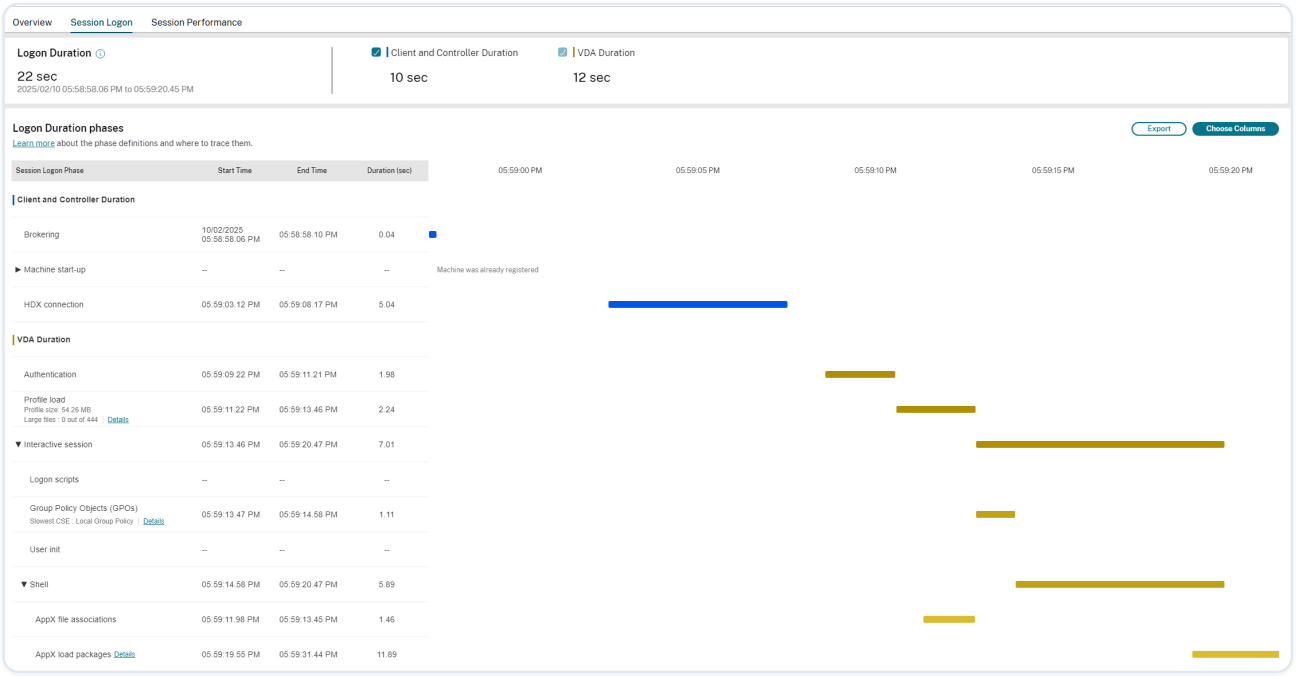
诊断用户登录问题

“**用户详细信息**”视图 > “**会话登录**”选项卡显示会话登录过程的全面视图。此选项卡显示总登录持续时间、客户端和控制器持续时间以及 VDA 持续时间。使用此数据可排查用户登录问题。

登录持续时间仅针对使用 HDX 首次连接到桌面或应用程序时进行测量。此数据不包括尝试使用远程桌面协议连接或从断开连接的会话重新连接的用户。具体而言，当用户最初使用非 HDX 协议连接并使用 HDX 重新连接时，不测量登录持续时间。

当用户登录到 Citrix Virtual Apps and Desktops™ 时，Monitor Service 会跟踪登录过程的各个阶段。这些阶段从用户通过 Citrix Workspace™ 应用程序连接时开始，直到应用程序或桌面准备就绪可供使用时结束。

“**会话登录**”选项卡包含“登录持续时间”阶段图表，其中绘制了各种登录阶段。登录持续时间表示建立连接并从 Delivery Controller™ 获取应用程序或桌面所花费的时间，以及对虚拟应用程序或桌面进行身份验证和登录所花费的时间。持续时间信息以秒（或秒的分数）为单位显示。



登录持续时间阶段图表清晰地显示了不同的登录阶段及其开始和结束时间。该图表显示了各个登录阶段的重叠情况。总登录时间可能不是各个登录阶段持续时间之和。这是因为各个阶段可能重叠，并且并非所有登录阶段都属于此表示形式。此外，某些阶段甚至可能在用户开始与虚拟应用程序或桌面交互后仍在继续，并且此持续时间不作为整体登录持续时间的一部分进行测量。

使用此视图可识别导致会话启动延迟的特定登录阶段。每个登录阶段的定义以及可从中跟踪信息的事件源有助于进一步排查故障。将鼠标悬停在图表上会显示一个工具提示，其中包含当前会话的阶段持续时间、用户的 7 天平均值以及交付组的 7 天平均值。此信息有助于将当前会话登录持续时间与 7 天平均值进行比较。对于 GPO 和配置文件详细信息，您可以进一步深入查看子阶段测量值。此可视化有助于轻松理解和排查与登录持续时间相关的问题。

先决条件

请确保满足以下先决条件，以便显示登录持续时间数据和深入分析：

1. 在 VDA 上安装 **赛睿用户配置文件管理器** 和 **赛睿用户配置文件管理器 WMI 插件**。
2. 确保 Citrix Profile Management Service 正在运行。
3. 对于 XenApp 和 XenDesktop 7.15 及更早版本站点，请禁用 GPO 设置“**不处理旧版运行列表**”。
4. 必须启用审核进程跟踪才能进行交互式会话深入分析。
5. 对于 GPO 深入分析，请增加组策略操作日志的大小。

注意：

- 登录持续时间仅在默认 Windows 外壳程序 (explorer.exe) 上受支持，而不支持自定义外壳程序。
- 仅当在 Remote PC Access 安装期间将 **Citrix User Profile Manager** 和 **Citrix User Profile Manager WMI Plugin** 作为额外组件安装时，Remote PC Access 的登录持续时间才可用。有关详细信息，请参阅 Remote PC Access 配置和序列注意事项 中的步骤 4。

排查用户登录问题的步骤

1. 在“**用户详细信息**”视图 > “**会话登录**”选项卡中，使用“登录持续时间”图表排查登录状态。
   - 如果用户正在登录，视图会反映登录过程。
   - 如果用户已登录，登录持续时间面板会显示用户登录到当前会话所花费的时间。
2. 检查登录过程的各个阶段。

登录过程阶段

客户端和控制器持续时间

从用户单击应用程序或桌面图标到键盘和鼠标控制权移交给最终用户以与会话交互所花费的时间。
代理
决定为用户分配哪个桌面所花费的时间。
计算机启动
如果会话需要启动计算机，这是启动虚拟机所花费的时间。以下小节提供了在不同阶段启动虚拟机所花费时间的细分：

- **开机** - 显示启动虚拟机所花费的时间
- **启动和注册** - 显示启动和注册虚拟机所花费的时间

您可以使用可折叠按钮折叠或展开**计算机启动**下的选项。
HDX 连接
完成从客户端到虚拟机的 HDX 连接设置所需步骤的时间。

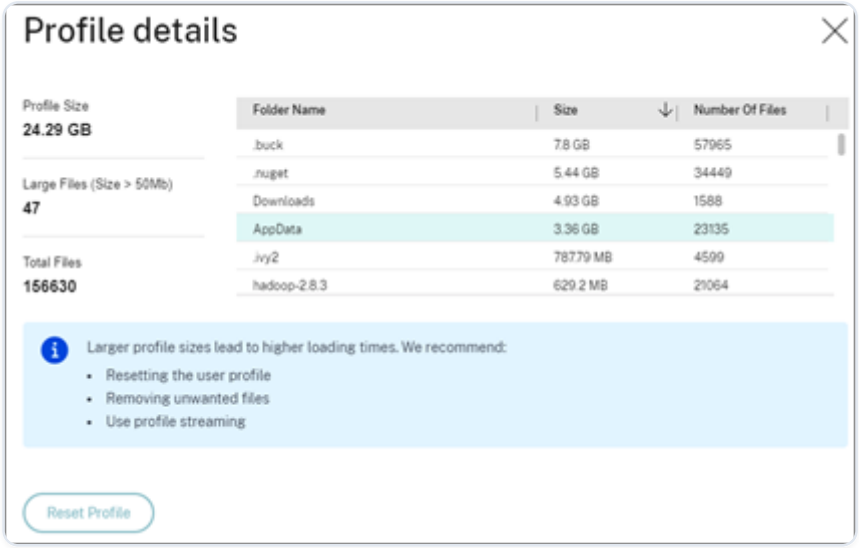
VDA 持续时间

VDA 上创建会话所花费的时间。
身份验证
完成远程会话身份验证所需的时间。
配置文件加载

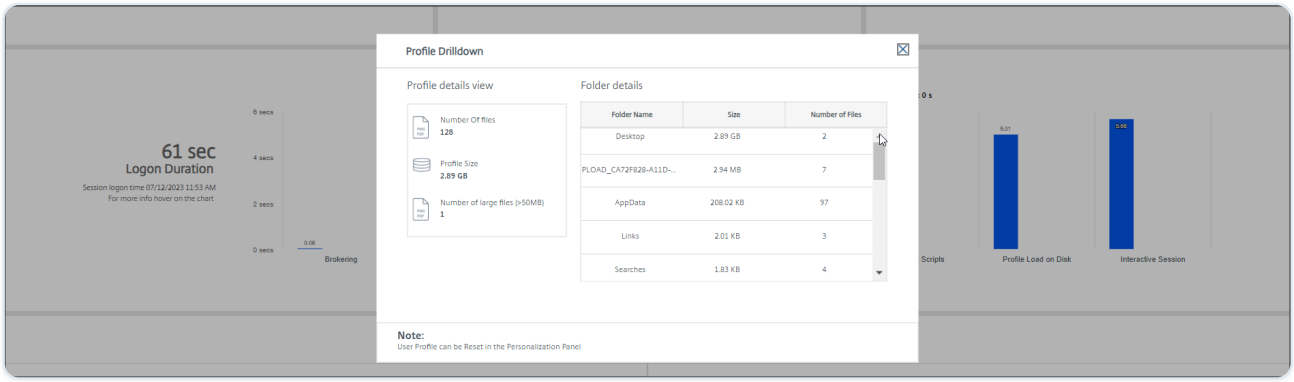
如果为用户或虚拟机配置了配置文件设置，则这是配置文件加载所需的时间。

如果配置了 Citrix Profile Management 和 FSLogix，则“配置文件加载”栏会包含 Citrix Profile Management 和 FSLogix 处理用户配置文件所花费的时间。此信息有助于管理员排查配置文件处理持续时间过长的问题。当配置了 Profile Management 和 FSLogix 时，“配置文件加载”栏会显示增加的持续时间。此增加是由此增强功能引起的，并不表示性能下降。此增强功能适用于 VDA 2407 或更高版本。

将鼠标悬停在“配置文件加载”栏上会显示一个工具提示，其中显示当前会话的用户配置文件详细信息。



单击**详细信息**以进一步深入分析配置文件根文件夹中的每个单独文件夹（例如，C:/Users/username）、其大小以及文件数量（包括嵌套文件夹中的文件）。



配置文件深入分析功能适用于 Delivery Controller 7 1811 或更高版本以及 VDA 1811 或更高版本。使用配置文件深入分析信息，您可以解决配置文件加载时间过长的问题。您可以：

- 重置用户配置文件
- 通过删除不需要的大文件来优化配置文件
- 减少文件数量以减少网络负载
- 使用配置文件流

默认情况下，配置文件根目录中的所有文件夹都显示在向下钻取中。要隐藏文件夹可见性，请在 VDA 计算机上编辑以下注册表值：

警告：

错误地添加和编辑注册表可能会导致严重问题，可能需要重新安装操作系统。Citrix 不保证可以解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。编辑注册表之前，请务必备份注册表。

1. 在 VDA 上，在 HKEY_LOCAL_MACHINE\Software\Citrix\Director\ 下添加新的注册表值 **ProfileFoldersNameHidden**。
2. 将值设置为 1。此值必须是 DWORD（32 位）值。现在已禁用文件夹名称可见性。
3. 要使文件夹名称再次可见，请将值设置为 0。

注意：

您可以使用 GPO 或 PowerShell 命令在多台计算机上应用注册表值更改。有关使用 GPO 部署注册表更改的详细信息，请参阅博客。

附加信息

- 配置文件深入分析不考虑重定向的文件夹。
- 根文件夹中的 NTUser.dat 文件可能对最终用户不可见。但是，它们包含在配置文件向下钻取中，并显示在“**根文件夹**”的文件列表中。
- AppData 文件夹中的某些隐藏文件不包含在配置文件向下钻取中。
- 由于某些 Windows 限制，文件数量和配置文件大小数据可能与“个性化”面板中的数据不匹配。

交互式会话

交互式会话是指用户配置文件加载后，将键盘和鼠标控制权“移交”给用户所需的时间。它通常是登录过程所有阶段中最长的持续时间，计算方式为：**交互式会话持续时间 = 桌面就绪事件时间戳（VDA 上的 EventId 1000）- 用户配置文件加载事件时间戳（VDA 上的 EventId 2）**。交互式会话有三个子阶段：Pre-userinit、Userinit 和 Shell。将鼠标悬停在“交互式会话”上可查看显示以下内容的工具提示：

- 子阶段
- 每个子阶段所用的时间

- 这些子阶段之间的总累计时间延迟

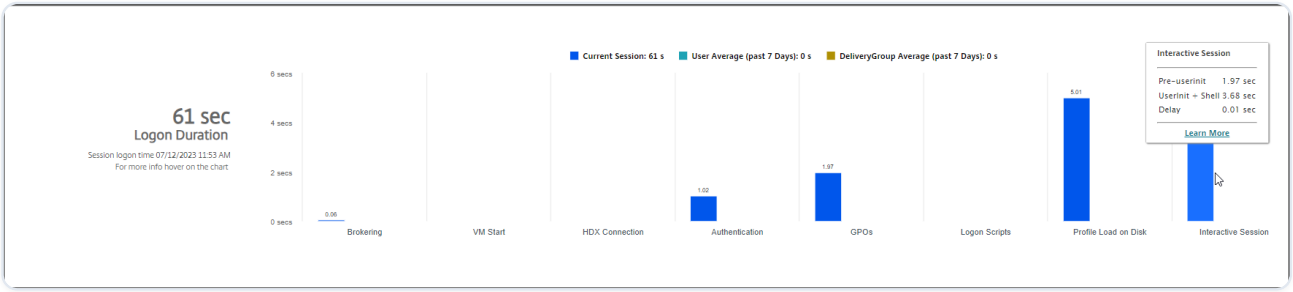
您可以使用可折叠按钮折叠或展开“**交互式会话**”下的选项。

> **注意：**
>
> 此功能适用于 VDA 1811 及更高版本。如果您在早于 7.18 的站点上启动了会话，然后升级到 7.18 或更高版本，则会显示“由于服务器错误，向下钻取不可用”消息。但是，如果您在升级后启动了会话，则不会显示错误消息。

> 要查看每个子阶段的时间持续时间，请在 VM (VDA) 上启用“审核进程跟踪”。当“审核进程跟踪”被禁用（默认）时，将显示 Pre-userinit 的时间持续时间以及 Userinit 和 Shell 的组合时间持续时间。您可以通过组策略对象 (GPO) 启用“审核进程跟踪”，如下所示：

1. 创建 GPO 并使用 GPO 编辑器对其进行编辑。
2. 转到 **计算机配置 > Windows 设置 > 安全设置 > 本地策略 > 审核策略**。
3. 在右侧窗格中，双击**审核进程跟踪**。
4. 选择**成功**，然后单击“确定”。
5. 将此 GPO 应用于所需的 VDA 或组。

有关审核进程跟踪以及启用或禁用它的详细信息，请参阅 Microsoft 文档中的审核进程跟踪。



“用户详细信息”视图中的“登录持续时间”面板。

- **交互式会话 – Pre-userinit：** 交互式会话中与组策略对象和脚本重叠的部分。可以通过优化 GPO 和脚本来缩短此子阶段。
- **交互式会话 – Userinit：** 当用户登录到 Windows 计算机时，Winlogon 会运行 userinit.exe。Userinit.exe 运行登录脚本，重新建立网络连接，然后启动 Windows 用户界面 Explorer.exe。交互式会话的此子阶段表示从 Userinit.exe 启动到虚拟桌面或应用程序用户界面启动之间的时间。
- **交互式会话 – Shell：** 在上一阶段，Userinit 开始初始化 Windows 用户界面。Shell 子阶段捕获从用户界面初始化到用户获得键盘和鼠标控制权之间的时间。
- **延迟：** 这是 **Pre-userinit 和 Userinit** 子阶段与 **Userinit 和 Shell** 子阶段之间的累计时间延迟。

总登录时间并非这些阶段的精确总和。例如，某些阶段并行发生，而在某些阶段，会发生更多处理，这可能导致登录持续时间长于总和。 总登录时间不包括 ICA® 空闲时间，即 ICA 文件下载与应用程序的 ICA 文件启动之间的时间。 要启用应用程序启动时自动打开 ICA 文件，请将浏览器配置为在下载 ICA 文件时自动启动 ICA 文件。有关详细信息，请参阅 CTX804493。

> **注意：**
>
> 登录持续时间图表以秒为单位显示登录阶段。任何小于一秒的持续时间值都显示为亚秒值。大于一秒的值四舍五入到最接近的 0.5 秒。该图表设计为将最高的 Y 轴值显示为 200 秒。任何大于 200 秒的值都将显示在条形图上方，并显示实际值。

登录脚本
如果为会话配置了登录脚本，则这是运行登录脚本所需的时间。
GPO
如果在虚拟机上启用了组策略设置，则这是登录期间应用组策略对象所需的时间。当您将鼠标悬停在 GPO 条形图上时，将显示根据 CSE（客户端扩展）应用每个策略所需时间的详细信息作为工具提示。



单击“**详细信息**”可查看包含策略状态和相应 GPO 名称的表格。详细信息中的时间持续时间仅表示 CSE 处理时间，不计入总 GPO 时间。您可以复制详细信息表格以进行进一步故障排除或在报告中使用。策略的 GPO 时间从事件查看器日志中检索。日志可能会根据为操作日志分配的内存（默认大小为 4 MB）而被覆盖。有关增加操作日志大小的更多信息，请参阅 Microsoft TechNet 文章 配置事件日志。
用户初始化

当用户登录到 Windows 计算机时，Winlogon 运行 userinit.exe。Userinit.exe 运行登录脚本，重新建立网络连接，然后启动 Windows 用户界面 Explorer.exe。交互式会话的此子阶段表示从 Userinit.exe 启动到虚拟桌面或应用程序用户界面启动之间的时间。

外壳

外壳子阶段捕获了从用户界面初始化到用户获得键盘和鼠标控制之间的时间。
AppX 文件关联
在新的 VDA 会话期间关联 AppX 文件所需的时间。
AppX 加载包
在新的 VDA 会话期间加载 AppX 包所需的时间。

> **注意：**
>
> uberAgent 必须与 Director 集成，才能在新的 VDA 会话期间收集 AppX 包加载持续时间。有关详细信息，请参阅 Citrix uberAgent 与 Director 集成。

导出数据

除了默认的“登录持续时间阶段”表选项（即“会话登录阶段”和“持续时间”）之外，您还可以在“会话登录”页面上选择以下列：

- 开始时间
- 结束时间
- 交付组 - 7 天平均值（秒）
- 用户 - 7 天平均值（秒）

您还可以将上述数据导出到 .CSV 文件。

故障排除技巧

要识别图表中的异常或意外值，请将当前会话每个阶段所花费的时间与该用户过去七天的平均持续时间以及此交付组中所有用户过去七天的平均持续时间进行比较。

根据需要上报。例如，如果**计算机启动**缓慢，问题可能出在虚拟机管理程序中，因此您可以将其上报给虚拟机管理程序管理员。

检查异常差异，包括：

- 缺少（当前）登录条
- 当前持续时间与此用户的平均持续时间之间存在重大差异。原因包括：

  - 安装了新应用程序。
  - 发生了操作系统更新。
  - 进行了配置更改。
  - 用户配置文件大小过大。在这种情况下，配置文件加载时间较长。
- 用户登录次数（当前和平均持续时间）与交付组平均持续时间之间存在重大差异。

如有需要，请单击**重新启动**以观察用户的登录过程，从而排查**计算机启动**或**代理**等问题。

诊断会话性能问题

用户详细信息页面上的**会话性能**选项卡具有增强的故障排除工作流，可帮助识别 HDX™ 用户会话中的问题。**会话拓扑和性能指标**面板有助于在单个视图中关联会话的组件视图和多个性能指标，并缩短解决会话体验问题的平均时间。

会话性能视图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-session-performance.png)

端到端网络跃点视图

端到端网络跃点视图提供了完整会话路径的可视化表示，极大地有助于故障排除。您可以从**用户详细信息** > **会话性能** > **会话拓扑**访问此视图。端到端网络跃点视图显示了连接的 HDX 会话的组件、元数据、链接和已发布的应用程序。

此视图可帮助管理员执行以下操作：

- 了解会话数据流。
- 识别特定跃点处的性能瓶颈。

会话性能指标

以下指标可根据上下文提供，以帮助管理员了解给定会话的性能。端到端网络跃点视图中显示的指标以近实时方式提供，并根据 UI 中显示的间隔定期刷新。

端点指标

端点指标对于排查 Citrix® 会话性能问题至关重要，因为它们提供了用户体验“最后一英里”的见解，并揭示了用户即时环境的详细信息。这些指标有助于识别本地瓶颈，例如 Wi-Fi 信号差、网络吞吐量低、端点设备限制，从而区分服务器端和客户端问题。通过与会话拓扑中的指标结合提供整体视图，端点数据可以更快地识别根本原因并更快地解决性能问题，从而改善用户体验。

使用 Citrix Studio 中的策略，根据您的要求启用或禁用列出的端点指标的收集。这些策略为 Citrix 管理员提供了精细的控制，以根据您的合规性要求报告指标。

策略名称	策略描述	UI 指标	默认值	值选项	VDA WINDOWS 版本	VDA MAC 版本	VDA LINUX 版本
端点统计间隔	允许从用户端点收集端点网络详细信息。启用此策略是其他端点相关策略生效的先决条件。	Wi-Fi 信号强度、网络接口类型、吞吐量（入站或出站）、链接速度、工作区类型、端点 CPU、端点内存、端点 GPU	启用	已启用或已禁用。可选择将频率修改为 60 秒 - 3600 秒之间。建议值为 60 秒。	2407 或更高版本	2607	2607
端点位置数据收集	允许使用 Locus 服务从用户端点收集端点位置和 ISP 详细信息 - `<https://locus.analytics.cloud.com>`	公共 IP 地址、国家/地区、城市和互联网服务提供商。	已禁用	已启用或已禁用	2411 或更高版本	2607	2607

策略名称	策略描述	UI 指标	默认值	值选项	VDA WINDOWS 版本	VDA MAC 版本	VDA LINUX 版本
端点网络延迟测量间隔	允许测量和收集端点与信标主机之间的网络延迟 - `<https://downloadplugins.citrix.com>`	网络延迟（在“端点网络详细信息”下）	已禁用	已启用或已禁用。可选择将频率修改为 60 秒 - 3600 秒之间。建议值为 60 秒。	2411 或更高版本	2607	2607

注意：

从 Citrix Virtual Apps and Desktops™ 2507 或更高版本开始，**端点位置数据收集**策略和**端点网络延迟测量间隔**策略默认处于禁用状态。因此，除非在 Studio 中手动启用这些策略，否则 Director 中无法获取相关数据。

可用的端点指标如下所示：

- 端点名称
- 端点 IP
- 端点操作系统
- Citrix Workspace™ 应用程序版本

下表列出了取决于受支持产品版本的指标：

功能名称	UI 参数	VDA WINDOWS 版本	VDA MAC 版本	VDA LINUX 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
端点网络详细信息	网络接口类型	2407 或更高版本	不适用	不适用	2405.10 或更高版本	2409 或更高版本	2408 或更高版本	2411 或更高版本	2411 或更高版本
	信号强度	2407 或更高版本	不适用	不适用	2405.10 或更高版本	2409 或更高版本	2408 或更高版本	不适用	不适用
	端点吞吐量（传入、传出）	2407 或更高版本	不适用	不适用	2405.10 或更高版本	2409 或更高版本	2408 或更高版本	不适用	不适用
	链接速度	2407 或更高版本	不适用	不适用	2405.10 或更高版本	2409 或更高版本	2408 或更高版本	2411 或更高版本	2411 或更高版本
	端点公共 IP 地址	2411 或更高版本	不适用	不适用	2409 或更高版本	2409 或更高版本	2408 或更高版本	2411 或更高版本	2411 或更高版本
	端点城	2411 或更	不适用	不适用	2409 或更	2409 或更	2408 或更	2411 或更	2411 或更

功能名称	UI 参数	VDA WINDOWS 版本	VDA MAC 版本	VDA LINUX 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
	市，端点国家/地区	高版本			高版本	高版本	高版本	高版本	高版本
	互联网服务提供商	2411 或更高版本	不适用	不适用	2409 或更高版本	2409 或更高版本	2408 或更高版本	2411 或更高版本	2411 或更高版本
	工作区类型	2411 或更高版本	不适用	不适用	2409 或更高版本	2409 或更高版本	2408 或更高版本	2411 或更高版本	2411 或更高版本
	访问类型（通过 Workspace / StoreFront）	2411 或更高版本	不适用	不适用	2409 或更高版本	2409 或更高版本	2408 或更高版本	2411 或更高版本	2411 或更高版本
	端点 CPU	2411 或更高版本	不适用	不适用	2409 或更高版本	2409 或更高版本	2408 或更高版本	不适用	2411 或更高版本

功能名称	UI 参数	VDA WINDOWS 版本	VDA MAC 版本	VDA LINUX 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
	端点内存	2411 或更高版本	不适用	不适用	2409 或更高版本	2409 或更高版本	2408 或更高版本	不适用	2411 或更高版本
	端点 GPU	2411 或更高版本	不适用	不适用	2409 或更高版本	2409 或更高版本	2408 或更高版本	不适用	不适用
	网络延迟	2411 或更高版本	不适用	不适用	2409 或更高版本	2409 或更高版本	2408 或更高版本	2411 或更高版本	2411 或更高版本

数据定义：

UI 参数	描述
端点名称	用于会话的用户端点设备的名称。
端点 IP	虚拟投递代理 (VDA) 可用的端点 IP 地址。它可能包含端点设备的私有或公共 IP 地址。
端点操作系统	端点设备的操作系统
Citrix Workspace 应用程序版本	已安装的 Citrix Workspace 应用程序版本
信号强度	显示无线信号的质量和强度。

UI 参数	描述
端点吞吐量（传入、传出）	指示数据进出网络接口的传输速率。类似于在端点上观察到的上传和下载互联网速度。
链接速度	指定网络连接类型，例如以太网、Wi-Fi 或蜂窝网络。
网络接口类型	表示网络连接的最大数据传输速率。
端点公共 IP 地址	您的互联网服务提供商分配给您设备的外部 IP 地址。
端点城市，端点国家/地区	设备的地理位置，包括国家/地区和城市。
互联网服务提供商	向最终用户设备提供互联网访问的公司名称。
工作区类型	正在使用的工作区类型，可以是 Citrix Workspace 应用程序或 Web 浏览器。
访问类型（通过 Workspace / StoreFront）	访问资源的方法，通过 Citrix Workspace 或 StoreFront。
端点 CPU	当前正在使用的 CPU 资源百分比。
端点内存	当前正在使用的内存资源百分比。
端点 GPU	当前正在使用的 GPU 资源百分比。
网络延迟测试	网络中经历的时间延迟，以毫秒为单位测量。

网络指标

网络指标对于 Citrix 会话故障排除至关重要，因为 Citrix 会话的性能和稳定性在很大程度上取决于底层网络条件。与本地应用程序不同，Citrix 会话涉及通过网络流式传输交互式桌面或应用程序体验，这意味着任何网络不稳定或瓶颈都将直接影响用户对性能的感知。

使用 Citrix Studio 中的策略，根据您的要求启用或禁用收集列出的网络指标。这些策略为 Citrix 管理员提供了精细的控制，以根据您的合规性要求报告指标。

策略名称	策略描述	UI 指标	默认值	值选项	虚拟投递代理版本
网络遥测	允许收集用户端点和后端组件之间的网络详细信息。	Citrix Gateway 和 Citrix Gateway 服务的所有 HDX insights 指标	已禁用	已启用或已禁用。可选择将频率修改为 60 秒 - 3600 秒之间。建议值为 60 秒。	Gateway 服务为 2411 或更高版本。Citrix Gateway 为 2503 或更高版本

Citrix 网关服务

下表列出了取决于受支持产品版本的指标：

功能名称	UI 参数	WINDOWS VDA 版本	MAC VDA 版本	LINUX VDA 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
网络指标	L7 服务器延迟	2411 或更高版本	2507 或更高版本	2507 或更高版本	2409 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用
	L7 客户端延迟	2411 或更高版本	2507 或更高版本	2507 或更高版本	2409 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用
	客户端重传 注意：仅适	2411 或更高版本	2507 或更高版本	2507 或更高版本	2409 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用

功能名称	UI 参数	WINDOWS VDA 版本	MAC VDA 版本	LINUX VDA 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
	用于 TCP 会话								
	吞吐量	2411 或更高版本	不适用	不适用	2409 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用

思杰网关

下表列出了取决于受支持产品版本的指标：

功能名称	UI 参数	思杰网关版本	WINDOWS VDA 版本	MAC 版本	LINUX 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
网络指标	WAN 延迟	Netscaler	2503 或	2507 或	2507 或	2503 或	2505 或	2505 或	不适用	不适用

功能名称	UI 参数	思杰网关版本	WINDOWS VDA 版本	MAC 版本	LINUX 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
		14.1-47.46 或更高版本	更高版本	更高版本	更高版本	更高版本	更高版本	更高版本		
	DC 延迟	Netscaler 14.1-47.46 或更高版本	2503 或更高版本	2507 或更高版本	2507 或更高版本	2503 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用
	服务器端重传	Netscaler 14.1-47.46 或更高版本	2503 或更高版本	2507 或更高版本	2507 或更高版本	2503 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用

功能名称	UI 参数	思杰网关版本	WINDOWS VDA 版本	MAC 版本	LINUX 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
	客户端重传	Netscaler 14.1-47.46 或更高版本	2503 或更高版本	2507 或更高版本	2507 或更高版本	2503 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用
	L7 服务器延迟	Netscaler 14.1-47.46 或更高版本	2503 或更高版本	2507 或更高版本	2507 或更高版本	2503 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用
	L7 客户端延迟	Netscaler 14.1-47.46 或更	2503 或更高版本	2507 或更高版本	2507 或更高版本	2503 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用

功能名称	UI 参数	思杰网关版本	WINDOWS VDA 版本	MAC 版本	LINUX 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
		高版本								
	客户端零窗口大小事件	Netscaler 14.1-47.46 或更高版本	2503 或更高版本	2507 或更高版本	2507 或更高版本	2503 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用
	客户端快速 RTO	Netscaler 14.1-47.46 或更高版本	2503 或更高版本	2507 或更高版本	2507 或更高版本	2503 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用
	服务器端零窗口大	Netscaler 14.1-47.46	2503 或更高版本	2507 或更高版本	2507 或更高版本	2503 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用

功能名称	UI 参数	思杰网关版本	WINDOWS VDA 版本	MAC 版本	LINUX 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
	小事件	或更高版本								
	服务器端快速 RTO	Netscaler 14.1-47.46 或更高版本	2503 或更高版本	2507 或更高版本	2507 或更高版本	2503 或更高版本	2505 或更高版本	2505 或更高版本	不适用	不适用

数据定义：

UI 参数	描述
WAN 延迟	由网络客户端（从 NetScaler® 到最终用户）引起的延迟。
DC 延迟	由网络服务器端（从 NetScaler 到后端服务器）引起的延迟。
L7 客户端延迟	在 ICA® 客户端和 NetScaler 实例之间观察到的平均 L7 延迟。此指标在交付路径中存在的非 Citrix 设备中很有用。

UI 参数	描述
L7 服务器延迟	在 NetScaler 设备和 Citrix Virtual App 之间观察到的平均 L7 延迟。当交付路径中存在非 Citrix 设备时，此指标很有用。
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标值较高表示由于重传导致带宽利用率高，但这不一定意味着用户体验不佳。注意：对于使用网关服务的会话，客户端重传仅适用于 TCP 会话。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。
客户端零窗口计数	客户端通告零 TCP 窗口的次数。
服务器端零窗口计数	服务器通告零 TCP 窗口的次数。

VDA 指标

功能名称	UI 参数	WINDOWS VDA 版本	MAC 版本	LINUX 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
VDA 指标	VDA CPU	2511 或更高版本	不适用	不适用	2503 或更高版本	2503 或更高版本	2503 或更高版本	不适用	不适用
	VDA 内存	2511 或更高版本	不适用	不适用	2503 或更高版本	2503 或更高版本	2503 或更高版本	不适用	不适用

功能名称	UI 参数	WINDOWS VDA 版本	MAC 版本	LINUX 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
	VDA 磁盘 IOPS	2511 或更高版本	不适用	不适用	2503 或更高版本	2503 或更高版本	2503 或更高版本	不适用	不适用
	VDA 磁盘延迟	2511 或更高版本	不适用	不适用	2503 或更高版本	2503 或更高版本	2503 或更高版本	不适用	不适用

HDX 指标

HDX 指标对于理解和排查用户虚拟体验的质量至关重要。这些指标直接衡量提供虚拟会话的 ICA/HDX 协议的性能。

注意：

ICA 指标从适用于 Windows 的 Citrix Workspace 应用程序版本 2405.10 或更高版本以及 Citrix Virtual Apps and Desktops 2407 或更高版本开始提供。但是，数据的更新和修复在最新版本中可用。有关每个数据点的推荐版本，请参阅下表：

功能名称	UI 参数	WINDOWS VDA 版本	MAC VDA 版本	LINUX VDA 版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本
ICA 指标	ICA RTT	2507 或更高版本	不适用	不适用	2503 或更高版本	2503 或更高版本	2503 或更高版本	2503 或更高版本
	网络延迟	2507 或更高版本	不适用	不适用	2503 或更高版本	2503 或更高版本	2503 或更高版本	2503 或更高版本
	HDX 连接类型	2411 或更高版本	不适用	不适用	2411 或更高版本	2411 或更高版本	2411 或更高版本	2411 或更高版本
	协议	2411 或更高版本	不适用	不适用	2411 或更高版本	2411 或更高版本	2411 或更高版本	2411 或更高版本
	EDT MTU	2411 或更高版本	不适用	不适用	2411 或更高版本	2411 或更高版本	2411 或更高版本	2411 或更高版本

数据定义：

UI 参数	描述
ICA RTT	衡量用户操作与屏幕响应之间的时间。从 Citrix Virtual Apps and Desktops 2507 版本开始，

UI 参数	描述
	Thinwire RTT 计数器表示此指标。以前的版本继续使用 EUEM RTT。
网络延迟	指示网络延迟和潜在的缓慢。从 Citrix Virtual Apps and Desktops 2503 版本开始，定义为客户端和服务器端延迟的总和。以前的版本继续使用 VDA 上报告的 HDX 延迟。
HDX 连接类型	用户会话的 HDX 连接类型。
协议	用于用户会话的底层协议。值可以是 *TCP* 或 *EDT*。
EDT MTU	MTU，即最大传输单元，是网络接口无需分段即可发送的最大数据包大小（以字节为单位）。EDT MTU 表示为用户的 EDT 会话建立的 MTU。

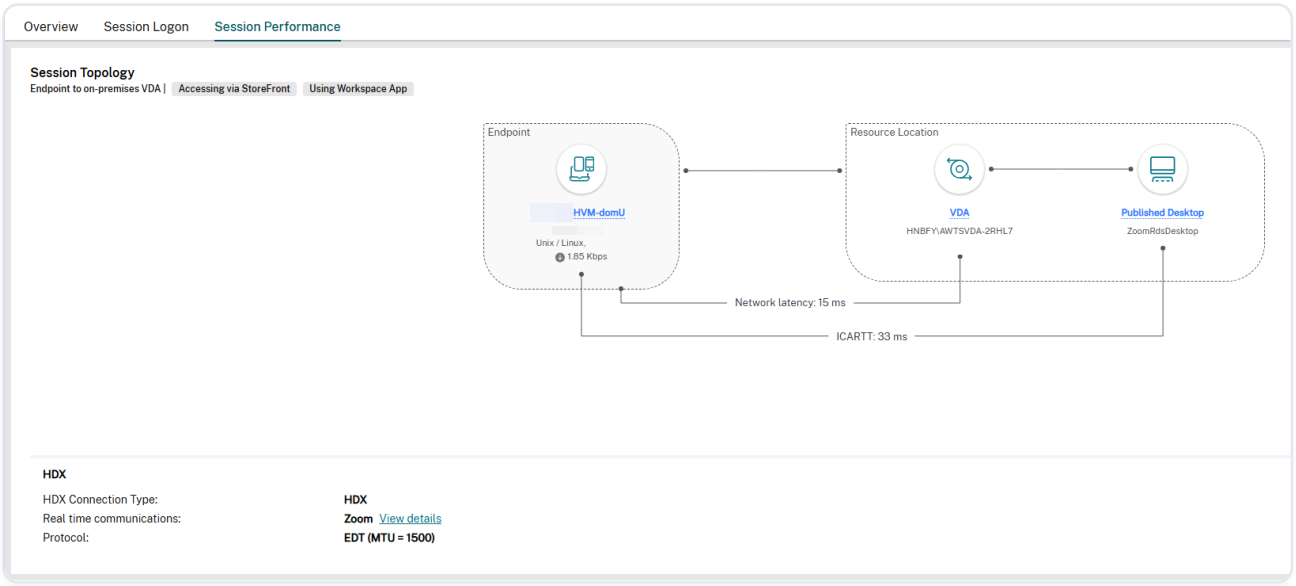
实时通信优化可见性

会话拓扑提供了 Citrix 会话中 Microsoft Teams、Zoom 和 WebEx 等实时通信 (RTC) 应用程序优化状态的全面可见性。它能查明应用程序是否已优化，并识别任何阻止最佳性能的缺失组件（例如必要的插件、插件管理或平台特定限制）。

优势：

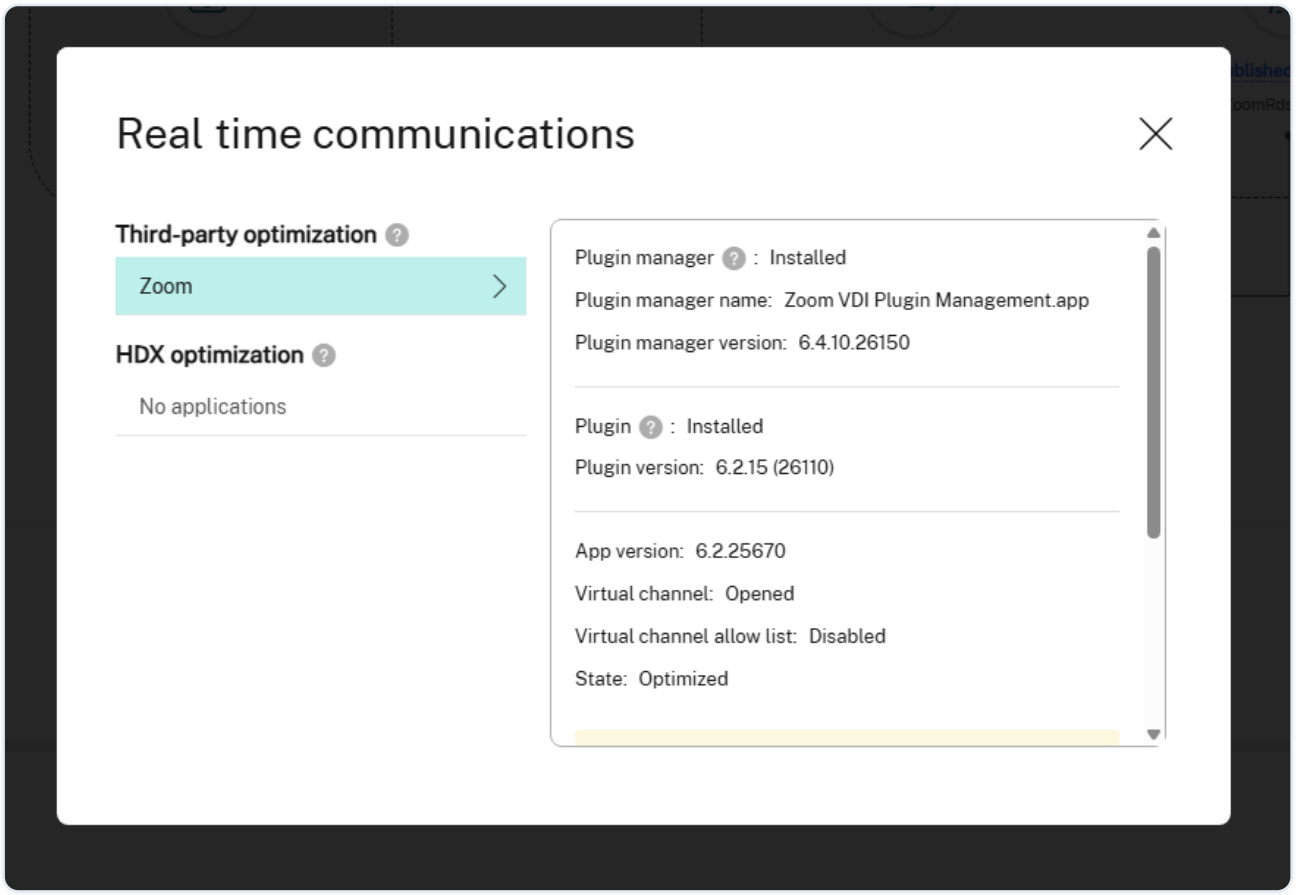
- 客户可以明确保证 RTC 应用程序的优化，消除了对会话是否真正优化的猜测。
- 直接了解缺失组件，以主动解决问题并实现全面优化。
- 更快的故障排除改善了重要通信工具的用户体验。

使用 **会话拓扑** 中的 **实时通信** 字段查看每个应用程序的优化详细信息。



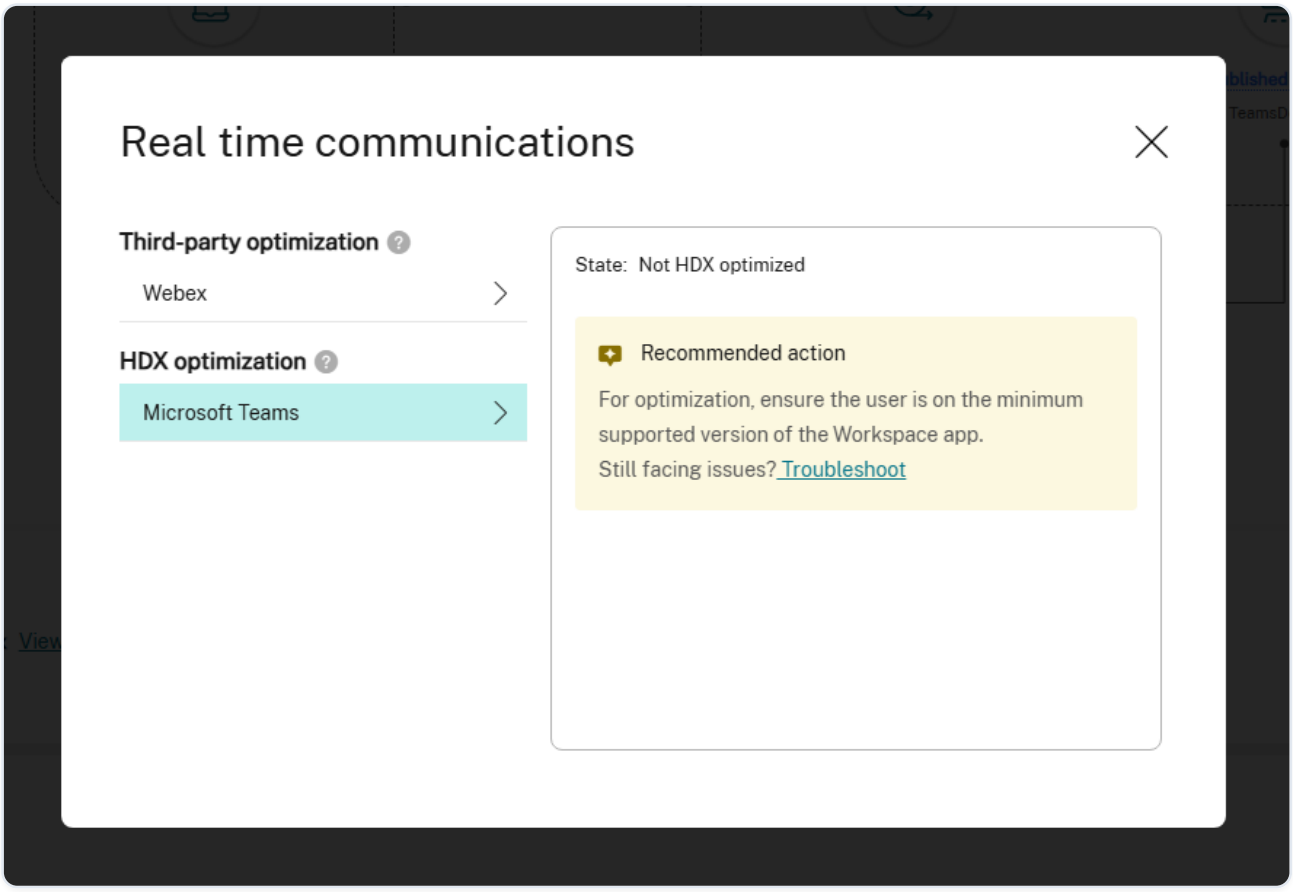
第三方优化应用程序使用 Citrix 技术创建虚拟通道，但应用程序供应商管理其他配置和设置。优化依赖于供应商拥有的解决方案。

单击 **会话拓扑** 屏幕中 **实时通信** 字段旁边的 **查看详细信息** 链接。将显示以下屏幕：



HDX 优化应用程序使用 Citrix 虚拟通道，并直接受 Citrix 配置和设置的影响。

在“**实时通信**”屏幕上单击“**HDX 优化**”部分。将显示以下图像：



实时通信详细信息每 5 分钟更新一次。下表列出了依赖第三方优化的应用程序的可用详细信息。请确保您使用的是受支持的产品版本以获得完整可见性。

注意：

- Microsoft Teams Slimcore 优化仅适用于已发布的桌面和根据供应商支持的新版 Teams。
- 对于 Zoom，从 6.3.10 版开始，供应商更改可用于获取插件详细信息和优化状态。有关详细信息，请参阅 Zoom 文档。

下表列出了依赖 Citrix HDX 优化的应用程序的可用详细信息。确保您使用的是受支持的产品版本以获得完整的可见性。

功能名称	UI 参数	虚拟投递代理版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本
微软团队 Slimcore	插件管理器、插件管理器名称、插件管理器版本	2503	2503	供应商不支持	供应商不支持
	应用程序版本、虚拟通道、虚拟通道允许列表	2503	2402	供应商不支持	供应商不支持
	插件、插件版本、状态	2507	2503	供应商不支持	供应商不支持
祖姆	插件管理器、插件管理器名称、插件管理器版本	2507	2503	2505	插件不可用
	应用程序版本、虚拟通道、虚拟通道允许列表	2507	2402	2402	2402
	插件、插件版本、状态	2507	2503	2505	插件不可用
网讯	插件管理器、插件管理器名称、插件管理器版本	2507	2503	插件不可用	插件不可用
	应用程序版本、虚拟通	2507	2402	2402	2402

功能名称	UI 参数	虚拟投递代理版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本
	道、虚拟通道允许列表				

下表列出了依赖 Citrix HDX 优化的应用程序的可用详细信息。确保您使用的是受支持的产品版本以获得完整的可见性。

功能名称	UI 参数	虚拟投递代理版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本
微软团队	状态	1906.2	2112	2203	2203

数据定义：

UI 参数	描述
插件管理器	显示插件管理器是否已安装。插件管理器是一个小型管理组件，用于打开虚拟通道并下载优化所需的媒体引擎（插件）。注意：功能可能因供应商而异。
插件管理器名称	已安装的插件管理器的名称。
插件管理器版本	已安装的插件管理器的版本。
插件	显示插件是否已安装。插件是优化所需的媒体引擎。注意：功能可能因供应商而异。
插件版本	端点上已安装插件的版本。
应用程序版本	表示虚拟投递代理 (VDA) 上的应用程序版本。

UI 参数	描述
虚拟通道	表示实时通信应用程序的虚拟通道是打开还是关闭。
虚拟通道允许列表	显示虚拟通道的状态。值为*已启用*或*已禁用*。
状态	显示特定用户会话的应用程序的优化状态

会话拓扑方案

会话拓扑适用于活动会话，并实时更新。已断开连接和已结束的会话会显示上次已知状态的拓扑，以便进行全面的会话后分析。

根据站点的部署方案，会话中涉及的组件包括以下全部或部分：

- 端点上的 Citrix Workspace 应用程序
- 网关服务/本地网关
- 云连接器 – 在混合连接的情况下，网关通过云连接器连接到 DaaS。
- VDA

因此，可能的网络拓扑如下：

- 端点上的 Citrix Workspace 应用程序通过 Citrix Workspace 和网关服务连接到本地 VDA。未使用 Cloud Connector 连接到 VDA。

会话拓扑视图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-session-topology1.png)

- 端点上的 Citrix Workspace 应用程序通过 Citrix Workspace 和网关服务，经由 Cloud Connector 连接到本地 VDA。

会话拓扑视图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-session-topology2.png)

- 端点上的 Citrix Workspace 应用程序通过 StoreFront™ 和本地 Gateway 连接到本地 VDA。

会话拓扑视图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-session-topology3.png)

- 端点上的 Citrix Workspace 应用程序通过 StoreFront 连接到本地 VDA。

会话拓扑视图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-session-topology4.png)

性能指标

性能指标面板提供了关联实时指标的功能，以识别用户会话中的问题。会话指标的趋势有助于指示这些指标随时间的变化情况。当您单击**会话性能**选项卡时，除了实时数据之外，您还可以查看过去 15 分钟和 48 小时的数据。这些图表有助于在单个视图中关联多个组件的性能指标。

会话性能指标(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-session-performance-trends.png)

> **注意：**
>
> - 借助过去 15 分钟指标支持，图表会绘制会话连接和断开连接的持续时间。断开连接的会话指标显示为零值。
> - 借助过去 48 小时指标支持，ICARTT、ICA 延迟和会话重新连接图表会使用历史数据指标进行更新。会话重新连接信息可帮助您查看和排查存在中断的网络连接。它还可以分析具有无缝体验的网络。该图表可查看会话重新连接次数、总会话重新连接次数、自动客户端重新连接和会话可靠性重新连接。

> 除了 ICARTT 和 ICA 延迟之外，还提供以下指标用于实时和过去 15 分钟的指标：

- 每秒帧数 - 每秒帧数是一个重要指标，指示会话响应能力。
- 可用输出带宽 - 可用输出带宽是衡量从 VDA 到端点传输数据的总可用带宽的指标。
- 已用输出带宽 - 已用输出带宽表示从 VDA 到端点传输以向用户显示会话的实际数据量。

分析可用输出带宽和已用输出带宽有助于检查是否有足够的带宽来提供会话，并检测会话是否受到带宽不足的影响。

当 ICA RTT 或会话登录持续时间数据无法填充时进行故障排除

以前，当 EUEM 服务或配置文件管理服务未能运行时，不会显示获取与 ICA RTT 或会话登录持续时间相关的数据失败的原因。借助此新功能，您可以获取失败原因以及针对该失败的相应解决方案。**了解更多**链接提供了 ICA RTT 和会话登录持续时间错误、失败原因以及下表中提到的解决方案：

错误类型	错误	错误消息	解决方案
ICA RTT 错误	未显示 ICA RTT 值。	**Citrix 最终用户体验监控未运行。**	1. 打开服务控制台。要打开此控制台，请单击“**开始**”，然后键入“**服务**”。

错误类型	错误	错误消息	解决方案
			2. 确保 Citrix 最终用户体验监控服务 正在运行。
			3. 重新打开桌面会话并尝试。必须显示 ICA RTT 值。
			4. 如果问题仍然存在，请联系 Citrix 管理员。
ICA RTT 错误	未显示 ICA RTT 值。	**Citrix 最终用户体验监控未安装。**	1. 重新安装 VDA。
			2. 打开“服务”控制台。要打开此控制台，请单击“**开始**”，然后键入“服务”
			3. 确保 Citrix 最终用户体验监控服务 正在运行。
			4. 重新打开桌面会话并重试。现在应显示 ICA RTT 值。
			5. 如果问题仍然存在，请联系 Citrix 管理员。
ICA RTT 错误	未显示 ICA RTT 值。	**获取数据时出错。**	1. 打开“服务”控制台。要打开此控制台，请单击“**开始**”，然后键入“服务”。
			2. 确保 **Windows 管理规范服务** 正在运行。

错误类型	错误	错误消息	解决方案
			3. 此外，请确保 WfShell.exe/ PicaShell.exe 进程在“**活动管理器**”>“**进程**”选项卡下运行。如果未运行，请重新打开桌面会话。
			4. 如果前面的步骤不起作用，请运行以下命令以确保存在 Citrix_Euem_Round Trip 实例：`Get-CimInstance -Namespace 'ROOT\Citrix\Euem' -Query "select * from Citrix_Euem_RoundTrip"`
			5. 如果 Citrix_Euem_Round Trip 实例存在，请重新打开桌面会话。
			6. 如果问题仍然存在，请联系 Citrix 管理员。
会话登录持续时间错误	未加载图表。	**Citrix 配置文件管理未运行**	1. 打开“服务”控制台。要打开此控制台，请单击“**开始**”，然后键入“服务”。
			2. 确保 **Citrix Profile Management Service** 正在运行。

错误类型	错误	错误消息	解决方案
			3. 重新打开桌面会话并尝试。必须显示图表。
			4. 如果问题仍然存在，请联系 Citrix 管理员。
会话登录持续时间错误	未加载图表。	**思杰配置文件管理未安装。**	1. 安装 Citrix 配置文件管理服务。
			2. 打开“服务”控制台。要打开此控制台，请单击“**开始**”，然后键入“服务”。
			3. 确保 **Citrix Profile Management Service** 正在运行。
			4. 重新打开桌面会话并尝试。必须显示图表。
			5. 如果问题仍然存在，请联系 Citrix 管理员。
会话登录持续时间错误	未加载图表。	**获取数据时出错。**	1. 打开“**服务**”控制台。要打开此控制台，请单击“**开始**”，然后键入“服务”。
			2. 确保 **Windows 管理规范服务** 正在运行。
			3. 如果上述服务已在运行，请运行以下命令以确保

错误类型	错误	错误消息	解决方案
			`LogonTimings instance is present`：`Get-CimInstance -Namespace 'ROOT\Citrix\Profile\Metrics' -Query "select * from LogonTimings"`
			`4.` 如果问题仍然存在，请联系 Citrix 管理员。
ICA RTT 错误	未显示 ICA RTT 值。	不支持控制台。	使用 HDX 启动会话。
ICA RTT 错误	未显示 ICA RTT 值。	不支持远程桌面协议 (RDP)。	使用 HDX 启动会话。
ICA RTT 错误	未显示 ICA RTT 值。	将 VDA 升级到版本 2402 或更高版本，以获取详细的错误检测并访问所有功能。	将 VDA 升级到 2402 或更高版本。
会话登录持续时间错误	未加载图表。	Citrix Profile Management WMI 插件未安装。	安装 Citrix 配置文件管理 WMI 插件。

诊断应用程序性能问题

Citrix Director 中的应用程序性能监控（与 uberAgent 集成）为管理员提供了对单个应用程序（包括已发布的和本地的）运行情况的细致洞察。此数据可帮助您确定问题是否由应用程序的资源消耗、网络依赖性或 UI 无响应引起。

先决条件

- VDA Windows 版本应大于或等于 2607 LTSR
- uberAgent 必须安装在 VDA 上
- 必须在 Studio 中启用“使用 uberAgent 应用程序性能数据增强 Director”策略。

策略名称	策略描述	UI 指标	默认值	值选项	VDA WINDOWS 版本	VDA（丽奴克斯、麦克）
使用 uberAgent 应用程序性能数据增强 Director	启用 Director 使用 uberAgent 提供的计算机指标数据来监控应用程序性能	应用程序名称, 是否已发布, 进程名称, CPU 使用率 %, 内存使用率 %, 工作集内存 (MB), 磁盘 IOPS, 磁盘延迟 (ms), 网络延迟 (ms), 输入延迟 (ms), CPU 使用率 % (P95), 内存使用率 % (P95), 输入延迟 (P95) (ms), 每秒页面错误	启用	已启用或已禁用	2607 LTSR 或更高版本	不可用

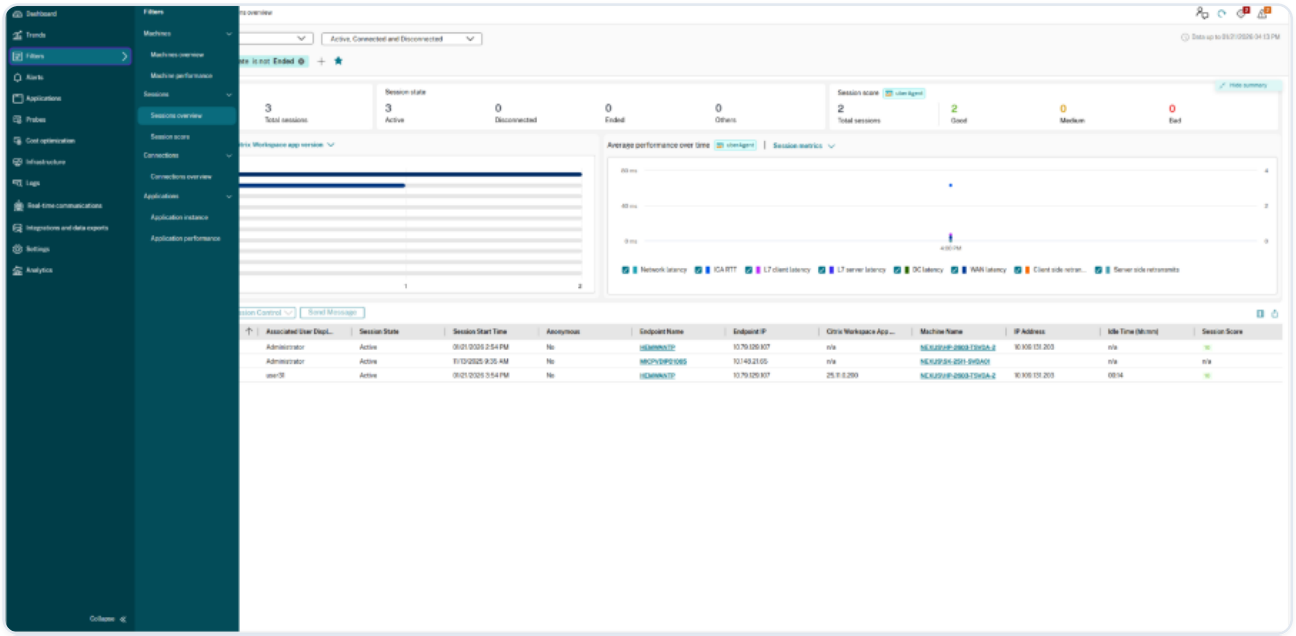
概述和主要功能

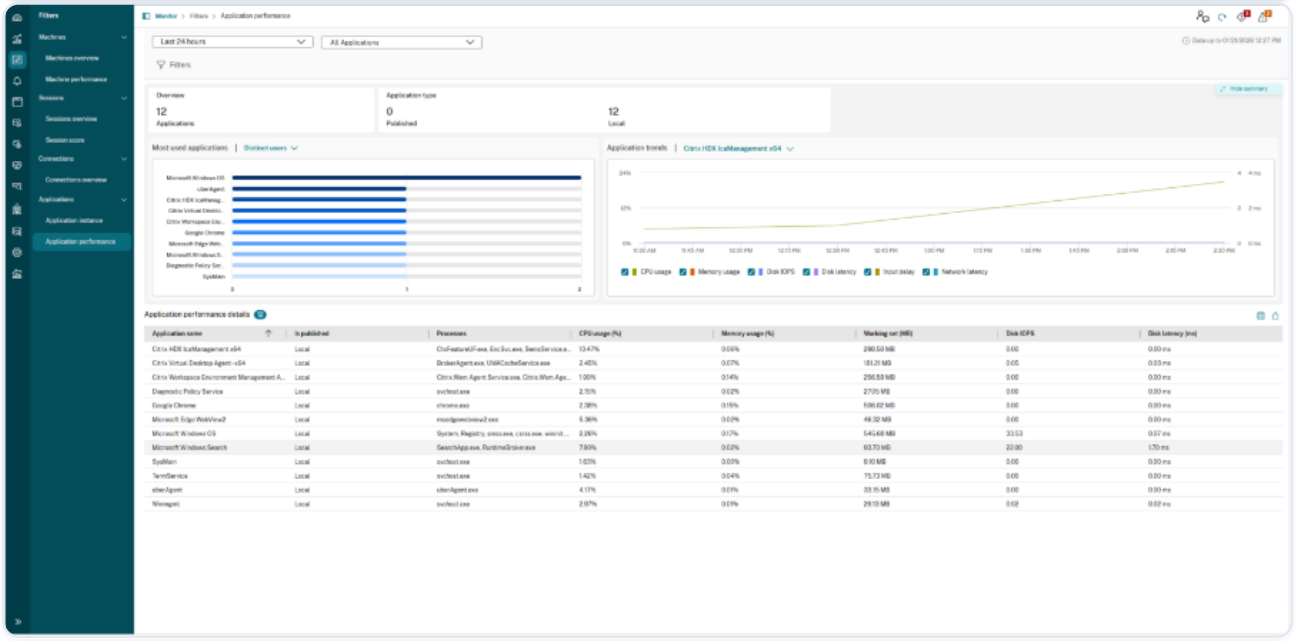
本页详细介绍了新的 **应用程序性能** 选项卡的文档，该选项卡侧重于对已发布应用程序和本地应用程序进行实时和历史监控。

主要功能包括：

- 时间范围筛选器：通过时间范围选项增强监控精度。
- 简化筛选器管理：用于管理筛选器的直观下拉菜单。
- 直观的筛选器构建：用于直接在主页上创建和修改筛选器的灵活工作流。

- 可视化：引入了应用程序分布图和随时间变化的性能图，以便即时了解应用程序性能趋势。

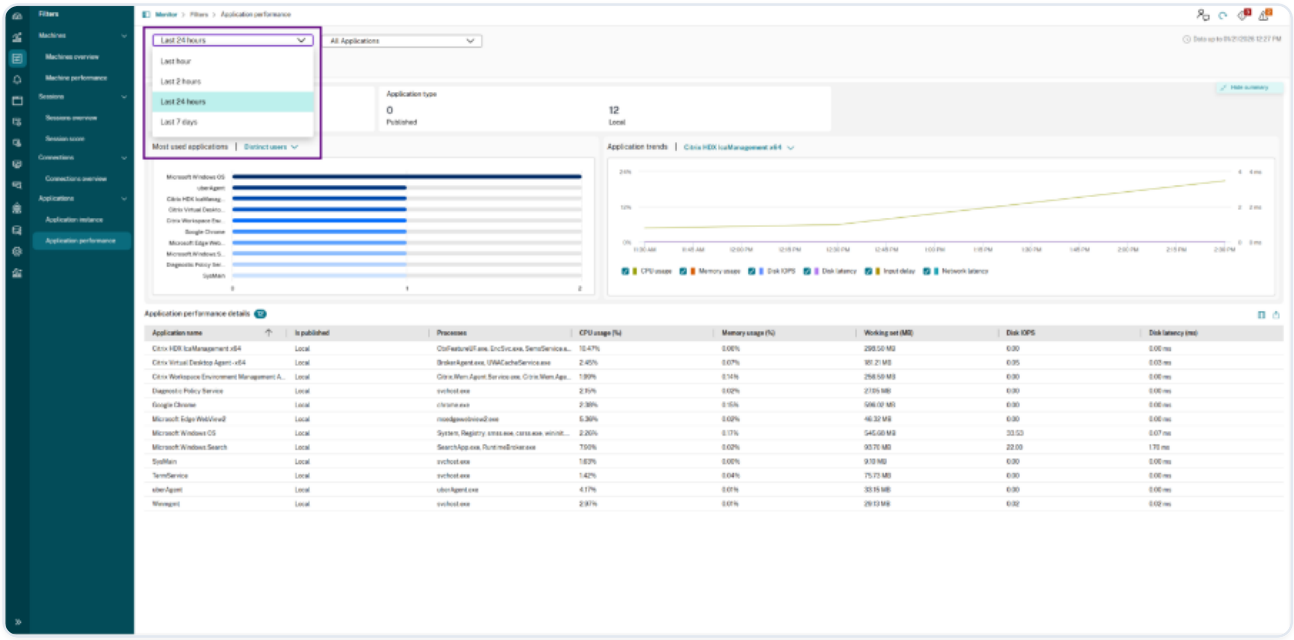




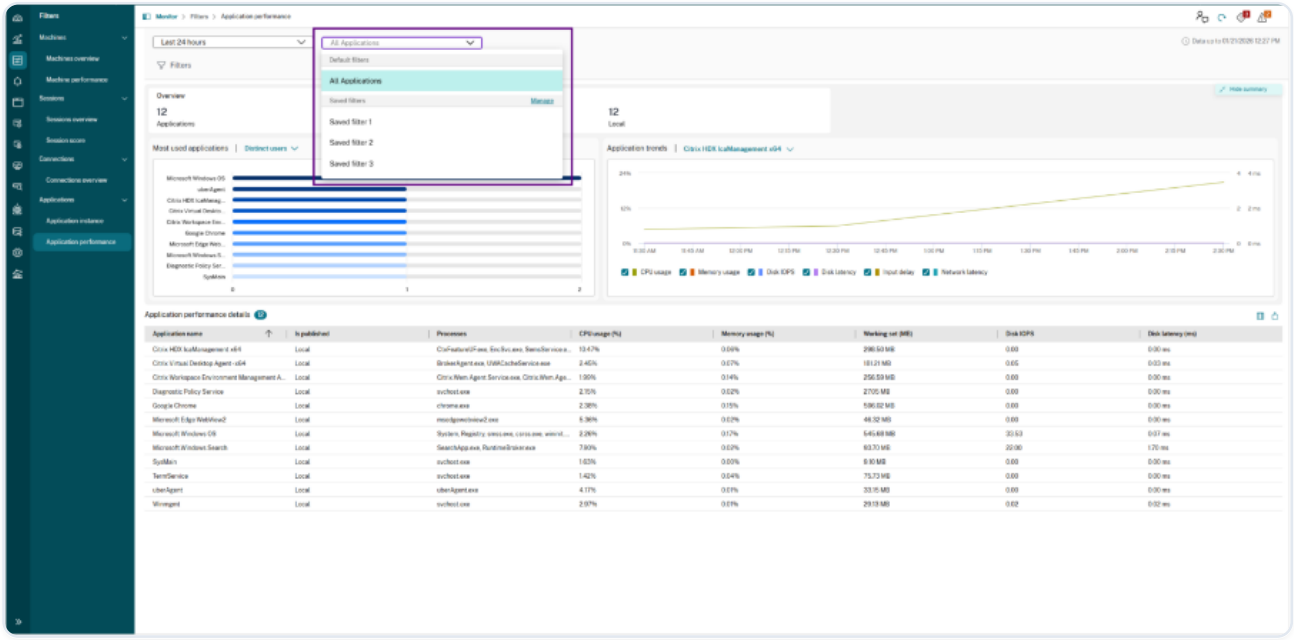
筛选数据

在页面顶部，您可以定义显示数据的范围。

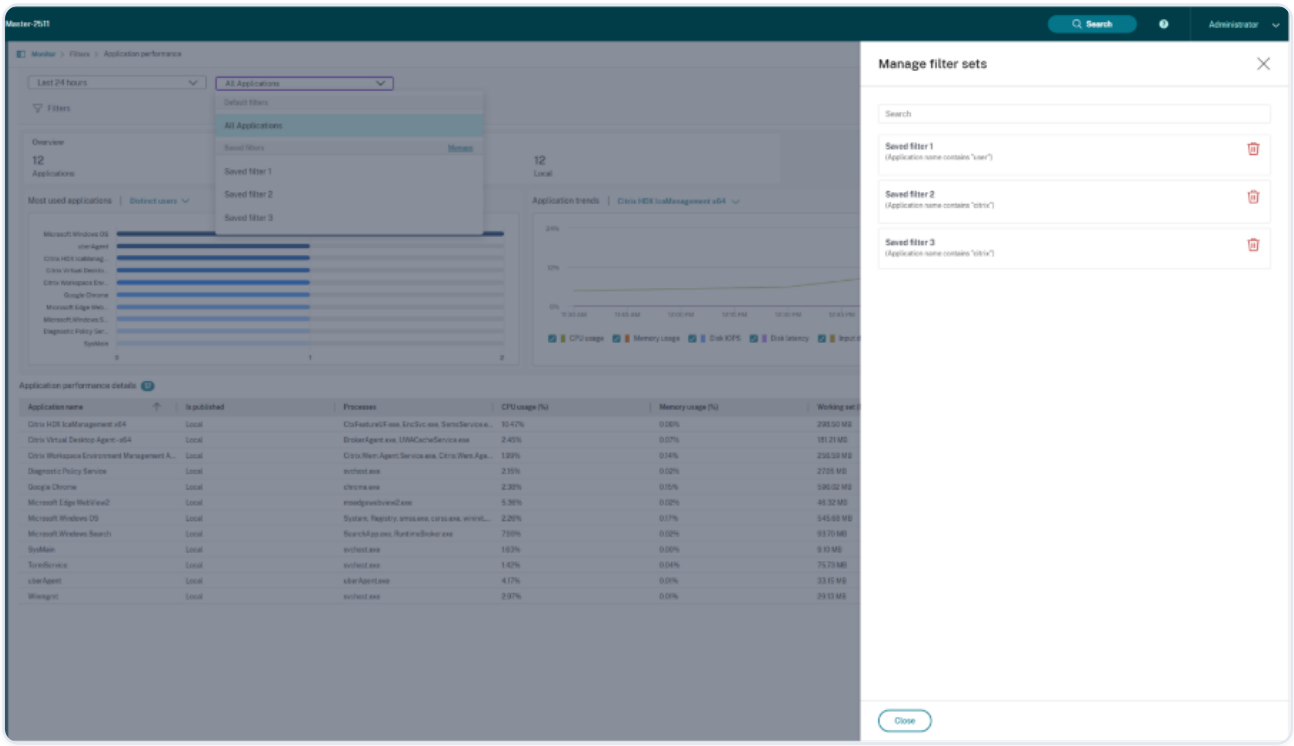
- **时间段：** 选择时间范围。时间范围筛选器包括 1 小时、2 小时、1 天或 7 天



- **应用程序范围：** 使用应用程序下拉菜单按特定筛选器筛选整个控制板，或查看**所有应用程序**。



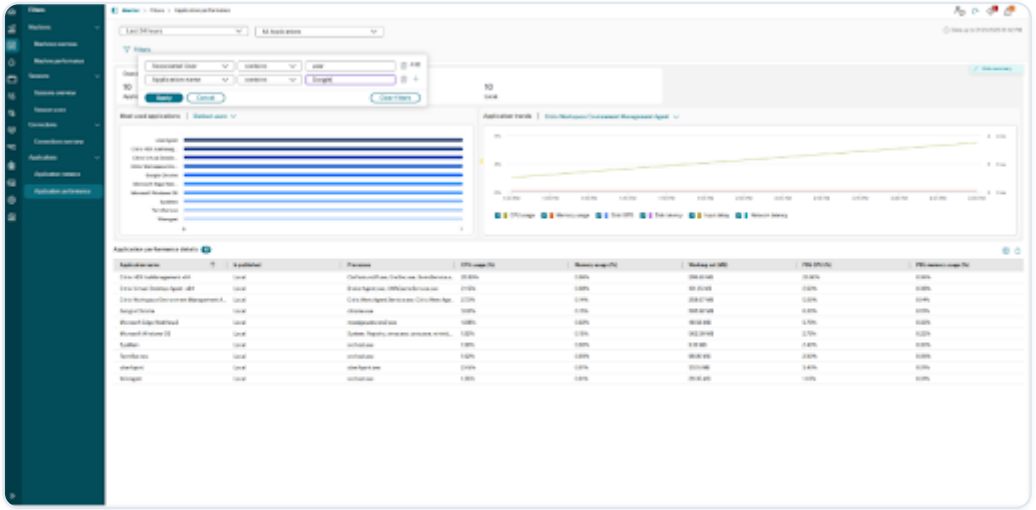
- **筛选器：** 使用“筛选器”图标进一步优化数据。
- **管理：** 单击“管理”将打开一个侧面板，您可以在其中搜索、查看或删除现有已保存的筛选器。

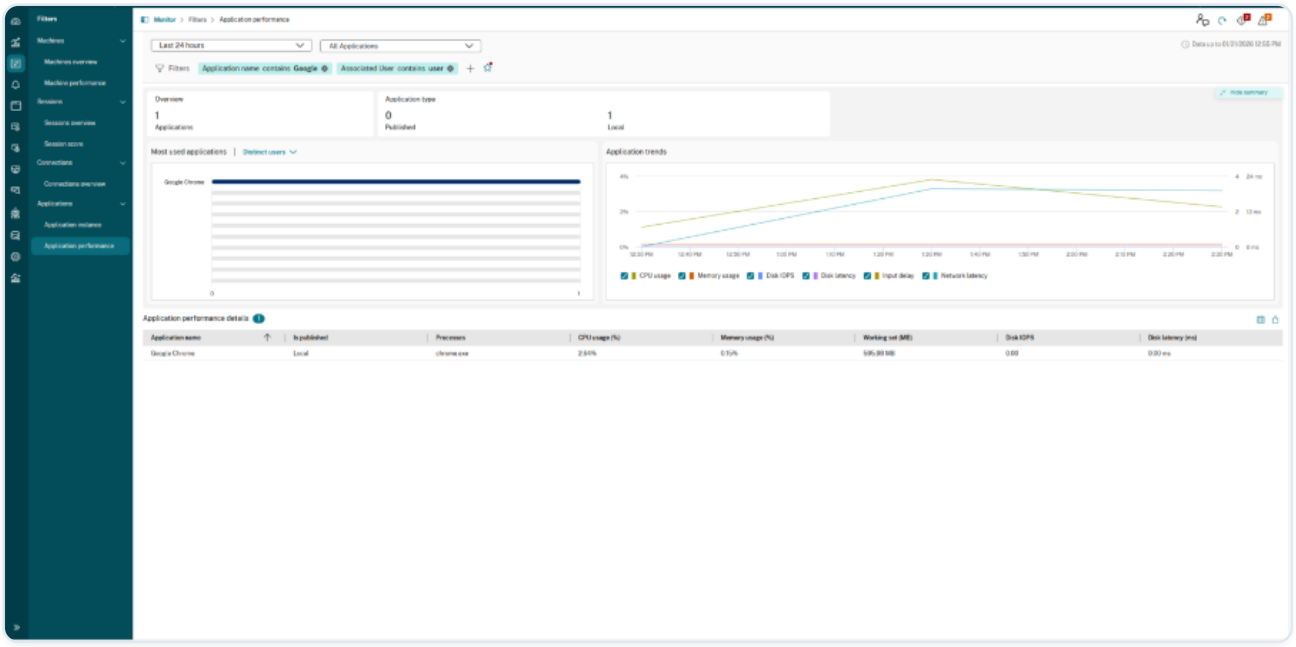


构建和应用筛选器

您现在可以直接在应用程序概览页面上构建复杂的筛选器集：

- 单击“筛选器”图标或现有筛选器旁边的“+”按钮。
- 选择条件（例如，应用程序名称）、运算符（例如，包含）和值（例如，Google）。





筛选器保存状态和工作流程

活动筛选器旁边的星形图标 (⋆) 直观地指示当前筛选器集的状态。这有助于指导管理员保存、应用和管理自定义筛选器。

筛选器状态	图标外观	含义	所需操作
未保存的筛选器	 (带红点的空心轮廓)	当前筛选条件组合**尚未保存**。	单击**空星形图标**以打开对话框，命名筛选器集并保存。
已保存的筛选器	 (已填充 / 实心)	当前活动的筛选器集与之前保存的筛选器**精确匹配**。	无需执行任何操作。您正在根据定义的模板查看数据。
已保存的筛选器有更改	 (填充有红点)	使用**已保存的筛选器**时，如果添加、删除任何其他筛选器或对任何列进行排序，则会出现红点，这意味着更改**尚未保存**。	单击**带红点的星形图标**以更新现有已保存的筛选器，或使用下拉菜单选择**另存为筛选器集**以创建新的筛选器。

筛选器操作按钮

添加新筛选器或修改已保存的筛选器时，以下控件和状态指示器将可用：

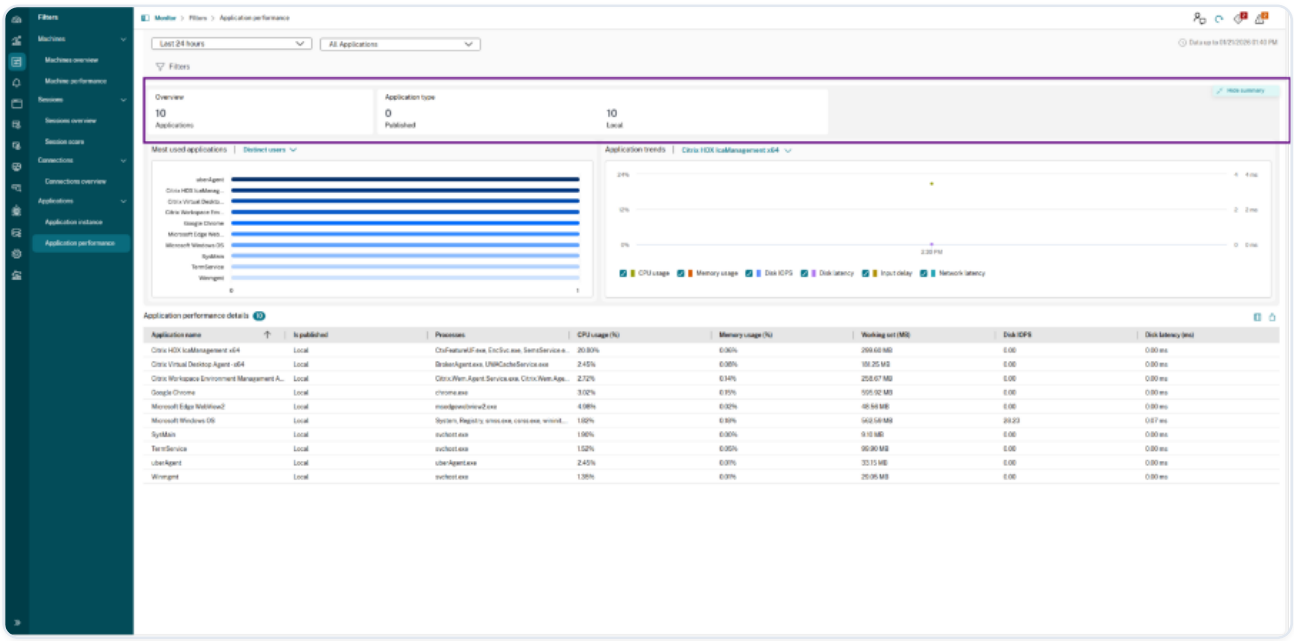
按钮	含义和操作
更新	将所有当前活动的筛选条件应用于图表和应用程序性能数据表。
取消	放弃对当前筛选器集所做的任何更改，并恢复到上次应用的筛选器。
清除筛选器	删除所有新添加的筛选条件。
图标	删除单击此图标时选定的筛选条件。

可视化

概览摘要

摘要窗格提供当前正在监视的应用程序的即时计数：

- **应用程序：** 环境中检测到的唯一应用程序名称的总数。
- **应用程序类型**：细分了在 VDA 上运行的**已发布**应用程序与**本地**应用程序的数量。

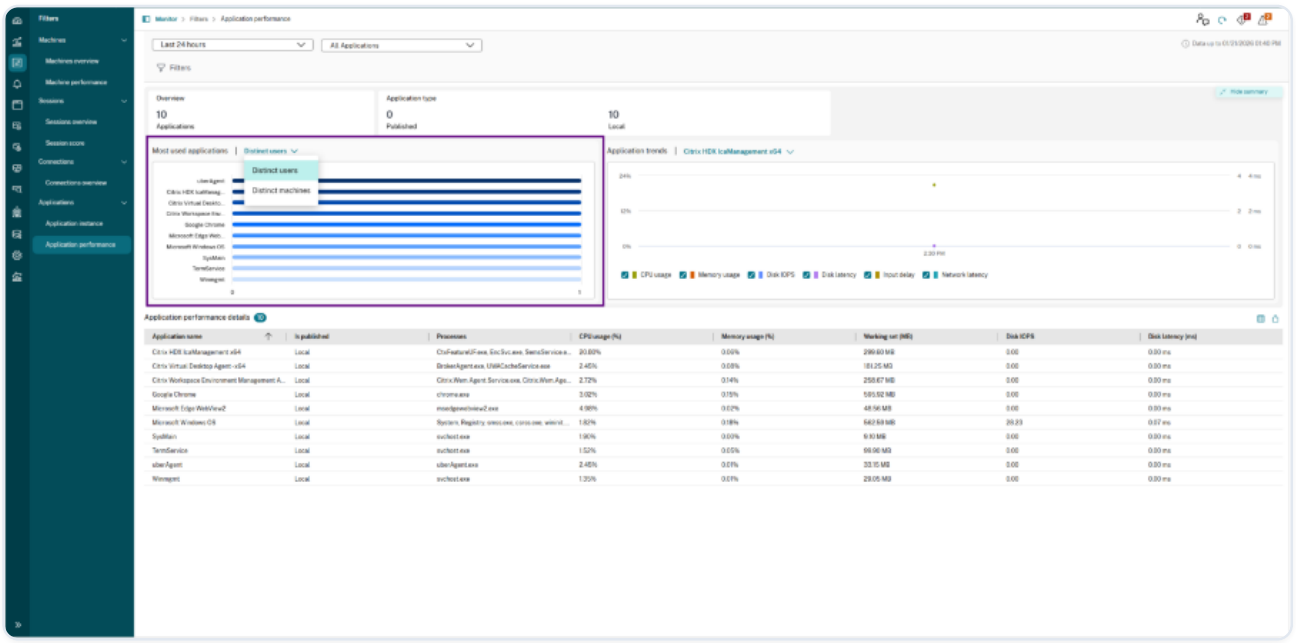


分布图

分布图用作直方图，它根据特定的性能类别对应用程序实例的数量进行分类。它旨在帮助您了解用户体验在您的环境中的“分布”。

- **指标分组**：X 轴表示所选指标（例如**UI 延迟**或**启动持续时间**）的范围，而 Y 轴表示这些范围内的出现次数。

- **视图视角**：下拉菜单允许您在两种视图之间切换数据表示形式：
  - **独立用户**：根据唯一用户数量显示性能分布
  - **独立计算机**：根据 VDA 数量显示分布。



性能图

性能图是一种时间序列可视化，它跟踪选定持续时间内的应用程序运行状况。它允许您将性能变化与特定的时间间隔和资源消耗相关联。

- **应用程序选择**：使用图表顶部的下拉菜单选择要分析的特定应用程序。
- **多指标关联**：该图表允许您同时叠加多个关键绩效指标 (KPI)，以查找响应能力和资源使用情况之间的关联：
  - **CPU 和内存使用情况**：显示应用程序的资源消耗百分比。
  - **磁盘 IOPS 和磁盘延迟**：识别存储瓶颈是否影响应用程序性能。
  - **输入延迟**：衡量用户操作与应用程序响应之间的时间。
  - **网络延迟**：跟踪与应用程序通信相关的网络延迟。

性能图表(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-performance-chart.png)

应用程序性能详细信息（表）

底部窗格提供每个应用程序实例的原始可操作数据。数据可以导出，并且可以选择要显示的列。

应用程序性能 1(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-app-performance1.png)

应用程序性能 2(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-app-performance2.png)

应用程序性能 3(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-app-performance3.png)

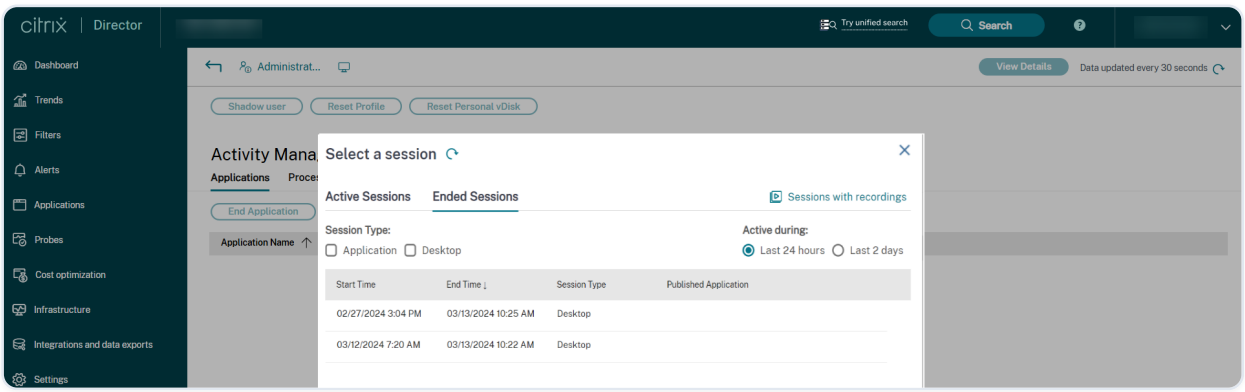
诊断已结束的用户会话

Citrix Director 现在可以显示处于活动、已断开连接或已终止状态的会话的详细信息。以前，您只能查看活动会话的详细信息。借助此功能，服务台管理员可以排查已结束或已终止状态的会话问题。已结束会话的详细信息可用于过去 24 小时和过去 2 天。您可以查看已结束或已终止会话的以下详细信息：

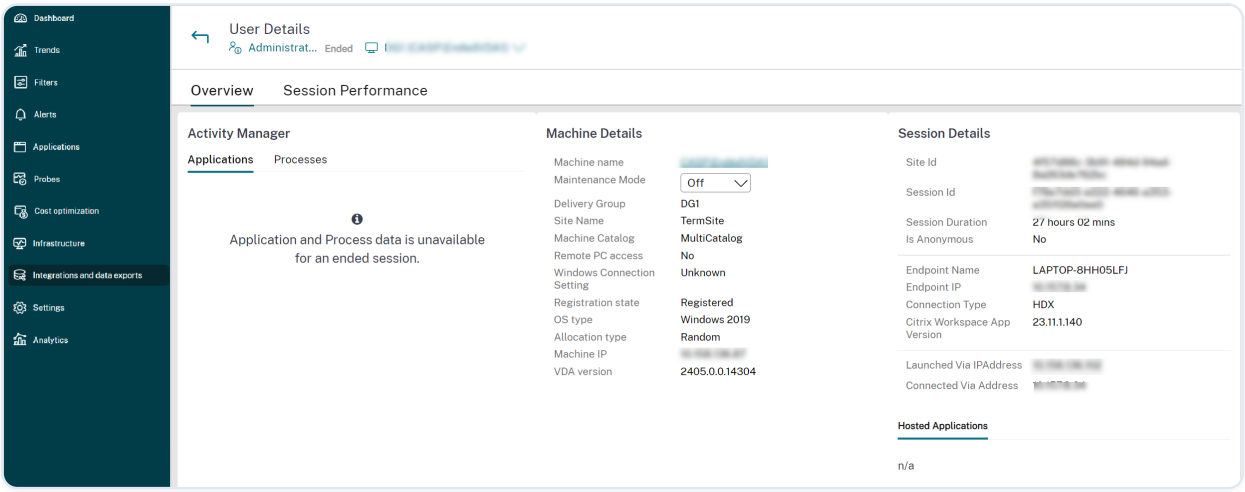
- 计算机详细信息面板 - 显示启动所选会话的计算机的可用详细信息
- 会话详细信息面板 - 显示所选会话的可用详细信息。
- 会话登录持续时间 - 显示所选会话的登录持续时间信息。您可以查看以下各项所用时间的图表：
  - 代理
  - 计算机启动
  - HDX™ 连接
  - 身份验证
  - GPO
  - 登录脚本
  - 磁盘上的配置文件加载
  - 交互式会话

要查看历史用户会话，请执行以下操作：

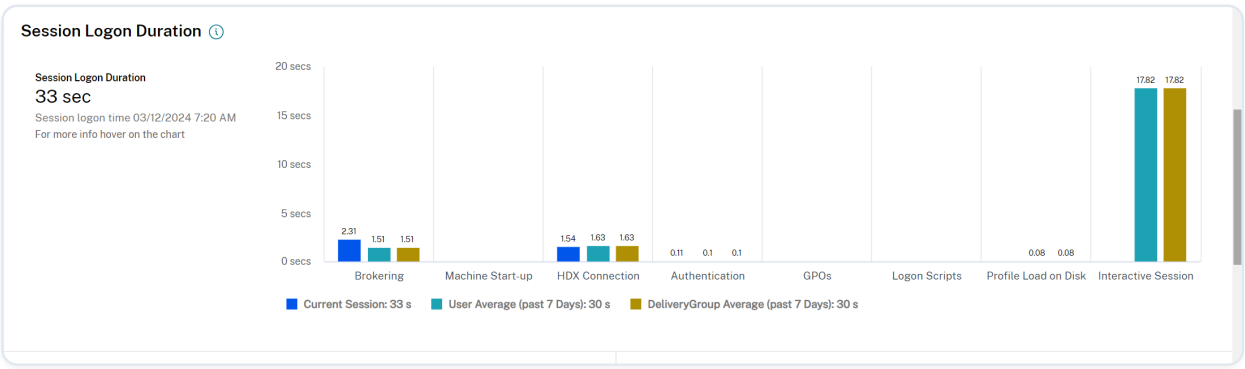
1. 单击 **筛选** > **会话**视图。
2. 点击**关联用户**以打开该用户的活动管理器。



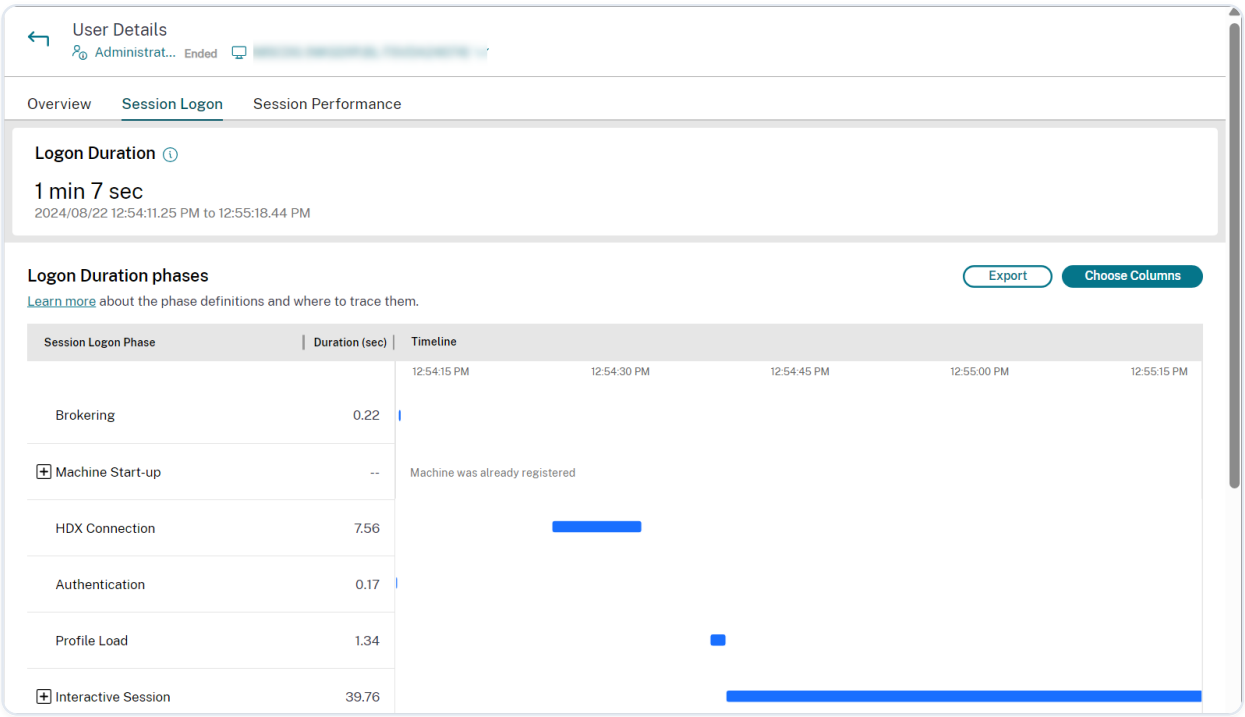
3. 从**已结束会话**部分选择所需的会话。
4. 查看**计算机详细信息**和**会话详细信息**面板。



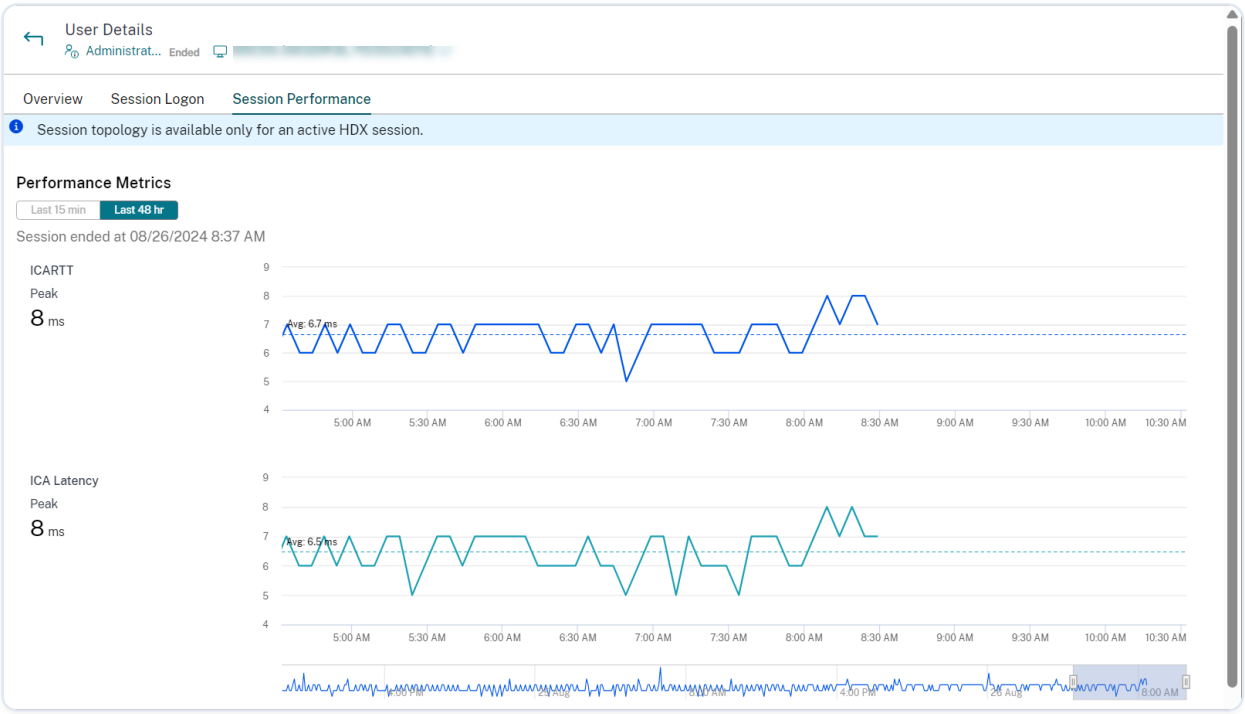
5. 向下滚动并查看已结束会话的**会话登录持续时间**。



6. 点击**会话登录**选项卡并查看详细信息。



7. 点击**会话性能**选项卡并查看详细信息。



影子用户

在 Director 中，使用影子用户功能直接查看或操作用户的虚拟机或会话。您可以跟踪 Windows 或 Linux VDA。用户必须连接到您要跟踪的计算机。通过检查用户标题栏中列出的计算机名称来验证这一点。

Director 会在新选项卡中启动会话跟踪，请更新您的浏览器设置以允许来自 Director URL 的弹出窗口。

从“**用户详细信息**”视图访问会话跟踪功能。选择用户会话，然后在“活动管理器”视图或“会话详细信息”面板中单击“**跟踪**”。

使用远程协助

跟踪 LINUX VDA

会话跟踪适用于运行 RHEL7.3 或 Ubuntu 16.04 Linux 发行版的 Linux VDA 7.16 版或更高版本。

> **注意：**
>
> - VDA 必须可从 Director UI 访问，会话跟踪才能正常工作。因此，会话跟踪仅适用于与 Director 客户端位于同一内网中的 Linux VDA。
> - Director 使用 FQDN 连接到目标 Linux VDA。请确保 Director 客户端可以解析 Linux VDA 的 FQDN。

- VDA 必须安装 python websockify 和 x11vnc 软件包。
- noVNC 连接到 VDA 使用 WebSocket 协议。默认情况下，使用 **ws://** WebSocket 协议。出于安全原因，Citrix 建议您使用安全的 **wss://** 协议。在每个 Director 客户端和 Linux VDA 上安装 SSL 证书。

按照 会话跟踪 中的说明配置 VDA 以进行会话跟踪。

1. 单击“**跟踪**”后，会话跟踪连接将初始化，并且用户设备上会显示确认提示。
2. 指示用户单击“**是**”以开始机器或会话共享。
3. 管理员只能查看被跟踪的会话。

影子化 WINDOWS VDA

Windows VDA 会话使用 Windows 远程协助进行影子化。在安装 VDA 时启用**用户 Windows 远程协助**功能。有关详细信息，请参阅启用或禁用功能。

1. 单击**影子化**后，影子化连接将初始化，并出现一个对话框，提示您打开或保存 .msrc 事件文件。
2. 如果未默认选择，请使用远程协助查看器打开事件文件。用户设备上将出现确认提示。
3. 指示用户单击**是**以开始机器或会话共享。
4. 如需更多控制，请要求用户共享键盘和鼠标控制。

简化 MICROSOFT INTERNET EXPLORER 浏览器以进行影子化

配置您的 Microsoft Internet Explorer 浏览器，使其使用远程协助客户端自动打开下载的 Microsoft 远程协助 (.msra) 文件。

为此，您必须在组策略编辑器中启用“自动提示文件下载”设置：

计算机配置 \> 管理模板 \> Windows 组件 \> Internet Explorer \> Internet 控制面板 \> 安全页 \> Internet 区域 \> 自动提示文件下载。

默认情况下，此选项对本地 Intranet 区域中的站点启用。如果 Director 站点不在本地 Intranet 区域中，请考虑手动将该站点添加到此区域。

使用 HDX 屏幕共享

Director 支持远程协助，使 IT 管理员和技术支持人员能够通过 HDX 屏幕共享技术向最终用户提供远程支持。此功能利用 Citrix 的原生 HDX 协议，为故障排除和用户协助场景提供安全、高性能的屏幕共享功能。

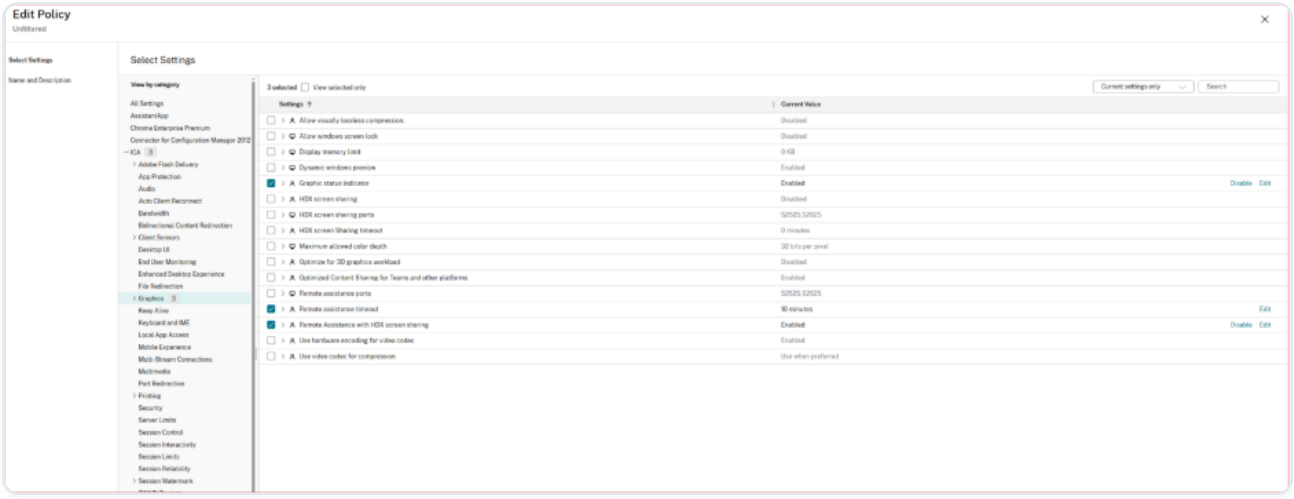
先决条件

组件	支持的环境或版本
操作系统	Windows、Linux（适用于单会话操作系统**或多会话操作系统**）
虚拟投递代理 (VDA)	CR 2511 或更高版本
导览器	CR 2511 或更高版本
交付控制器	CR 2511 或更高版本
TWPlayer (ThinWire 播放器)	在 Director UI 中启动影子会话时，可获取下载播放器的链接

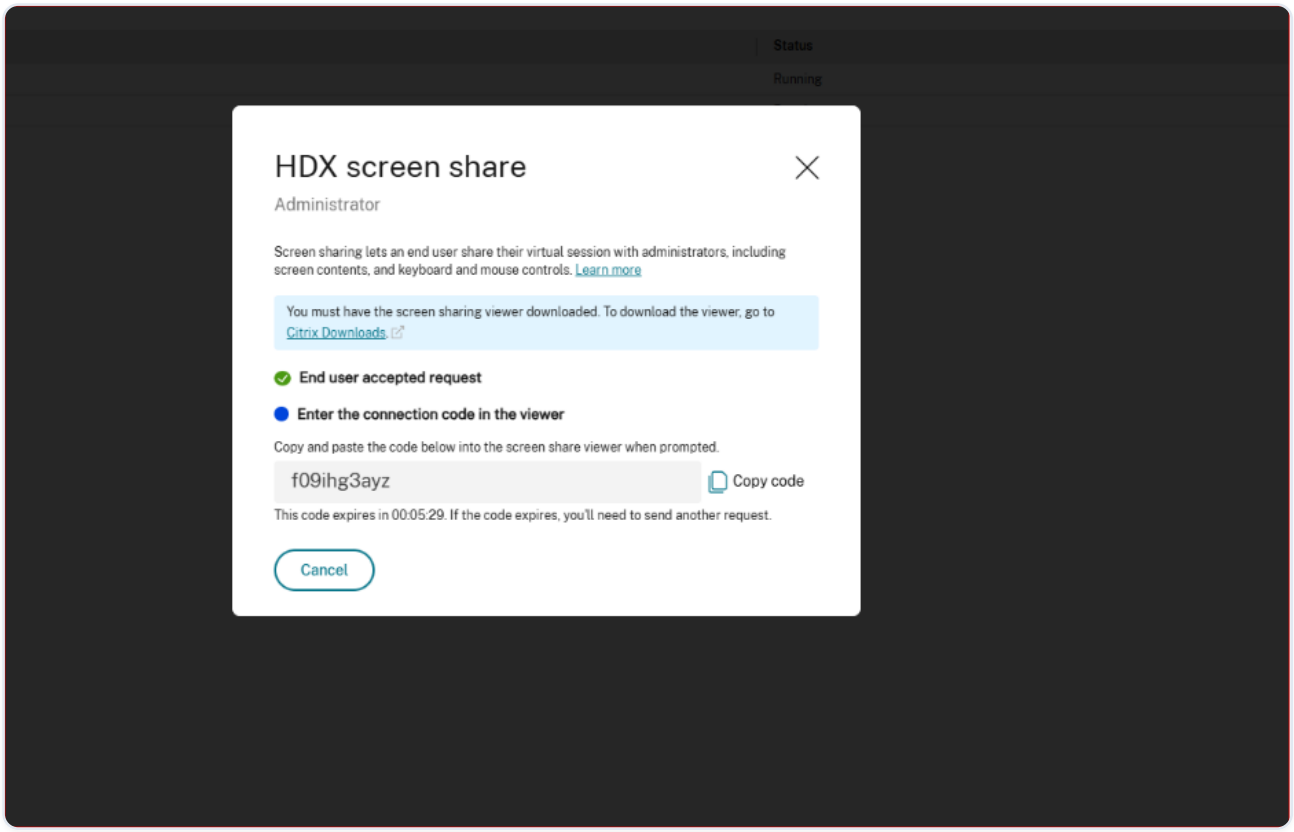
组策略配置

要使用 Director 和 HDX Screen Share 启用远程协助，请在 VDA 上配置以下组策略：

- 带 HDX 屏幕共享的远程协助
- 远程协助超时
- 图形状态指示器



TWPlayer (ThinWire 播放器) 是一个必需组件，必须下载一次才能启用 HDX 屏幕共享功能。在 Director UI 中启动影子会话时，可获取下载播放器的链接。



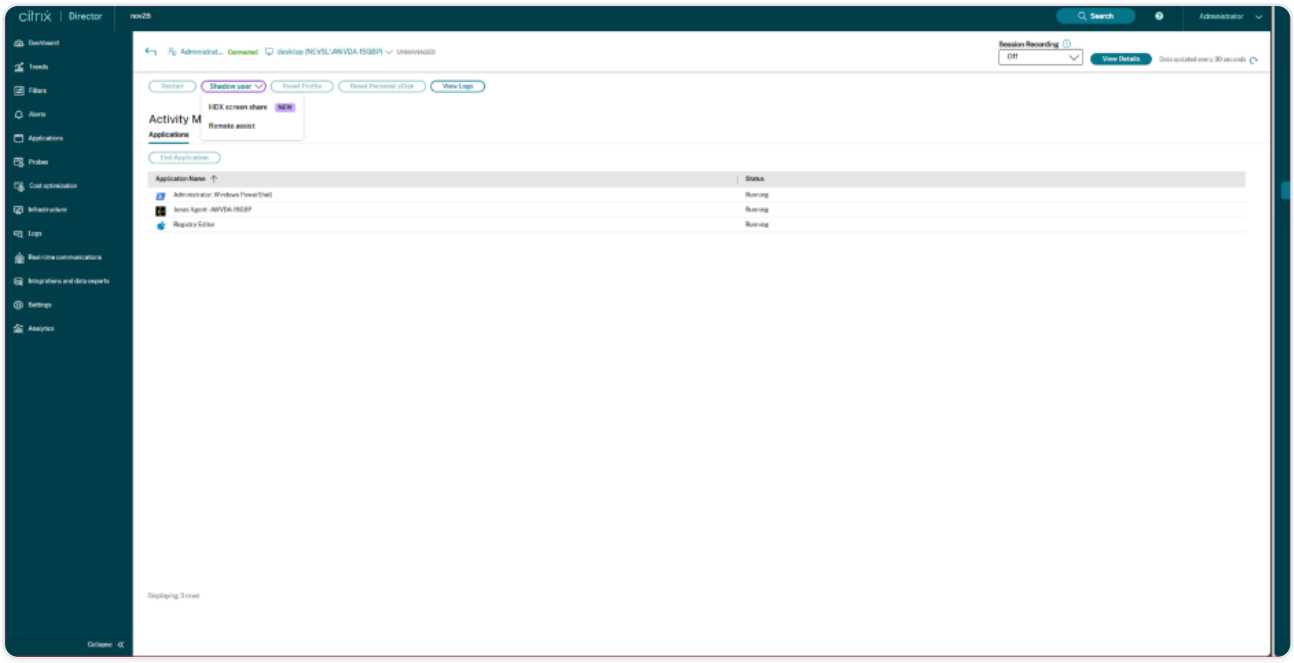
限制

- 已发布的应用程序（应用程序会话）无法进行影子操作 – 仅限桌面会话。

使用 Director 和 HDX Screen Share 的工作流程

以下步骤概述了管理员发起 HDX 屏幕共享会话的过程：

1. **发起影子会话**
    a. 登录 思杰 Director
    b. 导航到需要协助的用户会话
    c. 单击“影子”按钮
    d. 选择 HDX 屏幕共享
2. **启动查看器**
    a. 使用 TWPlayer/远程协助查看器打开生成的事件文件
    b. 等待用户接受连接请求
3. **查看会话**
    a. 会话屏幕显示在查看器窗口中
    b. 管理员可以实时观察用户操作



向用户发送消息

从 Director，向连接到一个或多个计算机的用户发送消息。使用此功能发送有关管理操作的即时通知，例如即将进行的桌面维护、计算机注销和重新启动以及配置文件重置。

1. 在“活动管理器”视图中，选择用户，然后单击“详细信息”。
2. 在“用户详细信息”视图中，找到“会话详细信息”面板，然后单击“发送消息”。
3. 在“主题”和“消息”字段中键入您的消息信息，然后单击“发送”。

如果消息发送成功，Director 中将显示确认消息。消息将显示在用户的计算机中。

如果消息发送失败，Director 中将显示错误消息。根据错误消息排查问题。完成后，再次键入主题和消息文本，然后再次单击“**重试**”。

用于限制用户操作的批量操作选项的自定义角色

此功能允许添加自定义角色，以限制管理员可以查看和控制的内容。新的自定义角色限制了选择批量操作（例如注销、断开连接或发送消息）的能力。此控制对于防止对用户进行无意或恶意的批量操作是必要的。

您现在可以使用以下步骤编辑角色以限制批量操作权限：

1. 登录到 Citrix Cloud。
2. 导航到“**角色**”，然后选择“**未启用执行批量操作**”角色。
3. 单击三个点并选择“**编辑**”。

4. 转至“**Director > 管理**”，然后选择“**对计算机电源操作、维护模式操作和会话管理执行批量操作**”复选框。
5. 确保还选择了以下角色：
    - **通过计算机目录成员身份启用/禁用计算机的维护模式**
    - **通过计算机目录成员身份启用/禁用桌面的维护模式**
    - **通过计算机目录成员身份对 Windows 桌面计算机执行电源操作**
    - **通过计算机目录成员身份对 Windows Server 计算机执行电源操作**

如果选择了步骤 5 中的选项，则用户可以执行单个操作。要执行批量操作，必须选择步骤 4 中的选项和步骤 5 中的选项。

解决应用程序故障

在**活动管理器**视图中，单击“应用程序”选项卡。您可以查看此用户有权访问的所有计算机上的所有应用程序，包括当前连接计算机的本地和托管应用程序，以及每个应用程序的状态。

> **注意：**
>
> 如果“应用程序”选项卡显示为灰色，请联系有权启用该选项卡的管理员。
>
> 此列表仅包含那些在会话中启动的应用程序。

对于多会话操作系统计算机和单会话操作系统计算机，会列出每个断开连接的会话的应用程序。如果用户未连接，则不显示任何应用程序。

操作	描述
结束无响应的应用程序	选择无响应的应用程序，然后单击“结束应用程序”。应用程序终止后，请用户再次启动它。
结束无响应的进程	如果您具有所需权限，请单击“进程”选项卡。选择与应用程序相关或占用大量 CPU 资源或内存的进程，然后单击“结束进程”。但是，如果您没有终止该进程所需的权限，则尝试结束进程会失败。
重新启动用户计算机	仅适用于单会话操作系统计算机，对于选定的会话，单击“重新启动”。或者，在“计算机详细信息”视图中，使用电源控件重新启动或关闭计

操作	描述
	算机。指示用户再次登录，以便您可以重新检查应用程序。对于多会话操作系统计算机，重新启动选项不可用。而是从用户处注销，然后让用户再次登录。
将计算机置于维护模式	如果计算机映像需要维护（例如修补程序或其他更新），请将计算机置于维护模式。在“计算机详细信息”视图中，单击“详细信息”并打开维护模式选项。上报给相应的管理员。

恢复桌面连接

在 Director 中，检查用户标题栏中当前计算机的用户连接状态。

如果桌面连接失败，将显示导致失败的错误，这有助于您决定如何进行故障排除。

操作	描述
确保计算机未处于维护模式	在“用户详细信息”页面上，确保维护模式已关闭。
重新启动用户的计算机	选择计算机，然后单击“**重新启动**”。如果用户的计算机无响应或无法连接，请使用此选项。例如，当计算机使用异常高的 CPU 资源时，这可能导致 CPU 无法使用。

恢复会话

如果会话断开连接，它仍然处于活动状态，并且其应用程序会继续运行，但用户设备不再与服务器通信。

在“用户详细信息”视图中，在“**会话详细信息**”面板中排查会话故障。您可以查看当前会话的详细信息，由会话 ID 指示。

操作	描述
结束无响应的应用程序或进程	单击“**应用程序**”选项卡。选择任何无响应的应用程序，然后单击“**结束应用程序**”。同样，选择任何无响应的相应进程，然后单击“**结束进程**”。此外，结束消耗异常高内存或 CPU 资源的进程，这可能导致 CPU 无法使用。

操作	描述
断开 Windows 会话	单击“**会话控制**”，然后选择“**断开连接**”。此选项仅适用于已代理的多会话操作系统计算机。对于未代理的会话，此选项处于禁用状态。
从用户会话注销	单击“**会话控制**”，然后选择“**注销**”。

要测试会话，用户可以尝试重新登录。您还可以跟踪用户以更密切地监视此会话。

生成 HDX™ 通道系统报告

在**用户详细信息**视图中，在**HDX**面板中检查用户计算机上的 HDX 通道状态。此面板仅在用户计算机使用 HDX 连接时可用。

如果出现消息指示信息当前不可用，请等待一分钟以刷新页面，或选择**刷新**按钮。HDX 数据更新所需时间比其他数据稍长。

单击错误或警告图标以获取更多信息。

> 提示：

> 您可以通过单击标题栏左侧的左右箭头，在同一对话框中查看其他通道的信息。

> HDX 通道系统报告主要由 Citrix 支持人员用于进行进一步故障排除。

1. 在 HDX 面板中，单击下载系统报告。
2. 您可以查看或保存 .xml 报告文件。
    - 要查看 .xml 文件，请单击打开。.xml 文件将显示在与 Director 应用程序相同的窗口中。
    - 要保存 .xml 文件，请单击保存。将出现“另存为”窗口，提示您选择 Director 计算机上的位置以下载文件。

重置用户配置文件

> **注意：**

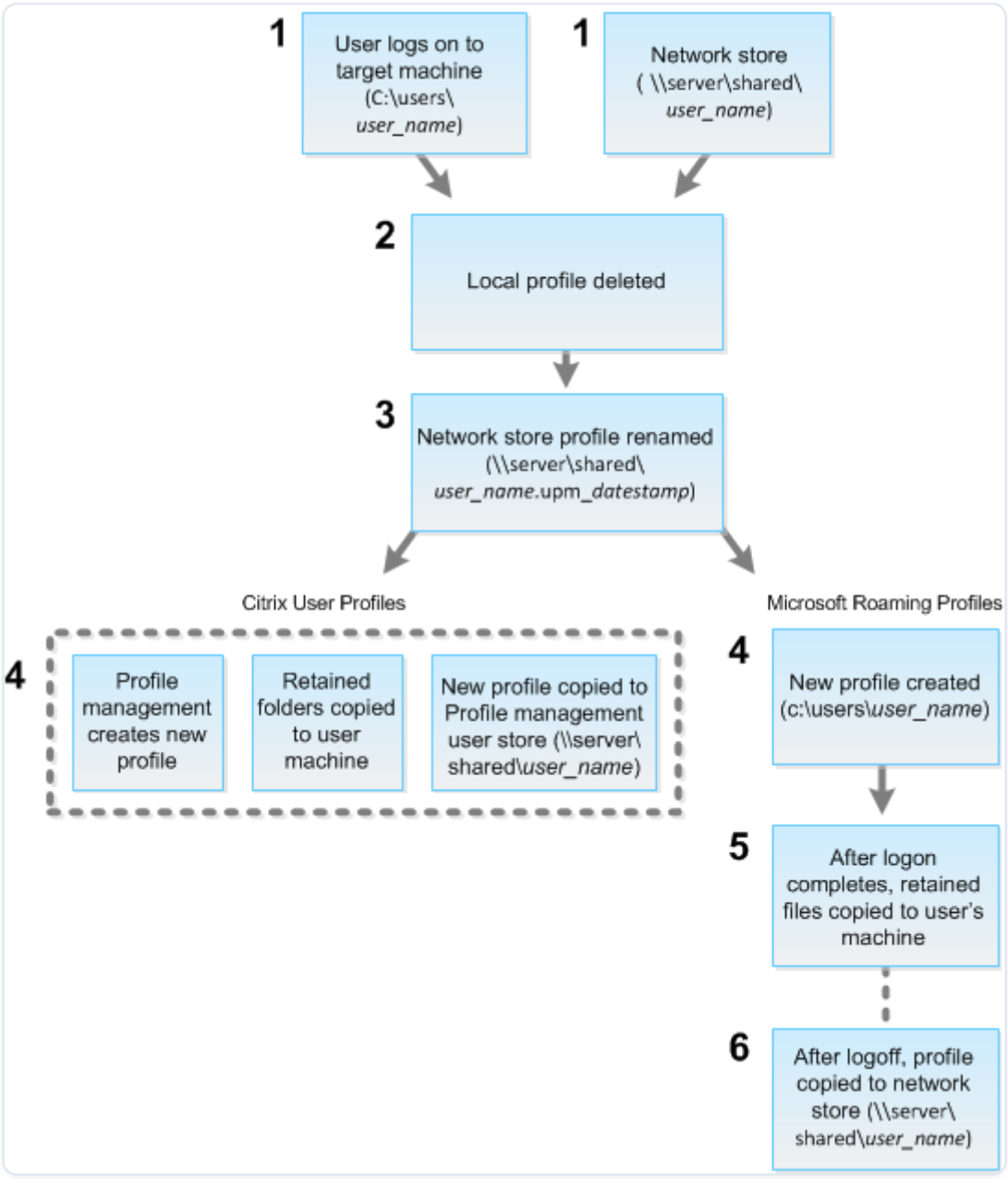
> 重置配置文件时，用户的文件夹和文件将保存并复制到新配置文件。但是，大多数用户配置文件数据会丢失（例如，注册表会重置，应用程序设置可能会被删除）。

> 重置功能适用于基于文件和基于容器的配置文件解决方案。

重置配置文件如何处理

任何 Citrix® 用户配置文件或 Microsoft 漫游配置文件都可以重置。用户注销并选择重置命令（在 Director 中或使用 PowerShell SDK）后，Director 首先识别正在使用的用户配置文件并发出相应的重置命令。Director 通过 Profile Management 接收信息，包括有关配置文件大小、类型和登录时间的信息。

此图说明了用户登录后重置用户配置文件的过程。



Director 发出的重置命令指定配置文件类型。Profile Management 服务随后尝试重置该类型的配置文件并查找相应的网络共享（用户存储）。如果用户由 Profile Management 处理，但收到漫游配置文件命令，则该命令将被拒绝（反之亦然）。

1. 如果存在本地配置文件，则将其删除。
2. 网络配置文件已重命名。
3. 下一个操作取决于要重置的配置文件是 Citrix 用户配置文件还是 Microsoft 漫游配置文件。

   对于 Citrix 用户配置文件，新配置文件是使用 Profile Management 导入规则创建的。文件夹被复制回网络配置文件，用户可以正常登录。如果漫游配置文件用于重置，则漫游配置文件中的任何注册表设置都将保留在重置配置文件中。如有必要，您可以配置 Profile Management，以便模板配置文件覆盖漫游配置文件。

   对于 Microsoft 漫游配置文件，Windows 会创建一个配置文件，当用户登录时，文件夹会复制回用户设备。当用户再次注销时，新配置文件会复制到网络存储。

在 Director 中重置用户配置文件

如果您使用的是 Citrix Virtual Desktops™ (桌面 VDA)，请执行以下操作：

1. 在 **Director** 中，搜索要重置其配置文件的用户，然后选择该用户的会话。
2. 单击 **重置配置文件**。
3. 指示用户从所有会话注销。
4. 指示用户重新登录。 从用户配置文件保存的文件夹和文件将复制到新配置文件。

如果您使用的是 Citrix Virtual Desktops (服务器 VDA)，则需要登录才能执行配置文件重置。然后，用户需要注销并重新登录才能完成配置文件重置。

> **重要提示：**
>
> 如果用户在多个平台（例如 Windows 8 和 Windows 7）上拥有配置文件，请指示用户首先重新登录到用户报告为问题的同一桌面或应用程序。此登录操作可确保重置正确的配置文件。如果配置文件是 Citrix 用户配置文件，则在用户桌面出现时，配置文件已重置。如果配置文件是 Microsoft 漫游配置文件，则文件夹还原可能仍会短暂进行。用户必须保持登录状态，直到还原完成。

> 如果配置文件未成功重置（例如，用户无法成功重新登录到计算机或某些文件丢失），则必须手动还原原始配置文件。

请注意以下事项：

- 如果用户存储作为用户配置文件解决方案启用，则新配置文件包含原始用户配置文件中的以下个人文件夹：
  - 桌面
  - Cookie 文件
  - 收藏夹
  - 文档
  - 图片
  - 音乐
  - 视频
- 从 Citrix Profile Management 2407 版开始，如果配置文件容器作为整个用户配置文件解决方案启用，则新配置文件将保留上述个人文件夹。
- 在 Windows 8 及更高版本中，重置配置文件时，Cookie 不会复制到新配置文件。

在重置失败后手动恢复配置文件

1. 指示用户从所有会话注销。
2. 如果存在本地配置文件，请将其删除。
3. 在网络共享上找到存档文件夹，该文件夹的名称后附加了日期和时间，即带有 .upm_datestamp 扩展名的文件夹。
4. 删除当前配置文件名。即不带 upm_datestamp 扩展名的那个。
5. 使用原始配置文件名重命名存档文件夹。即删除日期和时间扩展名。您已将配置文件恢复到其原始的、重置前的状态。

使用 PowerShell SDK 重置配置文件

您可以使用 Broker PowerShell SDK 重置配置文件。

NEW-BROKERMACHINECOMMAND

创建一个排队等待传送到特定用户、会话或计算机的命令。有关此 cmdlet 的更多信息，请参阅 `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>`。

示例

有关如何使用 PowerShell cmdlet 重置配置文件的详细信息，请参阅以下示例：

重置配置文件管理配置文件

- 假设您要重置 user1 的配置文件。使用 New-BrokerMachineCommand PowerShell 命令。例如：
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **重要提示：**
>
> `CommandData $byteArray` 必须采用以下格式：`<SID>[,<backup path>]`。如果您不提供备份路径，Profile Management 将生成一个以当前日期和时间命名的备份文件夹。

重置 Windows 漫游配置文件

- 假设您想重置 user1 的漫游配置文件。使用 New-BrokerMachineCommand PowerShell 命令。例如：
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

录制会话

您可以使用 Director 中**用户详细信息**和**计算机详细信息**屏幕上的会话录制控件来录制 ICA® 会话。此功能适用于 **Premium** 站点的客户。

动态会话录制

您可以使用**用户详细信息**屏幕上的会话录制控件来录制当前活动会话。有关动态会话录制的详细信息，请参阅会话录制服务文章。

基于策略的会话录制

要使用 DirectorConfig 工具在 Director 上配置基于策略的会话录制，请参阅配置会话录制策略中的**配置 Director 以使用会话录制服务器**部分。 仅当登录用户具有修改会话录制策略的权限时，Director 中才提供会话录制控件。此权限可以在会话录制授权控制台中设置，如授权用户中所述。

> **注意：**

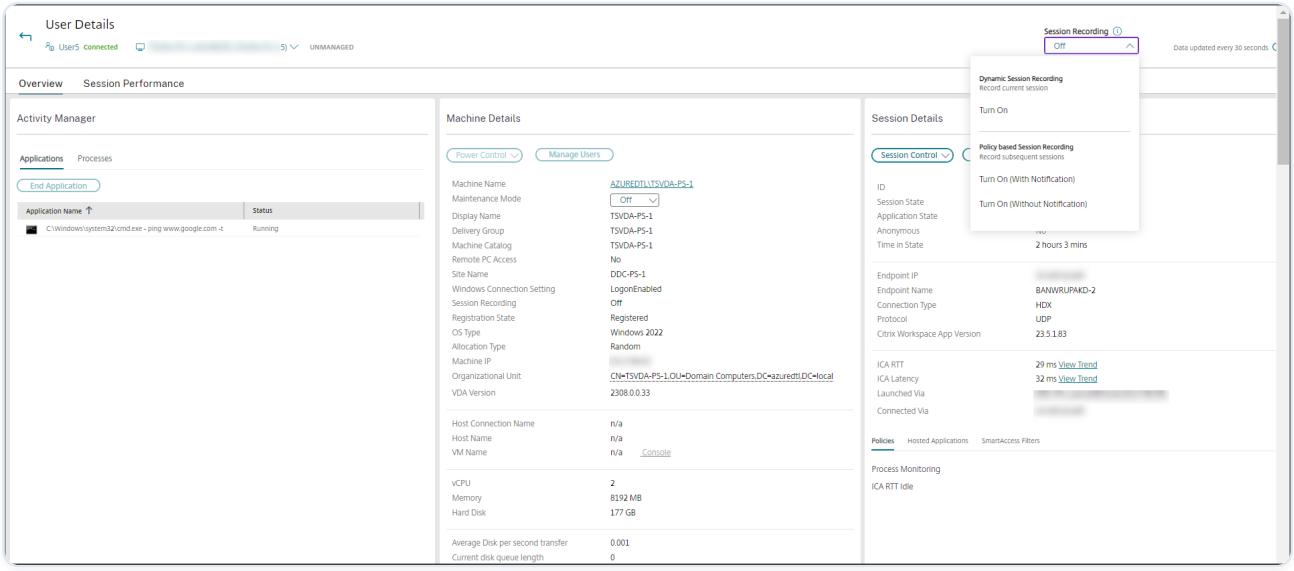
> 通过 Director 或会话录制策略控制台对会话录制设置所做的更改将从后续 ICA 会话开始生效。

Director 中的会话录制控件

您可以使用**用户详细信息** > **会话录制**操作来录制当前会话或后续会话。

- 启用动态会话录制 - 录制当前会话。
- 启用（带通知）- 录制后续会话，并在用户登录 ICA 会话时通知用户会话正在录制。
- 启用（不带通知）- 录制后续会话，并在不通知用户的情况下静默录制会话。
- 禁用 - 禁用用户的会话录制。

策略面板显示活动会话录制策略的名称。



计算机详细信息面板显示计算机的会话录制策略状态。

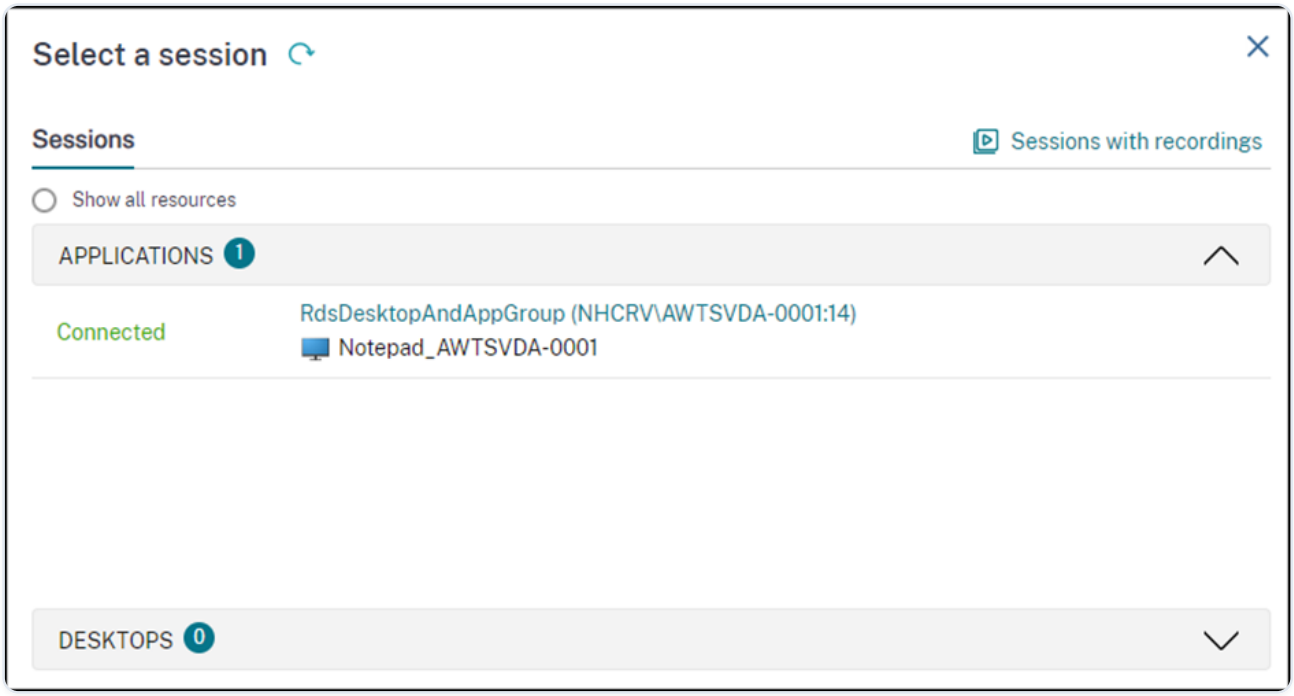
播放实时会话和录制会话

您可以播放录制会话和实时用户会话，以了解用户遇到的问题。在 Director 控制台中随时访问录制内容和会话相关指标，无需在多个会话录制服务器中搜索录制内容或寻找第三方应用程序来查看录制内容。这有助于将录制中发现的问题与性能指标关联起来。

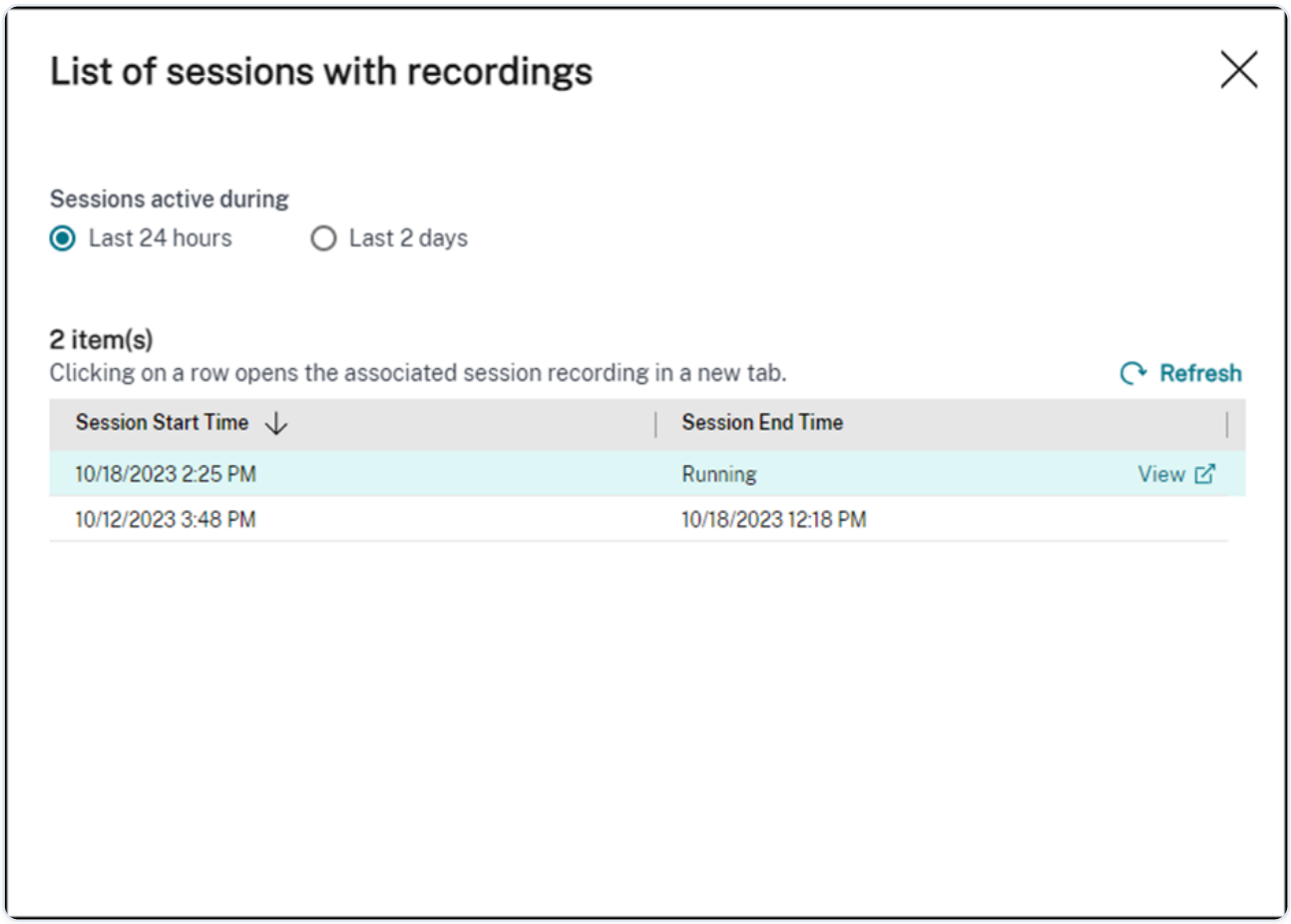
此功能需要满足以下条件：

- VDA 和会话录制服务器的版本为 2308 或更高版本。
- Delivery Controller™ 和 Director 的版本为 2311 或更高版本。

Director 将会话录制内容存储在集中式存储库中。单击“**会话选择器**”模式 > “**包含录制内容的会话**”链接时，将显示属于该用户的录制内容列表。



您可以选择查看过去 24 小时或过去 2 天内处于活动状态的会话录制内容。当前活动会话的实时录制内容将以“**会话结束时间**”为“**正在运行**”进行标记。



单击“**查看**”链接，使用 Citrix 会话录制播放服务器在新选项卡中播放录制内容。

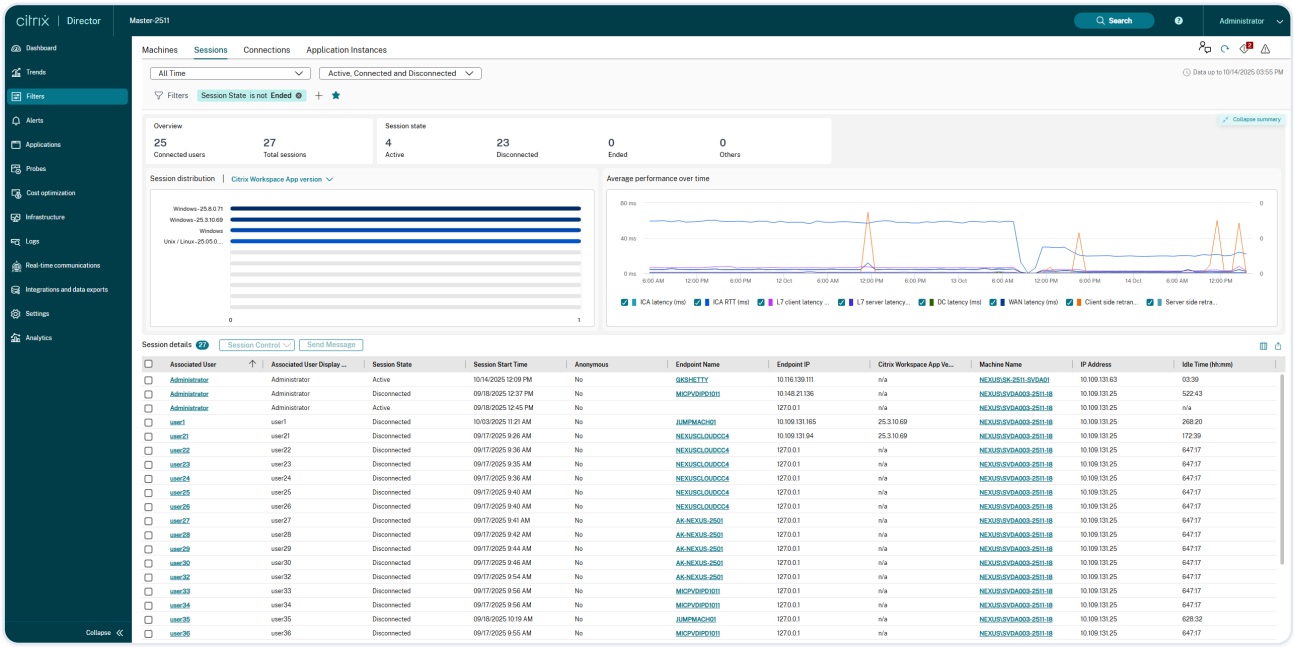
会话视图中的增强型筛选器

1. 概述和主要增强功能

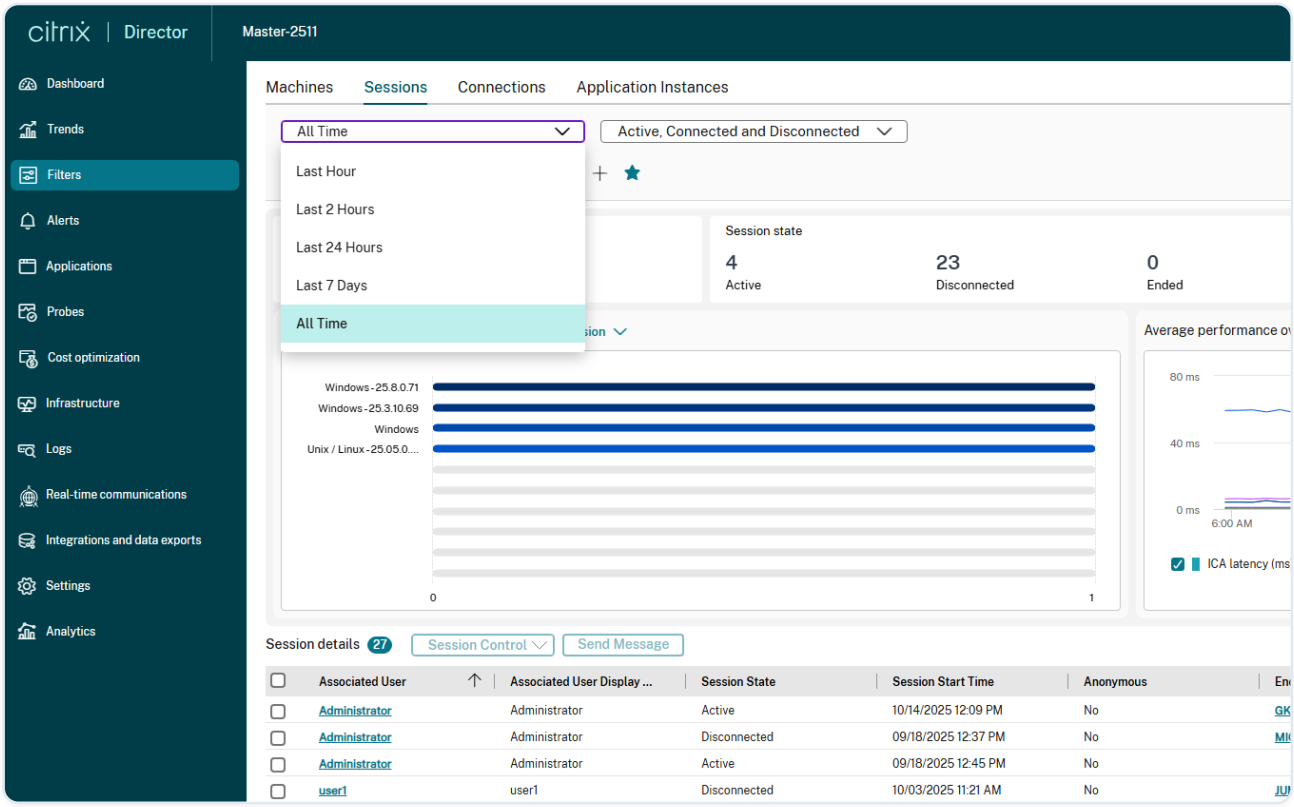
本页面详细介绍了会话视图的主要更新，该视图侧重于实时和历史用户会话监控。

主要增强功能包括：

- **新的时间范围筛选器**：通过新的时间范围选项提高监控精度。
- **简化的筛选器管理**：用于管理默认筛选器和已保存筛选器的新直观下拉菜单。
- **直观的筛选器构建**：用于直接在主页上创建和修改筛选器的新灵活工作流。
- **新的可视化**：引入了**会话分布**图表和**随时间变化的平均性能**图表，以便即时了解会话状态和性能趋势。



2. 新的时间范围筛选器



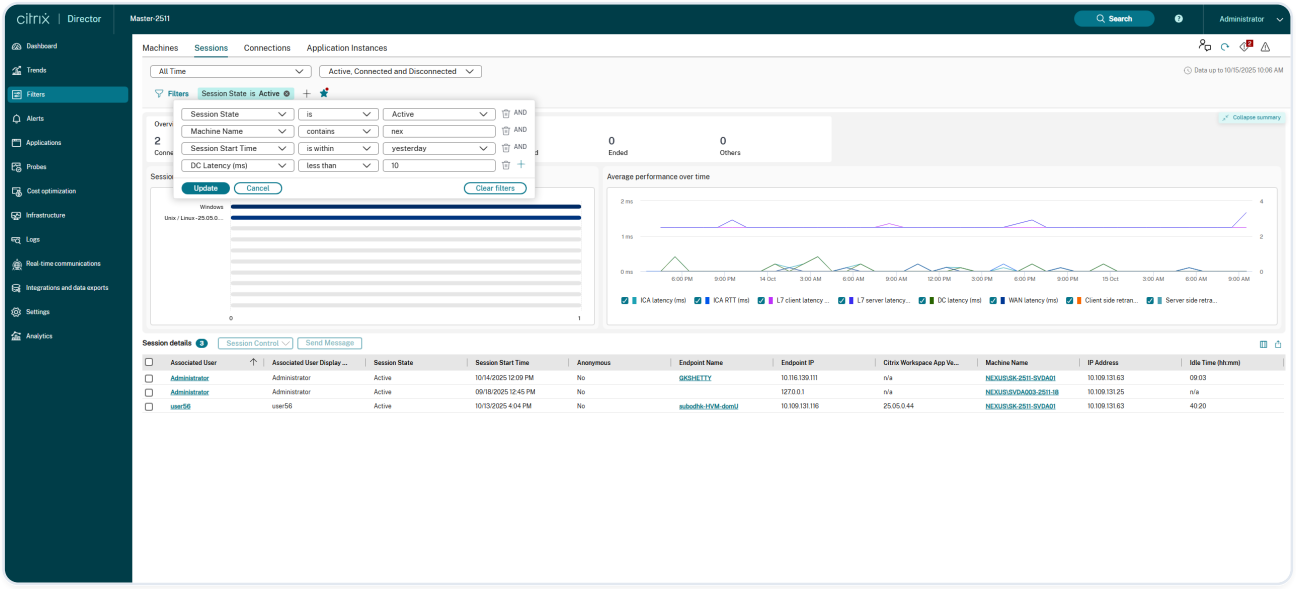
所选时间范围决定了图表和表格的数据集。除了现有选项外，我们还引入了新的精细时间筛选器：

时间筛选器	用途	用例
上一小时	**即时操作**。提供会话活动和性能指标的最新视图。	最适合**实时监控**以及观察管理操作的即时效果，例如重启服务或应用策略。
过去 2 小时 (新增)	**快速故障排除**。捕获最近的数据，以分析突然的峰值或下降。	非常适合**事件后分析**，使您能够精确查明问题（例如高延迟或低 IOPS）在过去两小时内开始的确切时间。
过去 24 小时	**每日概览**。显示一整天的聚合性能数据。	日常操作检查的默认设置，有助于识别在整个业务周期中的高峰使用时间和资源争用。
过去 7 天 (新增)	**每周趋势分析**。提供一周内会话行为的更广泛、持续的视图。	对于**容量规划**、识别每周重复出现的瓶颈以及评估环境的整体稳定性至关重要。
所有时间	**活动状态检查**。显示**所有当前已连接、活动或已断开连接的**	对于获取当前环境中**正在运行的会话**的完整计数至关重要。

时间筛选器	用途	用例
	会话（即未结束），无论其开始日期如何。	

3. 新的筛选器管理体验

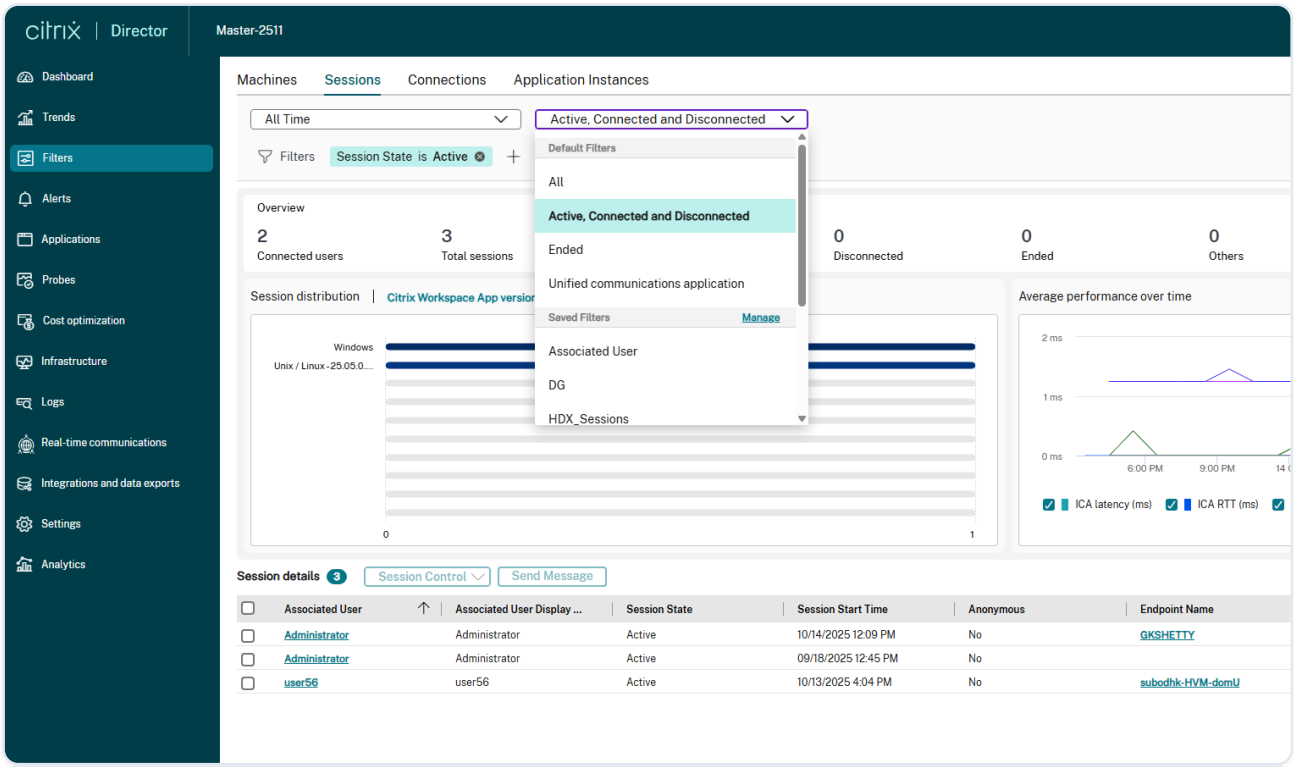
选择、创建和修改筛选器的过程已简化，并已移至数据表正上方。

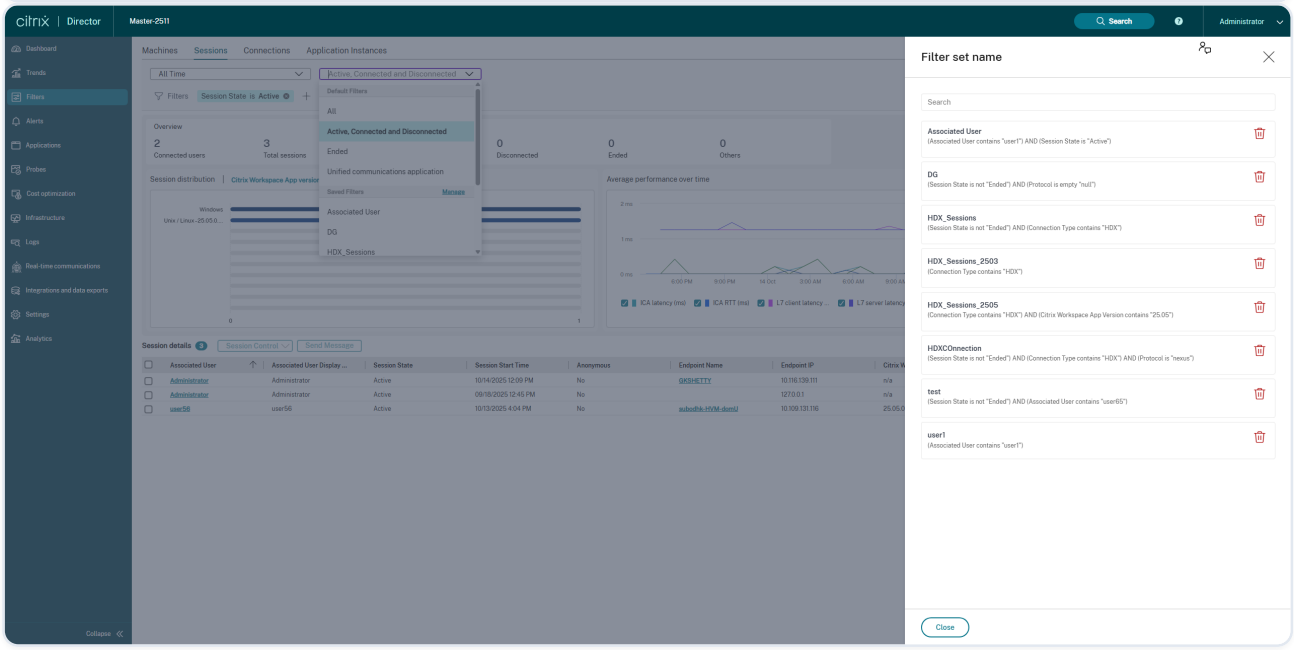


3.1. 访问筛选器

筛选器管理面板已从侧边选项卡移至中心下拉菜单：

1. **默认筛选器**：包含标准、开箱即用的筛选器（例如，活动、已连接和已断开连接）。
2. **已保存的筛选器**：列出管理员创建的所有自定义筛选器集。
3. **管理**：单击**管理**将打开一个侧面板，您可以在其中**搜索**、**查看**或**删除**现有的已保存筛选器。



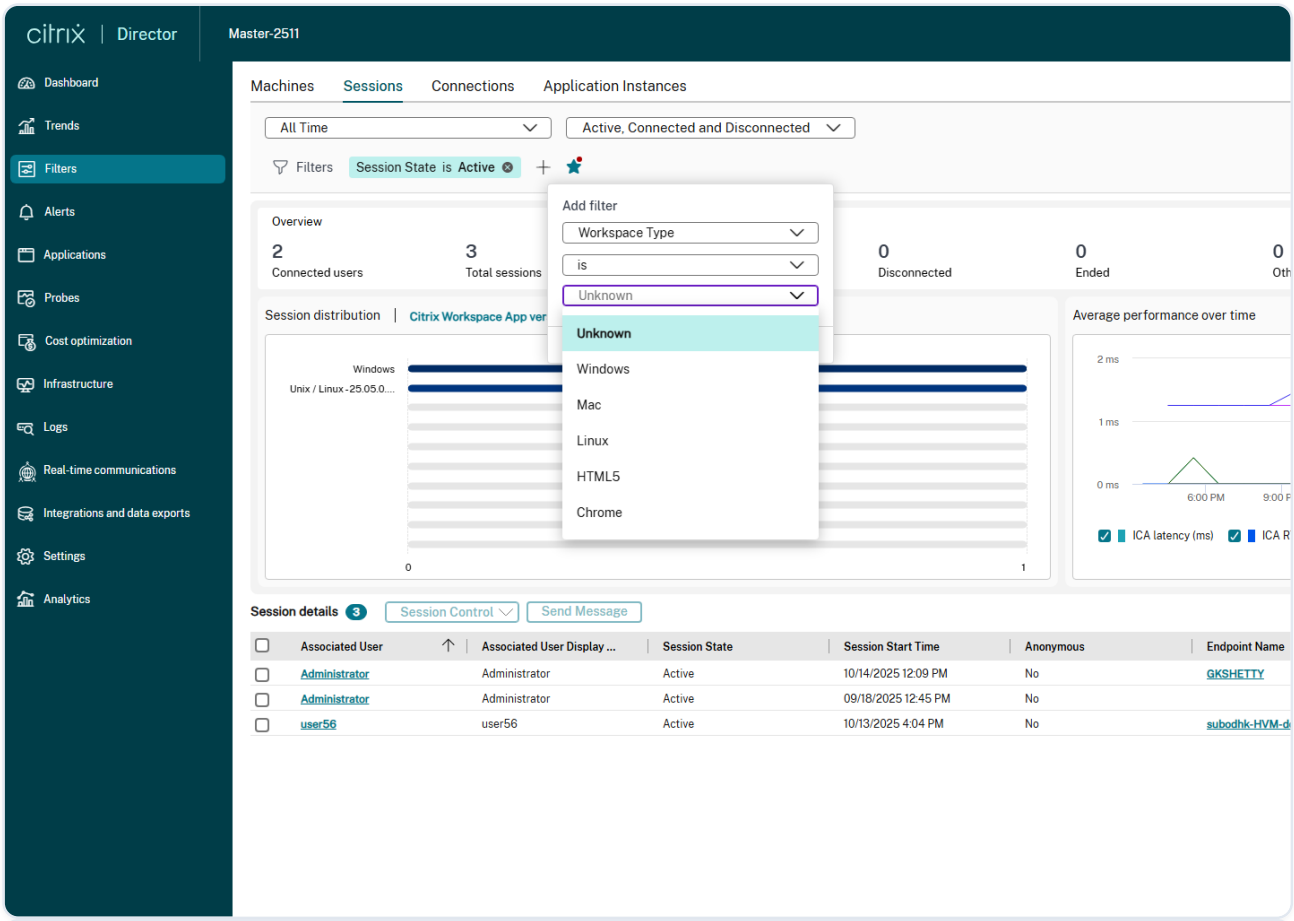


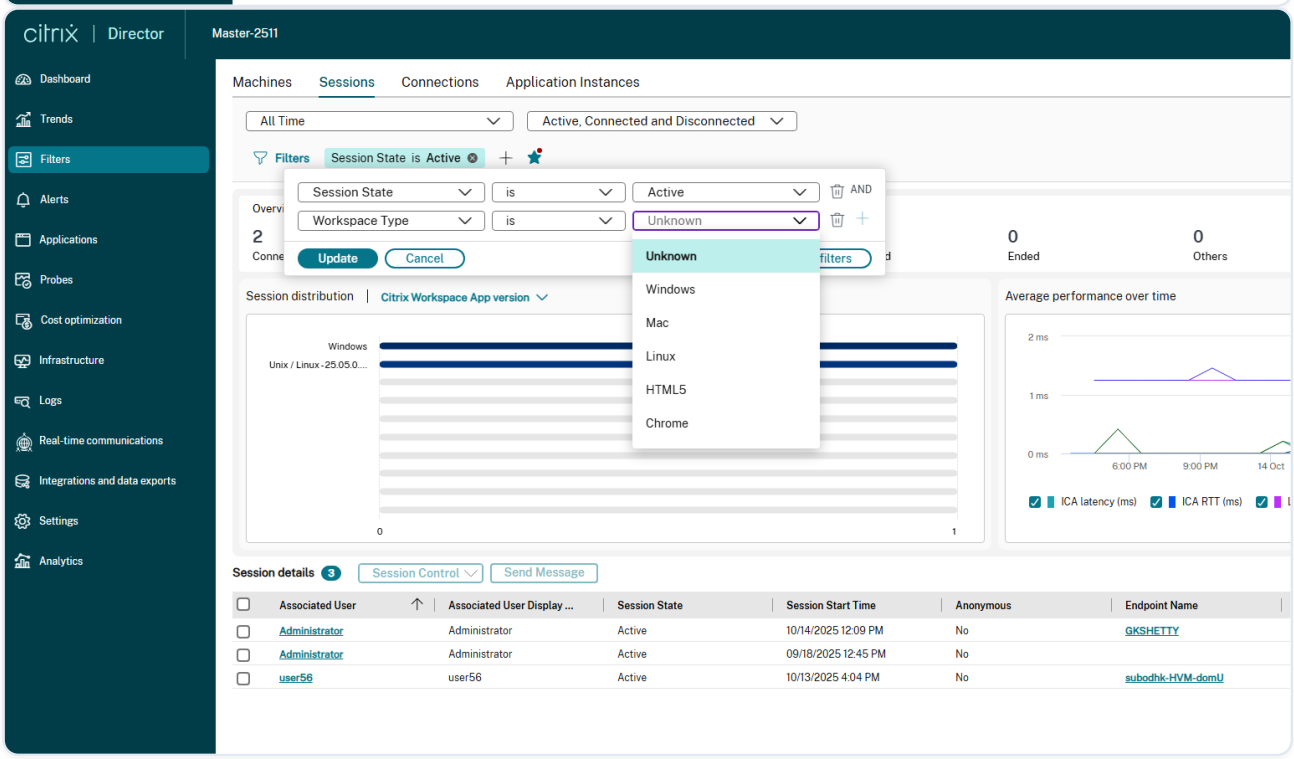
3.2. 构建和应用筛选器

您现在可以直接在会话概览页面上构建复杂的筛选器集：

1. 单击**筛选器**图标或现有筛选器旁边的**+**按钮。

选择条件（例如，**工作区类型**）、运算符（例如，是）和值（例如，Windows、Mac、Linux、HTML5、Chrome、未知）。





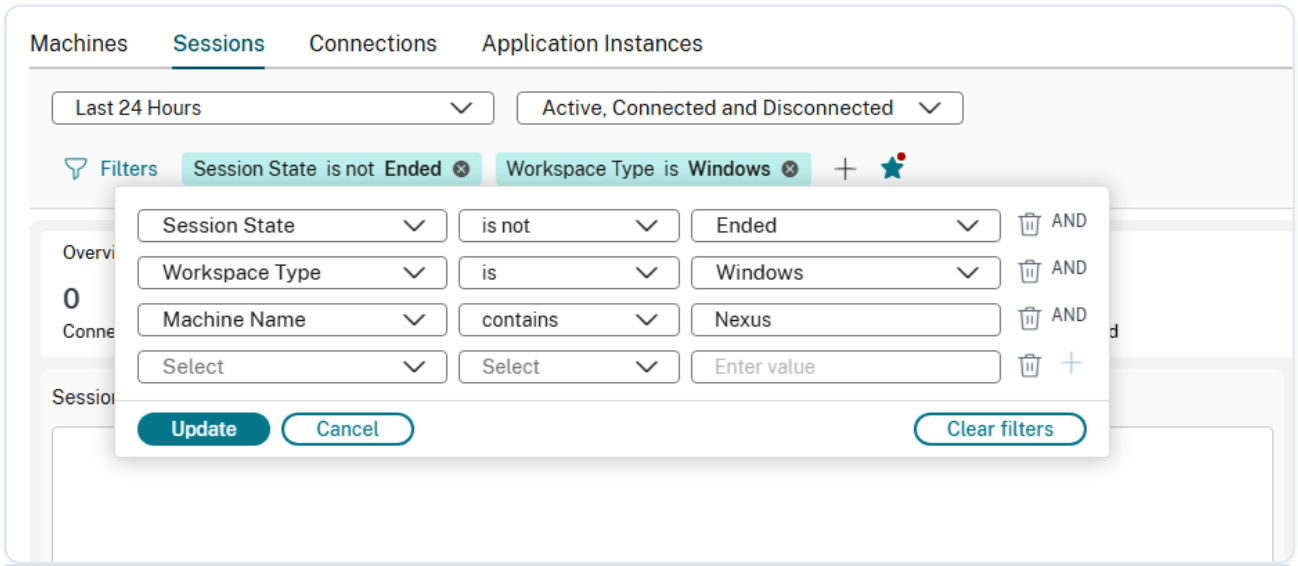
3.3. 筛选器保存状态和工作流程

活动筛选器旁边的星形图标 (⋆) 直观地指示当前筛选器集的状态。这有助于指导管理员保存、应用和管理自定义筛选器。

筛选器状态	图标外观	含义	所需操作
未保存的筛选器	 (带红点的空心轮廓)	当前筛选条件组合**尚未保存**。	单击**空星形图标**以打开对话框，命名筛选器集并保存。
已保存的筛选器	 (已填充 / 实心)	当前活动的筛选器集与之前保存的筛选器**精确匹配**。	无需执行任何操作。您正在根据定义的模板查看数据。
已保存的筛选器有更改	 (填充有红点)	使用**已保存的筛选器**时，如果添加、删除任何其他筛选器或对任何列进行排序，则会出现红点，这意味着更改**尚未保存**。	单击**带红点的星形图标**以更新现有已保存的筛选器，或使用下拉菜单选择**另存为筛选器集**以创建新的筛选器。
默认筛选器			

3.4. 筛选器操作按钮

添加新筛选器或修改已保存的筛选器时，以下控件和状态指示器将可用：



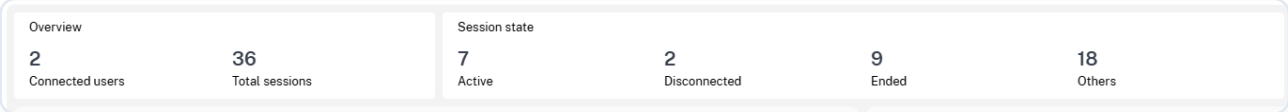
按钮	含义和操作
更新	将所有当前活动的筛选条件应用于图表和应用程序性能数据表。

按钮	含义和操作
取消	放弃对当前筛选器集所做的任何更改，并恢复到上次应用的筛选器。
清除筛选器	删除所有新添加的筛选条件。
图标	删除单击此图标时选定的筛选条件。

4. 新可视化：会话分析

已添加两个新图表，可即时、图形化地深入了解会话行为和性能。

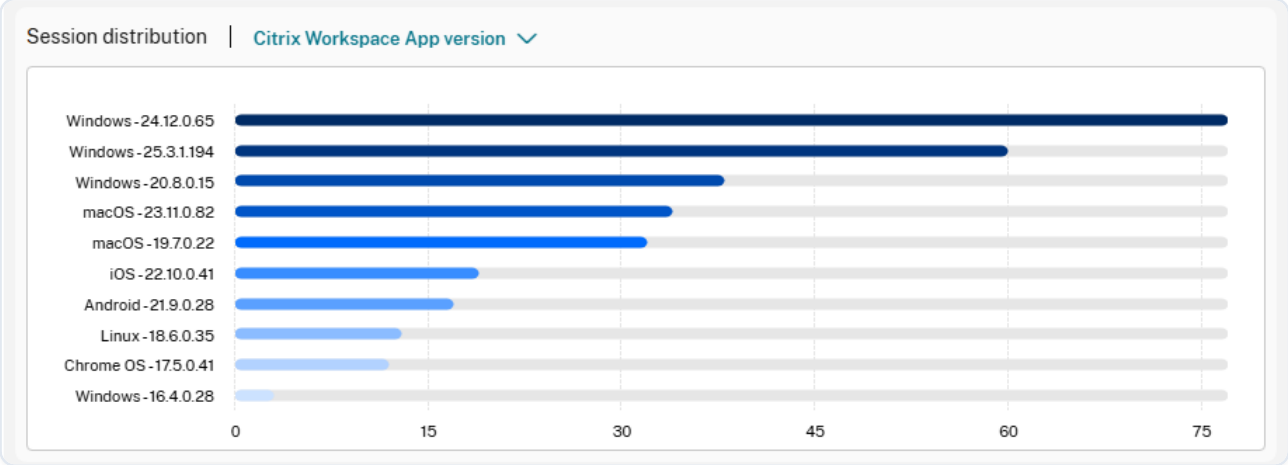
4.1. 摘要面板

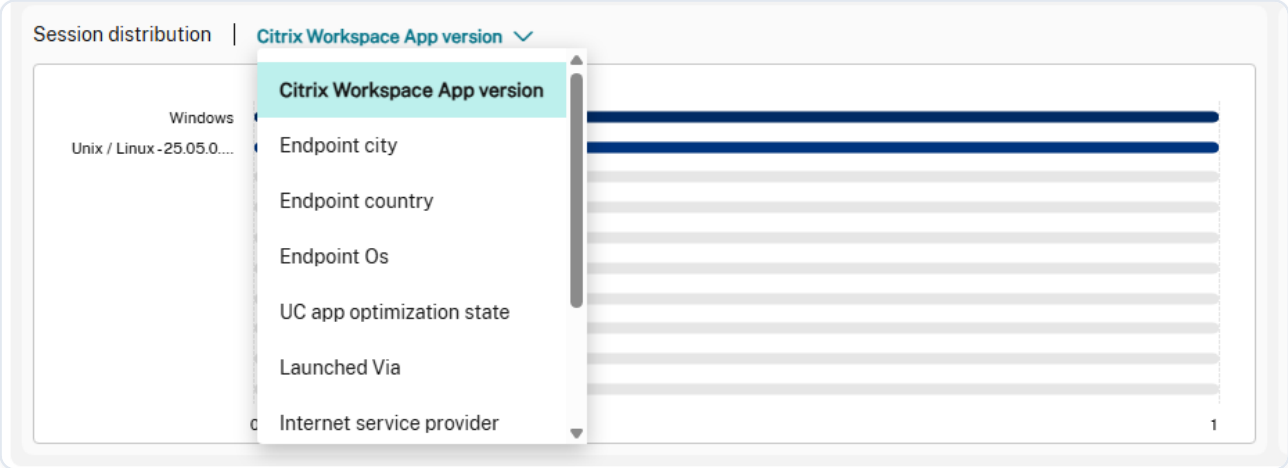


- **概述**：显示连接用户总数以及与其关联的总会话数。
- **会话状态**：根据会话状态（活动、已断开连接、已结束及其他）显示会话数。

此摘要可折叠，可帮助管理员根据上述分类采取必要措施，例如了解长时间运行的会话并在需要时将其结束，或根据断开连接的会话识别任何网络中断。

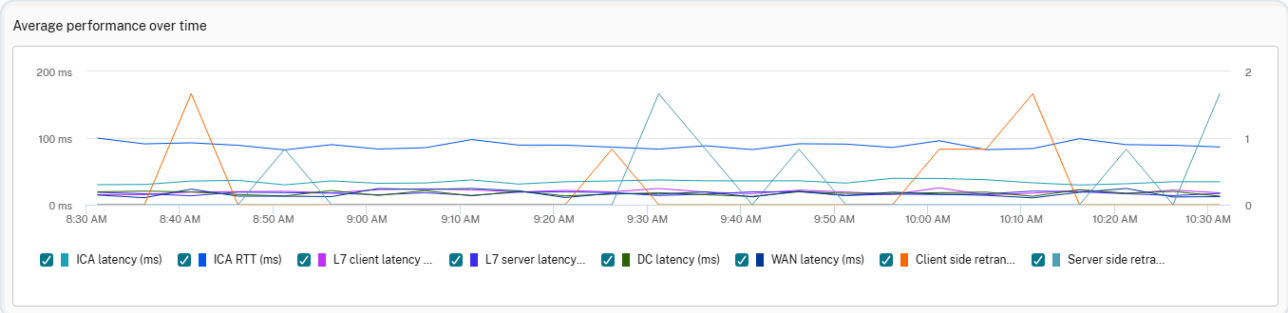
4.2. 会话分布

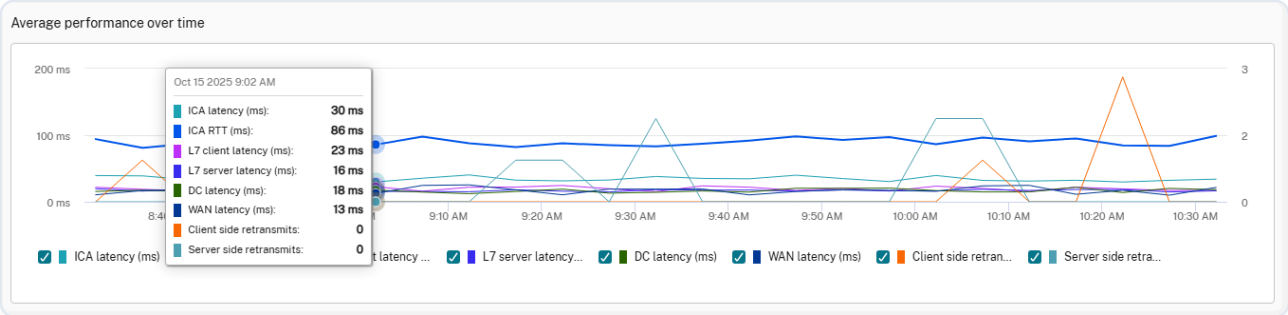


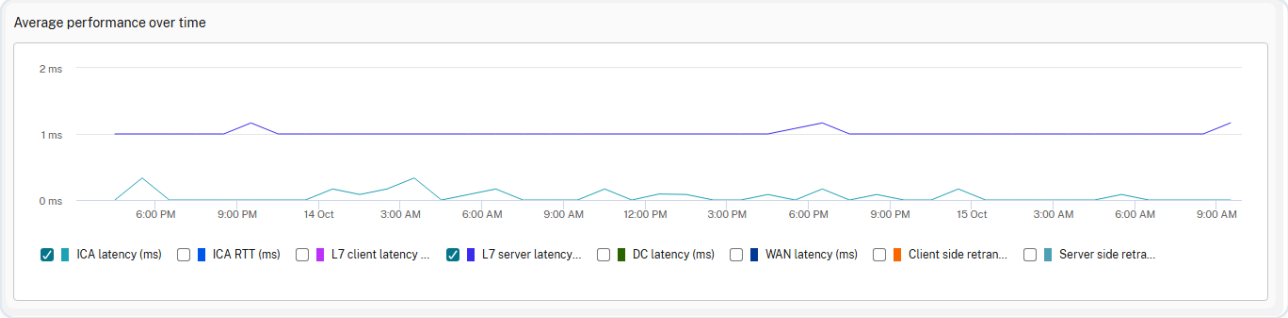


- **用途：**此图表按选定的分类指标细分当前筛选的会话，默认为 **Citrix Workspace App 版本**。
- **实用性：帮助管理员根据用户环境、客户端版本和连接设置快速识别会话趋势。例如，通过按工作区类型**筛选，可以显示有多少用户通过 Mac 与 Windows 或 HTML5 客户端连接。
- **支持的筛选器类型：**分布可以按以下方式细分：
  - Citrix Workspace 应用程序版本
  - 端点城市
  - 端点国家/地区
  - UC 应用优化状态
  - 启动方式
  - 互联网服务提供商
  - 机器名称
  - 协议
  - 工作区类型

4.3. 随时间变化的平均性能







- **用途：**跟踪当前筛选器和时间范围内包含的会话的关键会话性能指标。
- **跟踪的关键指标：** 此图表侧重于对用户体验至关重要的指标：
  - ICA 延迟（毫秒）
  - ICA RTT（毫秒）
  - L7 客户端延迟（毫秒）
  - L7 服务器延迟（毫秒）
  - DC 延迟（毫秒）
  - WAN 延迟（毫秒）
  - 客户端重传
  - 服务器端重传
- **实用性：**对于快速将用户投诉与历史性能数据关联起来至关重要。此图表中延迟或重传的任何向上尖峰都表明可能存在影响用户体验的网络或 VDA 性能问题。

混合多云部署的统一搜索

以前，在故障排除期间，当您在 Director 中搜索用户时，只有当用户来自本地站点时，您才能获取用户详细信息。如果用户来自云站点，则必须转到 Monitor 再次搜索。

借助此增强的搜索功能，您可以使用 Director 中的“**搜索**”选项搜索来自云站点或本地站点的用户。当您使用混合部署（包括云站点和本地站点）以及将 Director 用于故障排除目的时，可以使用此功能。无论用户来自本地站点还是云站点，您都可以获取其详细信息。如果站点存在于 Director 中，

您可以直接导航到 Director 中所选会话的活动管理器。如果站点不存在于 Director 中，您可以直接导航到 Monitor 中所选会话的活动管理器。然后，继续进行故障排除。

> **注意：**
>
> 您可以通过 Citrix Director 使用统一搜索控制台。
>
> 此功能缩短了解决问题的平均时间，并通过一个控制台为云用户和本地用户提供了无缝体验。额外的好处是，由于只有云站点详细信息添加到 Director 中，因此数据库大小不会快速增长。用户详细信息保存在云中。

> **注意：**
>
> 对于最多六个或更少的云站点，您可以在三秒内获得搜索结果。
>
> 要启用此功能，您需要将云站点连接到 Director。

将云站点连接到 Director

先决条件

要在 Citrix Director 中配置统一搜索，无需安装任何新组件。请确保满足以下要求：

- 对于统一搜索，所有 Delivery Controller 和安装了 Director 的计算机上都必须具有出站 Internet 访问权限。具体而言，请确保可以访问以下 URL：
  - Citrix 密钥注册: `<https://*.citrixnetworkapi.net/>`
  - 思杰云：`<https://*.citrixworkspacesapi.net/>`
  - 思杰桌面即服务：`<https://*.cloud.com/>`
  - 微软 Azure：`<https://*.windows.net/>`
- 如果 Delivery Controller 和 Director 计算机位于内网中，并且出站 Internet 访问通过代理服务器进行，请确保满足以下条件：
  - 代理服务器必须允许上述 URL 列表。

- 在 Director 的 **web.config** 和 **citrix.monitor.exe.config** 文件中添加以下配置。确保将此配置添加到 **configuration** 标记内：

```
<system.net>

    <defaultProxy>

        <proxy usesystemdefault="false" proxyaddress="http://
<your_proxyserver_address>:80" bypassonlocal="true" />

    </defaultProxy>

</system.net>
```

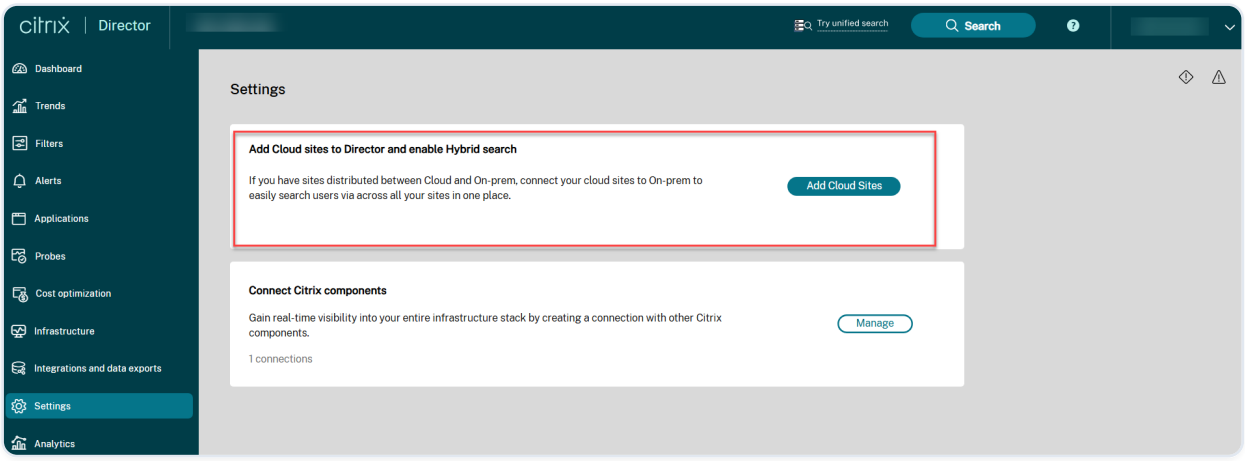
- Director **web.config** 位于安装 Director 的计算机上的 `C:\inetpub\wwwroot\Director\web.config`。
- **citrix.monitor.exe.config** 位于安装 Delivery Controller 的计算机上的 `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config`。

此设置由 Microsoft 在 IIS 上提供。有关详细信息，请参阅代理配置。配置文件中的 **defaultproxy** 字段控制 Director 和监视服务的出站访问。与 Citrix DaaS 的配置和通信要求将 **defaultproxy** 字段设置为 true。生效的策略可能会将此字段设置为 false。在这种情况下，您必须手动将该字段设置为 true。在进行更改之前，请备份配置文件。重新启动 Delivery Controller 上的监视服务以使更改生效。

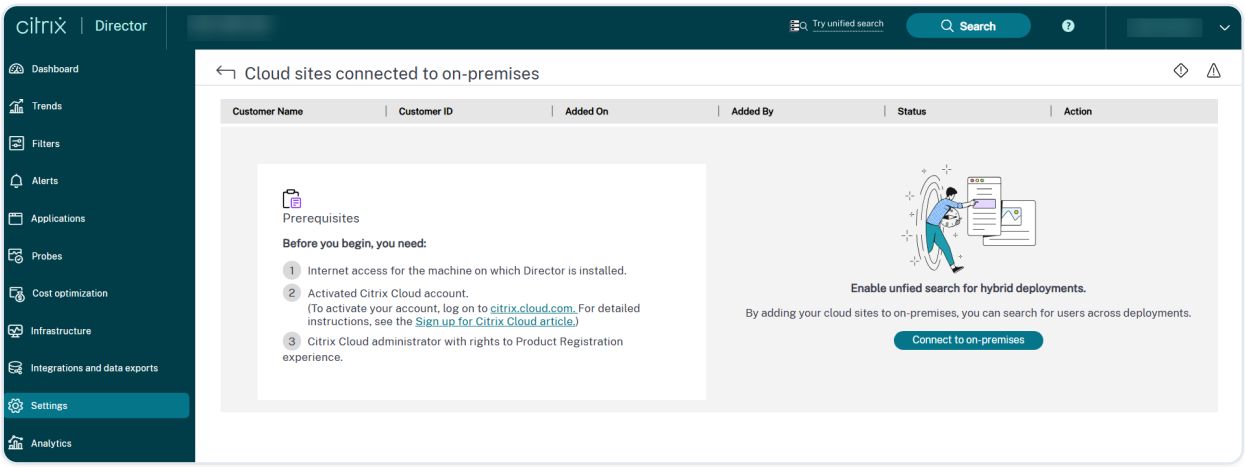
- 您拥有 DaaS 的有效 Citrix Cloud™ 权利。
- 您的 Citrix Cloud 帐户是具有产品注册体验权限的管理员帐户。有关管理员权限的详细信息，请参阅修改管理员权限。
- 确保安装 Citrix Director 的计算机具有 Internet 访问权限。
- 要使用 Citrix Cloud 服务，您必须能够通过 HTTPS 端口 443 连接到所需的 Citrix 地址。有关详细信息，请参阅Internet 连接要求。
- 确保您拥有执行产品注册的完全管理员访问权限。

配置步骤

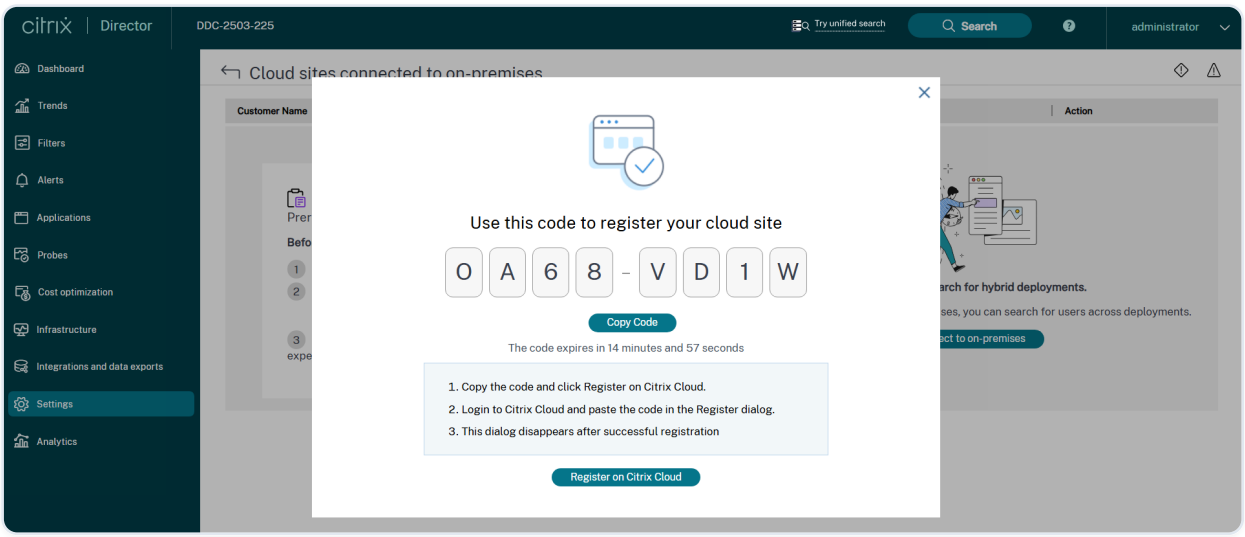
1. 以完全管理员身份登录 Director。此时将显示 Director 仪表板页面。
2. 单击**设置**选项卡。此时将显示**设置**页面。



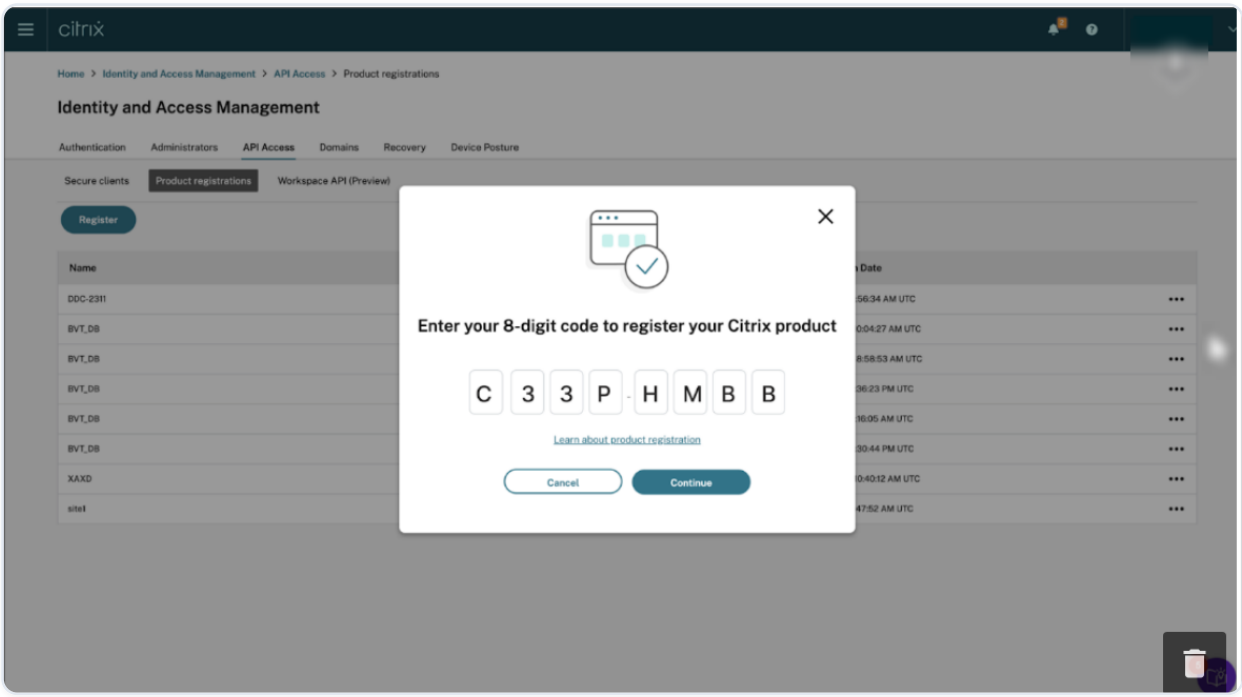
3. 单击**添加云站点**。此时将显示以下页面：



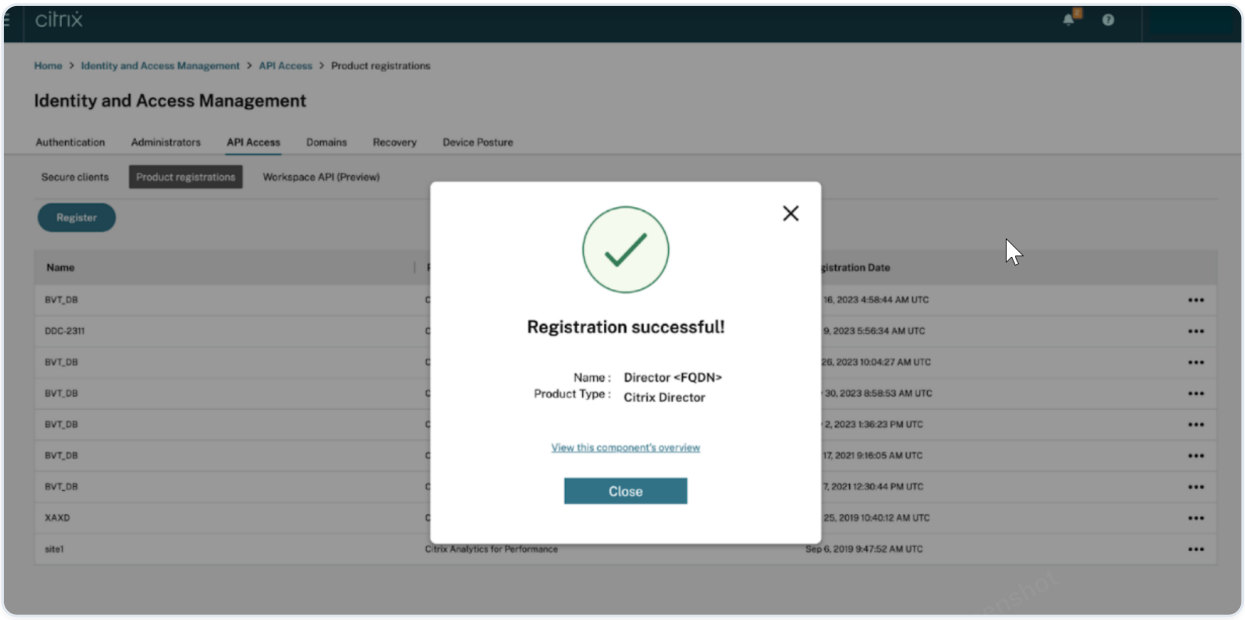
4. 检查先决条件，然后单击 **连接云站点** 以开始配置过程。将生成一个唯一的 8 位注册码，用于将此站点注册到 Citrix Cloud。



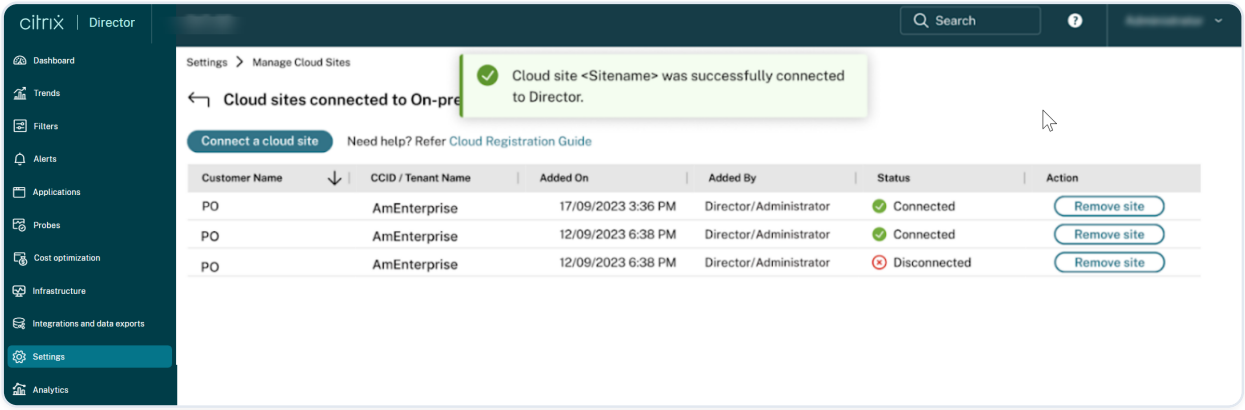
5. 单击 **复制代码** 以复制代码，然后单击 **在 Citrix Cloud 上注册**。您将被重定向到 Citrix Cloud 中的注册 URL。
6. 使用您的 Citrix Cloud 凭据登录并选择您的客户。
7. 将复制的注册码粘贴到 Citrix Cloud 的 **产品注册** 页面中。单击 **继续** 以注册站点。



8. 单击 **继续**。您的云站点将注册到 Citrix Director，您将收到以下消息：



9. 单击 **关闭**。将显示以下屏幕：



10. 要使用 Director 配置多个云站点，请从 Director 为每个站点重复上述配置步骤。

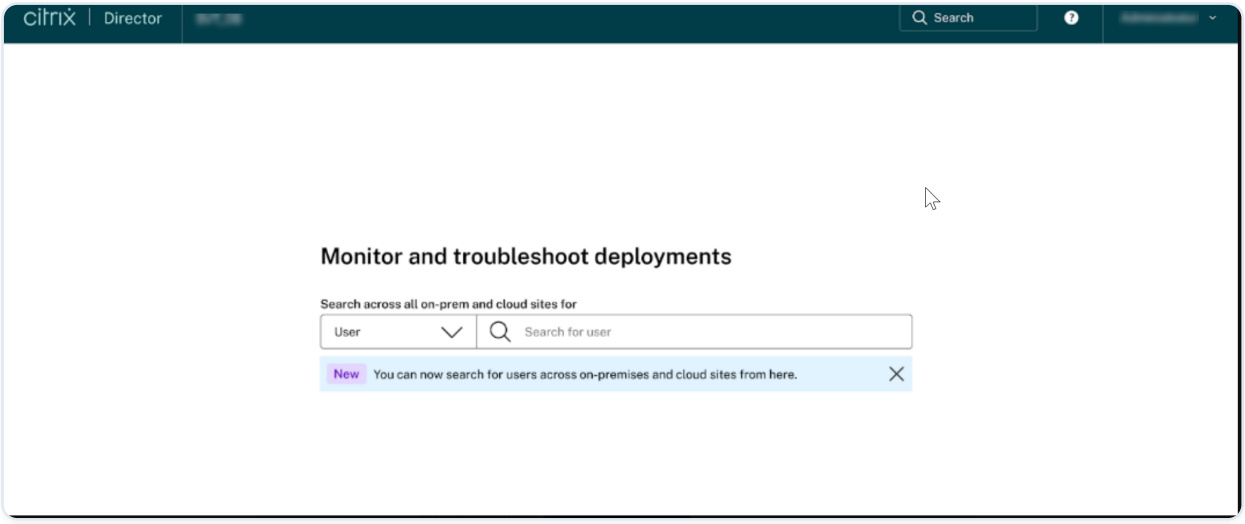
    如果每个站点运行多个 Director 实例，请从任意一个 Director 实例进行配置。连接到该站点的所有其他 Director 实例将在配置过程后的下一次刷新时更新。

> **注意：**
>
> 要将您的站点与 Citrix Director 断开连接，请单击 **删除站点**。此选项将删除现有配置。

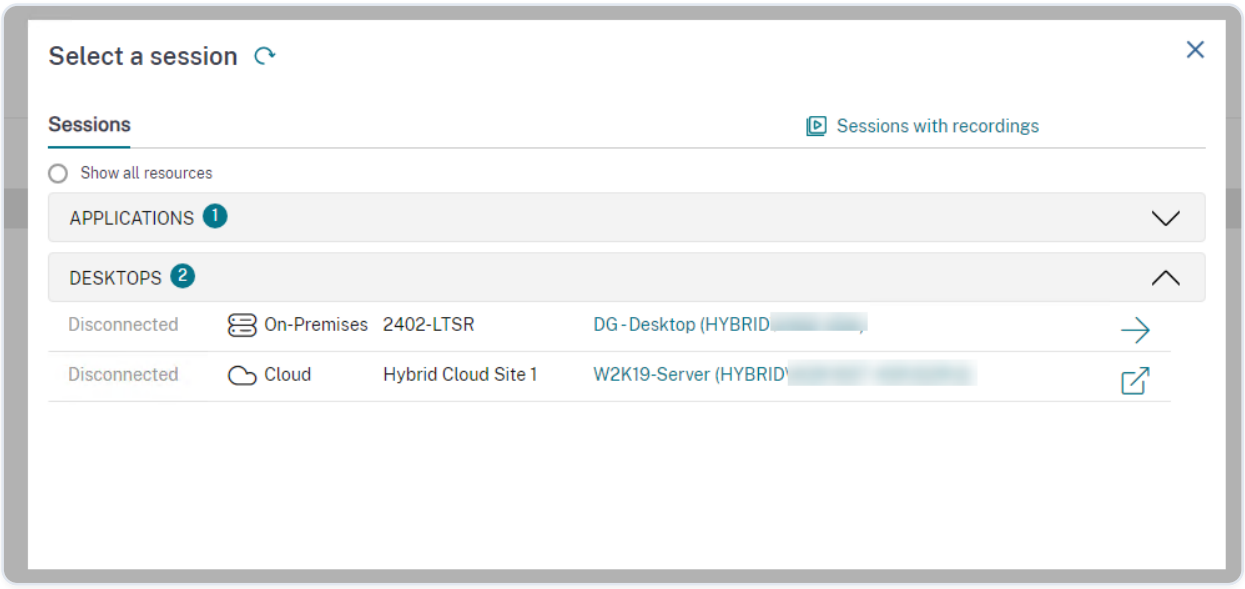
从混合部署中搜索用户

要搜索用户，请执行以下操作：

1. 在顶部导航栏中点击“**搜索**”。“**监视和故障排除部署**”页面随即显示：



2. 从下拉列表中选择“**用户**”并输入用户名。随即显示来自本地和云部署的活动会话和失败会话列表：



3. 选择要检查的会话：

- 如果是使用云部署的会话，将打开包含用户上下文的相关 DaaS Monitor URL 到“**活动管理器**”页面，以快速开始故障排除。
- 如果是使用本地部署的会话，“活动管理器”页面将快速打开以开始故障排除。

基础架构监控

Director 现在提供 Citrix Virtual Apps and Desktops™ 组件运行状况的可视性。此功能可帮助您轻松识别、排查和解决与基础结构相关的问题。目前，正在监视以下组件的运行状况：

- 交付控制器™
- 思杰预置™ 服务
- StoreFront™

为支持此功能，为 Citrix 组件引入了一个名为 `citrixinframonitor.msi` 的新 Windows 可执行文件。这有助于从 Provisioning Service 或 StoreFront 服务器收集相关运行状况指标并将其传输到 Director。但是，监视 Delivery Controller 不需要 `CitrixInfraMonitor.msi`。Delivery Controller 组件连接到 Citrix Virtual Apps and Desktops 站点后，会自动加入监视。

此功能可帮助您在 Director 中的单个控制板上获取有关 Delivery Controller、Provisioning Service 和 StoreFront 服务器的关键监视数据集和主动警报。每五分钟从受监视组件收集一次数据，以确保信息最新。

此功能旨在通过提供主动监视、详细指标和自动化警报来提高运营效率，确保您的 Citrix® 基础结构平稳高效地运行。

主要功能

实时监控：

- 持续监视 Citrix 基础结构组件，例如 Delivery Controller、Citrix Provisioning (Provisioning Service) 服务器和 StoreFront。
- 仪表板视图，显示系统运行状况、资源利用率和相关性能指标。

详细分析：

- 提供对系统运行状况指标的详细分析，例如每个组件的连接状态以及服务或进程状态。
- 资源利用率指标（如 CPU、内存和磁盘利用率）的详细信息。

自动警报和通知：

- 针对各种指标和状态的可自定义警报阈值，具有精细的范围。
- 通过电子邮件和 Webhook 进行实时通知。

用例

运营效率：

确保 Citrix 管理团队能够维护其 Citrix 服务器和服务的高可用性和性能。此功能还有助于通过在问题影响重要用户组之前主动识别并提醒管理员来最大程度地减少停机时间。

更快的工单解决：

监控服务器运行状况和性能的关键指标，以评估向用户交付虚拟应用程序和桌面的最佳方式。使用这些指标通过分析相关组件来诊断和解决与性能相关的用户投诉。

先决条件

- Citrix Virtual Apps and Desktops™ 2407 或更高版本
- 确保满足 Provisioning Service 的先决条件 或 StoreFront 的先决条件。
- 对于监控 Citrix Provisioning：
  - 监视 **DB Connectivity** 和 **License Server Reachability** 所需的最低版本为 Citrix Provisioning 2407
  - 监视 **PXE Service**、**TFTP Service** 和 **Total Reconnect Count** 所需的最低版本为 Citrix Infra Monitor 2411
- 运行 Citrix Infrastructure Monitor 所需的用户帐户或权限：

- 具有 Windows 管理员权限的用户帐户，用于在端点计算机上安装 Citrix Infrastructure Monitor。
- 具有以下 Director 权限的完全管理员用户帐户或自定义角色：
  - 创建\编辑\启用\删除警报策略
  - 创建\编辑\删除警报电子邮件服务器配置
  - 创建\编辑\管理与 Citrix 组件的连接（基础结构监视）
  - 消除警报
  - 查看警报策略
  - 查看警报
  - 查看仪表板页面
  - 查看基础设施监控页面

> **注意：**
>
> - 上述先决条件仅适用于 Provisioning Service 和 StoreFront 组件监控。
> - 如果您没有访问**警报**页面的权限，则**基础设施监控**页面上的**管理警报**选项将被禁用。

有关详细信息，请参阅以下内容：

- 基础架构监控入门
- 管理连接
- 基础架构控制板
- 高级警报策略
- 基础架构策略

基础设施监控入门

您可以使用以下方式连接到 Citrix Infrastructure Monitor：

- 手动连接 - 手动下载并安装 Citrix Infrastructure Monitor 服务。
- 自动连接 - UI 自动处理下载和安装。

在手动和自动连接后，您可以选择为 Citrix Infrastructure Monitor 配置 HTTPS。

有关详细信息，请参阅以下内容：

- 手动连接
- 自动连接
- 为 Citrix 基础设施监视器配置 HTTPS

Citrix Infrastructure Monitor 的手动连接

> **注意：**
>
> 以下两个步骤仅适用于 Provisioning Service 和 StoreFront™ 组件监控。

步骤 1：安装 Citrix 基础架构监视器

执行以下步骤以在目标组件上完成安装，从而建立安全数据收集的连接。

> **注意：**
>
> 您正在安装 Citrix Infrastructure Monitor 的计算机必须已安装 Provisioning Service 和 StoreFront。

步骤 1.1：识别目标组件

识别需要监控的目标组件，例如 Provisioning Service 或 StoreFront 服务器。

步骤 1.2 下载 Citrix 基础架构监视器

您可以从 步骤 1.1 中识别的目标服务器上的 Citrix 下载 页面下载 `CitrixInfraMonitor.msi`。

步骤 1.3：运行 Citrix 基础架构监视器

按照安装向导中的说明，在目标组件上运行 `CitrixInfraMonitor.msi` 安装程序。

> **注意：**
>
> 具有管理权限的用户可以在目标组件上安装和配置 Citrix Infrastructure Monitor。

> Citrix 基础设施监视器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/citrixinframonitoring-resize.gif)

安装成功后，您可以在“**服务**”部分查看 Citrix Infrastructure Monitor 服务：

Citrix 基础设施监视器(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/infra-services.png)

步骤 1.4：获取注册令牌

在安装了 Citrix 基础设施监视器的系统中，获取 `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` 处 `RegistrationToken.txt` 文件中提供的令牌，并准备好在 步骤 2：注册 Citrix 基础设施监视器 中使用。

端口要求

成功安装 `CitrixInfraMonitor.msi` 后，安装程序会为 9595 端口创建例外。如果您使用任何第三方防火墙，则可能需要手动允许此端口的 TCP 通信，才能使用 Citrix 基础设施监视服务。

下表提供了 Provisioning Service 和 StoreFront 计算机的入站端口要求详细信息：

源	目标	类型	端口	协议	目的
DDC	Provisioning Service 或 StoreFront 计算机	TCP	9595	HTTP 或 HTTPS	调用以从 Provisioning Service 或 StoreFront 计算机收集指标。

> **注意：**

> Provisioning Service 和 StoreFront 计算机不会为基础设施监控服务进行任何出站调用。

步骤 2：注册 Citrix 基础设施监控器

您可以使用以下方式注册 Citrix 基础设施监控器：

- Director 用户界面
- PowerShell SDK

从 Director 用户界面

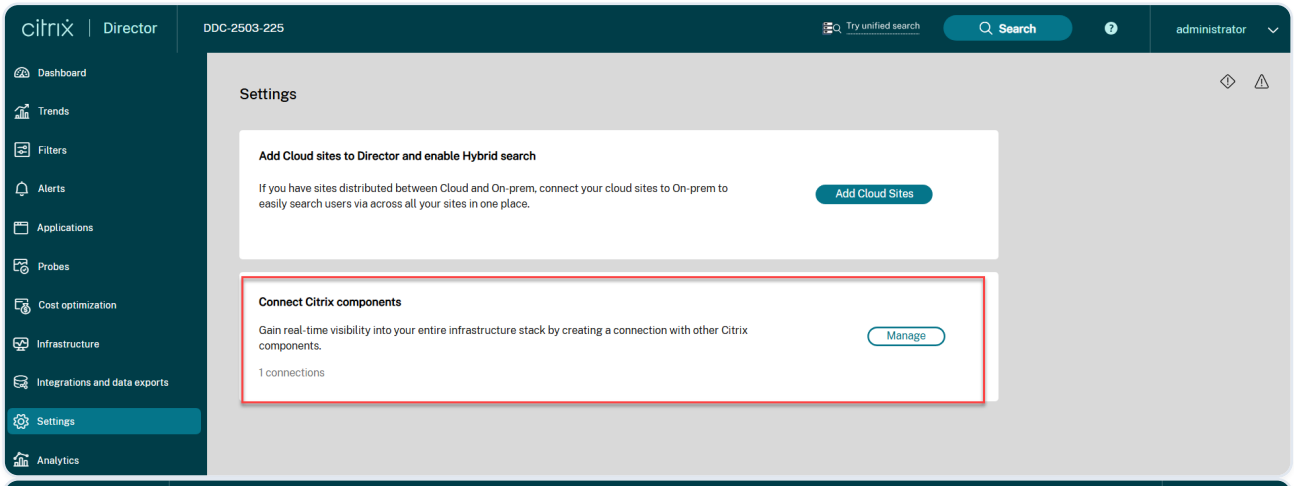
使用以下步骤在 Director UI 上完成注册：

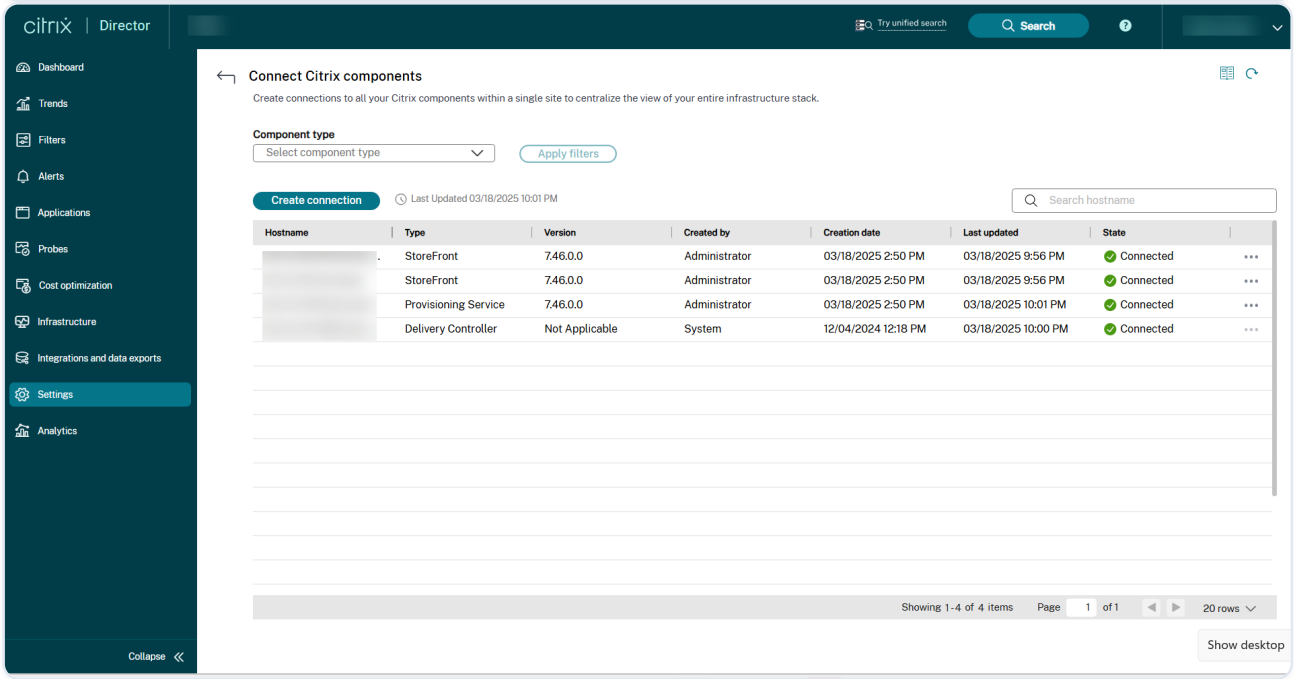
步骤 2.1：导航到“连接 CITRIX 组件”页面

单击“**设置**”>“**连接 Citrix 组件**”>“**管理**”。

或者，

单击**基础设施** > **管理**。





步骤 2.2：输入组件详细信息

在“**连接 Citrix 组件**”屏幕上，单击“**创建连接**”。将显示“**创建连接**”窗口。

确保 `CitrixInfraMonitor.msi` 已下载并安装在目标上。有关详细信息，请参阅本文档中的步骤 1。按照屏幕上的说明操作，并填写建立安全连接所需的组件详细信息。

- 从下拉列表中选择组件类型。组件可以是 Provisioning Service 或 StoreFront。
- 输入主机名。
- 输入域名。
- 输入 Provisioning Service 或 StoreFront 计算机的用户名。
- 输入 Provisioning Service 或 StoreFront 计算机的密码。

步骤 2.3：授权连接

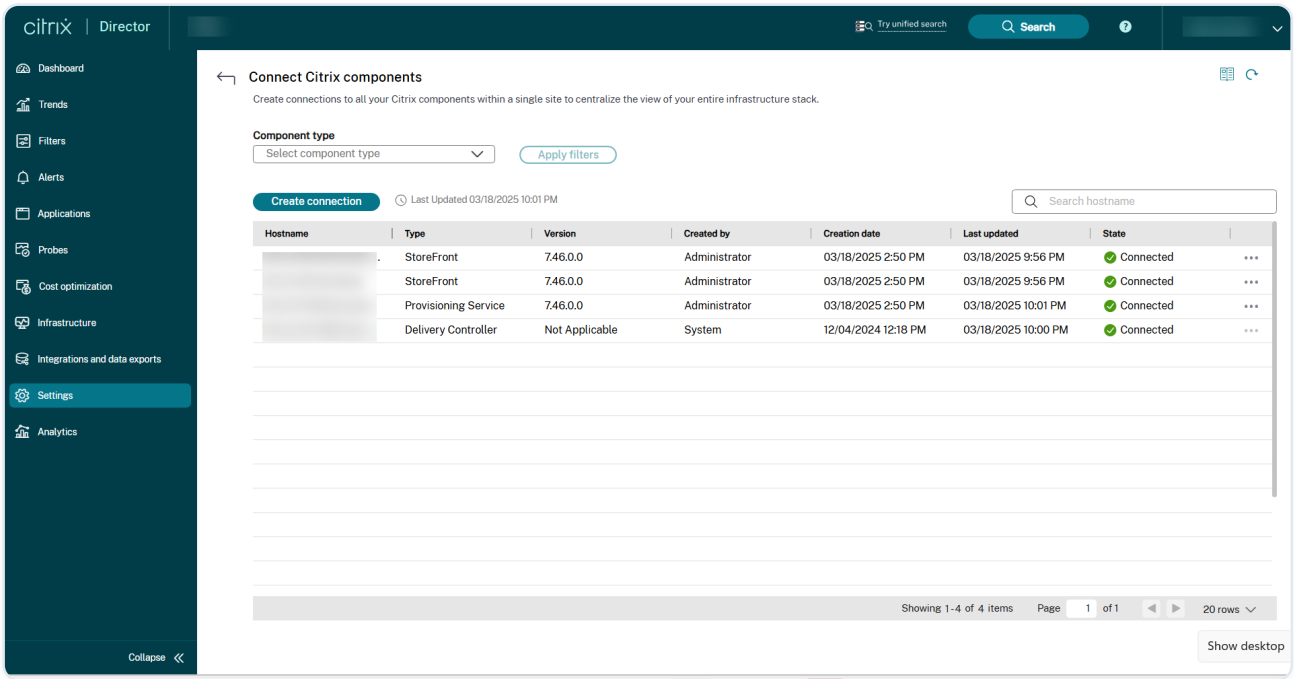
在安装了 Citrix Infrastructure Monitor 的系统中，从 `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` 处的 `RegistrationToken.txt` 文件中获取 Citrix Infrastructure Monitor 令牌。

在 Director UI 中输入获取的令牌详细信息。此令牌授权站点与组件之间的连接。

`RegistrationToken.txt` 文件中存在的令牌文本在您重新启动 Citrix Infrastructure Monitor 服务时会重新生成。注册成功后，令牌文件将从计算机中删除。如果由于任何原因需要重新创建新的令牌文件，请重新启动 Citrix Infrastructure Monitor 服务。出于安全原因，令牌文件在三次使用无效令牌注册失败后会被删除。

步骤 2.4：创建连接

填充详细信息后，单击“**创建**”。创建的连接可在“**连接 Citrix 组件**”页面上的连接列表中找到。



使用远程 PowerShell SDK

先决条件：

- 确保 Citrix 基础结构监视器已安装在 StoreFront 或 PVS 计算机上。

在 DDC 中注册 Citrix 基础结构监视器以与 PVS 或 StoreFront 计算机通信。此注册用于将 PVS 或 StoreFront 计算机上收集的基础结构运行状况指标发送到 DDC。

在 Delivery Controller™ 上运行以下 PowerShell 命令以注册 Citrix 基础结构监视器：

```
Add-MonitorDirectorAgent -Fqdn <FQDN of component> -Component <component>
-Domain <domain> -Username <username> -Password <password> -Token <token>
```

注意：

用户名和密码是可选参数。但是，如果您不提供这些参数，则某些指标将不可用。

上述命令的参数如下：

参数	描述
`Fqdn`	PVS 或 StoreFront 服务器的 FQDN。
`Component`	您正在载入的组件。例如：PVS 或 SF。PVS 代表 Citrix Provisioning™，SF 代表 StoreFront。
`Domain`	所有组件所属的域。
`Username`	管理员用户的用户名。
`Password`	管理员用户的密码。
`Token`	在安装了 Citrix Infrastructure Monitor 的系统中，从 `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` 处的 `RegistrationToken.txt` 文件中获取 Citrix Infrastructure Monitor 令牌。

注意：

- 当您重新启动 Citrix Infrastructure Monitor 服务时，`RegistrationToken.txt` 文件中存在的令牌文本会重新生成。注册成功后，令牌文件将从计算机中删除。如果需要重新注册，请重新启动 Citrix Infrastructure Monitor 服务。
- 出于安全原因，令牌文件在三次无效令牌注册尝试失败后会被删除。

成功注册 PVS 或 StoreFront 计算机后，计算机名称详细信息将显示在“**Director**”>“**基础结构**”选项卡上。

注册 Citrix Infrastructure Monitor 的示例命令如下：

```
Add-MonitorDirectorAgent -Component PVS -Fqdn NX-PVS-
-Domain  -Username  -Password  -Token
```

Citrix 基础架构监视器的自动连接

新的自动连接功能通过自动执行以下步骤来简化入门过程：

- 下载并安装 Citrix 基础架构监视器
- 验证连接

您只需在自动连接中手动添加组件详细信息。手动连接过程保持不变，要求用户下载代理、将其安装到目标计算机并提供必要的详细信息。

为适应此更改，UI 现在具有以下两个选项卡：

- 自动连接
- 手动连接

自动连接过程包含一个复选框，以确保在输入凭据之前满足所有先决条件。

自动连接的目标是使用户的入门过程尽可能顺畅。

先决条件

您可以从 Director UI 远程将 Citrix 基础架构监视器服务安装到计算机上。从 Director UI 进行远程安装需要对 Provisioning Service 和 StoreFront™ 计算机执行以下操作：

- 您必须在将安装 Citrix 基础架构监视器的目标计算机上拥有本地管理员权限。
- 目标计算机上必须提供 WMI。确保您的防火墙允许 WMI。有关更多详细信息，请参阅设置远程 WMI 连接。

- 目标计算机上必须提供 RPC。必须可以从 Delivery Controller™ 计算机访问管理共享（Admin$ 和 C$）。
- 目标计算机必须具有可解析的 DNS 主机名。

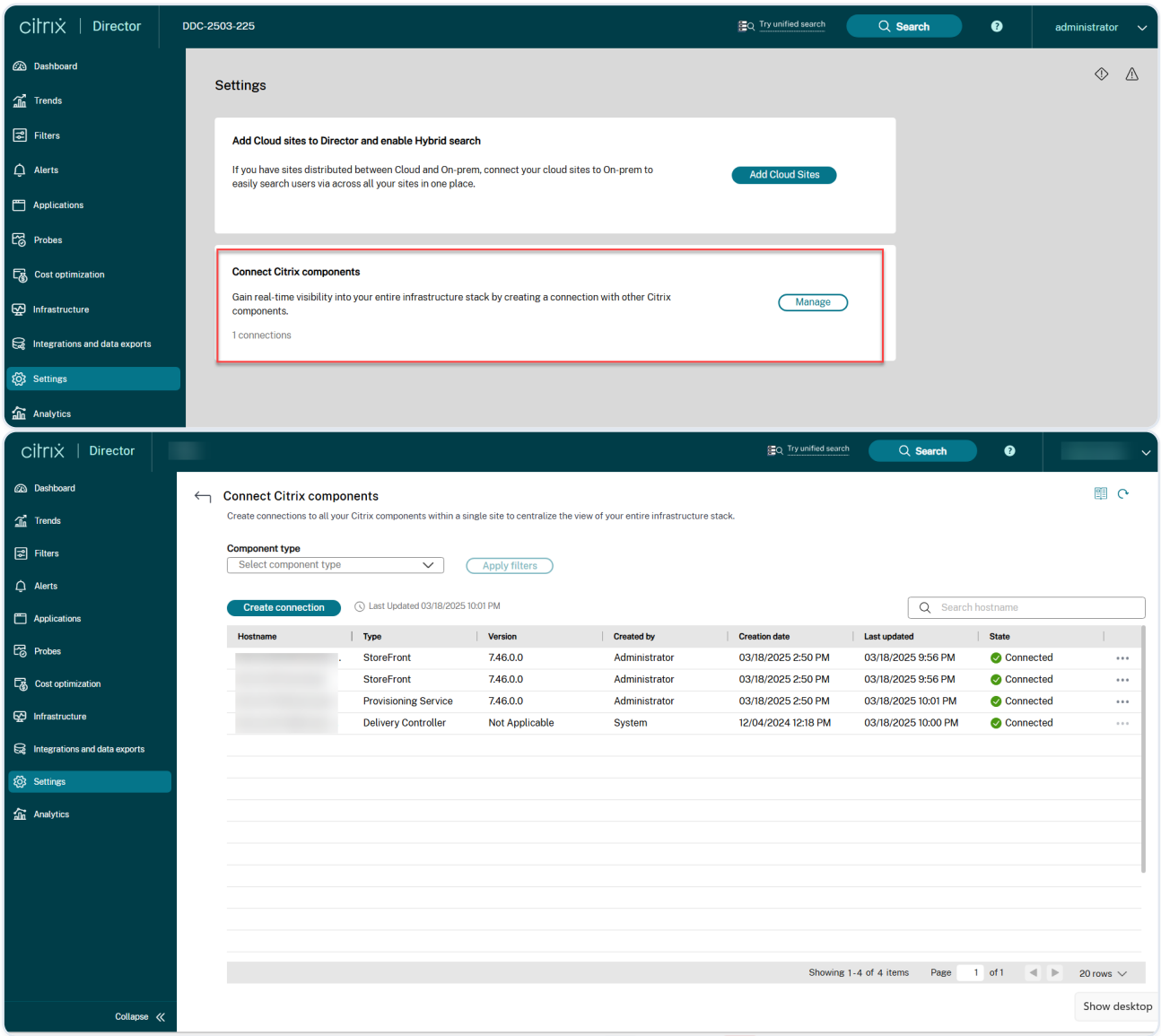
如果您的环境中无法满足这些要求，请参阅手动载入 Citrix Infrastructure Monitor。

自动进行 Citrix Infrastructure Monitor 的注册

您可以使用 Director UI 注册 Citrix Infrastructure Monitor。请按照以下步骤在 Director UI 上完成注册：

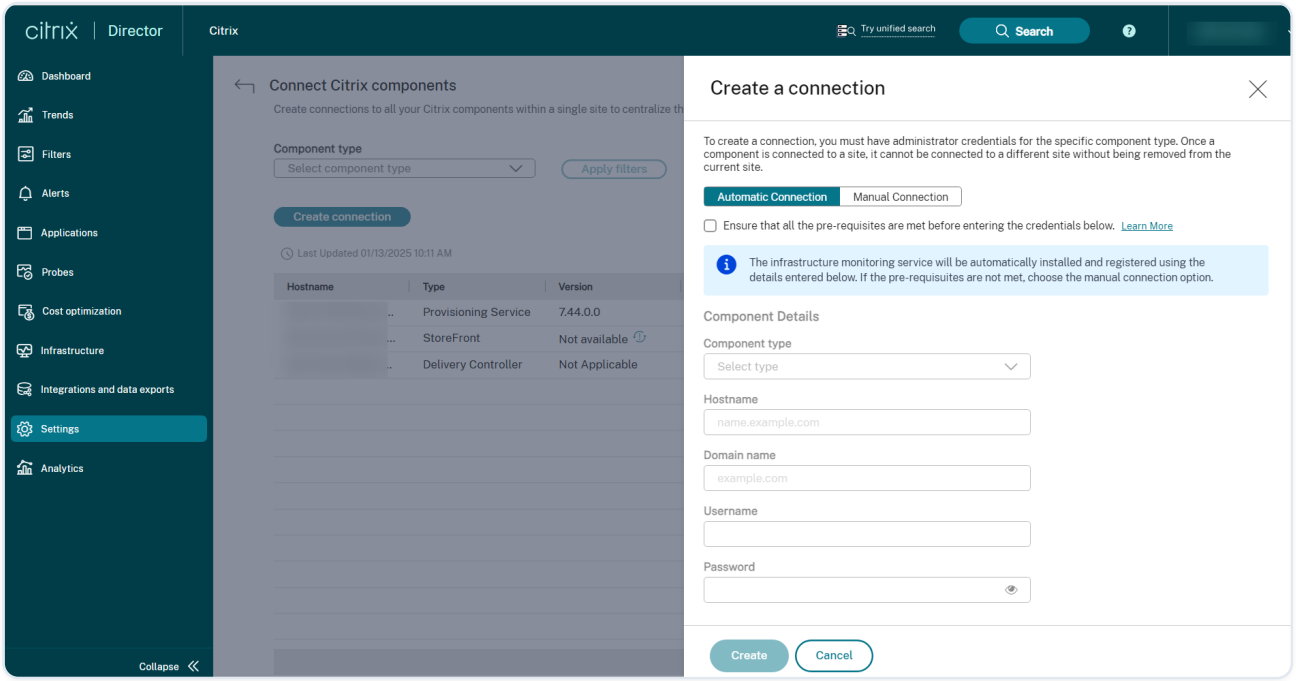
步骤 1：导航到“连接 Citrix 组件”页面

单击“**设置**”>“**连接 Citrix 组件**”>“**管理**”。



步骤 2：输入组件详细信息

在“连接 Citrix 组件”屏幕上，单击“**创建连接**”。将显示“**创建连接**”窗口。“**自动连接**”选项卡默认突出显示。



填写建立安全连接所需的组件详细信息。

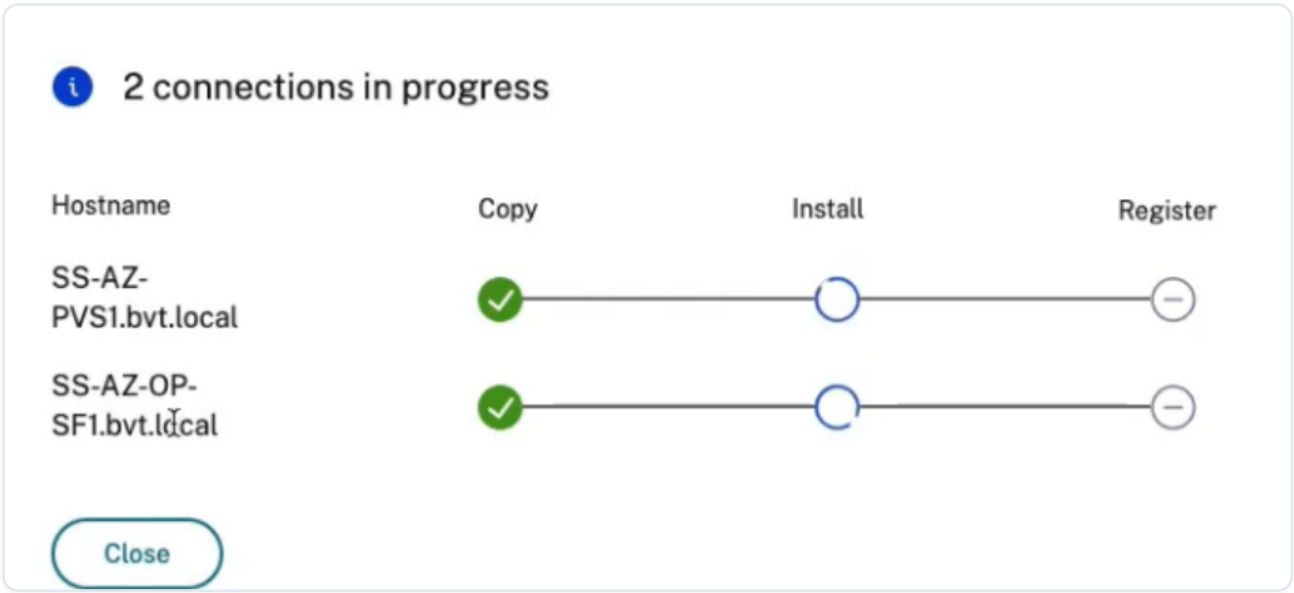
- 从下拉列表中选择组件类型。组件可以是 Provisioning Service 或 StoreFront。
- 输入主机名。
- 输入域名。
- 输入 Provisioning Service 或 StoreFront 计算机的用户名。
- 输入 Provisioning Service 或 StoreFront 计算机的密码。

基础设施监控服务将使用上述详细信息自动安装和注册。

步骤 3：创建连接

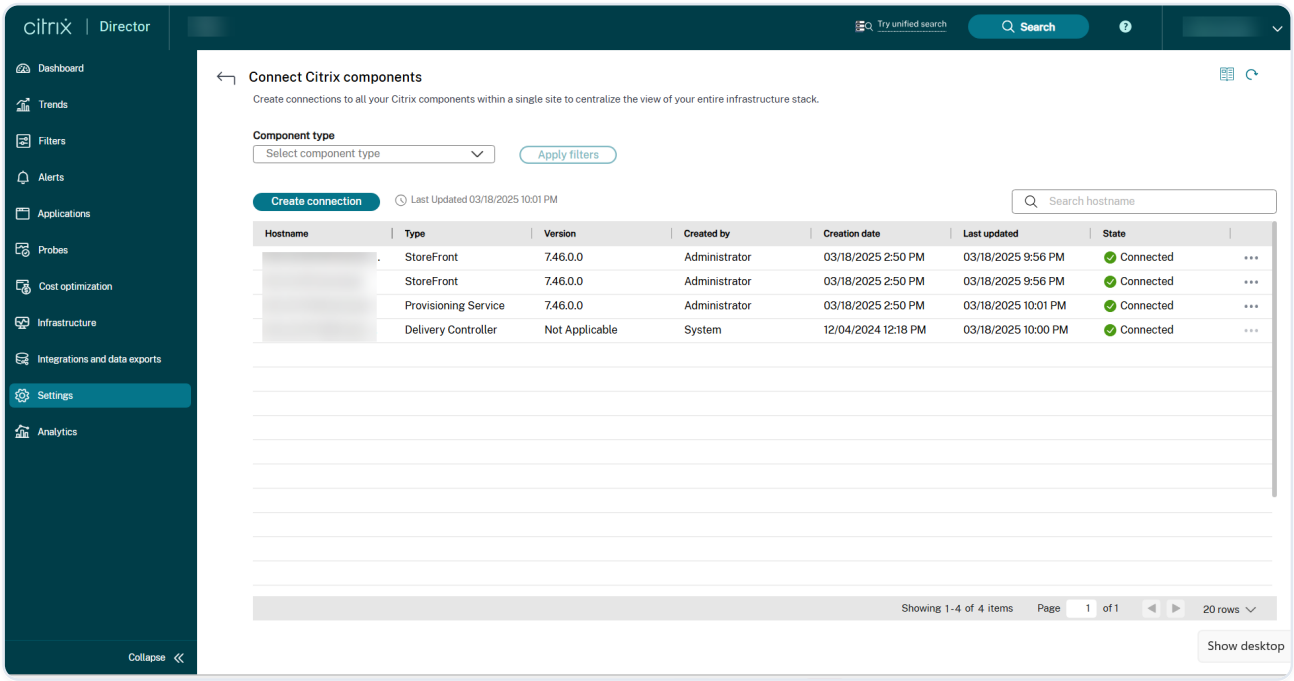
填写完详细信息后，单击“**创建**”。在接受请求之前会执行某些预检查。这些检查会验证是否满足先决条件，然后才能继续。满足先决条件后，自动连接过程会显示一个进度条，指示以下步骤：复制、安装和注册。如果任何步骤失败，用户会看到重试选项。

单击“**查看详细信息**”以查看自动连接过程的详细信息。



MSI 文件将下载并复制到安装位置，然后在此处进行安装和注册。完成后，创建的连接将在“连接 Citrix 组件”页面上的连接列表中可用。

如果连接失败，您可以重试连接。重试需要您提供管理员凭据。



错误处理

系统会执行先决条件预检查，如果任何检查失败，则会显示错误消息。

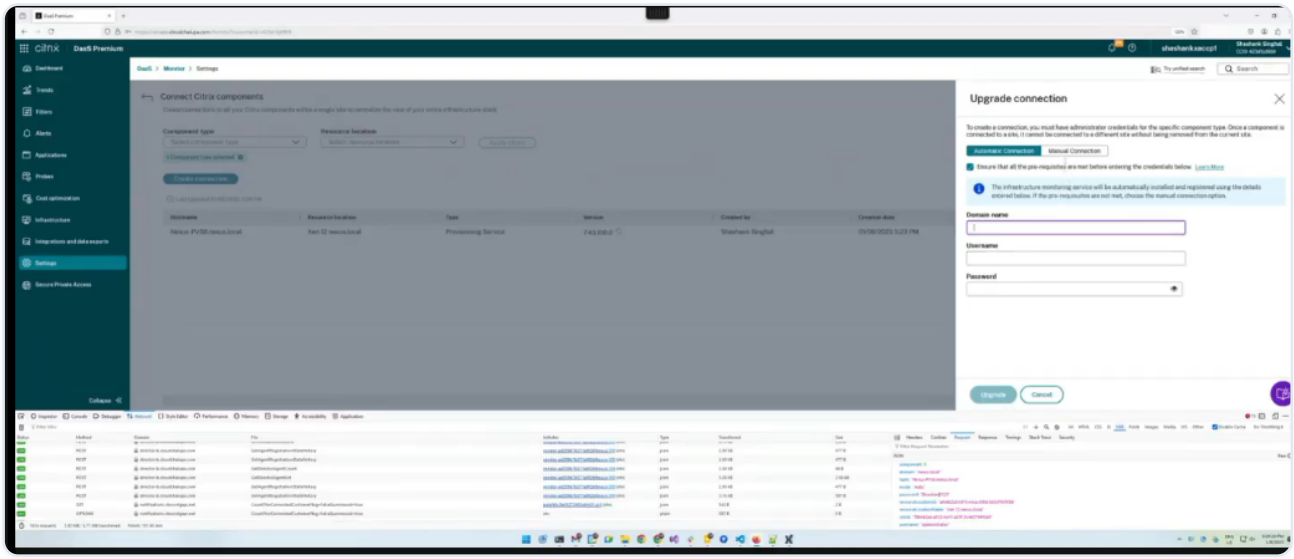
> **注意：**
>
> 预检查按特定顺序进行。例如，要检查 WMI 错误，凭据必须正确。

> 下表显示了错误消息和相应的解决方案：

错误场景	描述
FQDN 格式无效	FQDN 格式无效。要解决此问题，请更正 FQDN 格式。
无法访问的 FQDN	FQDN 计算机无法访问。
凭据无效	您的用户名或密码无效。
远程计算机上未设置 HTTPS。	在远程计算机上未设置用于启用 HTTPS 的环境变量，而监视器配置中已启用 HTTPS。要解决此问题，请在 **系统属性** > **高级** > **环境变量** > **编辑系统变量** 中设置值。
远程计算机上 HTTPS 设置不正确	在远程计算机上设置了用于启用 HTTPS 的环境变量，而监视器配置中已禁用 HTTPS。要解决此问题，请在 **系统属性** > **高级** > **环境变量** > **编辑系统变量** 中删除该值。
远程计算机上阻止了 Windows Management Instrumentation (WMI)。	Windows 防火墙 Defender 中 **允许的应用和功能** 部分中 WMI 的复选框未选中。要解决此问题，请确保 WMI 可以通过防火墙访问。
远程计算机上阻止了 SMB 端口。	必须为来自 Delivery Controller 的入站 TCP 连接启用端口 445。
远程计算机上禁用了管理共享	未满足自动连接的先决条件。

升级过程

如果您使用的是旧版 Citrix Infrastructure Monitor，则可以选择升级。这仅适用于 Provisioning Service 和 StoreFront。自动升级会显示进度条并需要管理员凭据。



您可以选择自动升级或手动升级。

仅当有新版本可用时才会出现升级提示。升级不需要注册。升级后，大约需要 5 分钟才能反映最新版本。

配置 Citrix Infrastructure Monitor 的 HTTPS 步骤

> **注意：**
>
> Citrix Infrastructure Monitor 服务也可以在 HTTP 模式下工作，在这种情况下，不需要以下配置。但是，我们建议您使用 HTTPS 模式。仅当您需要为 Citrix Infrastructure Monitor 配置 HTTPS 时才执行以下步骤。

步骤 1：将证书上传到计算机

1. 获取 `PFX` 证书，用于安装了 Citrix Infrastructure Monitor 的计算机。有关 PFX 文件生成的更多信息，请参阅 如何创建 PFX 文件。

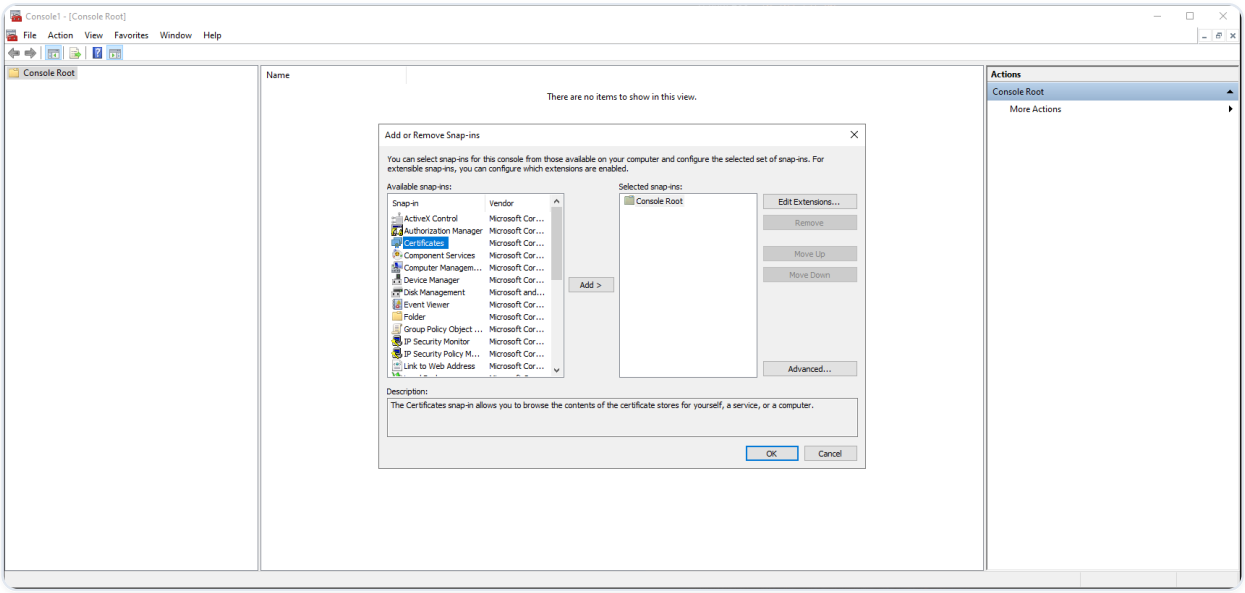
   > **注意：**
   >
   > 您也可以使用受密码保护的 PFX 文件。

2. 将证书上传到计算机上的任意位置。

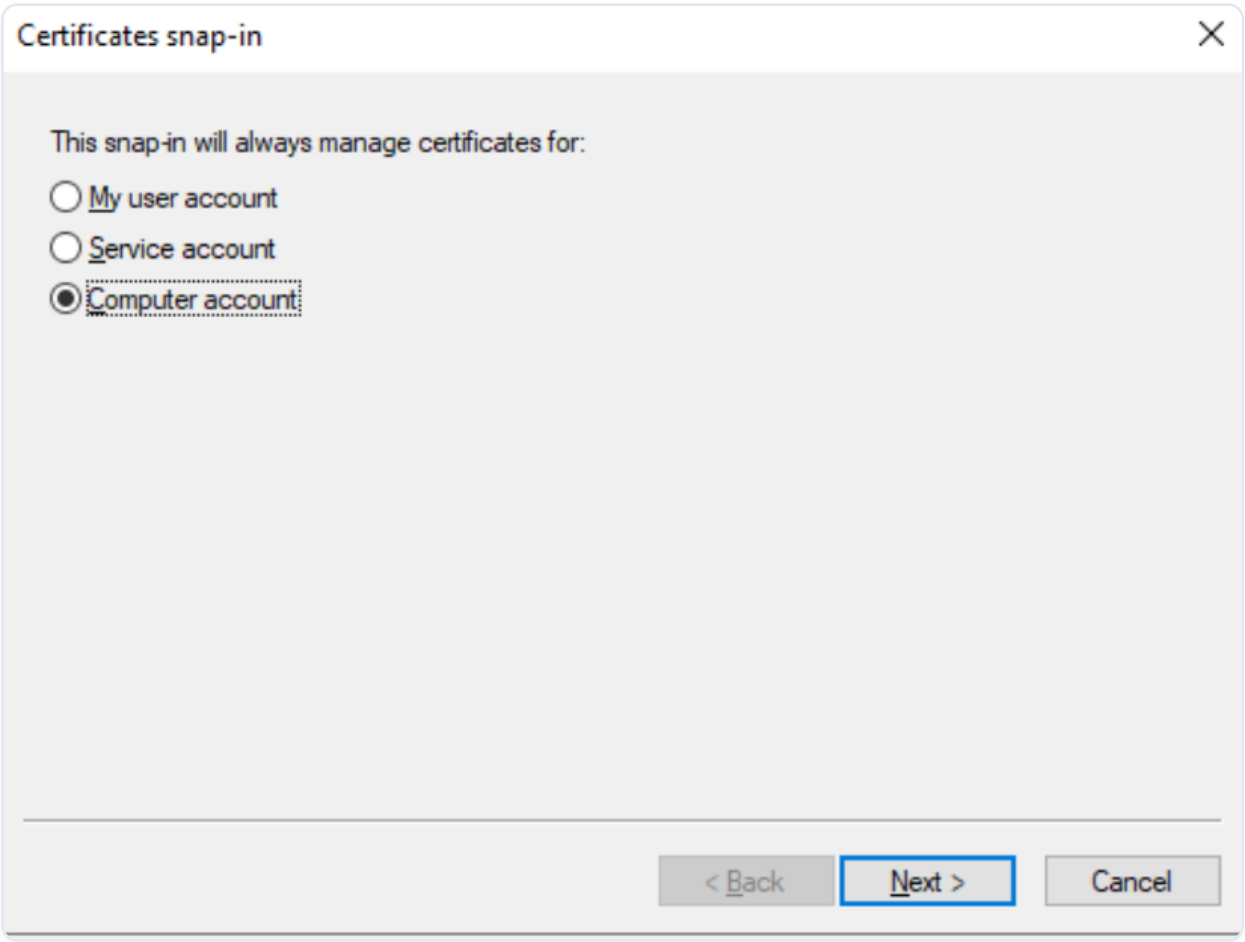
步骤 2：将证书导入计算机证书

1. 单击 **Start** > **Run** > 键入 `mmc`，然后单击 **OK**。将出现 **Console 1 -** 窗口。

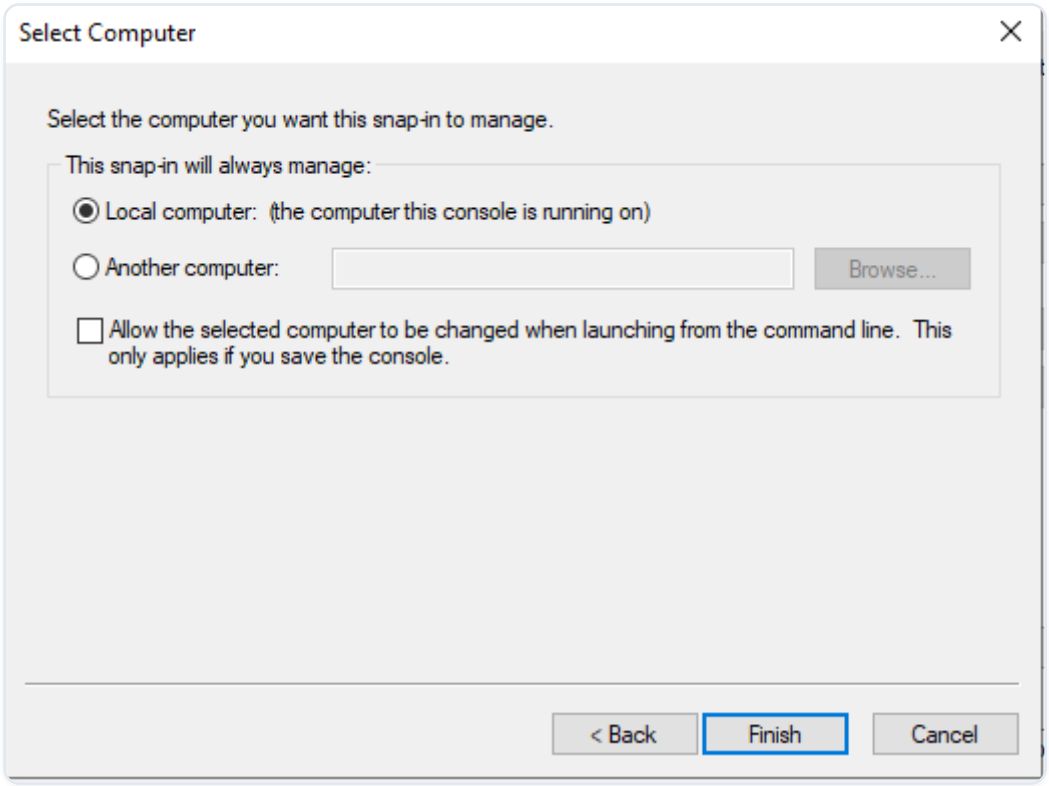
2. 在 **File** 菜单上，单击 **Add/Remove Snap-in**。将出现 **Add or Remove Snap-ins** 窗口。



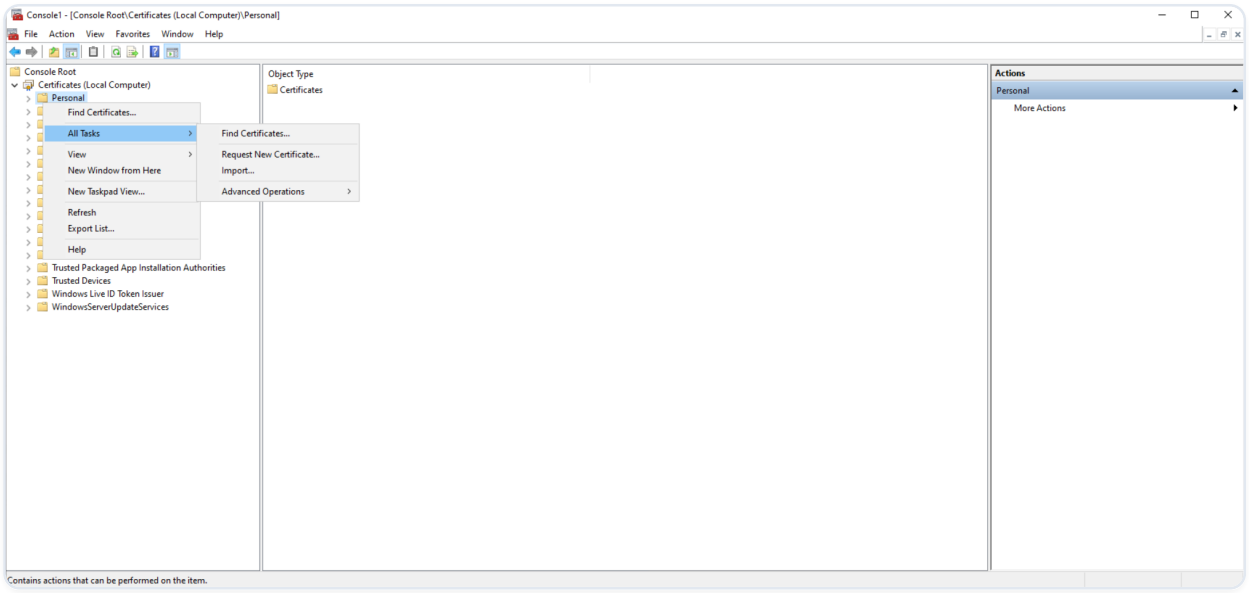
3. 在“**管理单元**”下，双击“**证书**”。此时将显示“**证书管理单元**”窗口。



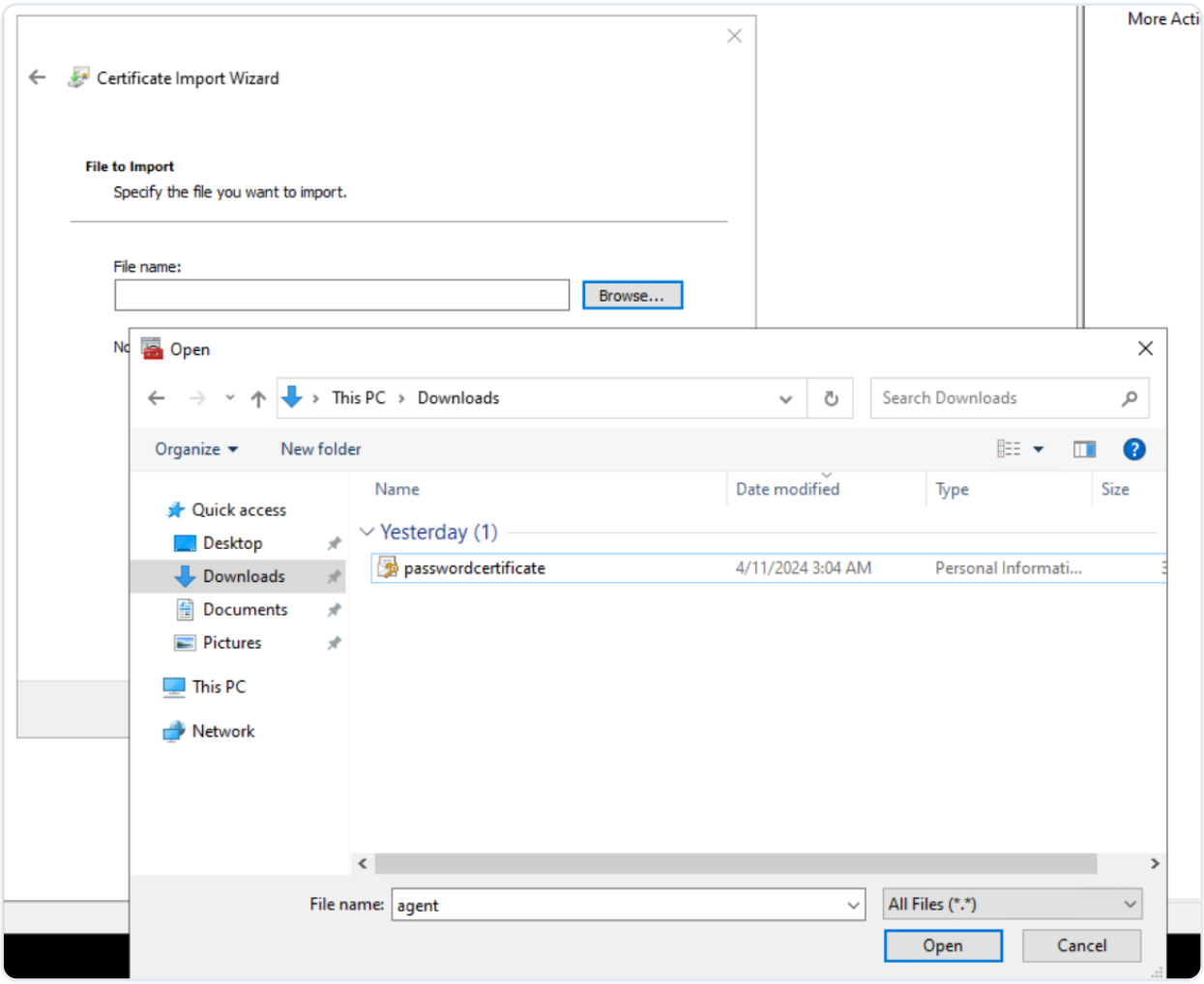
4. 选择“**计算机帐户**”，然后单击“**下一步**”。此时将显示“**选择计算机**”窗口。



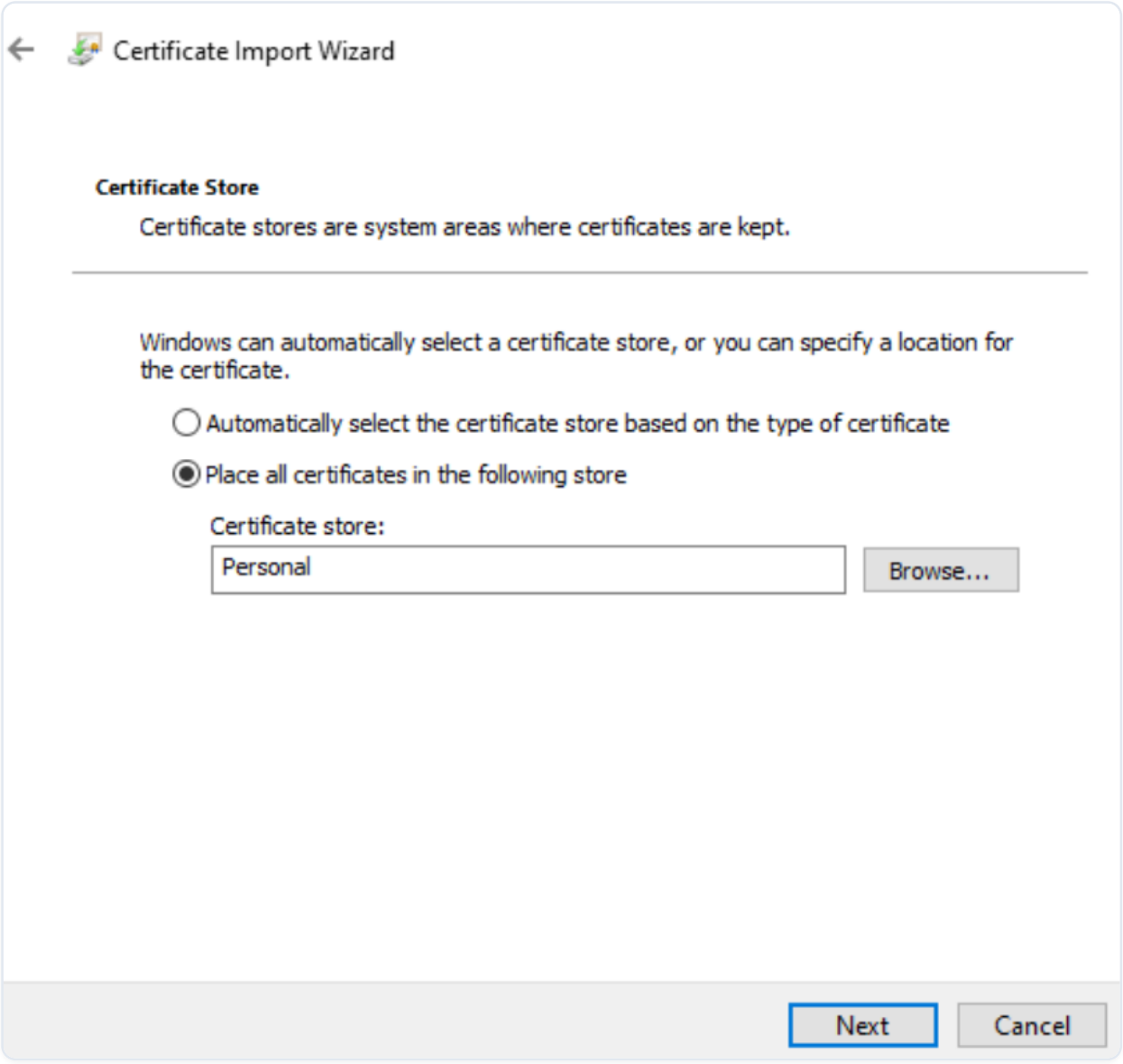
5. 选择“**本地计算机**”。
6. 单击“**完成**”。“**证书(本地计算机)**”部分将显示在新控制台的选定管理单元列表中。
7. 单击 **确定**。
8. 展开“**证书**”，右键单击“**个人**”>“**所有任务**”>“**导入**”。此时将显示“**欢迎使用证书导入向导**”。



9. 选择“**下一步**”>“**浏览文件**”。导航到上传 PFX 文件的位置，将文件类型更改为“**所有文件**”，然后选择相应的 PFX 证书。



10. 输入 PFX 密码。如果没有密码，可以将其留空。
11. 单击**下一步**。
12. 对于证书存储，请确保选中“**将所有证书放入以下存储**”选项，并将“**证书存储**”选择为“**个人**”。



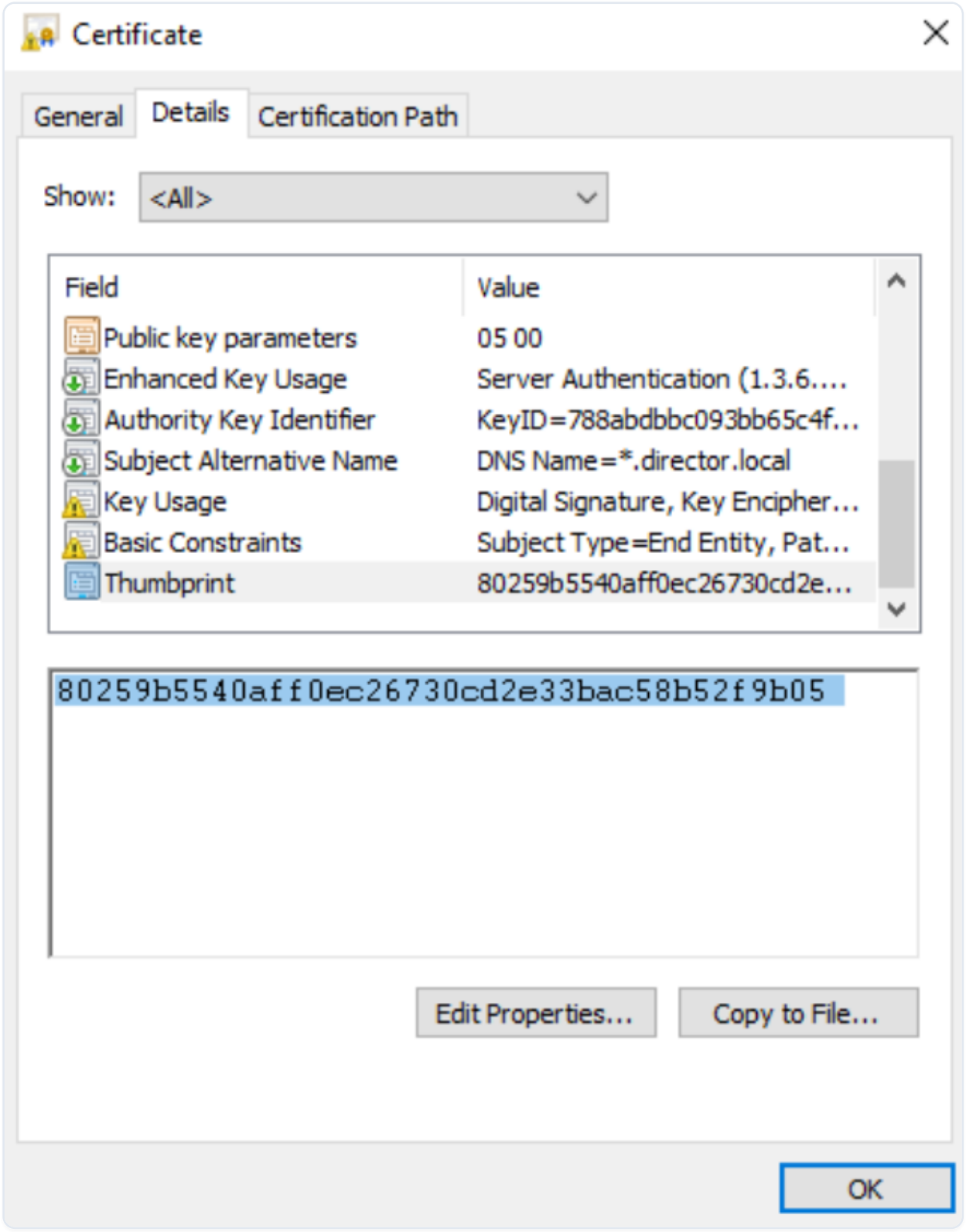
13. 单击**下一步**。
14. 查看详细信息，然后单击**完成**。
15. 等待确认。将显示*导入成功*消息。
16. 导航到**证书** > **个人**，并确保证书存在。
17. 从计算机中删除 PFX 证书文件。

步骤 3：提供证书的读取访问权限

1. 右键单击导入的证书 > **所有任务** > **管理私钥**。
2. 在打开的对话框中，选择**添加**，然后搜索**网络服务**。 单击**确定**。
3. 在**组或用户名**下选择 **NETWORK SERVICE**。
4. 在**NETWORK SERVICE 的权限**下允许*读取*访问权限。
5. 单击 **确定**。

步骤 4：获取指纹

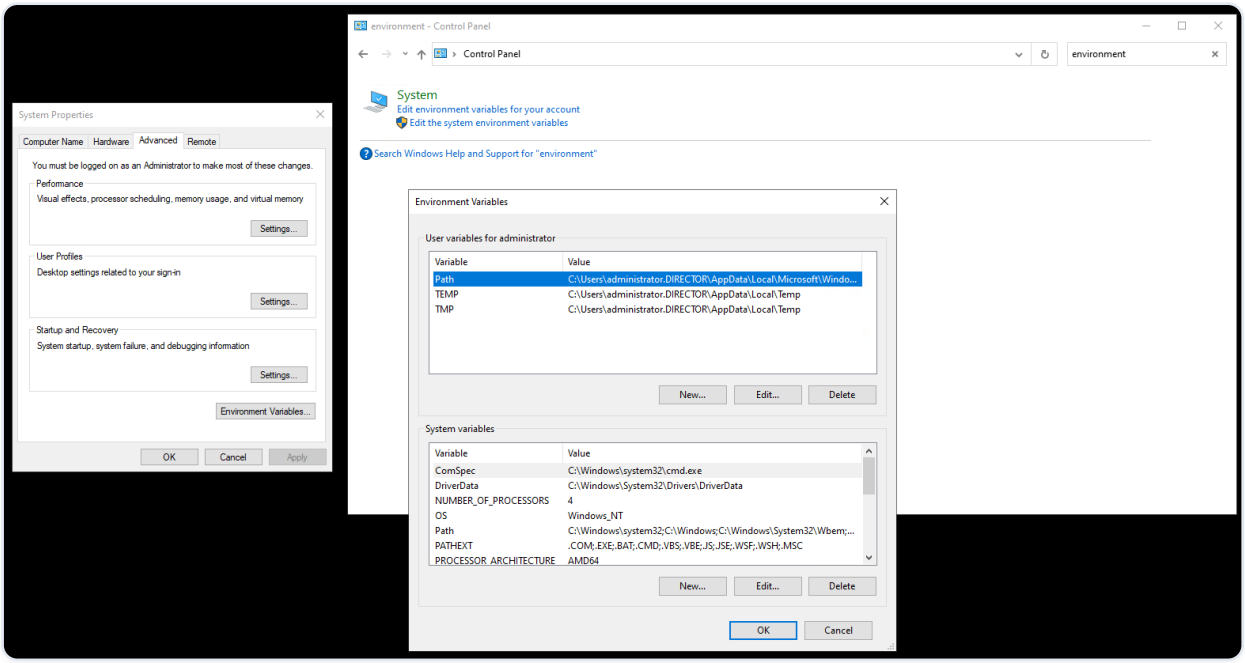
1. 双击导入的证书。
2. 在打开的对话框中，导航到**详细信息**选项卡并滚动到底部。
3. 点击 **指纹**。



4. 复制该值，并为下一步做好准备。

步骤 5：设置环境变量

1. 打开控制面板。
2. 搜索环境变量，然后选择 **编辑系统环境变量**。
3. 在 **系统变量（针对所有用户）** 下，点击 **新建**。



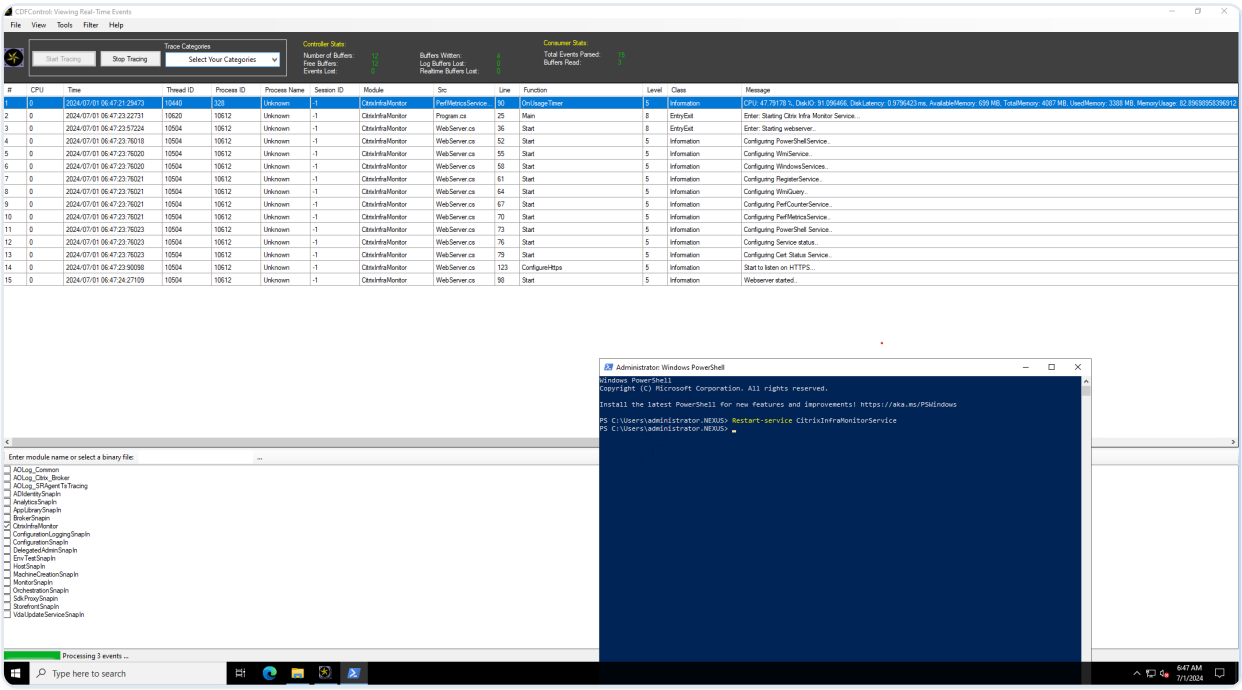
4. 将 **变量** 名称指定为 *DIRECTOR_AGENT_HTTPS_CERTIFICATE_THUMBPRINT*。
5. 在 **变量** 值下指定上一步中的指纹。
6. 单击 **确定**。

步骤 6：重新启动 CitrixInfraMonitorService

1. 打开 PowerShell 并运行以下命令：

```
Restart-Service CitrixInfraMonitorService
```

2. 通过捕获 **CitrixInfraMonitorService** 模块并查找日志行 **Start to listen on HTTPS...**，确保 HTTPS 已启用。



步骤 7: 在 Monitor 配置中启用 HTTPS

在 Delivery Controller™ 计算机上运行以下命令：

```
Set-MonitorConfiguration -DirectorAgentEnableHttps $true
```

管理连接

您可以在**连接 Citrix 组件**页面上查看、删除或编辑连接。

查看连接

您可以查看此视图中所有已连接和已断开连接的组件的详细信息。“**创建连接**”页面的不同列说明如下表所示：

列	说明
主机名	服务器名称。
类型	连接类型。可以是 Delivery Controller™、Provisioning Service 和 StoreFront。
版本	组件上安装的 `CitrixInfraMonitor.msi` 版本。此字段不适用于 Delivery Controller。
创建者	创建连接的人员姓名。

列	说明
创建日期	建立连接的日期。
上次更新	上次更新连接的日期。
状态	不同的状态包括“正在连接”、“已连接”和“已断开连接”。
	正在连接：此状态表示新组件的数据可能需要大约五分钟才能显示，而资源利用率数据可能需要大约 10 分钟才能可用。
	已连接：此状态表示组件与站点之间的连接已建立并正在运行。
	已断开连接：此状态表示组件与站点之间的连接已断开。导致“已断开连接”状态的可能原因包括服务器停机或站点无法连接到 Citrix Infrastructure Monitor。

> **注意：**
>
> 当连接到本地 Citrix Virtual Apps and Desktops™ 站点时，此视图中会自动填充 Delivery Controller 连接。

编辑连接

可能需要编辑连接以更新用于建立 Provisioning Service 或 StoreFront™ 连接的管理员凭据。

要编辑现有连接，请执行以下操作：

1. 从**设置**或**基础结构**选项卡导航到**连接 Citrix 组件**页面。
2. 在连接列表表中，单击感兴趣组件所在行末尾的三个点。
3. 单击“**编辑**”并根据需要更新详细信息。

删除组件

您可以从 Director UI 或使用 PowerShell 命令删除组件。

使用 Director UI

删除组件是从 Director 注销 Provisioning Service 或 StoreFront 连接的过程。注销过程完成后，将停止为所选组件收集新数据。要删除现有连接，请执行以下操作：

1. 从**设置**或**基础结构**选项卡导航到**连接 Citrix 组件**页面。
2. 在连接列表表中，单击感兴趣组件所在行末尾的三个点。
3. 点击 **移除**。连接已注销并从 Director 中移除。

使用 PowerShell SDK

如果您需要注销给定组件，请在 Delivery Controller 上运行以下 PowerShell 命令：

```
Remove-MonitorDirectorAgent -Fqdn <FQDN of component> -Component
<component>
```

删除 Citrix Infrastructure Monitor 注册的示例命令如下：

```
Remove-MonitorDirectorAgent -Component PVS -Fqdn [redacted]
```

> **注意：**
>
> 注销组件只会停止特定组件到 Director 的数据流。如果您需要卸载 Citrix Infrastructure Monitor，请从**控制面板**中卸载。

基础架构控制板

您可以在“**基础架构监控**”页面中查看组件的运行状况值。这些结果有助于主动分析和排查基础架构相关问题。

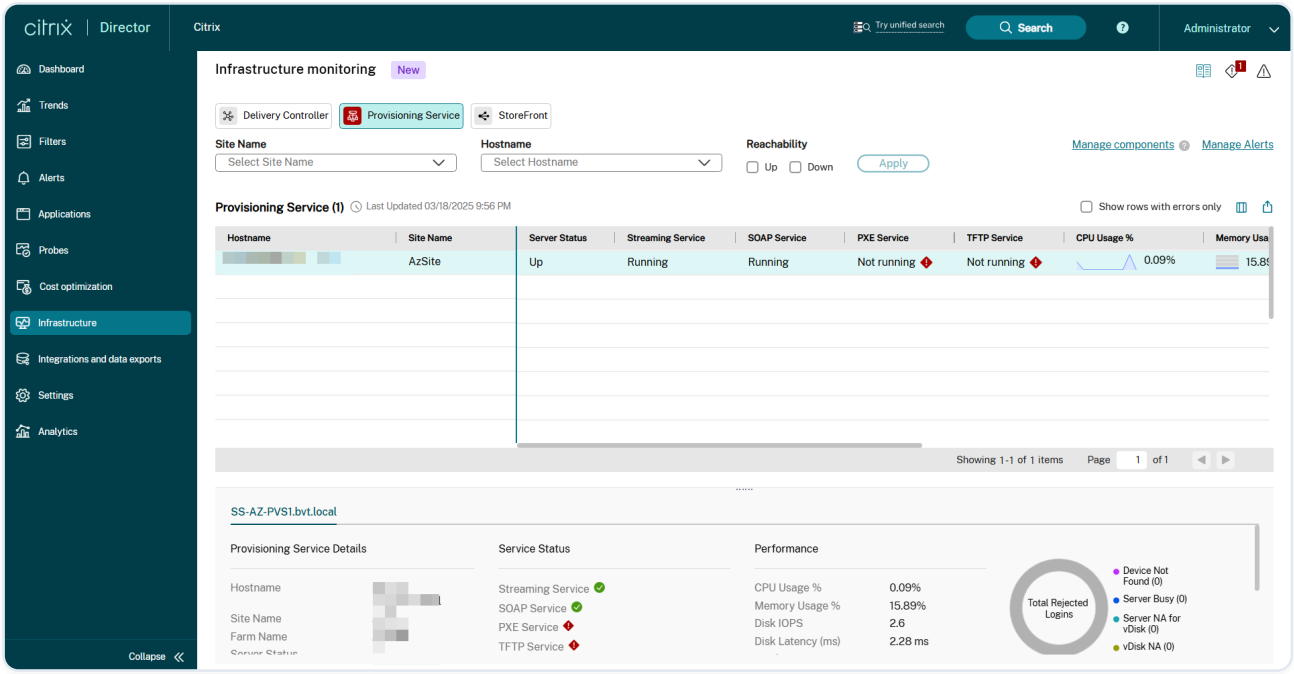
您可以通过以下方式筛选“**基础架构监控**”页面：

- 主机名 - 选择主机名
- 可访问性 - 选中“**正常**”（服务器可访问）或“**关闭**”（服务器不可访问）复选框
- 错误 - 选中“仅显示有错误的行”复选框。

使用“**管理列**”选项选择要在控制板中显示的数据。

Provisioning Service 运行状况指标

单击“**基础架构**”选项卡，然后选择“**Provisioning Service**”。Provisioning Service 的基础架构控制板随即显示：



将监控 Provisioning Service 服务器的以下详细信息：

类别	指标	描述
可访问性	主机名	安装了 Citrix Infrastructure Monitor 的 Provisioning Service 计算机的名称。此指标是一个字符串值。
	Provisioning Service 站点名称	Provisioning Service 站点的名称。此指标是一个字符串值。
	预配服务场名称	Provisioning Service 场的名称。此指标是一个字符串值。
	预配服务站点 ID	显示 Provisioning Service 服务器的站点 ID。此指标是一个字符串值。
	预配服务场 ID	显示 Provisioning Service 服务器的场 ID。此指标是一个字符串值。

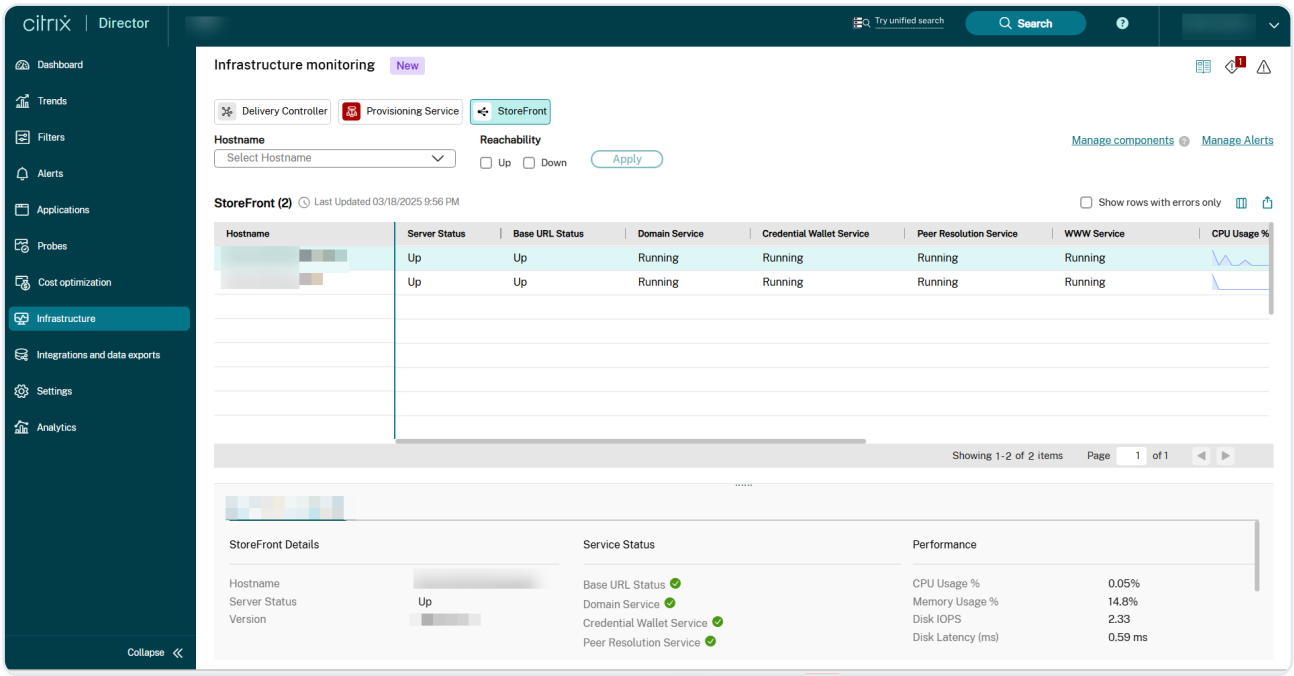
类别	指标	描述
	服务器状态	显示给定服务器的可达性状态。可能的值为 *Up*、*Down* 和 *Unknown*。
	上次启动时间	显示 Provisioning Service 服务器上次启动的时间。
	上次更新时间	显示从 Provisioning Service 服务器收集数据的时间。
依赖服务	流服务	显示流服务的状态。此指标显示 Windows 服务的状态。可能的值为：*未运行*、*正在运行*、*未安装* 和 *不适用*（带帮助图标）。
	SOAP 服务	显示简单对象访问协议 (SOAP) 服务的状态。此指标显示 Windows 服务的状态。可能的值为：*未运行*、*正在运行*、*未安装* 和 *不适用*（带帮助图标）。
	数据库连接	显示数据库连接状态。如果您使用的是 Citrix Provisioning 服务器版本 2402 或更早版本，可能会出现未知错误。可能的值为 *未连接*、*已连接*、*未知* 和 *不适用*（带帮助图标）。
	许可证服务器可达性	显示许可证服务器是否可达。如果您使用的是 Citrix Provisioning 服务器版本 2402 或更早版本，可能会出现未知错误。可能的值为 *未连接*、*已连接*、*未知* 和 *不适用*（带帮助图标）。
	总重新连接计数	显示会话重新连接的次数。

类别	指标	描述
	PXE 服务	显示预启动执行环境服务的状态。此指标显示 Windows 服务的状态。可能的值为：*未运行*、*正在运行*、*未安装* 和 *不适用*（带帮助图标）。
	TFTP 服务	显示普通文件传输协议服务的状态。此指标显示 Windows 服务的状态。可能的值为：*未运行*、*正在运行*、*未安装* 和 *不适用*（带帮助图标）。
资源利用率	CPU 使用率 %	使用折线图显示 CPU 使用率（百分比）。显示的值是过去 5 分钟结束时的最新值。
	平均 CPU %	显示 Provisioning Service 服务器在过去 10 分钟内的平均 CPU 百分比。
	峰值 CPU %	显示 Provisioning Service 服务器在过去 5 分钟内的峰值 CPU 百分比。
	内存使用率 %	使用堆栈图显示内存使用百分比。显示的值是过去 5 分钟结束时的最新值。
	平均内存 %	显示过去 10 分钟内 Provisioning Service 服务器的平均内存百分比。
	峰值内存 %	显示过去 5 分钟内 Provisioning Service 服务器的峰值内存百分比。
	磁盘 IOPS	使用折线图显示磁盘的输入和输出值。

类别	指标	描述
	平均磁盘 IOPS 百分比	显示过去 10 分钟内 Provisioning Service 服务器的平均磁盘 IOPS。
	峰值磁盘 IOPS %	显示 Provisioning Service 服务器在过去 10 分钟内的峰值磁盘 IOPS 百分比。
	磁盘延迟 (毫秒)	使用折线图显示磁盘的延迟值。
	平均磁盘延迟百分比	显示 Provisioning Service 服务器在过去 10 分钟内聚合的平均磁盘延迟。
	峰值磁盘延迟 %	显示 Provisioning Service 服务器在过去 5 分钟内的峰值磁盘延迟百分比。
影响	总计拒绝登录	总失败登录次数除以总登录尝试次数。
	活动设备计数	显示 Provisioning Service 服务器中活动设备的总数。此指标是一个整数值。

StoreFront™ 运行状况指标

单击“**基础结构**”选项卡，然后选择“**StoreFront**”。StoreFront 的基础结构控制板随即显示：



针对 StoreFront 服务器监视以下详细信息：

类别	指标	描述
可达性	主机名	显示 StoreFront 服务器的名称。此指标是一个字符串值。
	服务器状态	显示 StoreFront 服务器的状态。此指标显示 Windows 服务状态。可能的值为：*未运行*、*正在运行*、*未安装* 和 *不适用*（带帮助图标）。
	基本 URL 状态	显示基本 URL 的运行状况。如果 HTTP 状态代码为 200，则状态为“正常”。否则，值为“异常”。
	上次启动时间	显示 StoreFront 服务器上次启动的时间。
	上次更新时间	显示从 StoreFront 服务器收集数据的时间。
依赖服务	域服务	名为域服务的 Windows 服务的运行状况。此指标显示 Windows 服务的状态。可能的值为：*未运行*、*正在运行*、

类别	指标	描述
		*未安装*和*不适用*（带帮助图标）。
	凭据钱包服务	此服务是一个 Windows 服务，用于存储加密密码。可能的值为：*未运行*、*正在运行*、*未安装*和*不适用*（带帮助图标）。
	对等解析服务	此服务是一个 Windows 服务，负责服务器组间的网络通信，形成 StoreFront 服务器的对等网格。可能的值包括：*未运行*、*正在运行*、*未安装*和 *不适用*（带帮助图标）。
	WWW 服务	此指标是 StoreFront 服务器的 Web 服务。此指标显示 Windows 服务的状态。可能的值包括：*未运行*、*正在运行*、*未安装* 和 *不适用*（带帮助图标）。
资源利用率	CPU 使用率 %	使用折线图显示 CPU 使用率百分比。显示的值是过去五分钟结束时的最新值。
	平均 CPU %	显示 StoreFront 服务器在过去 10 分钟内的平均 CPU 百分比。
	峰值 CPU %	显示 StoreFront 服务器在过去五分钟内的峰值 CPU 百分比。此值有助于确定 CPU 所需的最大容量。
	内存使用率 %	使用堆叠图以百分比形式显示内存使用情况。显示的值是过去 5 分钟结束时的最新值。

类别	指标	描述
	平均内存 %	显示 StoreFront 服务器在过去 10 分钟内聚合的平均内存百分比。
	峰值内存 %	显示 StoreFront 服务器在过去 5 分钟内的峰值内存百分比。
	磁盘 IOPS	使用折线图显示磁盘的输入和输出值。
	平均磁盘 IOPS 百分比	使用浮点数显示 StoreFront 服务器的平均磁盘 IOPS。
	峰值磁盘 IOPS %	显示 StoreFront 服务器在过去 10 分钟内聚合的峰值磁盘 IOPS 百分比。
	磁盘延迟 (毫秒)	使用折线图显示磁盘的延迟值。
	平均磁盘延迟百分比	显示 StoreFront 服务器在过去 10 分钟内聚合的平均磁盘延迟。
	峰值磁盘延迟 %	显示 StoreFront 服务器在过去五分钟内的峰值磁盘延迟百分比。
影响	ICA® 证书有效期	显示 ICA 证书的有效性。可能的值为 *已过期*、*即将过期*、*有效* 和 *未找到*。
	ICA 证书链有效性	显示 StoreFront ICA 证书链是否有效。可能的值为 “*是*” 或 “*否*”。
	IIS 证书有效性	显示 IIS 证书的有效性。可能的值为 “*已过期*”、“*即将过期*”、“*有效*” 和 “*未找到*”。

类别	指标	描述
	IIS 证书链有效性	显示 StoreFront IIS 证书链是否有效。可能的值为 *“是”* 或 *“否”*。

Delivery Controller™ 运行状况指标

Delivery Controller 组件默认作为基础结构监视的一部分添加。连接到 Citrix Virtual Apps and Desktops™ 站点的 Delivery Controller 组件会自动载入以进行监视。

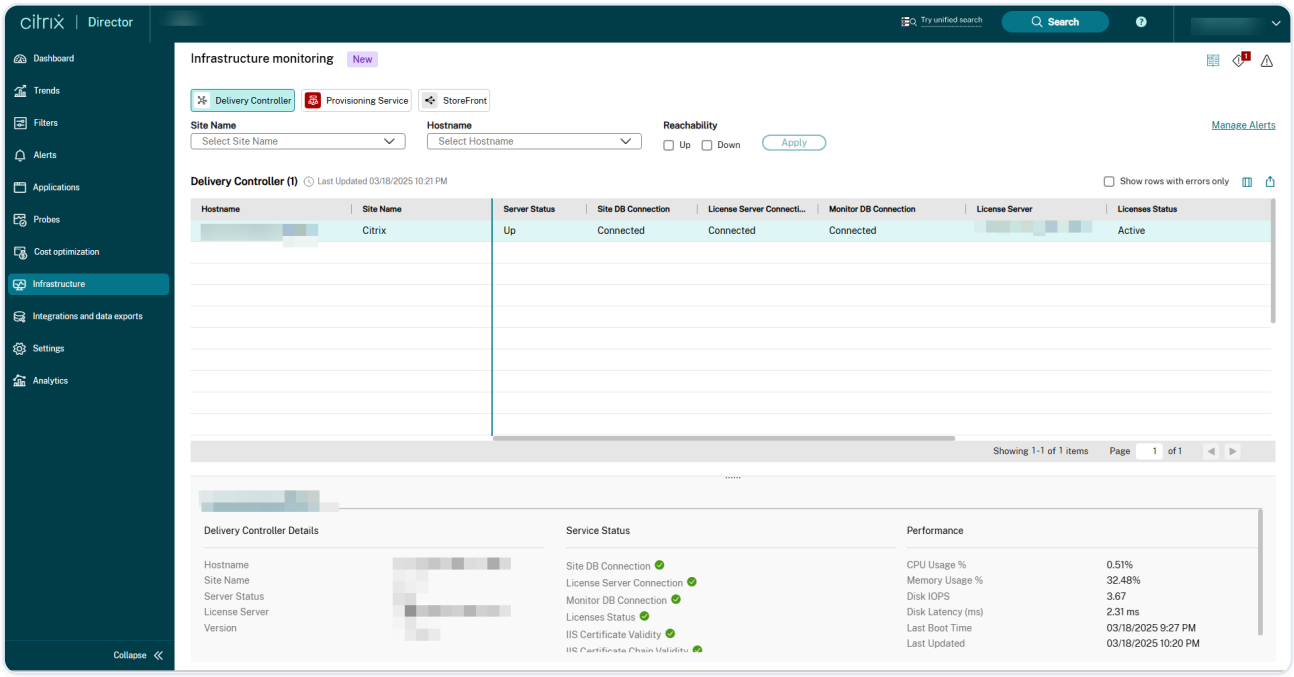
此功能使客户能够在基础结构监视控制板下监视控制器的运行状况并为其配置警报。警报功能使客户管理员能够在为交付控制器创建的任何策略处于严重或警告阶段时收到警报。

您可以选择所需的站点名称，详细信息将根据所选站点名称显示。您还可以选择**可达性状态**，例如 *正常*或 *关闭*。

注意： 监视 Delivery Controller 不需要 `CitrixInfraMonitor.msi` 文件。

您可以监控基础设施详细信息的单站点和多站点详细信息。

单击**基础结构**选项卡，然后选择 **Delivery Controller**。Delivery Controller 的基础结构控制板随即显示：



针对 Delivery Controller 监视以下详细信息：

类别	指标	描述
可达性	服务器状态	显示给定 Delivery Controller 的可达性状态。可能的值为*正常*和*关闭*。
	版本	交付控制器的版本。
	上次启动时间	显示 Delivery Controller 上次启动的时间。
	上次更新时间	显示从 Delivery Controller 收集数据的时间。
依赖服务	站点数据库连接	显示站点数据库连接的状态。可能的值为 *Not Connected*（未连接）、*Connected*（已连接）、*Unknown*（未知）和 *n/a*（不适用，带帮助图标）。**Unknown**：当未收集到指标或指标不可用时，将显示此值。**n/a**：不适用。当服务器状态为关闭时，将显示此值。
	许可证服务器连接	显示许可证服务器连接的状态。可能的值为 *Not Connected*（未连接）、*Connected*（已连接）、*Unknown*（未知）和 *n/a*（不适用，带帮助图标）。
	监视器数据库连接	显示监视器数据库连接的状态。可能的值为 *Not Connected*（未连接）、*Connected*（已连接）、*Unknown*（未知）和 *n/a*（不适用，带帮助图标）。
	许可证服务器	显示许可证服务器是否可访问。
	许可证状态	显示许可证的状态。

类别	指标	描述
资源利用率	CPU 使用率 %	使用折线图显示 CPU 使用率（百分比）。显示的值是过去 5 分钟结束时的最新值。
	平均 CPU %	显示 Delivery Controller 服务器在过去 10 分钟内的平均 CPU 百分比。
	峰值 CPU %	显示 Delivery Controller 服务器在过去 5 分钟内的峰值 CPU 百分比。
	内存使用率 %	使用堆栈图显示内存使用百分比。显示的值是过去 5 分钟结束时的最新值。
	平均内存 %	显示过去 10 分钟内聚合的 Delivery Controller 服务器的平均内存百分比。
	峰值内存 %	显示过去 5 分钟内 Delivery Controller 服务器的峰值内存百分比。
	磁盘 IOPS	使用折线图显示磁盘的输入和输出值。
	平均磁盘 IOPS 百分比	显示过去 10 分钟内聚合的 Delivery Controller 服务器的平均磁盘 IOPS。
	峰值磁盘 IOPS %	显示过去 10 分钟内 Delivery Controller 服务器的峰值磁盘 IOPS 百分比。
	磁盘延迟 (毫秒)	使用折线图显示磁盘的延迟值。
	平均磁盘延迟百分比	显示过去 10 分钟内聚合的 Delivery Controller 服务器的平均磁盘延迟。

类别	指标	描述
	峰值磁盘延迟 %	显示过去 5 分钟内 Delivery Controller 服务器的峰值磁盘延迟百分比。
影响	IIS 证书有效性	显示 IIS 证书的有效性。可能的值为 *“已过期”*、*“即将过期”*、*“有效”* 和 *“未找到”*。
	IIS 证书链有效性	显示 StoreFront IIS 证书链是否有效。可能的值为 *是* 或 *否*。

创建和管理警报

您可以设置警报，主动监控您感兴趣的条件和范围，并减少警报疲劳。警报可以配置严重性、重新警报间隔、通知媒介，并遵循产品中支持的警报生命周期。您可以从“**高级警报策略**”部分创建与基础结构相关的警报。

有关详细信息，请参阅“高级警报策略”(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/site-analytics/alerts-notifications.html#advanced-alert-policies) 页面。

应用程序和桌面探测

应用程序和桌面探测自动化了通过 StoreFront 串行测试启动站点中发布的应用程序和桌面来检查其运行状况的过程。探测结果可在 Director 中查看。

要求

- Delivery Controller 运行版本 7.18 或更高版本用于应用程序探测，运行版本 1906 或更高版本用于桌面探测。
- 运行探测代理的端点计算机是 Windows 计算机，其中安装了适用于应用程序探测的 Citrix Workspace™ app for Windows 1808 或更高版本，以及适用于桌面探测的 1906 或更高版本。不支持适用于统一 Windows 平台 (UWP) 的 Workspace 应用程序。
- Citrix Probe Agent 支持通过 StoreFront 和 Citrix Workspace 使用 Active Directory 凭据进行身份验证。如果端点设备通过 Citrix Gateway 连接到 StoreFront / Workspace，则可以使用 Citrix Gateway 域凭据或多重身份验证 (MFA) 进行身份验证。Citrix Probe Agent 不支持其他身份验证方法，例如单点登录 (SSO)。

> **注意：**
>
> - 如果用户在 Citrix Cloud™ 上启用了登录策略或条件身份验证，探测代理将无法登录 Storefront 或 Citrix Workspace 应用程序。
> - 探测代理仅支持 Active Directory 身份验证来对 Citrix Workspace app 进行身份验证。

- Citrix Probe Agent 仅在未部署代理服务器或负载均衡器（如 Citrix Gateway 或 Citrix ADC）时才起作用。
- 确保要在安装探测代理的端点计算机上安装 Microsoft .NET Framework 4.7.2 或更高版本。

运行探测所需的用户帐户或权限：

- 在每台端点计算机上用于探测的唯一 StoreFront 用户。StoreFront 用户无需是管理员；探测可以在非管理员上下文中运行。
- 具有 Windows 管理员权限的用户帐户，用于在端点计算机上安装和配置 Citrix Probe Agent。
- 用户必须是与用于应用程序或桌面启动的 VDA 相同的域的成员。探测代理目前不支持多个域。
- 重新使用现有用户帐户进行探测可能会导致用户从其活动会话中注销。具有以下权限的完整管理员用户帐户或自定义角色：
  - 交付组权限：
    - 只读
  - Director 权限：
    - 创建\\编辑\\删除警报电子邮件服务器配置 - 如果电子邮件服务器尚未配置
    - 创建\\编辑\\删除探测配置
    - 查看配置页面
    - 查看趋势页面

配置

您可以安排探测在非高峰时段跨多个地理区域运行。全面的探测结果有助于在用户遇到问题之前，排查与应用程序、托管计算机或连接相关的问题。

Citrix Probe Agent 2103 及更高版本支持站点聚合。配置 Citrix Probe Agent 时，选择“Workspace (StoreFront) 站点聚合已启用”选项以启用聚合站点中的应用程序和桌面枚举。支持以下站点组合：

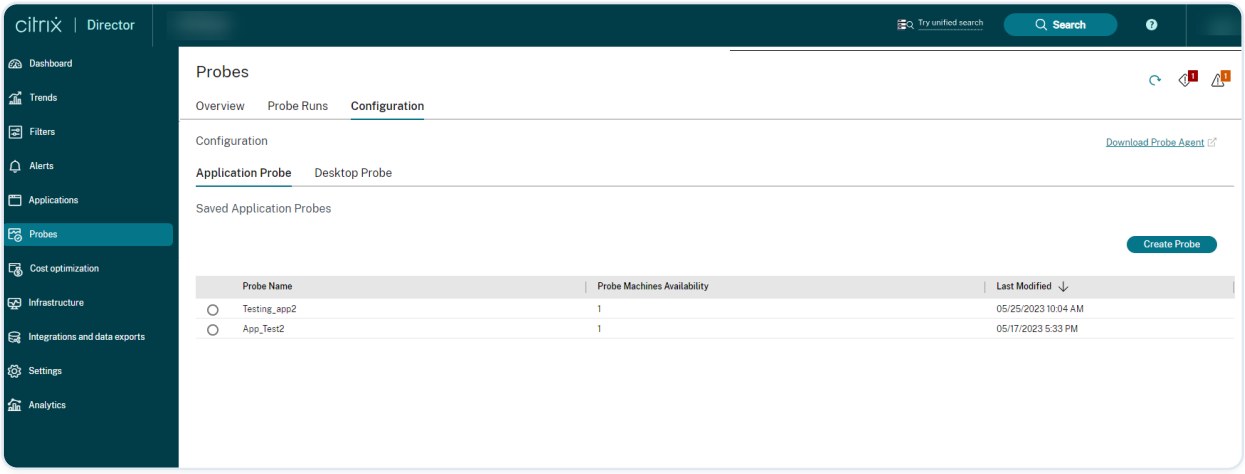
- 具有一个 StoreFront URL 的多个本地站点。
- 具有 StoreFront 或 Workspace URL 的本地和云站点。
- 具有一个 Workspace URL 的多个云站点。
- 通过 Citrix Gateway 连接到 StoreFront 或 Workspace 的本地站点。

> **注意：**
>
> 您必须创建单独的管理员或用户来配置只能访问一个站点的探测。

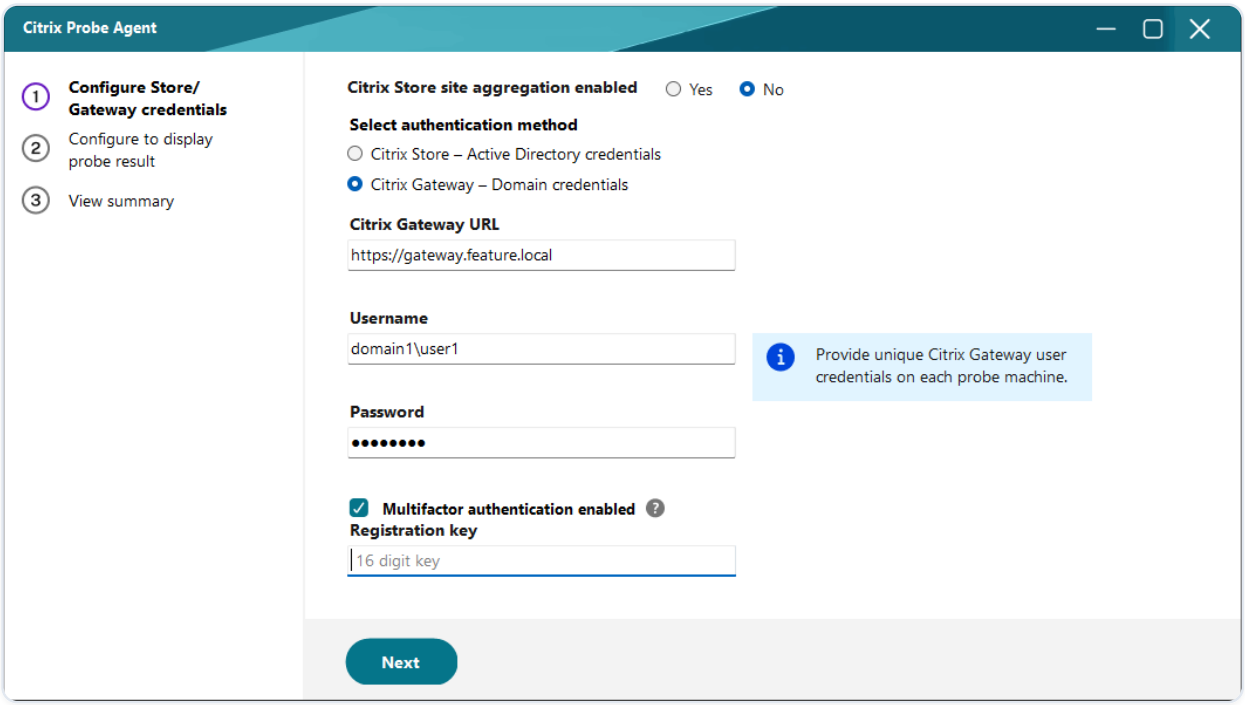
步骤 1：安装和配置 Citrix Probe Agent

Citrix Probe Agent 是一个 Windows 可执行文件，它模拟用户通过 StoreFront 实际启动应用程序或桌面的过程。它根据 Director 中的配置测试启动，并将结果报告给 Director。

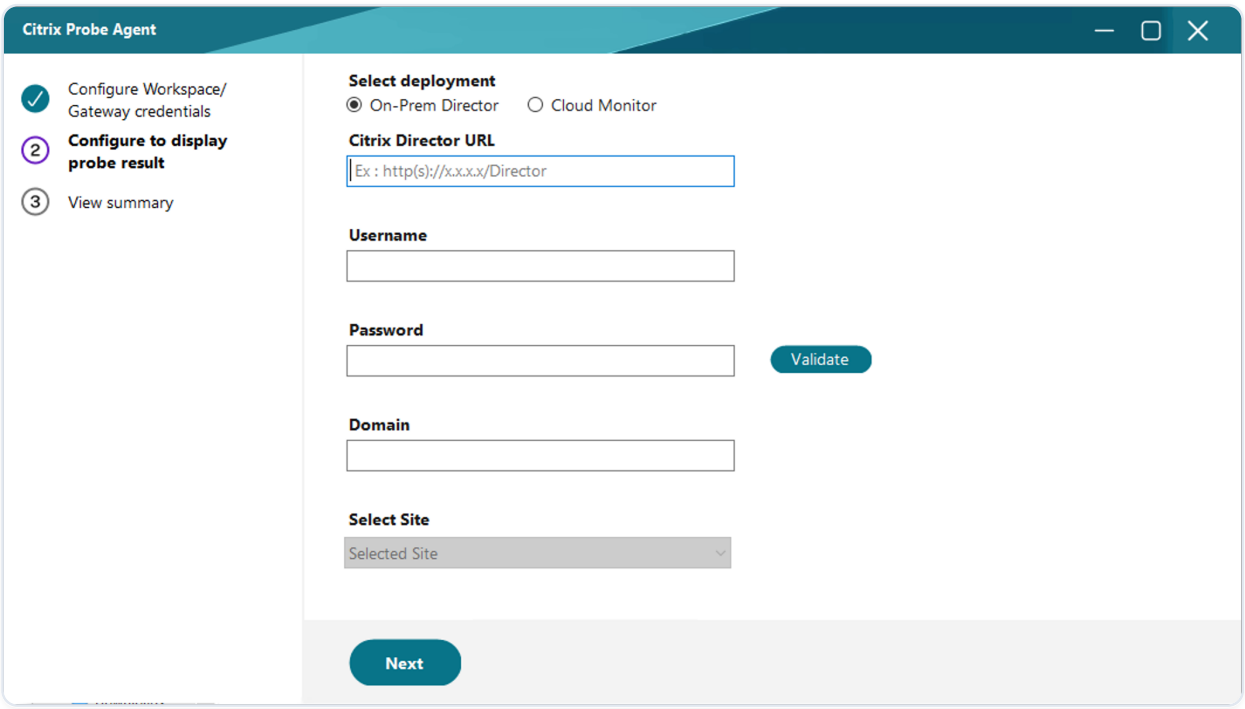
1. 确定要运行探测的端点计算机。
2. 具有管理权限的用户可以在端点计算机上安装和配置 Citrix Probe Agent。从Citrix 下载页面下载 Citrix Probe Agent 可执行文件。下载链接也可在 Director 的“**探测**”选项卡中找到。



3. 如果您有聚合站点，请选择“Workspace (StoreFront) Site Aggregation Enabled”选项以启用聚合站点中的应用程序和桌面枚举。
4. 选择身份验证方法并输入相关凭据。凭据经过加密并安全存储。
5. 使用您的 StoreFront Active Directory 凭据进行配置。在每台端点计算机上配置一个唯一的 Workspace (StoreFront) 用户。
6. 如果您的端点通过 Citrix Gateway 连接到 StoreFront，请选择 Citrix Gateway 选项并使用您的 Citrix Gateway 域凭据进行配置。



7. 如果您的网关支持多重身份验证选项，请选择该选项并输入 16 位身份验证密钥。此选项仅适用于使用单一登录方案配置了 LDAP 和原生 OTP 的 Citrix Gateway。
8. 在 **Configure To Display Probe Result** 选项卡中，输入您的 Director 凭据，然后单击 **Validate**。



9. 选择您的站点，然后单击 **Next**。
10. 在**查看摘要**选项卡中，确保配置的详细信息准确无误。如果需要进行更改，请转到相应的选项卡并进行更新。

注意：

您可以使用 Automating Citrix Probe Agent Installation and Configuration 中包含的 PowerShell 脚本来自动安装和配置 Citrix Probe Agent。

步骤 2：在 Director 中配置探测

限制：

如果从启用了交互式登录消息横幅的 Windows VDA 启动测试应用程序或桌面，则探测会失败。这是因为等待接受交互式登录消息会导致超时。 要在服务器 VDA 上禁用登录消息。转到“计算机配置”>“Windows 设置”>“安全设置”>“本地策略”>“安全选项”。

删除以下字段中的文本并更新 Microsoft 策略。

- 交互式登录：尝试登录用户的消息文本
- 交互式登录：尝试登录用户的消息标题

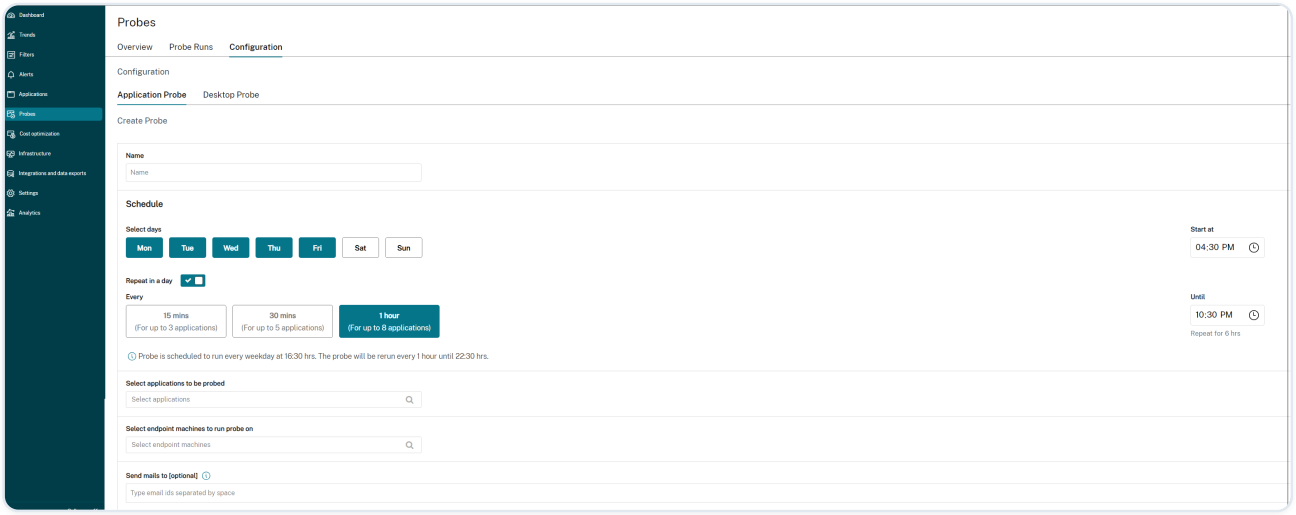
将探测用户分配给此特定的服务器 VDA，并禁用交互式登录消息横幅，以确保探测能够通过应用程序或桌面启动状态。

有关详细信息，请参阅 `<https://learn.microsoft.com/zh-cn/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`。

1. 转至**探测器** \> **应用程序探测**或**桌面探测**，然后单击**创建探测**。
2. 在“**创建探测**”页面中，输入探测的名称。
3. 选择计划：
   a. 选择您希望探测运行的星期几。
   b. 输入您希望探测运行的开始时间。

c. 此外，您可以选择“**一天内重复**”选项。输入结束时间以及您希望探测在一天内重复的间隔。例如，以下配置有助于在每周一、周三、周四和周日，从 12:08 到 16:34 之间每 30 分钟运行一次应用程序探测。

4. 根据间隔选择建议的要探测的应用程序或桌面数量。
5. 选择必须运行探测的端点计算机。
6. 输入管理员的电子邮件地址，以发送失败探测的结果。在 **Alerts** > **Email Server Configuration** 中配置您的电子邮件服务器。



在此配置中，应用程序会话将在每周一、周三、周四和周日的 12:08、12:38、13:08 等时间启动，直到 16:08。

注意：

- 配置后，代理将在下一个小时开始运行配置的探测。
- 在引入“**一天内重复**”选项之前设置的探测将继续按其计划时间运行。默认情况下，这些探测的“**一天内重复**”选项处于禁用状态。
- 建议您配置探测，使每次运行间隔 5 分钟，以防止重叠。

步骤 3：探测执行

代理根据从 Director 定期获取的探测配置运行探测。

它使用 StoreFront 串行启动选定的应用程序。代理通过 Monitor 数据库将结果报告回 Director。故障在五个特定阶段报告：

- **StoreFront 可达性** - 配置的 StoreFront URL 不可达。

- **StoreFront 身份验证** - 配置的 StoreFront 凭据无效。
- **StoreFront 枚举** - StoreFront 枚举应用程序列表不包含要探测的应用程序或桌面。
- **ICA® 下载** - ICA 文件不可用。
- **应用程序/桌面启动** – 应用程序或桌面无法启动。

步骤 4：查看探测结果

您可以在“**探测**”中查看探测结果。“探测”视图全面概述了探测结果。这些结果有助于主动分析和解决问题，从而为用户提供更流畅的会话启动体验。

“**概述**”选项卡在一个视图中提供了所有已配置探测的摘要。

Director 探测运行(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-probe-metrics-chart.png)

您可以根据时间段、探测类型、端点名称、应用程序名称、桌面名称和探测结果类型筛选探测。符合筛选条件的探测将显示每个探测、应用程序/桌面和端点的以下详细信息。

“**探测指标**”显示了已安排、已计划、已跳过、成功和失败运行的计数。

- 已完成运行 – 已完成的探测运行次数。
- 失败运行 – 失败的探测运行次数。
- 跳过的运行 – 由于端点不活动或服务不可用而未能完成的运行次数。
- 成功运行 – 在应用程序/桌面启动期间，在任何阶段都没有失败并成功完成的探测数量。

还会显示端点计算机的总数，以及活动和非活动计算机的数量。

探测失败阶段以可视化方式显示每个失败组的失败分布。通过分析大多数失败发生的阶段，可以更容易地解释探测结果并排除故障。图形表示显示了应用程序/桌面启动、ICA 文件下载、Storefront/Workspace 枚举、Storefront/Workspace 可达性和 Storefront/Workspace 身份验证的失败探测运行次数。

它有助于分析大多数失败发生的阶段。此信息有助于快速理解探测结果并排除故障。

某些探测运行可能无法完成，原因可能是端点处于非活动状态，或者服务不可用。

“**探测运行**”选项卡详细显示已完成的探测运行结果。您可以深入查看所选探测的每次单独运行的详细信息。您可以根据重要的关键点进行进一步筛选和分析。

Director 探测运行(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-probe-runs.png)

您可以根据时间段、探测类型、端点名称、应用程序名称、桌面名称和探测失败阶段筛选探测运行。探测失败阶段显示探测失败的阶段。单击探测名称、计划运行、失败运行、应用程序/桌面名称链接也会将您带到“探测运行”页面，其中包含符合筛选条件的探测运行列表。

成本优化

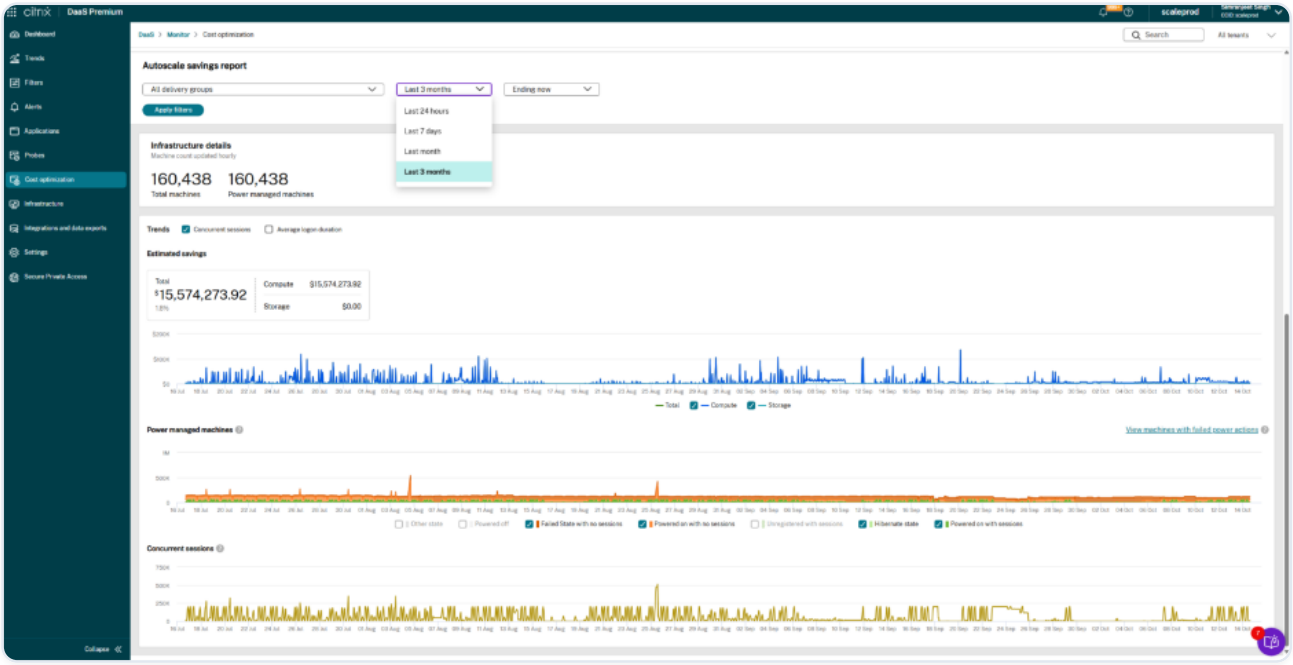
Citrix Director 现在引入了一项名为“成本优化”的新功能，可帮助您有效分析虚拟机和会话的使用情况。此功能提供富有洞察力的可视化表示，说明如何优化成本。它还有助于您消除不必要的计算机，从而降低成本。

为支持成本优化，还引入了以下警报：

- 启动失败操作和关机失败操作
- 计算机正常运行时间警报

您还可以检查具有近期电源操作的计算机，以分析导致用户问题的开机故障和增加成本的关机故障。有关详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/troubleshoot-deployments/machines.html#inspect-machines-with-recent-power-actions) 部分。

单击“**主页**”上的左侧菜单中的“**成本优化**”选项卡，以访问“**成本优化**”页面。



在“**成本优化**”主页上，您可以执行以下操作：

- 入门链接 - 访问此链接可了解有关成本优化功能的更多信息。
- 查看成本优化页面 - 您可以在“**成本优化**”页面上提供反馈
- 刷新数据。

- 查看警报 - 您可以查看严重警报和警告警报。

“**成本优化**”页面包括以下功能：

- 成本节约
- 基础设施规模调整

如何计算成本优化所需的成本?

每台计算机每小时的成本以管理程序支持的货币显示。本节介绍 Azure 计算机和其他计算机的成本计算方式。

Azure 计算机的成本

计算成本的优先级顺序如下：

1. 当 'Microsoft.Consumption/pricesheets/read' 权限可用时，有效价格将以 Azure 订阅中配置的货币显示。
2. 如果权限不可用，则显示 Azure 零售价格。有关详细信息，请参阅 Azure 零售价格概述。
3. 当有效价格或零售价格不可用时，成本将根据管理员在 Web Studio 中输入的成本显示。
4. 如果 Web Studio 中未提及成本，则默认成本为 1 美元。

要查找 Azure 的帐户详细信息并添加查找有效价格所需的权限，请执行以下操作：

1. 导航到 Citrix DaaS。
2. 单击“**托管**”选项卡以查找托管连接帐户。
3. 在“**托管**”选项卡中查找提及的“**应用程序 ID**”。

   托管选项卡(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/daas-azure-hosting.png)
4. 转到 Microsoft Entra ID，查找在步骤 3 中记下的“**应用程序 ID**”。
5. 转到“**订阅**”>“**访问控制 (IAM)**”> 选择为托管连接 SPN 配置的自定义角色。

   Azure 门户(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-portal.png)

   Azure 门户订阅(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/azure-portal-subscriptions.png)
6. 将 *Microsoft.Consumption/pricesheets/read* 权限添加到该角色。

如何验证 Azure 零售价格?

如果 `Microsoft.Consumption/pricesheets/read` 不可用，则会显示 Azure 零售价格。现在，您可以使用 Retail Rates Prices API 获取所有 Azure 服务的零售价格。以前，获取 Azure 服务价格的唯一方法是使用 Azure 定价计算器或 Azure 门户。有关详细信息，请参阅Azure 零售价格概述。

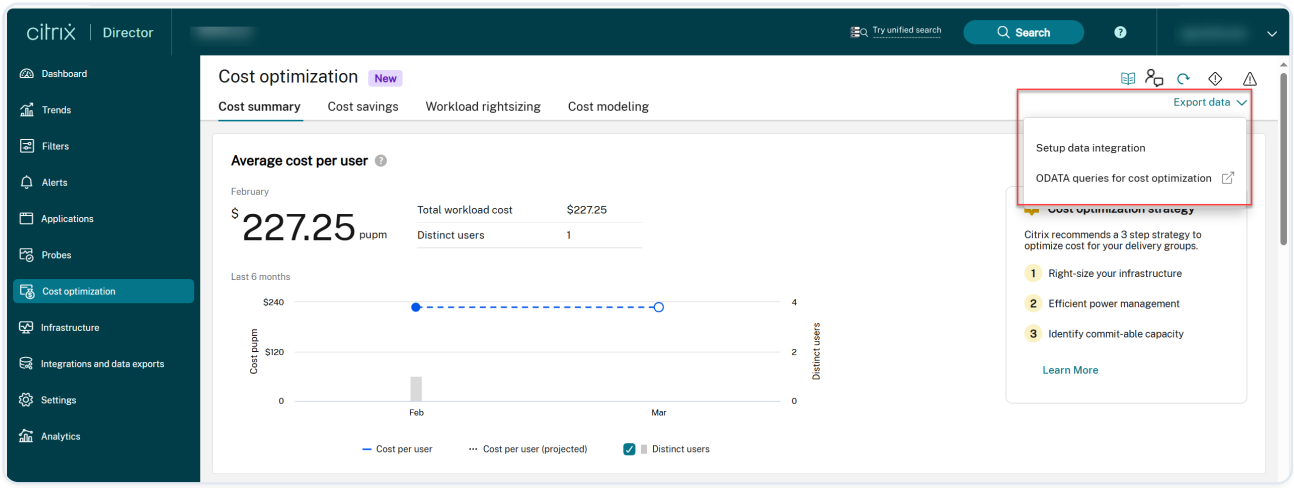
计算非 Azure 计算机的成本

对于其他计算机，成本是根据管理员在 Web Studio 中输入的成本显示的。如果在 Web Studio 中未提及成本，则默认为 1 美元。

导出数据

您可以使用数据集成和 ODATA 查询导出“**成本优化**”页面上的数据。要导出数据，请在“**成本优化**”页面上单击“**导出数据**”，将显示以下选项：

- 设置数据集成
- 用于成本优化的 ODATA 查询



设置数据集成

您可以将成本优化数据与 Monitor Service API 集成，通过该 API 可以收集数据以进行故障排除和问题分类。有关详细信息，请参阅集成和数据导出页面。

用于成本优化的 ODATA 查询

您可以使用**成本优化**页面上提供的 ODATA 示例查询来导出数据。

ODATA 入门

以下链接可帮助您开始使用 ODATA：

- ODATA 概述

- 使用 Citrix Cloud 中的 OData v4 端点访问 Citrix Monitor Service 数据的不同方法
- 在 Citrix Monitor Service 数据中使用 OData V4 聚合查询
- 如何使用 OData 和 API 客户端将 PowerBI 连接到 DaaS Monitor
- 使用 Postman 获取登录持续时间较长的用户详细信息
- 如何访问 Monitor Service 数据
- 数据访问协议
- 监控模型
- 监控通知

ODATA 示例查询

查找未使用的 VDA

要查找未使用的 VDA，您必须提供桌面组 ID、VDA 的开始日期和结束日期。

有关减少未使用的资源开支的更多信息，请参阅工作负载大小调整。

示例查询：

```
https://<DDC URL>/monitorodata/ResourceUtilizationSummary?
$apply=filter(DesktopGroupId eq desktop-group-id and granularity eq 1440
and SummaryDate ge startdate and SummaryDate lt enddate)/
groupby((MachineId), aggregate(cast(TotalSessionCount, Edm.Int32) with
average as AvgTotalSessionCount))/filter(AvgTotalSessionCount eq 0.0)/
aggregate($count as UnusedVDACount)
```

查找每日平均正常运行时间（分钟）

要查找每日平均正常运行时间（分钟），您必须提供以下信息：

- 桌面组 ID
- 开始日期
- 结束日期
- 结束日期和开始日期之间的天数差。

有关减少未使用的资源开支的更多信息，请参阅工作负载大小调整。

示例查询：

```
https://[<DDC URL>|https://api-us.cloud.com/monitorodata/
ResourceUtilizationSummary?$apply=filter(DesktopGroupId] /monitorodata/
ResourceUtilizationSummary?$apply=filter(desktopGroupId eq desktop-group-
id and granularity eq 1440 and SummaryDate ge startdate and SummaryDate lt
enddate)/groupby((MachineId), aggregate(cast(UptimeInMinutes, Edm.Int32)
div day-difference with sum as TotalUptimeInMinutes))/
aggregate(TotalUptimeInMinutes with average as
DailyAverageUptimeInMinutes)
```

查找失败的计算机电源操作

有关失败的计算机电源操作的更多信息，请参阅开机操作失败和关机操作失败。

示例查询：

```
https:// <DDC URL> /monitorodata/Machines?$filter=LifecycleState eq 0 and
DesktopGroup/SessionSupport eq 1 and
(cast(LastPowerActionReason,'Edm.Int32') eq 6 or
cast(LastPowerActionReason,'Edm.Int32') eq 7 or
cast(LastPowerActionReason,'Edm.Int32') eq 8) and
(cast(LastPowerActionFailureReason,'Edm.Int32') eq 300 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 402 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 401) and MachineRole eq
0&$orderby=Name&$skip=0&$top=50&$expand=DesktopGroup($select=Name)&$select
=Sid,Id,Name,IsAssigned,IPAddress,FaultState,LastDeregisteredCode,FailureD
ate,CurrentPowerState,CurrentSessionCount,IsInMaintenanceMode,LastPowerAct
ionFailureReason,LastPowerActionCompletedDate
```

查找总节省

有关成本节省的更多信息，请参阅成本节省 页面。

示例查询：

```
https://[<DDC URL>|https://api-us.cloud.com/monitorodata/
ResourceUtilizationSummary?$apply=filter(DesktopGroupId] /monitorodata/
MachineCostSavingsSummaries?$apply=aggregate(TotalAmountSaved with sum as
TotalAmountSavedSum)
```

查找计算机状态

有关成本节省的更多信息，请参阅成本节省 页面。

示例查询：

```
https:// <DDC URL> /monitorodata/MachineCostSavingsSummaries?
$filter=SummaryDate eq
2024-08-09T06:00:00Z&$select=TotalMachinesCount,PowerManagedMachinesOff,Po
werManagedMachinesInHibernate,PowerManagedMachinesOnWithSessions,PowerMana
gedMachinesOnWithoutSessions
```

成本节约

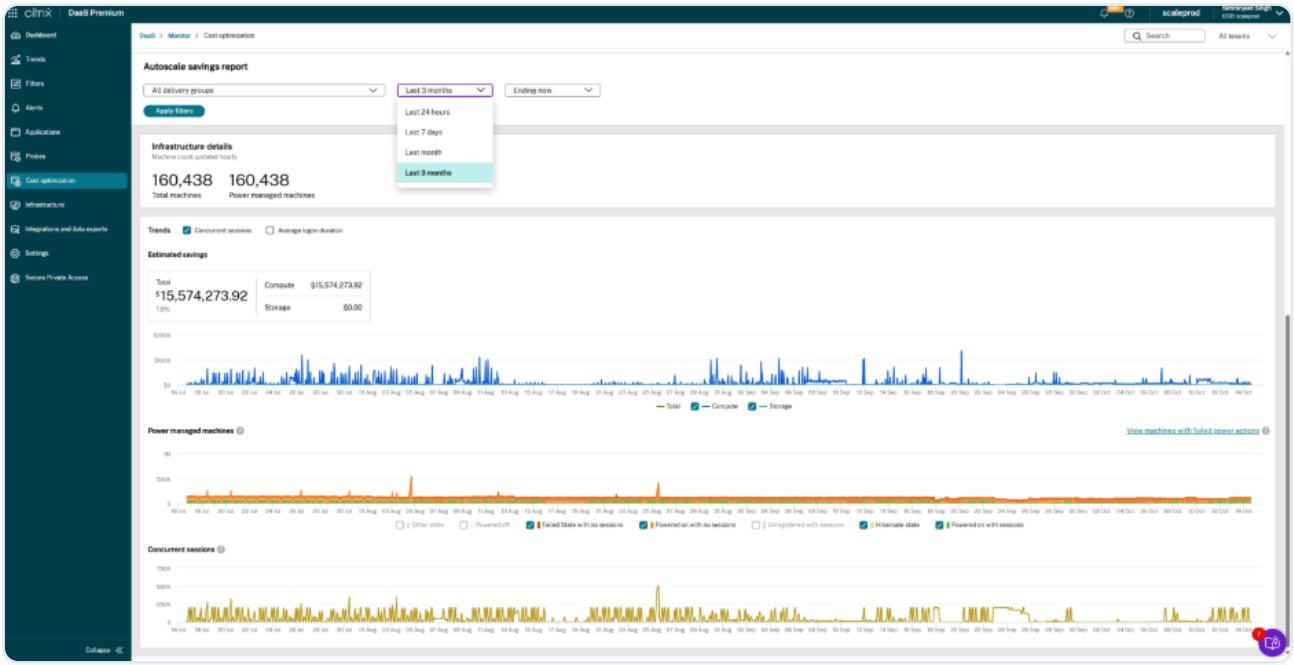
成本节约页面提供在选定期间内累计的基础架构节约的可视化表示，并预测剩余天数的预期节约。通过分析计算机使用情况和会话，此页面可帮助您识别已实现的节约和降低成本的机会。此页面提供：

- 深入了解基础架构成本优化
- 节约的金额
- 有关可能导致超出预计成本的各种情况的信息
- 识别和战略规划的潜在机会，以实现基础架构成本节约

计算机使用情况通常在高峰时段增加，需要更多资源。Autoscale™ 功能通过在需求低谷期自动关闭未使用的计算机来帮助您降低成本。预计节约取决于此使用模式。但是，在特定情况下，成本可能超出预期，例如存在未使用的计算机或 Autoscale 电源操作失败时。以前，识别这些情况背后的原因具有挑战性。

成本优化页面提供有关可能导致您超出预期成本的不同场景的详细信息。同样，例如，如果没有会话的计算机，它会向您显示进一步的成本节约机会。

在**主页**的左侧菜单中单击**成本优化**选项卡以访问**成本优化**页面。



在顶部的下拉列表中，如果站点同时具有云提供商和本地提供商，您现在可以按所有云提供商、所有本地提供商或单个提供商进行筛选。

注意：

> 选择后立即应用筛选器，无需单击“应用”按钮。

> **成本优化**页面包括**估算节约**和**自动缩放节约报告**。您可以以管理程序的货币或以已产生费用的百分比查看成本节约。

估算节约：此图形表示有助于评估基础架构资源的有效利用。成本节约以管理程序的货币或以已产生费用的百分比显示。此图显示了计算相关节约和存储节约所实现的节约。

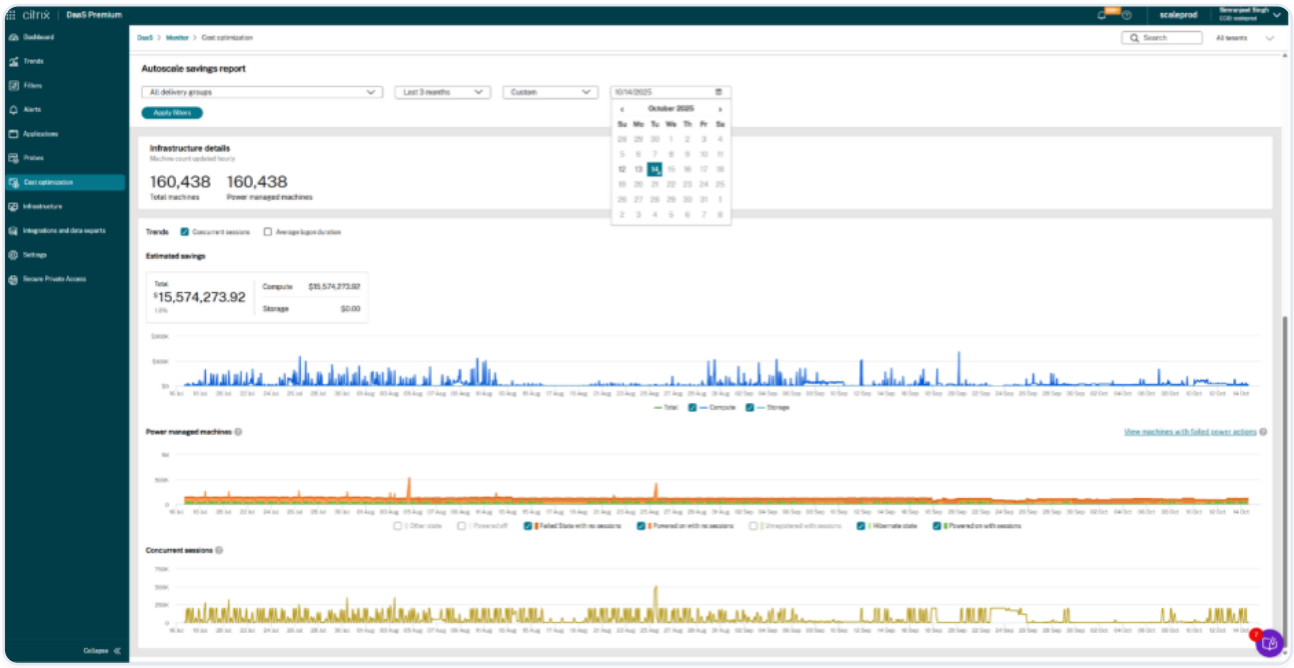
注意：

> 要查看存储节省情况：
>
> - 必须启用 Autoscale 才能优化计算成本。有关详细信息，请参阅Autoscale 入门。
> - 在 VM 关闭时将存储类型更改为较低层级以优化存储成本。有关详细信息，请参阅在 VM 关闭时将存储类型更改为较低层级文档。
> - 此功能目前仅适用于 Azure 计算机。

> 您可以查看最近的以下结果：

- 七天
- 三十天
- 三个月
- 六个月
- 十二个月

下图显示了估算基础架构节约部分：



下表列出了估算基础架构节约图的元素：

元素	描述
总节约	显示所选持续时间内在基础设施方面实现的总节省。节省的费用进一步分为存储和计算成本，并以表格形式提供。
预计节省	显示所选持续时间内在基础设施方面实现的节省金额。
电源管理计算机	显示电源管理机器的总数。
预计节约	显示在剩余持续时间内可以实现多少基础设施节省。
计算 - 总计	显示从计算相关节省中实现的总节省。

元素	描述
计算 - 自动缩放	显示通过使用自动缩放功能的计算相关节约实现的总节约。
计算 - 用户操作	显示从用户操作产生的计算相关节省中实现的总节省。
存储 - 总计	显示通过存储节省实现的总节省。
存储 - 自动缩放	显示通过使用自动缩放功能的存储节省实现的总节省。
存储 - 用户操作	显示从用户操作产生的存储节省中获得的总节省。

自动缩放节省报告：此图形表示形式提供了已配置并启用自动缩放功能的交付组的节省报告。此报告仅适用于电源管理的计算机。您可以选择一个交付组，然后选择今天、昨天、上周、下周、本月或下月的数据。您可以将鼠标悬停在任何图表上以检索特定的图表值。

> **注意：**
>
> 如果交付组被删除，您将无法在自动缩放节省报告中获取任何数据。
>
> 您可以从交付组下拉列表中深入查看以下选项：

- **所有交付组**：基础结构详细信息显示所有交付组信息。
- **所有单会话**：所有单会话计算机交付组的基础结构详细信息，以及当您将鼠标悬停在图表上时，机器电源状态、成功的自动缩放电源操作和会话的图形表示。
- **所有多会话**：所有多会话计算机交付组的基础结构详细信息，以及图形表示。
- **选择最多 15 个** - 基础结构详细信息显示所有选定的交付组（最多 15 个）以及图形表示。
- **排除最多 15 个** - 基础结构详细信息显示所有交付组（排除选定的交付组，最多 15 个）以及图形表示。

数据显示所选持续时间的数据。**预计节省**的图形表示是根据下拉菜单中的选择计算出的实际节省。当您将鼠标悬停在峰值点上时，会显示有关计算机电源状态、成功的 Autoscale 电源操作和会话的信息。

根据所选的交付组，您可以查看以下详细信息：

- **基础架构详细信息**
  - 计算机总数和电源管理计算机 - 显示计算机总数以及其中有多少台计算机是电源管理的。此数据为您提供了进一步的机会，可以考虑将剩余的非电源管理计算机转换为电源管理计算机，从而为更全面的覆盖启用 Autoscale 功能。“基础架构详细信息”部分中的数据显示每小时更新的最新已知信息。
- **目录详细信息**

  显示管理程序（服务提供商）的名称。有关详细信息，请参阅 支持的 VDA 托管平台。“目录详细信息”中的数据显示当前可用的最新数据（实时数据）。

  您可以获取以下详细信息：
  - **管理程序名称** - 显示站点连接到的管理程序的名称。当存在多个管理程序时，显示所有可用的管理程序。
  - **实例** - 显示实例的名称。
  - **每小时总成本** - 以管理程序支持的货币显示每台机器每小时的成本。对于 Azure 机器，当 Microsoft.Consumption/pricesheets/read 权限可用时，有效价格将以 Azure 订阅中配置的货币显示。如果权限不可用，则显示 Azure 零售价格。有关详细信息，请参阅 Azure 零售价格概述。对于其他机器，成本根据管理员在 Web Studio 中输入的成本显示。如果 Web Studio 中未提及成本，则默认成本为 $1。有关详细信息，请参阅 [如何计算优化成本的成本？
  - **每小时计算成本** - 显示与计算相关的节省所带来的成本节省。
  - **每小时存储成本** - 显示存储节省所带来的成本节省。
  - **计算机** - 显示所选实例的计算机数量。
- **Autoscale 配置（最新已知）**

  正在使用的标签 - 显示在 WebStudio 的 Autoscale 设置中配置的计算机标签。您还可以根据带标签的计算机筛选数据。在这种情况下，您将只获得带标签的计算机摘要。

  容量缓冲区（高峰）和容量缓冲区（非高峰）

  显示在高峰和非高峰时段，基于交付组最大需求已开机计算机的缓冲区百分比。
- **预计节省**

  显示在选定持续时间内基础设施实现的节省金额。您可以查看已启用自动缩放功能的 Azure 机器的计算相关节省和存储相关节省。

- **电源管理的计算机**

  启用自动缩放后，电源管理的计算机在不使用时会关闭以优化成本。您可以获取以下详细信息：

  - 已关机的计算机数量 - 此数据可帮助您分析已关机的计算机数量，从而有助于降低成本。
  - 休眠状态 - 此数据可帮助您分析有多少计算机处于休眠状态。
  - 无会话的开机机器 - 此数据为您提供了分析机器为何在没有任何会话的情况下处于活动状态的机会。此数据为您提供了规划更有效的基础设施节省策略的机会。
  - 有会话的开机计算机 - 此数据可帮助您分析已开机且具有活动会话的计算机数量。
  - 关机 - 此数据可帮助您分析已关机或挂起的计算机数量以及执行此操作的时间。您可以验证此数据并进行进一步修改，从而有助于降低成本。
  - 开机 - 此数据可帮助您分析有多少计算机已开机以及执行此操作的时间。您可以验证此数据并进行进一步修改，从而有助于降低成本。
  - 无会话的失败状态：此字段显示处于失败状态且没有活动会话的计算机数量。
  - 有会话的未注册状态：此字段显示处于未注册状态但仍在提供会话的计算机数量。

  > **注意：**
  >
  > 您可以查看处于“失败”状态且无会话的计算机数量，以及处于“电源操作失败”状态的计算机数量，并根据失败原因、时间以及交付组采取措施。这些计数是可点击的链接，可导航到“筛选器”页面以执行进一步操作。该计数包括单会话和多会话计算机。

- **并发会话**

  显示所选时间点的会话总数。此数据可帮助您确定何时关闭计算机以进行成本优化。

- **平均登录持续时间**

  显示用户在所选时间段内的平均登录时间。

工作负载规模调整

增强型工作负载规模调整页面可帮助您分析交付组的使用情况和规模调整方面。因此，可以根据计算机或用户活动来分析交付组。

基于计算机的分析使您能够：

- 根据使用情况对虚拟桌面进行分类，以识别没有活动或活动量低的计算机，并减少在未使用资源上的开支。使用情况分析

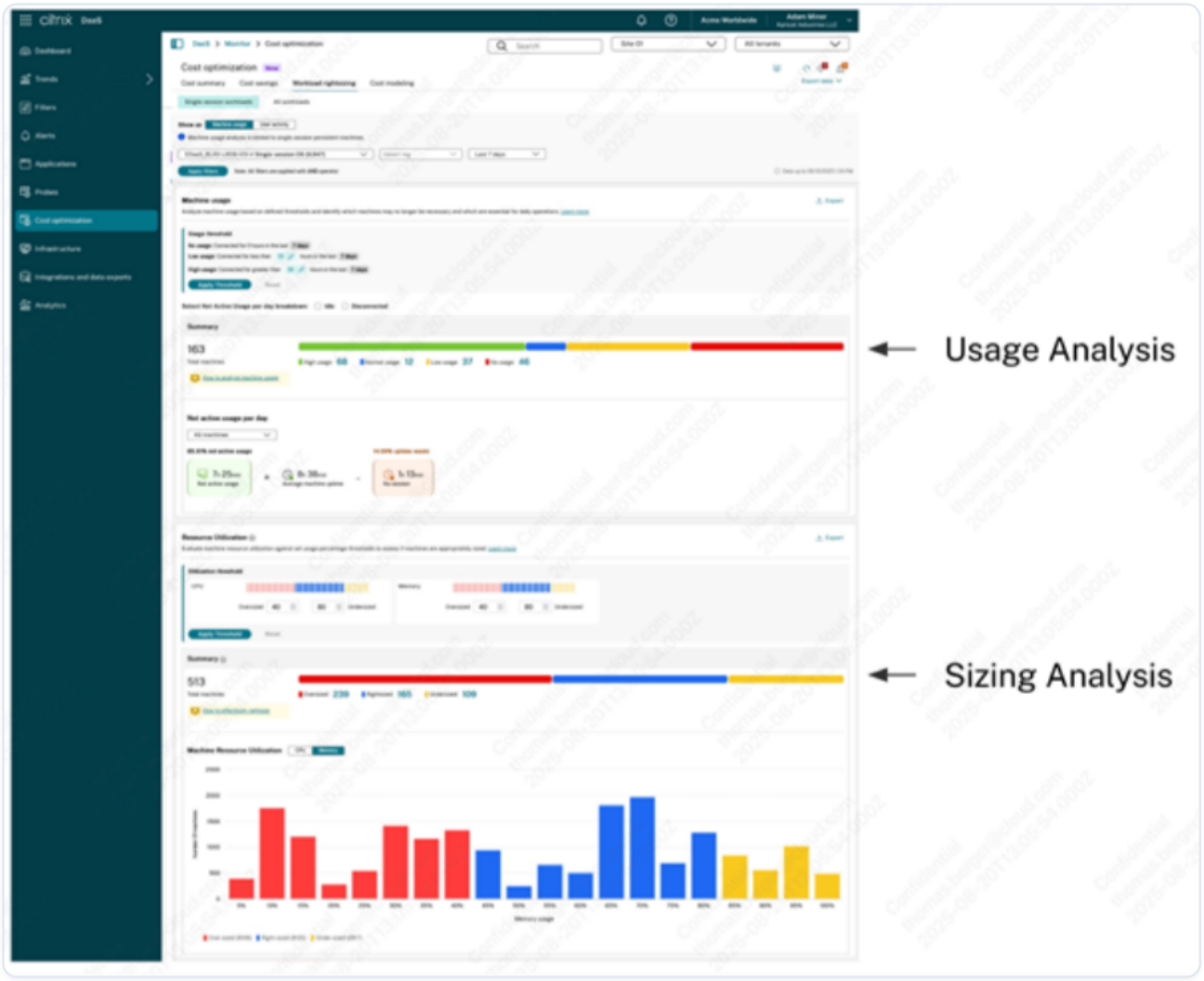
- 分析虚拟桌面上的资源利用率，以识别需要调整规模的计算机，从而降低成本或改善用户体验。规模调整分析

基于用户的分析使您能够：

- 根据用户的活动对其进行分类。考虑出于 IT 卫生原因删除没有活动的用户访问权限。使用率低的用户可以转移到共享资源，以更有效地利用资源。
- 分析用户的资源消耗，以识别资源消耗高于或低于平均水平的用户群，并更有效地分配用户。

在主页左侧菜单中单击“**成本优化**”选项卡。然后，单击“**工作负载规模调整**”选项卡以访问“**工作负载规模调整**”页面。

> **注意：**
>
> 在页面顶部，您可以在基于计算机的分析和基于用户的分析之间切换。
>
> 您还可以从“**成本优化选项卡 > 成本节约**”中的“**基础结构详细信息**”部分单击“**调整此交付组规模**”链接，以访问“**工作负载规模调整**”页面。



计算机分析非常适合将虚拟桌面静态分配给用户的场景，例如 Windows 365 Enterprise 或 Frontline 专用。用户分析对于分析具有随机分配虚拟桌面的交付组很有用。这两种分析目前都仅限于单会话计算机。

> **注意：**
>
> 经典的资源优化分析（可通过页面顶部的“所有工作负载”按钮访问）将在即将发布的版本中弃用。

使用情况分析

使用情况分析使您能够根据虚拟桌面的活动级别对其进行分类，如下所示：

- **低使用率或无使用率计算机（专用计算机）**：此类别中的计算机可能不再需要，可以移除以节省成本。
- **高使用率计算机（专用计算机）**：此类别对于日常操作至关重要，可能需要额外的服务连续性措施。

- **低使用率或无使用率用户（池化计算机）**：在选定时间范围内没有活动的用户可能不再需要分配到交付组。移除他们有助于降低环境成本。低活动用户可能会受益于重新分配。为了整合使用情况并降低成本，请考虑将拥有专用桌面的低活动用户移动到池化桌面。

要执行使用情况分析，请执行以下操作：

1. 根据交付组或标签选择计算机
2. 选择分析的时间范围。
3. 查看并配置定义低使用率和高使用率模式的阈值。
4. 检查显示基于配置阈值的虚拟桌面分类的摘要部分。
5. 查看显示每台计算机使用情况详细信息的净活动使用情况部分。空闲和断开连接时间可以包含在净活动使用情况分析中，也可以从中排除。
6. 使用下拉菜单关注特定类别。
7. 使用导出功能导出计算机名称和关联用户，以查看计算机名称及其关联用户。

注意：

所提供的示例说明了基于计算机的使用情况分析；但是，基于用户的分析步骤是等效的，此处不再单独讨论。



大小调整分析

大小调整分析根据资源利用率将虚拟桌面或用户分类如下：

- 过大计算机：拥有的资源超出所需；减少资源分配可以降低成本，而不会影响用户体验
- 过小计算机：缺少足够的资源；通过分配更多资源可以改善用户体验
- 大小适中计算机：介于过大和过小阈值之间
- 轻度用户：这些用户可能会受益于重新分配。为了整合和降低成本，请考虑将拥有专用桌面的轻度用户移动到共享池桌面。
- 中度用户：中度用户已正确分配到交付组中的计算机，应能获得最佳用户体验。
- 高级用户：高级用户消耗大量资源，当他们共享池桌面时，其高使用率可能会对该计算机上其他用户的整体体验产生负面影响。为了增强所有用户的体验并确保高级用户能够持续访问桌面，请考虑将这些用户移动到专用桌面或将其分配到单独的交付组。

要执行大小调整分析：

1. 根据交付组或标签选择计算机
2. 选择分析的时间范围。
3. 配置 CPU 和内存利用率的单独阈值。
4. 查看显示虚拟桌面分类的摘要部分
5. 分析显示 CPU 和内存分布的机器资源利用率图表
6. 根据资源类型微调机器配置并识别异常值
7. 使用导出功能导出机器名称和关联用户，以查看机器名称及其关联用户

> **注意：**
>
> 所提供的示例说明了基于机器的资源消耗分析；但是，基于用户的分析步骤是等效的，在此不单独讨论。



注意：

利用率分析使用所选时间范围内交付组的第 95 百分位利用率，这表明 95% 的 CPU 或内存利用率等于或低于设定值。

最佳实践

- 使用使用情况分析，通过移除未充分利用的机器来识别节省成本的机会。
- 应用大小调整分析以优化资源分配并改善用户体验。
- 对于静态分配的虚拟桌面场景，使用机器分析以进行准确分析。
- 对于池化虚拟桌面场景，使用用户活动以进行准确分析。
- 分析随机分配的虚拟桌面时，请考虑漫游模式。
- 导出详细报告以供进一步分析和文档编制。

关键术语和图表

机器净活跃使用率：净活跃使用率是通过从平均机器正常运行时间中扣除总正常运行时间浪费来计算的。所有时间均以分钟为单位。

净活跃使用率百分比：用户实际主动使用机器的时间。这是机器开机时至少有一个会话处于活动状态的持续时间。

平均机器正常运行时间：机器开机的总时间。

无会话：由于没有活动会话而浪费的正常运行时间。

空闲时间：由于空闲会话而浪费的正常运行时间。这是机器上所有会话都处于空闲状态的时间。

断开连接时间：由于会话断开连接而浪费的正常运行时间。这是机器上所有会话都处于断开连接状态的时间。

总机器数 - 显示机器总数。这包括在选定期间内已开机的所有机器。

平均会话密度 - 这是机器数量和选定时间段的平均值。指机器上的会话负载量，它会影响会话可用的资源。

未使用机器 - 显示在选定时间段内没有会话但仍处于开机状态的机器数量。

CPU 利用率：

机器群组 - 根据 CPU 利用率将机器组分为顶部、中部和底部，并提供相关信息。阈值限制可由管理员配置。

CPU 峰值范围 - 显示根据机器群组的利用率对应的 CPU 峰值范围。

机器数 - 显示与机器群组对应的机器数量。

会话密度 - 显示与机器群组对应的会话密度。

资源利用率趋势：

CPU 峰值范围 - 以带状显示 CPU 峰值范围。当您将鼠标悬停在带状图中的任何点上时，将显示该带状图的顶部和底部值。

内存峰值利用率 - 以图表形式显示所选计算机和所选时间的最高内存利用率。

平均会话密度 - 以图表形式显示所选计算机和所选时间的平均会话密度。

平均 ICA RTT - 显示会话的平均往返时间。当没有活动会话或会话断开连接时，此图表会显示中断。

平均登录持续时间 - 以图表形式显示所选计算机和所选时间段的平均登录持续时间。当在所选时间内开始新的登录时，此图表会显示数据。

成本摘要

成本摘要页面提供了运行 Citrix® 环境所产生费用的全面摘要。通过此增强功能，您可以了解：

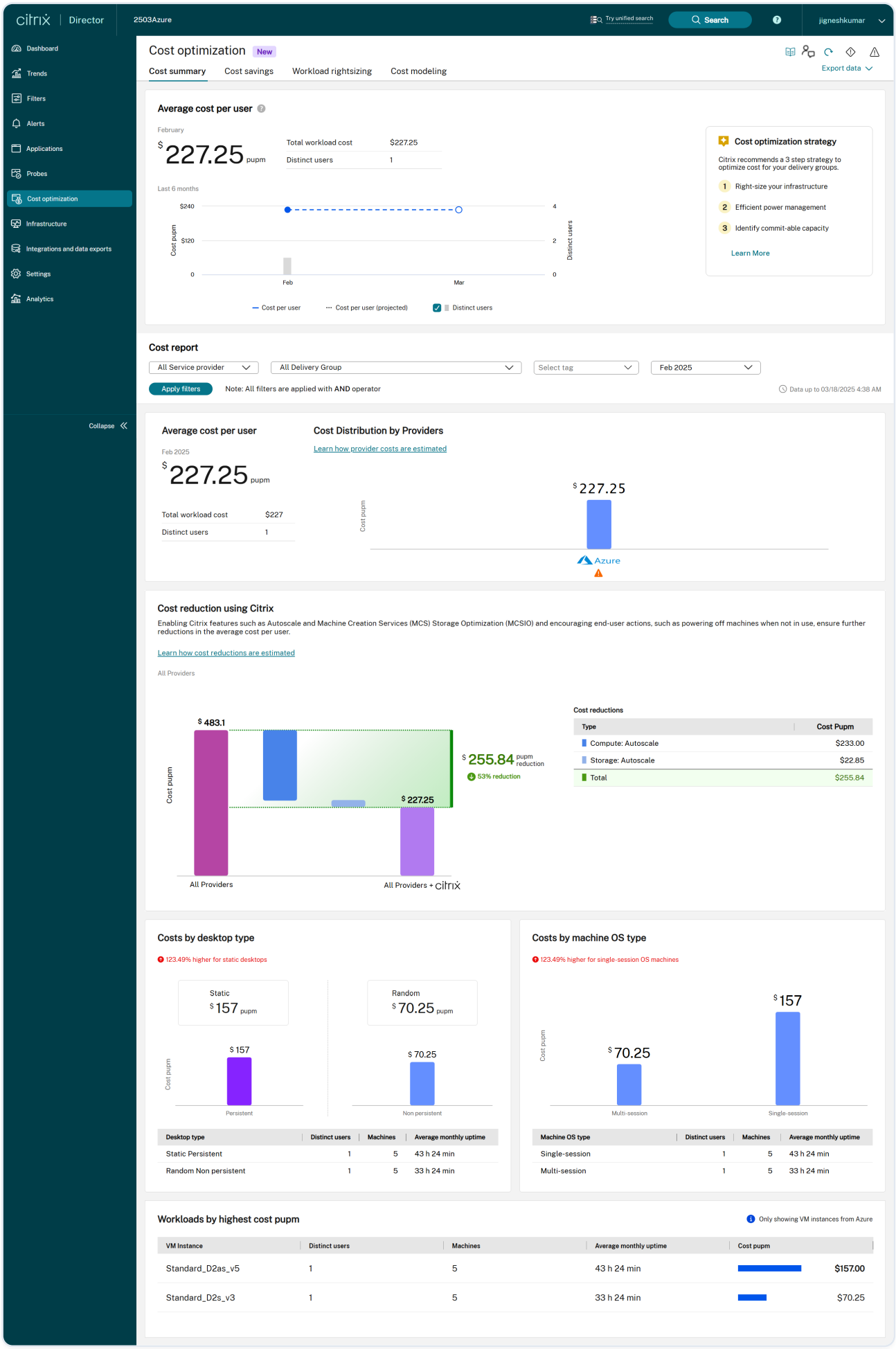
- 每个用户的总成本
- 根据所选工作负载提供商、桌面类型和虚拟机系列集交付虚拟化的成本

此页面提供：

- 深入了解向用户交付虚拟化应用程序或桌面的成本
- 节省的金额
- 按以下类别划分的成本和节省信息：
  - 平台提供商
  - 操作系统类型
  - 桌面类型
  - 虚拟机系列

> **注意：**
>
> **成本摘要**页面仅在站点每月运行至少 15 天时可用。

要访问“**成本摘要**”页面，请单击“**Director**”>“**成本优化**”>“**成本摘要**”。“**成本摘要**”页面随即显示：


citrix | Director
2503Azure
Try unified search
Search
jigneshkumar
Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and data exports
Settings
Analytics
Collapse
Cost optimization New
Cost summary
Cost savings
Workload rightsizing
Cost modeling
Export data
Average cost per user
February
$ 227.25 pupm
Total workload cost $227.25
Distinct users 1
Last 6 months
$240
$120
0
Cost pupm
4
2
0
Distinct users
Feb
Mar
Cost per user
Cost per user (projected)
Distinct users
Cost optimization strategy
Citrix recommends a 3 step strategy to optimize cost for your delivery groups.
1 Right-size your infrastructure
2 Efficient power management
3 Identify commit-able capacity
Learn More
Cost report
All Service provider
All Delivery Group
Select tag
Feb 2025
Apply filters
Note: All filters are applied with AND operator
Data up to 03/18/2025 4:38 AM
Average cost per user
Feb 2025
$ 227.25 pupm
Total workload cost $227
Distinct users 1
Cost Distribution by Providers
Learn how provider costs are estimated
$ 227.25
Cost pupm
Azure
Cost reduction using Citrix
Enabling Citrix features such as Autoscale and Machine Creation Services (MCS) Storage Optimization (MCSIO) and encouraging end-user actions, such as powering off machines when not in use, ensure further reductions in the average cost per user.
Learn how cost reductions are estimated
All Providers
$ 483.1
$ 255.84 pupm reduction
53% reduction
$ 227.25
Cost pupm
All Providers
All Providers + citrix
Cost reductions
Type
Cost Pupm
Compute: Autoscale $233.00
Storage: Autoscale $22.85
Total $255.84
Costs by desktop type
123.49% higher for static desktops
Static
$ 157 pupm
Random
$ 70.25 pupm
$ 157
$ 70.25
Cost pupm
Persistent
Non persistent
Desktop type
Distinct users
Machines
Average monthly uptime
Static Persistent 1 5 43 h 24 min
Random Non persistent 1 5 33 h 24 min
Costs by machine OS type
123.49% higher for single-session OS machines
$ 157
$ 70.25
Cost pupm
Multi-session
Single-session
Machine OS type
Distinct users
Machines
Average monthly uptime
Single-session 1 5 43 h 24 min
Multi-session 1 5 33 h 24 min
Workloads by highest cost pupm
Only showing VM instances from Azure
VM Instance
Distinct users
Machines
Average monthly uptime
Cost pupm
Standard_D2as_v5 1 5 43 h 24 min $157.00
Standard_D2s_v3 1 5 33 h 24 min $70.25

成本摘要页面包括：

- **每用户平均成本**

  您可以查看过去六个月的每月实际每用户成本以及当月的预计成本。此外，您还可以查看工作负载的总成本以及站点上的独立用户数量。如果涉及多种货币，并且其中一种是美元，则成本以美元显示。否则，成本将以列表中随机选择的一种货币显示。与上个月和上上个月相比的成本节省以百分比形式提供。此外，还显示了独立用户数量的变化。图形表示显示了每个月的趋势。

  您可以使用每用户平均成本并优化使用情况。

- **成本报告**

  您可以查看所选服务提供商、所选交付组和所选标签的成本报告。您可以单独查看过去三个月的报告，也可以查看过去三个月数据的合并视图。

- **使用 Citrix 降低成本**

  您可以通过启用 Citrix 功能（例如 Autoscale 和 Machine Creation Services™ (MCS)、存储优化 (MCSIO)）来进一步降低每用户平均成本。此外，还应鼓励最终用户采取行动，例如在不使用时关闭计算机。

  此数据显示应用 Citrix 功能后的总节省。它还显示了最终用户操作带来的节省。

- **按桌面类型划分的成本**

  您可以查看以下桌面类型的成本：

  - **静态持久：** 用户每次登录到相同的虚拟桌面，并且对桌面所做的更改都会保存。
  - **静态非持久：** 用户每次登录到相同的虚拟桌面，并且对桌面所做的更改不会保存。
  - **随机持久：** 用户从桌面池中分配一个虚拟桌面，并且对桌面所做的更改会保存。
  - **随机非持久性：** 用户从桌面池中分配到一个虚拟桌面，并且对桌面所做的更改不会保存。

  您可以查看每种计算机类型的不同用户数、计算机数以及平均每月正常运行时间。

  您可以使用此数据并计划通过将用户移动到不同类型的桌面来节省成本。例如，与随机非持久性桌面相比，静态持久性桌面类型需要更多的资源使用。因此，您可以计划将一些用户从静态持久性桌面类型移动到随机非持久性桌面类型。

- **按操作系统类型划分的成本**

  您可以查看单会话和多会话操作系统类型的成本。您可以查看计算机操作系统类型、不同用户数、计算机数以及平均每月正常运行时间。您可以使用此数据并计划通过将用户移动到不同类型的操作系统来节省成本。

- **按每月每用户最高成本划分的工作负载**

  您可以查看每月每用户最高成本的详细信息，包括虚拟机实例、不同用户数以及计算机的平均正常运行时间。此外，您还可以查看计算机数量和每用户成本。

  使用此数据查看每种虚拟机配置类型的成本，并决定将哪些配置分配给用户。

Azure 工作负载的成本建模

新的成本建模功能支持 Azure 工作负载，并根据使用模式提供建议。客户会收到关于 Azure 预留或节省计划哪种更适合提供最大成本节约的建议。Azure 预留客户以折扣固定成本预先预留特定数量的机器，而节省计划则允许他们承诺一定金额以获得折扣费率。该功能分析过去 28 天的数据以提供估算建议。这有助于客户通过对资源分配做出明智决策来节省成本。

> **注意：**

> 为了获得最佳估算，建议使用过去 28 天来自稳定环境的数据。避免使用来自异常活动期间的数据，例如假期或使用量突然激增。请等到您的使用量恢复到基线水平后再采纳这些建议。

> **优点：**

- 提供量身定制的成本节约建议。
- 支持预留和节省计划。
- 分析近期使用数据以提供准确见解。
- 有助于优化资源分配并降低开支。
- 在选择交付组、标签、VM 系列和区域方面提供灵活性。

> **注意：**

> 成本建模仅支持 Azure 工作负载。

计划类型

在 Azure 中，有两种节省成本的计划类型：

- **Azure Reservations**：客户决定预先保留多少台计算机。预留的固定成本与即用即付成本相比，具有不同的折扣费率。

- **Savings Plan**：客户承诺支付特定金额，而不是承诺购买特定数量的计算机。在该金额用完之前，他们将按折扣成本计费。之后，他们将支付即用即付成本。

“**成本建模**”页面为每个计划独立提供建议，显示潜在的节省。

单击“**成本优化 > 成本建模**”。此时将显示“**成本模型和云工作负载**”页面。

citrix | DaaS Premium | 0 - Production

DaaS > Monitor > Cost optimization

Try unified search | Search | 1 - Production

Cost optimization New

Cost summary | Cost savings | Workload rightsizing | Cost modeling

Export data

Cost model cloud workloads

We recommend that you filter only by long-term-use machines and production workloads. Delivery groups and machines used for testing or short-term use may skew the cost model results.

All delivery groups | Select tag | All VM series | All regions

Apply filters | Note: All filters are applied with **AND** operator

Data up to 04/03/2025 9:56 AM | Download report

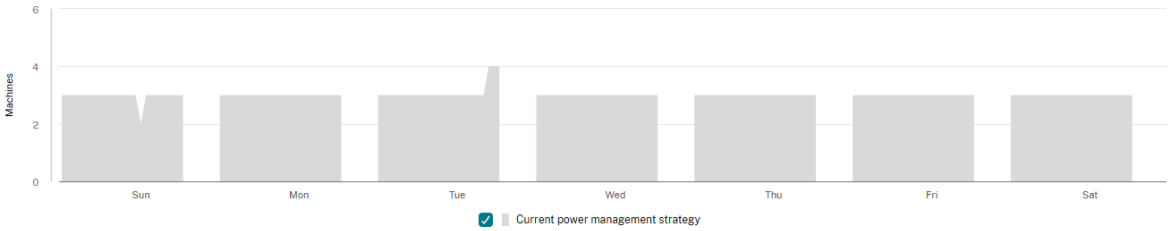
Cost model based on power management strategy

Choose from various Autoscale power management strategies to visualize concurrent machine consumption and savings opportunities.

No changes to Autoscale	Potential changes to Autoscale	
Current power management strategy Analyze potential savings opportunities by utilizing the existing Autoscale configuration.	**Deallocate machines at session end** Analyze potential savings opportunities if Autoscale is configured to deallocate machines at the end of a user's session. **95.45% reduced machine consumption**	**Deallocate machines for inactive session** Analyze potential savings opportunities if Autoscale is configured to deallocate machines when a session is inactive. **99.01% reduced machine consumption**

Concurrent machine consumption

Concurrent machine consumption is analyzed based on the last 28 days of historical consumption.



Savings opportunity

Determine the best commitment strategy and term length based on the selected power management strategy. View cost analysis

	Reserved instances		Savings plan	
	1 year	3 year	1 year	3 year
Potential savings opportunity	**40 %** Save up to $2,717.07 / yr	**61 %** Save up to $4,142.95 / yr	**31 %** Save up to $2,074.39 / yr	**53 %** Save up to $3,570.76 / yr
Commitment	$3,978.07 / yr	$2,552.20 / yr	$4,620.75 / yr	$3,124.39 / yr
Pay as you go	$72.58 / yr	$72.58 / yr	$72.58 / yr	$72.58 / yr
Total	**$4,050.65 / yr**	**$2,624.78 / yr**	**$4,693.33 / yr**	**$3,196.97 / yr**

Recommendations

Review the recommended changes to your commitment strategy based on the term length.

			Machines to be reserved		Savings plan hourly commitment (USD)	
Virtual machine series	Region	Current machines	1 year	3 year	1 year	3 year
Standard_D4s_v3	eastus	727	2	2	$0.26 / hr	$0.18 / hr
Standard_D8as_v4	eastus	21	1	1	$0.26 / hr	$0.18 / hr

Analyze per virtual machine series

Validate the optimum number of machines required per series by correlating with respective cost per user.

Virtual machine series

Standard_D4s_v3 in eastus

Export analysis



您可以根据需要选择所有交付组，最多 15 个（或实际数量）交付组，并排除最多 15 个（或实际数量）交付组。您可以从下拉列表中选择“**所有单会话**”或“**所有多会话**”。您还可以按“**标签**”、“**VM 系列**”和“**区域**”进行筛选。如果您未选择任何选项，则分析默认对整个适用数据集运行，并考虑过去 28 天的数据。

> **注意：**
>
> 成本建模建议基于过去 28 天的数据，并假设此期间的行为保持一致。

电源管理策略

数据分析因所选电源管理策略而异。您可以选择以下 Autoscale™ 电源管理策略之一，以可视化并发计算机消耗和节省机会：

- **当前电源管理策略**：选择此策略可使用现有 Autoscale 配置分析潜在节省。Autoscale 配置没有变化。建议的成本建模是根据当前 Autoscale 设置生成的，计算所有正在运行的计算机的成本。
- **在会话结束时解除分配计算机**：如果您愿意更改 Autoscale 配置以在用户会话结束时解除分配计算机以分析潜在节省，请选择此策略。建议的成本建模是根据更新的 Autoscale 配置生成的，仅计算活动会话时间的成本，忽略断开连接时间。
- **为非活动会话解除分配计算机**：如果您愿意更改 Autoscale 配置以在会话非活动时解除分配计算机以分析潜在节省，请选择此策略。建议的成本建模是根据更新的 Autoscale 配置生成的，仅计算会话处于活动状态而非空闲状态的时间的成本。

例如，如果计算机运行了 60 分钟，会话断开连接了 20 分钟，则剩余的 40 分钟是活动会话时间。如果用户在活动会话期间空闲了 10 分钟，则净使用时间仅为 30 分钟。

- 在“**当前电源管理策略**”中，净使用时间为 60 分钟。
- 在**会话结束时解除分配机器策略**中，不包括断开连接时间的净使用量为 40 分钟。
- 在**非活动会话解除分配机器策略**中，包括空闲时间在内的净使用量为 30 分钟。

这些标准作为分析的基准。这些策略有助于更准确地确定机器的净使用量。

机器消耗和建议

成本建模页面提供了有关机器消耗和建议的以下详细信息：

- **并发机器消耗图**：此图显示过去 28 天的基线使用情况，每个条形代表一周中的一天。基线是使用使用量的第 75 百分位 (p75) 计算的，这是一种类似于平均值或中位数的聚合指标。例如，对于每天和每小时（例如星期二上午 10 点），基线是通过分析前四个星期二上午 10 点的数据的

p75 来确定的。此过程对一周中的所有小时和天重复。将鼠标悬停在图表上，可以查看当前电源管理策略下消耗的机器数量，以及在应用 Autoscale 潜在更改时所选策略下消耗的机器数量。

- **节省机会**：查看 Azure 预留和节省计划在一年期和三年期内的潜在节省机会。将显示**承诺**和**即用即付**选项的节省机会。
- **建议**：查看对 Azure 预留和节省计划的建议更改。建议包括每个计划在所有适用的虚拟机系列、类型和区域组合下的承诺。数据适用于一年期和三年期。

按虚拟机系列分析

从下拉列表中选择虚拟机系列，以验证每用户成本方面的最佳机器数量。每月每用户成本是预计的每月每用户成本估算值。此估算有助于客户了解，如果他们在 Azure 预留下预留特定数量的机器，或在**节省计划**下承诺特定的每小时美元金额，则预计的每月每用户成本。查看 Azure 预留实例和节省计划每小时承诺的每用户成本。图表显示了各种预留级别（从**无预留**到**完全预留**，包括**最佳预留**）和每小时成本承诺级别（从**无承诺**到**最大承诺**，包括**最佳承诺**）的数据点。

成本建模页面提供了宝贵的见解和建议，可帮助客户优化其 Azure 工作负载并节省成本。通过分析使用模式并选择适当的计划，客户可以实现显著的节省。

功能兼容性矩阵

Citrix Director 7 2503 与以下版本兼容：

- Citrix Virtual Apps and Desktops™ 7 2112 及更高版本
- 思杰虚拟应用和桌面™ 7 1912 LTSR

在每个站点中，尽管您可以将 Director 与早期版本的 Delivery Controller™ 结合使用，但最新版本 Director 中的所有功能可能无法使用。Citrix 建议 Director、Delivery Controller 和 VDA 保持相同版本。

> **注意：**
>
> 升级 Delivery Controller 后，打开 Studio 时会提示您升级站点。有关详细信息，请参阅升级过程中的**升级顺序**部分。
>
> Director 升级后首次登录时，会对配置的站点执行版本检查。如果任何站点运行的 Controller 版本早于 Director 版本，Director 控制台上会显示一条消息，建议升级站点。此外，只要站点版本低于 Director 版本，Director 控制板上就会一直显示一条说明，指示此不匹配。

注意：

早期版本的 Citrix Director 不显示应用于在最新 VDA 版本上运行的用户会话的策略。Citrix Director 1912 及更早版本不显示应用于在 VDA 2003 及更高版本上运行的用户会话的策略。请使用 Citrix Director 2003 及更高版本查看这些策略。

下面列出了特定的 Director 功能，以及所需的 Delivery Controller (DC)、VDA 和其他依赖组件的最低版本以及许可证版本。

DIRECTOR 版本	功能	依赖项 - 所需最低版本	版本
2507	用于监视和故障排除的 Microsoft 呼叫质量仪表板	无	所有
2507	改进了对垂直和水平负载平衡警报的处理	无	所有
2507	会话拓扑中使用的端点数据收集的默认策略行为更改	无	所有
2507	Director 中 ICA RTT 和网络延迟测量的增强定义(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/troubleshoot-deployments/user-issues/session-performance.html#hdx-metrics.html)	无	所有
2507	针对实时通信应用程序的插件管理器和优化状态的增强可视性(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/troubleshoot-deployments/user-	无	所有

DIRECTOR 版本	功能	依赖项 - 所需最低版本	版本
	issues/session-performance.html#real-time-communications-optimization-visibility.html)		
2503	Azure 工作负载的成本建模	无	所有
2503	成本节约页面增强功能	无	所有
2503	Director 与 uberAgent 集成(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/install-and-configure.html#citrix-uberagent-integration-with-director)	VDA 2503（已安装 uberAgent）	所有
2503	本地应用程序使用情况报告(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/site-analytics/application-usage-monitoring.html)	VDA 2503	白金许可站点
2503	监控 VDA 登录持续时间详细信息	VDA 2503	所有
2503	针对 Provisioning Service 的附加指标收集(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/infrastructure-	VDA 2503	所有

DIRECTOR 版本	功能	依赖项 - 所需最低版本	版本
	monitoring/infrastructure-dashboard.html#provisioning-service-health-metrics)		
2503	将 HDX 优化监控扩展到 Microsoft Teams 之外的选项	VDA 2503	所有
2503	筛选器视图和会话性能选项卡中的会话自动重新连接详细信息	VDA 2503	所有
2503	Citrix Director 的统一平台体验	无	所有
2503	用于限制用户操作的批量操作选项的自定义角色	无	所有
2503	为 Provisioning Service 和 Delivery Controller 设置站点级别警报的规定	VDA 2503	所有
2503	与 Webhook 集成(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/integrations-and-data-exports.html#integrations-with-alerting-and-itsm-tools)	无	所有
2411	应用程序页面上使用最少和未使用的已发布应用程序报告(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/site-	DDC 7.16, VDA 7.15	白金许可站点

DIRECTOR 版本	功能	依赖项 - 所需最低版本	版本
	analytics/application-usage-monitoring.html#least-used-and-unused-published-apps-report)		
2411	活动管理器上 TCP 或 UDP 应用程序的枚举应用程序详细信息(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/spa-integration-with-director.html#session-topology-view-for-secure-private-access-apps.)	VDA 2411 和 DDC 2411	所有
2411	使用 PowerShell SDK 配置 Webhook	VDA 2411 和 DDC 2411	所有
2411	批量警报解除	VDA 2411 和 DDC 2411	所有
2411	在工作负载优化页面中的机器净活跃使用量	无	所有
2411	通过优化存储使用实现的成本节约 (预览)	无	所有
2411	成本摘要 (预览)	无	所有
2411	Delivery Controller 监控 (预览)	VDA 2411	所有
2411	从 UI 连接 Citrix 组件 (预览)	VDA 2411	所有

DIRECTOR 版本	功能	依赖项 - 所需最低版本	版本
2407	成本优化	无	所有
2407	集成和数据导出	VDA 2407	所有
2407	诊断历史用户会话（预览）	VDA 2407	所有
2407	Secure Private Access 会话的活动管理器（预览版）	VDA 2407	所有
2407	Director 与 TCP 和 UDP 应用程序的 Secure Private Access 集成（预览版）	VDA 2407	所有
2407	基础设施监控（预览版）	VDA 2407	所有
2407	未注册计算机警报(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/site-analytics/alerts-notifications.html#unregistered-machines-in-)	VDA 2407 和 DDC 2407	所有
2407	计算机正常运行时间警报	VDA 2407 和 DDC 2407	所有
2407	开机失败操作和关机失败操作警报	VDA 2407 和 DDC 2407	所有
2407	在警报电子邮件中包含 CSV 附件以及在警报 Webhook 中包含 JSON 有效负载的功能(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/	VDA 2407 和 DDC 2407	所有

DIRECTOR 版本	功能	依赖项 - 所需最低版本	版本
	director/site-analytics/alerts-notifications.html#enhancements-on-alert-content)		
2407	检查最近执行电源操作的计算机	VDA 2407	所有
2407	高级警报策略	VDA 2407 和 DDC 2407	所有
2407	针对云用户和本地用户的统一搜索(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/unified-search.html)	DDC 2407	所有
2407	仪表板上的已发布应用程序使用情况监控图表(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/site-analytics/application-usage-monitoring.html)	VDA 2407 和 DDC 2407	白金许可站点
2402 LTSR	Director 与 Web 和 SaaS 应用程序的 Secure Private Access 集成（预览版）	VDA 2402 LTSR	所有

DIRECTOR 版本	功能	依赖项 - 所需最低版本	版本
2402 LTSR	支持 Microsoft Teams 2.1 版或更早版本(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/troubleshoot-deployments/user-issues.html#microsoft-teams-optimization-status)	VDA 2402 LTSR	所有
2311	播放实时和录制会话(/zh-cn/citrix-virtual-apps-desktops/2607-ltsr/director/troubleshoot-deployments/user-issues/record-sessions.html#play-back-live-and-recorded-sessions)	VDA 2308 和 DDC 2311	所有
2311	会话拓扑和性能指标	多个版本 - 链接	所有
2311	最佳屏幕分辨率	无	所有
2311	MS Teams 优化	VDA 2311 和 DDC 最新版本	所有
2311	探测器概览增强功能	无	所有
2311	重新设计的会话登录持续时间视图	无	所有
2308	探测摘要和深入分析	无	所有
2308	Citrix Probe Agent 对 Citrix Gateway 多重身份验证的支持	思杰网关	所有
2308	禁用管理程序警报	无	所有

DIRECTOR 版本	功能	依赖项 - 所需最低版本	版本
2308	会话体验指标趋势	无	所有
2305	通过 Citrix Gateway 支持身份验证	无	所有
2305	Director 中的自动缩放管理	无	所有
2303	故障计算机警报	DC 7 2303	高级版
2203	支持 TLS 1.3	-	所有
2212	AMD GPU 可用的实时 GPU 利用率	运行 64 位 Windows 并启用 HDX 3D Pro 的 DC 7.14 和 VDA 7.14	所有
2212	高级探测计划	DC 7 1906 和 思杰探测代理 2209	高级版
1909	使用 Citrix Analytics for Performance 配置本地站点	DC 7 1906 和 VDA 1906	所有
1906	会话自动重新连接	DC 7 1906 和 VDA 1906	所有
1906	会话启动持续时间	DC 7 1906 和 VDA 1903	所有
1906	桌面探测	交付控制器 7 1906 和 Citrix 探测代理 1903	高级版
7.9 及更高版本	配置文件加载中的 Citrix Profile Management 持续时间	VDA 1903	所有
1811	配置文件深入分析	DC 7 1811 和 VDA 1811	所有

DIRECTOR 版本	功能	依赖项 - 所需最低版本	版本
1811	管理程序警报监控	DC 7 1811	高级版
1811	应用程序探测	DC 7 1811 和 Citrix 应用程序探测代理 1811	高级版
1811	Microsoft RDS 许可证运行状况	DC 7 1811 和 VDA 7.16	所有
1811	关键 RTOP 数据显示	DC 7 1811 和 VDA 1808	高级版
1808	导出筛选器数据	DC 7 1808	所有
1808	交互式会话深入分析	DC 7 1808 和 VDA 1808	所有
1808	GPO 深入分析	DC 7 1808 和 VDA 1808	所有
1808	使用 OData API 获取计算机历史数据	DC 7 1808	所有
7.18	应用程序探测	DC 7.18	高级版（以前称为白金版）
7.18	智能警报策略	DC 7.18	高级版（以前称为白金版）
7.18	健康助手链接	无	所有
7.18	交互式会话深入分析	无	所有
7.17	PIV 智能卡身份验证	无	所有
7.16	应用程序分析	DC 7.16 和 VDA 7.15	所有
7.16	OData API 版本 4	DC 7.16	所有
7.16	影子 Linux VDA 用户	VDA 7.16	所有
7.16	域本地组支持	无	所有

DIRECTOR 版本	功能	依赖项 - 所需最低版本	版本
7.16	计算机控制台访问	DC 7.16	所有
7.15	应用程序故障监控	DC 7.15 和 VDA 7.15	所有
7.14	以应用程序为中心的故障排除	DC 7.13 和 VDA 7.13	所有
7.14	磁盘监控	DC 7.14 和 VDA 7.14	所有
7.14	GPU 监控	DC 7.14 和 VDA 7.14	所有
7.13	会话详细信息面板上的传输协议	DC 7.x 和 VDA 7.13	所有
7.12	用户友好的连接和计算机故障描述	DC 7.12 和 VDA 7.x	所有
7.12	企业版中历史数据可用性增加	DC 7.12 和 VDA 7.x	企业
7.12	自定义报告	DC 7.12 和 VDA 7.x	高级版（以前称为白金版）
7.11	资源利用率报告	DC 7.11 和 VDA 7.11	所有
7.11	CPU、内存和 ICA RTT 条件的警报扩展	DC 7.11 和 VDA 7.11	Premium（以前称为 Platinum）
7.11	导出报告改进	DC 7.11 和 VDA 7.x	所有
7.11	与 Citrix ADM 集成	DC 7.11、VDA 7.x 和 MAS 版本 11.1 Build 49.16	高级版（以前称为白金版）
7.9	登录持续时间细分	DC 7.9 和 VDA 7.x	所有
7.7	主动监控和警报	DC 7.7 和 VDA 7.x	高级版（以前称为白金版）
7.7	Windows 身份验证集成	DC 7.x 和 VDA 7.x	所有

DIRECTOR 版本	功能	依赖项 - 所需最低版本	版本
7.7	单会话和多会话操作系统使用情况	DC 7.7 和 VDA 7.x	高级版（以前称为白金版）
7.6.300	支持 Framehawk 虚拟通道	DC 7.6 和 VDA 7.6	所有
7.6.200	会话录制集成	DC 7.6 和 VDA 7.x	高级版（以前称为白金版）
7	HDX Insight 集成	交付控制器 7.6、虚拟投递代理 7.x 以及 Citrix ADM	高级版（以前称为白金版）

数据粒度和保留

数据值的聚合

Monitor Service 收集各种数据，包括用户会话使用情况、用户登录性能详细信息、会话负载平衡详细信息以及连接和计算机故障信息。数据根据其类别以不同方式聚合。了解使用 OData 方法 API 呈现的数据值的聚合对于解释数据至关重要。例如：

- 连接会话和计算机故障在一段时间内发生。因此，它们以该时间段内的最大值形式公开。
- 登录持续时间是时间长度的度量，因此以该时间段内的平均值形式公开。
- 登录计数和连接故障是该时间段内发生次数的计数，因此以该时间段内的总和形式公开。

并发数据评估

会话必须重叠才能被视为并发。但是，当时间间隔为 1 分钟时，该分钟内的所有会话（无论是否重叠）都被视为并发。间隔的大小如此之小，以至于计算精度所涉及的性能开销不值得其增加的价值。如果会话发生在同一小时内，但不在同一分钟内，则不被视为重叠。

汇总表与原始数据的关联

数据模型以两种不同的方式表示指标：

- 汇总表以每分钟、每小时和每天的时间粒度表示指标的聚合视图。
- 原始数据表示在会话、连接、应用程序和其他对象中跟踪的单个事件或当前状态。

在尝试跨 API 调用或在数据模型本身中关联数据时，了解以下概念和限制非常重要：

- **部分间隔无汇总数据。** 指标汇总旨在满足长期历史趋势的需求。这些指标会聚合到汇总表中以用于完整间隔。在数据收集的开始（最旧的可用数据）和结束时，没有部分间隔的汇总数据。当查看一天的聚合（Interval=1440）时，这意味着第一个和最近的不完整天数没有任何数据。尽管原始数据可能存在于这些部分间隔中，但它从不进行汇总。您可以通过从特定汇总表中提取最小和最大 SummaryDate 来确定特定数据粒度的最早和最晚聚合间隔。SummaryDate 列表示间隔的开始。Granularity 列表示聚合数据的间隔长度。
- **按时间关联。** 指标会聚合到汇总表中以用于完整间隔，如上一节所述。它们可用于历史趋势，但原始事件的状态可能比为趋势分析汇总的数据更具时效性。任何基于时间的汇总数据与原始数据的比较都必须考虑到，对于可能发生的部分间隔或时间段的开始和结束，没有汇总数据。
- **遗漏和延迟事件。** 如果事件在聚合期间被遗漏或延迟，聚合到摘要表中的指标可能会略有不准确。尽管监控服务尝试维护准确的当前状态，但它不会回溯时间来重新计算摘要表中遗漏或延迟事件的聚合。
- **连接高可用性。** 在连接高可用性期间，当前连接的摘要数据计数中会出现空白，但会话实例仍将在原始数据中运行。
- **数据保留期。** 摘要表中的数据与原始事件数据的清理计划不同。数据可能因已从摘要表或原始表中清理而丢失。不同粒度的摘要数据，其保留期也可能不同。较低粒度的数据（分钟）比较高粒度的数据（天）清理得更快。如果由于清理导致某个粒度的数据丢失，则可能在较高粒度中找到。由于 API 调用只返回请求的特定粒度，因此某个粒度没有数据并不意味着同一时间段内较高粒度的数据不存在。
- **时区。** 指标以 UTC 时间戳存储。摘要表按小时时区边界进行聚合。对于不落在小时边界上的时区，数据聚合的位置可能会存在一些差异。

粒度和保留

Director 检索的聚合数据的粒度是所请求的时间 (T) 跨度的函数。规则如下：

- 0 \< T \<= 1 小时 - 使用每分钟粒度
- 0 \< T \<= 30 天 - 使用每小时粒度
- T \> 31 天 - 使用每日粒度

未从聚合数据中获取的请求数据来自原始会话和连接信息。此类数据往往增长迅速，因此有其自己的清理设置。清理可确保仅保留长期相关的有用数据。清理可确保更好的性能，同时保持报告所需的粒度。Premium 许可站点的客户可以将其清理保留期更改为所需的保留天数，否则将使用默认值。如果与站点数据库失去连接，监控服务将使用下表中指定的 Premium 授权的默认保留天数。

要访问这些设置，请在 Delivery Controller™ 上运行以下 PowerShell 命令：

```
asnp Citrix.*

 Get-MonitorConfiguration

 Set-MonitorConfiguration -<setting name> <value>
```

#	设置名称	受影响的架构表	监控页面中受影响的表和图表	PREMIUM 的保留天数	ADVANCED 的保留天数
1	GroomSessionsRetentionDays	MonitorData.Session 和 Monitordata.Connection 表	此设置会影响趋势页面上的会话详细信息、按用户会话划分的登录持续时间、基于应用程序的使用情况表。	90	31
2	GroomFailuresRetentionDays	MonitorData.MachineFailureLog 和 MonitorData.ConnectionFailureLog	趋势页面：此设置会影响故障选项卡上的图表和表格。	90	31
3	GroomLoadIndexesRetentionDays	MonitorData.LoadIndex	此设置会影响趋势页面上“负载评估器索引”选项卡中显示的数据。	3	3
4	GroomDeletedRetentionDays	LifecycleState 为“已删除”的 MonitorData.Machine、MonitorData.Catalog、	LifecycleState 为“已删除”的 Machine、Catalog、DesktopGroup 和	90	31

#	设置名称	受影响的架构表	监控页面中受影响的表和图表	PREMIUM 的保留天数	ADVANCED 的保留天数
		MonitorData.DesktopGroup 和 MonitorData.Hypervisor 实体。此设置还会删除任何相关的会话、会话详细信息、摘要、故障或负载索引记录。	Hypervisor 实体。此设置还会删除任何相关的会话、会话详细信息、摘要、故障或负载索引记录。		
5	GroomSummariesRetentionDays	MonitorData.DesktopGroupSummary、MonitorData.FailureLogSummary 和 MonitorData.LoadIndexSummary	此设置影响“趋势”页面上的所有图表数据。	365	31
6	GroomMachineHotfixLogRetentionDays	MonitorData.Hotfix	此设置影响“计算机详细信息”页面上显示的 VDA 热修复数据。	90	31
7	GroomMinuteRetentionDays	所有摘要表	此设置影响“趋势”页面上显示的“最近 2 小时”时间段的图表。	3	3

#	设置名称	受影响的架构表	监控页面中受影响的表和图表	PREMIUM 的保留天数	ADVANCED 的保留天数
8	GroomHourlyRetentionDays	所有摘要表	这会影响“趋势”页面上显示的每周图表。	32	31
9	GroomApplicationInstanceRetentionDays	MonitorData.ApplicationInstance	此设置会影响容量管理选项卡上的图表和表格以及趋势页面上的应用程序使用情况表。	90	不适用
10	GroomNotificationLogRetentionDays	MonitorData.NotificationLog	此设置会影响 Monitor 上显示的警报。	90	不适用
11	GroomResourceUsageRawDataRetentionDays	MonitorData.Resourceutilization	此设置影响在“历史计算机利用率”计算机详细信息页面中看到的 CPU 和内存图表，以及成本优化区域“工作负载调整大小”选项卡上的数据计算。	3	3
12	GroomResourceUsageMinuteDataRetentionDays	MonitorData.ResourceUtilizationSummary	此设置会影响“历史计算机利用率”计算机详细信息页面中显示的“最近 2	7	7

#	设置名称	受影响的架构表	监控页面中受影响的表和图表	PREMIUM 的保留天数	ADVANCED 的保留天数
			小时”时间段的 CPU 和内存图表，以及成本优化区域“工作负载规模调整选项卡”上的数据计算。		
13	GroomResourceUsageHourDataRetentionDays	MonitorData.Resourceutilizationsummary	此设置影响在“历史计算机利用率”计算机详细信息页面中看到的 CPU 和内存图表，以及成本优化区域“工作负载调整大小”选项卡上的数据计算。	30	30
14	GroomResourceUsageDayDataRetentionDays	MonitorData.Resourceutilizationsummary	此设置影响在“趋势”页面上的计算机“资源利用率”中以及特定计算机的“计算机利用率”页面中看到的 CPU 和内存图表。	365	31

#	设置名称	受影响的架构表	监控页面中受影响的表和图表	PREMIUM 的保留天数	ADVANCED 的保留天数
15	GroomProcessUsageRawDataRetentionDays	MonitorData.ProcessUtilization	此设置影响显示在计算机历史使用情况页面上的每个进程的资源趋势信息。	1	1
16	GroomProcessUsageMinuteDataRetentionDays	MonitorData.ProcessUtilizationMinuteSummary	此设置影响“历史计算机利用率”页面上显示的“最近 2 小时”的每个进程的 CPU 和内存使用情况图表。	3	3
17	GroomProcessUsageHourDataRetentionDays	MonitorData.ProcessUtilizationHourSummary	此设置会影响在计算机历史使用情况页面上显示的每个进程的 CPU 和内存使用趋势。	7	7
18	GroomProcessUsageDayDataRetentionDays	MonitorData.ProcessUtilizationDaySummary	此设置会影响在计算机历史使用情况页面上显示的每个进程的 CPU 和内存使用趋势。	30	30
19	GroomSessionMetricsDa	MonitorData.Sessionmetrics	此设置会影响用户详细信息页面“会	1	1

#	设置名称	受影响的架构表	监控页面中受影响的表和图表	PREMIUM 的保留天数	ADVANCED 的保留天数
	taRetentionDays		话性能”选项卡上显示的所有图表。		
20	GroomMachineMetricDataRetentionDays	MonitorData.Machinemetrics	此设置会影响“趋势”页面上“资源利用率”选项卡中的图表和表格。	3	3
21	GroomMachineMetricDaySummaryDataRetentionDays	MonitorData.MachineMetricDaySummary	此设置会影响“趋势”页面上“资源利用率”选项卡中的图表和表格。	365	31
22	GroomApplicationErrorsRetentionDays	MonitorData.ApplicationError	此设置会影响“应用程序”页面上“应用程序错误”列中显示的错误详细信息。	1	1
23	GroomApplicationFaultsRetentionDays	MonitorData.Applicationfailure	此设置会影响“应用程序”页面上“应用程序故障”列。	1	1

注意：

修改 Monitor Service 数据库上的值需要重新启动服务才能使新值生效。建议您仅在 Citrix 支持的指导下对 Monitor Service 数据库进行更改。

> 设置 GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays 和 GroomSessionMetricsDataRetentionDays 限制为默认值 1，而 GroomProcessUsageMinuteDataRetentionDays 限制为默认值 3。用于设置这些值的 PowerShell 命令已被禁用，因为进程使用数据往往会快速增长。 此外，基于许可证的保留设置如下：

- **高级版许可站点 -** 所有设置的清理保留期限制为 1000 天（Citrix 建议 365 天）。
- **高级许可站点 -** 所有设置的清理保留期限制为 31 天。
- **所有其他站点 -** 所有设置的清理保留期限制为 7 天。

例外：

- GroomApplicationInstanceRetentionDays 只能在高级许可站点中设置。
- GroomApplicationErrorsRetentionDays 和 GroomApplicationFaultsRetentionDays 在高级许可站点中限制为 31 天。

长期保留数据对表大小有以下影响：

- **每小时数据。** 如果允许每小时数据在数据库中保留长达两年，一个拥有 1000 个交付组的站点可能导致数据库按如下方式增长：

  1000 个交付组 × 24 小时/天 × 365 天/年 × 2 年 = 17,520,000 行数据。聚合表中如此大量的数据对性能的影响是显著的。鉴于仪表板数据是从此表中提取的，对数据库服务器的要求可能很高。过大的数据量可能会对性能产生巨大影响。
- **会话和事件数据。** 每次会话启动和建立连接/重新连接时收集的数据。对于大型站点（10 万用户），这些数据增长迅速。例如，这些表两年的数据量将超过 1 TB，需要高端企业级数据库。

集成和数据导出

Citrix Director 现在提供了一个新的 UI，用于集成和数据导出。此功能有助于提高对 Citrix Director 中可用的各种接口和第三方集成的认识。新引入的**集成和数据导出**页面列出了以下内容：

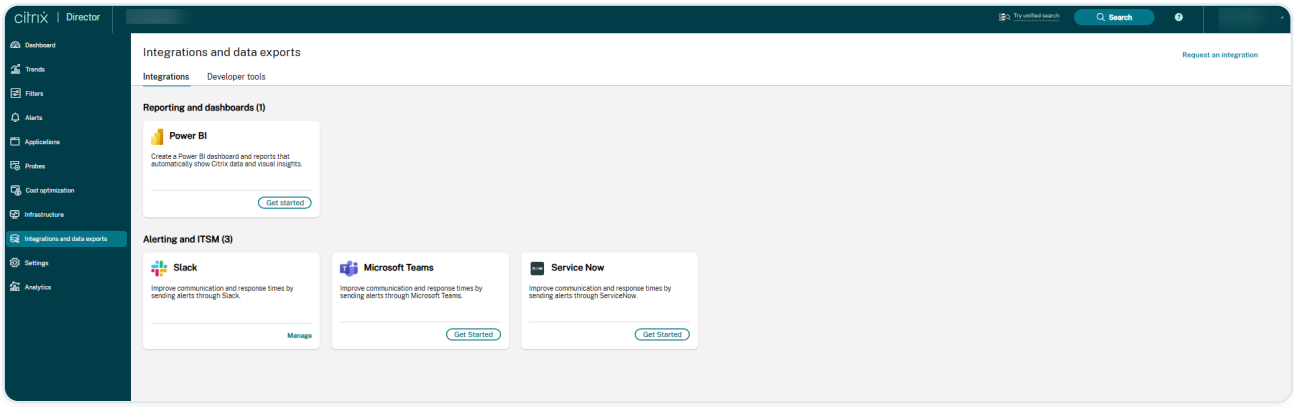
- 可用集成
- 支持的开发人员工具

此页面还描述了用于数据导出的 REST API 设置。此外，还提供了指南和文档的参考链接，以帮助您开始使用集成和开发人员工具。

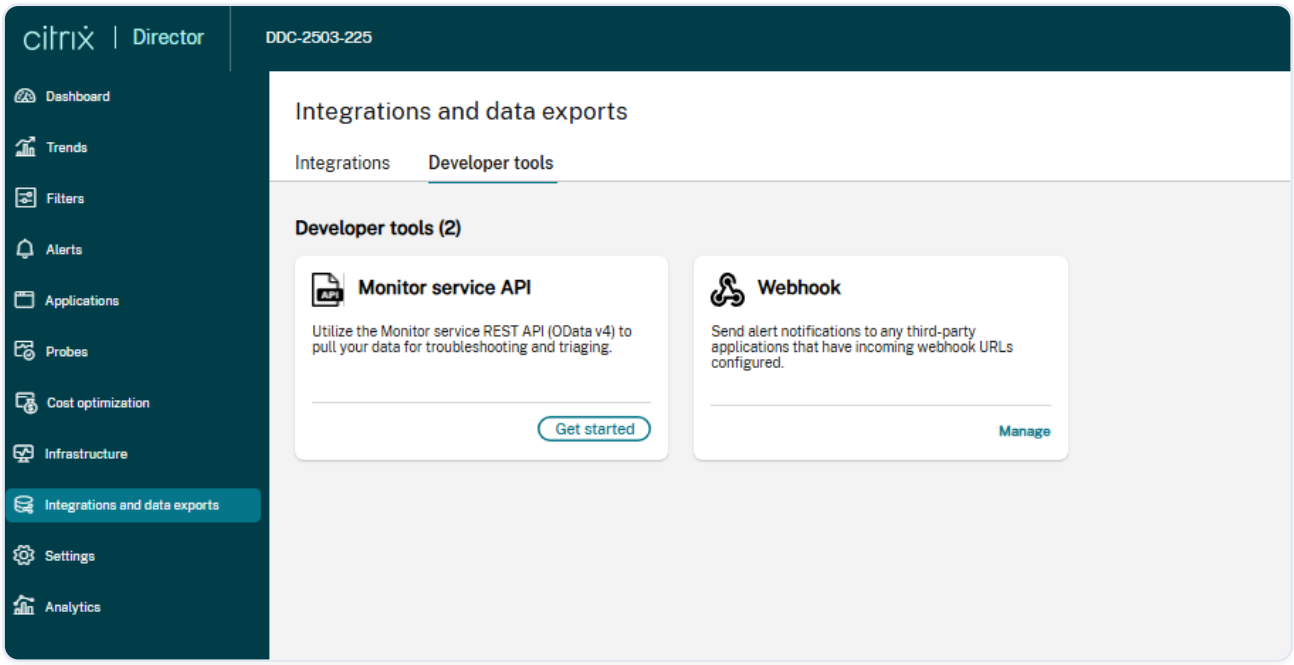
提供了以下集成选项用于收集 Citrix 监控指标：

- Citrix Monitor 服务 API - 您可以使用 Citrix Monitor 服务 API 从 Citrix Monitor 收集性能数据和事件，并将其导出到 Power BI。
- 警报和 ITSM - 您可以将警报通知发送到以下已配置传入 Webhook URL 的第三方应用程序：
  - 史拉克
  - 微软团队
  - ServiceNow

从左侧导航菜单中单击“**集成和数据导出**”。将显示“**集成和数据导出**”页面。



开发人员工具：



查看可用集成

“**集成**”选项卡显示了 Citrix Director 可用的集成。可用的集成分为以下几类：

- 报告和仪表板
- 警报和 ITSM

报告和仪表板

Power BI 可用于可视化通过 Citrix Director API 收集的指标。单击**开始使用**。将显示 **REST API** 开发人员工具详细信息页面。

单击 Monitor 服务 API 可获取有关其与 PowerBI 集成的资源和博客的参考链接。

此页面提供指向资源和博客的参考链接。

与警报和 ITSM 工具的集成

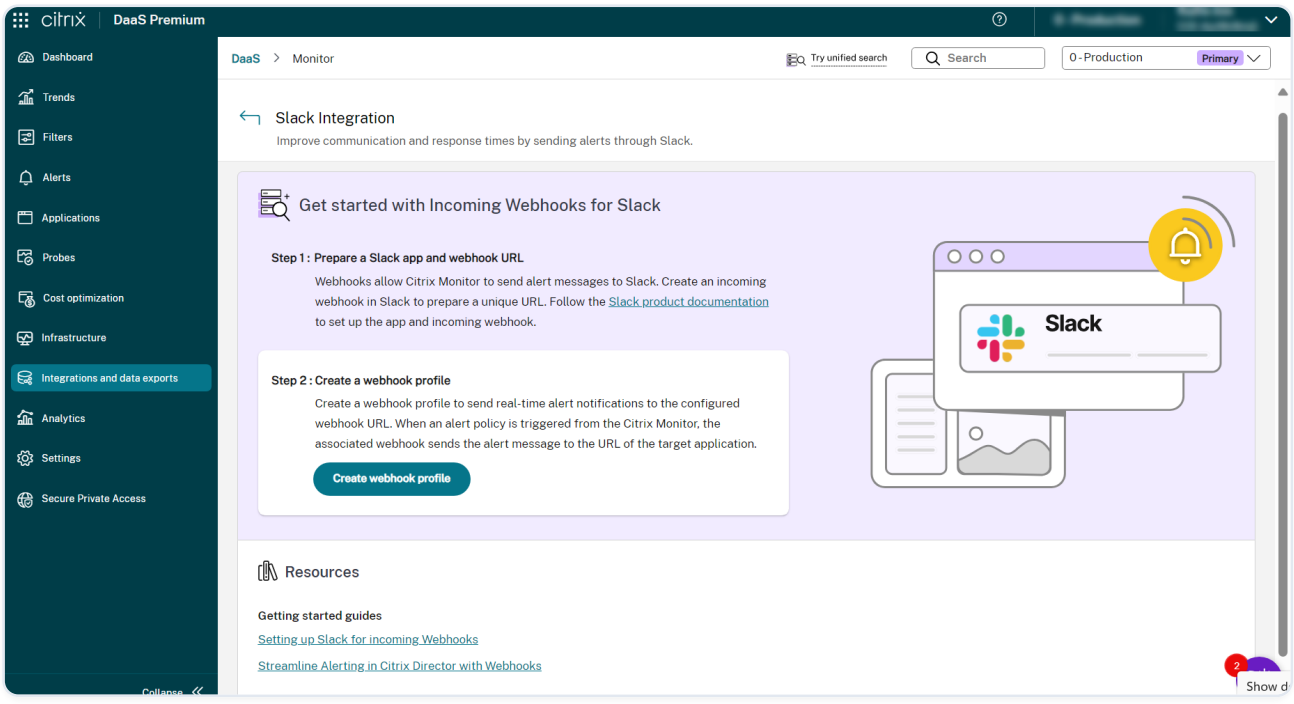
警报和 ITSM 工具包括：

- 史 Slack
- 微软团队
- ServiceNow

要将警报和 ITSM 工具与 Webhook 集成，请单击工具旁边的“**开始使用**”链接。此链接将打开特定警报和 ITSM 工具的集成页面，其中提供了有关先决条件和发送警报的具体步骤的详细信息。您可以设置工具和 Webhook URL。例如，要集成 Slack，您需要按照 Slack 文档创建频道和 Webhook URL。

完成此操作后，继续执行第二步以创建 Webhook 配置文件。

您还可以查阅参考资源。例如，与 Slack 集成的先决条件和说明如下：



与 Webhook 集成

1. 单击**集成**选项卡 > **警报和 ITSM** 部分 > 所选工具旁边的**开始使用**。该工具的**集成**页面随即打开。
2. 您可以访问资源和博客的参考链接。
3. 执行步骤 1。
4. 在步骤 2 中，单击**创建 Webhook 配置文件**。`<name of the tool>` **创建 Webhook 配置文件**页面随即显示。
5. 输入 Webhook 配置文件的**名称**。
6. 输入 Webhook 配置文件的**描述**。
7. 在**Webhook 配置**部分中选择所需的**方法**。
8. 根据上一步中选择的方法输入 **API/Webhook** URL。
9. 查看**消息**格式。
10. 在**标头**部分中添加键和值。
11. 单击**测试**以验证创建的 Webhook。
12. 如果 Webhook 验证成功，请单击**创建 Webhook**。Webhook 已创建。
13. 在 **开发人员工具** > **Webhook** > **管理** 中查看已创建的 Webhook 配置文件。**Webhook 配置文件开发人员工具详细信息**页面将打开。

您还可以在 **开发人员工具** > **Webhook** > **创建 Webhook 配置文件** 中创建 Webhook 配置文件。

将 Webhook 配置文件与 Citrix Alerts 集成

您可以在 **警报** > **高级警报策略** > **创建策略** 部分查看已创建的 Webhook 配置文件，并将其用作 Citrix Alerts 的一部分。

要将 Webhook 配置文件与新的 Citrix 警报策略集成，请执行以下操作：

1. 单击 **警报** > **高级警报策略** > **创建策略**。**创建高级警报策略**页面将显示。
2. 导航到 **通知渠道** > **使用 Webhook** 部分。
3. 选择 Webhook 配置文件。
4. 保存警报策略。

您可以通过执行以下操作将 Webhook 配置文件与现有警报策略集成：

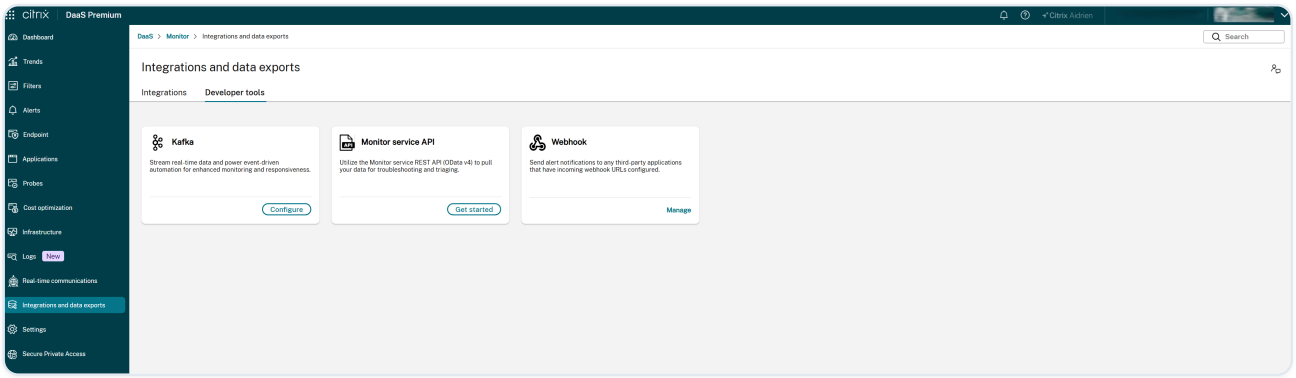
1. 单击 **警报** > **高级警报策略** > **编辑策略**。**编辑高级警报策略**页面将显示。
2. 导航到 **通知渠道** > **使用 Webhook** 部分。

3. 选择或更改 Webhook 配置文件。
4. 更新并保存警报策略。

查看支持的开发人员工具

点击“**开发人员工具**”选项卡以查看可用的开发人员工具。

可用的开发人员工具包括 Monitor 服务 API 和 Webhook。



Monitor 服务 API

单击“**开始使用**”。将打开“**Monitor 服务 API**”开发人员工具详细信息页面。您可以访问资源和博客的参考链接。

Web钩子

您可以在“**开发人员工具**”>“**Webhook**”>“**创建 Webhook 配置文件**”中查看和创建 Webhook 配置文件。

Citrix Director 故障原因和故障排除

以下表格描述了各种故障类别、原因以及解决问题所需采取的操作。有关详细信息，请参阅 枚举、错误代码和说明。

连接失败错误

类别	原因	问题	操作
N/A	[0] 未知。此错误代码未映射。	监控服务无法根据 Brokering 服务共享的信息确定报告的启动或连接失败的原因。	在控制器上收集 CDF 日志并联系 Citrix 支持。

类别	原因	问题	操作
[0] 无	[1] 无	无	N/A
[2] MachineFailure	[2] 会话准备	从交付控制器到 VDA 的会话准备请求失败。可能的原因：控制器与 VDA 之间的通信问题，Broker 服务在创建准备请求时遇到的问题，或导致 VDA 不接受请求的网络问题。	有关导致控制器与 VDA 之间通信问题的常见问题，请参阅知识中心文章 在 Citrix Virtual Apps and Desktops 中排查 Virtual Delivery Agent 与交付控制器的注册问题 中列出的故障排除步骤。
[2] MachineFailure	[3] 注册超时	VDA 已开机，但在尝试向交付控制器注册时发生超时。	验证 Citrix Broker Service 是否在交付控制器上运行，以及 Desktop service 是否在 VDA 上运行。如果已停止，请启动它们。
[1] ClientConnectionFailure	[4] 连接超时	VDA 准备好启动会话后，客户端未能连接到 VDA。会话已成功代理，但在等待客户端连接到 VDA 时发生超时。可能的原因：防火墙设置、网络中断或阻止远程连接的设置。	检查 Director 控制台，查看客户端当前是否有活动连接，这意味着没有用户受到影响。如果不存在会话，请检查客户端和 VDA 上的事件日志以查找任何错误。解决客户端和 VDA 之间的网络连接问题。
[4] 无可用许可证	[5] 许可	许可请求失败。可能的原因：许可证数量不足，或者许可证服务器已停机超过 30 天。	验证许可证服务器是否在线且可访问。解决与许可证服务器的任何网络连接问题，如果许可证服务器出现故障，请重新启动它。验证环境中是否有足够的许可证，并

类别	原因	问题	操作
			在必要时分配更多许可证。
[1] ClientConnectionFailure	[6] 票证	票证处理期间发生故障，表明客户端与 VDA 的连接与代理请求不匹配。启动请求票证由 Broker 准备并随 ICA® 文件一起交付。当用户尝试启动会话时，VDA 会使用 Broker 验证 ICA 文件中的启动票证。可能的原因：ICA 文件损坏或用户尝试进行未经授权的连接。	根据交付组中定义的用户组，验证用户是否可以访问应用程序或桌面。指示用户重新启动应用程序或桌面，以确定这是否是一次性问题。如果问题再次发生，请检查客户端设备的事件日志以查找错误。验证用户尝试连接的 VDA 是否已注册。如果未注册，请检查 VDA 上的事件日志并解决任何注册问题。
[1] ClientConnectionFailure	[7] 其他	客户端最初联系 VDA 后，但在完成连接序列之前，会话已报告为从 VDA 终止。	验证会话在启动前是否未被用户终止。尝试重新启动会话，如果问题仍然存在，请收集 CDF 日志并联系 Citrix 支持。
[1] ClientConnectionFailure	[8] 一般故障	会话启动失败。可能的原因：在代理仍在启动或初始化时请求了代理启动，或者在启动的代理阶段发生内部错误。	验证 Citrix Broker Service 正在运行，然后重试启动会话。
[5] 配置	[9] 维护模式	VDA 或 VDA 所属的交付组已设置为维护模式。	确定是否需要维护模式。如果不需要，请禁用相关交付组或计算机上的维护模式，并指示用户尝试重新连接。

类别	原因	问题	操作
[5] 配置	[10] 应用程序已禁用	最终用户无法访问该应用程序，因为它已被管理员禁用。	如果应用程序旨在用于生产环境，请启用该应用程序并指示用户重新连接。
[4] 无可用许可证	[11] 许可证功能被拒绝	正在使用的功能不在现有许可证的涵盖范围内。	请联系 Citrix 销售代表，确认现有 Citrix Virtual Apps and Desktops™ 许可证版本和类型涵盖的功能。
[3] NoCapacityAvailable	[13] 会话限制已达到	所有 VDA 都在使用中，没有容量来托管更多会话。可能的原因：所有 VDA 都在使用中（对于单会话操作系统 VDA），或者所有 VDA 都已达到配置的最大并发会话数（对于多会话操作系统 VDA）。	验证是否有任何 VDA 处于维护模式。如果不需要，请禁用维护模式以释放更多容量。考虑增加 Citrix 策略设置中**最大会话数**的值，以允许每个服务器 VDA 承载更多会话。考虑添加更多多会话操作系统 VDA。考虑添加更多单会话操作系统 VDA。
[5] 配置	[14] 不允许的协议	不允许使用 ICA 和 RDP 协议。	在交付控制器上运行 **Get-BrokerAccessPolicyRule** PowerShell 命令，并验证 **AllowedProtocols** 值是否列出了所有所需的协议。此问题仅在配置错误时发生。
[5] 配置	[15] 资源不可用	用户尝试连接的应用程序或桌面不可用。此应用程序或桌面可能不存在，或者没有可用的 VDA 来运行	验证应用程序或桌面是否仍已发布，并且 VDA 未处于维护模式。确定多会话操作系统 VDA 是否已满

类别	原因	问题	操作
		它。可能的原因：应用程序或桌面已取消发布，或者托管应用程序或桌面的 VDA 已达到最大负载，或者应用程序或桌面已设置为维护模式。	载。如果是，请预配更多多会话操作系统 VDA。验证是否有可用于连接的单会话操作系统 VDA。如有必要，请预配更多单会话操作系统 VDA。
[5] 配置	[16] ActiveSessionReconnectDisabled	ICA 会话处于活动状态并连接到不同的端点。但是，由于**活动会话重新连接**已禁用，客户端无法连接到活动会话。	在交付控制器上，验证**活动会话重新连接**是否已启用。验证注册表路径 **HKEY_LOCAL_MACHINE\Software\Citrix\Desktop\Server** 下的 **DisableActiveSessionReconnect** 值是否设置为 0。
[2] MachineFailure	[17] NoSessionToReconnect	客户端尝试重新连接到特定会话，但该会话已终止。	重试工作区控制重新连接。
[2] MachineFailure	[18] SpinUpFailed	VDA 无法启动以进行会话启动。这是管理程序报告的问题。	如果计算机仍处于关机状态，请尝试从 Citrix Studio 启动计算机。如果失败，请检查管理程序连接和权限。如果 VDA 是 PVS 预配的计算机，请在 PVS 控制台中验证计算机是否正在运行。如果没有，请验证计算机是否已分配个人虚拟磁盘，登录到管理程序以重置 VM。
[2] MachineFailure	[19] 拒绝	交付控制器向 VDA 发送请求，要求其准	通过 ping 验证交付控制器和 VDA 是否可

类别	原因	问题	操作
		备好接受来自最终用户的连接，但 VDA 主动拒绝了此请求。	以成功通信。如果不能，请解决任何防火墙或网络路由问题。
[2] MachineFailure	[20] 配置集失败	在会话启动期间，交付控制器未将所需的配置数据（例如策略设置和会话信息）发送到 VDA。可能的原因：控制器和 VDA 之间的通信问题、Broker Service 在创建配置集请求时遇到的问题，或导致 VDA 不接受请求的网络问题。	-
[3] NoCapacityAvailable	[21] MaxTotalInstancesExceeded	已达到应用程序的最大实例数。无法在 VDA 上打开应用程序的其他实例。此问题与应用程序限制功能有关。	如果许可允许，请考虑将应用程序设置“**限制同时运行的实例数**”增加到更高的值。
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	用户尝试打开应用程序的多个实例，但应用程序配置为每个用户只允许一个应用程序实例。此问题与应用程序限制功能有关。	默认情况下，每个用户只允许一个应用程序实例。如果每个用户需要多个实例，请考虑清除应用程序设置中的“**限制每个用户一个实例**”设置。
[1] ClientConnectionFailure	[23] 通信错误	交付控制器尝试向 VDA 发送信息（例如准备连接的请求），但在通信尝试期间发生错误。这可能是由网络中断引起的。	如果已启动，请在 VDA 上重新启动桌面服务以重新启动注册过程，并验证 VDA 是否成功注册。通过应用程序事件日志中的详细信息，确认针对 VDA 配置的交付控制器是准确的。

类别	原因	问题	操作
[3] NoCapacityAvailable	[100] NoMachineAvailable 监控服务将 [12] NoDesktopAvailable 转换为此错误代码。	分配用于启动会话的 VDA 处于无效状态或不可用。可能的原因：VDA 的电源状态未知或不可用，VDA 自上次用户会话以来未重新启动，会话共享已禁用而当前会话需要启用，或者 VDA 已从交付组或站点中移除。	验证 VDA 是否在交付组中。如果不在，请将其添加到相应的交付组。验证是否有足够的 VDA 已注册并处于就绪状态，以便能够启动用户请求的已发布的共享桌面或应用程序。验证托管 VDA 的管理程序是否未处于维护模式。
[2] MachineFailure	[101] MachineNotFunctional。监控服务将 [12] NoDesktopAvailable 转换为此错误代码。	VDA 未运行。可能的原因：VDA 已从交付组中移除，VDA 未注册，VDA 电源状态不可用，或者 VDA 遇到内部问题。	验证 VDA 是否在交付组中。如果不在，请将其添加到相应的交付组。验证 VDA 在 Citrix Studio 中是否显示为已开机。如果多台计算机的电源状态未知，请解决与管理程序连接或主机故障的任何问题。验证托管 VDA 的管理程序是否未处于维护模式。解决这些问题后，重新启动 VDA。

计算机故障类型

错误代码	错误代码 ID	问题	操作
未知	-	-	-
未注册	3	-	-
最大容量（在 Director 中表示为最大负载）	4	计算机报告其已达到最大容量，即最大负载指数	确保所有管理程序都已开机。通过增加管理程序容量或添加更多管理程序，向受影

错误代码	错误代码 ID	问题	操作
			响的交付组添加更多计算机。
启动停滞	2	虚拟机未完成其启动序列，并且未与管理程序通信。	确保虚拟机在管理程序上成功启动。检查虚拟机上的其他消息，例如操作系统问题。确保管理程序工具已安装在虚拟机上。确保 VDA 已安装在虚拟机上。
启动失败	1	虚拟机在尝试在管理程序上启动时遇到问题。	检查管理程序日志。
无	0	-	-

计算机注销原因（适用于故障类型为“未注册”或“未知”的情况）

错误代码	错误代码 ID	问题	操作
代理关机	0	VDA 经历了正常关机。	如果根据现有电源管理策略，您不希望 VDA 处于关闭状态，请将其开机。检查事件日志中的任何错误。
代理已挂起	1	VDA 处于休眠或睡眠模式。	将 VDA 退出休眠模式。考虑通过电源设置禁用 Citrix Virtual Apps and Desktops™ VDA 的休眠功能。
IncompatibleVersion	100	由于 Citrix 协议版本不匹配，VDA 无法与交付控制器通信。	使 VDA 和交付控制器版本保持一致。

错误代码	错误代码 ID	问题	操作
AgentAddressResolutionFailed	101	交付控制器无法解析 VDA 的 IP 地址。	验证 VDA 计算机帐户是否存在于 AD 中。如果不存在，请创建它。验证 DNS 中 VDA 的名称和 IP 地址是否准确。如果不准确，请更正。如果问题普遍存在，请验证交付控制器上的 DNS 设置。通过运行 `nslookup` 命令，验证控制器中的 DNS 解析。
[Cloud]:AgentAddressResolutionFailed	101	交付控制器无法解析 VDA 的 IP 地址。	验证 VDA 计算机帐户是否存在于 AD 中。如果不存在，请创建它。验证 DNS 中 VDA 的名称和 IP 地址是否准确。如果不准确，请更正。
AgentNotContactable	102	交付控制器和 VDA 之间发生了通信问题。	使用 ping 验证交付控制器和 VDA 是否可以成功通信。如果不能，请解决任何防火墙或网络问题。有关导致控制器和 VDA 之间通信问题的常见问题，请参阅知识中心文章 Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) 中列出的故障排除步骤。

错误代码	错误代码 ID	问题	操作
[Cloud]: AgentNotContactable	102	交付控制器和 VDA 之间发生了通信问题。	有关导致控制器和 VDA 之间通信问题的常见问题，请参阅知识中心文章 Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) 中列出的故障排除步骤。请联系 Citrix 支持。
AgentWrongActiveDirectoryOU	103	发生了 Active Directory 发现配置错误。VDA 注册表中配置的站点特定 OU（其中站点控制器信息存储在 AD 中）属于不同的站点。	确保 Active Directory 配置正确，或检查注册表设置。
EmptyRegistrationRequest	104	从 VDA 发送到交付控制器的注册请求为空。这可能是由于 VDA 软件安装损坏造成的。	重新启动 VDA 上的 Desktop 服务以重新启动注册过程，并通过应用程序事件日志验证 VDA 是否正确注册。
MissingRegistrationCapabilities	105	VDA 版本与交付控制器不兼容。	升级 VDA，或移除 VDA 然后重新安装。
MissingAgentVersion	106	VDA 版本与交付控制器不兼容。	如果问题影响所有计算机，请重新安装 VDA 软件。
InconsistentRegistrationCapabilities	107	VDA 无法将其功能告知 Broker。这可能是由于 VDA 和交付控制器版本不兼容所	使 VDA 和交付控制器版本保持一致。

错误代码	错误代码 ID	问题	操作
		致。注册功能随每个版本而变化，其表达形式与注册请求不匹配。	
NotLicensedForFeature	108	您尝试使用的功能未获得许可。	检查您的 Citrix 许可版本，或移除 VDA 然后重新安装。
[Cloud]: NotLicensedForFeature	108	您尝试使用的功能未获得许可。	联系 Citrix 支持。
不支持的凭据安全版本	109	VDA 和交付控制器未采用相同的加密机制。	使 VDA 和交付控制器版本保持一致。
无效注册请求	110	VDA 向 Broker 发出了注册请求，但请求内容已损坏或无效。	有关导致控制器与 VDA 之间通信问题的常见问题，请参阅知识中心文章 Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) 中列出的故障排除步骤。
单会话多会话不匹配	111	VDA 的操作系统类型与计算机目录或交付组不兼容。	将 VDA 添加到正确的计算机目录类型或包含相同操作系统的计算机的交付组中。
FunctionalLevelTooLowForCatalog	112	计算机目录设置为高于已安装 VDA 版本的 VDA 功能级别。	验证 VDA 的计算机目录功能级别与 VDA 的功能级别匹配。升级或降级计算机目录

错误代码	错误代码 ID	问题	操作
			以匹配 VDA 的功能级别。
FunctionalLevelTooLowForDesktopGroup	113	交付组设置为高于已安装 VDA 版本的 VDA 功能级别。	验证 VDA 的交付组功能级别与 VDA 的功能级别匹配。升级或降级计算机目录以匹配 VDA 的功能级别。
PowerOff	200	VDA 未正常关机。	如果 VDA 应该处于开机状态，请尝试从 Citrix Studio 启动 VDA，并验证其是否正常启动和注册。排查任何启动或注册问题。VDA 重新启动后，查看其事件日志以帮助确定关机的根本原因。
AgentRejectedSettingsUpdate	203	Citrix 策略等设置已更改或更新，但在将更新发送到 VDA 时出错。如果更新与已安装的 VDA 版本不兼容，则可能会发生这种情况。	如有必要，请升级 VDA。检查所应用的更新是否与 VDA 版本兼容。
SessionPrepareFailure	206	Broker 未完成对 VDA 上运行的会话的审计。	如果普遍存在，请在交付控制器上重新启动 Citrix Broker Service。
[Cloud]: SessionPrepareFailure	206	Broker 未完成对 VDA 上运行的会话的审计。	联系 Citrix 支持。
ContactLost	207	交付控制器与 VDA 失去连接。这可能是由网络中断引起的。	验证 Citrix Broker Service 是否在交付控制器上运行，以及 Desktop service 是否

错误代码	错误代码 ID	问题	操作
			在 VDA 上运行。如果已停止，请启动它们。如果已启动，请在 VDA 上重新启动 Desktop service 以重新启动注册过程，并验证 VDA 是否成功注册。通过应用程序事件日志中的详细信息，确认为 VDA 配置的交付控制器是否准确。使用 ping 验证交付控制器和 VDA 是否可以成功通信。如果不能，请解决任何防火墙或网络问题。
[Cloud]: ContactLost	207	交付控制器与 VDA 失去连接。这可能是由网络中断引起的。	验证 Desktop service 是否在 VDA 上运行。如果已停止，请启动它。

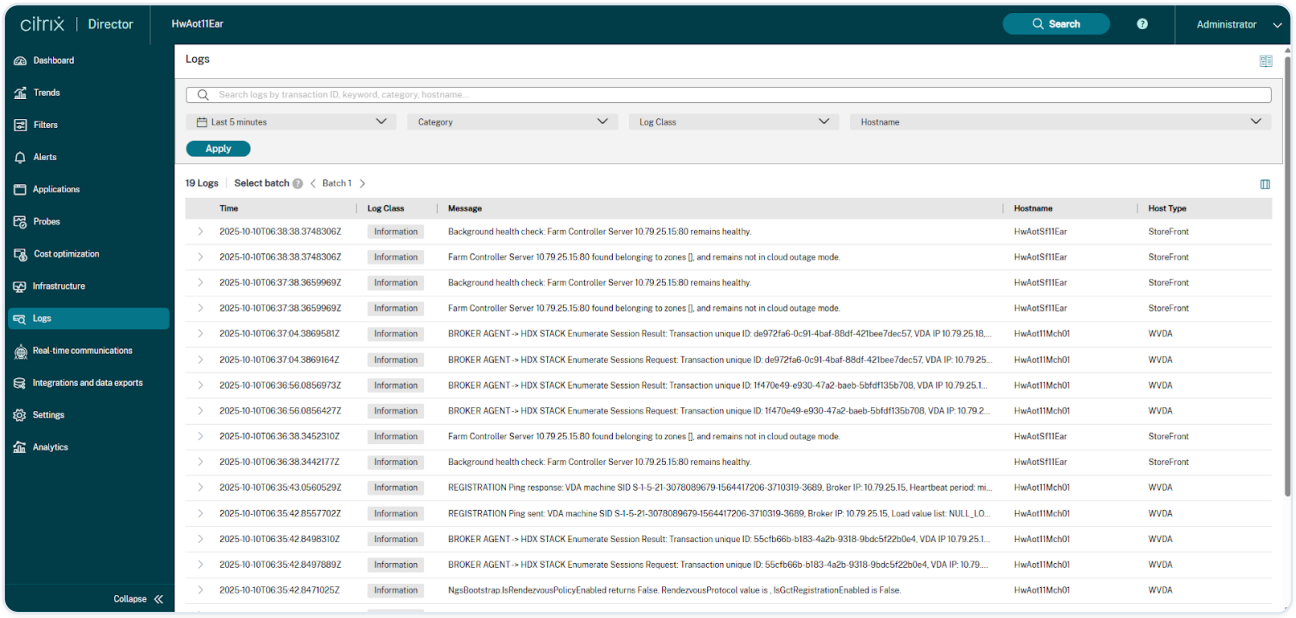
错误代码	错误代码 ID	问题	操作
BrokerRegistrationLimitReached	301	交付控制器已达到允许并发注册的 VDA 的最大配置数量。默认情况下，交付控制器允许 10,000 个 VDA 并发注册。	考虑向站点添加交付控制器或创建站点。您还可以通过 **HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\MaxWorkers** 注册表项增加允许并发注册到交付控制器的 VDA 数量。有关详细信息，请参阅知识中心文章 Registry Key Entries Used by Citrix Virtual Apps and Desktops (CTX117446)。增加此数量可能需要控制器更多的 CPU 和内存资源。
SettingsCreationFailure	208	Broker 未构建要发送到 VDA 的设置和配置集。如果 Broker 无法收集数据，则注册失败，VDA 将变为未注册状态。	检查交付控制器上的事件日志是否存在任何错误。如果日志中没有明显的特定问题，请重新启动 Broker 服务。Broker 服务重新启动后，重新启动受影响 VDA 上的 Desktop 服务，并验证它们是否成功注册。
[Cloud]: SettingsCreationFailure	208	Broker 未构建要发送到 VDA 的设置和配置集。如果 Broker 无法收集数据，则注册失败，VDA 将变为未注册状态。	重新启动受影响 VDA 上的 Desktop 服务，并验证它们是否成功注册。联系 Citrix 支持。

错误代码	错误代码 ID	问题	操作
SendSettingsFailure	204	Broker 未将设置和配置数据发送到 VDA。如果 Broker 可以收集数据但无法发送，则注册失败。	如果仅限于单个 VDA，请重新启动 VDA 上的 Desktop 服务以强制重新注册，并通过应用程序事件日志验证 VDA 是否成功注册。排查发现的任何错误。有关导致控制器和 VDA 之间通信问题的常见问题，请参阅知识中心文章 Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) 中列出的故障排除步骤。
代理请求	2	发生未知错误。	联系 Citrix 支持。
桌面重启	201	发生未知错误。	联系 Citrix 支持。
桌面已移除	202	发生未知错误。	联系 Citrix 支持。
会话审核失败	205	发生未知错误。	联系 Citrix 支持。
未知错误	300	发生未知错误。	联系 Citrix 支持。
注册状态不匹配	302	发生未知错误。	联系 Citrix 支持。
未知	-	发生未知错误。	联系 Citrix 支持。

日志

Citrix Director/Monitor 中的新日志视图旨在展示 Always On Tracing (AOT)，以显著增强管理员在 Citrix Virtual Apps and Desktops (CVAD) 环境中诊断和解决客户问题的能力。通过与您的集中式日

志服务器集成，此功能可提供跨各种核心组件（包括虚拟投递代理、投递控制器、StoreFront 和其他 Citrix 组件）的 AOT 日志的统一可搜索视图。这种集中式访问通过允许从单个控制台快速检索和分析日志来简化故障排除。



在产品文档中了解有关 Always On Tracing (AOT) 的架构和优势的更多信息。

先决条件和配置

要有效使用 Director 中的“日志”视图，您的环境需要正确配置并满足必要的先决条件。

- **CVAD 版本要求**：您必须运行 CVAD 2507 CU1 或 CVAD 2511（或更高版本）。
- 集中式日志服务器：您的客户管理的资源位置必须托管一个集中式日志服务器。了解有关安装和配置日志服务器的更多信息
- 当日志服务器配置为 HTTPS 模式（例如，`https://<LogServerFQDN>:port`）时，必须在 Director 和 DDC 计算机上安装并信任必要的证书。此证书必须由每台计算机上的计算机帐户管理。

入门

完成先决条件配置后，Director UI 中的新“日志”选项卡将为您的集中式 AOT 日志提供统一的可见性。

访问日志视图

日志视图可以直接作为 Director 中的专用选项卡访问，也可以从其他关键故障排除区域进行上下文导航：

- **专用“日志”选项卡**：使用导航面板直接在 Director/Monitor 界面中访问新的“日志”页面。

- **活动管理器**：单击一个选项以查看针对托管会话的计算机的相关日志。
- **计算机筛选器**：单击一个选项以查看其中已预填充计算机名称的相关日志。

使用日志视图

日志视图旨在提供灵活而强大的日志搜索功能，使管理员能够快速查明相关事件。

日志视图(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/dir-logs-view.png)

主搜索界面包括：

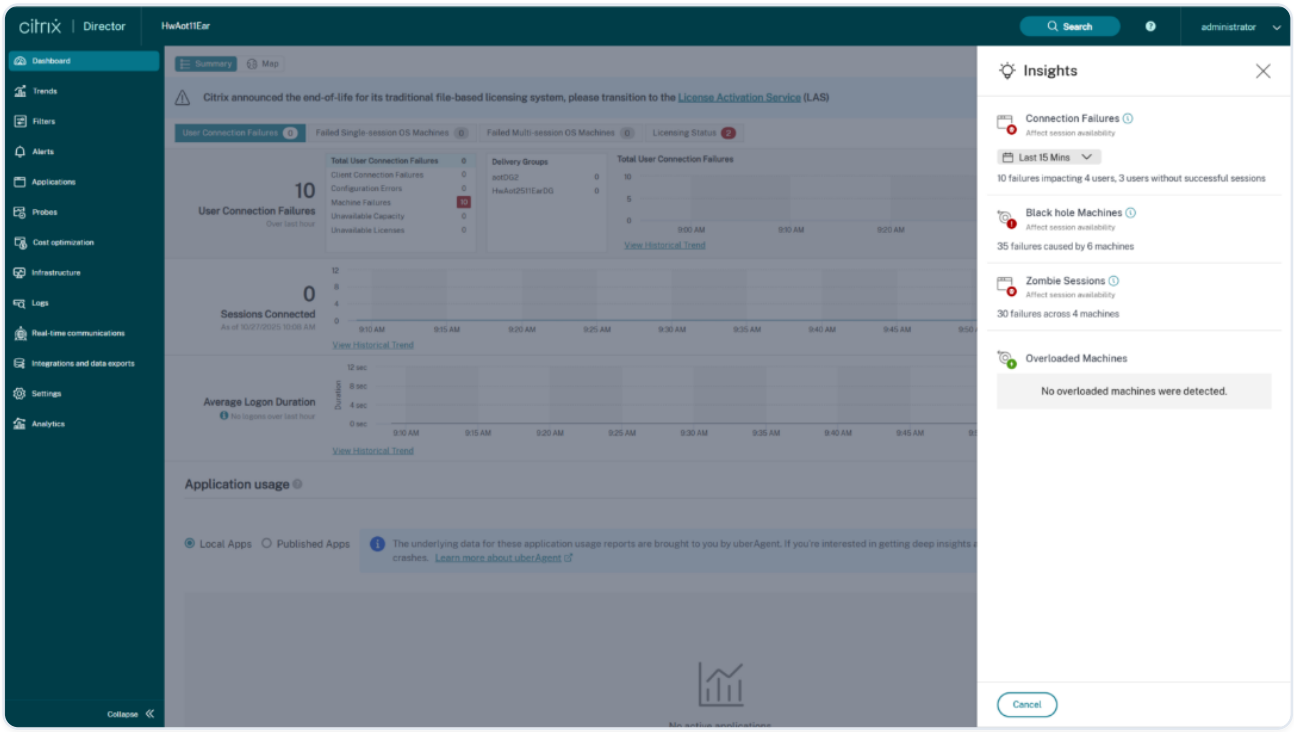
- **搜索栏**：一个功能强大的文本框，允许您按任意关键字搜索。常见的搜索词包括事务 ID、会话 ID、用户名或特定的错误消息。
- **筛选器选择器**：使用以下下拉筛选器以缩小搜索范围：
- **时间间隔**：按特定时间范围筛选日志。
- **类别**：按日志类别筛选。
- **日志类**：按日志消息的类筛选（例如，AOT_INFO）。
- **计算机名称**：筛选源自特定计算机名称的日志。

搜索结果以综合表格格式呈现，包含时间、消息、主机名、级别、模块、进程 ID 等关键属性。您可以展开单个日志条目以查看完整详细信息。Director 支持配置和查看与您的日志数据相关的自定义列。此外，结果会分页显示，以便于查看和导航大型数据集。

通过提供对所有 AOT 日志的即时、上下文感知访问，此功能旨在减少在工具之间切换和手动关联日志所花费的时间，从而加快问题解决速度。

洞察

“洞察”面板提供有关环境中会话失败或缓慢的信息。通过这些洞察深入探究特定指标有助于更快地排查并解决会话失败或缓慢问题。故障洞察专门帮助管理员提高会话可用性，这是决定用户体验的重要因素。这些洞察旨在帮助主动监控用户体验。因此，系统会显示当前故障的洞察（每 15 分钟刷新一次）。



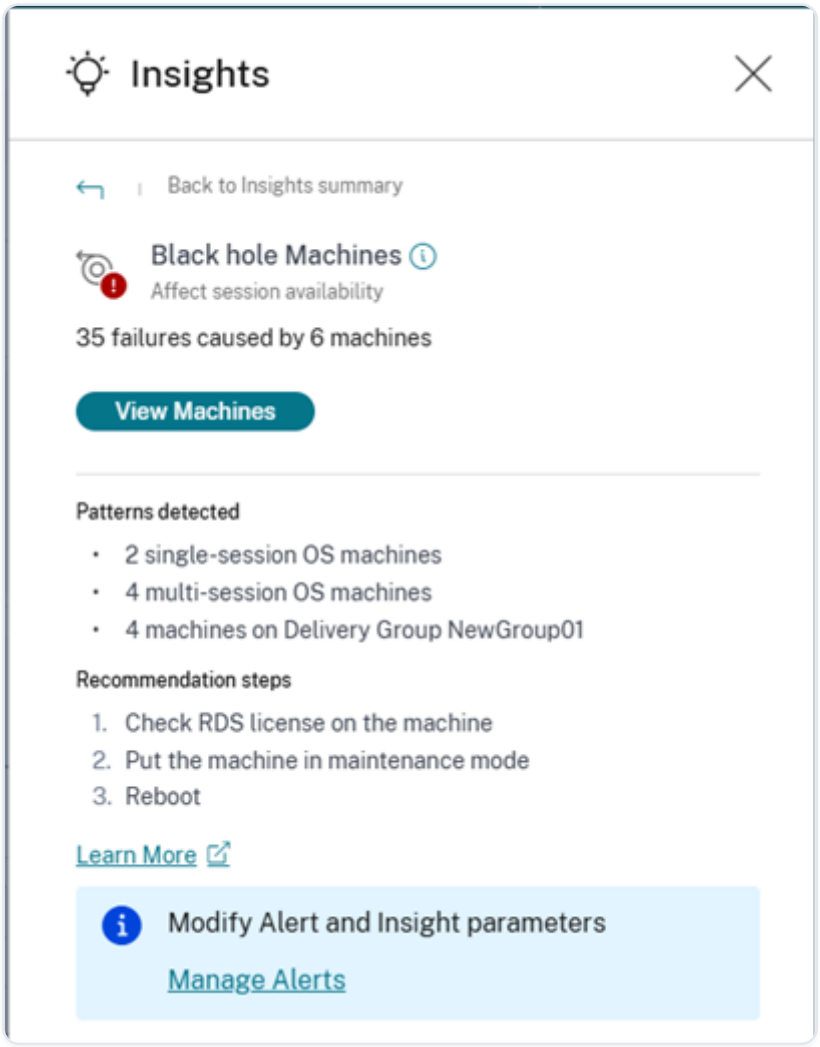
单击控制板中的洞察图标将显示洞察窗格，其中包含有关洞察的详细信息以及深入到“计算机”或“连接”视图的选项。管理员还可以从面板导航到警报配置。

此面板上提供黑洞计算机、僵尸会话、过载计算机和会话故障洞察。每个洞察展开后都会显示一个指向失败的会话或托管它们的计算机的链接。这会转到包含失败的计算机或会话的“筛选器”视图。单击特定的计算机或会话以查看详细指标后，可以从此处进一步深入。

每个洞察的展开视图显示了针对站点、交付组、单会话或多会话操作系统计算机检测到的主要故障模式。这些模式旨在帮助管理员发现是否存在遇到此问题的特定用户群。如果系统由于用户群分散而无法突出显示任何模式，建议深入分析。此外，还会显示建议采取的排查和解决问题的操作。

黑洞计算机

环境中的某些计算机虽然已注册且显示正常，但可能无法为分配给它们的会话提供服务，从而导致故障。未能为四个或更多连续会话请求提供服务的计算机称为黑洞计算机。这些故障的原因与可能影响计算机的各种因素有关，例如 RDS 许可证不足、间歇性网络问题或计算机上的瞬时负载。这些故障不包括因容量或许可证可用性导致的故障。环境中存在黑洞计算机增加了会话故障，导致会话可用性差。“黑洞计算机”洞察显示了环境中识别出的黑洞计算机数量。



黑洞计算机的建议操作：

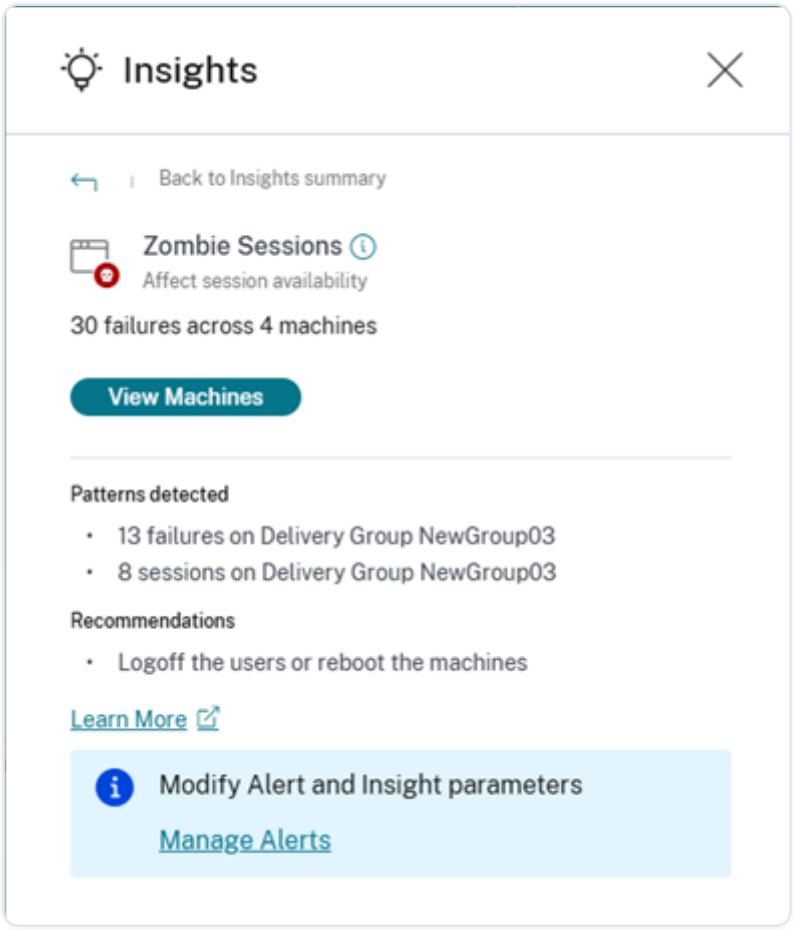
- 检查计算机上的 RDS 许可证
- 将计算机置于维护模式
- 重新启动

“检测到的模式”部分显示了在黑洞计算机中观察到的主要模式，具体取决于以下条件：

- 运行单会话或多会话操作系统的黑洞计算机数量
- 影响机器数量最多的交付组

僵尸会话

“僵尸会话”子窗格显示了由于环境中存在僵尸会话而导致的会话失败信息。僵尸会话是单会话操作系统计算机上废弃的会话，导致在该计算机上启动新会话失败。尝试在此计算机上启动会话会因“容量不可用”错误而失败。在废弃会话终止之前，所有未来的会话启动尝试都将失败。僵尸会话洞察旨在帮助发现这些具有废弃会话的计算机，并主动缓解这些故障。



僵尸会话的建议操作：

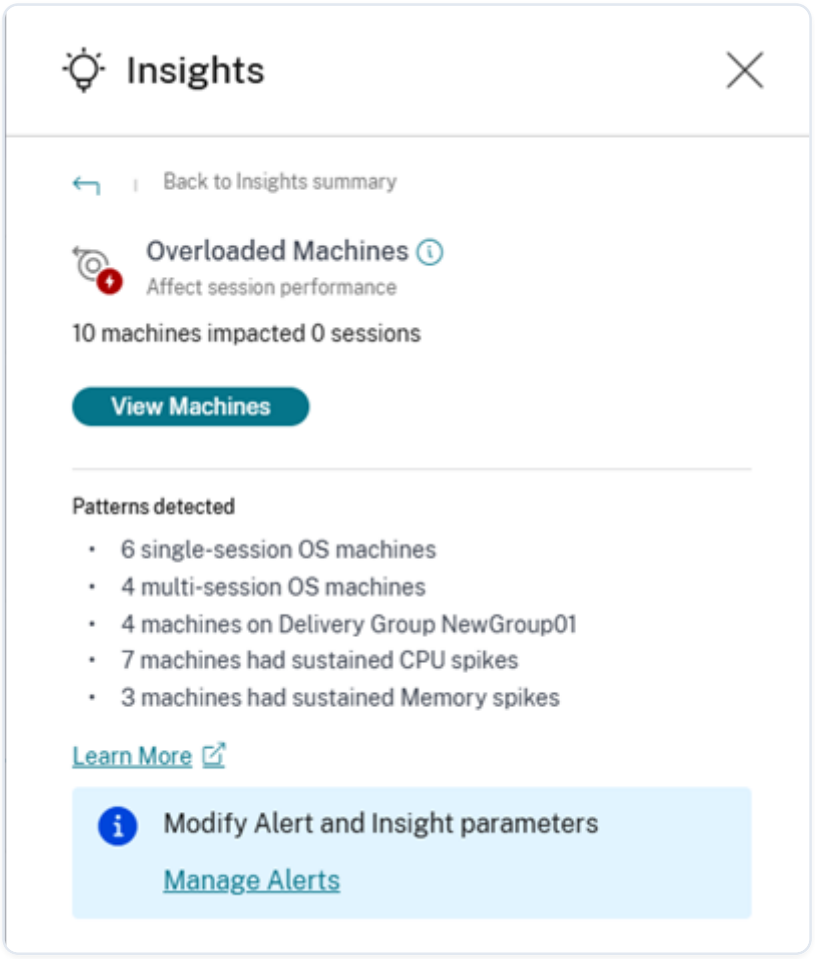
- 您可以使用适用于 Citrix DaaS 站点的 Monitor 将用户从僵尸会话中注销。
- 您可以重新启动包含僵尸会话的计算机。

“检测到的模式”部分显示了在僵尸会话中观察到的与以下条件相关的热门模式：

- 影响机器数量最多的交付组
- 影响会话数量最多的交付组

过载计算机

“过载计算机”洞察提供了对导致体验不佳的过载资源的可见性。经历持续 CPU 峰值、高内存使用率或两者兼有，且持续 5 分钟或更长时间，可能导致用户体验不佳的计算机被视为过载。

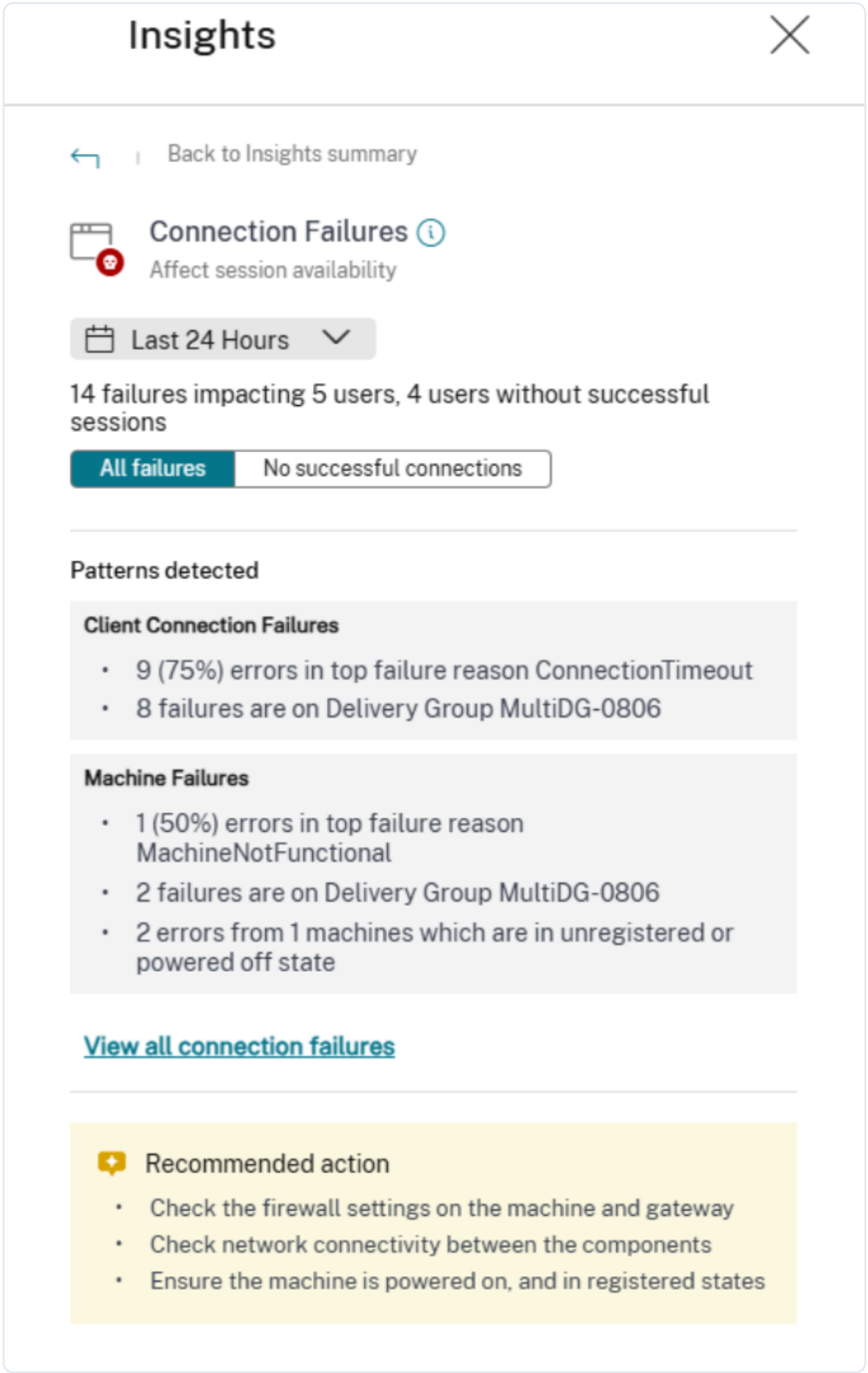


“检测到的模式”部分显示了在过载计算机中观察到的与以下条件相关的热门模式：

- 运行单会话或多会话操作系统的过载计算机数量
- 影响机器数量最多的交付组
- 具有持续内存或 CPU 峰值的过载计算机数量

连接失败

“连接失败”洞察列出了从端点（用户启动会话的位置）到计算机（会话代理的位置）之间由于各种问题导致的会话失败次数。这些失败可能由多种原因引起，例如防火墙配置不正确、网络通信问题或计算机不可用。


Insights
Back to Insights summary
Connection Failures
Affect session availability
Last 24 Hours
14 failures impacting 5 users, 4 users without successful sessions
All failures
No successful connections
Patterns detected
Client Connection Failures
9 (75%) errors in top failure reason ConnectionTimeout
8 failures are on Delivery Group MultiDG-0806
Machine Failures
1 (50%) errors in top failure reason MachineNotFunctional
2 failures are on Delivery Group MultiDG-0806
2 errors from 1 machines which are in unregistered or powered off state
View all connection failures
Recommended action
Check the firewall settings on the machine and gateway
Check network connectivity between the components
Ensure the machine is powered on, and in registered states

连接失败的两种类别是：

- 客户端连接失败 — 列出端点上发生通信错误的会话。
- 计算机失败 — 列出计算机上发生错误的会话。

此外，“连接失败”子面板显示以下建议以解决错误。

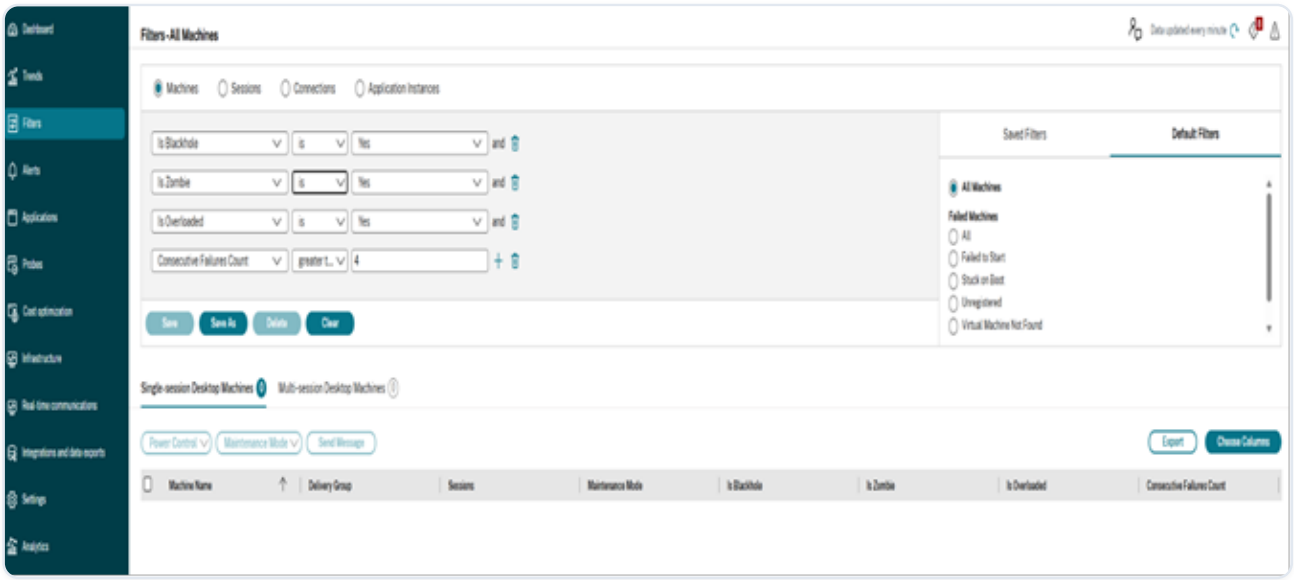
- 检查计算机和网关上的防火墙设置。
- 检查组件之间的网络连接。
- 确保计算机已开机并处于注册状态。

故障被分组以识别被阻止的用户，即在选定时间段内连接失败后没有成功会话的用户。两种故障类别都突出显示了模式。单击详细信息将打开“连接”视图，该视图经过筛选，显示在选定时间内由于环境中错误而失败的所有会话。此视图有助于分析已失败的各个会话并找出可能的根本原因。

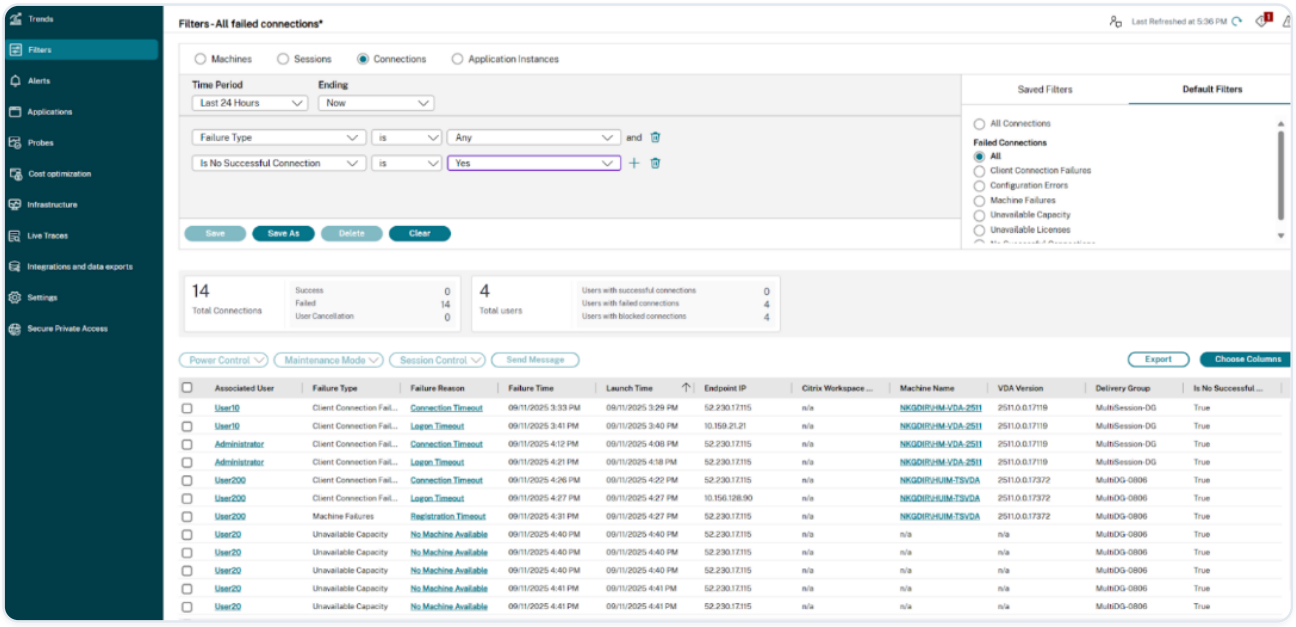
筛选视图

以下是添加到“筛选器”->“计算机”下的“计算机”视图的新筛选器和列：

- 连续故障计数：机器报告的连续会话启动故障次数
- 是否为黑洞：机器是否已被识别为黑洞机器
- 是否为僵尸：机器是否已被识别为僵尸机器
- 是否过载：机器是否已被识别为过载机器



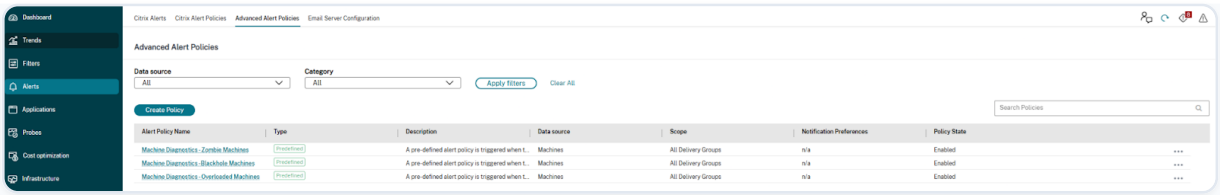
以下是“筛选器”->“连接”下的“连接”视图中添加的新筛选器和列：



警报

有 3 个新的“高级警报策略”可用并默认启用，通过在系统中识别出黑洞、僵尸或过载机器（跨所有交付组）时主动发出警报来帮助管理员

> **注意：**
>
> 在当前版本中，“高级警报策略”不支持连接故障。



管理默认策略

为了最大限度地发挥诊断洞察的价值，以下是有关默认警报策略的几个要点：

- **自定义：** 管理员可以为这些默认策略自定义**警报策略参数、范围或通知操作**。
- **限制：** 您**无法更改条件**或**删除**默认策略。
- **启用/禁用：** 可以根据需要**禁用或启用**策略。
- **通知：** 默认策略开箱即用**未配置通知**；它们只会导致**UI 警报**。**我们强烈建议管理员更新这些策略的通知首选项**。

注意：

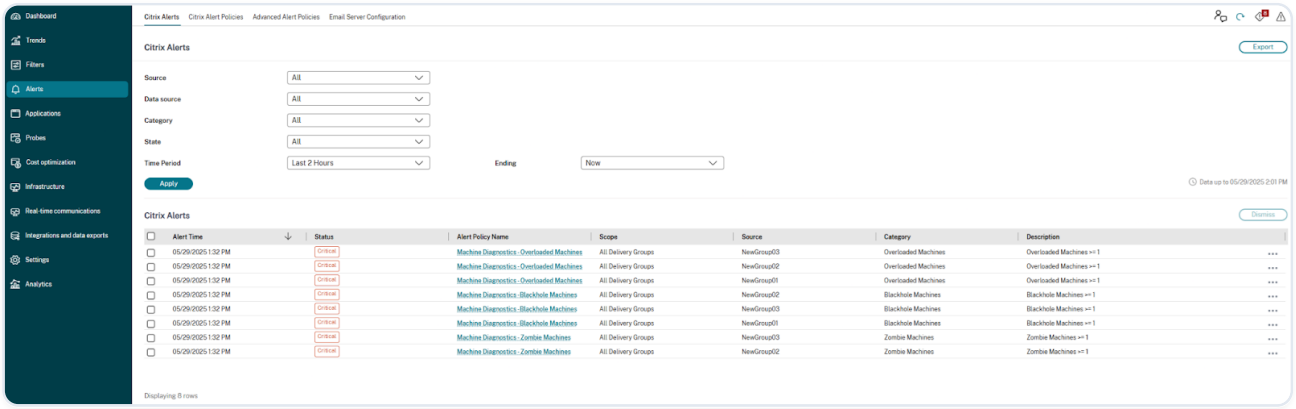
- “洞察”面板本身依赖于已启用的策略。如果您禁用默认策略且没有启用的自定义策略，“洞察”面板将停止刷新。
- 更新警报参数还会更改仪表板上相应洞察的计算。

创建自定义策略

您可以为这些洞察创建其他**自定义策略**。如果您创建自定义策略，我们建议**修改默认策略的范围**，以**排除任何交付组**，这些交付组由您的自定义策略涵盖。这可以防止重叠和潜在的重复警报。

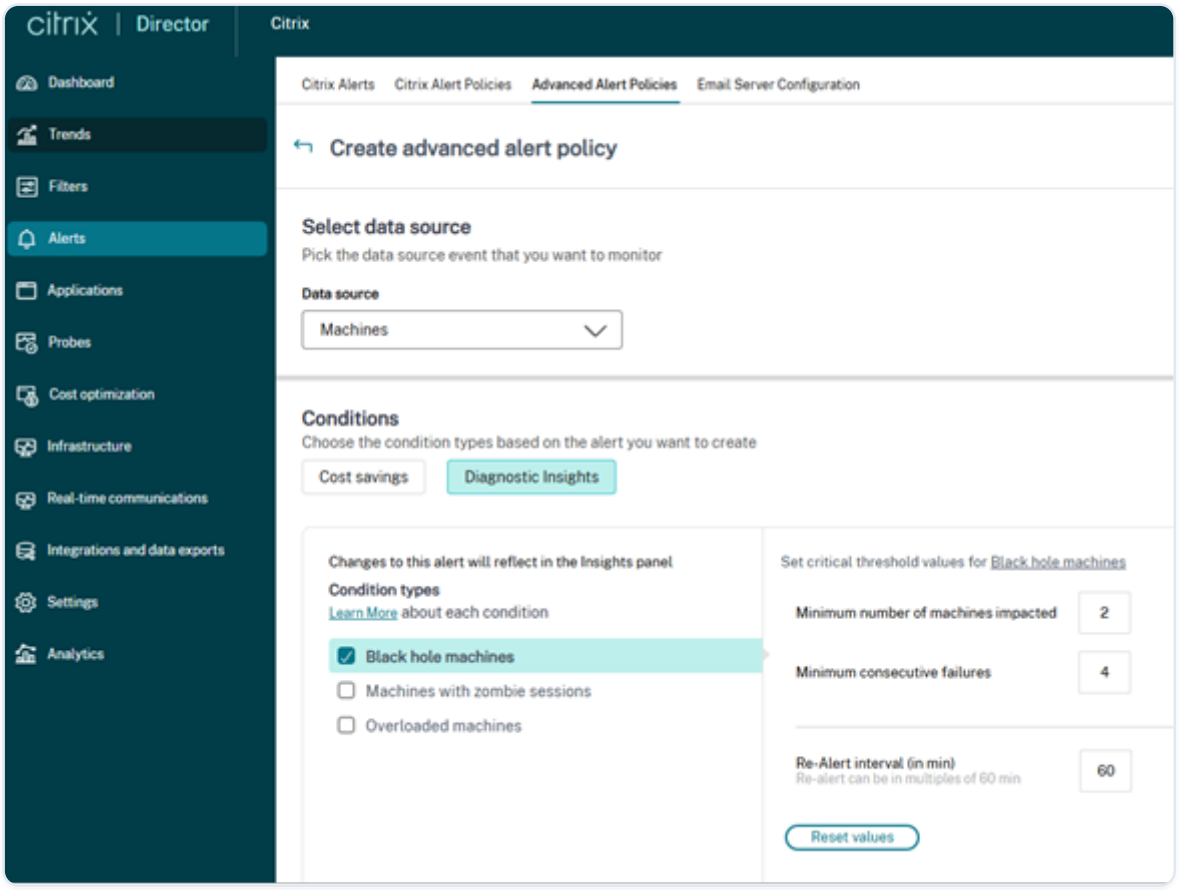
警报通知

以下是针对洞察提出的“Citrix 警报”的快速视图：



黑洞计算机警报

Monitor 每 15 分钟扫描一次黑洞计算机，并向管理员发送警报，以主动缓解用户遇到的会话失败。默认情况下，未能处理四个或更多连续会话请求的计算机被称为黑洞计算机。可以为选定的警报自定义警报条件和重新警报间隔。



导致会话失败的计算机的详细信息会通过警报电子邮件或 Webhook 有效负载发送。必须启用黑洞计算机警报策略才能接收这些通知。

僵尸会话计算机警报

当在 15 分钟间隔内环境中检测到具有僵尸会话的新计算机时，会生成僵尸会话计算机警报。

管理员可以自定义僵尸会话计算机警报的警报条件。

高级警报僵尸会话(/en-us/citrix-daas/media/dir-alert-zombie.png)

导致僵尸会话和故障的计算机详细信息将通过警报电子邮件或 Webhook 有效负载发送。

过载计算机警报

在配置的采样间隔内，持续出现 CPU 峰值、高内存使用率或两者兼有的计算机被视为过载。

管理员可以自定义过载计算机警报的警报条件和重新警报首选项。

过载计算机(/en-us/citrix-daas/media/dir-alert-overloaded-machines.png)

重新警报

对于特定的洞察警报，在配置的**重新警报间隔**内的通知行为是增量的。如果在此间隔期间识别出新的问题计算机，则重新警报电子邮件或 Webhook 将**仅包含这些新计算机**。每隔一个**重新警报间隔**（**默认为 24 小时**）将发送一次完整警报，其中列出给定交付组的所有问题计算机。

成功会话启动的地图视图

概述

Citrix Director 中的地图视图为管理员提供了其 Citrix 环境中成功启动的会话的全面地理可视化。此功能在全球范围内直观地映射用户连接，帮助 IT 团队快速识别区域性能模式、解决地理连接问题，并根据位置数据优化最终用户体验。地图显示颜色编码的连接点，指示不同地理位置的登录性能。

先决条件

下表列出了功能、端点指标和支持的产品版本：

VDA

VDA WINDOWS 版本	VDA MAC 版本	VDA LINUX 版本
2411 或更高版本	不适用	不适用

虚拟投递代理版本	适用于 WINDOWS 的 CITRIX WORKSPACE 应用程序版本	适用于 MAC 的 CITRIX WORKSPACE 应用程序版本	适用于 LINUX 的 CITRIX WORKSPACE 应用程序版本	适用于 HTML5 的 CITRIX WORKSPACE 应用程序版本	适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序版本
2411 或更高版本	2409 或更高版本	2409 或更高版本	2408 或更高版本	2411 或更高版本	2411 或更高版本

注意：

必须启用 Studio 策略“端点位置数据收集”才能访问和显示地图上的位置数据。请确保在继续操作之前配置此策略。

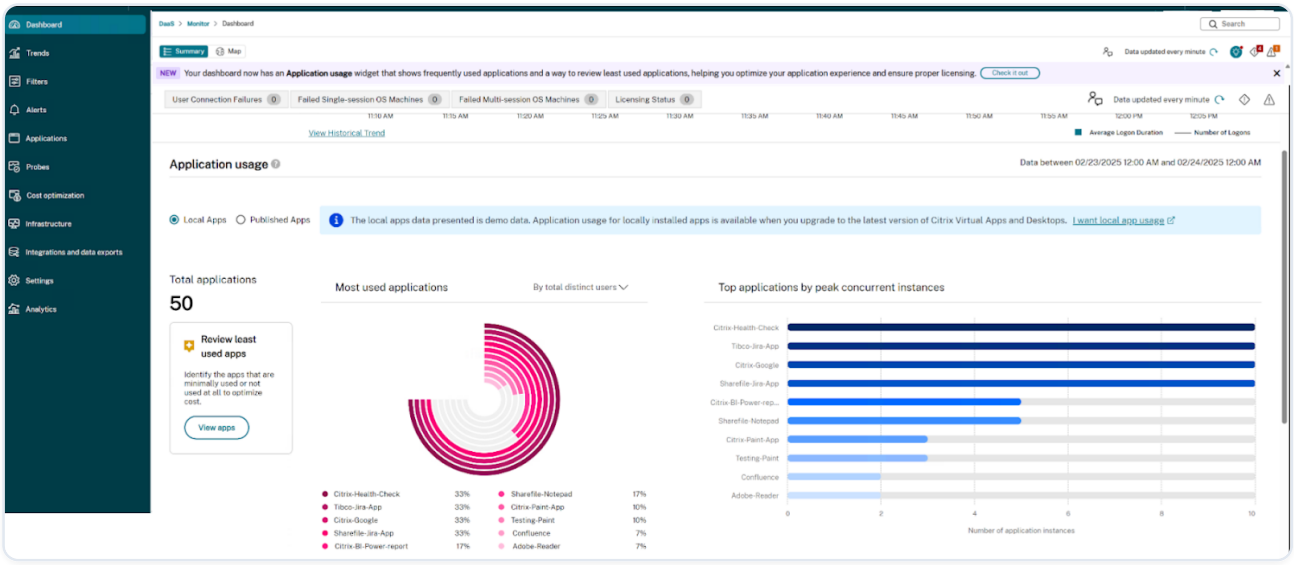
主要优势

- **地理性能洞察：** 即时可视化不同国家和地区的连接性能指标。
- **可自定义的性能阈值：** 定义您自己的低、中和高（差）登录持续时间标准。
- **连接密度可视化：** 通过颜色编码的指示器和不同大小的圆圈识别高流量地理区域。
- **全球部署概览：** 访问整个环境的关键摘要指标。
- **区域故障排除：** 按地理区域快速识别并解决性能问题。
- **实时监控：** 查看每 5 分钟自动更新的数据。

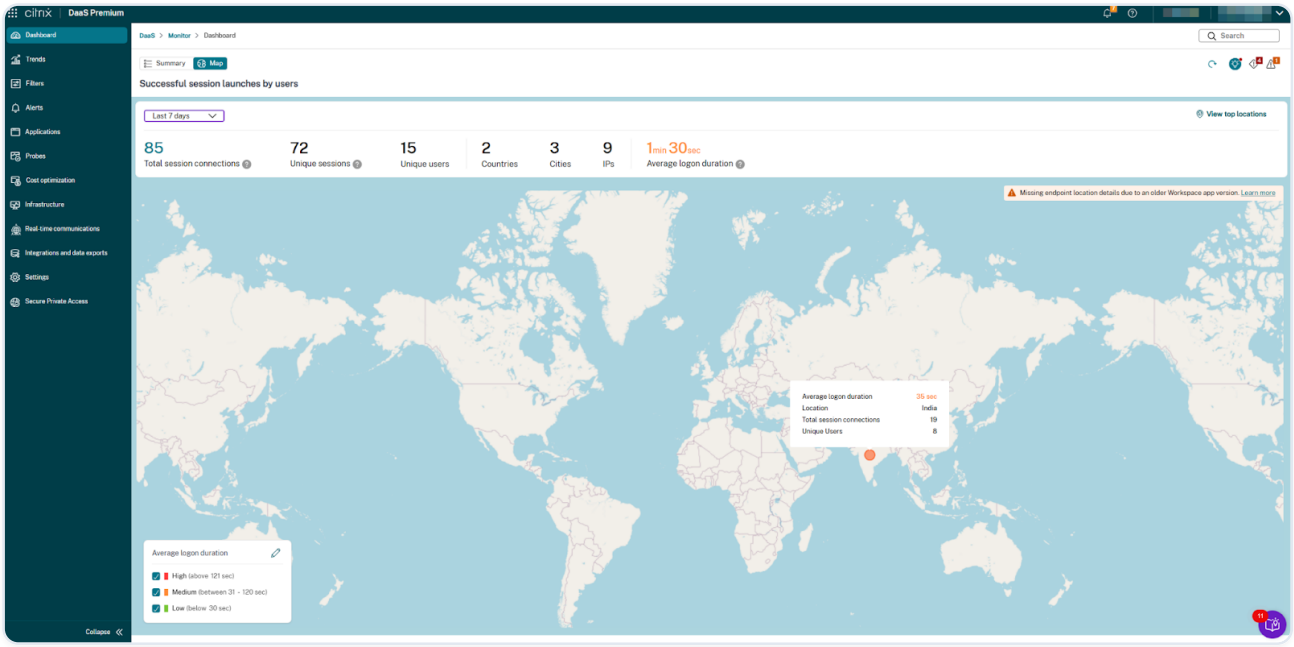
在拥有完整管理员权限的情况下，当您打开 Director 时，仪表板提供了一个集中位置来监控站点的运行状况和使用情况。

仪表板包含“摘要”和“地图”视图：

摘要视图：



地图视图：



用户界面组件

导航和视图选项

- **摘要/地图切换：** 在摘要统计信息和地理地图可视化之间切换
- **时间范围选择器：** 按时间段筛选数据（默认值：“上一小时”）
- **查看热门位置：** 选项，用于关注连接密度最高的区域
- **数据更新指示器：** 显示数据上次刷新时间（每 5 分钟更新一次）
- **通知图标**：与部署相关的系统警报和消息

摘要仪表板指标

在地图视图的顶部，管理员可以查看以下关键的部署范围指标：

指标	描述
会话连接总数	跨所有位置的会话连接总数
唯一会话数	已建立的单个会话数，不包括重复项
唯一用户数	建立连接的不同用户总数
国家/地区	连接源自的不同国家/地区数量
城市	连接源自的不同城市数量
IP 地址	建立连接的唯一 IP 地址总数

指标	描述
平均登录持续时间	在整个部署中建立会话所需的平均时间

性能分类

连接性能分为以下三个级别，具有可自定义的阈值：

性能级别	颜色代码	默认阈值	描述
低（良好）	绿色	低于 60 秒	登录体验快速，延迟极小
中等	橙色	61-120 秒*	可接受的登录时间
高 (差)	红色	超过 120 秒	需要关注的次优登录体验

> **注意：**
>
> 此界面允许管理员通过图例面板中的输入字段自定义这些阈值。

地图图例和阈值控件

交互式图例面板提供：

- **颜色编码的性能指标**以及相应的阈值
- **可编辑的阈值字段**，用于自定义中等性能范围（最小值和最大值）
- **验证消息**，确保最大阈值超过最小阈值，且既不为零也不为负
- **选择/筛选控件**，用于关注特定性能类别

系统要求和通知

Citrix Workspace 应用程序版本兼容性

当由于 Citrix Workspace 应用程序版本过旧而缺少端点位置详细信息时，地图会显示警告横幅：

- **警告消息：** “由于 Workspace 应用程序版本过旧，缺少端点位置详细信息。”
- **解决方案：** 升级到最新版本的 Workspace 应用程序可确保收集完整的地理数据

- **了解更多：** 横幅包含一个指向文档的链接，其中包含有关版本要求的更多信息

配置选项

设置性能阈值

- 在地图视图的左下角找到图例面板。
- 为“中等”性能类别输入自定义值：
  - 最小阈值（默认值：61 秒）
  - 最大阈值（默认值：120 秒）
  - “低”类别自动调整为“低于 ”。
  - “高”类别自动调整为“高于 ”。
  - 验证可确保最大阈值超过最小阈值，且两者均不为零或负数。
  - 更改后的阈值存储在浏览器缓存（本地存储）中，并且特定于该浏览器。

时间范围配置

1. 使用指标部分左上角的下拉菜单。
2. 选择所需的时间段（默认值：“上一小时”）。

地图和指标会自动更新，以反映所选时间段的数据。

地图视图用法

您可以将地图视图用于以下目的：

区域性能故障排除

1. 识别主要显示红色（高）登录持续时间指示器的区域。
2. 与为这些区域提供服务的基础设施组件关联。
3. 对受影响的地理区域实施有针对性的优化。

容量规划

1. 通过观察不同区域的圆圈大小来查看连接密度模式。
2. 识别需要额外资源的高流量地理区域（较大的圆圈）。
3. 根据区域使用模式规划基础设施扩展。

全局部署评估

1. 使用指标面板了解部署规模（总连接数、唯一用户数）。
2. 比较不同地理区域的登录性能。
3. 为不同位置建立基线性能预期。

阈值优化

1. 查看地图上绿色、橙色和红色指示器的分布。
2. 调整阈值以更好地反映特定环境的可接受性能。
3. 根据实际用户体验创建更有意义的性能分类。

故障排除

缺少地理数据

如果出现警告横幅“由于 Workspace 应用程序版本过旧，缺少端点位置详细信息”：

1. 识别使用过时 Citrix Workspace 应用程序版本的用户。
2. 计划分阶段升级到最新版 Citrix Workspace 应用程序。
3. 在地理数据最关键的区域优先进行升级。

性能分类问题

如果性能类别显示不准确：

1. 检查图例面板中的当前阈值设置
2. 根据需要调整“中等”类别的最小值和最大值
3. 确保阈值与您环境的实际性能特征和预期保持一致

数据刷新问题

如果数据似乎已过时：

1. 检查“数据每 5 分钟更新一次”指示器以查看上次刷新时间。

> **注意：**
>
> 在过去一周内，自动刷新已禁用。请手动刷新以获取最新数据。

1. 验证所选时间范围是否与您的故障排除期间匹配。
2. 如果可用，请使用“刷新”按钮手动更新数据。

最佳实践

- 根据基础架构改进情况，定期审查和调整性能阈值。
- 使用**查看热门位置**选项，重点关注连接量最高的区域。
- 比较基础架构更改前后的地理性能模式。
- 在最佳运行期间创建区域性能基线报告。
- 在设置性能预期时，请考虑区域网络状况。
- 告知用户升级到最新版本的 Citrix Workspace 应用程序以进行完整的数据收集。
- 定期检查**地图视图**以识别会话性能的新兴趋势。

思杰 艾德里安

Citrix Aidrien 与 Director 的集成在本地 Director 环境与 Citrix Cloud 之间提供了一个简化的桥梁。Citrix Aidrien 是 Citrix Cloud 中提供的一项由 AI 驱动的服务，旨在为 Citrix 和 NetScaler 解决方案提供产品内支持和帮助。

Citrix Aidrien 使管理员能够以自然语言提问，并接收由 Citrix 发布的 Citrix 和 NetScaler 解决方案文档丰富而成的即时答复。

当管理员在 Director 中单击“**Citrix Aidrien**”按钮时，他们将被重定向到 Citrix Cloud 界面。管理员可以使用其 Citrix Cloud 用户凭据进行身份验证，并继续在 Citrix Aidrien 中工作。

有关 Citrix Aidrien 以及 Citrix Director 中支持的用例的更多信息，请参阅 Citrix Aidrien。

先决条件

在使用 Director 中的 Citrix Aidrien 集成之前，请确保满足以下要求：

- 管理员拥有有效的 **Citrix Cloud 帐户**，并具有访问 Citrix Aidrien 的相应权限。
- **Citrix Aidrien 已启用**，并且已授予管理员访问权限。有关详细信息，请参阅 管理对 Citrix Aidrien 的访问。

> **注意：**

> 适用于本地 Director 的 Citrix Aidrien 集成仅使用 **Citrix 发布的文档**，并且不支持特定于环境的上下文。

> 在使用 Director 中的 Citrix Aidrien 集成之前，请确保满足以下要求：

- 管理员拥有有效的 Citrix Cloud 帐户。有关详细信息，请参阅 管理对 Citrix Cloud 的管理员访问权限。
- 确保在 Citrix Cloud 中启用了 Citrix Aidrien。有关更多详细信息，请参阅 在 Citrix Cloud 中启用 Citrix Aidrien。
- 管理员具有访问 Citrix Aidrien 的有效权限。要了解更多信息，请参阅 管理员对 Citrix Aidrien 的访问权限。

> **注意：**
>
> 1. 适用于本地 Director 的 Citrix Aidrien 集成仅使用 Citrix 发布的文档，并且不支持环境上下文。
> 2. Citrix Director 将显示 Aidrien 按钮，供所有使用 Director 控制台的管理员使用。

入门

从 Director 开始使用 Citrix Aidrien 非常简单：

1. 以管理员身份登录 Citrix Director。
2. 在 Director UI 的右上角找到并单击 Citrix Aidrien 按钮。
3. 您将被重定向到 Citrix Cloud 登录页面。
4. 使用您的 Citrix Cloud 用户凭据进行身份验证。
5. 成功登录后，Citrix Aidrien 将在 Citrix Cloud 中打开，您可以继续您的工作流程。
6. 除了满足先决条件外，Director 中无需进行额外的设置或配置。

会话分数指标

会话详细信息现在包含额外的数据点，用于排查会话性能问题并分析整体会话运行状况。这些额外数据提供了对单个会话整体用户体验的深入了解，并帮助管理员理解会话性能不佳的原因。下面列出了新增的数据点：

1. 会话体验摘要 – 它可快速了解会话体验。显示在选定时间段内环境中所有已启动会话的用户体验摘要。分析的会话分为良好、中等和差。管理员可以单击体验类别以打开详细会话视图（筛选器页面），其中包含自动应用的筛选器。
2. 会话和组件分数 – 会话摘要还提供了分析会话的平均会话和组件分数。虽然独立的平均分数可能不是一个非常有用的指标，但它仍然可以作为大多数会话体验的良好指标。同样，管理员可以使用平均组件分数来了解不良会话的潜在根本原因。
3. 会话分布 – 会话分布图已添加到筛选器页面。管理员可以按端点国家/地区、城市、端点操作系统、CWA 版本、ISP 等查看会话分布。
4. 性能趋势 – 会话性能趋势图也已添加到筛选器页面。性能图表有助于分析会话和组件性能趋势，并根据一天中的时间、国家/地区等识别任何重复模式。
5. 单个会话数据 – 会话详细信息表中已为每个会话添加了以下数据点 –

    a. 会话分数

    b. CPU 分数

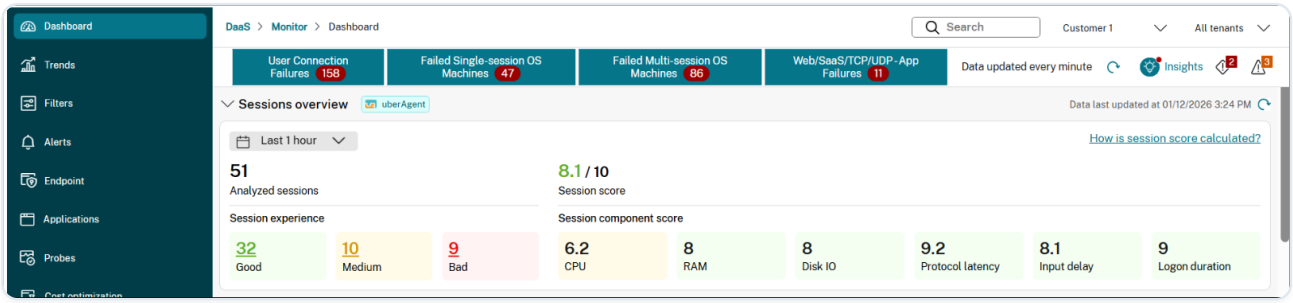
    c. RAM 分数

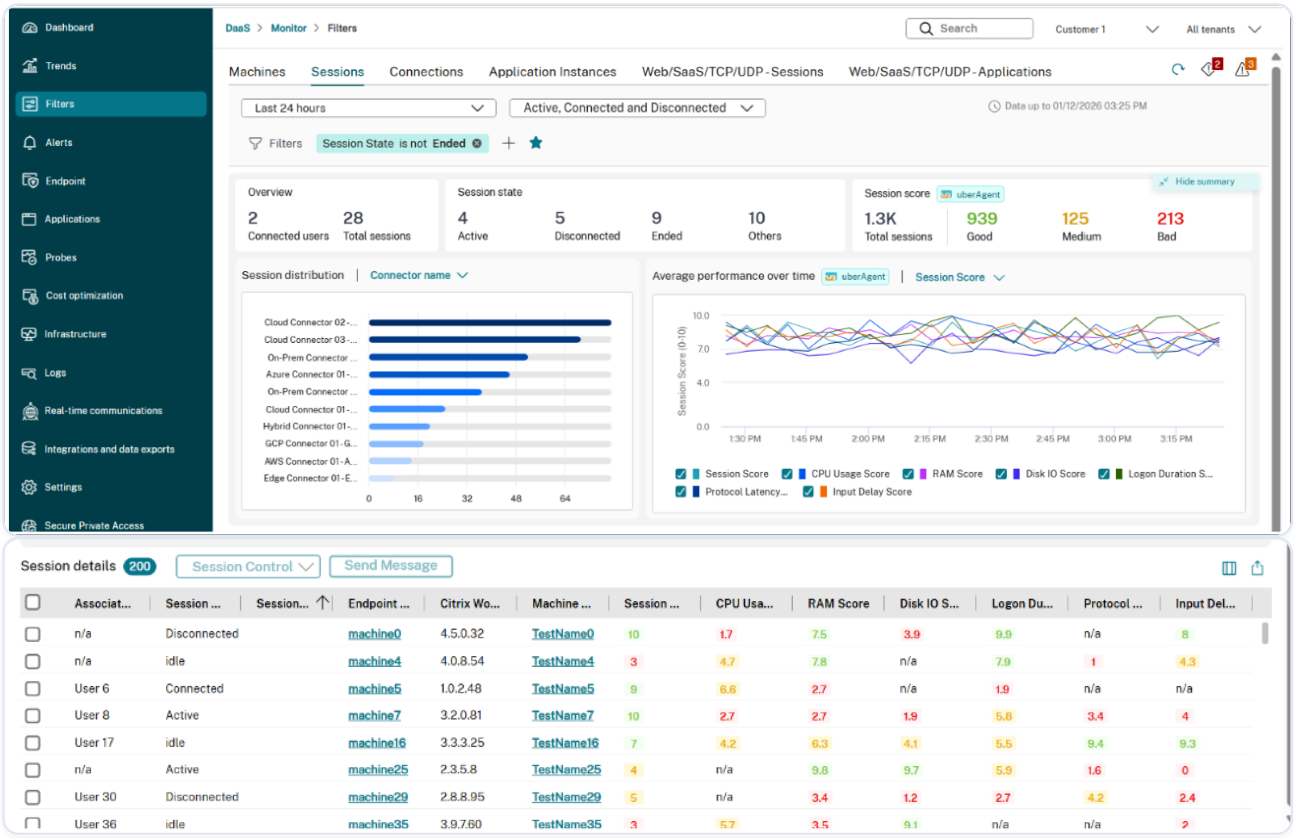
    d. 磁盘 IO 分数

    e. 协议延迟分数

    f. 输入延迟分数

    g. 登录持续时间分数





Director 中的端点安全策略激活和威胁检测报告

Citrix Workspace 应用程序正在引入内置安全检查，这些检查将自动检测高风险情况，例如在端点上启用了 Microsoft Recall，而无需任何手动配置。此类检测的实时可见性将在 Citrix Director 和 Monitor 中提供。该报告将使管理员能够快速评估风险并配置其保护策略，以确保更安全的环境。尽管对 Recall 等特定事件的检测是自动的，但事件防护需要管理员手动配置应用程序保护策略。所有已启用策略的激活事件也将在 Director 和 Monitor 中报告。通过利用主动风险管理和策略重新配置，管理员将能够加强其环境中的端点安全性，并减少新兴威胁的暴露。

以下报告将在 Director 中提供：

- **审计跟踪** -
- **自动检测** – 在其默认扫描期间，CWA 会检测端点上的各种威胁，例如 Windows Recall。如果检测到威胁，CWA 会将事件发送到 Director | Monitor。每个事件将报告以下数据 –
- 时间戳
- 用户名
- 端点名称
- 端点操作系统
- CWA 版本

- 事件名称
- 事件类型 – 检测或保护
- **配置策略的保护** – 管理员可以配置保护策略以防止某些事件，例如屏幕捕获、DLL 注入或键盘记录。反屏幕捕获策略也可用于防止 Recall 进行屏幕捕获尝试。在 Director | Monitor 中报告的保护事件将包含上述所有数据点。
- **聚合洞察和趋势** – 事件数据将聚合以报告以下信息：
  - 环境的检测/保护摘要，
  - 最受保护/检测到的事件，以及
  - 保护和检测事件随时间变化的趋势

此功能旨在通过帮助组织识别新出现的威胁并实时响应这些威胁，进一步加强 Citrix 安全交付应用程序的承诺。

管理员可以利用上述见解更好地了解其环境中的安全“威胁”，并设置保护策略以保护敏感数据、最大程度地降低安全风险，并支持制定旨在缓解此类风险的相关公司级策略。（例如，不鼓励使用 recall、keylogger 等工具）

安全私有访问与 Director 集成 (预览版)

安全私有访问与 Director 集成允许技术支持管理员或完全管理员监视和排查 Director 中的所有安全私有访问会话。要支持此功能，您必须使用 Director、安全私有访问、Citrix Workspace™ 应用程序和 VDA 的 2402 或更高版本。

可用操作包括查看以下内容的详细信息：

- 在 **选择会话** 弹出窗口 > **会话** 选项卡 > **Web SaaS 和客户端/服务器应用程序** 下，用户的 Secure Private Access 活动会话
- 在“**选择会话**”弹出窗口 > “**拒绝访问**”选项卡下，安全私有访问失败或被阻止的枚举以及失败的应用程序启动
- 活动和失败的应用程序启动的会话和应用程序详细信息视图
- 失败和被阻止的枚举的会话和应用程序详细信息视图

> **注意：**
>
> Secure Private Access 与 Director 的集成仅支持 Director 基于表单的身份验证，不支持集成 Windows 身份验证或基于智能卡的身份验证。

先决条件

1. 要支持此功能，您必须使用以下各项：
   - Director 2402 或更高版本
   - 安全私有访问 2402 或更高版本
   - Citrix Workspace 应用程序 2402 或更高版本
2. 确保至少一个 Citrix Virtual Apps and Desktops™ 站点已在 Director 上配置。
3. 设置安全私有访问。
4. 确保 Director 服务器与 Secure Private Access 服务器具有网络连接。

> **注意：**
>
> 必须在安全私有访问服务器上安装受信任的证书，才能成功建立与 Citrix Director 的连接。

5. 确保 Director 管理员用户具有以下权限：
   a. 在 Secure Private Access 管理控制台中，具有 Secure Private Access 完全管理员或只读管理员权限。
   b. 在 Citrix Studio 控制台中，具有 Citrix Virtual Apps™ 或 Desktops 帮助台、完全管理员或只读管理员权限。

配置 Director 以使用 Secure Private Access

1. 在安装了 Director 的计算机上，以管理员身份打开命令提示符。
2. 通过运行以下命令，转到 `DirectorConfig` 工具的路径：

```
cd c:\inetpub\wwwroot\Director\tools
```

3. 运行以下命令以配置 Secure Private Access：

```
DirectorConfig.exe /configspa
```

4. 输入安装 Secure Private Access 的计算机的 FQDN 以及端口号。
5. 确保与 Secure Private Access（服务器或负载均衡器）的连接是安全的，并且已应用受信任的证书。

```
PS C:\inetpub\wwwroot\Director\tools> .\DirectorConfig.exe /configspa

 Make sure the SPA server or load balancer is reachable from this Director machine
 Enter SPA server or load balancer FQDN including port [https://spa-server.mydomain.com:4[redacted]3] : https://[redacted]

 Checking connectivity to https://spa1.gwonprem.corp[redacted]

 Spa Server or load balancer: https://[redacted] is reachable.

 Checking Spa Server or load balancer is valid

 Retry with correct Spa Server FQDN which is reachable

 Director configuration encountered an error


=====================================================
Spa Server or load balancer FQDN https://[redacted] is either invalid or Spa server/load balancer is down
=====================================================
```

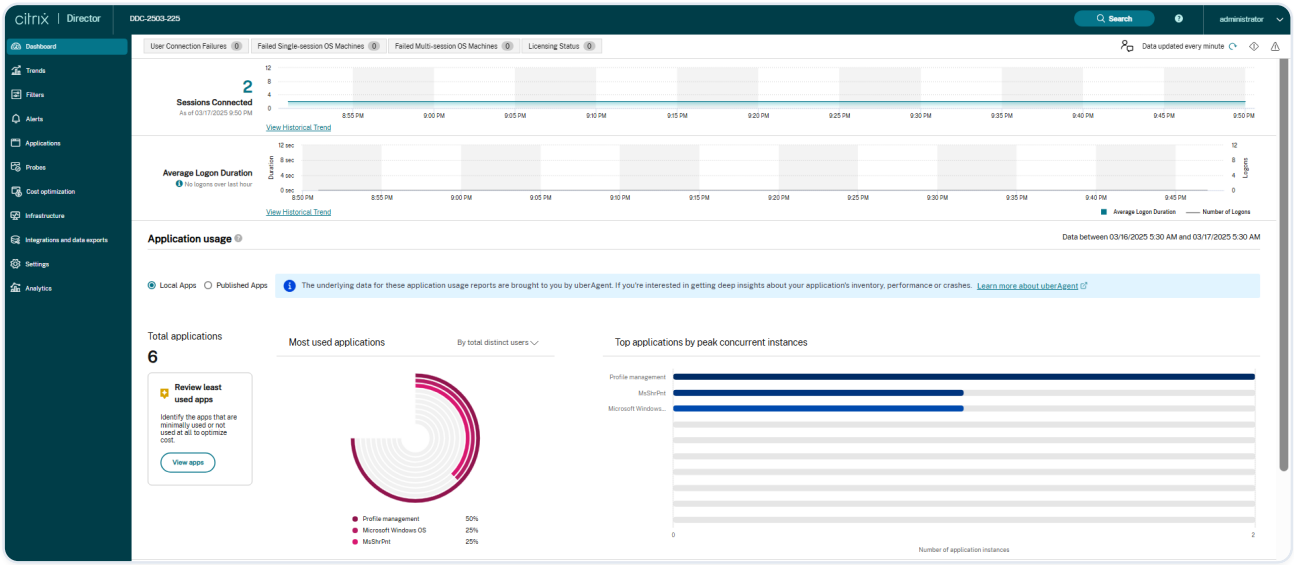
注意：

必须将管理员添加到 Secure Private Access 控制台，才能在 Director 中查看 Secure Private Access 会话详细信息。有关详细信息，请参阅管理管理员。

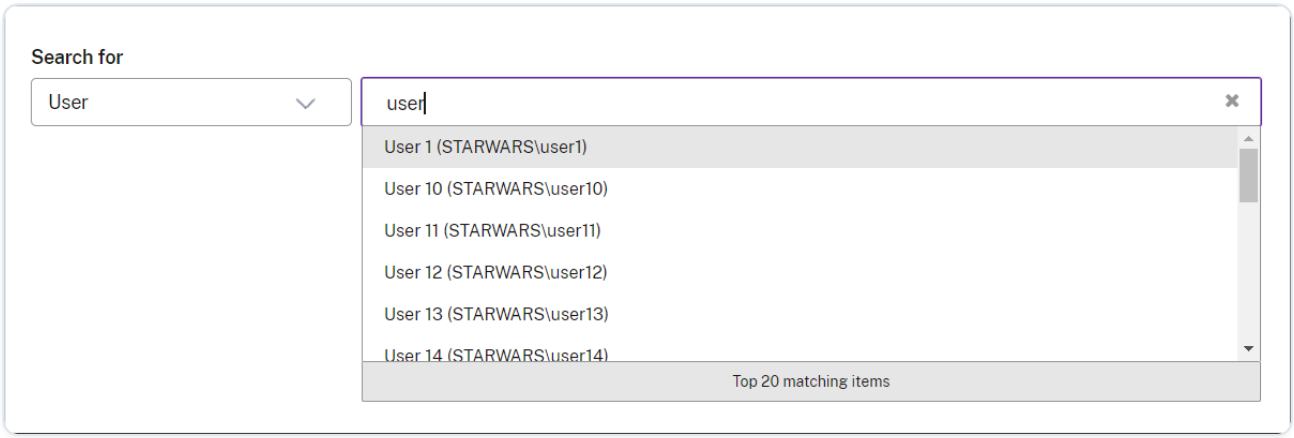
按用户查看 Secure Private Access 会话

在 Director 控制板上，单击**搜索**并输入用户名。此时将显示**选择会话**屏幕。

完全管理员：



帮助台管理员：



查看 Secure Private Access 会话的活动管理器

Citrix Director 为 Secure Private Access 会话提供了活动管理器视图，该视图可让您全面了解会话活动。活动管理器提供了所有成功打开、未能打开的应用程序和桌面，以及 Secure Private Access 应用程序中设置的策略结果的全面视图。此功能从 Citrix Virtual Apps and Desktops 2407 版或更高版本开始提供。

先决条件：

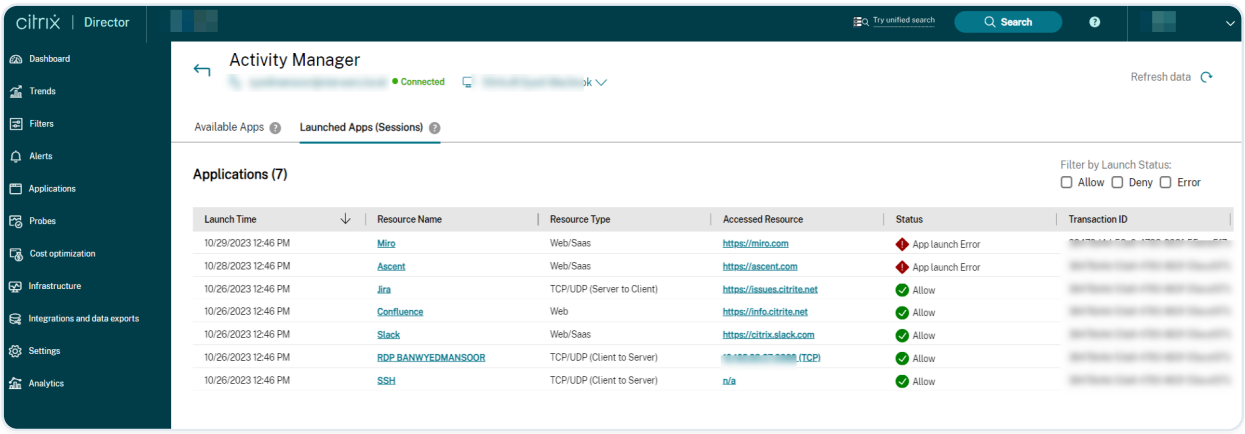
- Director 2407 或更高版本
- Secure Private Access 2407 或更高版本

活动管理器显示 **可用应用程序** 和 **已启动应用程序** 详细信息。您可以找到以下会话详细信息：

- 启动时间
- 资源名称
- 资源类型
- 访问的资源
- 状态
- 事务 ID

要查看活动管理器，请执行以下操作：

1. 在 Director 控制板上，单击**搜索**并输入用户名。此时将显示**选择会话**屏幕。
2. 选择使用 Secure Private Access 会话打开的会话。将显示所选会话的活动管理器。



3. 单击 **可用应用程序** 以查看 Citrix Workspace 应用程序中可用的应用程序。

或者，

单击 **已启动应用程序（会话）** 以查看在 Citrix Workspace 应用程序中打开的应用程序。

您可以根据 Secure Private Access 应用程序中设置的资源状态筛选资源：

- 允许 - 允许用户访问的资源。此状态是使用 Secure Private Access 应用程序下的策略设置的。此资源在 Citrix Workspace 应用程序中向用户显示。
- 拒绝 - 拒绝用户访问的资源。此状态是使用 Secure Private Access 应用程序下的策略设置的。此资源在 Citrix Workspace 应用程序中向用户显示。
- 错误 - 在 Secure Private Access 应用程序下允许用户访问的资源。但是，由于某些错误，该资源在 Citrix Workspace 应用程序中不可用。错误分为两种类型：枚举错误和会话错误。

查看可用应用程序

Citrix Workspace 应用程序中可用的 Web 和 SaaS 应用程序显示在“**可用应用程序**”部分下。此部分显示应用程序的上次枚举尝试以及枚举尝试的状态。

您可以查看以下详细信息：

- 资源名称
- 状态
- 事务 ID

您还可以使用应用程序状态（例如“**允许**”、“**拒绝**”和“**错误**”）筛选上述详细信息。您还可以使用向上和向下箭头对详细信息进行排序。

> **注意：**

> TCP/UDP 应用程序不显示在“**可用应用程序**”部分中。

查看已启动的应用程序

在 Citrix Workspace 应用程序中打开的应用程序显示在“**已启动的应用程序（会话）**”部分下。您可以查看以下详细信息：

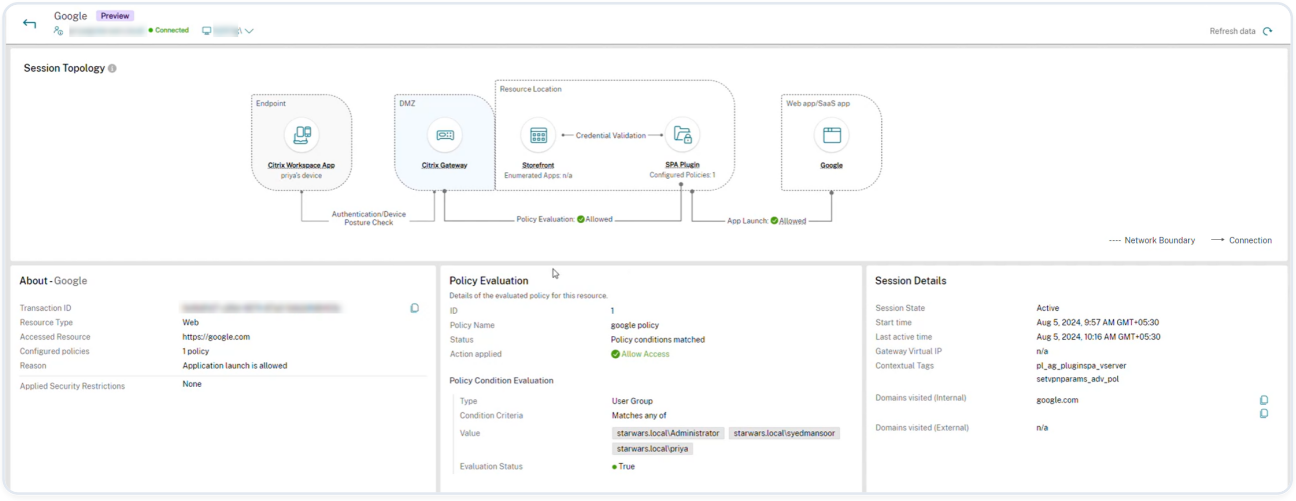
- 启动时间
- 资源名称
- 资源类型
- 已访问的资源
- 状态
- 事务 ID

您还可以使用应用程序状态（例如“**允许**”、“**拒绝**”和“**错误**”）筛选上述详细信息。您还可以使用向上和向下箭头对详细信息进行排序。

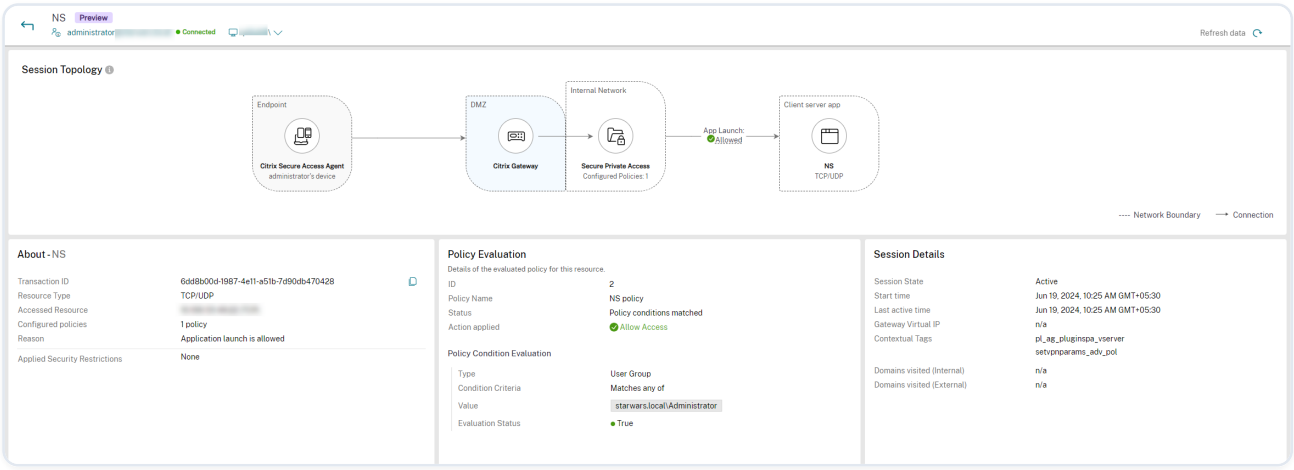
Secure Private Access 应用程序的会话拓扑视图

您可以查看使用 Secure Private Access 打开的应用程序的会话拓扑。从“**活动管理器**”中单击所需的应用程序以查看所选应用程序的会话拓扑。

Web/SaaS 应用程序：



TCP/UDP 应用程序：



会话拓扑视图提供了应用程序启动过程的流程。端点连接到 Citrix Gateway，Citrix Gateway 连接到 Secure Private Access 插件。使用 Secure Private Access 插件中的信息，应用程序得以启动。此功能适用于 Citrix Virtual Apps and Desktops 2407 或更高版本。

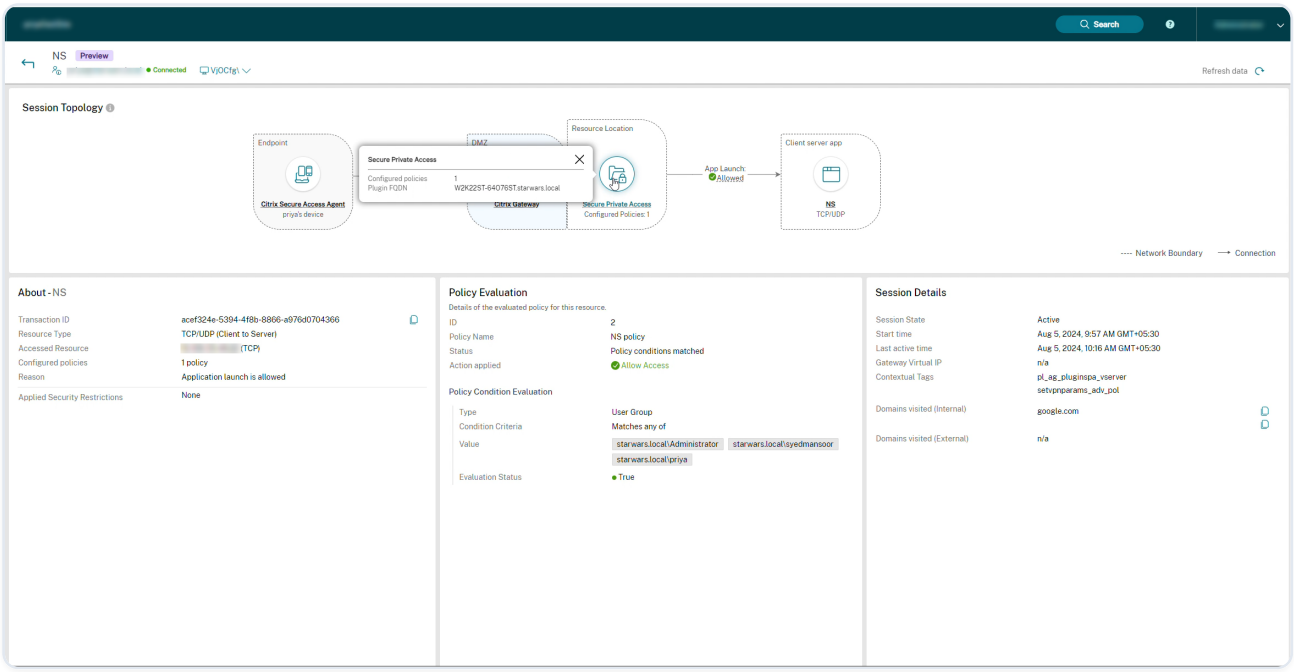
先决条件：

- Director 2407 或更高版本
- Secure Private Access 2407 或更高版本
- Citrix Secure Access 24.8.1.x 或更高版本

您可以查看以下内容：

- 端点 - 显示应用程序打开的端点。可能的选项是 Citrix Workspace 应用程序和 Citrix Secure Agent。将显示设备 ID。
- 内部网络 - 显示枚举的应用程序数量和配置的策略数量。
- 策略评估 - 显示在 Secure Private Access 应用程序上设置的策略结果。不同的值包括**允许**、**拒绝**、**受限访问**和**错误**。这仅适用于 Web 或 SaaS 应用程序。
- 应用程序已启动 - 显示应用程序类型和应用程序启动状态。应用程序类型的可能值为 Web/SaaS 应用程序或 TCP/UDP 应用程序。同样，应用程序启动状态的可能值为**允许**、**拒绝**、**受限访问**和**错误**。

您现在可以在 Secure Private Access 应用程序的**会话拓扑**视图中查看以下额外详细信息。此更改适用于 Web 和 SaaS 应用程序以及 TCP/UDP 应用程序。



端点：

点击**端点**内的链接以查看以下内容：

- **端点类型：**这可以是 Secure Access Agent 或 Citrix Workspace app。
- **访问详细信息：**查看端点是如何访问的，无论是通过 StoreFront™ 还是 Citrix Workspace app。
- **端点操作系统：**例如，Windows。
- **位置类型：**指示位置是内部还是外部。

资源位置：

点击**资源位置**内的链接以查看以下内容：

> **注意：**这仅适用于 Web 和 SaaS 应用程序。

- **枚举应用程序数量：**显示枚举应用程序的数量和商店 URL。
- **访问方法：**指示端点是通过 StoreFront 还是 Citrix Workspace app 访问的。

安全私有访问：

- **已配置策略：**显示已配置策略的数量。
- **FQDN 插件：**显示处理请求的代理的 FQDN。

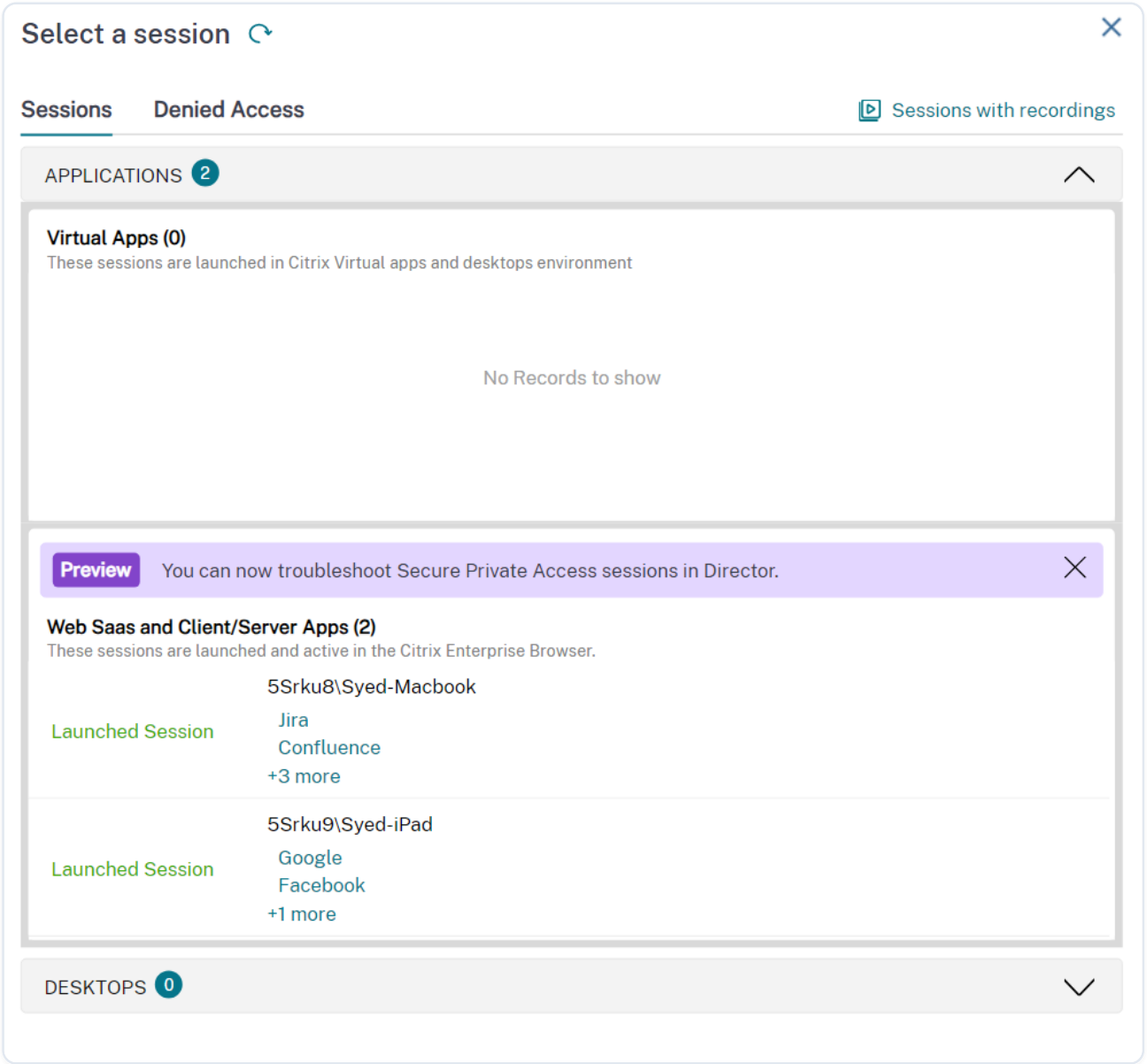
Web 和 SaaS 应用程序 / 客户端-服务器应用程序 (TCP/UDP)：

点击**Web 和 SaaS 应用程序 / 客户端-服务器应用程序**内的链接以查看以下内容：

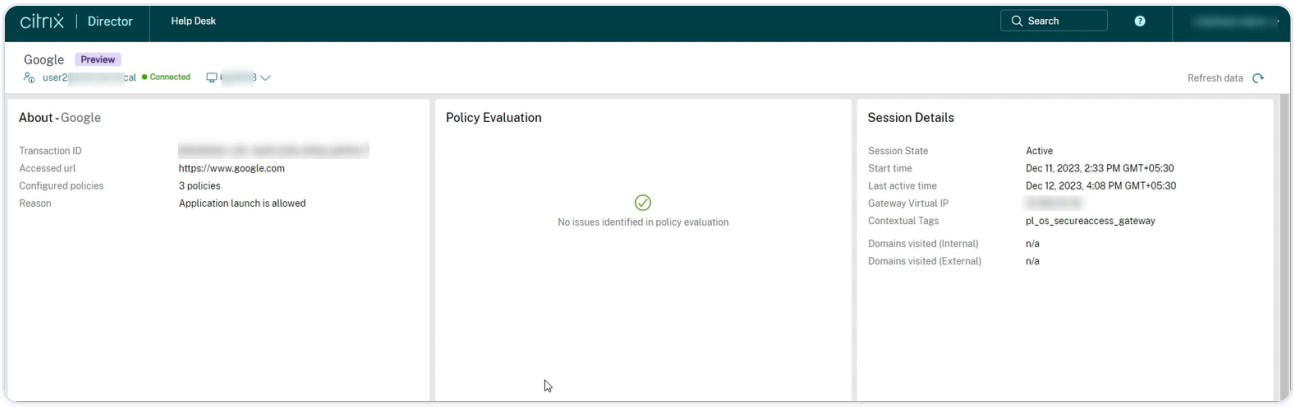
- **应用程序名称：** 应用程序的名称。
- **顶级 URL：** 对于 Web 或 SaaS 应用程序，将显示已发布的应用程序的 URL。对于 TCP/UDP 应用程序，将显示应用程序的协议 IP 地址。
- **应用程序类型：** 指示应用程序是 Web 或 SaaS 应用程序，还是 TCP/UDP 应用程序。
- **应用程序发布类型：** 指示应用程序是外部发布还是内部发布。

查看成功启动的 Web 应用和 SaaS 应用

成功启动的应用程序显示在“**Web SaaS 和客户端/服务器应用程序**”部分。



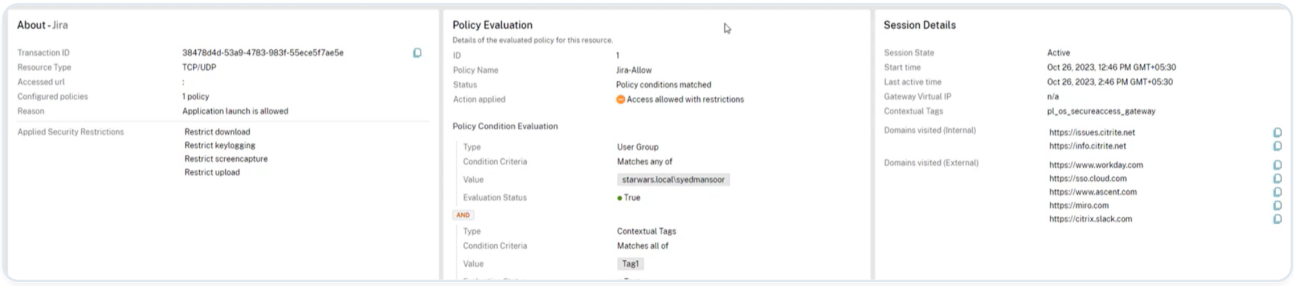
单击“**Web SaaS 和客户端/服务器应用程序**”部分中的应用程序以查看详细信息。



有关成功代码的更多信息，请参阅Citrix Director 相关代码。

查看访问被拒绝的应用的详细信息

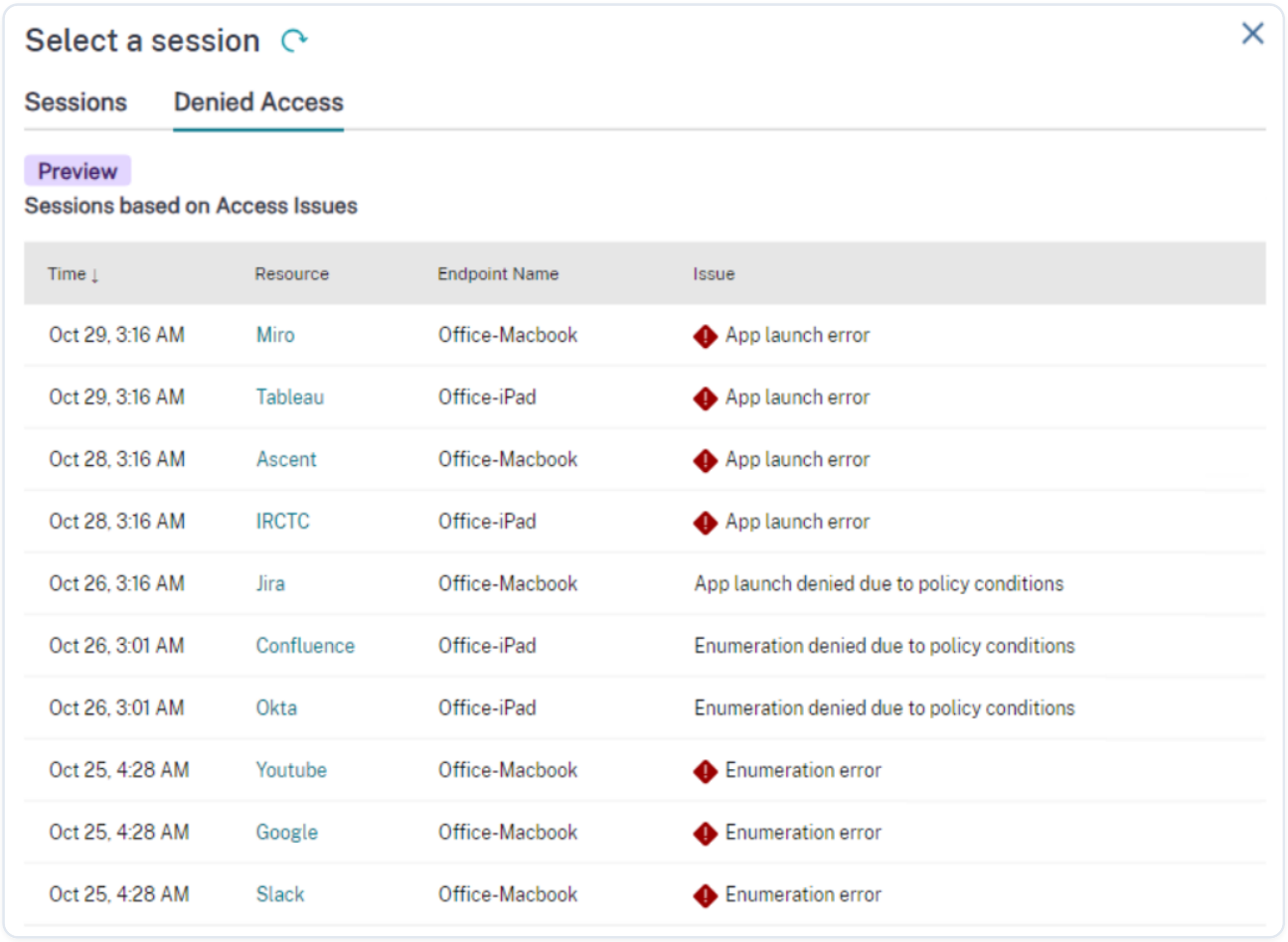
在“**选择会话**”屏幕上单击“**检查访问详细信息**”。



> **注意：**
>
> 当没有活动会话时，将显示“**检查访问详细信息**”按钮。
>
> 或者，

单击“**拒绝访问**”选项卡以查看访问被拒绝的应用。

“**拒绝访问**”选项卡随即打开。

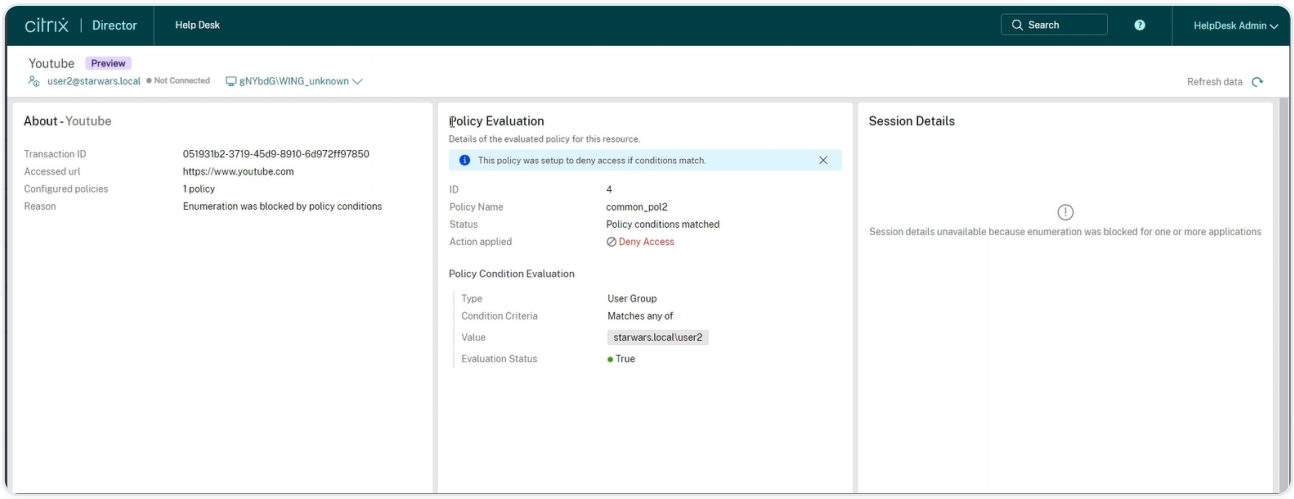


将显示会话详细信息，例如时间、资源、端点名称和失败原因。有关错误代码的更多信息，请参阅 Citrix Director 相关代码。

目前，已识别出以下问题：

- 由于策略条件，枚举被拒绝
- 应用程序启动错误
- 枚举错误
- 由于策略条件，应用程序启动被拒绝

从“**拒绝访问**”选项卡 > “**资源**”列中选择一个应用程序以查看详细信息：



成功或失败会话的以下详细信息将显示：

- 关于应用程序
- 策略评估
- 会话详细信息

关于应用程序

将显示成功、失败或被拒绝的应用程序的名称。同时，还将显示应用程序成功或失败的以下详细信息：

字段	描述
事务 ID	会话或枚举期间的 Citrix 事务 ID。
资源类型	显示资源类型。可能的值为 Web、SaaS、TCP/UDP（服务器到客户端）和 TCP/UDP（客户端到服务器）。
访问的资源	会话或枚举期间访问的资源的 URL。如果是 TCP 或 UDP 应用程序，则显示访问的资源类型是 TCP 还是 UDP。
配置的策略	会话或枚举中使用的策略数量。
原因	会话或枚举活动的分析。
应用的安全限制	显示在 Secure Private Access 应用程序中应用的安全限制。

策略评估

显示在成功会话的评估期间未发现任何问题。对于失败的会话或枚举，将显示所评估策略的以下详细信息：

字段	描述
ID	Citrix 事务 ID。
策略名称	策略的名称。如果存在多个策略，则显示与设置条件匹配的第一个策略。
状态	策略的状态。
已应用的操作	对策略应用的操作。例如，拒绝访问。
策略条件评估	
类型	策略条件的类型。
条件标准	在失败的会话或枚举中应用的策略的条件标准。
值	策略的值。
评估状态	策略的评估状态。不同的值包括“**允许**”、“**拒绝**”、“**限制访问**”和“**错误**”。

会话详细信息

对于失败的会话，将显示会话失败的原因。对于成功的会话，将显示以下详细信息：

字段	描述
会话状态	显示会话状态，无论是活动还是非活动。
开始时间	显示会话开始时间。
上次活动时间	显示成功会话的上次活动时间。
网关虚拟 IP	显示成功会话所连接的网关的虚拟 IP 地址。
上下文标签	显示上下文标签。安全私有访问插件上的上下文标签是应用于已验证用户会话的 NetScaler®

字段	描述
	Gateway 策略（会话、预身份验证、EPA）的名称。
访问的域（内部）	显示使用成功会话访问的内部域。
访问的域（外部）	显示使用成功会话访问的外部域。

Citrix DaaS™ MCP 本地服务器

Citrix DaaS MCP 服务器使支持 MCP 的 AI 代理能够连接到您的本地 Citrix Virtual Apps and Desktops™ Delivery Controller™ (DDC)。连接后，管理员可以使用兼容的 AI 客户端，通过自然语言查询站点信息、调查会话和计算机问题以及检索性能指标。

该服务器公开了 20 个只读工具，涵盖交付组、计算机目录、VDA 计算机、会话、用户、端点和站点范围的摘要。所有工具都是只读的，不会对 DDC 或站点执行任何写入操作。

Citrix DaaS MCP 服务器连接后，可以使用以下自然语言查询：

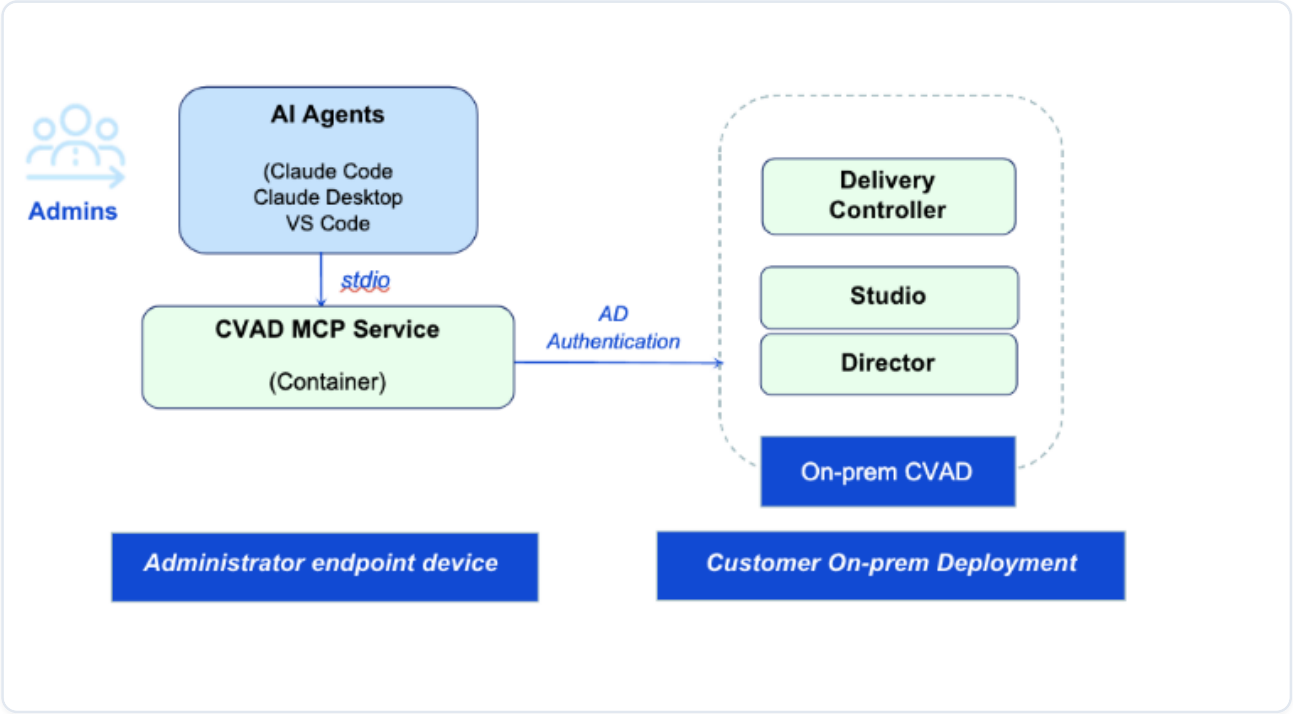
- “列出此站点中的所有交付组”
- “显示处于维护模式的计算机”
- “用户 john.smith 现在有哪些会话？”
- “显示用户 jane.doe 在过去 24 小时内的连接失败情况”
- “计算机 VDA-01 的资源使用情况和运行状况如何？”
- “哪些多会话计算机的负载最高？”
- “显示用户 john.smith 的登录明细”
- “列出所有组策略及其设置”
- “配置了哪些虚拟机管理程序连接？”
- “显示连接失败和会话计数的每小时摘要”

工作原理

Citrix DaaS MCP 本地服务器使用 模型上下文协议 (MCP)，这是一种开放协议，定义了 AI 代理如何与外部工具和数据源交互。该协议遵循客户端-服务器架构：

- **主机** - 运行 AI 代理的应用程序（例如，Claude Code、带有 MCP 扩展的 VS Code）。
- **客户端** - 主机内连接到 MCP 服务器并调用工具的组件。

- **服务器** - Citrix DaaS MCP Server Local，它公开用于查询交付控制器的工具。



该服务器在 Windows 计算机上的 Podman/Docker 容器内生成，并通过网络与 DDC 通信。当管理员发出自然语言查询时，AI 客户端将其转换为工具调用，Citrix DaaS MCP Server 根据 DDC 中的数据源（Studio 或 Director）执行查询，并将结果返回给 AI 客户端进行显示。

安全和身份验证

Citrix DaaS MCP Server Local 使用域管理员凭据向交付控制器进行身份验证。这些凭据在初始配置设置期间提供，并本地存储在安装服务器的计算机上。

主要安全特性：

- **加密的凭据存储** - 管理员凭据存储在 Windows 凭据管理器（操作系统凭据链）中，受登录用户的 Windows 帐户保护。只有配置服务器的用户才能访问存储的凭据。
- **只读访问** - 所有工具都是只读工具。服务器不会在交付控制器或 Citrix Virtual Apps and Desktops 站点内创建、修改或删除任何资源。
- **本地执行** - 服务器在管理员的计算机上本地运行。它不公开任何网络端点或接受入站连接。
- **凭据范围** - 服务器对所有查询使用配置的 DDC 管理员凭据。工具结果反映了配置帐户的权限。
- **无数据泄露** - 查询结果仅返回给本地 AI 客户端。MCP 服务器不向外部服务传输数据。

> **注意：**

> Citrix DaaS MCP Server Local 旨在供您组织内的管理员使用。请勿在机器或 AI 客户端可供未经授权的用户访问的环境中使用它。

> **注意：**
>
> 强烈建议在物理机上或在启用了嵌套虚拟化的虚拟机内使用 Windows 11。

支持的 AI 客户端

以下 AI 客户端已通过 Citrix DaaS MCP Server Local 验证：

AI 客户端	备注
Claude 代码	基于 CLI 的 AI 代理。在 Claude Code 配置中将 `citrix-daas-mcp-local` 添加为 MCP 服务器。

要从上面未列出的客户端进行连接，该客户端必须支持带 stdio 传输的模型上下文协议 (MCP)。有关添加 MCP 服务器的说明，请参阅客户端文档。

先决条件

- Windows 11 操作系统
- Node.js 18 或更高版本（建议使用 20 LTS）
- 在同一台计算机上安装了支持 MCP 的 AI 客户端
- 从计算机到 Citrix® Delivery Controller 的网络连接
- 具有站点 Citrix 管理员角色的域用户帐户
- Citrix Virtual Apps and Desktops 2402 LTSR 及更高版本

> **注意：**
>
> Citrix DaaS MCP Server Local 从与 Citrix Director 和 Studio 相同的底层源检索数据。适用于 Director 或 Studio 中某个功能的任何最低要求或先决条件也适用于通过 MCP 服务器提供的相应数据。如果某个功能需要特定的 VDA 版本、Citrix Virtual Apps and Desktops 版本或配置才能在 Director 中显示数据，则必须满足相同的要求，才能通过受支持工具中的 MCP 提供该数据。

入门

安装 Node.js

如果 `node -v` 已报告 v18 或更高版本，请跳过此部分。使用 NVM for Windows 安装 Node.js。在 PowerShell 中运行所有命令。

步骤 1：检查是否安装了 NVM

运行以下命令：

```
nvm version
```

如果此操作打印出版本号，则表示已安装 NVM，请继续执行步骤 2。如果无法识别该命令，请安装适用于 Windows 的 NVM：

```
winget install -e --id CoreyButler.NVMforWindows
```

安装后重新启动 PowerShell，以便 `nvm` 在您的 PATH 中可用。

步骤 2：安装并选择 Node.js 20

```
nvm install 20

nvm use <exact_version>
```

注意：

将 `<exact_version>` 替换为实际安装的版本，例如 20.15.1。

步骤 3：验证安装

运行以下命令并确认每个命令都返回版本号：

```
nvm version

node -v
```

```
npx -v
```

注意：

`node -v` 必须报告 v18 或更高版本。

安装和配置 Citrix DaaS MCP Server Local

步骤 1：获取捆绑包文件

从 Citrix 下载页面 下载 Citrix DaaS MCP Server Local 捆绑包文件。

步骤 2：运行配置命令

以管理员身份打开 PowerShell。导航到包含捆绑包文件的文件夹并运行：

```
npx -y .\citrix-daas-mcp-local-bundle-<version>.tgz config
```

将 `<version>` 替换为您下载的捆绑包文件的版本号。

步骤 3：完成交互式提示

config 命令会提示您输入以下环境详细信息：

提示	描述
Citrix DDC 主机	您的 Delivery Controller 的主机名。
Citrix DDC IP 地址	您的 Delivery Controller 的 IP 地址。
管理员用户	具有 DDC 权限的域管理员帐户（例如，`domain\username`）。
密码	管理员帐户的密码。

注意：

在未安装容器运行时的计算机上，config 命令会自动安装一个。如果安装提示您重新启动，请重新启动计算机并重新运行 config 命令。

步骤 4：验证安装

config 命令在配置完成后会运行内置自检。如果自检没有错误地完成，则服务器即可使用。

将 MCP 服务器连接到您的 AI 客户端

安装后，配置支持 MCP 的 AI 客户端以连接到 `citrix-daas-mcp-local` 服务器。有关添加 MCP 服务器的说明，请参阅您的 AI 客户端文档。

> **注意：**
>
> Claude Code 在步骤 3 中自动配置。其他 AI 客户端可能需要手动配置。

对于其他 AI 客户端（手动设置）

如果您使用的是其他支持 MCP 的客户端，则必须使用安装程序提供的输出手动添加服务器配置：

1. **查找配置** - 在安装过程结束时，在终端中查找标题为 的部分。
2. **复制 JSON** - 设置脚本会自动生成一个自定义 JSON 片段，其中包含您计算机的精确文件路径。复制整个 JSON 块。
3. **更新客户端** - 将复制的 JSON 粘贴到 AI 客户端的 MCP 配置文件中（有关确切的文件位置，请参阅特定客户端的文档）。
4. **重新启动** - 重新启动 AI 客户端或开始新的聊天会话以加载新的 MCP 服务器配置。

要复制的生成配置块示例：

```
{
  "citrix-daas-mcp-local": {
    "command": "C:\\path\\to\\node.exe",
    "args": [
      "C:\\path\\to\\daas-mcp-local\\cli.js",
      "run"
    ],
    "env": {
```

```
      "DAAS_MCP_LOCAL_CONFIG": "C:\\path\\to\\config.json"
    }
  }
}
```

连接后，验证服务器是否已加载及其工具是否可用。您可以通过发出自然语言查询（例如“列出此站点中的交付组”）进行测试。

常用工具参数

有几个工具共享通用的输入参数。下表描述了所有工具接受的输入格式。

计算机名称格式

接受计算机名称的工具支持以下格式：

格式	示例
规范 (DOMAIN\HOSTNAME)	`CTXCO\TestVDA1`
仅主机名	`TestVDA1`
完全限定域名 (FQDN)	`TestVDA1.ctxco.local`

如果提供的名称与单个计算机不完全匹配，该工具会尝试进行模糊查找。当有多台计算机匹配时，澄清响应会列出候选计算机。

用户名格式

接受用户名的工具使用 `domain\username` 格式（例如，`nkgdir\john.smith`）。搜索工具支持部分匹配。

时间窗口参数

多个工具接受时间窗口以控制回溯检索数据的时长：

参数	默认值	最大值	使用者
`latest_hours`	2 小时	2 小时	`get_session_metrics`, `get_endpoint_metrics`
`offset_hours`	2 小时	7 天	`get_connection_failures`（按用户）

可用工具

Citrix DaaS MCP Server Local 提供了 20 个按区域组织的工具。所有工具都是只读的，它们查询 Delivery Controller 并返回数据，而不会修改任何资源。

站点概述

工具	描述
`get_hourly_summaries`	按类型检索当前连接失败计数、按类型检索失败的 VDI 和 RDS 计算机计数，以及检索过去一小时内的连接会话活动。
`get_hypervisors_info`	列出所有虚拟机管理程序连接或检索特定虚拟机管理程序的详细配置。
`get_group_policy_list`	检索站点组策略列表，包括策略名称、优先级、启用状态、设置和筛选器。

交付组

工具	描述
`search_delivery_groups`	搜索并列出交付组，可按名称、维护模式、启用状态、共享类型和会话支持进行筛选。
`get_delivery_group_details`	按名称或 ID 检索特定交付组的详细信息。

计算机目录

工具	描述
`search_machine_catalogs`	搜索并列出计算机目录，可按名称、物理计算机、分配类型、预配类型和会话支持进行筛选。
`get_machine_catalog_details`	按名称或 ID 检索特定计算机目录的详细信息。

VDA 计算机

工具	描述
`search_vda_machines`	搜索计算机，可按交付组、计算机目录、代理版本、操作系统类型、标签、维护模式、电源状态、注册状态、会话状态和故障状态进行筛选。
`get_vda_machine_details`	按名称或 ID 检索特定 VDA 计算机的详细信息。
`get_vda_machine_resource_usage`	使用运行状况评估分析计算机资源利用率指标，包括统计分析（平均值、P95、最大值），以进行异常检测、饱和模式检测和可操作的建议。
`list_top_vda_machines_by_load_index`	列出按有效负载指数排名的负载最重的多会话操作系统 VDA 计算机。

会话

工具	描述
`search_sessions`	使用用户、计算机、交付组、计算机目录、代理版本、操作系统类型、会话状态、会话支持和正在使用的应用程序等筛选器搜索会话。
`get_session_details`	按会话 ID 检索特定会话的完整详细信息。
`get_session_metrics`	检索用户或会话在过去 2 小时内的会话性能指标。时间间隔内的指标中断可能表示该期间会话已断开连接。

工具	描述
`get_session_logon_breakdown_metrics`	检索用户的登录持续时间明细指标，显示每个登录步骤的持续时间、开始时间和结束时间。

用户和端点

工具	描述
`get_active_machines_by_user`	列出用户当前具有活动会话的 VDA 计算机，包括计算机名称、DNS 名称、IP 地址和代理版本。
`get_active_users_by_machine`	列出在特定计算机上具有活动会话的用户，包括用户名、UPN、全名和域。
`get_endpoint_metrics`	检索用户或会话在过去 2 小时内的端点（客户端）设备指标。
`get_connection_failures`	检索用户的失败连接尝试（最多过去 7 天）或按事务 ID 检索（最多 90 天），包括失败原因和失败时的计算机状态。

高级查询

工具	描述
`run_dynamic_odata`	针对 CVAD Monitor OData 服务运行自定义 OData 查询。支持最多 10,000 行的自动分页。
`get_odata_reference`	指示 AI 客户端检索 Citrix Monitor OData 文档。如果在线文档不可用，该工具将回退到与映像捆绑的参考文档。

更新配置

要更改任何设置（DDC 主机、管理员凭据等），请重新运行 config 命令：

```
npx -y .\citrix-daas-mcp-local-bundle-<version>.tgz config
```

已知限制

限制	详细信息
会话和端点指标窗口	`get_session_metrics` 和 `get_endpoint_metrics` 仅返回过去 2 小时的数据。
连接失败回溯	`get_connection_failures` 支持按用户名回溯最多 7 天。
OData 行限制	`run_dynamic_odata` 每次查询最多返回 10,000 行。
编排工具限制	检索配置详细信息的工具有最多 500 个的限制。计算机和会话列表可能会被截断。
单站点连接	服务器一次连接到一个 Citrix 站点。要查询不同的站点，请重新运行 config 命令并提供该站点的 Delivery Controller。
仅限本地执行	服务器必须与 AI 客户端在同一台计算机上运行。不支持远程或托管的 MCP 服务器部署。

故障排除

Citrix DaaS MCP Server Local 包含一个用于诊断问题的 doctor 命令。当服务器行为异常时运行它：

```
npx -y .\citrix-daas-mcp-local-bundle-<version>.tgz doctor
```

doctor 命令会检查服务器操作的每个阶段，并报告失败的阶段以及补救措施。

config 命令成功后，Citrix 工具或 citrix-daas-mcp-local MCP 服务器缺失或被阻止?

解决方案：

- 对于 Claude Code 以外的 AI 客户端，请手动配置 MCP 服务器。有关详细信息，请参阅其他 AI 客户端（手动设置）。
- 如果您的 AI 客户端强制执行 MCP 允许列表，请确保允许 `citrix-daas-mcp-local`。有关详细信息，请参阅您的 AI 客户端文档。
- 重启 AI 客户端或启动新会话。

安装后 NVM 未被识别?

解决方案：

- 关闭并重新打开 PowerShell。
- 运行 `nvm version` 以确认 NVM 在您的 PATH 中。
- 如果仍然无法识别，请重启计算机并重试。

Node.js 版本低于 18?

解决方案：

- 运行 `nvm install 20` 以安装 Node.js 20。
- 运行 `nvm use <exact_version>` 以切换到已安装的版本。
- 通过 `node -v` 进行验证。

容器运行时在配置期间安装失败?

解决方案：

- 在计算机上手动安装 Docker Desktop 或 Podman。
- 容器运行时可用后，重新运行配置命令。

系统启动后容器运行时未就绪?

解决方案：

- 容器运行时完成启动后，重新连接到 MCP 服务器。

多个容器正在运行?

解决方案：

- 关闭任何不再需要的 AI 客户端会话。相应的容器将自动停止。

服务器无响应或返回错误?

解决方案：

- 运行 doctor 命令并按照报告的补救措施进行操作。
- 验证与 DDC 的网络连接（确认可从本机访问 DDC 主机名和 IP）。
- 验证管理员凭据是否正确并具有所需的权限。

工具未在 AI 客户端中加载?

解决方案：

- 验证服务器是否在您的 AI 客户端的 MCP 服务器列表中显示为已连接。
- 添加服务器后重新启动 AI 客户端会话。
- 运行 doctor 命令以确认服务器配置有效。
- 检查是否已安装 Node.js 18 或更高版本，并且在您的 PATH 中可用。

查询返回空结果或意外错误?

解决方案：

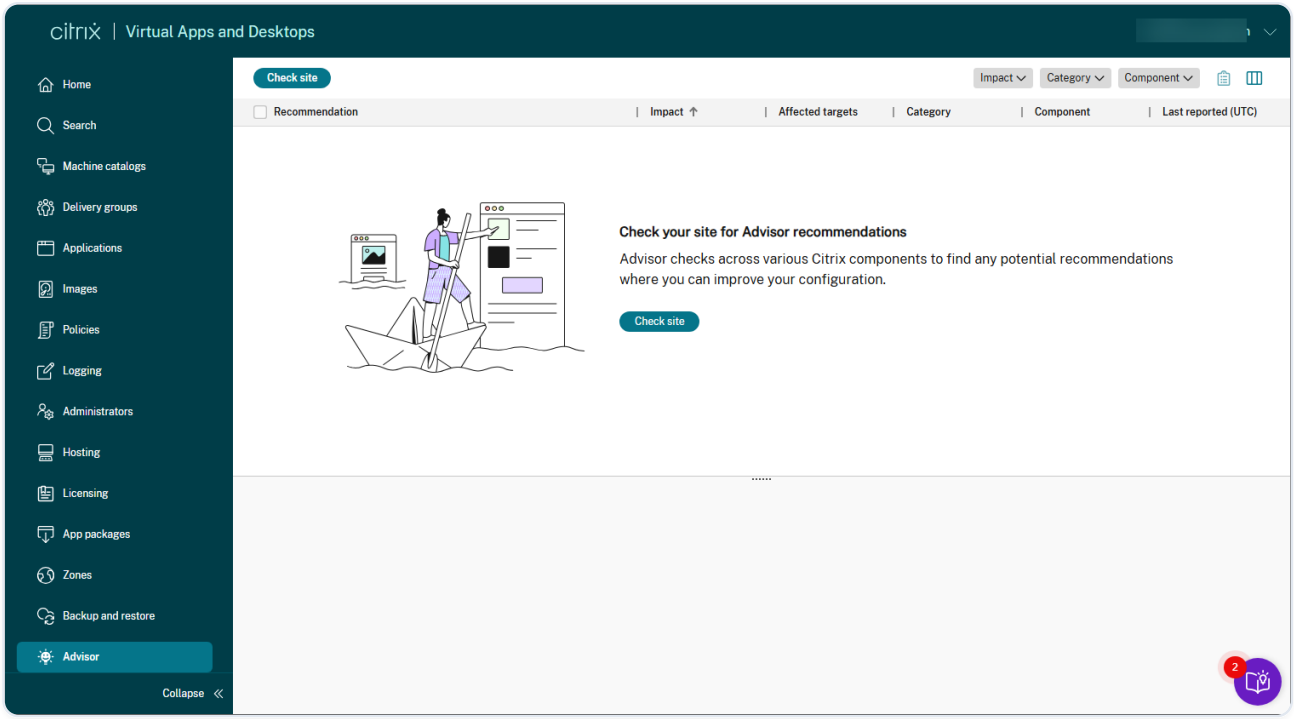
- 验证 DDC 可从本机访问。
- 确认配置的管理员帐户在 DDC 上具有所需的权限。
- 检查 Delivery Controller 服务是否正在运行。
- 运行 doctor 命令以进行全面诊断。

命令参考

命令	目的
`npx -y .\citrix-daas-mcp-local-bundle-<version>.tgz config`	安装或重新配置服务器和容器运行时。首次安装时运行自检。
`npx -y .\citrix-daas-mcp-local-bundle-<version>.tgz doctor`	诊断服务器配置或连接问题。

顾问

Citrix Advisor 是一项服务，可帮助您优化 Citrix Virtual Apps and Desktops 部署并增强其整体运行状况和就绪情况。它可自动执行环境检查并提供可操作的建议，使您能够主动识别配置问题、效率低下、资源浪费、偏离最佳实践等问题。



注意：

- 此服务仅适用于**完全管理员**。
- 我们建议您使用页面右上角的反馈图标提交反馈。

优势

借助 Advisor，您可以：

- **主动识别并解决问题**：在潜在问题、配置漂移以及偏离最佳实践影响用户、中断业务运营或损害安全性之前检测到它们。

- **优化环境性能和稳定性**：微调配置、优化资源分配并实施最佳实践，以增强 Citrix 部署的稳定性、安全性和性能。
- **简化操作并降低开销**：自动执行例行检查、简化复杂的修复任务并获得指导性帮助，从而降低运营开销并释放管理资源。
- **优化成本和资源利用率**：识别超支领域、发现资源优化机会，并确保有效利用 Citrix 技术，以最大限度地降低总拥有成本。
- **保持合规性并遵循最佳实践**：确保您的 Citrix 部署遵循 Citrix 最佳实践、安全标准和行业法规，从而降低风险并改善整体治理。
- **简化复杂任务**：简化管理任务，以支持健康、优化的环境。

检查建议

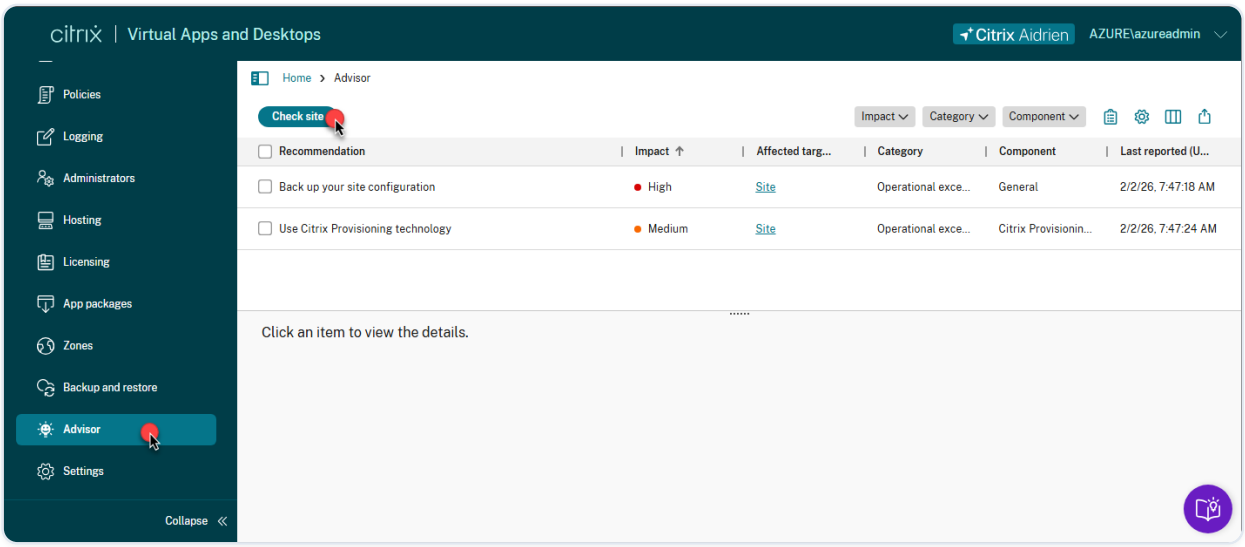
要检查您的站点以获取 Advisor 建议，请执行以下步骤：

1. 使用具有 **Full Administrator** 角色的帐户登录 Web Studio。
2. 在左侧窗格中，选择 **Advisor**。
3. 单击 **检查站点**。
4. 在 **检查站点** 页面上，选择您希望 Advisor 检查的类别。

类别	描述	参考
安全性	检测可能导致安全漏洞的威胁和漏洞的建议。	(#security-recommendations)
可靠性	确保和改进业务关键型应用程序连续性的建议。	可靠性建议
性能	旨在提高应用程序和桌面性能的建议，为最终用户提供更快、响应更灵敏的体验。	性能建议
卓越运营	旨在帮助您实现流程和工作流效率、资源可管理性以及部署最佳实践的建议。	卓越运营建议
成本优化	旨在通过调整资源规模、最大限度地减少浪费以及使容量与实际使用需求保持一致来降低总体支出的建议。	成本优化建议

5. 单击 **运行检查** 以运行站点检查并根据当前配置生成更新的建议。

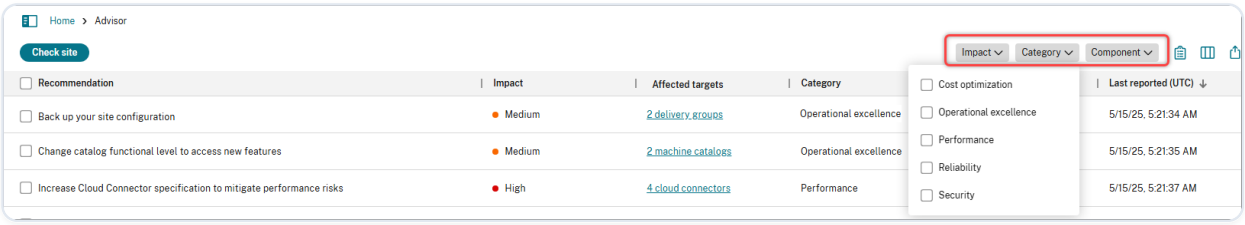
   所有建议都显示在列表中。



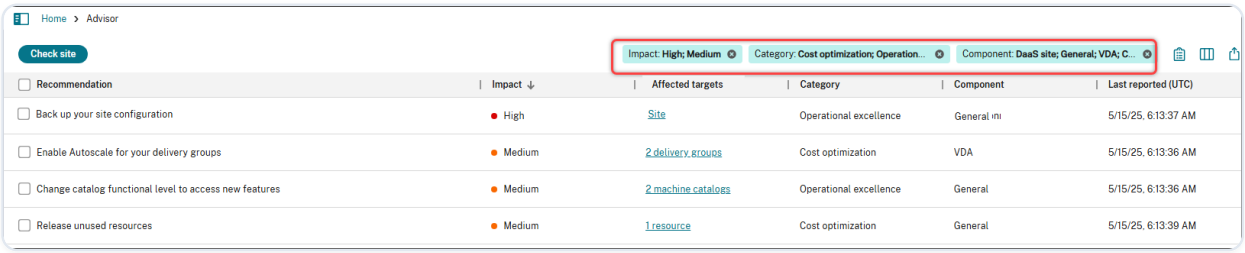
筛选建议

您可以按**影响**、**类别**或**组件**筛选建议，以专注于与您的部署最相关的信息。

1. 在 **Advisor** 中，找到建议列表右上角的筛选器。



2. 单击筛选器（例如，**类别**）以查看可用选项。
3. 选择一个或多个复选框以应用筛选器。列表会自动更新，仅显示与您的选择匹配的建议。
4. 同时使用多个筛选器以缩小列表范围。



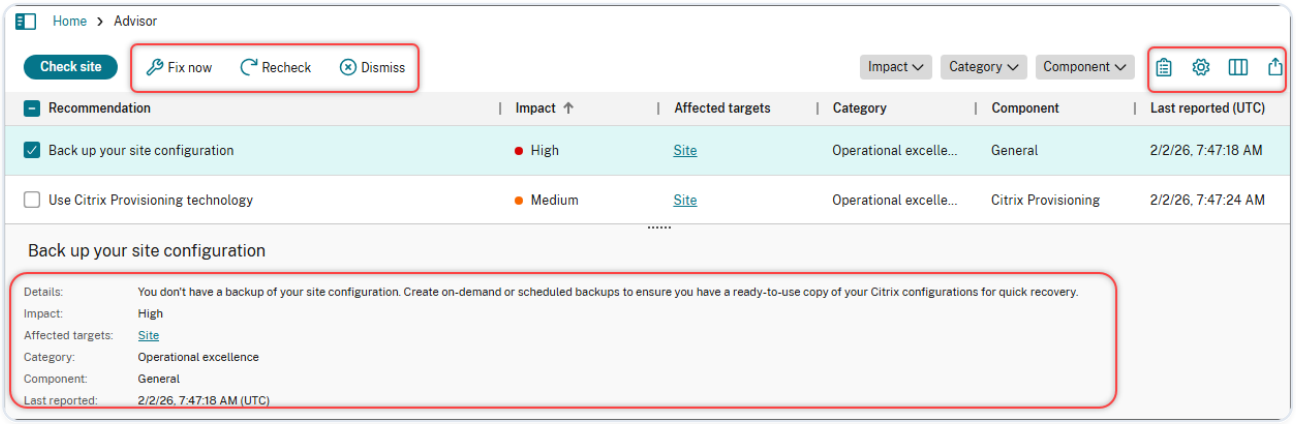
查看并处理建议

使用建议列表了解部署中的配置问题和改进机会。您可以对建议执行以下操作：

- 查看建议详细信息
- 实施建议的操作
- 关闭建议
- 关闭建议中受影响的特定目标
- 自定义检查规则
- 查看完整的站点检查报告

查看建议详情

要查看建议，请选择一个建议以在下部窗格中查看其详细信息。

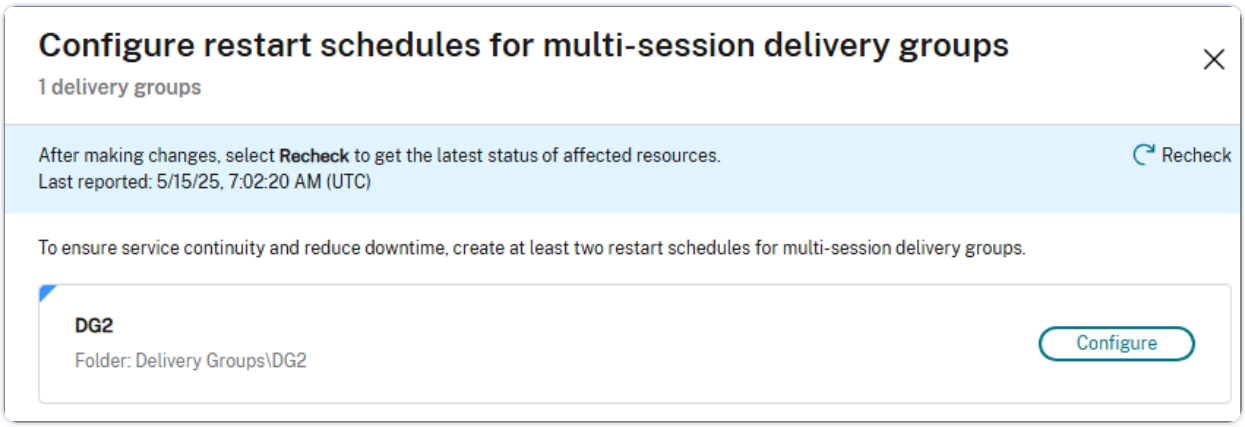


实施建议的操作

要实施建议的操作，请按照以下步骤操作：

1. 选择一个建议。
2. 在操作栏中单击**立即修复**。
3. 按照建议的步骤进行必要的更新。

   有时，当不支持或无法实现自动化配置时，您会被定向到支持文档。我们希望确保 Advisor 旨在尽可能直接在 UI 中提供自动化操作，从而最大限度地减少手动设置的需求。
4. 进行更新后，单击**重新检查**以更新受影响目标的状态。



> **注意：**
>
> UI 和步骤因建议而异。显示的屏幕截图仅用于说明目的。

关闭建议

如果某个建议与您的部署不相关或不需要采取措施，您可以将其从当前列表和未来的检查结果中删除：

1. 选择建议。
2. 在操作栏中点击“**忽略**”。

> **提示：**
>
> 要恢复建议，请单击建议列表上方右上角的**齿轮**图标，然后选择**管理已忽略的项目**

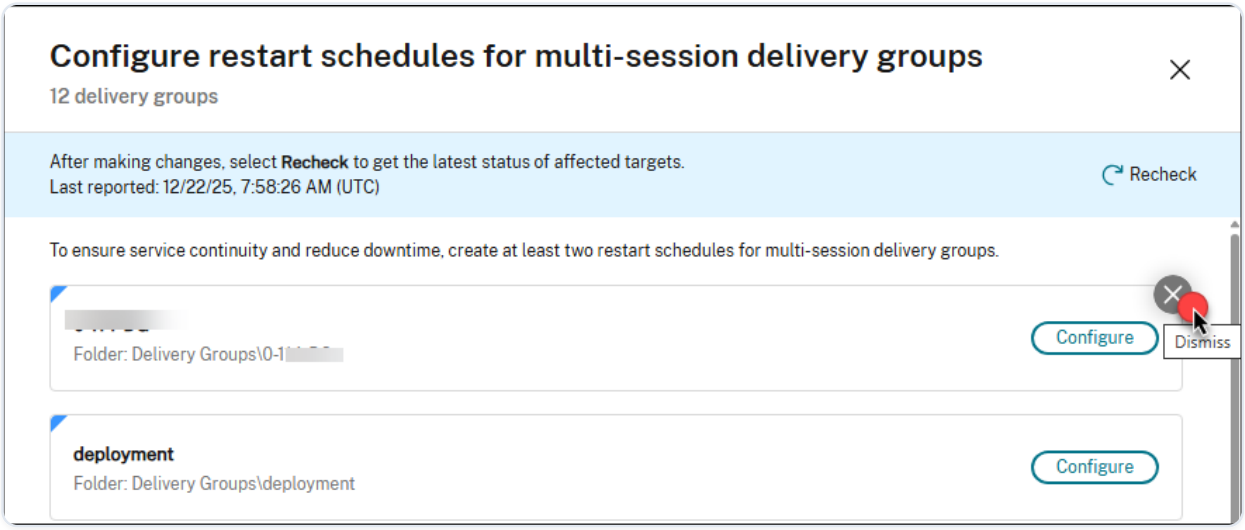
忽略建议中特定的受影响目标

如果某个建议包含有意不符合最佳实践的受影响目标（*例如*，测试、验证或临时资源），您可以从该建议中将其删除（也称为 `granular dismissal`）。

> **注意：**
>
> 精细忽略仅支持以下目标：计算机目录、交付组、应用程序组和区域。

> 详细步骤如下：

1. 选择建议。
2. 点击建议的“**受影响目标**”字段。建议页面将显示所有受影响的目标。
3. 将鼠标悬停在要忽略的受影响目标上。目标的右上角会出现一个“**忽略**”图标。



4. 点击“**忽略**”图标。将出现一个忽略确认对话框。
5. 如果需要，输入忽略备注，然后点击“**忽略**”。受影响的目标将从建议页面中移除。

> **提示：**
>
> 要恢复建议中已关闭的目标，请单击建议列表右上角的齿轮图标，然后选择 **管理已关闭的项目**。

自定义检查规则

您可以自定义 Advisor 检查规则以用于以下建议：

- **增强 Cloud Connector 硬件：** 调整 CPU、内存和磁盘使用率的阈值，并排除特定磁盘。
- **释放未使用的资源：** 定义用于计算机和应用程序的自定义未使用时间阈值。
- **优化 VDA 的 GPO 配置：** 修改 GPO 处理时间阈值。

要自定义单个建议的检查规则，请按照以下步骤操作：

1. 选择一个建议，然后单击操作栏中的 **自定义**。



2. 在 **自定义** 页面上，根据需要更新检查设置。
3. 单击 **保存**。更改将在下次运行检查时生效。

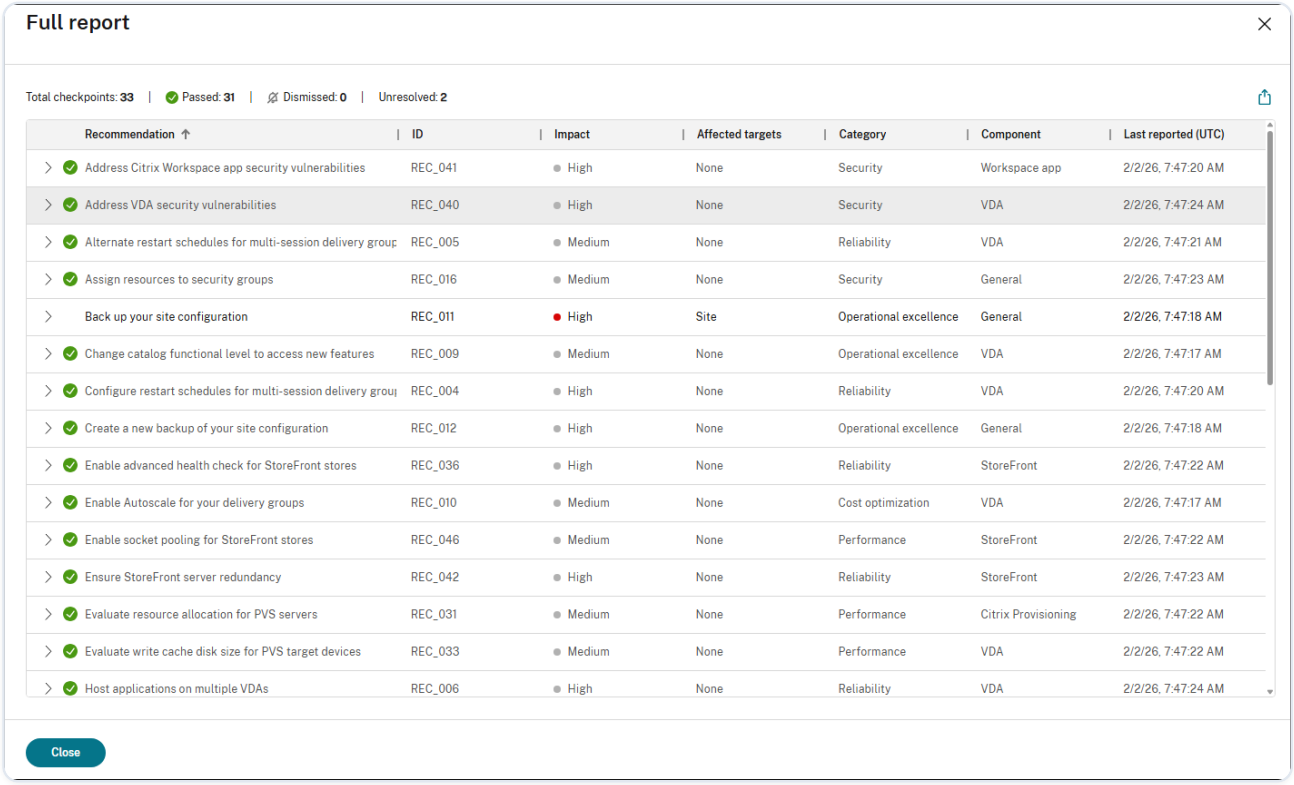
要从中心位置自定义所有三个建议的检查规则，请按照以下步骤操作：

1. 单击建议列表右上角的 **齿轮** 图标，然后选择 **自定义规则**。这三个建议将显示。
2. 单击建议旁边的 **编辑** 图标。
3. 根据需要更新检查设置。
4. 要更新其余建议的检查规则，请重复步骤 2-3。
5. 单击 **保存**。更改将在下次运行检查时生效。

查看完整的站点检查报告

完整报告提供了最新站点检查中所有 Advisor 建议的摘要。它包括已通过、已忽略和未解决的检查点，可帮助您评估 DaaS 站点的整体运行状况和优化机会。

要查看完整报告，请单击建议列表右上角的**查看完整报告**图标。



为 Advisor 检查设置 StoreFront™

Citrix Advisor 中与 StoreFront 相关的建议需要额外设置。要为 Advisor 检查设置 StoreFront，请完成以下步骤：

1. 通过创建相应的连接，将您的 StoreFront 服务器添加到基础结构监控中。有关详细信息，请参阅基础结构监控。
2. 如果您在 **手动连接** 模式下配置 StoreFront 连接，请确保已下载并安装 Citrix Infrastructure Monitoring 2603 或更高版本。要验证是否已安装所需版本：
   a. 转到 **Director > 设置**。
   b. 找到 **类型** 等于 `StoreFront` 的连接。
   c. 确认 **版本** 字段显示 `7.47` 或更高版本。

> **重要提示：**
>
> 根据 Advisor 建议对 StoreFront 部署应用更改后，请至少等待 6 小时再重新检查相同的建议。此延迟允许基础结构监视收集和处理更新的遥测数据，并确保 Advisor 评估最新数据。

参考

本节按类别列出了所有 Citrix Advisor 建议，以帮助您了解其目的和影响。

安全建议

建议	ID	影响	组件	描述
升级已达到生命周期结束的 VDA	REC_001	高	VDA	某些计算机正在使用已达到生命周期结束且不再受 Citrix 支持的 VDA 版本。将受影响的计算机升级到最新的 LTSR 或 CR VDA 版本。
将资源分配给安全组	REC_016	中等	常规	某些资源已分配给单个用户。Citrix 最佳实践是仅通过安全组分配用户访问权限，以简化管理并增强安全性。

建议	ID	影响	组件	描述
				重新配置交付组和应用程序组的用户分配，使其仅包含安全组。
升级已终止支持的 Citrix Workspace 应用程序版本	REC_017	高	Workspace 应用程序	某些端点设备使用的 Citrix Workspace 应用程序版本已终止支持。将设备升级到最新的 Workspace 应用程序版本，以降低可支持性和安全风险。为了简化版本管理和自动更新控制，请使用全局应用程序配置服务。此外，请考虑使用端点分析解决方案来强制执行最低 Workspace 应用程序版本才能访问应用商店。
对主机连接使用 HTTPS	REC_039	中等	常规	某些主机连接当前配置为使用 HTTP 而非 HTTPS。为确保与您的虚拟机管理程序进行安全通信，请将这些连接更新为使用 HTTPS。这需要在您的虚拟机管理程序上启用 HTTPS 并确保已安装有效的 TLS 证书。

建议	ID	影响	组件	描述
升级已达到生命周期结束 (EOL) 的 StoreFront 服务器版本	REC_043	高	StoreFront	某些 StoreFront 服务器正在运行已达到生命周期终止 (End of Life) 且不再受 Citrix 支持的版本。为了维护安全、可支持的环境，请将所有受影响的 StoreFront 服务器升级到最新的 LTSR 或 CR 版本。
为 StoreFront 基本 URL 使用 HTTPS	REC_044	高	StoreFront	某些 StoreFront 基本 URL 当前配置为使用 HTTP 而非 HTTPS。为了保护用户凭据和敏感数据，请将您的 StoreFront 服务器和关联的负载均衡器配置为使用 HTTPS。请确保基本 URL 以“https://”开头。这可确保所有通信都经过加密，并有助于防止中间人攻击等安全威胁。
StoreFront 和 Delivery Controller 之间使用 HTTPS 进行通信	REC_045	高	StoreFront	StoreFront 和 Delivery Controller 之间的流量目前通过未加密的 HTTP 传输，这可能会

建议	ID	影响	组件	描述
				使用户凭据面临安全威胁。为了保护您的环境，请在 Delivery Controller 上启用 HTTPS 并将 StoreFront 配置为使用安全连接。

注意：

StoreFront 相关建议需要额外设置。有关详细信息，请参阅为 Advisor 检查设置 StoreFront。

可靠性建议

建议	ID	影响	组件	描述
为多会话交付组配置重新启动计划	REC_004	高	VDA	某些多会话交付组未配置重启计划。计划重启有助于在多会话操作系统 VDA 中保持最佳性能、稳定性和资源可用性。为确保服务连续性并减少停机时间，请至少创建两个重启计划。通过将 VDA 标记为“偶数”和“奇数”等组，使用标签限制交替重启计划。
在多个 VDA 上托管应用程序	REC_006	高	VDA	某些已发布的应用程序仅托管在一个 VDA 上，

建议	ID	影响	组件	描述
				这可能会影响服务连续性并导致停机风险。请确保每个应用程序都托管在交付组中的多个 VDA 上，以帮助保持可用性和可靠性。
将 VDA 升级到与目录功能级别匹配	REC_008	高	VDA	某些计算机使用的 VDA 版本较早，不受最低目录功能级别支持，这可能会阻止它们注册。为避免注册问题，请将较早的 VDA 版本升级到与目录功能级别匹配。
为 StoreFront 商店启用高级运行状况检查	REC_036	中等	StoreFront	某些 StoreFront 服务器上有一个或多个商店未启用高级运行状况检查。StoreFront 使用高级运行状况检查结果中的附加信息，以确保在本地主机缓存 (LHC) 模式下将启动请求发送到适当的资源位置（区域）。如果没有高级运行状况检查，在 LHC 模式下启动可能会失败。为了提高 Citrix

建议	ID	影响	组件	描述
				环境的弹性，请为 StoreFront 服务器上的所有商店启用高级运行状况检查。
确保 StoreFront 服务器冗余	REC_042	高	StoreFront	某些 StoreFront 服务器组只包含一台服务器，这会造成单点故障，并在发生中断时缺乏冗余。为了提高弹性，请在服务器组中部署至少两台 StoreFront 服务器，并在它们前面放置负载均衡器，以确保无缝故障转移和不间断访问。

注意：

与 StoreFront 相关的建议需要额外设置。有关详细信息，请参阅为 Advisor 检查设置 StoreFront。

性能建议

建议	ID	影响	组件	描述
调整高资源消耗计算机的大小	REC_023	中等	VDA	某些计算机显示出性能紧张的迹象，例如高 CPU 或内存利用率，或高会话计数。这表明计算机的规模不足以处理其支持的

建议	ID	影响	组件	描述
				工作负载，这可能导致糟糕的用户体验和性能下降。请考虑更改计算机大小以增加为计算机分配的资源，或将高级用户重新分配到具有高性能计算机的交付组。
评估 PVS 服务器的资源分配	REC_031	中等	预配	某些 Citrix Provisioning (PVS) 服务器显示出性能紧张的迹象，例如 CPU 或内存利用率高。服务器资源分配不足可能导致性能不佳和启动时间延长。请根据需要考虑增加这些 PVS 服务器的 CPU 和内存分配。
增加 PVS 服务器的资源分配	REC_032	高	预配	某些 Citrix Provisioning (PVS) 服务器显示出性能压力迹象，例如关键 CPU 或内存利用率。服务器资源分配不足可能导致性能不佳和启动时间延长。请考虑根据需要增加这些 PVS 服务器的 CPU 和内存分配。

建议	ID	影响	组件	描述
评估 PVS 目标设备的写入缓存磁盘大小	REC_033	中等	VDA	某些 Citrix Provisioning (PVS) 目标设备上的写入缓存磁盘使用量已接近阈值。为避免性能问题和用户会话失败，请评估当前的写入缓存磁盘大小并根据需要进行增加。
优化 VDA 的 GPO 配置	REC_035	中等	VDA	某些用户会话在登录期间经历了长时间的 GPO 处理，影响了性能。为了增强对环境设置的控制，请阻止 VDA 组织单位的组策略继承，并仅应用相关的策略和安全配置。此外，考虑利用 Citrix Workspace Environment Management 异步处理设置，以加快会话登录速度。
为 StoreFront 商店启用套接字池	REC_046	中等	StoreFront	某些 StoreFront 商店未启用套接字池。套接字池通过维护一个随时可用的网络连接（套接字）池来增强效率，用于与 Delivery Controllers 或

建议	ID	影响	组件	描述
				Cloud Connectors 进行通信。StoreFront 不会为每个请求创建新套接字然后将其关闭（这是一个高开销的过程），而是从池中重用现有连接。为了提高整体环境性能和效率，请在所有商店上启用套接字池，特别是对于传输层安全 (TLS) 连接。

注意：

与 StoreFront 相关的建议需要额外设置。有关详细信息，请参阅 为 Advisor 检查设置 StoreFront。

卓越运营建议

建议	ID	影响	组件	描述
将 VDA 升级到最新版本	REC_002	低	VDA	某些计算机正在使用较旧的 VDA 版本。升级到最新的 LTSR 或 CR VDA 版本以访问新功能、改进和安全增强功能。

建议	ID	影响	组件	描述
使用 Citrix 预配技术	REC_003	中等	预配	站点中的所有计算机都是手动预配的，并且不使用 Citrix 预配技术，例如 Machine Creation Services (MCS) 或 Citrix Provisioning Services (PVS)。使用 MCS 或 PVS 可确保 VDA 一致性，最大限度地减少手动任务，并简化环境扩展操作。
备份您的站点配置	REC_011	高	常规	您没有站点配置的备份。创建按需或计划备份，以确保您拥有可立即使用的 Citrix 配置副本，以便快速恢复。
重置受污染的 Active Directory 帐户	REC_049	中等	预配	某些计算机目录包含在 AD 身份服务中标记为“受污染”的 AD 帐户。必须重置这些帐户才能用于后续预配操作。

注意：

> StoreFront 相关建议需要额外设置。有关详细信息，请参阅 为 Advisor 检查设置 StoreFront。

成本优化建议

建议	ID	影响	组件	描述
为交付组启用自动缩放	REC_010	中等	VDA	一些符合条件的交付组未使用自动缩放。启用自动缩放以实现一致的计算机电源管理，在有效平衡成本和用户体验的同时保持可用性。
释放未使用的资源	REC_013	中等	常规	一些专用工作负载（例如计算机或应用程序）已超过 30 天未使用。为了减少不必要的开支并优化成本，请将未使用的计算机释放回可用池并管理未使用的应用程序。

Citrix VDA 升级服务 (VUS)

技术预览版中的功能

技术预览版中的功能可在非生产或有限生产环境中使用，并为客户提供分享反馈的机会。Citrix 不接受技术预览版功能的任何支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、关键性和重要性采取行动。

这并非交付任何材料、代码或功能的承诺、保证或法律义务，也不应作为 Citrix 产品采购决策的依据。任何功能或特性的开发、发布和时间安排均由我们全权决定，并且可能在不另行通知或咨询的情况下进行更改。

Citrix VDA 升级服务概述

Citrix VDA 升级服务 (VUS) 是 Citrix Virtual Apps and Desktops™ (CVAD) 的一个组件，旨在为您的 Citrix 环境中持久性 Virtual Delivery Agents (VDA) 提供简化的升级流程。该服务有助于使您的环境保持最新的 VDA 版本，从而提升性能和安全性，并启用新的 Citrix DaaS 功能。

管理员可以利用 VUS 检查更新、安排升级和监控升级进度。升级可以立即启动，也可以安排在特定日期和时间进行，使您能够选择最佳的升级时间。

升级 VDA 从未如此简单。在您的 VDA 或映像上安装 VDA 升级代理，在 Web Studio 中右键单击计算机或计算机目录，选择“升级 VDA”，然后选择最适合您环境的选项。

在升级之前，请查看升级周期选项。您的 VDA 有两种升级轨道可用：长期服务版本 (LTSR) 和当前版本 (CR)。LTSR 具有更长的支持生命周期，提供更高的稳定性和更少的升级频率。CR 版本发布更频繁，提供最新和最强大的功能。有关详细信息，请参阅 生命周期里程碑。

使用 VUS 升级 VDA 的先决条件

要使用 VUS 执行 VDA 升级，必须满足以下前提条件。

为您的站点启用 VDA 升级服务

要为您的 2503 站点启用 VUS，请运行以下 PowerShell cmdlet：

```
Set-VusSite -Enabled $true
```

启用后，通过运行以下 PowerShell cmdlet 将最新 VDA 版本导入到您的 CVAD 站点：

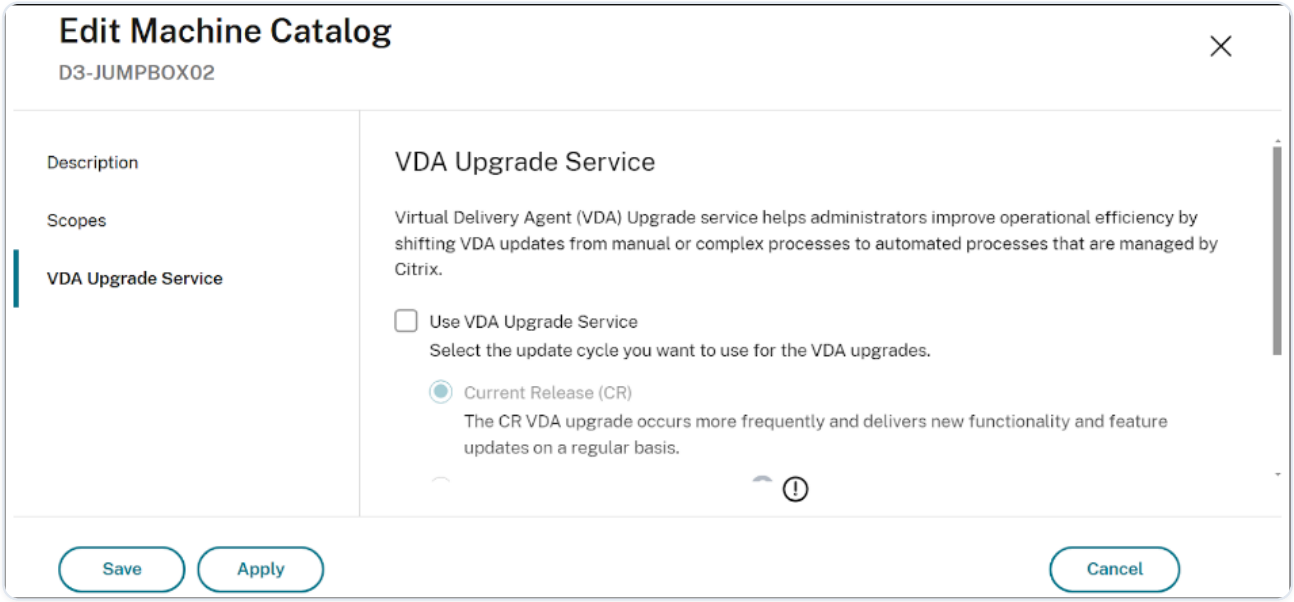
```
Import-VusVdaReleasesMetadata -Path '[<CVAD-2503-ISO>\Support\VdaUpdateServiceMetadata\vda_releases.xml]'
```

启用 VDA 升级服务

要启用 VDA 升级服务功能，请在创建或编辑计算机目录时使用 VDA 升级选项。管理员在启用 VUS 时必须从以下升级周期中进行选择：

- LTSR
- CR
- LTSR 早期访问版本 (EAR)
- CR EAR

要从 Web Studio 为计算机目录启用 VDA 升级服务，请右键单击目录，单击“编辑目录”，选择“VDA 升级服务”选项卡，选中“使用 VDA 升级服务”复选框，然后选择一个升级轨道。



要使用 PowerShell 为计算机目录启用 VDA 升级服务，请使用 `Set-VusCatalogUpgradeType` cmdlet。

升级类型可以设置为“LTSR”、“CR”、“EAR_CR”或“EAR_LTSR”。

示例：`Set-VusCatalogUpgradeType -CatalogName "Workstation catalog" -UpgradeType LTSR`

> **注意：**

> 启用 VDA 升级选项不会导致 VDA 自动升级。所有通过 VUS 进行的 VDA 升级都必须作为由管理员明确执行的单独任务启动。

VDA 要求

VDA 版本

- 对于使用 MCS 创建的计算机：
  - 2311 或更高版本
- 对于使用 Websocket VDA 注册 添加的计算机
  - 2311 或更高版本
- 对于手动预配的计算机
  - 2411 或更高版本

预配类型

- 使用非 Citrix 预配™ 服务预配的单会话或多会话持久性计算机。
- 单会话 MCS 预配的持久性计算机（已加入 AD、已加入 Microsoft Entra 和未加入域的）。
- 远程电脑访问计算机。

VDA 升级代理

- VDA 升级代理 7.44 或更高版本必须安装并在 VDA 上处于活动状态。代理可以安装：
  - 作为附加组件，在升级 VDA 或修改 VDA 安装时。
  - 使用 Citrix Virtual Apps and Desktops™ ISO 中提供的独立 MSI。
    - MSI 名称：CitrixUpgradeAgent_x64.msi
    - 路径：x64\虚拟桌面组件

权限

您必须在 CVAD 中具有完全管理员或计算机目录管理员角色。

VDA 状态

要使通过 VUS 计划的升级按预期进行，目标升级的 VDA 必须满足以下先决条件：

- VDA 不得手动置于维护模式。

- 要成功进行 VDA 升级，不能有用户登录。
  - 当升级过程开始在整个升级窗口期间排空用户会话时，VDA 将置于维护模式。升级成功完成后，它们将退出维护模式。
  - 如果在整个升级窗口期间用户有活动会话或断开连接的会话，则升级将在升级窗口结束时取消。

> **注意：**
>
> 可以使用 VUS 中的强制注销选项 终止活动会话和断开连接的会话。

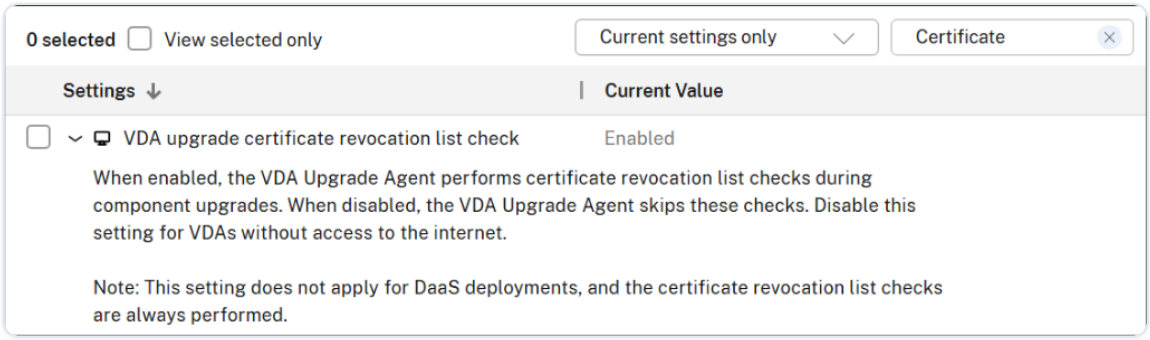
- 未通过 MCS 预配（手动预配）的 VDA 必须在通过 VUS 执行升级之前添加到交付组。
- VDAs 必须处于开机状态。

> **注意：**
>
> 当计划 VDA 升级时，AutoScale™ 不会停止对计算机进行电源管理。在升级进行期间，请考虑禁用交付组上的 AutoScale 计划。

连接

- VDA 必须能够通过 HTTPS 与 Delivery Controller 通信以进行 VDA 升级。
  - 为验证 VDA 安装程序是否由有效证书签名，VDA 必须与以下 URL 通信。
    - `<http://crl3.digicert.com/>` *
    - `<http://crl4.digicert.com/>` *
    - `<http://ocsp.digicert.com/>` *
    - `<http://cacerts.digicert.com/>` *
- 如果 VDA 无法访问互联网，请将 VDA 配置为绕过证书吊销列表 (CRL)。
  - 禁用“VDA 升级证书吊销列表检查”Citrix® 策略设置，并将其分配给交付组。
    - 策略说明：
      - 启用后，VDA 升级代理在组件升级期间执行证书吊销列表检查。

- 禁用后，VDA 升级代理会跳过这些检查。对于无法访问互联网的 VDA，请禁用此设置。

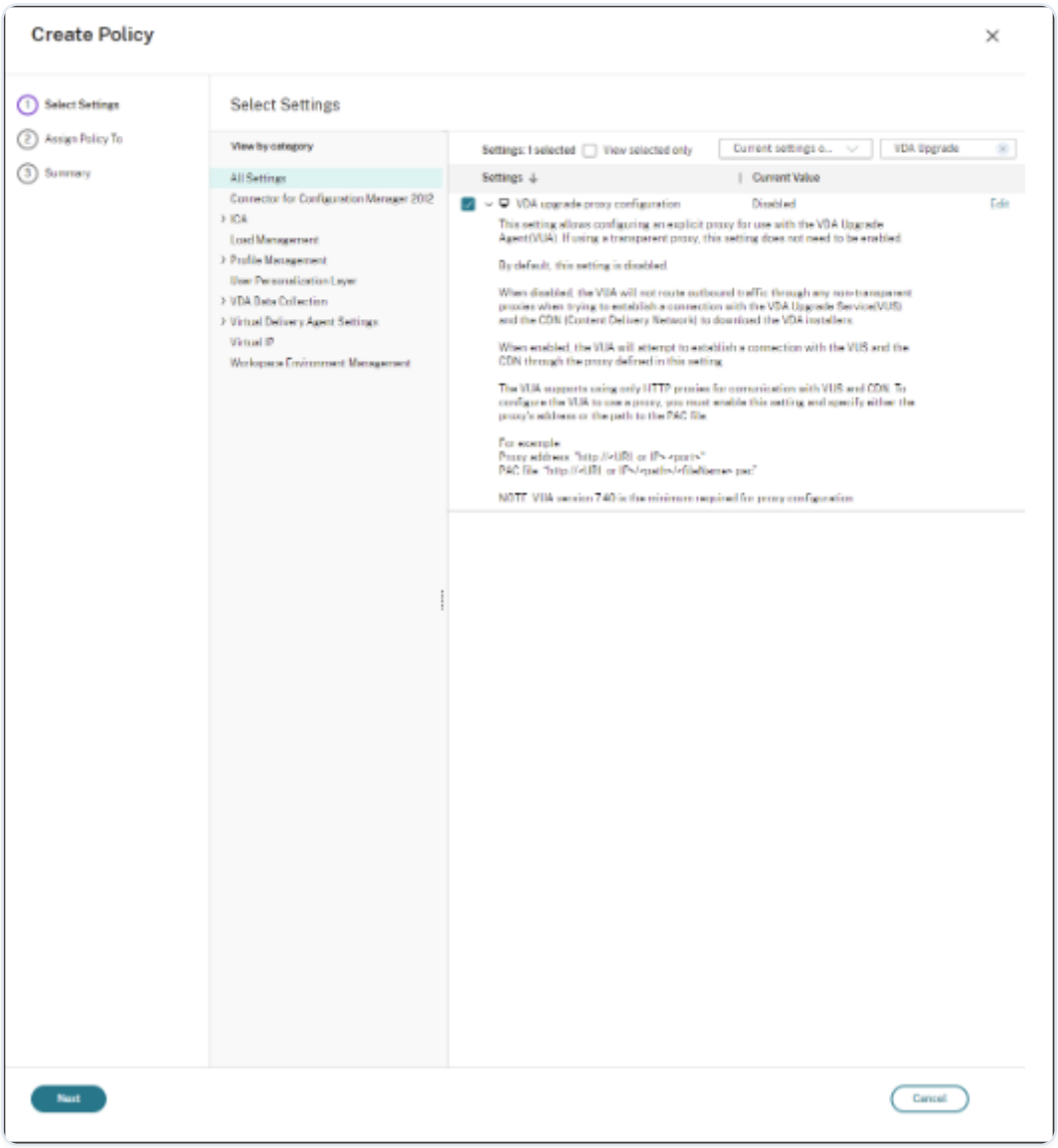


具有代理配置的 VDA

如果您的 VDA 通过代理访问互联网，请将 VDA 升级代理配置为通过该代理发送其流量。仅支持 Hostname: Port (IP:Port) 和 PAC 文件形式的代理。不支持 SOCKS5 代理。

通过 Web Studio 或注册表配置 VDA 升级代理以使用代理：

- 使用 Web Studio 配置 VDA 升级代理代理。
  - 在“**创建策略**”页面上，从“**设置**”中选择“**VDA 升级代理配置**”设置。



  - 为使用代理的 VDA 启用此设置。此设置默认禁用。

启用 VDA 升级代理配置设置(/en-us/citrix-virtual-apps-desktops/2607-ltsr/media/vda-upgrade-studio2.png)

  - 在设置中输入代理地址或 PAC 文件的路径。

- 使用注册表进行 VDA 升级代理代理配置
  - **密钥：** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
    - **值类型：** `String`
    - **值名称：** `ProxySettings`
    - **值数据：** 代理地址或 PAC 文件路径。
      - 例如：

- **代理地址：** `http://<URL or IP>:\<port>`
- **PAC 文件：** `http://<URL or IP>/\<path/\<filename>.pac`

使用 VDAWorkstationCoreSetup.exe 安装的 VDA

如果 VDA 最初是使用 VDAWorkstationCoreSetup.exe 安装的，则仍可以使用 VUS 进行升级，VUS 利用 `VDAWorkstationSetup.exe`。

使用 VUS 升级通过 `VDAWorkstationCoreSetup.exe` 安装的 VDA 时，您应查看安装选项以确保仅启用所需功能，尤其是在从最小核心安装迁移时。

使用 VDA 升级服务升级 VDA

您可以通过 VDA 升级服务启动 VDA 升级，方法是选择目标计算机目录、单个计算机或计算机组，然后选择“升级 VDA”。

> **注意：**
>
> Citrix® 建议在执行升级之前（如果可能）备份 VDA。

安排升级

Citrix 中的 VDA 升级过程可以在目录级别、计算机组级别或单个计算机级别执行，具体取决于要求。升级可以设置为立即开始，也可以提前最多 7 天安排日期和时间。

注意事项

- **目录与计算机组与计算机范围：** 目录升级非常适合批量更新，而单独或按组升级计算机则可以实现更精细的控制。
- **计划：** 升级可以提前最多 7 天进行计划。如果使用计算机目录级别升级，在升级计划后添加到目录的计算机不包含在现有计划升级中。

主要区别

功能	按目录升级	按计算机升级	计算机组
升级范围	整个目录	单个计算机	计算机目录中的计算机组

功能	按目录升级	按计算机升级	计算机组
计划控制	单个计划适用于计算机目录中的所有 VDA，最适合大规模升级操作	VDA 单独计划，主要用于测试和一次性升级	VDA 分组计划，让您可以灵活地在不同时间升级不同的 VDA 组
管理	通过 Web Studio 中的计算机目录节点或 `New-VusCatalogSchedule` cmdlet 进行管理	通过 Web Studio 中的搜索节点或 `New-VusMachineUpgrade` cmdlet 进行管理	通过 Web Studio 中的搜索节点或通过将计算机列表传递给 `New-VusMachineUpgrade` cmdlet 进行管理
用例	整个计算机目录的批量升级	针对性升级和测试场景的精细控制	对 VDA 子集的有针对性控制。可用于错开目录内的升级
可用 VDA 版本	对于 CR 和所有当前支持的 LTSR VDA 版本，最新版本以及之前 2 个 (N-2) 版本可供升级。有关详细信息，请参阅 (https://docs.citrix.com/zh-cn/citrix-daas/upgrade-vda-test/upgrade-vda-features#vda-versions-available)	对于 CR 和所有当前支持的 LTSR VDA 版本，最新版本以及之前 2 个 (N-2) 版本可供升级。有关详细信息，请参阅 (https://docs.citrix.com/zh-cn/citrix-daas/upgrade-vda-test/upgrade-vda-features#vda-versions-available)	只有最新的 LTSR 或 CR VDA 版本可供升级
附加组件	在每个 VDA 上安装或升级 VDA 组件。取消选中某个组件不会卸载该功能，但该组件将不会升级	在 VDA 上安装或升级 VDA 组件。取消选中某个组件不会卸载该功能，但该组件将不会升级	升级一组计算机时，VDA 升级服务无法管理附加组件。注意：附加功能（例如“启用还原清理”）可用于计算机组升级
附加功能	可以启用或升级附加功能	可以启用或升级附加功能	可以启用或升级附加功能

功能	按目录升级	按计算机升级	计算机组
并发	在安排升级时作为设置进行控制。有关详细信息，请参阅 (https://docs.citrix.com/zh-cn/citrix-daas/upgrade-vda-test/upgrade-vda-features#concurrency)	单个 VDA 已升级	根据升级计划中选择的 VDA 数量自动进行负载平衡
故障阈值	可以设置故障阈值，以防止在给定数量的 VDA 升级失败时进行未来的升级。有关更多信息，请参阅故障阈值。	故障阈值不适用于单机升级。	故障阈值不适用于机器组升级。请考虑将要升级的机器组大小设置为可接受的最大 VDA 故障数量。

计划升级的工作原理

VDA 上的 VDA 升级代理定期与 Delivery Controller 通信，以确定是否应升级 VDA。 VDA 可以安排立即升级，也可以提前最多 7 天升级。提前安排升级时，可以设置升级开始的日期和时间（UTC）。

升级持续时间设置了计划升级开始时间之后进行升级的时长。默认情况下，对于计算机目录和机器组升级，Citrix 会在整个升级持续时间内对 VDA 升级进行负载平衡，以提高性能并避免瓶颈。

升级开始后，VDA 将进入维护模式，直到升级完成。如果 VDA 上存在会话，则 VDA 不会升级，直到没有会话为止。当 VDA 处于维护模式时，无法向其代理新会话。如果用户在升级窗口期间断开会话连接，则在升级完成之前，用户将无法重新连接。

VDA 将继续尝试升级，直到计划的升级持续时间完成。如果在整个升级持续时间内都存在会话，则升级将被取消，并且 VDA 的维护模式将关闭。考虑更长的升级持续时间以提高 VDA 升级成功率。

> **注意：**
>
> 在计划升级之前手动置于维护模式的 VDA 将无法升级。

可用的 VDA 版本

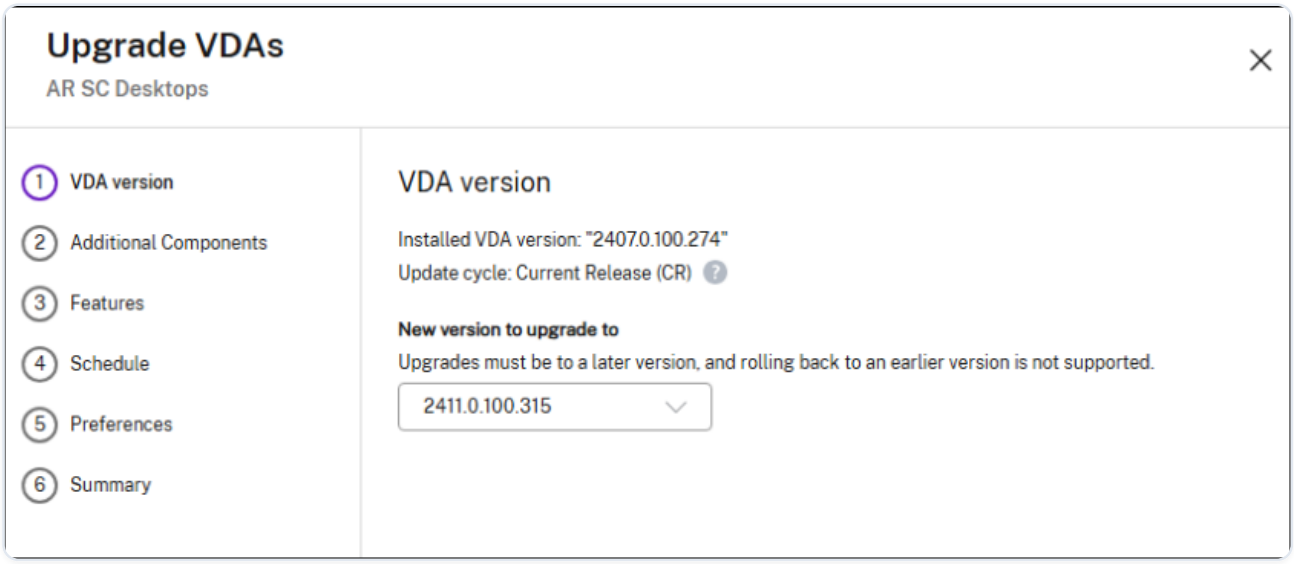
VDA 升级服务为 CR 版本维护 N-2 个 VDA 版本，并为所有当前支持的 LTSR 版本维护 N-2 个 CU 版本。

发布新的 CVAD 版本时，您可以更新 VUS 以包含更新的 VDA 版本，而无需更新整个站点。VUS 使用 **vda_releases.xml** 文件填充可用的 VDA 版本。**vda_releases.xmld** 文件位于 CVAD 元安装程序中的以下位置：

<CVAD-ISO\>\Support\VdaUpdateServiceMetadata\vda_releases.xml

要将较新的 vda_releases.xml 文件导入 VUS，请运行以下 cmdlet：`Import-VusVdaReleasesMetadata -Path '[Path to vda_releases.xml]'`

在 Web Studio 中，升级目录或单个计算机时，UI 会提示您选择要将 VDA 升级到的版本。



要使用 PowerShell 确定可用的 VDA 版本，请使用 `Get-VusAvailableVdaVersion` cmdlet。

如果未通过 cmdlet 传递计算机或目录，则 cmdlet 将返回所有升级路径的最新可用版本。

要获取资源可用的特定版本，请通过 `Get-VusAvailableVdaVersion` cmdlet 传递 VDA（-MachineName、-MachineUid 或 -MachineUuid）或目录（-CatalogName、-CatalogUid 或 -CatalogUuid）。

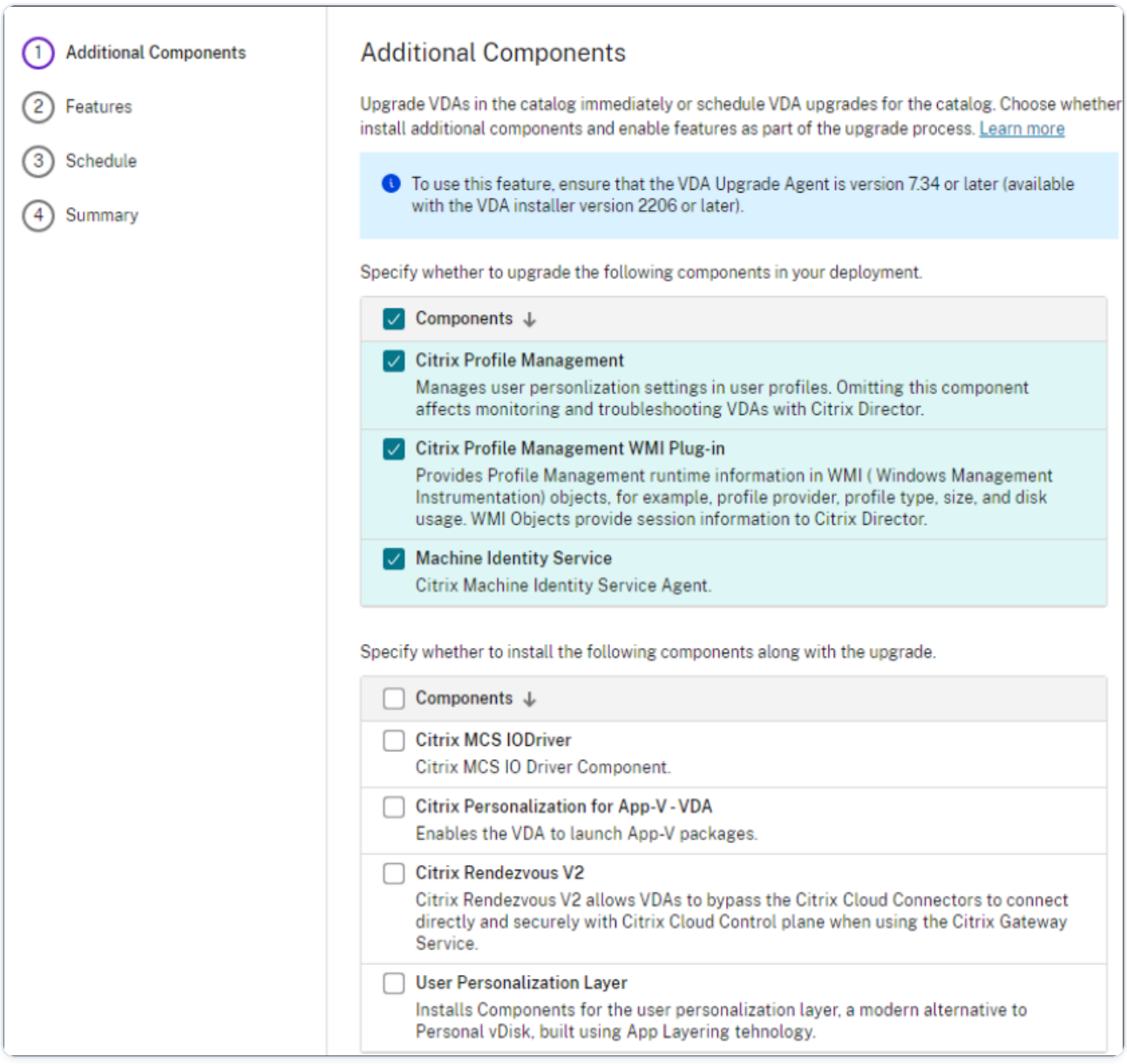
例如：`Get-VusAvailableVdaVersion -CatalogName '[Name of your Machine Catalog]'`

```
PS V:\> Get-VusAvailableVdaVersion -CatalogName 'CR-2303'

UpgradeType Version
----------- -------
         CR 2411.0.100.315
         CR 2407.0.100.274
         CR 2402.0.100.629
```

附加组件

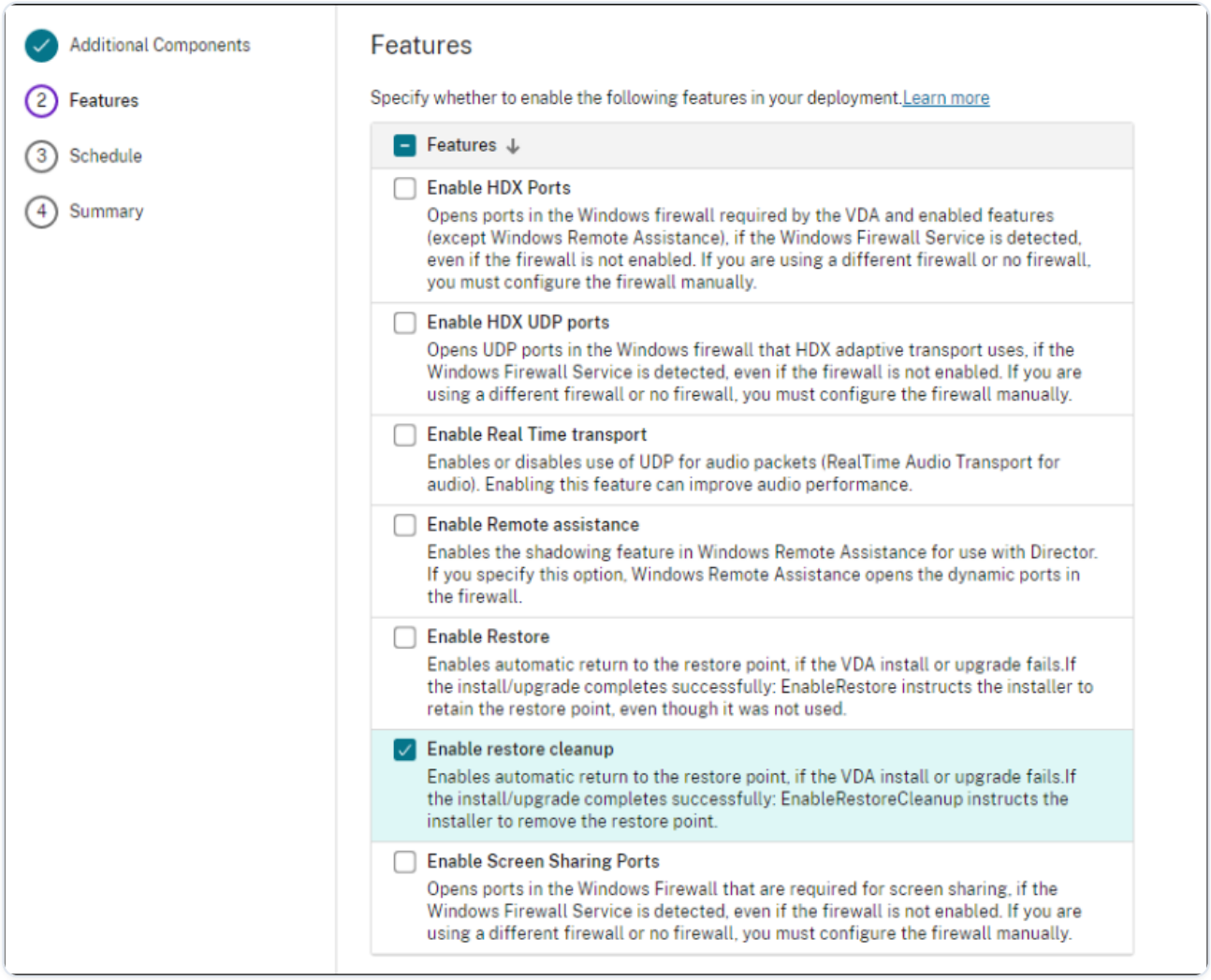
通过计算机目录或单个计算机升级 VDA 时，可以安装或升级附加组件。如果您未选中某个组件，它将不会卸载该组件，但该组件不会作为 VDA 整体升级的一部分进行升级。



功能

可以通过 VDA 升级服务在 VDA 上启用或升级功能。如果您未选中某个功能，它将不会禁用该功能，但该功能不会作为 VDA 整体升级的一部分进行升级。

默认情况下，**启用还原清理**复选框处于选中状态。Citrix 建议启用还原清理功能，以简化管理并改进失败升级的恢复。启用此功能后，将在升级开始前创建系统还原点。如果升级失败，VDA 将还原到系统还原点。VDA 成功安装后，还原点将被删除。有关详细信息，请参阅安装或升级失败时还原。



注意：

Windows 系统还原仅在单会话操作系统（例如 Windows 10 和 11）上受支持。必须在 VDA 上启用 Windows 系统还原功能，“启用还原清理”功能才能正常工作。如果选择了“启用还原”或“启用还原清理”，但未在 VDA 上配置 Windows 系统还原，则升级可能会失败。

并发

升级计算机目录时，VUS 允许您定义同时升级的 VDA 的最大数量。这有助于减少 Internet 连接或文件服务器的负载，并且与故障阈值结合使用时，如果多个 VDA 升级失败，则可以停止升级。

计划升级开始后，目录中的所有 VDA 都将置于维护模式。将对与定义的并发最大值设置匹配数量的 VDA 启动升级。一旦 VDA 升级完成，另一个 VDA 将开始升级，以保持同时升级的 VDA 的并发数量。

如果未为计算机目录计划升级指定并发，Citrix 将根据目录中 VDA 的总数和升级持续时间使用默认并发值。

升级平均需要大约 30 分钟才能完成，但这会因环境条件而异。考虑将并发设置为一个数量，使所有 VDA 都能在提供的升级持续时间内完成升级。例如，如果您有 20 个 VDA 设置为在 4 小时内升级，则每小时需要升级 5 个 VDA。使用平均升级持续时间 30 分钟，您可以将并发值设置为 3，以满足每小时 5 个 VDA 升级的要求（每 30 分钟升级 3 次，即每小时更新 6 次）。

故障阈值

升级计算机目录时，使用故障阈值可防止在给定数量的 VDA 失败后进一步升级 VDA。故障阈值可以缩小导致升级失败的问题的影响范围，从而减少管理员的故障排除工作。

故障阈值可防止任何未来的 VDA 启动升级，但不会停止已开始升级的 VDA。例如，如果计算机目录有 100 个 VDA，并发设置为 10 个 VDA，故障阈值设置为 3，如果所有 VDA 升级都失败，则至少有 13 个 VDA 将尝试升级，其余 87 个将从未启动，并且升级将被取消。

在计划升级开始时，10 个并发 VDA 开始升级，如果第一次升级失败，另一个 VDA 将开始升级以保持 10 个并发同时升级。如果第二次升级失败，另一个 VDA 将开始升级。如果第三次升级失败，所有当前正在升级过程中的 VDA 将继续，并且升级计划中其余的 VDA 将被取消升级。

VDA 安装程序位置

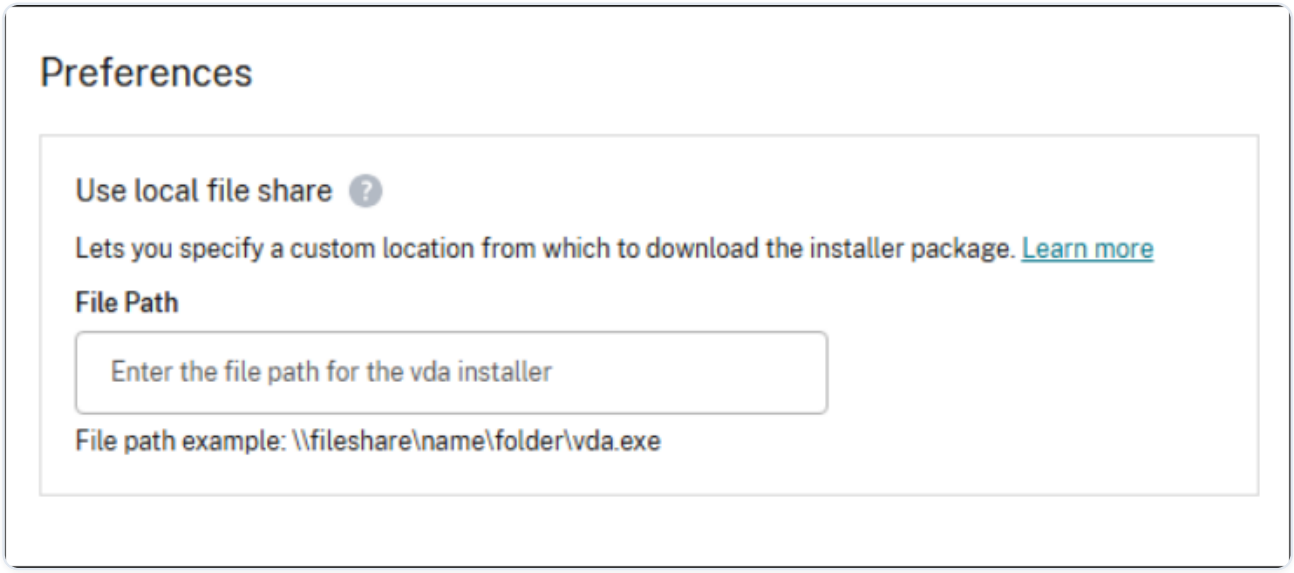
VDA 安装程序必须托管在您环境中的本地文件共享上。文件共享和 VDA 安装程序的要求如下：

文件共享必须满足以下先决条件。

- 文件共享权限
    - 包含 VDA 安装程序包的网络共享必须对作为本地系统 (NT AUTHORITY\SYSTEM 主体) 运行的 VDA 升级代理服务具有读取访问权限。
    - 已加入域的 VDA：
        - 本地系统帐户（VUA 作为本地系统运行）在访问网络共享时使用计算机凭据。

    - 必须向域计算机授予文件共享的读取访问权限。
    - 在“高级共享设置”中，必须启用“**文件和打印机共享**”。
  - 未加入域的 VDA：
    - 本地系统帐户（VUA 作为本地系统运行）在访问网络共享时使用“**匿名登录**”。
    - 在“**网络和共享中心，密码保护共享**”中，必须禁用此功能。
    - 在文件夹权限的“**安全**”选项卡中，必须向“**匿名登录**”授予读取访问权限。
    - 在“高级共享设置”中，必须启用“**文件和打印机共享**”。
    - 必须将共享文件夹名称添加到“**网络访问安全策略**”中。
- VDA 安装程序
  - VDA 安装程序必须从 Citrix 下载 网站下载并放置在文件共享中。
  - 必须下载适用于计算机目录的相关 VDA 安装程序。
    - 如果目录类型是多会话，请使用 **多会话操作系统 VDA 安装程序**。
    - 如果目录类型是单会话，请使用 **单会话操作系统 VDA 安装程序**。
  - 对于给定的升级，文件共享上的安装程序版本必须与 VUS 发布的版本完全匹配。使用 `Get-VusAvailableVersion` PowerShell cmdlet 确定可用版本。

安装程序的路径应是包含可执行文件的文件路径。例如，`\\hostname\VDA-Packages\VDAWorkstationSetup_2308.exe`。



通过 PowerShell 使用 VUS 时，在安排升级时请使用 `-VdaWorkstationPackageUri`（单会话操作系统）或 `-VdaServerPackageUri`（多会话操作系统）参数。

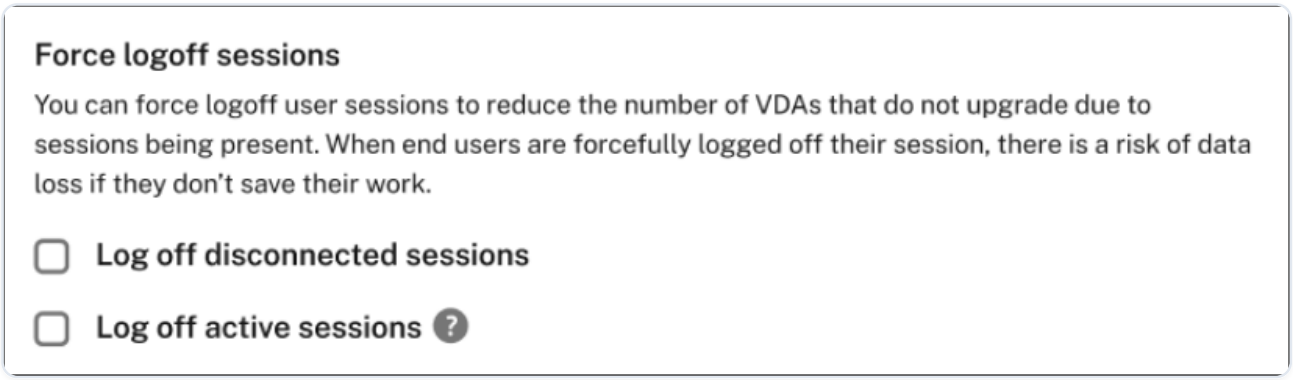
强制注销会话

为了增加在计划升级期间可用于升级的 VDA 数量，请考虑在升级期间强制注销用户会话。强制注销发生在每个 VDA 开始升级时，而不是在整个计划升级窗口开始时。

由于不同的 VDA 在计划期间的不同时间开始升级，因此用户只会在其特定 VDA 开始升级时被注销。

要在使用 Web Studio 进行计划升级期间强制注销断开连接的会话，请选择**注销断开连接的会话**选项。

要在使用 Web Studio 进行计划升级期间强制注销活动会话，请选择“**注销活动会话**”选项。如果注销活动会话，用户将在升级开始前 10 分钟在其会话中收到通知，提醒他们在自动注销前保存工作。



要在使用 PowerShell 进行计划升级期间强制注销断开连接的会话，请在计划升级时使用 `-LogoffOption` 参数。`-LogoffOption` 的可用选项如下所示：

- **仅活动会话：** 如果在计划升级窗口期间 VDA 上存在活动会话，则用户将被注销。在用户注销前 10 分钟将显示横幅以提供警告。在升级窗口期间，具有断开连接会话的 VDA 不会被注销。如果断开连接的会话在整个升级窗口期间仍然存在，则该 VDA 升级将被取消。
- **仅断开连接的会话：** 如果在计划升级窗口期间 VDA 上存在断开连接的会话，则用户将被注销。用户不会收到其断开连接的会话将被注销的通知。在升级窗口期间，具有活动会话的 VDA 不会被注销。如果活动会话在整个升级窗口期间仍然存在，则该 VDA 升级将被取消。
- **活动和断开连接的会话：** 如果在计划升级窗口期间 VDA 上存在断开连接或活动会话，则用户将被注销。对于活动会话，在用户注销前 10 分钟将显示横幅以提供警告。
- **不注销：** 活动和断开连接的会话不会被注销。如果在整个升级计划期间 VDA 上存在会话，则升级将在计划升级窗口结束时取消。

在可能的情况下，Citrix 建议强制注销会话，以增加成功升级的 VDA 数量。

> **重要提示：**

> 强制注销会话可能导致用户丢失其会话中未保存的工作。

编辑或取消 VDA 工作流

为目录计划升级后，您可以编辑升级的开始时间和持续时间，或完全取消升级。

要使用 UI 在计算机目录级别编辑或取消升级，请右键单击具有现有计划升级的计算机目录，然后单击“**编辑计划的 VDA 升级**”。要使用 PowerShell 编辑现有计算机目录级别升级，请使用 `Set-VusCatalogUpgrade` 和 `Remove-VusCatalogUpgrade` cmdlet。

要在计算机级别编辑或取消升级，请在搜索节点中，右键单击具有现有计划升级的计算机，然后单击“**编辑计划的 VDA 升级**”。您无法同时编辑多个计算机的计划 VDA 升级。要使用 PowerShell 编辑现有计算机级别升级，请使用 `Set-VusMachineUpgrade` 和 `Remove-VusMachineUpgrade` cmdlet。

监控和故障排除

监控计划的 VDA 升级

VDA 和计算机目录有两个属性，可帮助监控 VDA 升级的就绪情况和当前状态，这些属性在 Studio 中或 VDA 或目录的详细信息窗格中显示为可用于筛选的列。

- VDA 升级
- VDA 升级状态

VDA 升级

VDA 升级提供有关 VDA 或计算机目录是否已配置 VDA 升级代理以及 VDA 是否为最新版本或是否有可用升级的信息。可用状态如下：

VDA 升级 (STUDIO)	VDA 升级 (POWERSHELL)	描述
目录级别		
未配置	缺少升级类型	尚未为计算机目录选择升级轨道（CR、LTSR、CR EAR 或 LTSR EAR）。
已计划	UpgradeScheduled	已为计算机目录计划升级。

VDA 升级 (STUDIO)	VDA 升级 (POWERSHELL)	描述
可用	UpgradeAvailable	目录中的 VDA 不在升级轨道的最新版本上。建议进行升级。
最新	UpToDate	目录中的 VDA 处于升级轨道的最新版本。无需执行任何操作。
未知	未知	正在检索最新的 VDA 升级状态。
计算机级别		
未配置	缺少升级类型	尚未为 VDA 的计算机目录选择升级轨道（CR、LTSR、CR EAR 或 LTSR EAR）。
已计划	UpgradeScheduled	已为 VDA 安排了升级。
可用	UpgradeAvailable	VDA 不在升级轨道的最新版本上。建议进行升级。
最新	UpToDate	VDA 处于升级轨道的最新版本。无需执行任何操作。
正在检查状态	未知	正在检索最新的 VDA 升级状态。

注意：

对于使用 LTSR 轨道的 VDA，只有当 VDA 位于最新长期服务 (LTSR) 版本的最新累积更新 (CU) 上时，目录才会显示为“最新”。如果 VDA 位于以前的 LTSR 版本的最新 CU 上，VDA 升级仍将显示为“**可用**”。

VDA 升级状态

VDA 升级状态提供有关计划升级状态的信息。VDA 升级状态如下：

VDA 升级状态 (STUDIO)	VDA 升级状态 (POWERSHELL)	描述
目录级别		
未计划	NotScheduled	此目录未计划升级。
已计划	UpgradeScheduled	此目录已计划升级。
进行中	UpgradeInProgress	此目录正在进行升级。
已取消	UpgradeCancelled	目录的升级已取消。这可能是由于手动取消或达到故障阈值。
失败	UpgradeFailed	目录的计划升级失败。
成功	UpgradeSuccessful	目录的计划升级已成功完成。注意：成功的升级并不意味着目录中的所有 VDA 都已成功升级。
-	空	目录未计划升级。
计算机级别		
已计划	UpgradeScheduled	已为 VDA 安排了升级。
等待升级	UpgradeInUpgradeWindow	已安排的升级处于活动状态，但 VDA 尚未开始升级。有关 VDA 升级如何进行负载平衡的更多信息，请参阅“并发”。
进行中	UpgradeInProgress	VDA 正在升级。
已取消	UpgradeCancelled	VDA 的计划升级在开始之前已取消。
升级失败	UpgradeFailed	VDA 已开始升级，但升级未能成功完成。有关更多信息，请参阅“故障排除”。
成功	UpgradeSuccess	VDA 已成功升级。

VDA 升级状态 (STUDIO)	VDA 升级状态 (POWERSHELL)	描述
验证失败	UpgradeValidationFailed	下载 VDA 安装程序的元数据时，证书验证失败。
-	空	未为 VDA 安排升级。

计划的 VDA 升级故障排除

如果遇到升级失败，以下日志可以帮助您识别和解决问题。您还可以与 Citrix 技术支持共享这些日志，以加快协助过程。

VDA 安装日志

排除升级失败故障时，请收集并查看 VDA 初始安装和失败升级的日志。安装和升级日志可在以下位置找到。

- VDA 安装的安装日志位于：
  - %temp%/Citrix/XenDesktop 安装程序
- VDA 安装的升级日志位于：
  - C:\Windows\Temp\Citrix\XenDesktop 安装程序 **或**
  - C:\Windows\SystemTemp\Citrix\XenDesktop 安装程序

VDA 升级代理版本

通过 VUS 收集数据以排查升级失败问题时，了解 VDA 上升级代理的版本非常重要。要检查 VDA 升级代理版本，请使用以下 cmdlet: `Get-VusComponentVersion -ComponentType VUS`。它会列出所有 VDA 及其 VDA 升级代理版本。

要在目录级别检查 VDA 升级代理版本，可以使用以下脚本：

> **注意：**
>
> 此脚本仅供参考，可能需要根据您的特定环境进行调整。我们建议您在生产环境中使用此脚本之前对其进行彻底测试。

```
Param( [Parameter (Mandatory=$true)] [string] $CatalogName ) try { $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-Object -Property UUID
```

```
if($Uuids -eq $null) { throw "Cannot find CatalogName " +$CatalogName } Write-Output("Catalog Name passed is "+$CatalogName)
```

```
foreach($Uuid in $Uuids) { $compVersion = Get-VusComponentVersion -MachineId $machine.UUID -ComponentType VUS $Machine = Get-BrokerMachine -UUID $compVersion.MachineId Write-Output(“MachineName: “+ $Machine.MachineName+”, Machine UUID:”+$machine.MachineId+”, VUA Version:”+ $compVersion.Version) } } catch { Write-Output(“Exception Occured”) Write-Host $_ }
```

与 VDA 升级代理相关的日志

VDA 升级代理 (VUA) 日志可以提供重要信息，用于排查升级失败以及 VUA 与 VDA 升级服务通信问题。您可以收集的日志包括：

- Citrix 诊断工具 (CDF) 跟踪。CDF 模块名称为 `VdaUpgradeAgent`。
- Windows 事件日志。在 **事件查看器 > Windows 日志 > 应用程序 > Citrix VDA 升级代理服务** 中查看日志。

有一个注册表设置，允许管理员启用循环日志文件，该文件捕获用于故障排除的关键信息，同时防止日志文件过大。日志文件的总大小上限为 20 MB。创建以下注册表项以启用文件日志记录：

- **项：** `HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent`
- **值名称：** `LogToFile`
- **值类型：** `REG_DWORD`
- **值数据：**
  - `0` - 文件跟踪已禁用
  - `1` - 文件跟踪已启用

要在 VDA 上使用 PowerShell 创建 LogToFile 注册表项，请使用以下 cmdlet：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent -Name LogToFile -Value 1 -PropertyType DWord -Force
```

若要大规模为计算机组启用 LogToFile，请考虑通过组策略首选项在所有 VDA 组织单位 (OU) 上创建 LogToFile 注册表。

> **注意：**
>
> - 当 `LogToFile=1` 设置时，日志仅写入文件。它们不会出现在 CDF 跟踪中。
> - 注册表更改生效需要重新启动 VDA 升级代理服务
> - 日志文件在 C:\ProgramData\Citrix\Update Services\Logs 文件夹中创建

排查 VDA 升级下载失败问题

请按照以下步骤排查并解决与 VDA 升级功能相关的下载失败问题：

1. 如果启用了 URL 过滤，请确保已将相关 URL 添加到允许列表中。请参阅连接性。
2. 将必要的 URL 添加到允许列表后，请尝试重新安排 VDA 升级。

您可以启用 CDF 跟踪或将 `LogToFile` 设置为 `1` 以捕获详细日志进行分析。如果下载失败问题仍然存在，请检查错误。如果您看到以下错误消息“Download Failed: This access control list is not in canonical form and therefore cannot be modified”，则表示文件夹 `C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA` 上的权限不正确。

要解决此问题，请执行以下任一操作：

- **选项 1：** 使用以下命令重置文件夹上的访问控制列表 (ACL)。(该命令使用所有匹配文件的默认继承 ACL 重置 ACL。)
  - icacls.exe "C:\ProgramData\Citrix\UpgradeServices\下载\VDA" /reset /T /C /L /Q
- **选项 2：**删除 Downloads 文件夹下的 VDA 文件夹，然后安排 VDA 升级。

排查 VDA 升级验证失败

请按照以下步骤排查并解决与 VDA 升级功能相关的下载失败问题：

1. 如果启用了 URL 过滤，请确保已将相关 URL 添加到允许列表中，特别是撤销检查所需的证书吊销列表 (CRL) 或在线证书状态协议 (OCSP) URL。请参阅VDA 升级要求。
2. 将必要的 URL 添加到允许列表后，请尝试重新安排 VDA 升级。

我们建议启用 CDF 跟踪或将 `LogToFile` 设置为 `1` 以捕获详细日志进行分析。日志可能包含以下错误：

- RevocationStatusUnknown
- 吊销功能无法检查证书的吊销状态。
- 吊销功能无法检查吊销，因为吊销服务器处于脱机状态。

VDA 升级代理依赖 Windows 系统调用来验证证书并执行吊销检查。上述错误表明代理无法建立与 CRL 或 OCSP URL 的连接。

Windows CryptoAPI 目前不支持代理设置。请查阅具有代理配置的 VDA 部分，以配置 VDA 代理以方便出站 CRL 调用。

Citrix 始终开启追踪

Always On Tracing (AOT) 是 Citrix 推出的一种现代诊断框架，旨在持续捕获 Citrix Virtual Apps and Desktops (CVAD) 环境中的相关日志数据。AOT 是 Citrix Diagnostic Facility (CDF) 跟踪的子集，其中包含来自其他组件的附加日志，在排查常见故障（例如 VDA 注册和应用程序/桌面启动等）时非常有用。

与需要手动干预的传统工具不同，AOT 默认在后台运行，确保在出现问题时（即使问题无法重现）也能获得关键信息。

AOT 旨在通过以下方式简化 IT 管理员和 Citrix 支持团队的故障排除，从而缩短平均解决时间：

- 自动捕获用户会话和系统事件的日志数据。
- 无需重现问题。
- 无需工程级专业知识即可轻松访问和读取日志。
- 启用自助服务日志数据，以减少对 Citrix 支持的依赖。

主要优势

- 更快的 MTTR（平均解决时间）
- 始终开启，无需手动启动跟踪
- 常见问题的自我诊断
- 通过完整上下文简化向 Citrix 支持的升级
- 安全、合规的日志处理，敏感数据已编辑

有关详细信息，请参阅 Always On Tracing

第三方通知

此版本的 Citrix Virtual Apps and Desktops™ 可能包含根据以下文档中定义的条款获得许可的第三方软件：

- Citrix Virtual Apps and Desktops 第三方通知 （PDF 下载）
- Citrix Assistant App 第三方通知 - 预览 （PDF 下载）
- FlexNet Publisher 2017 (11.15.0.0) 的非商业软件披露 （PDF 下载）
- FlexNet Publisher 文档补充：FlexNet Publisher 11.15.0 中使用的第三方和开源软件 （PDF 下载）

SDK 和 API

此版本提供了多个 SDK 和 API。要访问这些 SDK 和 API，请转到 Build anything with Citrix。在此处，选择 **Citrix Workspace** 以访问 Citrix Virtual Apps and Desktops 及其相关组件的编程信息。

> **注意：**
>
> Citrix Virtual Apps and Desktops™ SDK 和 Citrix Group Policy SDK 可以作为模块或管理单元安装。多个组件 SDK（例如 Citrix Licensing、Citrix Provisioning 和 StoreFront）仅使用管理单元进行安装。
>
> 此产品支持 PowerShell 版本 3 到 5。

思杰虚拟应用和桌面™ SDK

当您安装 Delivery Controller™ 或 Studio 时，此 SDK 会自动作为 PowerShell 模块安装。这使您无需添加管理单元即可使用此 SDK 的 cmdlet。（如果您选择将此 SDK 作为管理单元安装，下面提供了说明。）

权限

您必须使用具有 Citrix 管理权限的身份运行 shell 或脚本。尽管 Controller 上本地管理员组的成员自动拥有完全管理权限以允许安装 Citrix Virtual Apps 或 Citrix Virtual Desktops™，但 Citrix 建议在正常操作中，您创建具有适当权限的 Citrix 管理员，而不是使用本地管理员帐户。

访问并运行 cmdlet

1. 在 PowerShell 中启动 shell：打开 Studio，选择 **PowerShell** 选项卡，然后单击 **Launch PowerShell**。
2. 要在脚本中使用 SDK cmdlet，请在 PowerShell 中设置执行策略。有关 PowerShell 执行策略的信息，请参阅 Microsoft 文档。
3. 如果要使用管理单元（而不是模块），请使用 `Add-PSSnapin`（或 `asnp`）cmdlet 添加管理单元。

V1 和 V2 表示管理单元的版本。XenDesktop 5 管理单元是版本 1。Citrix Virtual Apps and Desktops 以及更早的 XenDesktop 7 版本管理单元是版本 2。例如，要安装 Citrix Virtual Apps and Desktops 管理单元，请键入 `Add-PSSnapin Citrix.ADIdentity.Admin.V2`。要导入所有 cmdlet，请键入：`Add-PSSnapin Citrix.*.Admin.V*`

您现在可以使用 cmdlet 和帮助文件了。

- 要访问此 SDK 的帮助文件，请在 Categories 列表中选择产品或组件，然后选择 **Citrix Virtual Apps and Desktops SDK**。
- 有关 PowerShell 指南，请参阅 Windows PowerShell Integrated Scripting Environment (ISE)。

组策略 SDK

Citrix Group Policy SDK 使您能够显示和配置组策略设置和筛选器。此 SDK 使用 PowerShell 提供程序创建一个虚拟驱动器，该驱动器对应于计算机和用户设置以及筛选器。该提供程序作为 `New-PSDrive` 的扩展出现。

要使用组策略 SDK，必须安装 Studio 或 Citrix Virtual Apps and Desktops SDK。

Citrix 组策略 PowerShell 提供程序可作为模块或管理单元使用。

- 要使用该模块，无需执行额外操作。
- 要添加管理单元，请键入 `Add-PSSnapin citrix.common.grouppolicy`。

要访问帮助，请键入：`help New-PSDrive -path localgpo:/`。

要创建虚拟驱动器并加载设置，请键入 `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>`，其中 Controller 字符串是您要连接并从中加载设置的站点中 Controller 的完全限定域名。

Citrix 虚拟应用和桌面 表述性状态转移接口

借助 Citrix Virtual Apps and Desktops REST API，您可以自动管理 Citrix Virtual Apps and Desktops 部署中的资源。

Citrix Virtual Apps and Desktops REST API 可在 `<https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis>` 处获取。不适用于 Citrix Virtual Apps and Desktops 的 API 已相应标记。请遵循其中的指导来配置对 API 服务的访问，并使用 API 来管理和优化您的资源。

监控服务 OData

Monitor API 允许使用 OData API 的版本 3 或 4 访问 Monitor Service 数据。您可以根据从 Monitor Service 数据查询的数据创建自定义监视和报告仪表板。OData V.4 基于 ASP.NET Web API，并支持聚合查询。

有关详细信息，请参阅 Monitor Service OData API。

OEM 指南

本节提供了 Citrix 关于在 Citrix Virtual Apps and Desktops HDX 会话中部署和优化选定 OEM 供应商产品的指导。该文档涵盖了支持的配置、设计注意事项和故障排除最佳实践，以帮助管理员在虚拟化环境中成功集成第三方硬件和软件。请注意，尽管 Citrix 验证了 HDX 传输层的互操作性，但设备和应用程序特定的行为仍由各自的 OEM 供应商负责。

纽昂斯

Citrix Virtual Apps and Desktops 支持 Nuance PowerMic 和 Philips SpeechMike 听写麦克风在 HDX 会话中使用，从而在已发布的应用程序和虚拟桌面中实现语音听写和麦克风控制。

这些设备常用于依赖语音识别工作流的环境中。在 Citrix 会话中，听写麦克风显示为复合 USB 设备，可公开音频和 HID 接口。Citrix HDX 通过 HDX 音频虚拟通道处理音频输入，同时将所需的设备接口重定向到会话，以确保应用程序兼容性和按钮功能，从而支持这些设备。

本页面介绍了支持的场景，并提供了在 Citrix Virtual Apps and Desktops 环境中启用 Nuance PowerMic 和 Philips SpeechMike 设备的指南。

配置

设计注意事项

> **重要 — 第三方声明**

> Nuance PowerMic 和 Philips SpeechMike 设备以及相关的语音识别软件均为第三方产品。Citrix Virtual Apps and Desktops 仅在虚拟化和 HDX 传输层支持这些设备。

> Citrix 不开发、认证或支持第三方设备驱动程序、固件、语音识别引擎或特定于应用程序的功能。设备行为（例如转录准确性、按钮映射和应用程序响应能力）由第三方软件和底层环境条件决定。

> 对于与设备硬件、固件、驱动程序或语音识别应用程序行为相关的问题，请联系相应的设备或应用程序供应商。客户应在将这些设备部署到生产 Citrix 环境之前，直接与供应商验证第三方兼容性和支持的配置。

要求和配置

要求

Citrix® 控制平面

- Citrix Virtual Apps and Desktops™ 2402 或更高版本
- 思杰 DaaS

会话主机

- 操作系统
  - Windows 十一
  - Windows Server 2019 或更高版本
- VDA
  - Windows: 2402 版本或更高版本

> **注意：**
>
> 当会话主机是 Windows Server 时，必须在服务器上启用麦克风访问，因为默认情况下它是禁用的。

客户端设备

- 操作系统
  - Windows 十一
  - 林纳克斯
- Workspace 应用程序
  - Windows: 2402 版本或更高版本
  - Linux：版本 2601 或更高版本

注意：

- 旧版本的适用于 Linux 的 Citrix Workspace 应用程序可能需要在客户端端点上进行额外配置，并且可能存在一些功能缺失。
- Nuance PowerMic 和 Philips SpeechMike 设备在单跳 Citrix Virtual Apps and Desktops 会话中受支持。多跳或嵌套虚拟化场景可能导致性能下降，不建议用于对延迟敏感的听写工作流。

配置

听写麦克风是复合 USB 设备，可同时公开音频和 HID 接口。HID 接口通过 USB 重定向进行重定向，而音频流量则通过 HDX 音频通道传输。以下步骤为每个受支持的设备型号配置分设备 USB 重定向。

PowerMic 4

PowerMic 4 是一个具有 8 个接口的复合设备。HID 接口（04、05、06、07）通过 USB 重定向进行重定向；音频通过 HDX 音频通道传输。

1. 在 Citrix Web Studio 中，启用**客户端 USB 设备重定向**策略设置。
2. 编辑**客户端 USB 设备重定向规则（版本 2）**策略设置并添加以下规则，然后单击**保存**：

```
Connect: VID=0554 PID=0064 split=1 intf=04,05,06,07 #Nuance PowerMic4 HID
controls

Deny: VID=0554 PID=0064 split=1 intf=00,01,02 #Nuance PowerMic4 audio

Deny: VID=0554 PID=0064 split=1 intf=03 #Nuance PowerMic4 mouse
```

1. 编辑**允许自动连接现有 USB 设备**策略设置。清除**使用默认值**复选框，选择**自动重定向可用 USB 设备**，然后单击**保存**。
2. 编辑**允许自动连接新到达的 USB 设备**策略设置。清除**使用默认值**复选框，选择**自动重定向可用 USB 设备**，然后单击**保存**。

配置这些设置后，PowerMic 4 设备将自动呈现在后续的 HDX 会话中，无需任何额外的最终用户操作。

PowerMic 3

PowerMic 3 是一个具有 4 个接口的复合设备。HID 接口 (03) 通过 USB 重定向进行重定向；音频通过 HDX 音频通道传输。

1. 在 Citrix Web Studio 中，启用**客户端 USB 设备重定向**策略设置。
2. 编辑**客户端 USB 设备重定向规则（版本 2）策略设置并添加以下规则，然后单击保存**：

```
Connect: VID=0554 PID=1001 split=01 intf=03 #Nuance PowerMic3

 Deny: VID=0554 PID=1001 split=01 intf=00,01,02 #Nuance PowerMic3 audio
```

1. 编辑**允许现有 USB 设备自动连接**策略设置。清除**使用默认值**复选框，选择**自动重定向可用 USB 设备**，然后单击**保存**。
2. 编辑**允许新到达的 USB 设备自动连接**策略设置。清除**使用默认值**复选框，选择**自动重定向可用 USB 设备**，然后单击**保存**。

配置这些设置后，PowerMic 3 设备将自动呈现在后续的 HDX 会话中，并且不需要任何额外的最终用户操作。

飞利浦 SpeechMike

Philips SpeechMike 是一种具有 7 个接口的复合设备。HID 接口（03、04、05、06）通过 USB 重定向进行重定向；音频通过 HDX 音频通道传输。

1. 在 Citrix Web Studio 中，启用**客户端 USB 设备重定向**策略设置。
2. 编辑**客户端 USB 设备重定向规则（版本 2）策略设置并添加以下规则，然后单击保存**：

```
Connect: VID=0911 PID=0c1c split=1 intf=03,04,05,06 #Philips SpeechMike

 Deny: VID=0911 PID=0c1c split=1 intf=00,01,02 #Philips SpeechMike audio
```

1. 编辑**允许现有 USB 设备自动连接**策略设置。清除**使用默认值**复选框，选择**自动重定向可用 USB 设备**，然后单击**保存**。
2. 编辑**允许新到达的 USB 设备自动连接**策略设置。清除**使用默认值**复选框，选择**自动重定向可用 USB 设备**，然后单击**保存**。

配置这些设置后，Philips SpeechMike 设备将自动呈现在后续的 HDX 会话中，并且不需要任何额外的最终用户操作。

设计注意事项和客户端注意事项

设计注意事项

在 Citrix Virtual Apps and Desktops 环境中规划使用 Nuance PowerMic 或 Philips SpeechMike 设备时，请考虑以下可能影响设备行为和用户体验的设计因素。

Studio 中的音频策略设置

Citrix 建议在 Studio 中使用默认音频策略设置。修改默认选项可能会导致音频性能不稳定。

网络延迟和会话拓扑

听写工作流对延迟敏感。高网络延迟或抖动可能导致音频传输延迟、转录准确性降低，或者说话与文本在应用程序中显示之间出现可感知的延迟。

引入双跳场景的环境（例如，通过另一个虚拟化层或远程访问解决方案访问虚拟桌面）会进一步加剧延迟，并可能对实时听写和按钮响应能力产生负面影响。

为获得最佳效果，请确保网络条件支持用户端点和会话主机之间的低延迟音频流。

音频和设备重定向行为

听写麦克风依赖于 HDX 音频通道和重定向设备接口的组合。糟糕的网络条件、相互竞争的实时工作负载或受限的客户端资源可能会影响音频和控制信号传输到会话中的方式，从而可能导致行为不稳定。

Citrix 建议在大规模部署之前，在预期的生产条件下验证麦克风行为，尤其是在网络质量不稳定的环境中。

应用程序特定依赖项

最终用户体验在很大程度上取决于会话中运行的语音识别应用程序。某些应用程序可能会引入其自身的缓冲、处理延迟或兼容性限制，这些因素超出了 Citrix Virtual Apps and Desktops 的控制范围。

Citrix 不控制或验证应用程序级别的语音识别准确性、转录性能或按钮映射。客户应与应用程序供应商核实应用程序兼容性和支持的设备型号。

用户期望和工作流验证

听写工作流需要近乎实时的反馈。如果环境条件不符合性能预期，用户可能会遇到转录延迟或设备响应不一致的问题。

Citrix 建议在生产部署之前验证端到端工作流（包括网络路径、客户端端点、虚拟化层和应用程序行为），以确保解决方案满足用户生产力要求。

客户端设备注意事项

在 HDX 会话中使用 Nuance PowerMic 或 Philips SpeechMike 设备时，客户端端点在整体听写体验中起着关键作用。管理员在设计和验证客户端部署时应考虑以下因素。

客户端平台和 Workspace 应用程序版本

Citrix 建议在客户端设备上使用当前受支持的 Citrix Workspace 应用程序版本。较旧的客户端版本可能缺少音频重定向或复合 USB 设备处理的优化，这可能导致麦克风性能下降或按钮行为不一致。

Windows、macOS 和 Linux Workspace 应用程序客户端之间实现方式的差异也可能影响听写设备如何枚举并重定向到会话中。

客户端硬件和资源可用性

听写工作流依赖于实时音频捕获和传输。即使在低延迟网络环境中，CPU、内存或音频子系统功能有限的客户端设备也可能在音频发送到 VDA 之前引入额外的延迟或失真。

为确保结果一致，请在生产中将使用的同类端点上验证设备行为。

USB 连接和设备拓扑

Nuance PowerMic 和 Philips SpeechMike 设备可能会公开多个 USB 接口。端点上的 USB 集线器、扩展坞或虚拟化 USB 控制器可能会影响这些接口如何呈现给 Citrix 会话。

Citrix 建议使用计划的端点连接拓扑测试听写设备，尤其是在依赖共享工作站、热插拔或扩展坞解决方案的环境中。

本地音频和外围设备使用

客户端端点上使用音频输入设备的其它本地应用程序可能会争夺系统资源，并可能影响听写性能。管理员在验证用户工作流时，应考虑并发的本地音频使用情况，例如会议或录音工具。

__index__

监视站点的历史趋势

“趋势”视图访问每个站点的以下参数的历史趋势信息：

- 会话
- 连接失败
- 计算机故障
- 登录性能
- 负载评估
- 容量管理
- 计算机使用情况
- 资源利用率
- 每个站点的网络分析。

要查找此信息，请单击“**趋势**”菜单。

放大钻取功能允许您通过放大某个时间段（单击图表中的数据点）并向下钻取以查看与趋势相关的详细信息来浏览趋势图表。此功能使您能够更好地了解受影响的人员或内容的详细信息。

要更改每个图表的默认范围，请对数据应用不同的筛选器。

选择您需要历史趋势信息的时间段。时间段的可用性取决于您的 Director 部署，具体如下：

- 最长可达去年（365天）的趋势报告可在高级版许可站点中获取。
- 最长可达上个月（31天）的趋势报告可在增强版许可站点中获取。
- 最长可达最近7天的趋势报告可在非高级版和非增强版许可站点中获取。

> **注意：**

- 在所有 Director 部署中，当时间段设置为上个月（**截至当前**）或更短时，会话、故障和登录性能趋势信息以图表形式提供。对于选择为具有自定义结束日期的上个月或去年的时间段，趋势信息以图表形式提供，而非表格形式。
- Monitor Service 的清理保留值控制趋势数据的可用性。默认值可在数据粒度和保留中获取。高级版许可站点的客户可以将其清理保留更改为所需的保留天数。
- IIS Manager 中的以下参数控制可供选择的自定义结束日期范围。但是，所选日期的数据可用性取决于正在测量的特定指标的清理保留设置。

参数	默认值
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

可用趋势

查看会话趋势： 在**会话**选项卡中，选择交付组和时间段，以查看有关并发会话计数的更详细信息。

会话自动重新连接列显示会话中自动重新连接的次数。当会话可靠性或客户端自动重新连接策略生效时，将启用自动重新连接。当端点上发生网络中断时，以下策略将生效：

- 会话可靠性生效（默认情况下为 3 分钟），在此期间，Citrix Receiver™ 或 Citrix Workspace™ 应用程序会尝试连接到 VDA。
- 客户端自动重新连接在 3 到 5 分钟内生效，在此期间，客户端会尝试连接到 VDA。

两次重新连接都会被捕获并显示给用户。重新连接发生后，此信息最多可能需要 5 分钟才能显示在 Director UI 上。

自动重新连接信息可帮助您查看和排查存在中断的网络连接。它还可以分析具有无缝体验的网络。您可以查看在筛选器中选择的特定交付组或时间段的重新连接次数。向下钻取可提供其他信息，例如会话可靠性或客户端自动重新连接、时间戳、端点 IP 以及安装了 Workspace 应用程序的计算机的端点名称。

默认情况下，日志按事件时间戳降序排序。此功能适用于适用于 Windows 的 Citrix Workspace 应用程序、适用于 Mac 的 Citrix Workspace 应用程序、适用于 Windows 的 Citrix Receiver 和适用于 Mac 的 Citrix Receiver。此功能需要 Delivery Controller™ 7 1906 或更高版本以及 VDA 1906 或更高版本。

有关会话重新连接的详细信息，请参阅会话。

有关策略的详细信息，请参阅客户端自动重新连接策略设置和会话可靠性策略设置。

有时，自动重新连接数据可能不会在 Director 中显示，原因如下：

- Workspace 应用程序未将自动重新连接数据发送到 VDA。
- VDA 未将数据发送到监视服务。
- Delivery Controller 会丢弃 VDA 有效负载，因为它们可能没有相应的会话。

> **注意：**
>
> 有时，如果设置了某些 Citrix Gateway 策略，则可能无法正确获取客户端 IP 地址。

> **查看连接失败趋势：** 在“失败”选项卡中，选择连接、计算机类型、失败类型、交付组和时间段，以查看包含有关站点中用户连接失败的更详细信息的图表。

查看计算机故障趋势： 在**单会话操作系统计算机故障**选项卡或多会话操作系统计算机选项卡中，选择故障类型、交付组和时间段，以查看包含站点中计算机故障详细信息的图表。

查看登录和重新连接性能趋势： 在登录和重新连接性能选项卡中，选择交付组和时间段，以查看包含站点中用户登录和重新连接持续时间详细信息的图表。此视图可帮助您了解登录或重新连接的数量以及整体性能。

图表包括：

- **登录事件、登录持续时间和阶段**（例如代理、交互式会话等），提供启动新会话时的用户体验洞察。
- **重新连接事件和重新连接持续时间**，提供从断开连接的会话重新连接时的用户体验洞察。

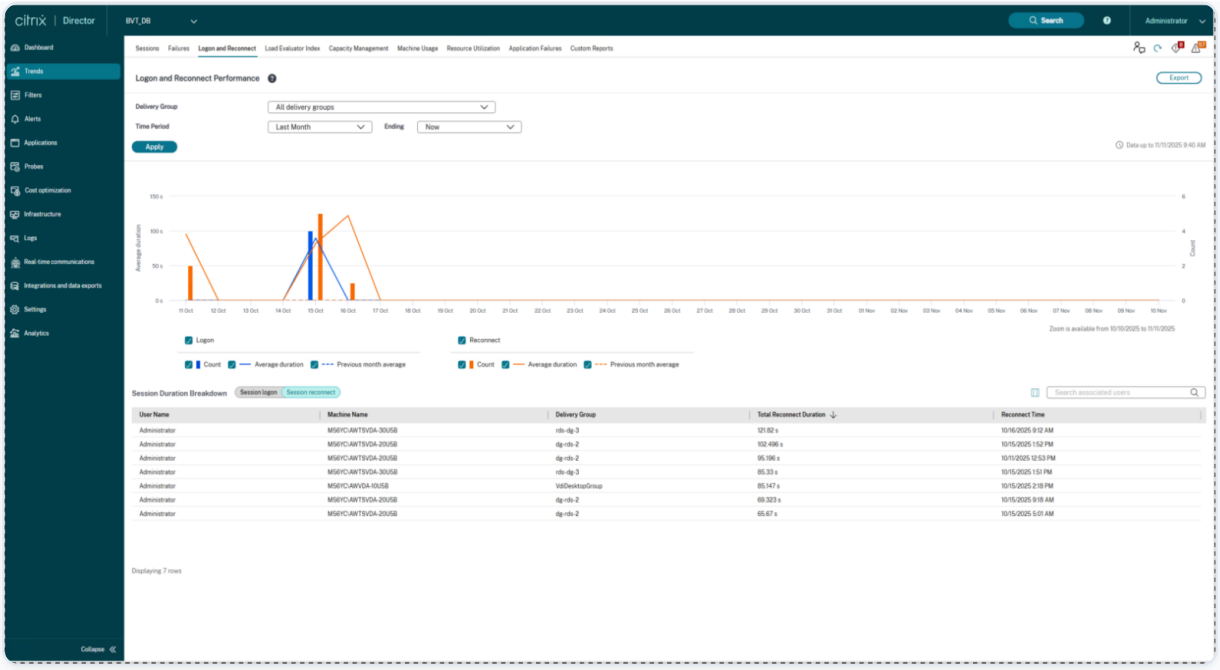
使用图例根据正在分析的趋势选择所需的指标。

- 计数
- 平均持续时间

- 上一个（时间范围）平均值

图表下方的表格按用户会话或连接显示**会话登录**和**会话重新连接**详细信息。您可以使用表格上方的选择在指标之间切换，选择要显示的列，按任意列排序，并将报告导出为 PDF、Excel 或 CSV 格式。

> **注意：**
>
> 会话重新连接持续时间在 **Director 和 VDA 2511 CR 或更高版本**上受支持。



查看负载评估趋势： 在**负载评估器索引**选项卡中，查看包含多会话操作系统计算机之间负载分布详细信息的图表。此图表的筛选选项包括交付组或交付组中的多会话操作系统计算机、多会话操作系统计算机（仅当选择了交付组中的多会话操作系统计算机时可用）以及范围。

查看托管应用程序使用情况： 此功能的可用性取决于您的组织许可证。 在**容量管理**选项卡中，选择**托管应用程序使用情况**选项卡。选择交付组和时间段，以查看显示并发使用峰值的图表以及显示基于应用程序使用情况的表格。在“基于应用程序的使用情况”表格中，您可以选择特定的应用程序以查看详细信息以及正在使用或已使用该应用程序的用户列表。

查看单会话和多会话操作系统使用情况： “趋势”视图按站点和交付组显示单会话操作系统的使用情况。当您选择**站点**时，使用情况按交付组显示。当您选择交付组时，使用情况按用户显示。 “趋势”视图还按站点、交付组和计算机显示多会话操作系统的使用情况。当您选择**站点**时，使用情况按交付组显示。当您选择交付组时，使用情况按计算机和用户显示。当选择计算机时，使用情况按用户显示。

查看虚拟机使用情况：在计算机使用情况选项卡中，选择**单会话操作系统计算机或多会话操作系统计算机**以实时查看您的 VM 使用情况，从而能够快速评估站点的容量需求。 单会话操作系统可用性 - 按整个站点或特定交付组的可用性显示单会话操作系统计算机 (VDI) 的当前状态。 多会话操作系统可用性 - 按整个站点或特定交付组的可用性显示多会话操作系统计算机的当前状态。

您可以单击显示的横幅上的以下链接，以通过**成本优化**更好地了解计算机使用情况：

- 预计节省 - 此链接将您定向到**成本优化**页面上的**预计节省**部分，其中显示了所有交付组的详细信息。
- 节省报告 - 此链接将您定向到**成本优化**页面上的**节省报告**部分，其中显示了所有交付组的详细信息。

> **注意：**
>
> 可用计数器中显示的计算机数量包括处于维护模式的计算机。

> **查看资源利用率：在资源利用率**选项卡中，选择**单会话操作系统计算机或多会话操作系统计算机**以深入了解每台 VDI 计算机的 CPU 和内存使用情况以及 IOPS 和磁盘延迟的历史趋势数据，从而更好地进行容量规划。 此功能需要 Delivery Controller 和 VDA **版本 7.11** 或更高版本。 图表显示了平均 CPU、平均内存、平均 IOPS、磁盘延迟和并发会话峰值的数据。您可以深入到计算机，查看占用 CPU 的前 10 个进程的数据和图表。

按交付组和时间段进行筛选。CPU、内存使用情况和并发会话峰值图表可用于过去 2 小时、24 小时、7 天、月和年。平均 IOPS 和磁盘延迟图表可用于过去 24 小时、月和年。您可以单击横幅上的**查看**链接，以通过成本优化更好地了解计算机使用情况。此链接会将您带到**成本优化**页面中的**工作负载调整**选项卡，其中显示了从**资源利用率**选项卡中选择的交付组的详细信息。

> **注意：**
>
> - 必须将监视策略设置**启用进程监视**设置为**允许**，才能在历史计算机利用率页面上的“前 10 个进程”表中收集和显示数据。默认情况下，此策略设置为**禁止**。默认情况下会收集所有资源利用率数据。可以使用**启用资源监视**策略设置禁用此功能。图表下方的表格显示了每台计算机的资源利用率数据。有关详细信息，请参阅监视策略设置。
> - 平均 IOPS 显示每日平均值。峰值 IOPS 计算为所选时间范围内 IOPS 平均值的最高值。（IOPS 平均值是 VDA 上每小时收集的 IOPS 的每小时平均值）。

- 计算机深入分析列出了平均 CPU 或平均内存使用率超过 1% 的进程，这可能意味着有时列出的进程少于 10 个。

查看网络分析数据：此功能的可用性取决于您组织的许可证和您的管理员权限。此功能需要 Delivery Controller **版本 7.11** 或更高版本。

在**网络**选项卡中，监视您的网络分析，该分析提供了网络的上下文用户、应用程序和桌面视图。借助此功能，Director 通过 Citrix ADM 中的 HDX Insight 报告提供部署中 ICA 流量的高级分析。有关详细信息，请参阅配置网络分析

查看应用程序故障： 应用程序故障选项卡显示与 VDA 上已发布的应用程序相关的故障。

此功能需要 Delivery Controller 和 VDA **版本 7.15** 或更高版本。支持运行 Windows Vista 及更高版本的单会话操作系统 VDA，以及运行 Windows Server 2008 及更高版本的多会话操作系统 VDA。有关详细信息，请参阅历史应用程序故障监视。

默认情况下，仅显示来自多会话操作系统 VDA 的应用程序故障。您可以使用监视策略设置应用程序故障的监视。有关详细信息，请参阅监视策略设置。

查看探测结果：“**探测结果**”选项卡显示在“配置”页面中已配置探测的应用程序和桌面的探测结果。此处记录了发生故障的启动阶段。

有关详细信息，请参阅应用程序和桌面探测。

创建自定义报告：“自定义报告”选项卡提供了一个用户界面，用于生成包含监控数据库中实时和历史数据的自定义报告，并以表格形式显示。

此功能需要 Delivery Controllers **7.12 版**或更高版本。

从以前保存的自定义报告查询列表中，您可以单击“**运行并下载**”以 CSV 格式导出报告，单击“**复制 OData**”以复制并共享相应的 OData 查询，或者单击“**编辑**”以编辑查询。 您可以基于计算机、连接、会话或应用程序实例创建自定义报告查询。根据计算机、交付组或时间段等字段指定筛选条件。指定自定义报告中所需的其他列。预览显示报告数据的示例。保存自定义报告查询会将其添加到已保存查询列表中。

您可以基于复制的 OData 查询创建自定义报告查询。为此，请选择 OData 查询选项并粘贴复制的 OData 查询。您可以保存生成的查询以供以后执行。

注意：

使用 OData 查询生成的预览和导出报告中的列名未本地化，而是以英文显示。

图表上的标记图标指示该特定时间范围内的重要事件或操作。将鼠标悬停在标记上并单击以列出事件或操作。

注意：

- 对于早于 7 的 VDA，不收集 HDX™ 连接登录数据。对于较早的 VDA，图表数据显示为 0。
- 在 Citrix Studio 中删除的交付组在 Director 趋势筛选器中仍可供选择，直到与其相关的数据被清除。选择已删除的交付组会显示可用数据的图表，直到保留期结束。但是，表格不显示数据。
- 将包含活动会话的计算机从一个交付组移动到另一个交付组，会导致新交付组的“**资源利用率和负载评估器索引**”表格显示从旧交付组和新交付组整合的指标。