# Citrix 虚拟应用和桌面™ 7 2203 LTSR

> **重要提示：**
>
> 当前版本 (CR) 和长期服务版本 (LTSR) 的产品生命周期策略在 生命周期里程碑 中进行了描述。

> Citrix Virtual Apps and Desktops 提供了一种虚拟化解决方案，可将应用程序和桌面交付到任何设备、任何网络，同时增强数据安全性、降低成本并提高生产力。

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

累积更新 6 (CU6) 是 2203 LTSR 的最新更新。LTSR 也适用于 Citrix Virtual Apps and Desktops 1912 以及 XenApp and XenDesktop 版本 7.15。

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

## 早期版本

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

对于更早的版本，文档已存档在 旧版文档 中。

## Citrix Cloud™ 中的 Citrix 虚拟应用和桌面

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

## 有用链接

- Citrix 可支持性包
- LTSR 常见问题解答

- 思杰虚拟应用和桌面服务选项
- 产品生命周期日期
- 适用于 Citrix Workspace 应用程序的 LTSR 计划
- 弃用

# 新增功能

## 累积更新 7 (CU7)

发布日期: Aug 28, 2025

### 关于此版本

Citrix Virtual Apps and Desktops™ 7 2203 LTSR 累积更新 7 (CU7) 修复了自 2203 LTSR CU5 发布以来报告的 25 个以上问题。

2203 LTSR（一般信息）

2203 LTSR（功能和升级信息）

此版本中的新增功能

Citrix Virtual Apps and Desktops 7 2203 LTSR CU5 中修复的问题

此版本中的已知问题

弃用和删除

Citrix 产品订阅权益资格日期

### 下载

Citrix 虚拟应用和桌面 7 2203 LTSR CU7

### 新部署

#### 如何从头开始部署 CU7?

您可以使用 CU7 元安装程序，基于 CU7 设置全新的 Citrix Virtual Apps and Desktops 环境。在此之前，我们建议您熟悉该产品：

在开始规划部署之前，请仔细阅读 Citrix Virtual Apps and Desktops 7 2203 LTSR（初始版本） 部分，并特别注意 技术概述、安装和配置 和 安全性 部分。确保您的设置满足所有组件的 系统要求。

# 现有部署

### 我需要更新什么?

CU7 为 2203 LTSR 的 15 个 基线组件 提供了更新。请记住：Citrix 建议您将部署的所有 LTSR 组件更新到 CU7。例如：如果 Citrix Provisioning 是您的 LTSR 部署的一部分，请将 Citrix Provisioning 组件更新到 CU4。如果 Citrix Provisioning 不是您部署的一部分，则无需安装或更新它。

## 2203 LTSR CU7 基线组件

| 2203 CU7 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
|---|---|---|
| 单会话 VDA | 2203.0.7000.7522 | 单会话 VDA |
| 多会话 VDA | 2203.0.7000.7522 | 多会话 VDA |
| 交付控制器 | 2203.0.7000.7522 | 交付控制器(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#delivery-controller) |
| 思杰工作室 | 7.33.7000.57 | Citrix 工作室 |
| 思杰监控台 | 7.33.7000.26 | Citrix 监控器 |
| Citrix 组策略管理 | 7.33.7000.20 | Citrix 组策略管理(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/policies/policies-processes.html) |
| Citrix 组策略客户端扩展 | 7.33.7000.16 | |
| 思杰 StoreFront | 2203.0.7000.7 | Citrix 店面 |
| Citrix 预配 | 7.33.40 | Citrix 预配 |
| 通用打印服务器 | 7.33.7000.18 | 通用打印服务器 |
| 会话录制 | 22.3.7000 | 会话录制 |
| Linux 虚拟投递代理 | 22.03.6000 | Linux 虚拟投递代理 |
| 配置文件管理 | 22.3.7000.10 | 配置文件管理 |

| 2203 CU7 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| Citrix 联合身份验证服务 | 10.9.700.16 | Citrix 联合身份验证服务 (FAS) |
| 浏览器内容重定向 | 15.32.7000.10 | 浏览器内容重定向 |
| Citrix 探针代理 2305 | 2305.1.0.0 | 下载 |

## 2203 LTSR CU7 兼容组件

以下组件（版本见下）与 LTSR 环境兼容。它们不符合 LTSR 权益（延长生命周期和仅修复累积更新）。Citrix® 可能会要求您在 2203 环境中将这些组件升级到更新版本。

| 兼容组件和功能 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 应用程序分层 | 2309 | Citrix 应用分层 |
| HDX RealTime 优化包 | 2.9.600 | HDX RealTime 优化包 |
| 许可证服务器 | 11.17.2.0_BUILD_53100 | 许可证服务器 |
| 用户个性化层 | 25.3.3 | 用户个性化层 |
| 会话录制 Web 播放器 | 22.3.7000.6 | 会话录制 Web 播放器 |
| 微软团队优化 | 15.32.3000.9 | 微软团队优化 |
| 工作区环境管理 | 22.12.0 | 工作区环境管理 |
| XenApp & XenDesktop 7.15 LTSR VDA (最新版本)* | 仅限最新累积更新 | 文档(/zh-cn/xenapp-and-xendesktop/7-15-ltsr.html) |

## 2203 LTSR CU7 值得注意的排除项

以下功能、组件和平台不符合 2203 生命周期里程碑和权益的条件。具体来说，累积更新和扩展生命周期权益被排除在外。对已排除功能和组件的更新可通过常规当前版本获得。

| 排除的组件和功能 |
| --- |
| AppDisks™ |
| AppDNA® |

| 排除的组件和功能 |
| --- |
| Citrix SCOM 管理包 |
| 帧鹰 |
| 个人 vDisk |
| StoreFront 思杰在线集成 |
| 许可证激活服务 |

| 排除的 WINDOWS 平台 * |
| --- |
| Windows 2008 32 位（适用于通用打印服务器） |

* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

## 新增功能

Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 7 (CU7) 中提供以下新功能和增强功能。

> **注意：**
>
> 如果您使用的是 2203 LTSR CU7，我们建议遵循以下升级路径之一：
>
> - 升级到 2402 LTSR CU3 或更高版本的累积更新。
> - 升级到 2507 或更高版本。
> - 通常，建议升级到未来发布的版本。

### 基于文件的许可系统 EOL 通知

传统上用于激活各种本地组件的基于文件的许可系统将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活 Citrix 产品套件中产品的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 Citrix 本地组件的唯一方式。为了获得支持，您的 Citrix Virtual Apps and Desktops 部署必须是 LAS 兼容版本。LAS 兼容的最低所需 CVAD 版本为：

- CVAD 2203 LTSR CU7
- CVAD 2402 LTSR CU3
- CVAD 2507 LTSR
- CVAD 2411

如果您有任何疑问或疑虑，请联系客户服务。对于不遵守这些要求的行为，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法规定的任何其他补救措施。这些要求不适用于法律或法规禁止的情况。

### 交付控制器

#### 许可服务器版本与 Citrix Virtual Apps and Desktops 站点的兼容性

对于 Citrix Virtual Apps and Desktops 站点的创建和升级，请确保许可服务器运行的最低版本为 11.17.2 build 53100。

## 已修复的问题

以下问题已在 Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU6 之后得到修复：

### 交付控制器™

- 由于任务定义中的变量名无效，Monitor Service 清理可能会失败。此问题会影响 `GroomResourceUtilization` 任务，也可能影响其他清理任务。
- 在存储了数月数据的大型 MonitorDB 上，您可能会遇到 CPU 使用率过高的问题。添加索引可将 CPU 使用率降低约 10-15%
- 在使用非标准小数符号（如“,”）的情况下，将 1912 CU8 升级到 2203 CU4 后，您可能无法创建新的计算机目录或启动现有 VDA。
- 在 Citrix Studio 中进行自动站点升级期间，将 Delivery Controller 从 2203 CU5 升级到 2402 CU1 可能会失败。Delivery Controller 升级完成，但站点更新未成功完成。

### 图形

- 升级到 VDA 2402 后，重启后的第一个 ICA® 会话可能会显示灰屏，通过断开连接并重新连接或先启动应用程序会话即可解决。
- 升级到 Citrix Virtual Apps and Desktops (CVAD) 2203 CU5 或 2402 后，访问 WMI 实例 `Citrix_Client_Enum` 可能会失败，并显示“Provider Load Failure”错误。

### 元安装程序

- 升级到 VDA 2203 后，重启后的第一个 ICA 会话无法启动。您可以通过第二次启动会话来解决此问题。
- 将 VDA 从 2203 CU3 升级到 CU5 会重置 `HKLM\SYSTEM\CurrentControlSet\Services\picadm` 下的所有注册表设置，包括删除 `DisableFullStreamWrite` 条目。如果您希望这些设置保持不变，则可能需要在升级后重新应用它们。

### 通用打印服务器

#### 打印

- 从 Universal Print Server (UPS) 升级到 2203 LTSR CU5 后，选择打印机时可能会遇到长时间延迟。打印机可能会停留在“正在连接到打印机”状态，并需要一分钟以上才能变为可用。

### 适用于单会话操作系统的 VDA

#### 会话/连接

- 启动会话后，多次插拔音频设备会导致会话停止识别音频设备。
- 在关机期间，您可能会遇到带有停止代码的蓝屏错误。

#### 系统异常

- 使用 Windows 11 24H2 时，会话在启动期间挂起并显示黑屏。
- 升级到 VDA 2203 CU5 或 CU6 后，您可能无法登录服务器，会话在登录或注销期间停止响应。
- 您可能会间歇性地遇到蓝屏错误，错误代码为 PAGE_FAULT_IN_NONPAGED_AREA (0x50)，这是由于 picadm.sys 模块中的问题导致的。
- 在 CVAD 2203 CU5 中，您的设备可能会因为 picadm.sys 的新问题而显示蓝屏错误。
- 可能会间歇性地出现错误代码为 PAGE_FAULT_IN_NONPAGED_AREA (0x50) 的蓝屏错误，这是由于 picadm.sys 模块中的问题导致的。

### 适用于多会话操作系统的 VDA

#### 剪贴板

- 当您使用 Citrix Workspace™ for HTML5 时，在 Excel 中复制和粘贴大量数据后，会话会崩溃。
- 在多会话场景中，如果您复制的字符数超过大约 2,493 个，复制和粘贴功能可能会停止工作。
- CtxSvcHost.exe 在剪贴板操作期间可能会崩溃，这是由于剪贴板 DLL 中的问题导致的。

### 会话/连接

- 主机到客户端的 URL 重定向会通过将大写字母转换为小写字母来修改区分大小写的 URL 参数，这可能会导致在访问需要特定字母大小写的应用程序时出现故障。
- 客户端用户可能会遇到随机的 USB 重定向失败，导致 Pinpad、TCR 和 Printers 等 USB 设备在会话期间消失。
- 在关机期间，您可能会遇到带有停止代码的蓝屏错误。
- 当您从 Citrix Workspace App for Linux 启动会话时，会话似乎已打开，但会立即关闭，不显示任何错误。

### 系统异常

- 升级到 VDA 2203 CU5 或 CU6 后，您可能无法登录服务器，会话在登录或注销期间停止响应。
- 您可能会间歇性地遇到蓝屏错误，错误代码为 PAGE_FAULT_IN_NONPAGED_AREA (0x50)，这是由于 picadm.sys 模块中的问题导致的。
- 在 CVAD 2203 CU5 中，您的设备可能会因为 picadm.sys 的新问题而显示蓝屏错误。
- 可能会间歇性地出现错误代码为 PAGE_FAULT_IN_NONPAGED_AREA (0x50) 的蓝屏错误，这是由于 picadm.sys 模块中的问题导致的。
- 更新到 2203 CU5 VDA 后，退出应用程序后会话不会关闭。
- LastPingTime 未在 2203 CU5 的注册表中更新，这可能会导致您断开连接。
- 您可能会遇到随机崩溃，并显示错误检查代码，表明驱动程序存在问题。
- 主机到客户端的 URL 重定向会修改区分大小写的 URL 参数，将大写字母转换为小写字母，这可能会导致在访问需要特定字母大小写的应用程序时出现故障。

## Citrix 供应™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

## Linux 虚拟投递代理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

## 配置文件管理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

## 会话录制

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### StoreFront™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

# 累积更新 6 (CU6)

发布日期: Jan 08, 2025

## 关于此版本

Citrix Virtual Apps and Desktops™ 7 2203 LTSR 累积更新 6 (CU6) 修复了自 2203 LTSR CU5 发布以来报告的 25 个以上问题。

2203 LTSR（一般信息）

2203 LTSR（功能和升级信息）

此版本中的新增功能

Citrix Virtual Apps and Desktops 7 2203 LTSR CU5 中修复的问题

此版本中的已知问题

弃用和删除

Citrix 产品订阅权益资格日期

## 下载

Citrix 虚拟应用和桌面 7 2203 LTSR CU6

## 新部署

### 如何全新部署 CU6?

您可以使用 CU6 元安装程序，基于 CU6 设置全新的 Citrix Virtual Apps and Desktops 环境。在此之前，我们建议您熟悉产品：

在开始规划部署之前，请仔细阅读 Citrix Virtual Apps and Desktops 7 2203 LTSR（初始版本） 部分，并特别注意 技术概述、安装和配置 和 安全性 部分。确保您的设置满足所有组件的 系统要求。

# 现有部署

### 我需要更新什么?

CU6 为 2203 LTSR 的 15 个 基线组件 提供了更新。请记住：Citrix 建议您将部署的所有 LTSR 组件更新到 CU6。例如：如果 Citrix Provisioning 是 LTSR 部署的一部分，请将 Citrix Provisioning 组件更新到 CU4。如果 Citrix Provisioning 不是部署的一部分，则无需安装或更新它。

## 2203 LTSR CU6 基线组件

| 2203 CU6 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
|---|---|---|
| 单会话 VDA | 2203.0.6000.6286 | 单会话 VDA |
| 多会话 VDA | 2203.0.6000.6286 | 多会话 VDA |
| 交付控制器 | 2203.0.6000.6286 | 交付控制器(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#delivery-controller) |
| 思杰工作室 | 7.33.6000.29 | Citrix 工作室 |
| 思杰监控台 | 7.33.6000.20 | Citrix 监控器 |
| Citrix 组策略管理 | 7.33.6000.9 | Citrix 组策略管理(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/policies/policies-processes.html) |
| Citrix 组策略客户端扩展 | 7.33.6000.9 | |
| 思杰 StoreFront | 2203.0.6000.11 | Citrix 店面 |
| Citrix 预配 | 7.33.40 | Citrix 预配 |
| 通用打印服务器 | 7.33.6000.23 | 通用打印服务器 |
| 会话录制 | 22.3.6000 | 会话录制 |
| Linux 虚拟投递代理 | 22.03.6000 | Linux 虚拟投递代理 |
| 配置文件管理 | 22.3.6000.7 | 配置文件管理 |

| 2203 CU6 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| Citrix 联合身份验证服务 | 10.9.6000.9 | Citrix 联合身份验证服务 (FAS) |
| 浏览器内容重定向 | 15.32.6000.9 | 浏览器内容重定向 |
| Citrix 探针代理 2305 | 2305.1.0.0 | 下载 |

## 2203 LTSR CU6 兼容组件

以下组件（版本如下）与 LTSR 环境兼容。它们不享受 LTSR 权益（延长生命周期和仅修复累积更新）。Citrix® 可能会要求您在 2203 环境中将这些组件升级到更新版本。

| 兼容组件和功能 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 应用程序分层 | 2309 | Citrix 应用分层 |
| HDX RealTime 优化包 | 2.9.600 | HDX RealTime 优化包 |
| 许可证服务器 | 11.17.2.0_Build 51000 | 许可证服务器 |
| 用户个性化层 | 24.9.0 | 用户个性化层 |
| 会话录制 Web 播放器 | 22.3.6000.11 | 会话录制 Web 播放器 |
| 微软团队优化 | 15.32.3000.9 | 微软团队优化 |
| 工作区环境管理 | 22.12.0 | 工作区环境管理 |
| XenApp & XenDesktop 7.15 LTSR VDA (最新版本)* | 仅限最新累积更新 | 文档(/zh-cn/xenapp-and-xendesktop/7-15-ltsr.html) |

## 2203 LTSR CU6 值得注意的排除项

以下功能、组件和平台不符合 2203 生命周期里程碑和权益的条件。具体而言，累积更新和扩展生命周期权益被排除在外。排除的功能和组件的更新可通过常规当前版本获得。

| 排除的组件和功能 |
| --- |
| AppDisks™ |
| AppDNA® |

| 排除的组件和功能 |
| --- |
| Citrix SCOM 管理包 |
| 帧鹰 |
| 个人 vDisk |
| StoreFront 思杰在线集成 |
| 许可证激活服务 |

| 排除的 WINDOWS 平台 * |
| --- |
| Windows 2008 32 位（适用于通用打印服务器） |

* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

## 新增功能

以下新功能和增强功能在 Citrix Virtual Apps and Desktops™ 7 2203 LTSR 累积更新 6 (CU6) 中可用：

### 支持将 WBC 磁盘放置在与 OS 磁盘相同的存储位置

从 2203 LTSR CU6 版本开始，在 XenServer®、VMware 和 SCVMM 虚拟化环境中，如果您在创建主机连接时将可用 OS 存储列表配置为与可用临时存储列表相同，MCS 现在会将回写缓存 (WBC) 磁盘放置在与 OS 磁盘相同的存储位置。

此实现有助于降低管理 OS 和 WBC 磁盘的复杂性。有关创建主机连接的信息，请参阅 连接和资源 。

## 已修复的问题

以下问题已在 Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU5 之后得到修复：

### 思杰监控台

- 在多林站点中使用多会话或单会话桌面 VDA 时，以用户为中心的搜索功能不起作用。
- 在 Director 2203 中，由于范围目标无效，用户无法编辑和保存默认的智能警报策略。如果目标 ID 为空或无效，策略将正常工作但验证失败，从而导致错误消息。
- 您可能会遇到无法访问自定义报告的问题。

- 由于缺少枚举值，您可能无法在 Director 筛选器 > 计算机中看到计算机列表。

### Citrix 策略

- 您可能会遇到 CseEngine.exe 进程内存利用率过高的问题，这可能导致计算机注册问题。

### 思杰工作室

- 当将 Studio 用作已发布的应用程序或在 ICA® 会话下的已发布 VDA 中使用 Studio 时，Studio 控制台可能会冻结。
- 当 Broker 应用程序的“名称”和“已发布名称”都更改时，App-V 应用程序详细信息中的“交付方式”字段可能为空。

### 交付控制器™

- 您可能会遇到一个问题，即由于续订的证书使用了组织名称或所需名称，导致 VDA 升级期间 VUA 验证失败。
- 您可能会在监控 SQL 数据库中遇到频繁的死锁，并观察到 Citrix 监控服务的 CPU 和内存使用率很高。
- 您可能会在 Citrix 2203 CU2 中遇到 Machine Creation Services™ (MCS) 的间歇性问题，即尝试添加到现有目录的计算机中只有一半成功。尽管这些计算机出现在 Active Directory 中，但只有成功的计算机显示在 Studio 中，而失败的计算机在手动从 Active Directory 导入之前不会显示在您的 Nutanix 虚拟机管理程序中。
- 您可能会在存储了数月数据的大型 MonitorDB 上遇到高 CPU 使用率。添加索引可以将 CPU 使用率降低约 10-15%。

### 图形

- 您在工作时可能会遇到间歇性屏幕黑屏，持续约 10 秒，在此期间 Citrix 软件图形进程 (Ctxgfx.exe) 会重置。twencode 线程遇到访问冲突异常，导致 ctxExceptionHandler 记录小型转储并引发此问题。ctxExceptionHandler 已设置为生成完整转储以供检查。
- 在 CVAD 2203 LTSR CU2 的本地 Director 中，您可能会看到“代理”和“VM 启动”指标始终显示为 N/A。当 VDA 配置为仅在您启动时才启动时，会发生这种情况。您在查看登录性能数据时可能会遇到此问题。
- 您在工作时可能会遇到间歇性屏幕黑屏，持续约 10 秒，在此期间 Citrix 软件图形进程 (Ctxgfx.exe) 会重置。twencode 线程遇到访问冲突异常，导致 ctxExceptionHandler 记录小型转储并引发此问题。ctxExceptionHandler 已设置为生成完整转储以供检查。

### 元安装程序

- 您可能会遇到一个问题，即缺失的托管实例 (MI) 状态需要重新启动或恢复。这可能会影响 VUA 的功能。
- 从 CVAD 2203 CU5 升级后，文件 `Microsoft.IdentityModel.Abstractions.dll` 从 Citrix Virtual Desktop Agent 安装目录中缺失。

### 通用打印服务器

#### 打印

- 您可能会遇到一个问题，即打印机在 Citrix 会话中无法工作，导致 Print Spooler 崩溃，从而产生多个事件 ID 1102 和 1106 错误。
- Citrix 打印管理服务可能会间歇性终止，导致重定向的打印机停止工作。

### 适用于单会话操作系统的 VDA

- 升级到 CVAD 2203 后，您可能会遇到打开桌面时大约 10 秒的延迟。
- 您可能会遇到一个问题，即 Citrix Cloud™ VDA 中的 Citrix 音频重定向服务失败，影响会话期间的音频功能。

#### 剪贴板

- 当您使用 VDA 2203 LTSR Cu4 并在 WebP 格式中复制和粘贴内容时，`WfShell` 停止工作。
- 您可能会遇到问题，即 VDA 中大型图像和 Excel 图表的会话剪贴板重定向失败，导致您无法将这些项目复制并粘贴到客户端。

#### 会话/连接

- 您可能会遇到一个问题，即在升级到 2203 CU4 后，注销会话或终止已发布的应用程序窗口需要 2-3 分钟才能从 VDA 中清除。
- 如果在初始会话期间后台处理程序服务重新启动，客户端映射的打印机在重新连接后可能会消失。从同一客户端重新连接时，打印机仍然可见。

#### 智能卡

- 您可能会遇到一个内存泄漏问题，即服务器 VDA 实例上的 Citrix 智能卡服务内存消耗高达 100%。

#### 系统异常

- 在使用快捷方式“Windows + Print Screen”时，您可能会遇到 Virtual Delivery Agent (VDA) 中“explorer.exe”进程崩溃的问题。

- 在 Citrix 会话期间，当您在基于 WebRTC 的应用程序中录制来自重定向网络摄像头的流时，可能会注意到图像失真。
- 当没有活动会话时，在进入或退出中断期时，您可能会遇到单会话随机机器断电的情况。
- 此版本不支持 32 位 Web 应用程序的 FIDO2。

### 适用于多会话操作系统的 VDA

- 当您重新连接到使用 Machine Creation Services (MCS) 预配的虚拟投递代理 (VDA) 时，它可能会因空闲断开连接而注销，导致 VDA 在 Director 中显示为未注册。此问题也影响非 MCS VDA，并在 VDA 通过 RDP 断开连接或在 RDP 会话中空闲时发生。
- 您可能会遇到 Citrix Cloud VDA 中 Citrix 音频重定向服务失败的问题，这会影响会话期间的音频功能。
- 漫游时，您可能会遇到音频应用程序崩溃的问题，这是由 icaendpoint.dll 模块挂起引起的。
- 当已发布的 New Microsoft Teams 应用程序在安装了 VDA 2402 或 VDA 2402 CU1 的 Windows 2022 操作系统上作为无缝应用程序运行时，您可能会遇到系统托盘图标不响应左键单击的问题。这仅在应用程序最小化时发生；当您处于完整桌面会话中时，它工作正常。

#### 剪贴板

- 当您使用 VDA 2203 LTSR Cu4 并在 WebP 格式中复制和粘贴内容时，`WfShell` 停止工作。
- 您可能会遇到 VDA 中会话剪贴板重定向对大型图像和 Excel 图表失败的问题，导致您无法将这些项目复制并粘贴到客户端。

#### 会话/连接

- 您可能会注意到，当自动客户端重新连接 (ACR) 被禁用时，每次重新连接都会记录事件“MetaFrame 9006”，从而产生许多不需要的错误消息。
- 您可能会遇到 VDA 随机无响应并进入未注册状态的问题，导致用户被踢出其 ICA 会话。
- 升级到 2203 CU4 后，您可能会遇到注销会话或终止已发布的应用程序窗口需要 2-3 分钟才能从 VDA 中清除的问题。
- 您可能会注意到，在其他系统托盘图标列表中，Citrix WinFrame Shell 项目的数量不断增加，即使 ICA 会话中只显示一个电池图标。这种累积发生在系统设置的“个性化”>“任务栏”>“其他系统托盘图标”下。
- 如果在初始会话期间重新启动了后台处理程序服务，则客户端映射的打印机在重新连接后可能会消失。从同一客户端重新连接时，打印机仍然可见。

### 智能卡

- 您可能会遇到服务器 VDA 实例上的 Citrix 智能卡服务存在内存泄漏问题，内存消耗高达 100%。

### 系统异常

- 在多会话设置中播放视频时，您可能会遇到 Windows Media 重定向问题。
- 您可能会遇到 Citrix VDA 相关的 TermService 崩溃。
- 您可能会遇到一个问题，即尽管 VDA 接收到了电池状态，但电池状态未在 Windows 11 多会话 VDA 上显示。
- 读取许可证状态时，wdica32.exe 上可能会发生错误检查 0x50。

### Citrix 供应™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### Linux 虚拟投递代理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### 配置文件管理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### 会话录制

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### StoreFront™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

# 累积更新 5 (CU5)

发布日期：Jun 04, 2024

## 关于此版本

Citrix Virtual Apps and Desktops™ 7 2203 LTSR 累计更新 5 (CU5) 修复了自 2203 LTSR CU4 发布以来报告的 25 个以上问题。

2203 LTSR（一般信息）

2203 LTSR（功能和升级信息）

此版本中的新增功能

Citrix Virtual Apps and Desktops 7 2203 LTSR CU4 中修复的问题

此版本中的已知问题

弃用和删除

Citrix 产品订阅权益资格日期

## 下载

Citrix 虚拟应用和桌面 7 2203 LTSR CU5

## 新部署

### 如何从头开始部署 CU5?

您可以使用 CU5 元安装程序，基于 CU5 设置全新的 Citrix Virtual Apps and Desktops 环境。在此之前，建议您先熟悉产品：

在开始规划部署之前，请仔细阅读 Citrix Virtual Apps and Desktops 7 2203 LTSR（初始版本） 部分，并特别注意 技术概述、安装和配置 和 安全性 部分。确保您的设置满足所有组件的 系统要求。

## 现有部署

### 我需要更新什么?

CU5 为 2203 LTSR 的 15 个 baseline components 提供了更新。请记住：Citrix 建议您将部署中的所有 LTSR 组件更新到 CU5。例如：如果 Citrix Provisioning 是 LTSR 部署的一部分，请将 Citrix Provisioning 组件更新到 CU4。如果 Citrix Provisioning 不是部署的一部分，则无需安装或更新它。

## 2203 LTSR CU5 基线组件

| 2203 CU5 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 单会话 VDA | 2203.0.5000.5310 | 单会话 VDA |
| 多会话 VDA | 2203.0.5000.5310 | 多会话 VDA |
| 交付控制器 | 2203.0.5000.5310 | 交付控制器(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system- |

| 2203 CU5 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| | | requirements.html#delivery-controller) |
| 思杰工作室 | 7.33.5000.17 | Citrix 工作室 |
| 思杰监控台 | 7.33.5000.16 | Citrix 监控器 |
| Citrix 组策略管理 | 7.33.5000.10 | Citrix 组策略管理(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/policies/policies-processes.html) |
| Citrix 组策略客户端扩展 | 7.33.5000.9 | |
| 思杰 StoreFront | 2203.0.5000.6 | Citrix 店面 |
| Citrix 预配 | 7.33.40 | Citrix 预配 |
| 通用打印服务器 | 7.33.5000.8 | 通用打印服务器 |
| 会话录制 | 22.3.5000 | 会话录制 |
| Linux 虚拟投递代理 | 22.03.5000 | Linux 虚拟投递代理 |
| 配置文件管理 | 22.3.5000.2 | 配置文件管理 |
| Citrix 联合身份验证服务 | 10.9.5000.8 | Citrix 联合身份验证服务 (FAS) |
| 浏览器内容重定向 | 15.32.5000.7 | 浏览器内容重定向 |
| Citrix 探测代理 2305 | 2305.1.0.0 | 下载 |

## 2203 LTSR CU5 兼容组件

以下组件（版本如下）与 LTSR 环境兼容。它们不符合 LTSR 权益（延长生命周期和仅修复的累积更新）的条件。Citrix® 可能会要求您在 2203 环境中将这些组件升级到更新版本。

| 兼容组件和功能 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 应用程序分层 | 2309 | Citrix 应用分层 |

| 兼容组件和功能 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| HDX RealTime 优化包 | 2.9.600 | HDX RealTime 优化包 |
| 许可证服务器 | 11.17.2.0_BUILD_47000 | 许可证服务器 |
| 用户个性化层 | 24.3.2 | 用户个性化层 |
| 会话录制 Web 播放器 | 22.3.5000.2 | 会话录制 Web 播放器 |
| 微软团队优化 | 15.32.3000.9 | 微软团队优化 |
| 工作区环境管理 | 22.12.0 | 工作区环境管理 |
| XenApp & XenDesktop 7.15 LTSR VDA (最新版本)* | 仅限最新累积更新 | 文档(/zh-cn/xenapp-and-xendesktop/7-15-ltsr.html) |

## 2203 LTSR CU5 值得注意的排除项

以下功能、组件和平台不符合 2203 生命周期里程碑和权益的条件。具体而言，累积更新和扩展生命周期权益被排除在外。对被排除的功能和组件的更新可通过常规当前版本获得。

| 排除的组件和功能 |
| --- |
| AppDisks™ |
| AppDNA® |
| Citrix SCOM 管理包 |
| 帧鹰 |
| 个人 vDisk |
| StoreFront 思杰在线集成 |

| 排除的 WINDOWS 平台 * |
| --- |
| Windows 2008 32 位（适用于通用打印服务器） |

* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

# 新增功能

Citrix Virtual Apps and Desktops™ 7 2203 LTSR 累积更新 5 (CU5) 中没有新功能和增强功能。

# 已修复的问题

以下问题已在 Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU4 之后得到修复：

### 思杰监控台

- 当您在多林站点中使用多会话或单会话桌面 VDA 时，以用户为中心的搜索功能不起作用。

### Citrix 策略

- 当您在 Windows 11 多会话计算机上安装 Studio 并打开组策略管理控制台时，加载 Citrix 组策略模块时会显示以下错误消息：`ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p. The memory could not be %s.`
- Citrix Studio 错误地显示了交付组 `uuid`，而不是“分配给”中 **策略** 选项卡中的名称。

### 思杰工作室

- 当 Studio 作为已发布的应用程序使用时，或者在 ICA® 会话下的已发布 VDA 中使用时，Studio 控制台可能会冻结。
- 当您通过 Citrix Studio 添加 StoreFront™ 服务器地址并将其分配给交付组时，商店默认设置为关闭。

### 交付控制器™

- 创建\更新计算机目录任务在可用区 B 中失败，但在可用区 A 和 C 中正常工作，因为无法在您的云连接中启动卷服务实例。运行以下命令以更新站点数据库表，以便在 SQL Server 上使用新的 VolumeWorkerTemplate。`UPDATE HostingUnitServiceSchema.VolumeServiceConfigurationBaseTemplate SET TemplateId = 'ami-09b42976632b27e9b' WHERE RegionName = 'ap-southeast-2'`

> **注意：**
>
> 可用区可能因客户而异。

- 管理程序重新启动后，由于配置了高峰时段电源管理，虚拟机无法启动。
- 当密码字段为空时，已发布的资源可能无法枚举。

### 图形

- 当您使用 Citrix Virtual Apps and Desktops 2203 时，重新连接到断开连接的会话时，可能会出现黑屏。

### 元安装程序

- 当您将 VDA 2203 CU3 版本与 Windows 10 结合使用时，如果配置了 Rendezvous 代理，VDA 安装程序不会托管自定义 WCF 端口。
- 尝试将 Citrix Virtual Apps and Desktops 从 1912 LTSR 版本升级到 2305 或 2203 LTSR 版本可能会失败，并显示以下错误消息：我们发现了不受支持的配置。

### 微软团队优化

- Microsoft Teams 2.1 默认未在 VDA 上进行优化。

### 监控

- 监控数据库中 `MonitorData.ResourceUtilization` 表的更新延迟。

### 通用打印服务器

#### 打印

- 从打印机安全权限中删除“Everyone”组后，Citrix Universal™ Print Server 可能无法按预期工作。
- 按照知识中心文章 CTX140208 中所述安装的 HP Color LaserJet 2800 Series PS 驱动程序在 VDA 升级期间可能会被卸载。
- 当您使用 VDA 版本 1912 CU5 和操作系统版本 2012 R2 时，来自生产 Citrix UPS 打印服务器的各种打印作业失败，并显示以下错误消息：`CCgpStream::Open: WaitForMultipleObjects time out. InternalUpcRemoteOpenStream: Failed to Open Stream. Abort Job.`
- 当您在 Citrix Virtual Apps and Desktops 版本 2212 或 2305 中使用 UPS 版本 2212 或 2305 以及 Windows 10 VDA 时，使用 CUPS 的打印机显示以下消息：

  `Access Denied, cannot connect message`

### 适用于单会话操作系统的 VDA

#### 键盘

- 当您将文件从本地工作站复制并粘贴到 VDA LTSR 2203 的 Citrix 会话中时，`Wfshell.exe` 进程可能会崩溃。

- 已发布的远程应用程序中的“复制到剪贴板”选项不适用于 CU3 和 CU4 版本。

**会话/连接**

- 在闰日 VDA 重启后，`WebSocketService.exe` 进程无法启动。
- 当您使用 Windows 10 VDA 版本 2308 时，`ctxappvservice.exe` 进程可能会崩溃。
- 当您使用 Citrix VDA LTSR 1912 CU3 及更高版本，并且系统具有附加连接且随着附加用户数量的增加而更可能出现问题时，Citrix HDX™ HTML5 Video 可能会崩溃。
- 在 ICA 会话重新连接期间，第三方消息应用程序的聊天窗口可能会自动显示在前台。
- 当您使用一台计算机时，用户会话启动会间歇性失败。
- 当从安装了 Citrix Workspace™ App 版本 2210 或 2303 的 Windows 10 端点连接到安装了 VDA 2203 CU3 的 Windows 10 时，尝试在 WebRTC 应用程序中选择摄像头会导致会话断开连接。
- 启用 IPv6 时，VDA 可能会间歇性注销。
- 尝试使用智能卡重新连接到 Citrix Virtual Apps and Desktops 版本 2203 LTSR CU2 上的 VDA 会话可能会导致欢迎屏幕卡住。
- 当您启动虚拟桌面（Win10 多会话）并插入耳机时，在调整系统音频音量时，UAC 声音会出现明显的延迟。
- 将内容从桌面上的已发布的 Microsoft Visio 或 Visio 应用程序复制到用户设备上的应用程序可能会失败。
- 在非英语操作系统上，Citrix HDX 3D Pro 警告对话框中显示的消息可能会损坏。
- 当您启动连接到运行版本 2203 LTSR CU2 并安装了 Microsoft Defender Application Control 的 VDA 的会话时，可能会出现几秒钟的灰屏。
- 在远程 PC 访问中，某些事件记录在“Citrix-HostCore-ICA Service/Admin”中。当使用 **Ctrl+Alt+Del** 断开会话时，会记录事件 ID 43 和 46。在英语操作系统的 VDA 中，它按预期工作。在日语操作系统的 VDA 中，事件 ID 37 到 50 未记录在“Citrix-HostCore-ICA Service”中。
- 浏览器服务检查端点中是否提供了 `ctxcsb`，如果不可用，则通过 GVCH 遵守 BCR 功能交换并关闭该功能。
- 如果您使用 Microsoft 帐户登录 Excel 或 Word 并且启用了特殊文件夹重定向，则在打开并输入几个字符后，Excel 或 Word 365 会在 `sfrhook.dll` 上崩溃。如果禁用特殊文件夹重定向，则不会出现此问题。
- ACR 重新连接后，终端服务进程可能会崩溃。
- 当您使用 SFCR 模式设置浏览器内容重定向时，BCR 网页可能无法加载完整页面。
- 由于以下模块的访问冲突，**OpenTEXT ETX** 应用程序无法打开：

`C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll`

- 当您使用 Virtual Apps and Desktops 2203 LTSR、Citrix Workspace app 2203 LTSR CU3 (2303 或 2205) 和 Windows 11 22h2 的 VDA 2203 LTSR 重新连接后，设置在左侧显示器左半部分的应用程序会错误地显示在屏幕中央。
- 如果打印机或打印服务器无法访问，会话登录和注销可能需要很长时间才能响应。

#### 系统异常

- 当您使用 VDA 时，picadd.sys 上可能会出现致命异常，并显示带有错误检查代码 0x96 的蓝屏。这适用于所有操作系统。
- 当您使用 VDA 版本 LTSR 2203 CU 4.1 时，VDA 可能会在会话开始时或会话期间的任何时间执行错误检查，并显示消息 `Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED: Tdica.sys`。

### 适用于多会话操作系统的 VDA

#### 键盘/鼠标

- 在 Windows Server 2022 中，如果鼠标被应用程序或操作系统移动到指定位置，则在应用程序或操作系统将鼠标移动到其他位置之前，您无法再次将鼠标移动到该位置。
- 已发布的远程应用程序中的“复制到剪贴板”选项不适用于 CU3 和 CU4 版本。

#### 会话/连接

- 在闰日 VDA 重启后，`WebSocketService.exe` 进程无法启动。
- 尽管会话空闲时间限制生效，但“警告空闲时间已过期”消息对话框未在 2022 OS VDA 上的 ICA 会话中显示。
- 在 Server 2019 VDA 版本 LTSR 2203 CU3 中，`WmiPrvSE.exe` 崩溃。
- 当您使用 Citrix VDA 版本 LTSR 1912 CU3 及更高版本时，如果系统具有附加连接并且随着附加用户数量的增加而更可能出现问题，则 Citrix HDX HTML5 视频可能会崩溃。
- 当 Citrix Workspace 应用程序的某些进程在已发布的应用程序会话中运行时，它们可能无法按预期关闭。
- 在 ACR 重新连接后，终端服务进程可能会崩溃。
- 当您使用 SFCR 模式设置浏览器内容重定向时，BCR 网页可能无法加载完整页面。
- 由于访问冲突，**OpenTEXT ETX** 应用程序无法打开，涉及以下模块：

`C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll`

- 如果打印机或打印服务器无法访问，会话登录和注销可能需要很长时间才能响应。
- WebSocketService (HTML5 视频重定向 WebSocker 服务) 可能会崩溃。

#### 系统异常

- 当您使用 VDA 时，可能会遇到 picadd.sys 上的致命异常，并显示带有错误检查代码 0x96 的蓝屏。这适用于所有操作系统。
- 当您使用 VDA 版本 LTSR 2203 CU 4.1 时，VDA 可能会在会话开始时或会话期间的任何时候执行错误检查，并显示消息 `Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED: Tdica.sys`。

### Citrix 供应™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### Linux 虚拟投递代理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### 配置文件管理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### 会话录制

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### StoreFront

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

# 累积更新 4 (CU4)

发布日期：November 16, 2023

## 关于此版本

Citrix Virtual Apps and Desktops™ 7 2203 LTSR 累积更新 4 (CU4) 修复了自 2203 LTSR CU3 发布以来报告的 60 多个问题。

2203 LTSR（一般信息）

2203 LTSR（功能和升级信息）

此版本中的新增功能

Citrix Virtual Apps and Desktops 7 2203 LTSR CU3 中修复的问题

此版本中的已知问题

弃用和删除

Citrix 产品订阅优势资格日期

## 下载

Citrix 虚拟应用和桌面 7 2203 LTSR CU4

## 新部署

### 如何从头开始部署 CU4?

您可以使用 CU4 元安装程序设置基于 CU4 的全新 Citrix Virtual Apps and Desktops 环境。在此之前，我们建议您熟悉产品：

在开始规划部署之前，请仔细阅读 Citrix Virtual Apps and Desktops 7 2203 LTSR（初始版本） 部分，并特别注意 技术概述、安装和配置 和 安全 部分。确保您的设置满足所有组件的 系统要求。

## 现有部署

### 我需要更新什么?

CU4 为 2203 LTSR 的 15 个 基线组件 提供了更新。请记住：Citrix 建议您将部署中的所有 LTSR 组件更新到 CU4。例如：如果 Citrix Provisioning 是您的 LTSR 部署的一部分，请将 Citrix Provisioning 组件更新到 CU4。如果 Citrix Provisioning 不是您部署的一部分，则无需安装或更新它。

## 2203 LTSR CU4 基线组件

| 2203 CU4 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 单会话 VDA | 2203.0.4000.4310 | 单会话 VDA |
| 多会话 VDA | 2203.0.4000.4310 | 多会话 VDA |
| 交付控制器 | 2203.0.4000.4310 | 交付控制器(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#delivery-controller) |

| 2203 CU4 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 思杰工作室 | 7.33.4000.15 | Citrix 工作室 |
| 思杰监控台 | 7.33.4000.26 | Citrix 监控器 |
| Citrix 组策略管理 | 7.33.4000.2 | Citrix 组策略管理(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/policies/policies-processes.html) |
| Citrix 组策略客户端扩展 | 7.33.4000.5 | |
| 思杰 StoreFront | 2203.0.4000.13 | Citrix 店面 |
| Citrix 预配 | 7.33.40 | Citrix 预配 |
| 通用打印服务器 | 7.33.4000.11 | 通用打印服务器 |
| 会话录制 | 22.3.4000 | 会话录制 |
| Linux 虚拟投递代理 | 22.03.3000.6 | Linux 虚拟投递代理 |
| 配置文件管理 | 22.3.4000.7 | 配置文件管理 |
| Citrix 联合身份验证服务 | 10.9.4000.6 | Citrix 联合身份验证服务 (FAS) |
| 浏览器内容重定向 | 15.32.4000.12 | 浏览器内容重定向 |
| Citrix 探针代理 2305 | 2305.1.0.0 | 下载 |

## 2203 LTSR CU4 兼容组件

以下组件（版本如下）与 LTSR 环境兼容。它们不享受 LTSR 权益（延长生命周期和仅修复的累积更新）。Citrix® 可能会要求您在 2203 环境中将这些组件升级到更新版本。

| 兼容组件和功能 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 应用程序分层 | 2309 | Citrix 应用分层 |
| HDX RealTime 优化包 | 2.9.600 | HDX RealTime 优化包 |

| 兼容组件和功能 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 许可证服务器 | 11.17.2.0_BUILD_44000 | 许可证服务器 |
| 用户个性化层 | 23.9.1 | 用户个性化层 |
| 会话录制 Web 播放器 | 22.3.4000.4 | 会话录制 Web 播放器 |
| 微软团队优化 | 15.32.3000.9 | 微软团队优化 |
| 工作区环境管理 | 22.12.0 | 工作区环境管理 |
| XenApp & XenDesktop 7.15 LTSR VDA (最新版本)* | 仅限最新累积更新 | 文档(/zh-cn/xenapp-and-xendesktop/7-15-ltsr.html) |

## 2203 LTSR CU4 值得注意的排除项

以下功能、组件和平台不符合 2203 生命周期里程碑和权益的条件。具体而言，累积更新和扩展生命周期权益被排除在外。排除的功能和组件的更新可通过常规当前版本获取。

| 排除的组件和功能 |
| --- |
| AppDisks™ |
| AppDNA® |
| Citrix SCOM 管理包 |
| 帧鹰 |
| 个人 vDisk |
| StoreFront 思杰在线集成 |

| 排除的 WINDOWS 平台 * |
| --- |
| Windows 2008 32 位（适用于通用打印服务器） |

* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

## 新增功能

Citrix Virtual Apps and Desktops 7 2203 LTSR 累积更新 4 (CU4) 中没有新功能和增强功能。

# 已修复的问题

## 2203 LTSR 累积更新 4 (CU4) 更新 1 中已修复的问题

### 适用于单会话和多会话操作系统的 VDA

#### 系统异常

- VDA 可能会在 picadd.sys 上遇到致命异常，并显示蓝屏，其中包含以下错误消息：

  错误：Bug Check 0x96 INVALID_WORK_QUEUE_IT

> **注意：**
>
> 此修复仅在 CU4 Update 1 最小安装程序中可用。

## 2203 LTSR 累积更新 4 (CU4) 中修复的问题

自 Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU3 发布以来，以下问题已得到修复：

### 思杰监控台

- 内存使用情况可能不会显示在 **Citrix Director console > Trends > Load Evaluator Index** 中。
- 在 Citrix Director 中，**Director console > Trends > Machine Usage > Multi-session OS Machines** 中的计算机使用情况在所有交付组的“正在使用”列中显示为 0（零）。

### Citrix 策略

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\VCPolicies 设置中的虚拟通道策略值 **VirtualChannelWhiteList** 可能会损坏，并在重启后无法应用于 VDA。当您从 C:\ProgramData\Citrix\GroupPolicy 文件夹中删除文件或剪切文件夹中的内容并将其粘贴到其他位置时，会出现此问题。
- 组策略建模值显示禁用值而不是实际值。例如，**显示内存单位**值显示为禁用而不是实际值 65536 KB。
- 当您将 VDA 升级到 LTSR CU7 版本时，尝试在不同域上应用 Citrix 用户策略可能会失败。
- 当您从 **Citrix Group Policy Modelling Wizard** 中选择用户并选择“**跳到向导的最后一页而不收集其他数据**”选项时，此错误消息可能会显示在“**摘要**”页面上：

  **值不能为 null。**

**参数名称键**

- 配置文件重置后，文件夹重定向可能会间歇性失败。

**思杰工作室**

- Citrix Studio 中的日志记录视图可能无法显示数据。

**交付控制器™**

- 某些 Citrix XML 性能计数器可能无法添加到性能监视器图中。
- 尝试在 XenServer® 池主服务器上创建新的托管连接可能会失败，并显示以下错误消息：

  **无法联系主机服务器。请检查连接是否具有有效的主机地址，以及主机服务器是否已开机并正常工作。**

  **未能获取 XenServer 主机列表。**

- VDA 可能无法注册，并可能停留在初始化状态，会话计数显示为 -1。
- 当运行 Microsoft Windows 11 的持久性 VDA 重置密码时，您可能无法登录 VDA。事件日志中可能会每 30 天出现一次域信任关系失败错误消息。
- 在创建 AWS 计算机目录时，即使相应的准备虚拟机已终止并删除，prepare-identity 卷也可能不会自动删除。
- 通过此修复，Machine Creation Services™ 支持 vSAN 8。

**元安装程序**

- 当您安装适用于多会话操作系统的 VDA 并启用**启用与服务器计算机的连接**选项并升级 VDA 时，升级向导中会显示**主 MCS 映像的其他组件**文本，而不是**用于启用与服务器的代理连接的其他组件**。

> **注意：**
>
> 此修复适用于 Citrix Virtual Apps and Desktops 1912 LTSR CU8 及更高版本，以及从 1912 LTSR CU 升级到 1912 LTSR CU8 及更高版本。但是，此修复不适用于 XenApp and XenDesktop 7.15 LTSR CU，以及从 XenApp and XenDesktop 7.15 LTSR 升级到 Citrix Virtual Apps and Desktops 1912 LTSR CU 的情况。

### 通用打印服务器

#### 客户端

- 使用 Citrix Universal™ Print Server 打印文件时，打印后台处理程序服务可能会意外退出。

### 适用于单会话操作系统的 VDA

#### 安装、卸载、升级

- 当您将 Citrix Virtual Apps and Desktops 2203 LTSR 从 CU1 升级到 CU2 时，在以下注册表项下手动创建的值 **EnableVistaMousePointers**、**EnforceUserPolicyEvaluationSuccess**、**Flag** 和 **CitrixDoD** 可能会消失：
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

    名称: `EnableVistaMousePointers`

    类型: DWORD

    值：1
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy`

    名称: `EnforceUserPolicyEvaluationSuccess`

    类型: DWORD

    数据: 0
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\Smart Card Hook`

    名称: `Flag`

    类型: DWORD

    值: 0
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits

    名称: `CitrixDoD`

    类型: DWORD

    值: 0

- 将 VDA 升级到 1912 LTSR CUx 或 2203 LTSR CUx 后，注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI 下的 **ApplicationLaunchWaitTimeoutMS** 值可能无法恢复。

#### 键盘

- 当您在英国和美国等键盘布局之间切换时，会话中的键盘可能会出现间歇性语言问题。
- 当您在 Ubuntu 上使用 Citrix Workspace™ 应用程序，且 VDA 版本为 2203 LTSR CU3 或更早版本时，键盘布局同步可能无法正常工作。例如，如果用户将本地和服务器端键盘布局从英语更改为德语，即使两个键盘都具有德语布局，键盘也可能显示不正确的字符输出。

#### 打印

- 当您重新启动启用了通用打印服务器策略的 VDA 时，通用打印服务器的负载平衡可能无法启动。
- 本地打印机在首次启动时可能无法重定向到会话。但是，在后续启动时，本地打印机会被重定向。

#### 会话/连接

- 当您使用 `servervdi` 命令行参数安装 Virtual Delivery Agent 时，Windows 音频服务可能不会自动启动。此错误消息会显示在通知区域中：

  **音频服务未运行。**

- 会话可能会在 Cloud Studio 或 Monitor 中保持在“**正在注销**”状态，直到系统启动。当 RemotePC VDA 从 RemotePC 内部关闭时，会出现此问题。
- 当您使用剪贴板映射从会话 1 复制内容并尝试将其粘贴到会话 2 时，内容可能不会出现在会话 2 的剪贴板中。当会话 2 在从会话 1 复制内容后启动时，会出现此问题。
- 将 VDA 升级到版本 2203 后，Skype for Business 应用程序启动时可能会显示启动画面并变得无响应。
- 当 Citrix Print Manager Service 被禁用时，在运行 Microsoft Windows Server 的全新安装的 VDA 版本 2203 LTSR CU2 上，客户端驱动器映射 (CDM) 可能无法工作。
- 当 VDA 上启用了 Shellbridge 功能时，来自 HTML5 和 Android 的无缝应用程序会话可能会显示意外的 UI 窗口，从而阻止用户输入。
- 注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy 下的 **SaveRsopToFile**、**SaveRsopToMemory** 和 **SaveRsopToRegistry** 值可能无法恢复。
- 当连接到用户设备的音频设备超过八个时，Citrix 音频重定向可能无法与 VDA 版本 2203 LTSR CU3 配合使用。

- 在运行 macOS Ventura 的适用于 Mac 的 Citrix Workspace 应用程序上，网络摄像头重定向可能会失败。
- 将 VDA 升级到版本 2203 LTSR CU3 后，尝试使用自定义 ICA® 文件启动应用程序可能会失败。
- 如果 VDA 上未安装会话录制代理，并且您运行 **Get-BrokerSessionRecordingStatus**、**Start-BrokerSessionRecording** 和 **Stop-BrokerSessionRecording** PowerShell 命令，则 VDA 会在几秒钟内注销并重新向 Delivery Controller 注册。此操作对现有会话没有影响。如果 VDA 上安装了会话录制代理，则 PowerShell 命令将正常工作。

#### 智能卡

- 当您使用智能卡启动会话并尝试解锁锁定的会话时，您可能会收到输入密码而不是智能卡 PIN 的提示。当您安装了 Microsoft 补丁 KB5018410 时，会出现此问题。
- 从 VDA 注销时，CtxSvcHost (CtxSmartCardSvc) 可能会意外退出。

#### 系统异常

- 安装了 VDA 的某些第三方应用程序的内部网站可能不允许在没有提示的情况下访问。
- Citrix PDF 通用打印机驱动程序可能会因 acfpdfuamd64.dll 模块故障而意外退出。
- wfica32.exe 进程可能会意外退出。
- VDA 可能会在 Wdica.sys 上遇到致命异常并显示蓝屏。
- Citrix 软件图形进程 (Ctxgfx.exe) 可能会持续消耗会话中所有可用内存，导致会话最终断开连接。
- 图形状态指示器进程 GfxStatusIndicator.exe 可能会反复退出。
- 将 VDA 从版本 2203 LTSR CU2 升级到 CU3 后，VDA 可能会在 picadm.sys 上遇到致命异常并显示蓝屏。

#### 用户体验

- 在 Microsoft Excel 中复制和粘贴大量数据时，wfshell.exe 进程可能会无响应。

### 适用于多会话操作系统的 VDA

#### 键盘

- 升级 VDA 到版本 2305 或版本 2203 LTSR CU3 后，快捷键组合可能无法正常工作。例如，在 Word 文档中，对选定的单词按 **Ctrl+Shift+K** 键会使其大写。但是，如果释放 **K** 键并再次按下，更改不会恢复。

- 在 Ubuntu 上使用 Citrix Workspace 应用程序，且 VDA 版本为 2203 LTSR CU3 或更早版本时，键盘布局同步可能无法正常工作。例如，如果用户将本地和服务器端的键盘布局从英语更改为德语，即使两个键盘都具有德语布局，键盘也可能显示不正确的字符输出。

### 打印

- 重新启动启用了通用打印服务器策略的 VDA 时，通用打印服务器的负载平衡可能无法启动。
- 首次启动时，本地打印机可能无法重定向到会话。但是，在后续启动期间，本地打印机会被重定向。

### 会话/连接

- 会话可能在 Cloud Studio 或 Monitor 中保持“正在注销”状态，直到系统启动。当 RemotePC VDA 从 RemotePC 内部关闭时，会出现此问题。
- 在 Citrix 服务器中使用 Adobe Acrobat Reader DC 打开 PDF 文件时，可能会出现以下错误消息：

  **Werfault.exe - 应用程序错误**

  **应用程序无法正常启动 (0xc0000142)。单击“确定”关闭应用程序。**

- 即使您从会话注销或会话断开连接，会话录制也可能继续录制。
- 在不中断会话的情况下在端点之间切换时，如果启用了计划的重新启动通知，则可能会出现多个重新启动通知。
- 当您打开应用程序的 2 个实例并将 **DisableToggler** 设置为五秒时，您可能需要等待大约 30 秒才能在第二个应用程序中键入内容。
- 当您使用剪贴板映射从会话 1 复制内容并尝试将其粘贴到会话 2 时，内容可能不会出现在会话 2 的剪贴板中。当会话 2 在内容从会话 1 复制后启动时，会出现此问题。
- 将 VDA 升级到版本 2203 后，Skype for Business 应用程序启动时可能会显示启动画面并变得无响应。
- 更改客户端的 DPI 值后重新连接到会话时，新值可能不会应用于会话。
- 将 VDA 升级到版本 2203 LTSR CU2 后，VDA 可能会注销。
- 在将 VDA 升级到 2203 LTSR CU3 版本后，尝试使用自定义 ICA 文件启动应用程序可能会失败。
- 在运行 macOS Ventura 的 Mac 版 Citrix Workspace 应用程序上，网络摄像头重定向可能会失败。
- 如果启用了 shellbridge，您可能无法通过单击窗口上的 **X** 图标注销会话。

- 通过此修复，浮动通知可能会在无缝会话中正确显示。您必须启用 shellbridge 才能使此修复生效。但是，此修复存在以下视觉限制：
  - 浮动通知周围有黑色背景。
  - 浮动通知会覆盖部分本地任务栏区域。

#### 智能卡

- 当您使用智能卡启动会话并尝试解锁锁定的会话时，您可能会收到输入密码而不是智能卡 PIN 的提示。当您安装了 Microsoft 补丁 KB5018410 时，会出现此问题。
- 当您从 VDA 注销时，CtxSvcHost (CtxSmartCardSvc) 可能会意外退出。

#### 系统异常

- Citrix PDF 通用打印机驱动程序可能会因 acfpdfuamd64.dll 模块故障而意外退出。
- wfica32.exe 进程可能会意外退出。
- VDA 可能会在 Wdica.sys 上遇到致命异常并显示蓝屏。
- 在使用 Microsoft Teams 时，Citrix HDX HTML5 视频重定向服务 (WebSocketService.exe) 可能会意外退出。
- 将 VDA 从 2203 LTSR CU2 版本升级到 CU3 后，VDA 可能会在 picadm.sys 上遇到致命异常并显示蓝屏。

#### 用户体验

- 在 Microsoft Excel 中复制和粘贴大量数据时，wfshell.exe 进程可能会无响应。

#### 用户界面

- 在 Windows Server 2019 及更早版本上，VDA 可能无法将鼠标事件发送到端点，从而导致应用程序中出现图形或鼠标问题。

### Citrix 置备™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### Linux 虚拟投递代理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### 配置文件管理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### 会话录制

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

**StoreFront™**

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

# 累积更新 3 (CU3)

发布日期：June 1, 2023

## 关于此版本

Citrix Virtual Apps and Desktops™ 7 2203 LTSR 累积更新 3 (CU3) 修复了自 2203 LTSR CU2 发布以来报告的 60 多个问题。

2203 LTSR（一般信息）

2203 LTSR（功能和升级信息）

此版本中的新增功能

Citrix Virtual Apps and Desktops 7 2203 LTSR CU2 中修复的问题

此版本中的已知问题

弃用和删除

Citrix 产品订阅权益资格日期

## 下载

Citrix 虚拟应用和桌面 7 2203 LTSR CU3

## 新部署

### 如何从头开始部署 CU3?

您可以使用 CU3 元安装程序设置一个全新的基于 CU3 的 Citrix Virtual Apps and Desktops 环境。在此之前，我们建议您熟悉该产品：

在开始规划部署之前，请查阅 Citrix Virtual Apps and Desktops 7 2203 LTSR（初始版本） 部分，并密切关注 技术概述、安装和配置 和 安全性 部分。确保您的设置满足所有组件的 系统要求。

# 现有部署

### 我需要更新什么?

CU3 为 2203 LTSR 的 15 个 基线组件 提供了更新。请记住：Citrix 建议您将部署中的所有 LTSR 组件更新到 CU3。例如：如果 Citrix Provisioning 是您的 LTSR 部署的一部分，请将 Citrix Provisioning 组件更新到 CU3。如果 Citrix Provisioning 不是您部署的一部分，则无需安装或更新它。

## 2203 LTSR CU3 基线组件

| 2203 CU3 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
|---|---|---|
| 单会话 VDA | 2203.0.3000.3300 | 单会话 VDA |
| 多会话 VDA | 2203.0.3000.3300 | 多会话 VDA |
| 交付控制器 | 2203.0.3000.3300 | 交付控制器(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#delivery-controller) |
| 思杰工作室 | 7.33.3000.18 | Citrix 工作室 |
| 思杰监控台 | 7.33.3000.24 | Citrix 监控器 |
| Citrix 组策略管理 | 7.33.3000.10 | Citrix 组策略管理(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/policies/policies-processes.html) |
| Citrix 组策略客户端扩展 | 7.33.3000.17 | |
| 思杰 StoreFront | 2203.0.3000.14 | Citrix 店面 |
| Citrix 预配 | 2203.0.17 | Citrix 预配 |
| 通用打印服务器 | 2203.0.3000.9 | 通用打印服务器 |
| 会话录制 | 22.3.3000 | 会话录制 |
| Linux 虚拟投递代理 | 22.03.3000.6 | Linux 虚拟投递代理 |

| 2203 CU3 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 配置文件管理 | 22.3.3000.3 | 配置文件管理 |
| Citrix 联合身份验证服务 | 10.9.3000.10 | Citrix 联合身份验证服务 (FAS) |
| 浏览器内容重定向 | 15.32.3000.7 | 浏览器内容重定向 |
| Citrix 探测代理 2305 | 2305.1.0.0 | 下载 |

## 2203 LTSR CU3 兼容组件

以下组件（版本如下）与 LTSR 环境兼容。它们不符合 LTSR 权益（延长生命周期和仅修复累积更新）的条件。Citrix® 可能会要求您在 2203 环境中将这些组件升级到更高版本。

| 兼容组件和功能 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 应用程序分层 | 23.4.0 | Citrix 应用分层 |
| HDX RealTime 优化包 | 2.9.600 | HDX RealTime 优化包 |
| 许可证服务器 | 11.17.2.0 构建 42000 | 许可证服务器 |
| 用户个性化层 | 23.4.0 | 用户个性化层 |
| 会话录制 Web 播放器 | 22.3.3000.4 | 会话录制 Web 播放器 |
| 微软团队优化 | 15.32.3000.9 | 微软团队优化 |
| 工作区环境管理 | 22.12.0 | 工作区环境管理 |
| XenApp & XenDesktop 7.15 LTSR VDA (最新版本)* | 仅限最新累积更新 | 文档(/zh-cn/xenapp-and-xendesktop/7-15-ltsr.html) |

## 2203 LTSR CU3 值得注意的排除项

以下功能、组件和平台不符合 2203 生命周期里程碑和权益的条件。具体而言，累积更新和扩展生命周期权益被排除在外。对排除的功能和组件的更新可通过常规当前版本获得。

| 排除的组件和功能 |
| --- |
| AppDisks™ |

| 排除的组件和功能 |
| --- |
| AppDNA® |
| Citrix SCOM 管理包 |
| 帧鹰 |
| 个人 vDisk |
| StoreFront 思杰在线集成 |

| 排除的 WINDOWS 平台 * |
| --- |
| Windows 2008 32 位（适用于通用打印服务器） |

* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

## 新增功能

Citrix Virtual Apps and Desktops™ 7 2203 LTSR 累积更新 3 (CU3) 中提供以下新功能和增强功能：

### 从 Citrix VDA 会话到客户端端点的通配符重定向

从 CU3 版本开始，双向内容重定向在定义要重定向的 URL 时支持使用通配符。有关详细信息，请参阅从 Citrix VDA 到客户端的通配符重定向。

## 已修复的问题

自 Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU2 以来，已修复以下问题：

### 思杰监控台

- 会话建立后，Citrix Director 的“计算机详细信息”页面中计算机的显示名称会恢复为交付组名称。

### Citrix 策略

- 通过此修复，多个内存问题已得到修复。
- 策略设置值可能会显示为 **Kpbs** 而不是 **Kbps**。

### 交付控制器™

- 如果启用了站点聚合或具有特定代理策略的交付组，启动应用程序或桌面会创建新会话，而不是重新连接到现有会话。

- 在使用 HTTPS 端口 443 时，尝试创建 MCS 计算机目录可能会失败。
- 当保留内存小于配置内存时，尝试启动虚拟机可能会失败并显示此错误消息：

  **无效的内存设置：内存预留 (sched.mem.min) 应等于 memsize (94208)。虚拟机启动失败。无法打开 MemSched 模块。解析调度程序特定配置参数时出错。**

- Citrix Broker Service (Brokerservice.exe) 在与许可证服务器断开连接后可能会意外退出。
- 此修复改进了 Citrix Virtual Apps and Desktops 2203 LTSR 的整体性能。
- 通过此修复，在以下场景中 NT5DS 是默认的时间同步协议：

  a. 主映像未加入域 (NDJ) 且

  b. 在 MCS 预配期间，您选择虚拟机为 Active Directory (AD) 或混合 Azure Active Directory (HAAD)

- 通过此修复，您可以更改现有预配方案的网络设置，以便在新子网上创建新的虚拟机。使用 `Set-ProvScheme` 命令中的 `parameter -NetworkMapping` 更改网络设置。有关详细信息，请参阅 更改现有预配方案的网络设置。

### 联邦身份验证服务

- 您无法在 Windows 11 桌面上安装 VDA。您会收到以下错误：

  **Citrix 身份验证身份断言 VDA 插件安装失败，错误代码为 1603。**

### 授权

- 仅当允许使用强密码套件时，Citrix Studio（许可管理 PowerShell 管理单元）可能无法与许可服务器通信。

### 微软团队优化

- HTML5 视频重定向服务 (CtxHdxWebSocketService) 可能会意外退出。

### 元安装程序

- Delivery Controller 安装程序在 2203 LTSR 版本中缺少命令行选项 **/No_Pending_Reboot_Check**，该选项在 1912 版本中可用。
- 升级 VDA 时，注册表项设置 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\SetDisplayRequiredMode 可能会被删除。

- 尝试将 VDA 升级到 2203 LTSR CU2 版本可能会失败。

## 安全问题

- 此修复解决了安全问题。有关详细信息，请参阅知识中心文章 CTX559370。

## 通用打印服务器

### 服务器

- Citrix XTE 服务可能会在通用打印服务器上意外退出，导致打印作业停留在队列中。
- EMFPrint.exe 进程可能会在 Citrix Universal Print Server 2203 上意外退出。

## 适用于单会话操作系统的 VDA

### 安装、卸载、升级

- 尝试将 VDA 从 1912 LTSR CU3 版本升级到 2203 LTSR CU2 版本可能会失败。
- 此修复引入了一个命令行选项 **/no_pending_reboot_check**，该选项可在安装或升级核心组件时，防止检查计算机上是否存在来自以前 Windows 安装的待处理重新启动。
- 通过此修复，VUA 工具在执行升级时会比较主版本，从而支持 CU 版本升级。您现在可以执行 LTSR 升级，例如从 2203.0.0.x 升级到 2203.0.1000.x (CU1)。
- 启用“失败时启用还原”功能后，在 VDA 升级或安装期间可能无法创建还原点。

### 键盘

- 在已发布的应用程序中，当您将光标置于可编辑字段中时，虚拟键盘可能不会自动出现。

### 会话/连接

- 尝试从 Citrix Universal™ Print Server 在共享会话打印机上打印文档可能会失败。此问题在升级到 Citrix Virtual Apps and Desktops 1912 LTSR CU4 后发生。
- 通过用户会话重新连接到用户设备时，注册表 HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream 下的 Microsoft Teams 重定向密钥 **MSTeamsRedirSupport** 可能会丢失。此问题在 RDP 会话仍然存在时发生。
- 尝试重新连接到会话可能会失败。
- 当您从物理 VDA 的本地控制台接管当前连接的用户会话时，连接到物理 VDA 的所有或部分显示器可能仍处于省电模式。
- 当 Windows 系统没有 C 盘时，尝试安装 VDA 2203 版本可能会失败。
- 将 VDA 升级到 2203 版本后，Skype for Business 应用程序可能会在启动画面处无响应。

- 插入显示器时，无缝窗口可能会消失。
- 在双跳场景中，您可能会在第一次跳跃期间看到两个额外未使用的网络摄像头。
- 在运行 Microsoft Windows 10 版本 21H2 的 VDA 2203 版本上，Windows“开始”菜单可能会显示一个空框，而不是“**电源 > 断开连接**”选项。
- ICA® 服务可能无法在未加入域且非英语的 Windows 10 H2 VDA 上打开。
- 通过此修复，双向内容重定向支持在定义要重定向的 URL 时使用通配符。有关详细信息，请参阅 从 Citrix VDA 到客户端的通配符重定向。
- 尝试使用优化的 Microsoft Teams 共享某些自定义应用程序可能会失败。
- 启用 shellbridge 后，所有启动程序都在 HDX™ 已发布的应用程序会话中启动。注销应用程序可能会阻止正常注销。如果问题仍然存在，请在以下注册表中将值设置为 0：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix 虚拟桌面代理

  名称: Shellbridge

  类型：REG_DWORD

  值: 0

- 处于**开机**状态的池化计算机可能会自动关机并变为未注册状态。 [
- 将音频设备添加到用户会话时，除了 Skype for Business 的声音外，您无法听到任何设备的声音。将显示以下错误消息：

  **错误 - 没有更多可用设备插槽 - 添加设备失败。**

  当连接到端点的播放或录制设备超过八个时，会出现此问题。

### 系统异常

- CseEngine.exe 服务在 VDA 上消耗的内存可能高于预期。
- Citrix HDX RAVE Service (CtxSvcHost.exe) 可能会意外退出。
- 启动已发布的桌面时，打开**文件资源管理器**并单击**网络 > \Client** 下重定向的本地 C 盘，**文件资源管理器**可能会意外退出。
- 升级到 Citrix Virtual Apps and Desktops 2203 LTSR 或 2203 LTSR CU1 版本后，重新连接到 VDA 会话的尝试可能会间歇性失败。
- VDA 可能会在 tdica.sys 上遇到致命异常并显示蓝屏。尝试重新连接到会话时会出现此问题。
- 如果 USB 设备快速插入和移除，VDA 可能会遇到错误检查代码 **000000CA**。

- 当使用 **Key Storage Provider** 作为**加密**提供程序创建证书模板时，在 VDA 上启用 SSL 的尝试可能会失败。
- DllHost.exe 进程可能会意外退出，并显示以下错误消息：

  **COM 代理不再工作**

- 会话启动期间，VDA 可能会在 ControlUP 自定义虚拟通道初始化时遇到致命异常并显示蓝屏。
- HTML5 视频重定向服务 (CtxHdxWebSocketService) 可能会意外退出。
- Citrix 软件图形进程 (Ctxgfx.exe) 可能会在 VDA 上消耗过多的非分页内存，导致虚拟机无响应。
- 以最小化或全屏模式打开已发布的应用程序时，可能会出现黑屏。当您将 VDA 从 1912 LTSR 升级到 2203 LTSR CU1 或 CU2 版本时，会出现此问题。

### 用户体验

- 多次尝试从 Microsoft Access 应用程序复制内容可能会失败，因为应用程序中的粘贴按钮被禁用。
- 当您从 Citrix Gateway 登录且 **LDAP SSO Name Attribute** 设置为 **UserPrincipalName** 时，Citrix 水印可能会错误地显示登录名称。

## 适用于多会话操作系统的 VDA

### 安装、卸载、升级

- 借助此修复，VUA 工具在执行升级时会比较主版本，从而支持 CU 版本升级。您现在可以执行 LTSR 升级，例如从 2203.0.0.x 升级到 2203.0.1000.x (CU1)。

### 键盘

- 将光标置于可编辑字段中时，虚拟键盘可能不会在已发布的应用程序中自动出现。
- 当您打开应用程序的 2 个实例并将 **DisableToggler** 设置为五秒时，您可能需要等待大约 30 秒才能在第二个应用程序中键入内容。

### 打印

- 在 Mac 客户端上，注销并重新登录后，打印机的默认纸张大小可能无法保留。

### 会话/连接

- CseEngine.exe 服务在 VDA 上消耗的内存可能高于预期。
- 尝试从 Citrix Universal Print Server 在共享会话打印机上打印文档可能会失败。此问题在升级到 Citrix Virtual Apps and Desktops 1912 LTSR CU4 后发生。

- 当您以匿名用户身份从 VDA 启动应用程序时，可能会出现以下错误消息：

  **用户名或密码不正确。**

- 尝试安装 VDA 2203 版本可能会失败，如果 Windows 系统没有 C 盘。
- 启动已发布的桌面后，打开**文件资源管理器**并单击**网络 > \客户端**下的重定向本地 C 盘时，**文件资源管理器**可能会意外退出。
- 当证书模板以 **Key Storage Provider** 作为**加密**提供程序创建时，尝试在 VDA 上启用 SSL 可能会失败。
- Citrix Director 2203 版本可能会将已发布应用程序启动的交互式会话详细信息（例如 **Userinit** 和 **Shell**）显示在单行而不是单独的行上。
- 当您从一个无缝窗口悬停到另一个窗口时，拖放操作可能会失败。
- 尝试使用优化的 Microsoft Teams 共享某些自定义应用程序可能会失败。
- CtxRaveSvc.exe 服务可能会变得无响应，并且无法从远程桌面服务接收会话更改通知。
- VDAs 上的 WebSocketService.exe 进程可能会消耗比预期更高的内存。
- 当您以最小化或全屏模式打开已发布的应用程序时，可能会出现黑屏。当您将 VDA 从 1912 LTSR 升级到 2203 LTSR CU1 或 CU2 版本时，会出现此问题。
- 处于开启状态的池化计算机可能会自动关闭并变为未注册状态。 [

**系统异常**

- 会话可靠性功能会导致重新连接，在此期间 VDA 可能会遇到致命异常并显示蓝屏。
- Citrix HDX RAVE 服务 (CtxSvcHost.exe) 可能会意外退出。
- Microsoft Windows winlogon.exe 进程可能会意外退出，导致会话关闭。当您将 VDA 从 1912 LTSR CU4 版本升级到 2203 LTSR 时，由于 icagfxstack.dll 模块故障，会出现此问题。
- 终端服务进程可能会因为故障模块 RPM.dll 而意外退出。
- 如果 USB 设备快速插入和移除，VDA 可能会遇到错误检查代码 000000CA。
- DllHost.exe 进程可能会意外退出，并显示以下错误消息：

  **COM 代理已停止工作**

- 在安装了 UiPath Remote Runtime 组件的多会话操作系统 VDA 上，服务主机 (svchost.exe) 进程可能会消耗比预期更多的内存。
- 在会话启动期间，VDA 可能会在 ControlUP 自定义虚拟通道初始化时遇到致命异常并显示蓝屏。

- 启用浏览器内容重定向后，尝试播放 YouTube 视频时，WebSocketAgent.exe 服务可能会意外退出。
- HTML5 视频重定向服务 (CtxHdxWebSocketService) 可能会意外退出。
- Citrix 软件图形进程 (Ctxgfx.exe) 可能会在 VDA 上消耗过多的非分页内存，导致虚拟机无响应。

### 用户体验

- 从 Microsoft Access 应用程序复制内容的多次尝试可能会失败，因为应用程序中的粘贴按钮被禁用。
- 当您从 Citrix Gateway 登录且 **LDAP SSO 名称属性**设置为 **UserPrincipalName** 时，Citrix 水印可能会错误地显示登录名称。

### 虚拟桌面组件 – 其他

- 在使用双管理员模式时，尝试启动已发布的 App-V 应用程序可能会失败。
- 如果 App-V 缓存重定向到持久性驱动器，则在非持久性计算机上启动 App-V 应用程序可能会失败。

### Citrix 置备™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### Linux 虚拟投递代理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### 配置文件管理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### 会话录制

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### StoreFront™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

## 累积更新 2 (CU2)

发布日期: December 08, 2022

# 关于此版本

Citrix Virtual Apps and Desktops™ 7 2203 LTSR 累积更新 2 (CU2) 修复了自 2203 LTSR CU1 发布以来报告的 50 多个问题。

2203 LTSR（一般信息）

2203 LTSR（功能和升级信息）

此版本中的新增功能

Citrix Virtual Apps and Desktops 7 2203 LTSR CU1 中修复的问题

此版本中的已知问题

弃用和删除

Citrix 产品订阅优势资格日期

# 下载

思杰虚拟应用和桌面 7 2203 LTSR CU2

# 新部署

### 如何从头开始部署 CU2?

您可以使用 CU2 元安装程序设置基于 CU2 的全新 Citrix Virtual Apps and Desktops 环境。在此之前，我们建议您熟悉产品：

在开始规划部署之前，请仔细阅读 Citrix Virtual Apps and Desktops 7 2203 LTSR（初始版本） 部分，并特别注意 技术概述、安装和配置 和 安全性 部分。确保您的设置满足所有组件的 系统要求。

# 现有部署

### 我需要更新什么?

CU2 为 2203 LTSR 的 15 个 基线组件 提供了更新。请记住：Citrix 建议您将部署中的所有 LTSR 组件更新到 CU2。例如：如果 Citrix Provisioning 是您的 LTSR 部署的一部分，请将 Citrix Provisioning 组件更新到 CU2。如果 Citrix Provisioning 不是您部署的一部分，则无需安装或更新它。

# 2203 LTSR CU2 基线组件

| 2203 CU2 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
|---|---|---|
| 单会话 VDA | 2203.0.2000.2071 | 单会话 VDA |
| 多会话 VDA | 2203.0.2000.2071 | 多会话 VDA |
| 交付控制器 | 2203.0.2000.2071 | 交付控制器(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#delivery-controller) |
| 思杰工作室 | 7.33.2000.21 | Citrix 工作室 |
| 思杰监控台 | 7.33.2000.21 | Citrix 监控器 |
| Citrix 组策略管理 | 7.33.2000.12 | Citrix 组策略管理(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/policies/policies-processes.html) |
| Citrix 组策略客户端扩展 | 7.33.2000.11 | |
| 思杰 StoreFront | 2203.0.2000.5 | Citrix 店面 |
| Citrix 预配 | 2203.0.11 | Citrix 预配 |
| 通用打印服务器 | 2203.0.2000.2066 | 通用打印服务器 |
| 会话录制 | 22.3.2000 | 会话录制 |
| Linux 虚拟投递代理 | 22.03.2000.5 | Linux 虚拟投递代理 |
| 配置文件管理 | 22.3.2000.1 | 配置文件管理 |
| Citrix 联合身份验证服务 | 10.9.2000.9 | Citrix 联合身份验证服务 (FAS) |
| 浏览器内容重定向 | 15.32.2000.1 | 浏览器内容重定向 |
| Citrix 探测代理 2206 | 2209.1.0.0 | 下载 |

## 2203 LTSR CU2 兼容组件

以下组件（版本如下）与 LTSR 环境兼容。它们不符合 LTSR 权益（延长生命周期和仅修复累积更新）的条件。Citrix® 可能会要求您在 2203 环境中升级到这些组件的更高版本。

| 兼容组件和功能 | 在“程序和功能”中显示的 版本 | 文档 |
|---|---|---|
| 应用程序分层 | 2208.0.0 | Citrix 应用分层 |
| HDX RealTime 优化包 | 2.9.500 | HDX RealTime 优化包 |
| 许可证服务器 | 11.17.2.0 构建 40000 | 许可证服务器 |
| 用户个性化层 | 22.6.3 | 用户个性化层 |
| 会话录制 Web 播放器 | 22.3.2000.8 | 会话录制 Web 播放器 |
| 微软团队优化 | 15.32.1000.9 | 微软团队优化 |
| 工作区环境管理 | 2209 | 工作区环境管理 |
| XenApp & XenDesktop 7.15 LTSR VDA (最新版本)* | 仅限最新累积更新 | 文档(/zh-cn/xenapp-and-xendesktop/7-15-ltsr.html) |

## 2203 LTSR CU2 值得注意的排除项

以下功能、组件和平台不符合 2203 生命周期里程碑和权益的条件。具体而言，累积更新和扩展生命周期权益被排除在外。对已排除功能和组件的更新可通过常规当前版本获取。

| 排除的组件和功能 |
|---|
| AppDisks™ |
| AppDNA® |
| Citrix SCOM 管理包 |
| 帧鹰 |
| 个人 vDisk |
| StoreFront 思杰在线集成 |

| 排除的 WINDOWS 平台 * |
| --- |
| Windows 2008 32 位（适用于通用打印服务器） |

* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

# 新增功能

Citrix Virtual Apps and Desktops™ 7 2203 LTSR 累积更新 2 (CU2) 中没有新功能和增强功能。

# 已修复的问题

以下问题已在 Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU1 之后得到修复：

### Citrix 策略

- 当 CseEngine.exe 正在获取组策略对象 (GPO) 时，可能会生成不正确的 DNS 查询。

### 思杰工作室

- 尝试使用 Citrix Studio 控制台中的 **DBCreator**、**Securityadmin** 和 **Public permissions** 创建新的 Citrix Virtual Apps and Desktops 站点可能会失败。
- 此修复程序提供了在创建计算机目录时搜索域的功能。有关详细信息，请参阅 创建计算机目录 。
- 导航到 **交付组 > 电源管理** 后，尝试更新高峰时段栏可能会失败。

### 交付控制器™

- 如果某些域控制器已关闭，Citrix Studio 可能会显示计算机的安全标识符 (SID) 而不是帐户名称。

### 图形

- 某些应用程序的最大帧速率限制为每秒 22 帧 (FPS)，而不是默认最大值 30 FPS。

### 适用于单会话操作系统的 VDA

#### 会话/连接

- 可能会将两个 VDA 而不是一个分配给单个用户。
- 退出会话时，服务器可能会变得无响应。此问题是由于 icausbb.sys 中存在无限循环而发生的。
- 启动 Citrix 发布应用程序时，无缝模式可能无法生效，导致已发布的应用程序具有黑色背景。

- 尝试重新配置运行适用于 Windows 版本 2203 的 Citrix Workspace™ 应用程序的多会话操作系统 VDA 可能会失败。
- 当您将通用 Windows 平台 (UWP) 应用程序作为 VM 托管应用程序启动时，将显示“**应用程序未运行**”应用程序状态。
- 启用“**基于虚拟化的安全性**”功能后，当您通过用户设备使用远程电脑访问来访问工作站，然后断开连接时，当您实际到达工作站并登录系统时，可能会出现黑屏。
- 重新连接到已发布的应用程序后，可能会启动两个已发布的应用程序，并且 Delivery Controller 可能会将应用程序状态显示为“应用程序未运行”。
- 在会话重新连接期间，如果电源线已插入，电池状态指示器可能会消失。
- 浏览器内容重定向扩展可能无法与最新版本的 Chrome 配合使用，导致优化的 Microsoft Teams 呼叫断开连接。
- 使用最新版本的 Chrome 时，浏览器内容重定向扩展可能会失败，并导致优化的 Microsoft Teams 呼叫断开连接。

#### 系统异常

- 当使用带双显示器的 Ubuntu 18 客户端时，**ctxgfx** 进程可能会导致 Windows VDA 2112 版本上的 CPU 占用率过高。
- Citrix 音频重定向服务可能无法与 VDA 2203 版本配合使用。
- wfshell.exe 或 PicaVcHost.exe 进程可能会意外退出，并出现异常代码 0xc0000374。当您在“允许重定向到客户端的 URL”策略设置中设置长字符串时，会出现此问题。
- wfshell.exe 进程可能会由于错误的 CtxUiMon.dll 模块而意外退出。
- 如果安装了 Microsoft Azure 信息保护 (AIP) 并启用了 Citrix Hook，Microsoft 365 应用程序可能会意外退出。

#### 用户体验

- 在 Windows 11 计算机上安装 VDA 2203 版本时，右键单击“**开始**”菜单可能不起作用。

### 适用于多会话操作系统的 VDA

#### 会话/连接

- 退出会话时，服务器可能会无响应。此问题是由于 icausbb.sys 中存在无限循环而导致的。
- 尝试重新配置运行 Citrix Workspace app for Windows 2203 版本的会话多操作系统 VDA 可能会失败。
- 在“客户端打印机名称”下列出的“适用于以下 VDA 版本”策略仅显示 Virtual Delivery Agent 5.6 Feature Pack 1 作为可用版本。

- 借助此修复，可以使用新的用户设置来配置多会话 VDA 的会话、空闲和断开连接计时器。有关详细信息，请参阅 会话限制策略设置 文档。
- 通过启用了屏幕保护程序的 VDA 从无缝发布的应用程序重新连接的会话中可能会出现屏幕保护程序。
- 重新连接到已发布的应用程序时，可能会启动两个已发布的应用程序，并且 Delivery Controller 可能会将应用程序状态显示为“应用程序未运行”。
- 借助此修复，在将虚拟通道添加到允许列表时，可以在进程路径中使用通配符。有关详细信息，请参阅 虚拟通道安全性 文档。
- 在会话重新连接期间，如果电源线已插入，电池状态指示器可能会消失。
- 当 RPM 未按预期释放锁而阻止注销过程时，VDA 可能会变得无响应。
- 浏览器内容重定向扩展可能无法与最新版本的 Chrome 配合使用，导致优化的 Microsoft Teams 呼叫断开连接。
- 使用最新版本的 Chrome 时，浏览器内容重定向扩展可能会失败，并导致优化的 Microsoft Teams 呼叫断开连接。

#### 系统异常

- VDA 可能会在 tdica.sys 上遇到致命异常，并显示带有错误检查代码 0x0000007E 的蓝屏。
- VDA 可能会在 picavc.sys 或 picadm.sys 上遇到致命异常，并显示蓝屏。
- 当使用带双显示器的 Ubuntu 18 客户端时，**ctxgfx** 进程可能会导致 Windows VDA 2112 版本上的 CPU 使用率过高。
- 当虚拟通道断开连接时，wfshell.exe 进程可能会意外退出。
- wfshell.exe 或 PicaVcHost.exe 进程可能会意外退出，并出现异常代码 0xc0000374。当您在“允许重定向到客户端的 URL”策略设置中设置长字符串时，会出现此问题。
- wfshell.exe 进程可能会因 CtxUiMon.dll 模块故障而意外退出。
- 当您尝试连接到在多会话操作系统上运行版本 2203 的 VDA 时，logonui.exe 进程可能会无响应并显示黑屏或被终止。但是，事件日志可能会出现。
- 在多会话操作系统 VDA 上运行的终端服务可能会间歇性地注销并退出。

### Citrix 供应™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### Linux 虚拟投递代理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### 配置文件管理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### 会话录制

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### StoreFront™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

# 累积更新 1 (CU1)

发布日期: August 03, 2022

## 关于此版本

累积更新 1 于 August 24, 2022 重新发布为累积更新 1100。此次重新发布解决了问题 LCM-11719，该问题在某些情况下阻止了单会话 VDA 升级到 2203 累积更新 1。

Citrix Virtual Apps and Desktops™ 7 2203 LTSR 累积更新 1 (CU1) 修复了自 2203 LTSR 初始版本发布以来报告的 30 多个问题。

2203 LTSR（一般信息）

2203 LTSR（功能和升级信息）

此版本的新增功能

Citrix Virtual Apps and Desktops 7 2203 LTSR（初始版本）中修复的问题

此版本中的已知问题

弃用和移除

Citrix 产品订阅权益资格日期

## 下载

思杰虚拟应用和桌面 7 2203 LTSR CU1

# 新部署

### 如何从头开始部署 CU1?

您可以使用 CU1 元安装程序，基于 CU1 设置全新的 Citrix Virtual Apps and Desktops 环境。在此之前，我们建议您熟悉该产品：

在开始规划部署之前，请仔细阅读 Citrix Virtual Apps and Desktops 7 2203 LTSR（初始版本） 部分，并密切关注 技术概述、安装和配置 和 安全性 部分。确保您的设置满足所有组件的 系统要求。

# 现有部署

### 我需要更新什么?

CU1 为 2203 LTSR 的 15 个 基线组件 提供了更新。请记住：Citrix 建议您将部署中的所有 LTSR 组件更新到 CU1。例如：如果 Citrix Provisioning 是您的 LTSR 部署的一部分，请将 Citrix Provisioning 组件更新到 CU1。如果 Citrix Provisioning 不是您部署的一部分，则无需安装或更新它。

## 2203 LTSR CU1 基线组件

| 2203 CU1 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
|---|---|---|
| 单会话 VDA | 2203.0.1100.1178 | 单会话 VDA |
| 多会话 VDA | 2203.0.1100.1178 | 多会话 VDA |
| 交付控制器 | 2203.0.1100.1178 | 交付控制器(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#delivery-controller) |
| 思杰工作室 | 7.33.1100.27 | Citrix 工作室 |
| 思杰监控台 | 7.33.1100.40 | Citrix 监控器 |
| Citrix 组策略管理 | 7.33.1100.18 | Citrix 组策略管理(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/policies/policies-processes.html) |
| Citrix 组策略客户端扩展 | 7.33.1100.16 | |

| 2203 CU1 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 思杰 StoreFront | 2203.0.1000.10 | Citrix 店面 |
| Citrix 预配 | 7.33.5 | Citrix 预配 |
| 通用打印服务器 | 7.33.1100.18 | 通用打印服务器 |
| 会话录制 | 22.3.1100.1178 | 会话录制 |
| Linux 虚拟投递代理 | 22.03.1000.7 | Linux 虚拟投递代理 |
| 配置文件管理 | 22.3.1000.4 | 配置文件管理 |
| Citrix 联合身份验证服务 | 10.9.1100.18 | Citrix 联合身份验证服务 (FAS) |
| 浏览器内容重定向 | 15.32.1100.9 | 浏览器内容重定向 |
| Citrix 探测代理 2206 | 2206.1.0.0 | 下载 |

## 2203 LTSR CU1 兼容组件

以下组件（版本如下）与 LTSR 环境兼容。它们不符合 LTSR 权益（延长生命周期和仅修复累积更新）的条件。Citrix® 可能会要求您在 2203 环境中将这些组件升级到更新版本。

| 兼容组件和功能 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 应用程序分层 | 2206.0.0 | Citrix 应用分层 |
| HDX RealTime 优化包 | 2.9.400.2702 | HDX RealTime 优化包 |
| 许可证服务器 | 11.17.2.0 构建 39000 | 许可证服务器 |
| 用户个性化层 | 22.6.1 | 用户个性化层 |
| 会话录制 Web 播放器 | 22.3.1000.5 | 会话录制 Web 播放器 |
| 微软团队优化 | 15.32.1000.9 | 微软团队优化 |
| 工作区环境管理 | 2203.1.0.1 | 工作区环境管理 |

| 兼容组件和功能 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| XenApp & XenDesktop 7.15 LTSR VDA (最新版本)* | 仅限最新累积更新 | 文档(/zh-cn/xenapp-and-xendesktop/7-15-ltsr.html) |

## 2203 LTSR CU1 值得注意的排除项

以下功能、组件和平台不符合 2203 生命周期里程碑和权益的条件。具体而言，累积更新和扩展生命周期权益被排除在外。对被排除的功能和组件的更新可通过常规当前版本获得。

| 排除的组件和功能 |
| --- |
| AppDisks™ |
| AppDNA® |
| Citrix SCOM 管理包 |
| 帧鹰 |
| 个人 vDisk |
| StoreFront 思杰在线集成 |

| 排除的 WINDOWS 平台 * |
| --- |
| Windows 2008 32 位（适用于通用打印服务器） |

* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

## 已修复的问题

自 Citrix Virtual Apps and Desktops™ 7 2203 LTSR（初始版本）以来，已修复以下问题：

### 思杰监控台

- 卸载 VDA 后，Citrix Windows Management Instrumentation (WMI) 的命名空间可能仍然存在。
- Citrix Studio 和 Citrix Director 中的活动会话计数可能不匹配。

### Citrix 策略

- VDA 可能无法向 Delivery Controller™ 注册并保持未注册状态。

- 在 Citrix Studio 中用于分配策略的标签或交付组无法枚举超过 250 的限制。

### 思杰工作室

- Citrix Studio 中涉及计算机目录的操作（例如访问、创建、删除或枚举目录）可能很慢。如果使用 Nutanix 管理程序托管连接，则会出现此问题。

### 交付控制器

- 将 Citrix Virtual Apps and Desktops 升级到版本 1912 LTSR 可能不会更新 Citrix.AzureRmPlugin.dll.config 配置文件，并且与 Microsoft Azure Resource Manager 的连接可能会失败。
- 更新 Machine Creation Services™ 目录时，如果选择虚拟机，然后选择相关快照，可能会出现以下错误消息：

  **发生意外错误。请联系 Citrix 技术支持。**

- 在恢复与 System Center Virtual Machine Manager (SCVMM) 的连接后，尝试启动计算机可能会失败。
- 当您使用静态 IP 地址从主映像创建 VDA 2203 LTSR 版本计算机时，Machine Creation Services (MCS) 在映像准备期间可能不会启用 DHCP。

### 适用于单会话操作系统的 VDA

#### 键盘

- 使用适用于 Linux 的 Citrix Workspace™ 应用程序打开的会话中，键盘快捷方式 **Ctrl+Break** 可能无法正常工作。

#### 会话/连接

- 插入或拔出显示器时，无缝窗口的位置可能不正确。
- 使用 Microsoft Teams 中的屏幕共享功能共享某些第三方应用程序可能会失败。
- 当您尝试调整 Microsoft Teams 中共享应用程序的窗口大小时，指示应用程序正在共享的红色边框可能与应用程序的实际大小不匹配。
- 当您在 VDA 2112 版本上运行连接质量指示器时，可能会报告不正确的往返时间 (RTT) 和延迟值。

  此修复允许您在禁用 HDX 自适应缩放功能时使用旧版 NetScaler® L7 延迟测量。NetScaler L7 延迟和 VDA HDX 自适应缩放功能不能同时启用。

  要使此修复中的功能生效，您必须按如下方式在 VDA 注册表中禁用 HDX™ 自适应缩放功能：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd

名称: AdaptiveScalingEnabled

类型: DWORD

值: 0

- 在启用图形状态指示器策略的情况下调整 Desktop Viewer 窗口大小可能会失败，并可能短暂出现灰屏。灰屏有时可能会持续存在，直到您重新启动 VDA。
- 使用 Microsoft Teams 中的屏幕共享功能共享某些已发布的应用程序可能会失败。
- 在使用 Citrix HDX 优化版 Microsoft Teams 时，Citrix HDX HTML5 视频重定向服务 (WebSocketService.exe) 可能会导致会话泄漏。
- 当 Citrix WEM Agent 安装在没有配置信息的 VDA 计算机上时，VDA 升级可能会失败。
- 单会话 VDA 升级到 2203 累积更新 1 可能会失败，并出现以下错误消息：

  `IcaConfigConsole.exe failed with error code -4`

  作为一种解决方法，请在升级前在目标计算机上创建以下注册表项：

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

  有关详细信息，请参阅知识中心文章 CTX463588。

  注意：此问题已在累积更新 1100（累积更新 1 的重新发布版本）中解决。

**系统异常**

- wfshell.exe 进程可能会意外退出，导致从已发布的应用程序启动新应用程序失败。
- CTXCDF 中的错误可能导致 Windows Management Instrumentation Provider Service (WMIPRVSE.exe) 停止并生成事件日志中的事件 ID 5612。
- WebSocketService.exe 进程可能会意外退出，导致 Microsoft Teams 呼叫失败并显示以下错误消息：

  **仍在连接到远程设备。呼叫尚不可用。**

- PicaVcHost.exe 进程可能会遇到访问冲突并意外退出。

**用户体验**

- 用户设备和 VDA 上主按钮设置为 **“左”** 的左手鼠标可能无法按预期工作。

### 用户界面

- 在使用屏幕共享功能时向其他用户提供屏幕控制可能会导致不正确的中文翻译提示，显示 `<xxx>` **想要查看您的桌面而不是** `<xxx>` **想要控制您的桌面**。

## 适用于多会话操作系统的 VDA

### 会话/连接

- 已解决以下 HDX 发布应用程序问题：
  - Microsoft Office 密码提示可能不会出现。
  - **打印机和扫描仪** 等设备可能不会显示在 **设置** 菜单中。
  - 新创建的文件夹可能不会显示在 **文件资源管理器** 应用程序中。
  - **文件资源管理器** 菜单中的 **打开设置** 不起作用。
  - 在 Microsoft Word 或 Microsoft Excel 等应用程序中，当您使用 **保存** 或 **打开** 选项重命名、创建或删除文件夹时，窗口不会自动刷新。但是，您可以手动刷新窗口。
  - 在启动通用 Windows 平台 (UWP) 应用程序期间，应用程序会在 Citrix Workspace 应用程序的会话完成进度条消失后 8-13 秒显示在屏幕上。因此，用户可能会尝试多次启动。
  - 在 Windows 11 版本 22H2 上的 HDX 无缝会话中，如果打印对话框已打开，则打印窗口可能会部分显示。
  - **文件资源管理器** 的搜索栏不起作用。
  - 如果之前启动了非 UWP 应用程序，则无法成功启动通用 Windows 平台 (UWP) 应用程序。
  - 当 Microsoft Office 365 版本 16.0.7967 及更高版本的应用程序作为 Windows Server 2019 主机中的应用程序发布时，Office 许可证激活失败。

  要启用此修复，请执行以下步骤：
  - 添加以下注册表详细信息：

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent

    名称: Shellbridge

    类型：REG_DWORD

    值：1
  - 确保安装了以下操作系统更新：

    Windows 11：KB5014019

Windows 服务器 2022：KB5014021

视窗 10：KB5014023

Windows 服务器 2019：KB5014022

- 在 Citrix Virtual Apps and Desktops 1912 CU 上安装 VDA 期间，注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Session 上的 TermService 权限可能无法恢复，从而导致会话失败。
- 在 VDA 版本 2112 上运行连接质量指示器时，可能会报告不正确的往返时间 (RTT) 和延迟值。

  当 HDX 自适应缩放功能被禁用时，此修复允许您使用旧版 NetScaler L7 延迟测量。NetScaler L7 延迟和 VDA HDX 自适应缩放功能不能同时启用。

  要使此修复中的功能生效，您必须在 VDA 注册表中禁用 HDX 自适应缩放功能，如下所示：

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd

  名称: AdaptiveScalingEnabled

  类型: DWORD

  值: 0

- 在“**客户端打印机名称**”下列出的“**适用于以下 VDA 版本**”策略仅显示 Virtual Delivery Agent 5.6 Feature Pack 1 作为可用版本。
- 尝试重新连接到会话可能会失败，并且会话可能会从 Citrix Director 中消失。系统会启动新会话，而不是重新连接到现有会话。要启用此修复，请设置以下注册表项：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy

  名称: EnforceUserPolicyEvaluationSuccess

  类型：REG_DWORD

  值: 0

- 当 Citrix WEM Agent 安装在没有配置信息的 VDA 计算机上时，VDA 升级可能会失败。

**系统异常**

- wfshell.exe 进程可能会意外退出，导致从已发布的应用程序启动新应用程序失败。

- CTXCDF 中的错误可能导致 Windows Management Instrumentation Provider Service (WMIPRVSE.exe) 停止并生成事件日志中的事件 ID 5612。
- 当虚拟通道断开连接时，wfshell.exe 进程可能会意外退出。
- 关闭“**打开设置**”窗口时，文件资源管理器可能会意外退出。
- 在多会话操作系统 VDA 上，终端服务可能会间歇性退出。系统事件日志中会记录事件 ID 7011，并显示以下消息：

  **等待 TermService 服务事务响应时超时（30000 毫秒）。**

### 用户体验

- 用户设备和 VDA 上主按钮设置为“**左**”的左手鼠标可能无法按预期工作。

### 用户界面

- 在 Citrix 会话和本地端点之间拖放文件可能会失败，即使启用了**拖放**策略。出现 **CtxDnDSourceProxy** 弹出错误。

## 虚拟桌面组件 – 其他

- 如果 App-V 缓存重定向到持久性驱动器，则尝试在非持久性计算机上启动 App-V 应用程序可能会失败。

## Citrix 置备™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

## Linux 虚拟投递代理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

## 配置文件管理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

## 会话录制

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

## StoreFront™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

# 2203 LTSR（初始版本）

## 关于此版本

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

Citrix Virtual Apps and Desktops 1912 和 XenApp and XenDesktop 版本 7.15 也提供 LTSR。

此 Citrix Virtual Apps and Desktops 版本包括新版 Windows Virtual Delivery Agent (VDA) 以及多个核心组件的新版本。您可以：

- **安装或升级站点：** 使用此版本的 ISO 安装或升级核心组件和 VDA。安装或升级到最新版本可让您使用最新功能。
- **在现有站点中安装或升级 VDA：** 如果您已有部署，并且尚未准备好升级核心组件，您仍然可以通过安装（或升级到）新的 VDA 来使用一些最新的 HDX™ 功能。当您想在非生产环境中测试增强功能时，仅升级 VDA 会很有帮助。

将 VDA 升级到此版本（从版本 7.9 或更高版本）后，您无需更新计算机目录的功能级别。**7.9（或更高版本）**值仍是默认功能级别，并且适用于此版本。有关详细信息，请参阅VDA 版本和功能级别。

有关安装和升级说明：

- 如果您正在构建新站点，请按照安装和配置中的顺序进行操作。
- 如果您正在升级站点，请参阅升级部署。

## 2203 LTSR 初始版本基线组件

| 2203 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 单会话 VDA | 2203.0.0.33220 | 单会话 VDA |
| 多会话 VDA | 2203.0.0.33220 | 多会话 VDA |
| 交付控制器 | 2203.0.0.33220 | 交付控制器(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#delivery-controller) |
| 思杰工作室 | 7.33.0.70 | Citrix 工作室 |

| 2203 基线组件 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 思杰监控台 | 7.33.0.67 | Citrix 监控器 |
| Citrix 组策略管理 | 7.33.0.33 | Citrix 组策略管理(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/policies/policies-processes.html) |
| Citrix 组策略客户端扩展 | 7.33.0.22 | |
| 思杰 StoreFront | 2203.0.0.36 | Citrix 店面 |
| Citrix 预配 | 2203.0.0 | Citrix 预配 |
| 通用打印服务器 | 7.33.0.12 | 通用打印服务器 |
| 会话录制 | 22.3.0 | 会话录制 |
| Linux 虚拟投递代理 | 22.03.0.16 | Linux 虚拟投递代理 |
| 配置文件管理 | 22.3.0.7 | 配置文件管理 |
| Citrix 联合身份验证服务 | 10.9.0.23 | Citrix 联合身份验证服务 (FAS) |
| 浏览器内容重定向 | 15.32.0.17 | 浏览器内容重定向 |
| Citrix 探测代理 | 2103.1.0.0 | 下载 |

## 2203 LTSR 初始版本兼容组件

以下组件（版本见下）与 LTSR 环境兼容。它们不符合享受 LTSR 权益的条件（延长生命周期和仅修复累积更新）。Citrix 可能会要求您在 2203 环境中将这些组件升级到更新版本。

| 兼容组件和功能 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 应用程序分层 | 2202.0.0 | Citrix 应用分层 |
| HDX RealTime 优化包 | 2.9.400 | HDX RealTime 优化包 |
| 许可证服务器 | 11.17.2.0 构建 37000 | 许可证服务器 |

| 兼容组件和功能 | 在“程序和功能”中显示的 版本 | 文档 |
| --- | --- | --- |
| 用户个性化层 | 21.12.5.7 | 用户个性化层 |
| 会话录制 Web 播放器 | 22.3.0.24 | 会话录制 Web 播放器 |
| 微软团队优化 | 15.32 | 微软团队优化 |
| 工作区环境管理 | 2203.1.0.1 | 工作区环境管理 |
| XenApp & XenDesktop 7.15 LTSR VDA (最新版本)* | 仅限最新累积更新 | 文档(/zh-cn/xenapp-and-xendesktop/7-15-ltsr.html) |

## 2203 LTSR 首次发布值得注意的排除项

以下功能、组件和平台不符合 2203 生命周期里程碑和权益的条件。具体而言，累积更新和扩展生命周期权益被排除在外。对已排除功能和组件的更新可通过常规当前版本获得。

| 排除的组件和功能 |
| --- |
| AppDisks™ |
| AppDNA® |
| Citrix SCOM 管理包 |
| 帧鹰 |
| 个人 vDisk |
| StoreFront 思杰在线集成 |

| 排除的 WINDOWS 平台 * |
| --- |
| Windows 2008 32 位（适用于通用打印服务器） |

* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

## 新增功能

本文列出了 Citrix Virtual Apps and Desktops™ 7 2203 LTSR（初始版本）的新增功能和增强功能。更新按组件进行组织。

### 用于管理本地主机缓存 (LHC) 的 PowerShell 命令

您现在可以使用 PowerShell 命令在 Delivery Controller 上管理 LHC。有关详细信息，请参阅本地主机缓存 PowerShell 命令。

### 混合权利许可证

从 2203 LTSR 初始版本开始，以前不受支持的公共云主机连接现在可以使用新的 **混合权利许可证** 进行部署。因此，您现在可以将本地部署与云部署结合使用。支持的公共云主机连接包括：AWS、Azure 和 Google Cloud。如果您的部署具有公共云主机连接，则在没有混合权利许可证的情况下无法升级到当前版本。有关详细信息，请参阅以下内容：

- 通过混合权利进行过渡和升级 (TTU)
- 升级部署
- Citrix 预配
- 系统要求

### 虚拟投递代理 (VDA) 2203

Windows 单会话操作系统和多会话操作系统 VDA 的 2203 版本包含以下增强功能。这些项目是本文前面列出的任何 VDA 安装和升级项目的补充。

#### Windows 登录屏幕的键盘布局增强功能

2203 LTSR 初始版本解决了当无法进行单点登录时（例如，在使用服务连续性时进行基于连接租约的启动期间），VDA 提示的 Windows 登录屏幕上出现的键盘布局问题。在此版本之前，Windows 登录屏幕上使用的是 VDA 的键盘布局。

从 2203 LTSR 初始版本开始，当您登录到 VDA 上的虚拟会话时，现在可以使用本地客户端键盘布局输入凭据。

#### 自适应音频更新

自适应音频和 UDP 音频现在有了新的实现。有关详细信息，请参阅通过 UDP 实时传输的音频和音频 UDP 端口范围。

### 思杰监控台

#### 支持 TLS 1.3

Citrix Director 现在支持 TLS 版本 1.3。

## 思杰工作室

### 当前版本的主机支持更改

从 2203 LTSR 初始版本开始，产品的当前版本支持在以下公共云主机上运行 VDA（交付应用程序和桌面的计算机）：

- 亚马逊网络服务
- Google 云平台
- 微软 Azure 资源管理器

> **重要提示：**

> 如果您想在部署中添加公共云主机连接，则需要混合权利许可证。有关混合权利许可证的信息，请参阅通过混合权利进行过渡和升级 (TTU)。

> 有关支持的主机和虚拟化资源的完整列表，请参阅系统要求。

### 许可证有效性检查

Citrix Studio 现在会自动检查主机连接所用许可证的有效性。如果主机连接的许可证无效，则该连接将置于维护模式。因此，您无法执行某些操作，例如编辑连接和关闭维护模式。例如，在以下情况下许可证会变为无效：

- 许可证已过期。在这种情况下，请联系您的 Citrix 销售代表续订或购买新许可证。
- 许可证已从许可证服务器中删除。

## Citrix Provisioning™ 2203 LTSR 初始版本

Citrix Provisioning 2203 LTSR 初始版本包含新增功能和修复。

## Linux 虚拟投递代理 2203 LTSR 初始版本

Linux Virtual Delivery Agent 2203 LTSR 初始版本包含新增功能和修复。

## Profile Management 2203 LTSR 初始版本

Profile Management 2203 LTSR 初始版本包含新增功能和修复。

## Session Recording 2203 LTSR 初始版本

Session Recording 2203 LTSR 初始版本包含新功能，且不包含修复。

### StoreFront™ 2203 LTSR 初始版本

StoreFront 2203 LTSR 初始版本包含新功能和修复。

### 工作区环境管理™ 2203

Workspace Environment Management 2203 包含新功能和修复。

## 已修复的问题

自 Citrix Virtual Apps and Desktops™ 7 2112 以来，已修复以下问题：

### 微软团队优化

- 当打开超过 1000 个应用程序窗口时，应用程序共享枚举失败，并且共享托盘中未列出任何应用程序。

### 适用于单会话操作系统的 VDA

#### 键盘

- 在连接到运行版本 1912 LTSR CU3 的 Android 设备上，当您激活文本输入字段时，屏幕键盘可能不会自动出现。
- 当您启动用户会话时，通用客户端输入法编辑器 (IME) 可能不会自动设置。因此，键盘不会自动与端点同步。
- 此修复解决了适用于 HTML5、Mac 和 Linux 客户端的 Citrix Workspace™ 应用程序上的俄语键盘映射问题。

#### 打印

- 在已发布的桌面中启用客户端打印机重定向时，某些客户端打印机设置可能不会与 VDA 上的打印机设置同步。
- 会话打印机可能会在会话重新连接期间消失，导致无法通过远程桌面 (RDP) 访问 VDA。

#### 会话/连接

- 当您退出会话时，服务器可能会变得无响应。当您使用通用 USB 重定向时，会出现此问题。
- 在启用了本地 IME 的已发布的 Microsoft Outlook 应用程序上执行以下步骤，可能会导致在电子邮件窗口中输入随机字符串：
    - 打开电子邮件窗口。
    - 按 Esc 键显示 **Want to save your changes?** 对话框并输入一些随机文本。
    - 按 Esc 键关闭对话框。

- 启用 Citrix IME 后，某些第三方应用程序可能无响应，并且用户会话中的应用程序启动可能会失败。此问题是由于 CtxIme 模块故障引起的。

#### 系统异常

- VDA 可能会遇到致命异常，并显示带有错误检查代码 0x0000010D (WDF_VIOLATION) 的蓝屏。
- 当您将 VDA 升级到版本 2009 或更高版本时，事件日志中可能会出现 Kernelbase 崩溃错误 (KERNELBASE.dll)。此问题在使用 Google Chrome 和 Microsoft Edge 浏览器时发生。

#### 用户界面

- 在多显示器环境中，如果将主显示器设置为纵向模式，SAS 通知可能会旋转 90 度显示。

#### 用户体验

- 在用户设备和 VDA 上，将主按钮设置为“**左**”的左手鼠标可能无法按预期工作。

### 适用于多会话操作系统的 VDA

#### 键盘

- 在连接到运行版本 1912 LTSR CU3 的 Android 设备上，激活文本输入字段时，屏幕键盘可能不会自动出现。

#### 打印

- 在发布的桌面中启用客户端打印机重定向时，某些客户端打印机设置可能不会与 VDA 上的打印机设置同步。
- 会话打印机可能会在会话重新连接期间消失，导致无法通过远程桌面 (RDP) 访问 VDA。

#### 会话/连接

- 将 **HideStatusMessages** 的值设置为 1 以隐藏“正在启动”栏，可能会导致注册表项 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ 无法按预期工作。
- 某些第三方应用程序在无缝会话中可能会无响应。
- 退出会话时，服务器可能会无响应。此问题在使用通用 USB 重定向时发生。
- 启用 Citrix IME 时，某些第三方应用程序可能无响应，并且用户会话中的应用程序启动可能会失败。此问题是由于 CtxIme 模块故障引起的。
- 当许可证服务器上的许可证用尽且禁用了“**许可证突发模式**”功能时，可能会出现带有“**访问被拒绝**”错误消息的黑屏冻结。

- 当 EDT 作为传输协议时，用户设备可能会因网络不稳定而与 VDA 断开连接。网络恢复后，重新连接到 VDA 需要很长时间。
- 退出 Citrix 虚拟会话时，可能会出现以下一个或多个问题：
  - VDA 仍然列出已终止的会话和 logonui.exe 进程。logonui.exe 进程可以被强制终止。
  - 会话在 Citrix Studio 中显示为空白用户名。
  - 您可能无法启动更多会话。

#### 系统异常

- 当您将远程桌面连接 (mstsc.exe) 作为已发布的应用程序启动时，CredentialUIBroker.exe 进程可能会意外退出。
- Citrix Stack Control Service (SCService64.exe) 可能会意外退出。
- 当您将 VDA 升级到版本 2009 或更高版本时，事件日志中可能会出现 Kernelbase 崩溃错误 (KERNELBASE.dll)。此问题在使用 Google Chrome 和 Microsoft Edge 浏览器时发生。

### Citrix 供应™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### Linux 虚拟投递代理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### 配置文件管理

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### 会话录制

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

### StoreFront™

有关已修复问题的详细信息，请参阅其文档中的已修复问题文章。

# 已知问题

## 备注

- 本文 2203 初始版本、CU1、CU2、CU3 和 CU4 部分中描述的已知问题在 CU5 中仍然存在，除非它们包含在已修复问题的列表中。

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

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

## 2203 CU7 中的已知问题

- 如果您从 2203 LTSR CU7 升级到 2402 LTSR CU1 或 CU2（包括 2411 及更早版本），升级可能会失败。作为一种解决方法，您可以直接升级到更新的版本，例如 2402 LTSR CU3/CVAD 2503 或更高版本。
- 在部分升级的站点上创建新的 AWS/Azure 主机连接可能会失败。建议在完全升级的站点上创建新的主机连接。
- 在全屏模式下使用浏览器内容重定向并打开多个选项卡时，当一个选项卡被缓慢拖出时，您可能会看到浏览器视口弹出。一旦停止拖动，浏览器视口就会调整到浏览器屏幕。
- 使用 HTML5 视频重定向时，对于未自动播放的视频，即使视频控件可用，您也可能看不到它们。

## 2203 CU6 中的已知问题

- 此版本不支持 32 位 Firefox 浏览器使用 FIDO2。

## 2203 CU5 中的已知问题

- 如果您已安装 Citrix Workspace 应用程序版本 22.03.5000（该版本在 Citrix Virtual Apps and Desktops 2203 CU4 VDA 和 CU4 Update 1 中提供），并尝试升级到最新版本，则升级可能会因自动更新弹出窗口而失败。 在将 VDA 更新到 CU5 之前，请使用以下解决方法：

  a. 升级到 Citrix Workspace 应用程序版本 2203.1 LTSR CU6 或 Citrix Workspace 应用程序 2402 LTSR。

  b. 禁用自动更新。有关详细信息，请参阅使用组策略对象管理模板配置 Citrix Workspace 更新。

  c. 对于 Citrix Workspace™ 应用程序更新提示，选择**稍后提醒我**。

## 2203 CU4 中的已知问题

- 如果您将 Windows、IIS 和 Citrix Director 安装在 C:\ 盘以外的驱动器中，并将 Citrix Director 升级到 2203 LTSR CU4 版本，则 Citrix Director 图标可能会显示为空白。但是，您可以单击该图标以启动 Citrix Director。

  您可以使用以下解决方法来帮助正确显示图标。

1. 打开命令提示符并运行命令 echo **%systemdrive%**。
2. 复制命令的输出。
3. 右键单击 Citrix Director 图标 > 更多 > 打开文件位置。
4. 打开记事本，然后将图标从文件资源管理器拖动到记事本。
5. 在内容中，将“C:”替换为在步骤 2 中复制的输出并保存。
6. Citrix Director 图标现在将正确显示。

- 将 StoreFront™ 升级到 2203 LTSR CU4 版本时，尝试启动资源或应用程序枚举可能会失败。

  > **注意：**
  >
  > 此问题已在 2203 LTSR CU4 Update 1 中修复。

- VDA 可能会在 picadd.sys 上遇到致命异常，并显示带有错误检查代码 0x96 的蓝屏。

  > **注意：**
  >
  > 此问题已在 2203 LTSR CU4 Update 1 中修复。

## 2203 CU3 中的已知问题

- 某些音频设备在设备列表中可能显示不正确的名称。
- 如果无法访问 Internet，则尝试将 Citrix Workspace 应用程序与 VDA 安装一起安装可能会失败。作为一种解决方法，您必须跳过安装 Citrix Workspace 应用程序，或者在安装 VDA 之前安装 Microsoft WebView（这是 Citrix Workspace 应用程序的先决条件）。

## 2203 CU2 中的已知问题

- 如果无法访问 Internet，则尝试将 Citrix Workspace 应用程序与 VDA 安装一起安装可能会失败。作为一种解决方法，您必须跳过安装 Citrix Workspace 应用程序，或者在安装 VDA 之前安装 Microsoft WebView（这是 Citrix Workspace 应用程序的先决条件）。
- 尝试将 Session Recording 从 Citrix Virtual Apps and Desktops™ 2203 LTSR CU1 升级到 CU2 可能会失败。将显示以下错误消息：

  **无法完成安装。**

  **安装未完成，因为在初始化过程中出现问题。产品将运行，但性能可能会下降。**

- Profile Management 可能会在登录期间重置自定义的 Outlook OST 路径。

## 2203 CU1 中的已知问题

- 如果无法访问 Internet，则尝试在安装 VDA 的同时安装 Citrix Workspace 应用程序可能会失败。作为一种解决方法，您必须在安装 VDA 之前跳过安装 Citrix Workspace 应用程序或安装 Microsoft WebView（这是 Citrix Workspace 应用程序的先决条件）。
- VDA 可能会在 tdica.sys 上遇到致命异常，并显示带有错误检查代码 0x0000007E 的蓝屏。

## 2203 初始版本中的已知问题

### 常规

- 如果您启动应用程序栏，然后在适用于 Windows 的 Citrix Workspace 应用程序中打开“连接中心”菜单，则应用程序栏不会显示在其托管服务器下。
- 如果您使用适用于 Windows 的 Citrix Workspace 应用程序并以垂直位置启动应用程序栏，则该栏会覆盖“开始”菜单或系统时钟托盘。
- 安装 Skype for Business Web App 插件后，网络摄像头可能无法枚举，并且 Firefox 上的会议页面可能不会自动刷新。
- 当您从 StoreFront 启动应用程序时，应用程序可能不会在前台启动，或者应用程序在前台但可能没有焦点。作为一种解决方法，请单击任务栏中的图标将应用程序置于最前面，或在应用程序屏幕中单击以使其获得焦点。
- 使用 Windows 10 1809 LTSC 时，`VCLibs` 依赖项无法安装。
- 当用户选择主机上已获得焦点的组合框时，该组合框可能无法正确显示。作为一种变通方法，请选择另一个 UI 元素，然后选择该组合框。
- 您已启用本地应用程序访问。如果您启动 Windows 2012 R2 VDA 会话，断开连接并重新连接会话，然后启动本地应用程序并将其最大化，则 VDA 任务栏可能会截断该应用程序。

- 在 Azure 环境中，如果使用 ICA® 会话登录 VDA，并且为同一桌面启动无缝应用程序，则可能会看到大约五分钟的黑屏。
- Citrix Hypervisor™ 不支持带有 GFS2 SR 的 MCS 完全克隆 VM。
- 如果 Citrix Virtual Apps and Desktops 部署（其 VM 托管在 Citrix Hypervisor 8.2 上）在单个 MCS 目录中使用多个 GFS2 SR，则目录中的 VM 在部署期间无法访问 VDI。系统会报告错误“VDI is currently in use”。
- 当 Microsoft Office 365 版本 16.0.7967 及更高版本中的应用程序作为 Windows Server 2019 主机上的应用程序发布时，Office 许可证激活失败。Citrix 正在与 Microsoft 合作解决此 Microsoft 限制。支持的解决方法是安装 Windows Server 2016 VDA，这些 VDA 不包含行为异常的 Web 身份验证管理器组件。
- 当组策略评估失败时，会话管理器会终止会话启动。这是为了防止用户访问通过组策略限制的资源。以下用户实现的修复提供了一个注册表切换，供管理员解除强制执行，这有助于最终用户连接到会话，即使组策略评估失败也是如此：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy

  名称: EnforceUserPolicyEvaluationSuccess

  类型：REG_DWORD

  Value: 0 (启用当前修复)

- 在多会话操作系统 VDA 上运行的终端服务可能会间歇性退出。事件 ID 7011 会记录在系统事件日志中，并显示以下消息：

  **等待 TermService 服务事务响应时，发生超时（30000 毫秒）。**

- 当您在启用了八个以上 HDX 音频设备的客户端上连接到单会话 RemotePC 或工作站虚拟投递代理 (VDA) 时，您的高清体验 (HDX) 音频设备会禁用。作为一种解决方法，请选择以下选项之一：

  - 从启用了少于八个 HDX 音频设备的客户端连接到单会话 RemotePC 或工作站 VDA。
  - 在单会话 RemotePC 或工作站 VDA 启动后启用 HDX 音频设备。
  - 连接到多会话 RemotePC 或工作站 VDA。

- VDA 可能会在 tdica.sys 上遇到致命异常，并显示带有错误检查代码 0x0000007E 的蓝屏。
- 在某些情况下，当您使用客户端 IP 策略筛选器时，用于评估策略的 IP 地址不正确。

### 工作室

- 在站点创建期间，添加许可证以启用混合权利许可证后，公共云主机（例如 Microsoft Azure、Google Cloud Platform 和 Amazon Web Services）不会显示在连接类型列表中，直到站点创建完成。

### 导览器

- **Citrix Director > Machine Details** 上的 **Console** 链接无法在 Microsoft Edge 44 和 Firefox 68 ESR 浏览器中启动计算机控制台。

### 图形

- 共享最小化应用程序时，应用程序的标题栏也可能被共享。
- 将策略“**拖动时查看窗口内容**”设置为“**禁止**”在 ESXi 和 Hyper-V 上不起作用。
- 如果您使用 64 位网络摄像头应用程序通过 Theora 压缩启动视频预览，会话可能会崩溃。
- 某些应用程序的最大帧速率限制为 22 帧每秒 (FPS)，而不是默认的最大 30 FPS。修复程序将在 2203 LTSR CU2 中提供。作为一种解决方法，请在 VDA 上设置以下注册表值：
  - Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
  - 值： EnableTimerPeriod = 1

  要激活此设置，您必须断开连接并重新启动会话。

### 打印

- 在虚拟桌面上选择的通用打印服务器打印机不会显示在控制面板的“**设备和打印机**”窗口中。但是，当用户在应用程序中工作时，他们可以使用这些打印机。此问题仅在 Windows Server 2012、Windows 10 和 Windows 8 上发生。有关详细信息，请参阅 CTX213540。
- 默认打印机在打印对话框窗口中可能未正确标记。此问题不影响发送到默认打印机的打印作业。

### 机器创建服务™ (MCS)

- 在 GCP 环境中，当您更新预配方案的自定义属性时，更改不会应用于目录中新添加的计算机。要解决此问题，请在更新预配方案的自定义属性后，为目录创建新的更新映像。
- 当您创建具有自定义属性的目录，并使用 `Set-ProvScheme` 更改预配方案而未更新在目录创建期间设置的相同自定义属性时，`Set-ProvScheme` 中未提及的属性将设置为其默认值。此外，如果在目录创建期间将任何自定义属性设置为其非默认值，则在运行 `Set-ProvScheme` 后，它将被覆盖为其默认值。

### 第三方问题

- Chrome 仅支持网页周围的工具栏、选项卡、菜单和按钮的 UI 自动化。由于此 Chrome 问题，在触摸设备上的 Chrome 浏览器中，自动键盘显示功能可能无法工作。作为一种解决方法，运行 `chrome --force-renderer-accessibility` 或者您可以打开一个新的浏览器选项卡，键入 `chrome://accessibility`，并为特定或所有页面启用 **Native accessibility API** 支持。此外，当您发布无缝应用程序时，可以使用 `--force-renderer-accessibility` 开关发布 Chrome。
- 在浏览器内容重定向中，使用 YouTube HTML5 视频播放器启动 YouTube 视频后，全屏模式可能无法工作。您单击视频右下角的图标，视频不会调整大小，导致页面整个区域留下黑色背景。作为一种解决方法，请单击全屏按钮，然后选择剧场模式。

# 弃用和删除

本文中的公告旨在提前通知您即将淘汰的平台、Citrix 产品和功能，以便您能够及时做出业务决策。Citrix 会监控客户使用情况和反馈，以确定何时撤回这些产品和功能。公告可能会在后续版本中发生变化，并且可能不包括所有已弃用的功能。有关产品生命周期支持的详细信息，请参阅 Product Lifecycle Support Policy 文章。有关长期服务版本 (LTSR) 服务选项的信息，请参阅 < `<https://support.citrix.com/article/CTX205549>` >。

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

## 弃用

已弃用的项目不会立即删除。Citrix 将继续支持它们，但它们将在未来的版本中删除。

| 项目 | 弃用版本 | 删除版本 | 替代方案 |
| --- | --- | --- | --- |
| 基于文件的许可 | 2507 | --- | 许可证激活服务 (LAS) 是用于 Citrix 产品套件产品激活的下一代技术。使用基于文件的许可的客户需要在 April 15, 2026 之前升级到兼容版本并完成此技术过渡。在 April 15, 2026 之后，LAS 将是激活和许可 Citrix 本地组件的唯一方式。 |

| 项目 | 弃用版本 | 删除版本 | 替代方案 |
| --- | --- | --- | --- |
| 支持 WebRTC SDP 格式（方案 B） | 2308 | --- | 将 Citrix Workspace™ App 升级到受支持的版本。 |
| 支持 Microsoft Teams 优化中的单窗口模式 | 2308 | --- | 将 Citrix Workspace 应用程序升级到支持多窗口模式的版本。有关详细信息，请参阅功能矩阵和版本支持。 |
| 将 Citrix Provisioning 目标设备导入 Citrix Virtual Apps and Desktops™ 目录进行管理 | 1912 LTSR | - | 使用 Citrix Provisioning 导出设备向导。 |
| 主机到客户端 (URL) 重定向 | 2203 | --- | --- |
| 支持四个 AWS 特定命令：`Revoke-HypSecurityGroupIngress`、`Revoke-HypSecurityGroupEgress`、`Grant-HypSecuritygroupegress` 和 `Grant-HypSecurityGroupIngress`，用于云和本地环境。 | 2203 | | |
| VDA 元安装程序中的适用于 Windows 的 Citrix Files 和适用于 Outlook 的 Citrix Files。 | 2203 | | 使用独立安装程序。 |
| VDA 元安装程序中的 WEM 代理组件。 | 2203 | | |

| 项目 | 弃用版本 | 删除版本 | 替代方案 |
| --- | --- | --- | --- |
| 用于远程电脑访问的 SCCM 集成的局域网唤醒选项。 | 2012 | | 使用独立局域网唤醒功能。 |
| 适用于 XenApp 和 XenDesktop、Provisioning Services 以及 StoreFront 的 Citrix SCOM 管理包。有关可受监控的产品版本，请参阅Citrix SCOM 管理包文档。 | 1912 | | 使用 Director 监控和管理您的部署。有关 SCOM EOL 和替代方案的更多信息，请参阅 https://support.citrix.com/article/CTX266943。 |
| 移动性 SDK / 移动 SDK（来自前 Citrix Labs） | 7.16 | | 已被移动体验策略设置以及托管桌面/应用程序的本机体验取代。 |

## 移除

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

| 项目 | 宣布弃用的版本 | 移除的版本 | 替代方案 |
| --- | --- | --- | --- |
| Citrix 许可证管理控制台（最后包含在 Windows 许可证服务器 11.16.3 build 30000 中，并在 Windows 许可证服务器 v11.16.6 build 31000 中移除）。 | 2003 | 2006 | 使用 Citrix 许可管理器。 |
| 在 Windows 10 版本 1709 及更早版本上支持 Citrix 间接显示驱动程序 (IDD) 图形适配器。 | 2003 | 2003 | 使用 Citrix Virtual Apps and Desktops 7 1912 LTSR 虚拟投递代理。 |

| 项目 | 宣布弃用的版本 | 移除的版本 | 替代方案 |
| --- | --- | --- | --- |
| 使用 GRID 9 或更早版本显示驱动程序的 Nvidia GPU (NVENC) 硬件编码。 | 2003 | 2003 | 将 GRID 10 显示驱动程序与 Citrix Virtual Apps and Desktops 7 2003 或更高版本 VDA 结合使用，或使用 Citrix Virtual Apps and Desktops 7 1912 LTSR VDA。 |
| 自助密码重置 (SSPR) 功能。 | 2003 | 2006 | |
| 对适用于 VDA 和核心服务器组件的 Microsoft .NET Framework 4.8 之前版本的支持。包括 Delivery Controller、Studio、Director 和 StoreFront。 | 1912 | 2003 | 升级到 .NET Framework 4.8 版。 |
| Windows Server 2012 R2 上的虚拟投递代理。 | 1912 | 2003 | 在受支持的操作系统上安装 VDA。 |
| Citrix Virtual Apps and Desktops Premium edition 的 AppDNA® 应用程序迁移组件。 | 1909 | 2003 | |
| 在 32 位 (x86) 计算机上安装 Studio。 | 1909 | 2003 | 安装在受支持的 x64 操作系统上。 |
| 支持无缝应用程序中的 Excel 挂钩。此功能用于为每个 Microsoft Excel 2010 工作簿创建单独的任务栏图标。 | 1909 | 1909 | |

| 项目 | 宣布弃用的版本 | 移除的版本 | 替代方案 |
| --- | --- | --- | --- |
| Windows Server 2012 R2（包括 Service Pack）上的核心服务器组件。包括：Delivery Controller™、Studio 和 Director。 | 1906 | 2003 | 安装在较新的受支持操作系统上。 |
| 支持 Microsoft SQL Server 2008 R2、2012 和 2014 版本（包括所有 Service Pack 和版本）上的站点配置、配置日志记录和监视数据库。 | 1906 | 2003 | 在受支持的 Microsoft SQL Server 版本上安装数据库。 |
| 支持 x86 平台上的 Windows 10 VDA。 | 1906 | 1909* | 在受支持的 x64 操作系统上安装 VDA。*Citrix Virtual Apps and Desktops 7 1912 LTSR 仍支持此功能。 |
| 从 Citrix 虚拟应用和桌面 安装介质中移除 Citrix 智能工具代理。 | 1903 | 1906 | |
| 从 StoreFront 中删除以下已终止生命周期产品的 Delivery Controller 选项：VDI-in-a-Box 和 XenMobile（9.0 及更早版本）。 | 1903 | 1903 | |
| 支持 Red Hat Enterprise Linux/ CentOS 7.5 上的 Linux VDA。 | 1903 | 1903 | 在更高版本的 Red Hat Enterprise Linux 上安装 Linux VDA。 |

| 项目 | 宣布弃用的版本 | 移除的版本 | 替代方案 |
| --- | --- | --- | --- |
| StoreFront 支持 Citrix Virtual Apps and Desktops（以前称为 XenApp and XenDesktop）与 Citrix Receiver 和 Workspace Hub 之间的 TLS 1.0 和 TLS 1.1 协议。 | 7.17 | 2203 | 将 Citrix Receiver 升级到支持 TLS 1.2 协议的 Citrix Workspace 应用程序。有关 Citrix Workspace 应用程序的更多信息，请参阅 (/zh-cn/citrix-workspace-app)。 |
| StoreFront 支持用户访问桌面设备站点上的桌面 | 1811 | 1912 | 将 桌面锁定 用于非域加入用例。 |
| 支持 Framehawk 显示远程处理技术 | 1811 | 1903 | 启用 Thinwire 和 自适应传输。 |
| 支持所有 Citrix Virtual Apps and Desktops（以及 XenApp 和 XenDesktop）版本中的 Citrix Smart Scale。此功能将于 31 May 2019 终止支持。 | 1808 | 1906 | 考虑在 Citrix Cloud 上使用 Virtual Apps and Desktops Service 以改进电源管理功能。 |
| 思杰 StoreFront、思杰 VDA、思杰 Studio、思杰 Director 和 思杰 Delivery Controller 对 Microsoft .NET Framework 4.5.1、4.5.2、4.6、4.6.1、4.6.2 和 4.7 版本的支持。 | 7.18 | 1808 | 升级到 .NET Framework 4.7.1 或更高版本。（如果尚未安装，安装程序会自动安装 .NET Framework 4.7.1。） |
| 支持在 Red Hat Enterprise Linux 7.3 上运行 Linux VDA。 | 7.18 | 1808 | 在更高版本的 Red Hat Enterprise Linux 上安装 Linux VDA。 |

| 项目 | 宣布弃用的版本 | 移除的版本 | 替代方案 |
| --- | --- | --- | --- |
| VDA 支持策略设置“自动安装内置打印机驱动程序”。 | 7.16 | 7.16 | 无。此策略设置仅支持在早期操作系统（Windows 7、Windows Server 2012 R2 及更早版本）上的 VDA。 |
| 支持 SUSE Linux Enterprise Server 11 服务包 4 上的 Linux VDA。 | 7.16 | 7.16 | 在受支持的 SUSE 版本上安装 Linux VDA。 |
| VDA 支持 Citrix WDDM 驱动程序 | 7.16 | 7.16 | Citrix WDDM 驱动程序不再随 VDA 一起安装。 |
| Windows 10 版本 1511 (Threshold 2) 及更早的 Windows 单会话操作系统版本（包括 Windows 8.x 和 Windows 7）上的 VDA（请参阅 `<https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/>`）。 | 7.15 LTSR（和 7.12） | 7.16 | 在 Windows 10 最低版本 1607 (Redstone 1) 或更新的半年频道上安装单会话操作系统 VDA。如果使用 1607 LTSB，我们建议使用 7.15 VDA。请参阅 CTX224843。 |
| Windows Server 2008 R2 和 Windows Server 2012（包括服务包）上的 VDA | 7.15 LTSR（和 7.12） | 7.16 | 在受支持的操作系统上安装 VDA。 |
| 桌面合成重定向（以前称为 DirectX 命令远程处理）(DCR) | 7.15 LTSR | 7.16 | 使用 Thinwire。 |

| 项目 | 宣布弃用的版本 | 移除的版本 | 替代方案 |
| --- | --- | --- | --- |
| Citrix Receiver for Web 经典体验（“绿色气泡”用户界面） | 7.15 LTSR（和 StoreFront 3.12） | 1903 | Citrix Receiver for Web 统一体验。 |
| Windows Server 2012 和 Windows Server 2008 R2 上的核心组件（包括服务包）。包括：交付控制器、工作室、总监、店面、许可证服务器和通用打印服务器。 | 7.15 LTSR | 7.18 | 在受支持的操作系统上安装组件。 |
| Windows Server 2012 和 Windows Server 2008 R2（包括 Service Pack）上的自助密码重置 (SSPR) 功能 | 7.15 LTSR | 7.18 | 安装在较新的受支持操作系统上。 |
| Windows 7、Windows 8 和 Windows 8.1（包括服务包）上的 Studio | 7.15 LTSR | 7.18 | 在受支持的操作系统上安装 Studio。 |
| Flash 重定向 | 7.15 LTSR | 1912 | 将视频内容创建为 HTML5 视频。对托管内容使用 HTML5 视频重定向，对公共网站使用浏览器内容重定向。有关详细信息，请参阅 (/zh-cn/xenapp-and-xendesktop/7-15-ltsr/multimedia/flash-redirection.html) [Flash 重定向生命周期结束]说明。 |

| 项目 | 宣布弃用的版本 | 移除的版本 | 替代方案 |
| --- | --- | --- | --- |
| Citrix Online 集成 (Goto 产品) 与 StoreFront | 7.14 (和 StoreFront 3.11) | StoreFront 3.12 | |
| 在 VDA 安装期间创建并添加到 VDA 计算机上的本地管理员组的用户帐户 CtxAppVCOMAdmin 不再创建。底层“COM”机制也已删除。 | 7.14 | 7.14 | Windows 服务 CtxAppVService 执行相同的功能。它会自动安装和配置，无需用户交互。 |
| 通用打印服务器 UpsServer 组件在 Windows Server 2008 32 位上的支持 | 7.14 | 7.14 | 安装在较新的受支持操作系统上。 |
| StoreFront 和 Web 版 Receiver 在 Internet Explorer 8 环境中 | 7.13 | 7.13 | |
| VDA 命令行安装选项 /no_appv，以阻止安装 Citrix App-V 组件 | 7.13 | 7.13 | 使用命令行安装选项 /exclude "Citrix Personalization for App-V – VDA"。 |
| 完整产品安装程序不再在新安装中安装 Citrix.Common.Commands 管理单元，并在升级现有安装时自动将其删除。 | 7.13 | 7.13 | 由 Citrix.Common.Commands 管理单元提供的某些 PowerShell 命令仍在 XenApp 6.5 SDK 中可用。 |
| 由 *-CtxIcon cmdlet 提供的用于操作图标数据的部分功能。 | 7.13 | 7.13 | 现在由 Broker Service 中的 *-BrokerIcon cmdlet 提供。 |

| 项目 | 宣布弃用的版本 | 移除的版本 | 替代方案 |
| --- | --- | --- | --- |
| 旧版 Thinwire 模式 | 7.12 | 7.16 | 使用 Thinwire。如果您在 Windows Server 2008 R2 上使用旧版 Thinwire 模式，请迁移到 Windows Server 2012 R2 或 Windows Server 2016，并使用 Thinwire。 |
| 从 StoreFront 2.0、2.1、2.5 和 2.5.2 进行就地升级 | 7.13 | 7.16 | 从这些版本之一升级到更高受支持的版本，然后升级到 XenApp 和 XenDesktop 7.16。 |
| 从 XenDesktop 5.6 或 5.6 FP1 进行就地升级 | 7.12 | 7.16 | 将您的 XenDesktop 5.6 或 5.6 FP1 部署迁移到当前的 XenDesktop 版本。为此，请首先升级到 XenDesktop 7.6 LTSR（包含最新 CU），然后升级到最新的 Citrix Virtual Desktops（以前称为 XenDesktop）版本或 LTSR 版本。 |
| 在 32 位 (x86) 计算机上安装 Delivery Controller、Director、StoreFront 或 License Server。 | 7.12 | 7.16 | 安装在受支持的 x64 操作系统上。 |
| 连接租用 | 7.12 | 7.16 | 使用 本地主机缓存。 |
| 在 Windows XP 上使用的 XenDesktop 5.6。不支持在 | 7.12 | 7.16 | 在受支持的操作系统上安装 VDA。 |

| 项目 | 宣布弃用的版本 | 移除的版本 | 替代方案 |
| --- | --- | --- | --- |
| Windows XP 上安装 VDA。 | | | |
| 支持 CloudPlatform 连接 | 7.12 | 2003 | 使用其他受支持的管理程序或云服务。 |
| 支持 Azure 经典部署（也称为 Azure 服务管理）连接 | 7.12 | 2003 | 考虑在 Citrix Cloud 上使用 Virtual Apps and Desktops 服务。 |
| AppDisks 功能（以及支持该功能的 AppDNA 与 Studio 的集成） | 7.13 | 2003 | 使用 Citrix 应用程序分层。 |
| Personal vDisk 功能 | 7.15 | 2006† | 使用 Citrix App Layering 用户层 或 用户个性化层 技术。 |

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

# 系统要求

## 简介

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

在开始安装之前，请查看 准备安装。

除非另有说明，否则如果未在计算机上检测到所需版本，组件安装程序会自动部署软件必备项（例如 .NET 和 C++ 软件包）。Citrix® 安装介质也包含部分此类必备软件。

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

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

### 硬件要求

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

下表列出了核心组件的最低要求。

| 组件 | 最低要求 |
| --- | --- |
| 所有核心组件和 StoreFront™ 位于一台服务器上，仅用于评估，而非生产部署 | 5 GB RAM |
| 所有核心组件和 StoreFront 位于一台服务器上，用于测试部署或小型生产环境 | 12 GB RAM |
| Delivery Controller™（本地主机缓存需要更多磁盘空间） | 5 GB RAM，800 MB 硬盘 |
| 工作室 | 1 GB RAM，100 MB 硬盘 |

| 组件 | 最低要求 |
| --- | --- |
| 监控工具 | 2 GB RAM，200 MB 硬盘 |
| StoreFront | 2 GB RAM，有关磁盘建议，请参阅 StoreFront 文档 |
| 许可证服务器 | 8 GB RAM；有关磁盘建议，请参阅(/zh-cn/licensing.html) |

### 交付桌面和应用程序的 VM 大小调整

由于硬件产品复杂且动态的性质，并且每个部署都有独特的需求，因此无法提供具体的建议。通常，Citrix Virtual Apps™ VM 的大小调整基于硬件而非用户工作负载。RAM 是一个例外。对于消耗更多 RAM 的应用程序，您需要更多的 RAM。

有关详细信息：

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

## 微软 Visual C++

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

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

## 交付控制器

支持的操作系统：

- Windows 服务器 2022
- Windows Server 2019，Standard 和 Datacenter 版本，以及带有 Server Core 选项的版本
- Windows Server 2016，标准版和数据中心版，以及 Server Core 选项

要求：

- 如果尚未安装 Microsoft .NET Framework 4.8（或更高版本），则会自动安装。
- Windows PowerShell 版本 3.0、4.0 或 5.0。
- Microsoft Visual C++ 2015–2019 可再发行组件。
- 如果您从 Citrix Virtual Apps and Desktops 2407 版升级到 2411 版或更高版本，或者执行 2411 版或更高版本的新安装，请首先将许可证服务器更新到最新版本（11.2.17 build 53100 版或更高版本）。然后，升级 Delivery Controller。否则，UI 上将显示警告消息，并且命令行安装将失败。

## 数据库

站点配置、配置日志记录和监控数据库支持的 Microsoft SQL Server 版本：

- SQL Server 2019，快速版、标准版和企业版。
- SQL Server 2017，速成版、标准版和企业版。
  - 对于新安装：默认情况下，如果在安装 Controller 时未检测到现有受支持的 SQL Server 安装，则会安装带有累积更新 16 的 SQL Server Express 2017。
  - 对于升级，任何现有的 SQL Server Express 版本都不会升级。
- SQL Server 2016 SP2，速成版、标准版和企业版。

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

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

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

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

- 安装 Controller 时，会安装带有累积更新 20 的 Microsoft SQL Server Express LocalDB 2019，以用于本地主机缓存功能。（此安装独立于站点数据库的默认 SQL Server Express 安装。）
- 升级 Controller 时，现有的 Microsoft SQL Server Express LocalDB 版本不会自动升级。有关替换要求和过程，请参阅替换 SQL Server Express LocalDB。

**更多数据库信息：**

- 数据库
- CTX114501 列出了最新支持的数据库
- 数据库大小调整指南
- 本地主机缓存

## 思杰工作室

支持的操作系统：

- Windows 服务器 2022
- Windows Server 2019 标准版和数据中心版
- Windows Server 2016，标准版和数据中心版
- Windows 十一
- Windows 10（仅限 64 位）

要求：

- 如果尚未安装 Microsoft .NET Framework 4.8（或更高版本），则会自动安装。
- Microsoft Management Console 3.0（随所有受支持的操作系统提供）。
- Windows PowerShell 版本 3.0、4.0 或 5.0。

## 思杰监控台

支持的操作系统：

- Windows 服务器 2022
- Windows Server 2019，Standard 和 Datacenter 版本，以及带有 Server Core 选项
- Windows Server 2016，标准版和数据中心版，以及 Server Core 选项

要求：

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

Citrix 配置文件管理：

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

系统中心操作管理器 (SCOM) 集成要求：

- Windows 服务器 2012 R2
- 系统中心 2012 R2 操作管理器

查看 Director 支持的浏览器：

- Internet Explorer 11。Internet Explorer 不支持兼容模式。使用推荐的浏览器设置访问 Director。安装 Internet Explorer 时，请接受默认设置以使用推荐的安全和兼容性设置。如果您已安装浏览器但选择不使用推荐设置，请转至 **工具 > Internet 选项 > 高级 > 重置** 并按照说明操作。
- 微软 Edge。
- Firefox ESR（延长支持版本）。
- Chrome 浏览器.

建议用于查看 Director 的最佳屏幕分辨率为 1366 x 1024。

# 适用于单会话操作系统的虚拟投递代理 (VDA)

支持的操作系统：

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

要求：

- 如果尚未安装 Microsoft .NET Framework 4.8（或更高版本），则会自动安装。
- Microsoft Visual C++ 2015–2019 可再发行组件。

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

某些多媒体加速功能（例如 HDX MediaStream Windows Media 重定向）要求在安装 VDA 的计算机上安装 Microsoft Media Foundation。如果计算机未安装 Media Foundation，则多媒体加速功能将

不会安装且无法工作。安装 Citrix 软件后，请勿从计算机中删除 Media Foundation。否则，用户将无法登录到计算机。在大多数受支持的 Windows 单会话操作系统版本中，Media Foundation 支持已安装且无法删除。但是，N 版本不包含某些与媒体相关的技术；您可以从 Microsoft 或第三方获取该软件。有关详细信息，请参阅 准备安装。

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

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

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

## 适用于多会话操作系统的虚拟投递代理 (VDA)

支持的操作系统：

- Windows 11（仅支持 Citrix DaaS™）
- Windows 10（仅限 x64，且仅支持 Citrix DaaS），任何当前处于主流支持的版本。
- Windows Server 2022，标准版和数据中心版
- Windows Server 2019，标准版和数据中心版
- Windows Server 2016，标准版和数据中心版

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

- 如果尚未安装 Microsoft .NET Framework 4.8（或更高版本），则会自动安装。
- Microsoft Visual C++ 2015–2019 可再发行组件。

如果尚未安装和启用远程桌面服务角色服务，安装程序会自动安装并启用它们。

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

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

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

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

有关在不再受支持的 Windows 操作系统上安装 VDA 的信息，请参阅 早期操作系统。

# 主机/虚拟化资源

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

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

远程 PC 访问的局域网唤醒功能需要 Microsoft System Center Configuration Manager 至少 2012 版本。

支持的虚拟机管理程序：

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

  CTX131239 包含当前版本信息以及已知问题的链接。

  有关详细信息，请参阅 Citrix Hypervisor 虚拟化环境。
- **Microsoft System Center 虚拟机管理器**

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

  CTX131239 包含当前版本信息以及已知问题的链接。

  有关详细信息，请参阅 Microsoft System Center Virtual Machine Manager 虚拟化环境。
- **努坦尼克斯 阿克罗波利斯**

  CTX131239 包含当前版本信息以及已知问题的链接。

  有关详细信息，请参阅 Nutanix 虚拟化环境。
- **威睿 vSphere (vCenter + ESXi)**

  不支持 vSphere vCenter 链接模式操作。

  CTX131239 包含当前版本信息以及已知问题的链接。

  有关详细信息，请参阅 VMware 虚拟化环境。

支持的公共云主机：

- **亚马逊网络服务 (AWS)**

有关使用 AWS 预配虚拟机的详细信息，请参阅 Citrix DaaS 文档的 Amazon Web Services 虚拟化环境 部分。

- **谷歌云平台**

  有关使用 Google Cloud 预配虚拟机的详细信息，请参阅 Citrix DaaS 文档的 Google Cloud 环境 部分和 部署指南。

- **Microsoft Azure 资源管理器**

  有关使用 Microsoft Azure Resource Manager 预配虚拟机的详细信息，请参阅 Citrix DaaS 文档的 Microsoft Azure Resource Manager 虚拟化环境 部分。

将公共云主机连接添加到部署时，请考虑以下事项：

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

# Active Directory 功能级别

支持以下 Active Directory 林和域功能级别：

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

> **注意：**

> 在升级 Citrix Virtual Apps and Desktops 站点之前，请检查各项功能的要求，因为较新的功能和 VDA 可能需要特定的最低 Active Directory 功能级别。

# HDX

## 音频

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

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

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

## HDX 视窗媒体 传输

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

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

## HDX 3D 专业版

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

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

- GPU 直通可用于：
  - 思杰 XenServer 服务器®
  - 能多益 AHV
  - VMware vSphere 和 VMware ESX，在其中称为虚拟直接图形加速 (vDGA)
  - Windows Server 2016 中的 Microsoft Hyper-V，其中它被称为离散设备分配 (DDA)。
- vGPU 可用于：

- Citrix 虚拟机监控程序
- 能多益 AHV
- 威睿 vSphere

请参阅 `<https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html>`。

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

图形处理单元 (GPU)：

- 对于基于 CPU 的压缩（包括无损压缩），HDX 3D Pro 支持主机计算机上与所交付应用程序兼容的任何显示适配器。
- 对于使用 NVIDIA GRID API 的虚拟化图形加速，您可以将 HDX 3D Pro 与 GRID 10 驱动程序支持的所有 NVIDIA GRID GPU 配合使用（请参阅 NVIDIA GRID）。NVIDIA GRID 可提供高帧率，从而带来高度交互的用户体验。
- Intel Xeon 处理器 E3 系列数据中心图形平台支持虚拟化图形加速。有关详细信息，请参阅 `<https://www.citrix.com/intel>` 和 `<https://www.intel.com/content/www/us/en/servers/data-center-graphics.html>`。
- AMD FirePro S 系列服务器卡支持通过 AMD RapidFire 进行虚拟化图形加速。请参阅 AMD Virtualization Solution)。

用户设备：

- HDX 3D Pro 支持主机计算机上 GPU 支持的所有显示器分辨率。为在满足最低推荐用户设备和 GPU 规格的情况下获得最佳性能，Citrix 建议 LAN 连接的最大显示器分辨率为 1920 x 1200 像素，WAN 连接的最大显示器分辨率为 1280 x 1024 像素。
- Citrix 建议用户设备至少具有 1 GB RAM 和 1.6 GHz 或更高时钟速度的 CPU。使用默认的深度压缩编解码器（低带宽连接必需）需要更强大的 CPU，除非解码通过硬件完成。为获得最佳性能，Citrix 建议用户设备至少具有 2 GB RAM 和 3 GHz 或更高时钟速度的双核 CPU。
- 对于多显示器访问，Citrix 建议使用配备四核 CPU 的用户设备。
- 用户设备无需 GPU 即可访问通过 HDX 3D Pro 交付的桌面或应用程序。
- 必须安装 Citrix Workspace 应用程序。

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

# 通用打印服务器

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

UpsServer 组件支持以下系统：

- Windows 服务器 2022
- Windows Server 2019 服务器
- Windows Server 2016 服务器

要求：

- Microsoft Visual C++ 2015-2019 可再发行组件
- Microsoft .NET Framework 4.8（至少需要此版本）

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

独立的客户端和服务器组件包也可供下载。

有关详细信息，请参阅预配打印机。

# 其他

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

在此版本中使用 Citrix Provisioning（以前称为 Provisioning Services）时，版本 7.x 包含在 XenApp and XenDesktop 7.x 生命周期和 Citrix Virtual Apps and Desktops 生命周期中。有关版本兼容性的详细信息，请参阅 Product Matrix。

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

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

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

支持多个 NIC。

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

有关 Microsoft App-V 的支持版本，请参阅 App-V。

有关该功能支持的浏览器信息，请参阅本地应用程序访问。

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

此产品支持 PowerShell 版本 3 到 5。

# 技术概述

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

思杰虚拟应用和桌面允许：

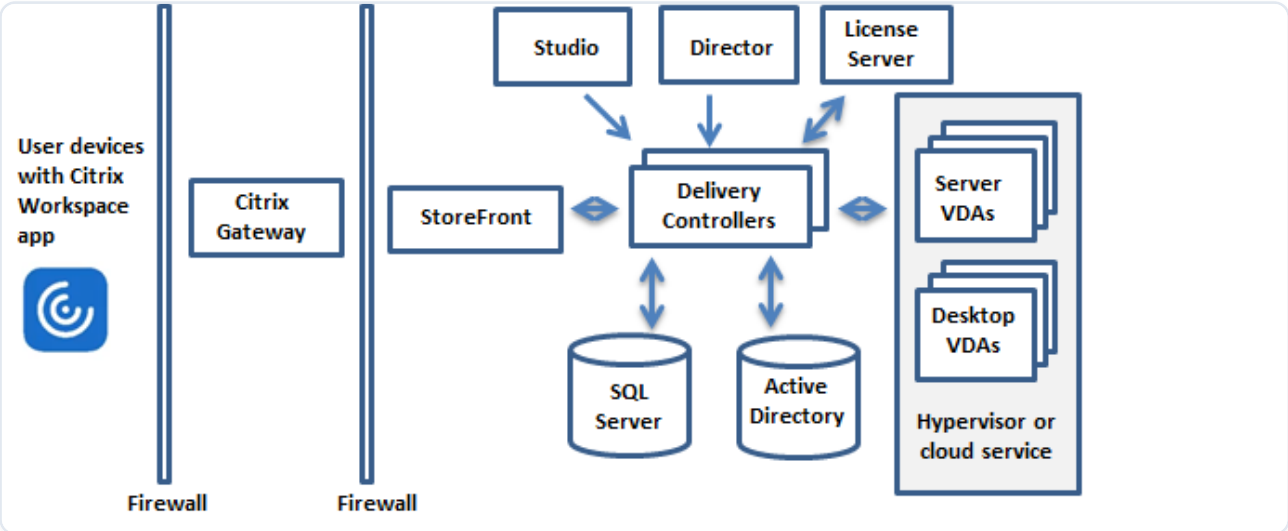
- 最终用户独立于设备的操作系统和界面运行应用程序和桌面。
- 管理员管理网络并控制来自选定设备或所有设备的访问。
- 管理员从单个数据中心管理整个网络。

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

## 关键组件

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

此图显示了典型部署（称为站点）中的关键组件。



## 交付控制器™

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

- 分发应用程序和桌面
- 验证和管理用户访问
- 在用户及其桌面和应用程序之间代理连接
- 优化用户连接
- 对这些连接进行负载平衡。

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

Monitor Service 收集历史数据并将其放入监控数据库中。此服务使用 TCP 端口 80 或 443。

来自 Controller 服务的数据存储在站点数据库中。

Controller 管理桌面的状态，根据需求和管理配置启动和停止桌面。在某些版本中，Controller 允许您安装 Profile Management 以管理虚拟化或物理 Windows 环境中的用户个性化设置。

## 数据库

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

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

## 虚拟投递代理 (VDA)

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

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

“VDA”一词通常用于指代代理及其安装的计算机。

VDA 适用于单会话和多会话 Windows 操作系统。适用于多会话 Windows 操作系统的 VDA 允许多个用户同时连接到服务器。适用于单会话 Windows 操作系统的 VDA 每次只允许一个用户连接到桌面。Linux VDA 也可用。

## 思杰店面™

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

## Citrix Workspace™ 应用程序

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

## 思杰工作室

Studio 是管理控制台，您可以在其中配置和管理 Citrix Virtual Apps and Desktops 部署。Studio 无需单独的管理控制台即可管理应用程序和桌面的交付。Studio 提供向导，指导您完成环境设置、创建用于托管应用程序和桌面的工作负载以及将应用程序和桌面分配给用户。您还可以使用 Studio 为您的站点分配和跟踪 Citrix 许可证。

Studio 从 Controller 中的 Broker 服务获取其显示的信息，通过 TCP 端口 80 进行通信。

## 思杰监控台

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

Director 显示：

- 来自 Controller 中 Broker 服务的实时会话数据，其中包括 Broker 服务从 VDA 中的 broker 代理获取的数据。
- 来自 Controller 中 Monitor 服务的历史站点数据。

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

您还可以通过 Director 使用 Windows 远程协助查看和与用户会话交互。

### Citrix 许可证服务器

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

### 管理程序或其他服务

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

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

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

## 附加组件

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

### Citrix 置备™

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

### 思杰网关

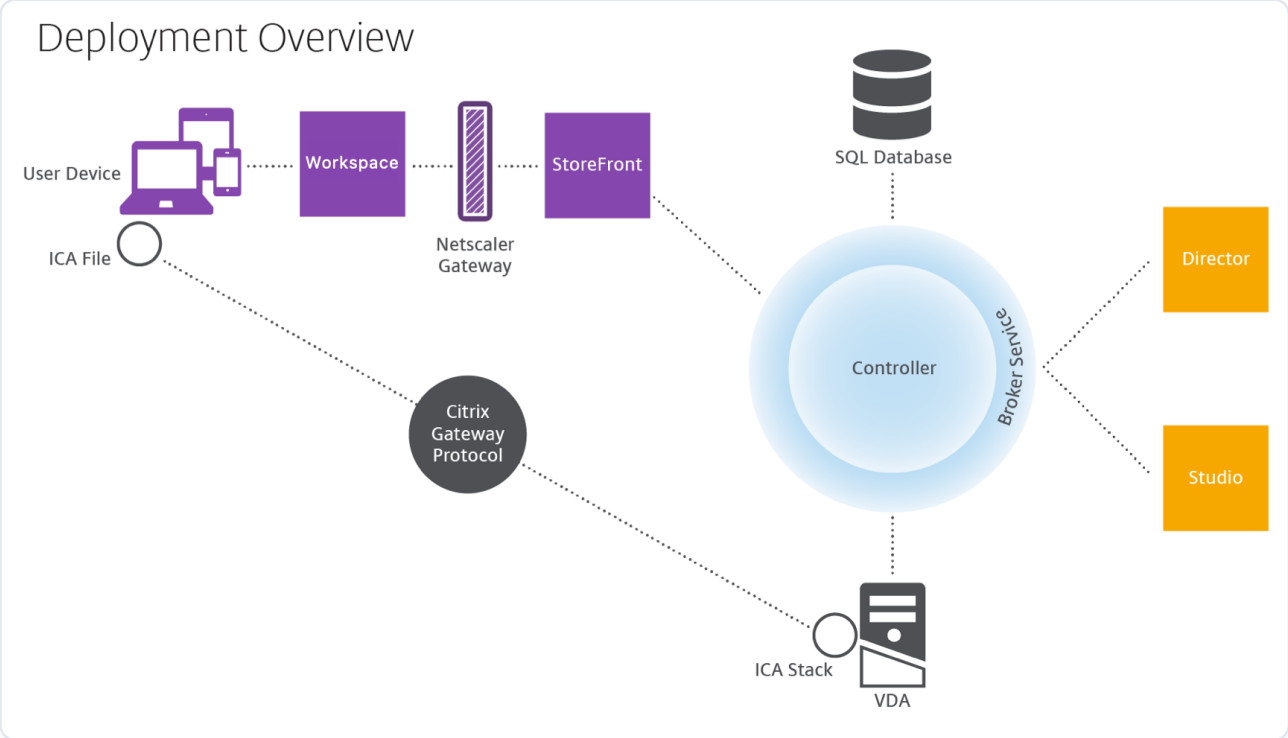
当用户从公司防火墙外部连接时，Citrix Virtual Apps and Desktops 可以使用 Citrix Gateway（以前称为 Access Gateway 和 NetScaler® Gateway）技术通过 TLS 保护这些连接。Citrix Gateway 或 VPX 虚拟设备是部署在非军事区 (DMZ) 中的 SSL VPN 设备。它通过公司防火墙提供单一安全访问点。

### 思杰 SD-WAN™

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

## 典型部署的工作原理

站点由具有专用角色的计算机组成，这些角色支持可扩展性、高可用性和故障转移，并提供按设计安全的解决方案。站点由安装了 VDA 的服务器和桌面计算机以及管理访问的 Delivery Controller 组成。




VDA 使用户能够连接到桌面和应用程序。对于大多数交付方法，它安装在数据中心的虚拟机上，但也可以安装在物理 PC 上以实现远程电脑访问。

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

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

# 用户连接的处理方式

要启动会话，用户可以通过安装在用户设备上的 Citrix Workspace 应用程序或 StoreFront 网站进行连接。

用户选择所需的物理或虚拟桌面或虚拟应用程序。

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

用户连接流程(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/user-connections.png)

Broker Service 确定用户被允许访问哪些桌面和应用程序。

凭据验证后，有关可用应用程序或桌面的信息通过 StoreFront-Citrix Workspace 应用程序路径发送回用户。当用户从此列表中选择应用程序或桌面时，该信息会沿路径返回到 Controller。然后，Controller 确定适当的 VDA 来托管特定的应用程序或桌面。

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

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

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

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

# 数据访问的工作原理

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

部署中的数据访问(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/data-access.png)

在 Controller 中，Broker Service 报告机器上每个会话的会话数据，提供实时数据。Monitor Service 也跟踪实时数据并将其作为历史数据存储在监控数据库中。

Studio 仅与 Broker Service 通信。它只访问实时数据。Director 通过 Broker Agent 中的插件与 Broker Service 通信，以访问站点数据库。

Director 还可以访问 Citrix Gateway 以获取 HDX 数据信息。

# 交付桌面和应用程序

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

## 计算机目录

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

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

有效的计算机类型包括：

- **多会话操作系统：** 具有多会话操作系统的虚拟或物理计算机。用于交付 Citrix Virtual Apps 发布应用程序（也称为基于服务器的托管应用程序）和 Citrix Virtual Apps 发布桌面（也称为服务器托管桌面）。这些计算机允许多个用户同时连接。
- **单会话操作系统：** 具有单会话操作系统的虚拟或物理计算机。用于交付 VDI 桌面（运行单会话操作系统且可选择进行个性化的桌面）、VM 托管应用程序（来自单会话操作系统的应用程序）和托管物理桌面。每次只能有一个用户连接到这些桌面中的每一个。
- **远程电脑访问：** 允许远程用户从运行 Citrix Workspace 应用程序的任何设备访问其物理办公电脑。办公电脑通过 Citrix Virtual Desktops 部署进行管理，并且要求在允许列表中指定用户设备。

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

## 交付组

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

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

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

有关详细信息，请参阅创建交付组。

## 应用程序组

应用程序组比使用更多交付组提供应用程序管理和资源控制优势。使用标签限制功能，您可以将现有计算机用于多个发布任务，从而节省与部署和管理更多计算机相关的成本。标签限制可以被认为是细分（或分区）交付组中的计算机。应用程序组在隔离和排查交付组中部分计算机的问题时也很有用。

有关详细信息，请参阅 创建应用程序组。

# 更多信息

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

# 活动目录

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

系统要求 文章列出了林和域支持的功能级别。要使用策略建模，域控制器必须运行 Windows Server 2003 到 Windows Server 2012 R2。这不影响域功能级别。

本产品支持：

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

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

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

## 在多 Active Directory 林环境中部署

此信息适用于最低版本 XenDesktop 7.1 和 XenApp 7.5。它不适用于早期版本的 XenDesktop 或 XenApp。

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

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

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

> **注意：**

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

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

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

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

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

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

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

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

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

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

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

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

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

如果存在外部信任，请在 VDA 上进行以下更改：

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

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

下表列出了支持的信任类型：

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

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

# 数据库

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

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

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

Citrix 建议您定期备份数据库，以便在数据库服务器发生故障时可以从备份进行恢复。每个数据库的备份策略可能有所不同。有关说明，请参阅 CTX135207。

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

## 高可用性

有几种高可用性解决方案可供考虑，以确保自动故障转移：

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

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

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

不支持在 SQL 群集或 SQL 镜像安装中的节点上安装控制器。

## 安装数据库软件

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

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

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

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

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

使用 Windows Update 使 SQL Server 保持最新。

## 通过站点创建向导设置数据库

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

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

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

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

1. 在两台服务器 A 和 B 上安装 SQL Server 软件。
2. 在服务器 A 上，创建打算用作主数据库的数据库。备份服务器 A 上的数据库，然后将其复制到服务器 B。
3. 在服务器 B 上，还原备份文件。
4. 在服务器 A 上启动镜像。

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

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

### 自动设置

如果您具有所需的数据库权限，请在站点创建向导的“**数据库**”页面上选择**从 Studio 创建和设置数据库**。然后提供主数据库的名称和地址。

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

### 脚本化设置

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

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

   - *名称中包含“SysAdmin”的脚本*。一个创建数据库和 Delivery Controller 登录的脚本。这些任务需要 securityadmin 权限。
   - *名称中包含“DbOwner”的脚本*。一个在数据库中创建用户角色、添加登录名，然后创建数据库架构的脚本。这些任务需要 `db_owner` 权限。
   - *名称中包含“Mixed”的脚本*。一个脚本中的所有任务，无论所需权限如何。

   您可以指明脚本的存储位置。

   > **注意：**

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

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

数据库管理员随后创建数据库。每个数据库必须具有以下特征：

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

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

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

有关 SQLCMD 详细信息，请参阅 Microsoft 文档。

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

Studio 会提示您继续站点创建。您将返回到“**数据库**”页面。输入地址。如果无法联系到任何托管数据库的服务器，则会出现错误消息。

## 设置数据库所需的权限

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

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

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

** 当通过 Studio 或使用 Studio 或 SDK 生成的脚本从站点中删除控制器时，不会删除控制器对数据库服务器的登录。这是为了避免可能删除同一台计算机上除此 Citrix 产品之外的其他服务正在使用的登录。如果不再需要，必须手动删除登录。此操作需要 `securityadmin` 服务器角色成员身份。

使用 Studio 执行这些操作时，Studio 用户必须拥有一个明确属于相应服务器角色的数据库服务器帐户，或者能够提供属于此类帐户的凭据。

### 首选数据库权限脚本

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

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

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

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

有关详细信息，请参阅 cmdlet 帮助。

## 数据库地址格式

您可以使用以下任一形式指定数据库地址：

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

对于 AlwaysOn 可用性组，请在位置字段中指定该组的侦听器。

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

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

## 更改数据库位置

创建站点后，您可以更改配置日志记录和监视数据库的位置。（您无法更改站点数据库的位置。）更改数据库位置时：

- 以前数据库中的数据不会导入到新数据库中。
- 检索日志时，无法从两个数据库聚合日志。
- 新数据库中的第一个日志条目指示发生了数据库更改，但它未标识以前的数据库。

启用强制日志记录时，无法更改配置日志记录数据库的位置。

要更改数据库的位置，请执行以下操作：

1. 确保在您希望数据库驻留的服务器上安装了受支持的 Microsoft SQL Server 版本。根据需要设置高可用性功能。
2. 在 Studio 导航窗格中选择“**配置**”。
3. 选择要为其指定新位置的数据库，然后在“**操作**”窗格中选择“**更改数据库**”。

4. 指定新位置和数据库名称。
5. 如果您希望 Studio 创建数据库并且您具有相应的权限，请单击“**确定**”。出现提示时，单击“**确定**”，然后 Studio 会自动创建数据库。Studio 会尝试使用您的凭据访问数据库。如果失败，系统会提示您输入数据库用户的凭据。然后 Studio 会将数据库架构上载到数据库。凭据仅在数据库创建期间保留。
6. 如果您不希望 Studio 创建数据库，或者您没有足够的权限，请单击“**生成脚本**”。生成的脚本包含手动创建数据库和（如果需要）镜像数据库的说明。在上载架构之前，请确保数据库为空，并且至少有一个用户具有访问和更改数据库的权限。

### 更多信息

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

## 交付方法

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

### 简介

选择合适的应用程序交付方法有助于提高可扩展性、管理效率和用户体验。

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

对于桌面，请考虑已发布的桌面或 VDI 桌面。

## Citrix Virtual Apps™ 已发布的应用程序和桌面

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

**用例：**

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

**优点和注意事项：**

- 数据中心内可管理且可扩展的解决方案。
- 最具成本效益的应用程序交付解决方案。
- 托管应用程序集中管理，用户无法修改应用程序。这提供了始终如一、安全可靠的用户体验。
- 用户必须在线才能访问其应用程序。

**用户体验：**

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

**处理、托管和交付应用程序：**

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

**会话管理和分配：**

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

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

## VM 托管应用程序

使用单会话操作系统计算机交付 VM 托管应用程序

**用例：**

- 您需要一个安全、提供集中管理并支持每台主机服务器多个用户的基于客户端的应用程序交付解决方案。您希望为这些用户提供以高清无缝显示的应用程序。
- 您的用户包括内部员工、外部承包商、第三方协作者以及其他临时团队成员。您的用户不需要离线访问托管应用程序。
- 应用程序类型：可能与其他应用程序不兼容或可能与操作系统交互的应用程序，例如 Microsoft .NET Framework。这些类型的应用程序非常适合在虚拟机上托管。

**优点和注意事项：**

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

**用户体验：**

- 与在多会话操作系统计算机上托管共享应用程序相同的无缝应用程序体验。

**处理、托管和交付应用程序：**

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

**会话管理和分配：**

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

## VDI 桌面

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

VDI 桌面托管在虚拟机上，并为每个用户提供桌面操作系统。

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

为 VDI 桌面创建计算机目录时，您可以创建以下类型的桌面之一：

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

## 远程电脑访问

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

远程电脑访问使用与交付虚拟桌面和应用程序相同的 Citrix Virtual Apps and Desktops 组件。因此，部署和配置远程电脑访问的要求和过程与部署 Citrix Virtual Apps and Desktops 以交付虚拟资源的要

求和过程相同。这种一致性提供了统一的管理体验。用户通过使用 Citrix HDX™ 交付其办公电脑会话来获得最佳用户体验。

有关更多信息，请参阅Remote PC Access。

# 网络端口

完整的网络端口信息在 Citrix 技术使用的通信端口 中提供。

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

您可能需要端口信息：

- 用于法规遵从。
- 如果 Citrix Virtual Apps and Desktops™ 组件与其他 Citrix 产品或组件之间存在网络防火墙，以便您可以适当地配置该防火墙。
- 如果您使用第三方宿主防火墙（例如防恶意软件软件包随附的防火墙），而不是操作系统的宿主防火墙。
- 如果您更改这些组件上的宿主防火墙配置（通常是 Windows 防火墙服务）。
- 如果您重新配置组件功能以使用不同的端口或端口范围，然后想要禁用或阻止配置中未使用的端口。

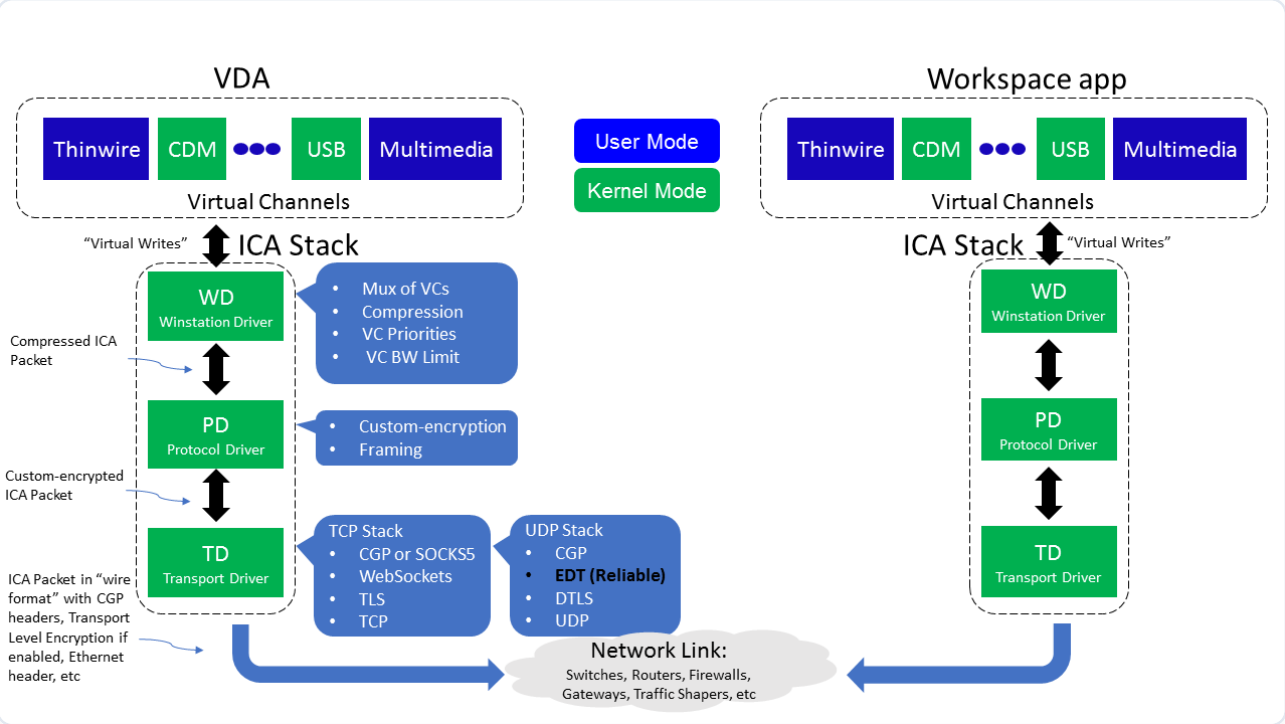
某些端口已在 Internet Assigned Numbers Authority (IANA) 注册。有关这些分配的详细信息可在 `<http://www.iana.org/assignments/port-numbers>` 处获取。但是，IANA 持有的描述性信息并不总是反映当今的使用情况。

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

## HDX™

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

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

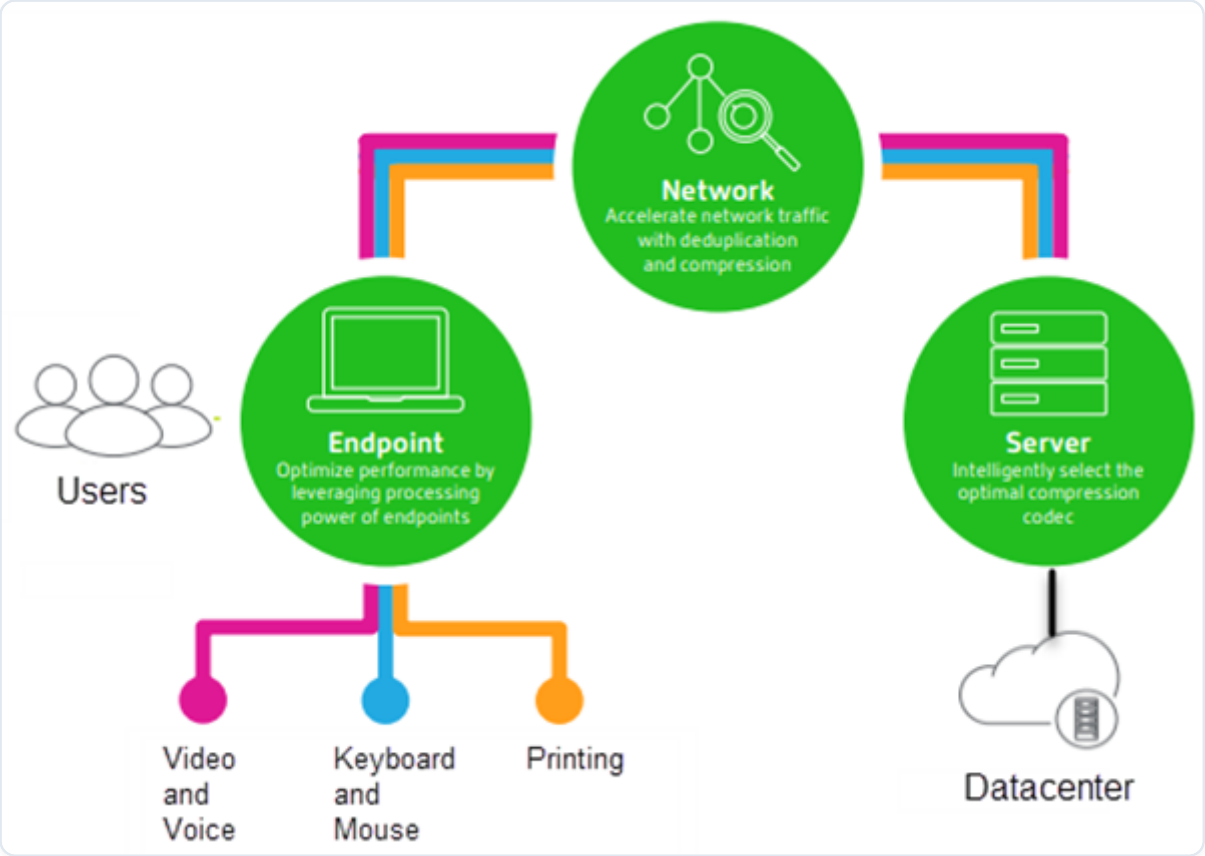



HDX 围绕以下三个技术原则设计：

- 智能重定向
- 自适应压缩
- 数据去重

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

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




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

有关详细信息，请参阅通过高清用户工作区提高工作效率。

## 在设备端

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

## 在网络上

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

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

## 在数据中心

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

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

# HDX 洞察

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

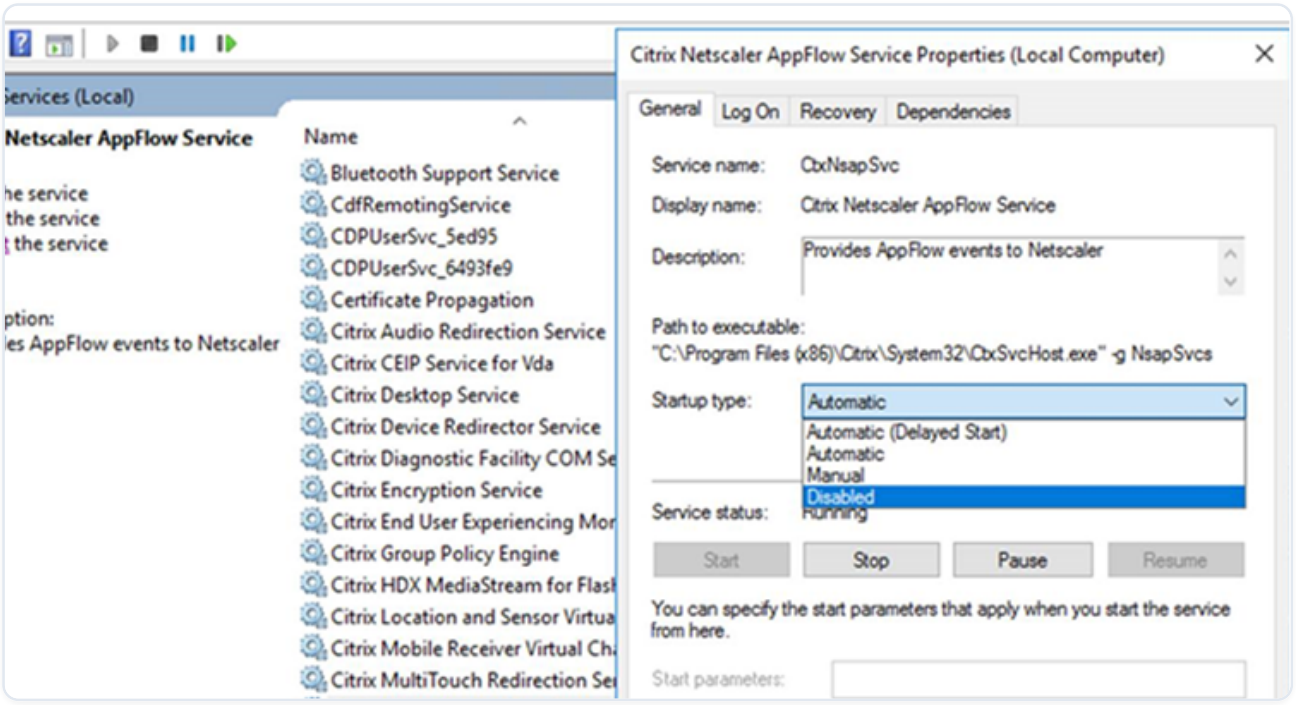
您可以启用 NetScaler 使用 HDX Insight 虚拟通道以未压缩格式传输所有必需的数据点。如果禁用此功能，NetScaler 设备将解密和解压缩分布在各种虚拟通道上的 ICA® 流量。使用单个虚拟通道可降低复杂性、增强可扩展性并更具成本效益。

**最低要求：**

- Citrix 虚拟应用和桌面™ 7 v1808
- XenApp 和 XenDesktop 7.17
- NetScaler 版本 12.0 内部版本 57.x
- 适用于 Windows 的 Citrix Workspace™ 应用程序 1808
- 适用于 Windows 的 Citrix Receiver 4.10
- 适用于 Mac 的 Citrix Workspace 应用程序 1808
- 适用于 Mac 的 Citrix Receiver 12.8

## 启用或禁用 HDX Insight 虚拟通道

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




## 在虚拟桌面上体验 HDX 功能

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

  a. 下载 Chrome 浏览器扩展程序 并将其安装到虚拟桌面。

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

- 要了解 HDX 如何提供高清音频：

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

  b. 在桌面上使用数字音频播放器（例如 iTunes）播放音乐文件。

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

- HDX 会根据客户端、平台、应用程序和网络带宽自动选择最佳交付方法，然后根据不断变化的条件进行自我调整。
- HDX 可优化 2D 和 3D 图形及视频的性能。

- HDX 使用户设备能够直接从 Internet 或 Intranet 上的源提供商流式传输多媒体文件，而不是通过主机服务器。如果未满足此客户端内容获取的要求，则媒体交付将回退到服务器端内容获取和多媒体重定向。通常，无需调整多媒体重定向功能策略。
- 当多媒体重定向不可用时，HDX 会向虚拟桌面交付丰富的服务器渲染视频内容：在包含高清视频的网站（例如 `<http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/>`）上观看视频。

须知：

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

## 客户端自动重新连接和会话可靠性

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

**客户端自动重新连接：**

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

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

在自动客户端重新连接期间，会话会重新启动，并期望网络连接。在自动客户端重新连接进行期间，用户无法与会话交互。

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

默认客户端自动重新连接设置：

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

有关详细信息，请参阅自动客户端重新连接策略设置。

**会话可靠性：**

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

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

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

重新连接后，客户端和服务器会从它们交换协议的同一点恢复。会话窗口会失去半透明效果，并为应用程序显示相应的通知区域弹出窗口。

默认会话可靠性设置

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

有关详细信息，请参阅 会话可靠性策略设置。

**NetScaler 与自动客户端重新连接和会话可靠性：**

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

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

## HDX 自适应吞吐量

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

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

> **重要提示：**

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

> 此功能有以下要求：

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

## 提高发送到用户设备的图像质量

以下视觉显示策略设置控制从虚拟桌面发送到用户设备的图像质量。

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

## 提高视频会议性能

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

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

HDX 网络摄像头视频压缩要求启用以下策略设置（所有设置默认均已启用）。

- 客户端音频重定向
- 客户端麦克风重定向
- 多媒体会议
- Windows Media 重定向

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

## 网络流量优先级

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

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

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

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

仅当配置了多个会话可靠性端口或 CGP 端口时，才支持服务质量。

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

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

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

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

要使包含这些设置的策略生效，用户必须注销，然后重新登录网络。

## 显示或隐藏远程语言栏

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

要从 VDA 禁用客户端对语言栏功能的控制：

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

## Unicode 键盘映射

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

### 启用或禁用 Unicode 键盘布局映射

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

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名称: EnableKlMap

类型: DWORD

值：1

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

### 启用 Unicode 键盘布局映射兼容模式

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

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名称: DisableWindowHook

类型: DWORD

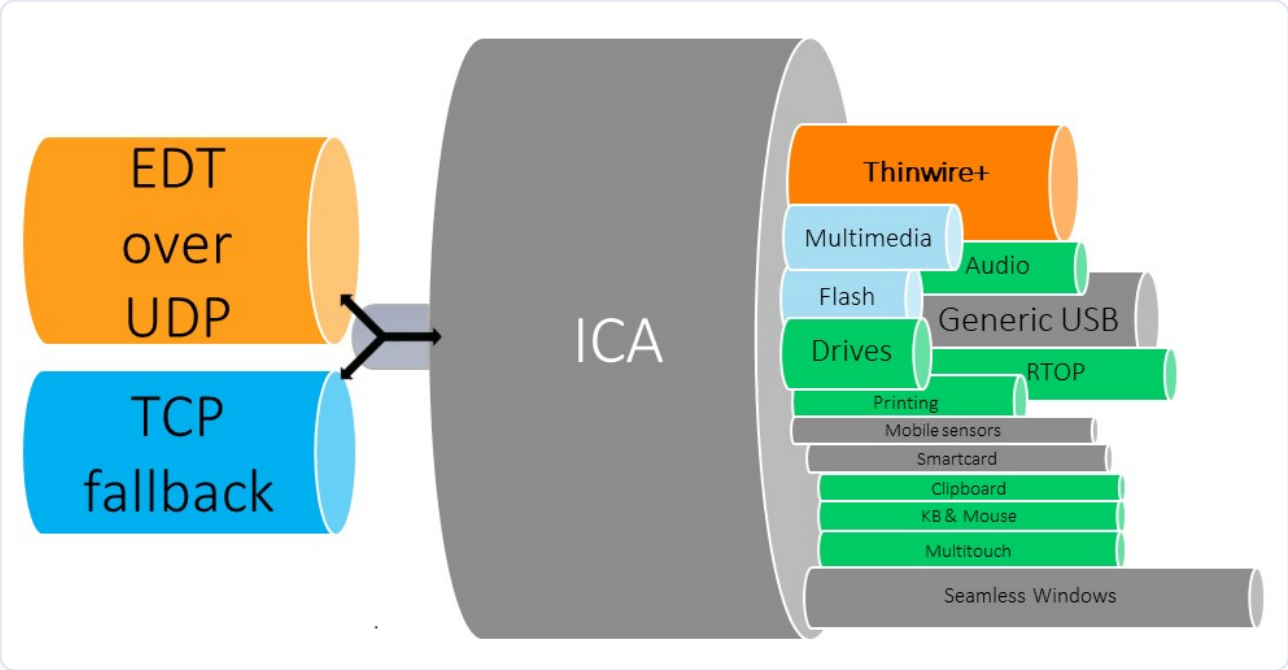
值：1

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

## 自适应传输

自适应传输是 Citrix Virtual Apps and Desktops™ 中的一种机制，它能够使用 Enlightened Data Transport (EDT) 作为 ICA 连接的传输协议。当 EDT 不可用时，自适应传输会切换到 TCP。

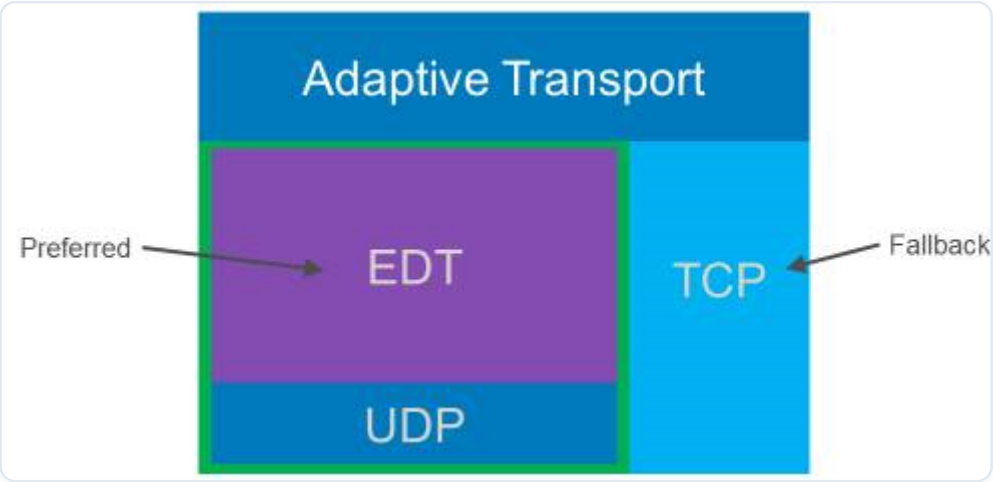
EDT 是一种基于用户数据报协议 (UDP) 构建的 Citrix 专有传输协议。它在具有挑战性的长距离连接上提供卓越的用户体验，同时保持服务器可伸缩性。EDT 提高了不可靠网络上所有 ICA® 虚拟通道的数据吞吐量，从而提供更好、更一致的用户体验。




当自适应传输设置为**首选**时，EDT 用作主要传输协议，TCP 用于回退。默认情况下，自适应传输设置为**首选**。您可以将自适应传输设置为**诊断模式**用于测试目的，这只允许 EDT 并禁用回退到 TCP。

对于适用于 Windows、Mac 和 iOS 的 Citrix Workspace™ 应用程序，EDT 和 TCP 连接会在初始连接、会话可靠性重新连接和自动客户端重新连接期间并行尝试。这样做可以减少连接时间，如果底层 UDP 传输不可用且必须使用 TCP。如果自适应传输设置为**首选**并且连接是使用 TCP 建立的，自适应传输会继续尝试每五分钟切换到 EDT。

对于适用于 Linux 和 Android 的 Citrix Workspace 应用程序，EDT 连接会首先尝试。如果连接不成功，Citrix Workspace 应用程序会在 EDT 请求超时后尝试使用 TCP 连接。




### 系统要求

以下是使用自适应传输和 EDT 的要求：

- 控制平面

  - 思杰 DaaS（以前称为 思杰 Virtual Apps and Desktops service）
  - Citrix Virtual Apps and Desktops 1912 或更高版本
- 虚拟投递代理
  - 版本 1912 或更高版本（推荐 2103 或更高版本）
  - 版本 2012 是使用 EDT 与 Citrix Gateway Service 所需的最低版本
- StoreFront™
  - 版本 3.12.x
  - 版本 1912.0.x
- Citrix Workspace 应用程序
  - Windows：版本 1912 或更高版本（推荐 2105 或更高版本）
  - Linux：版本 1912 或更高版本（推荐 2109 或更高版本）
  - Mac：版本 1912 或更高版本（推荐 2108 或更高版本）
  - iOS：Apple App Store 中提供的最新版本
  - Android: Google Play 中提供的最新版本
- Citrix 网关 (ADC)
  - 13.0.52.24 或更高版本
  - 12.1.56.22 或更高版本
- 防火墙（从 VDA 角度）
  - UDP 1494 入站 – 如果会话可靠性已禁用
  - UDP 2598 入站 – 如果会话可靠性已启用
  - UDP 443 入站 – 如果 VDA SSL 已启用 ICA 加密 (DTLS)
  - UDP 443 出站 – 如果使用 Citrix Gateway Service。有关详细信息，请参阅 Citrix Gateway service 文档。

### 注意事项

- 启用会话可靠性以使用 EDT MTU Discovery，并与 Citrix Gateway 和 Citrix Gateway service 结合使用 EDT。
- 确保 EDT MTU 设置得当以避免分段。否则，在某些情况下可能会影响性能或导致会话无法启动。有关详细信息，请参阅 EDT MTU Discover 部分。

- 有关将 EDT 与 Citrix Gateway service 结合使用的要求和注意事项的详细信息，请参阅 HDX Adaptive Transport with EDT support for Citrix Gateway service。
- 有关支持 EDT 的 Citrix Gateway 配置详细信息，请参阅 Configure Citrix Gateway to support Enlightened Data Transport and HDX Insight。
- 目前不支持 IPv6。

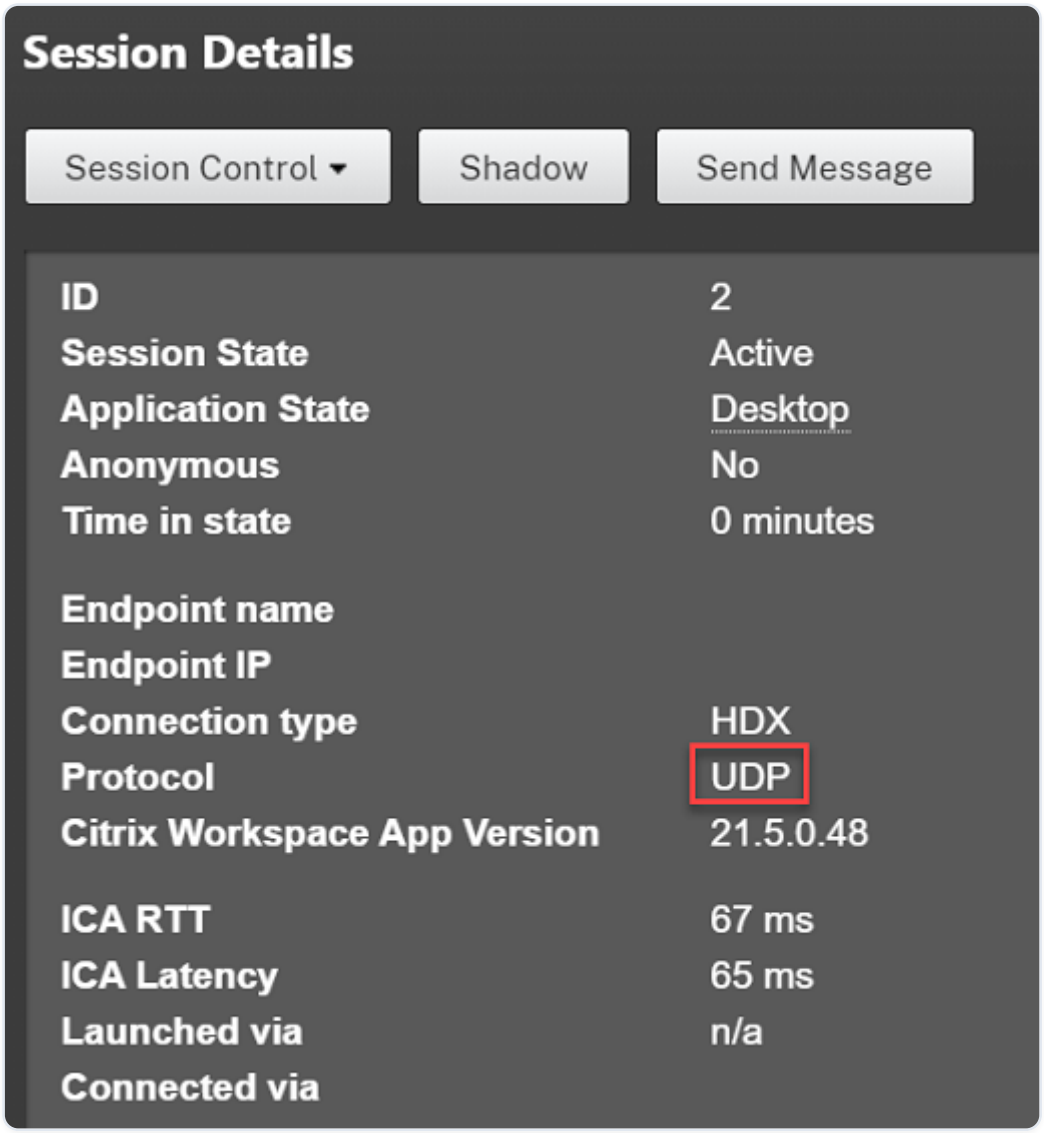
### 配置

自适应传输默认启用。您可以使用 Citrix 策略中的 **HDX™ 自适应传输**设置配置以下选项。

- **首选**。这是默认设置。自适应传输已启用，它使用 EDT 作为首选传输协议，并回退到 TCP。
- **诊断模式**。自适应传输已启用，并强制使用 EDT。回退到 TCP 已禁用。此设置仅建议用于测试和故障排除。
- **关闭**。自适应传输已禁用，仅使用 TCP 进行传输。

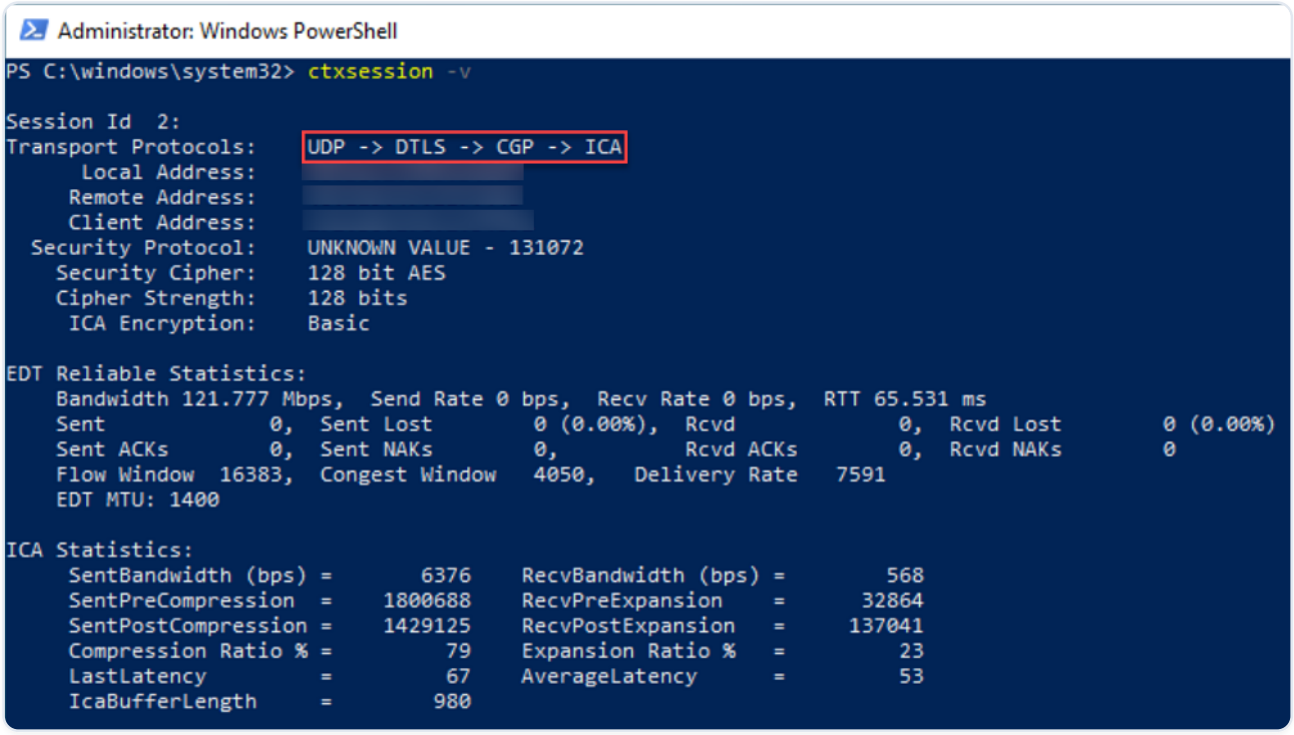
要确认 EDT 正用作会话的传输协议，您可以使用 Director 或 VDA 上的 CtxSession.exe 命令行实用程序。

在 Director 中，查找会话并选择**详细信息**。如果**连接类型**为 **HDX** 且**协议**为 **UDP**，则 EDT 正用作会话的传输协议。如果**连接类型**为 **RDP**，则 ICA 未在使用中，并且**协议**显示 N/A。有关详细信息，请参阅 Monitor sessions。




要使用 CtxSession.exe 实用程序，请在会话中启动命令提示符或 PowerShell 并运行 `ctxsession.exe`。要查看详细统计信息，请运行 `ctxsession.exe -v`。如果正在使用 EDT，则传输协议将显示以下其中一项：

- **UDP > ICA** (会话可靠性已禁用)
- **UDP > CGP > ICA**（会话可靠性已启用）
- **UDP > DTLS > CGP > ICA**（ICA 已进行 DTLS 端到端加密）




### EDT MTU 发现

MTU 发现允许 EDT 在建立会话时自动确定最大传输单元 (MTU)。这样做可以防止 EDT 数据包碎片化，从而避免性能下降或会话建立失败。

#### 系统要求

- VDA 最低版本 1912（建议使用 2103 或更高版本）
- Citrix Workspace 应用程序
  - Windows: 版本 1912 或更高版本（建议使用 2105 或更高版本）
  - Mac: 版本 2108 或更高版本
  - Linux: 版本 2109 或更高版本
  - Android: 版本 21.5 或更高版本
- 思杰 ADC：
  - 13.0.52.24
  - 12.1.56.22
- 必须启用会话可靠性

如果您使用的客户端平台或版本不支持此功能，请参阅 CTX231821，了解有关配置适合您环境的自定义 EDT MTU 的详细信息。

> **重要提示：**
>
> 多流 ICA 不支持 MTU 发现。

### 在 VDA 上控制 EDT MTU 发现

MTU 发现默认处于启用状态。要禁用此功能，请删除 **EDT MTU Discovery** 注册表值并重新启动 VDA。有关详细信息，请参阅通过注册表管理的 HDX 功能列表中的 EDT MTU Discovery 设置。

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

## 容忍丢包模式

> **重要提示：**
>
> - 此功能至少需要适用于 Windows 的 Citrix Workspace 应用程序 2002。
> - Citrix Gateway 或 Citrix Gateway Service 不支持容错模式。此模式仅适用于直接连接。

> 容错模式使用 EDT Lossy 传输协议，以增强通过高延迟和数据包丢失网络连接的用户的用户体验。

最初，会话使用 EDT 建立。如果达到或超过延迟和数据包丢失阈值，则适用的虚拟通道将从 EDT 切换到 EDT Lossy，而其他虚拟通道仍保留在 EDT 上。如果延迟和数据包丢失低于阈值，则适用的虚拟通道将切换回 EDT。

默认阈值为：

- 数据包丢失：5%
- 延迟：300 毫秒 (RTT)

容错模式默认处于启用状态。您可以使用容错模式阈值设置禁用该模式或调整数据包丢失和延迟阈值。

### 系统要求

- Citrix 虚拟投递代理 (VDA) 2003
- 适用于 Windows 的 Citrix Workspace 应用程序 2002
- 会话可靠性已启用。有关会话可靠性的详细信息，请参阅 会话可靠性策略设置。

## 已知问题

自适应传输和 EDT 存在以下问题：

- 数据包分段可能导致性能下降，甚至无法启动会话。您可以调整 EDT MTU 以避免此问题。请使用 MTU 发现或 CTX231821 中所述的解决方法。
- 如果启用了 MTU 发现，从 Windows 客户端启动会话时可能会出现灰色或黑色屏幕。要解决此问题，请升级到适用于 Windows 的 Workspace 应用程序 2105 或更高版本，或适用于 Windows 的 Workspace 应用程序 1912 CU4 或更高版本。
- 当通过 Citrix Gateway 或 Citrix Gateway Service 连接时，Linux 和 Android 客户端可能无法回退到 TCP。当客户端与网关之间的 EDT 协商成功，而网关与 VDA 之间的 EDT 协商失败时，就会发生这种情况。要解决此问题，请升级到适用于 Linux 的 Workspace 应用程序 2104 或更高版本以及适用于 Android 的 Workspace 应用程序 21.5 或更高版本。
- 非对称网络路径可能导致不通过 Citrix Gateway 或 Citrix Gateway Service 的连接的 MTU 发现失败。要解决此问题，请升级到 VDA 版本 2103 或更高版本。
- 使用 Citrix Gateway 或 Citrix Gateway Service 时，非对称网络路径可能导致 MTU 发现失败。这是由于网关上的一个问题，导致 EDT 数据包标头中的“不分段 (DF)”位无法传播。此问题的修复程序尚未推出。
- 对于通过 DS-Lite 网络连接的用户，MTU 发现可能会失败。当启用数据包处理时，某些调制解调器无法遵守 DF 位，从而阻止 MTU 发现检测分段。在这种情况下，可用的选项包括：
  - 禁用用户调制解调器上的数据包处理。
  - 禁用 MTU 发现并使用 CTX231821 中所述的硬编码 MTU。
  - 禁用自适应传输以强制会话使用 TCP。如果只有部分用户受到影响，请考虑在客户端禁用它，以便其他用户可以继续使用 EDT。
- 当通过 VPN 连接时，某些用户无法启动已发布的应用程序。不显示任何错误。有关详细信息，请参阅 CTX280797。

## 故障排除

要对自适应传输和 EDT 进行故障排除，我们建议如下：

1. 彻底审查并验证要求、注意事项和已知问题。
2. 检查 Studio 或 GPO 中是否存在覆盖所需 **HDX 自适应传输** 设置的 Citrix 策略。
3. 检查客户端上是否存在覆盖所需 HDX 自适应传输设置的设置。这可以是 GPO 首选项、使用可选的 Workspace 应用程序管理模板配置的设置，或者在注册表或客户端配置文件中手动配置的 **HDXoverUDP** 设置。
4. 在多会话 VDA 计算机上，确保 UDP 侦听器处于活动状态。在 VDA 计算机中打开命令提示符并运行 `netstat -a -p udp`。有关详细信息，请参阅如何确认 HDX Enlightened Data Transport 协议。
5. 在内部启动一个直接会话，绕过 Citrix Gateway，并检查正在使用的协议。如果会话使用 EDT，则 VDA 已准备好通过 Citrix Gateway 将 EDT 用于外部连接。
6. 如果 EDT 适用于直接内部连接，但不适用于通过 Citrix Gateway 的会话：
   - 确保启用了会话可靠性
   - 确保 Gateway 已启用 DTLS
7. 检查网络防火墙和VDA机器上运行的防火墙是否已配置适当的防火墙规则。
8. 检查您的用户连接是否需要非标准 MTU。有效 MTU 低于 1500 字节的连接会导致 EDT 数据包分段，这反过来会影响性能，甚至导致会话启动失败。此问题在使用 VPN、某些 Wi-Fi 接入点以及 4G 和 5G 等移动网络时很常见。有关如何解决此问题的信息，请参阅MTU 发现部分。

### 与 Citrix SD-WAN™ 的互操作性

Citrix SD-WAN 广域网优化 (WANOP) 提供跨会话令牌化压缩（数据去重），包括基于 URL 的视频缓存，从而显著减少带宽。如果办公室位置有两人或更多人观看相同的客户端获取视频，或传输或打印相同文件或文档的很大一部分，则会发生带宽减少。此外，通过在分支机构设备上运行 ICA 数据缩减和打印作业压缩过程，WANOP 提供了 VDA 服务器 CPU 卸载，并实现了更高的 Citrix Virtual Apps and Desktops 服务器可扩展性。

目前，SD-WAN WANOP 不支持 EDT。但是，如果正在使用 SD-WAN WANOP，则无需禁用自适应传输。当用户启动通过启用 WANOP 的 SD-WAN 的会话时，它会自动将会话设置为使用 TCP 作为传输协议。非 WANOP 会话在可能的情况下继续使用 EDT。

## Citrix ICA® 虚拟通道

> **警告：**

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

## 什么是 ICA 虚拟通道?

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

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

新的虚拟通道有时会随 Citrix Virtual Apps and Desktops 服务器和 Citrix Workspace app 产品的最新版本发布，以提供更多功能。

虚拟通道(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/ica-virtual-channels-1.png)

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

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

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

以下功能包含在此注册表路径下的 VirtualDriver 注册表值中：

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

或者

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

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

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

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

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

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

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

### 64 位兼容性

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

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

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

### 通用 USB 虚拟通道

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

- ctxusbm.sys
- ctxusbr.sys

### ICA 虚拟通道的工作原理

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

由 Shell 加载的虚拟通道模块，例如：

- EUEM
- 特文
- 剪贴板
- 多媒体
- 无缝会话共享
- 时区

有些以内核模式加载，例如：

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

### 服务器端的图形虚拟通道

从 XenApp 7.0 和 XenDesktop 7.0 开始，`ctxgfx.exe` 托管用于工作站和终端服务器会话的图形虚拟通道。`Ctxgfx` 托管与相应驱动程序交互的平台特定模块（RDSH 使用 `Icardd.dll`，工作站使用 `vdod.dll` 和 `vidd.dll`）。

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

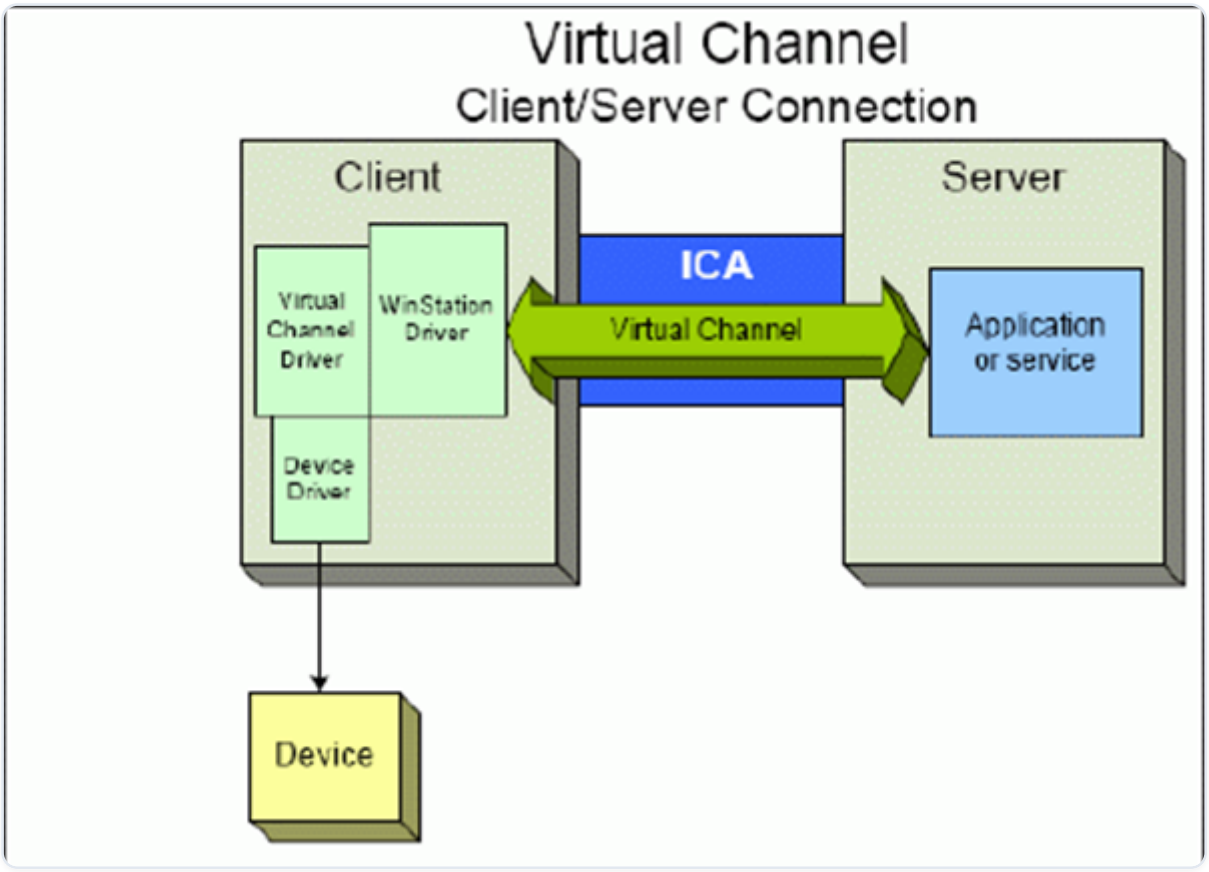
### 在 Windows 服务中托管专用通道

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

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

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

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




本概述包含使用虚拟通道的客户端-服务器数据交换。

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

## 使用虚拟通道 SDK 创建自己的虚拟通道

> **注意：**

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

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

**注意：**

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

## 使用 ICA 客户端对象 SDK 创建自己的虚拟通道

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

**重要提示：**

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

## 虚拟通道的直通功能

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

以下功能在单跳或多跳中以相同方式运行：

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

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

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

- 双向音频
- 文件传输
- 通用 USB 重定向
- 无缝
- 思睿线

> **重要提示：**

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

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

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

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

我们支持以下传统虚拟通道及其功能：

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

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

## 安全性和 ICA 虚拟通道

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

## 最佳实践

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

在创建使用虚拟通道功能的脚本时，请记住以下准则。

**虚拟通道命名：**

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

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

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

**双跳支持：**

| 虚拟通道 | 是否支持双跳？ |
| --- | --- |
| 音频 | 否 |
| 浏览器内容重定向 | 否 |
| CDM | 是 |

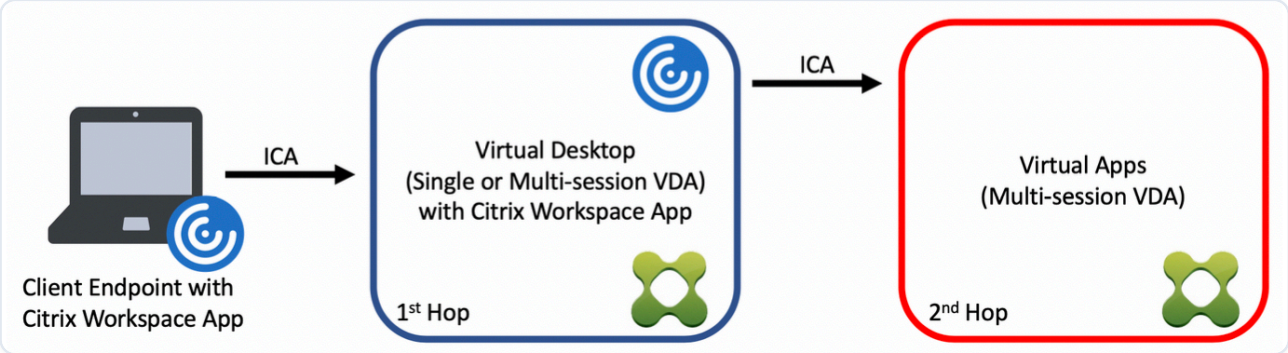
| 虚拟通道 | 是否支持双跳？ |
| --- | --- |
| CEIP | 否 |
| 剪贴板 | 是 |
| 康体纽姆 (MRVC) | 否 |
| 控制虚拟通道 | 是 |
| HTML5 视频重定向 (v1) | 是 |
| 键盘、鼠标 | 是 |
| 多点触控 | 否 |
| NSAPVC | 否 |
| 打印 | 是 |
| SensVC | 否 |
| 智能卡 | 是 |
| 特温 | 是 |
| USB 虚拟通道 | 是 |
| WAYCOM 设备 -K2M 使用 USB VC | 是 |
| 网络摄像头视频压缩 | 是 |
| Windows Media 重定向 | 是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

## 另请参阅

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

# Citrix 虚拟应用和桌面™ 中的双跳

在 Citrix 客户端会话中，“双跳”一词是指在 Citrix Virtual Desktops 会话中运行的 Citrix Virtual Apps 会话。下图说明了双跳。




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

您可以使用双跳部署模型来支持各种用例。其中一个常见示例是 Citrix Virtual Desktops 和 Citrix Virtual Apps 环境由不同实体管理的情况。此方法还可以有效解决应用程序兼容性问题。

## 系统要求

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

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

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

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

## 双跳中 HDX™ 的部署注意事项

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

### 图形

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

### 延迟

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

### 多媒体

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

### USB 设备重定向

HDX 包含通用和优化重定向模式，以支持各种 USB 设备类型。请特别注意每一跳中使用的模式，并使用下表作为参考以获得最佳结果。有关通用和优化重定向模式的更多信息，请参阅 通用 USB 设备。

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

**注意：**

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

## 支持例外

双跳会话支持大多数 HDX 功能和特性，但以下情况除外：

- 浏览器内容重定向
- 本地应用访问
- 适用于 商用 Skype 的 实时优化包
- 针对 Microsoft Teams 的优化

# 安装和配置

在开始每个部署步骤之前，请查阅参考文章，以了解在部署过程中看到和指定的内容。

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

## 准备

查阅 准备安装 并完成所有必要的任务。

- 有关概念、功能、与早期版本的差异、系统要求和数据库的信息。
- 决定核心组件安装位置时的注意事项。
- 权限和 Active Directory 要求。
- 有关可用安装程序、工具和界面的信息。

## 安装核心组件

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

## 创建站点

安装核心组件并启动 Studio 后，系统会自动引导您 创建站点。

## 安装一个或多个 Virtual Delivery Agent (VDA)

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

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

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

# 安装可选组件

如果计划使用 Citrix Universal Print Server，请在其打印服务器上安装其服务器组件。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-core.html) 或 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-command.html)。

要允许 StoreFront 使用 SAML 断言等身份验证选项，请安装 (/zh-cn/federated-authentication-service.html)。

要让最终用户更好地控制其用户帐户，请安装 (/zh-cn/self-service-password-reset.html)。

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

- (/zh-cn/provisioning.html) 是一个可选组件，它通过将主映像流式传输到目标设备来预配计算机。
- (/zh-cn/netscaler-gateway) 是一种安全的应用程序访问解决方案，可为管理员提供精细的应用程序级策略和操作控制，以保护对应用程序和数据的访问。
- (/zh-cn/netscaler-sd-wan) 是一组可优化 WAN 性能的设备。

# 创建计算机目录

在 Studio 中创建站点后，系统会引导您 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/install-configure/machine-catalogs-create.html)。

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

# 创建交付组

在 Studio 中创建第一个计算机目录后，系统会引导您 创建交付组。

交付组指定哪些用户可以访问所选目录中的计算机以及这些用户可用的应用程序。

# 创建应用程序组（可选）

创建交付组后，您可以选择 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/install-configure/application-groups-create.html)。您可以为跨不同交付组共享的应用程序或交付组内部分用户使用的应用程序创建应用程序组。

# 准备安装

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

- 一个或多个 Delivery Controller
- 思杰工作室
- 思杰迪雷克特
- 思杰思拓坊™
- Citrix 许可证服务器
- 一个或多个 Citrix Virtual Delivery Agent (VDA)
- 可选组件和技术，例如通用打印服务器、联合身份验证服务和自助密码重置

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

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

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

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

## 安装前需要查看的信息

- 技术概述：如果您不熟悉产品及其组件。
- 安全：规划部署环境时。
- 已知问题：您在此版本中可能会遇到的问题。
- 数据库：了解系统数据库以及如何配置它们。在 Controller 安装期间，您可以安装 SQL Server Express 作为站点数据库。在安装核心组件后创建站点时，您可以配置大多数数据库信息。
- 远程电脑访问：如果您正在部署一个环境，使用户能够远程访问其办公室中的物理计算机。
- 连接和资源：如果您正在使用虚拟机管理程序或其他服务来托管或预配用于应用程序和桌面的 VM。在创建站点时（安装核心组件后），您可以配置第一个连接。在此之前设置您的虚拟化环境。

- Microsoft System Center Configuration Manager：如果您正在使用 ConfigMgr 管理对应用程序和桌面的访问，或者正在将局域网唤醒功能与远程电脑访问结合使用。
- **公共云主机连接：** 如果您拥有混合权利许可证，则可以创建到公共云的主机连接。有关混合权利许可证的信息，请参阅混合权利。有关公共云权利以及此更改原因的信息，请参阅 CTX270373。

## 组件安装位置

查看 系统要求，了解支持的平台、操作系统和版本。组件先决条件会自动安装，但另有说明的除外。有关 Citrix StoreFront 和 Citrix 许可证服务器的受支持平台和先决条件，请参阅其文档。

您可以将核心组件安装在同一台服务器上或不同的服务器上。

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

  在其他服务器上安装其他组件之前，请先安装 Citrix 许可证服务器和许可证。
- 要在 Server CoreOS（例如 Delivery Controller）上安装受支持的组件，您必须使用命令行。该操作系统类型不提供图形界面，因此请在其他位置安装 Studio 和其他工具，然后将它们指向 Controller 服务器。

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

确保每个操作系统都具有最新更新。

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

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

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

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

> **提示：**

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

> Windows 10 单会话计算机的优化指南可在 CTX216252 中找到。

不应安装组件的位置：

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

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

## 权限和 Active Directory 要求

您必须是域用户，并且是安装组件的计算机上的本地管理员。

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

在开始安装之前配置您的 Active Directory 域。

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

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

有关详细信息：

- 安全最佳实践
- 委派管理
- 有关 Active Directory 配置的 Microsoft 文档

# 安装指南、注意事项和最佳实践

## 安装任何组件期间

- 从完整产品介质安装或升级 Delivery Controller、Studio、许可证服务器或 Director 时，如果 Citrix 安装程序检测到计算机上存在先前 Windows 安装挂起的重新启动，则安装程序将停止并显示退出/返回代码 9。系统将提示您重新启动计算机。

  这不是 Citrix 强制重新启动。这是由于之前在计算机上安装的其他组件导致的。如果发生这种情况，请重新启动计算机，然后再次启动 Citrix 安装程序。

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

  在安装过程中，您还可以选择参与其他 Citrix 技术，这些技术会收集诊断信息以用于维护和故障排除。有关这些计划的信息，请参阅 Citrix Insight Services。
- 当您安装（或升级）Studio 时，Google Analytics 会自动收集（并稍后上传）。安装 Studio 后，您可以使用注册表项 `HKLM\Software\Citrix\DesktopStudio\GAEnabled` 更改此设置。值为 **1** 表示启用收集和上传，**0** 表示禁用收集和上传。
- 如果 VDA 安装失败，MSI 分析器会解析失败的 MSI 日志，显示确切的错误代码。如果这是已知问题，分析器会建议一篇 CTX 文章。分析器还会收集有关失败错误代码的匿名数据。此数据包含在 CEIP 收集的其他数据中。如果您终止 CEIP 注册，则收集的 MSI 分析器数据将不再发送到 Citrix。

## VDA 安装期间

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

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

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

### VDA 可支持性工具

每个 VDA 安装程序都包含一个可支持性 MSI，其中包含用于检查 VDA 性能的 Citrix 工具，例如其整体运行状况和连接质量。在 VDA 安装程序图形界面的**附加组件**页面上启用或禁用此 MSI 的安装。通过命令行，您可以使用 `/exclude "Citrix Supportability Tools"` 选项禁用安装。

默认情况下，可支持性 MSI 安装在 `c:\Program Files (x86)\Citrix\Supportability Tools\` 中。您可以在 VDA 安装程序图形界面的**组件**页面上更改此位置，或使用 `/installdir` 命令行选项。请记住，更改位置会更改所有已安装的 VDA 组件，而不仅仅是可支持性工具。

可支持性 MSI 中的当前工具：

- Citrix Health Assistant：有关详细信息，请参阅 CTX207624。
- VDA 清理实用程序：有关详细信息，请参阅 CTX209255。

如果您在安装 VDA 时未安装这些工具，CTX 文章中包含指向当前下载包的链接。

### VDA 安装后和安装期间的重新启动

VDA 安装结束时需要重新启动。默认情况下，该重新启动会自动发生。

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

为最大程度地减少 VDA 安装期间所需的重新启动次数：

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

如果您在安装 VDA 之前未安装这些必备项：

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

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

### 安装或升级失败时恢复

> **注意：**
>
> 此功能适用于单会话和多会话 VDA。

> 如果单会话 VDA 安装或升级失败，并且启用了“失败时恢复”功能，则计算机将恢复到安装或升级开始前设置的还原点。

如果多会话 VDA 安装或升级失败，并且启用了“失败时还原”功能，则计算机将恢复到安装或升级开始之前执行的备份。

当启用此功能启动单会话 VDA 安装或升级时，安装程序会在实际安装或升级开始前创建一个系统还原点。如果 VDA 安装或升级失败，计算机将恢复到还原点状态。`%temp%/Citrix` 文件夹包含部署日志和有关还原的其他信息。

当启用此功能的多会话 VDA 安装或升级开始时，安装程序会在实际安装或升级开始之前创建服务器备份。如果 VDA 安装或升级失败，计算机将恢复到备份状态。`%temp%/Citrix` 文件夹包含部署日志和有关恢复的其他信息。创建服务器备份所需的时间取决于所需备份的大小以及服务器可用的资源量。备份存储在 *C:\WindowsImageBackup\servername* 中。

默认情况下，此功能处于禁用状态。

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

> **注意：**

> 此 GPO 设置不适用于恢复多会话 VDA。

> 在安装或升级单会话或多会话 VDA 时启用此功能：

- 使用 VDA 安装程序的图形界面时（例如，使用 **Autostart** 或 `XenDesktopVDASetup.exe` 命令，不带任何还原或静默选项），请在 **Summary** 页面上选中 **Enable automatic restore if update fails** 复选框。

  如果安装/升级成功完成，则不使用还原点/备份，但会保留。

- 使用命令行运行 VDA 安装程序，并使用 `/enablerestore` 或 `/enablerestorecleanup` 选项。
  - 如果您使用 `/enablerestorecleanup` 选项，并且安装/升级成功完成，则还原点/服务器备份将自动删除。
  - 如果您使用 `/enablerestore` 选项，并且安装/升级成功完成，则还原点不会被使用，但会保留。

## 安装程序

### 完整产品安装程序

使用 ISO 中提供的完整产品安装程序，您可以：

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

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

### 独立 VDA 安装程序

独立 VDA 安装程序可在 Citrix 下载页面上获取。（它们无法从产品安装介质中获取。）独立 VDA 安装程序比完整产品 ISO 小得多。它们更容易适应以下部署：

- 使用已暂存或本地复制的电子软件分发 (ESD) 软件包

- 拥有物理机
- 拥有远程办公室

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

有三个独立的 VDA 安装程序可供下载。

**VDAServerSetup.exe：**

安装适用于多会话操作系统的 VDA。它支持完整产品安装程序提供的所有适用于多会话操作系统的 VDA 选项。

**VDAWorkstationSetup.exe：**

安装适用于单会话操作系统的 VDA。它支持完整产品安装程序提供的所有适用于单会话操作系统的 VDA 选项。

**VDAWorkstationCoreSetup.exe：**

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

此安装程序不安装或不包含用于以下目的的组件：

- 应用程序虚拟化。
- Profile Management。从安装中排除 Citrix Profile Management 会影响 Citrix Director 显示。有关详细信息，请参阅安装 VDA。
- 计算机身份服务。
- Citrix 可支持性工具。
- 适用于 Windows 的 Citrix Files。
- 适用于 Outlook 的 Citrix Files。
- Citrix WEM 代理。

`VDAWorkstationCoreSetup.exe` 安装程序不安装或不包含适用于 Windows 的 Citrix Workspace 应用程序。

使用 `VDAWorkstationCoreSetup.exe` 相当于使用完整产品或 `VDAWorkstationSetup` 安装程序安装单会话操作系统 VDA，并且：

- 在图形界面中：在“**环境**”页面上选择“远程电脑访问”选项。
- 在命令行界面中：指定 `/remotepc` 选项。
- 在命令行界面中：指定 `/components vda` 加上 `/exclude` 选项，该选项列出了所有有效的附加组件名称。

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

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

## Citrix 安装返回代码

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

- 0 = 成功
- 1 = 失败
- 2 = 部分成功
- 3 = 部分成功且需要重新启动
- 4 = 失败且需要重新启动
- 5 = 用户取消
- 6 = 缺少命令行参数
- 7 = 发现新版本
- 8 = 成功且需要重新启动
- 9 = 文件锁定重新启动
- 10 = 已中止
- 11 = 介质失败
- 12 = 许可证失败
- 13 = 预检失败
- 14 = 因待重启检查而中止
- -1 = 退出

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

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

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

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

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

要使用组策略设置配置 RDS 许可证服务器：

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

Windows 10 工作负载需要相应的 Windows 10 许可证激活。我们建议您遵循 Microsoft 文档来激活 Windows 10 工作负载。

## Microsoft Azure 资源管理器 云环境

在您的 Citrix Virtual Apps and Desktops™ 部署中使用 Microsoft Azure Resource Manager 预配虚拟机时，请遵循本文中的指导。

我们假设您熟悉以下内容：

- Azure 活动目录：`<https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/>`
- 同意框架: `<https://docs.microsoft.com/zh-cn/azure/active-directory/manage-apps/plan-an-application-integration>`

- 服务主体: `<https://docs.microsoft.com/zh-cn/azure/active-directory/develop/app-objects-and-service-principals/>`

### Azure 按需预配

借助 Azure 按需预配，仅当 Citrix Virtual Apps and Desktops 在预配完成后启动开机操作时，才会创建 VM。

当您使用 MCS 在 Azure Resource Manager 中创建计算机目录时，Azure 按需预配功能具有以下特点：

- 降低存储成本
- 加快目录创建速度

创建 MCS 目录时，Azure 门户会在资源组中显示网络安全组、网络接口、基础映像和身份磁盘。

Azure 门户不会显示 VM，直到 Citrix Virtual Apps and Desktops 为其启动开机操作。有两种类型的计算机，其区别如下：

- 对于池化计算机，操作系统磁盘和回写缓存仅在 VM 存在时才存在。当您在控制台中关闭池化计算机时，该 VM 在 Azure 门户中不可见。如果您定期关闭计算机（例如，在工作时间之外），可以显著节省存储成本。
- 对于专用计算机，操作系统磁盘在 VM 首次开机时创建。Azure 门户中的 VM 保持存储状态，直到计算机身份被删除。当您在控制台中关闭专用计算机时，VM 在 Azure 门户中仍然可见。

### 连接到 Azure 资源管理器

连接和资源 介绍了创建连接的向导。以下信息涵盖了 Azure Resource Manager 连接的特定详细信息。

注意事项：

- Citrix® 建议使用具有参与者角色的服务主体。但是，请参阅最低权限部分以获取最低权限列表。
- 首次创建连接时，Azure 会提示您授予其必要的权限。对于将来的连接，您仍然需要进行身份验证，但 Azure 会记住您之前的同意，并且不会再次显示提示。
- 用于身份验证的帐户必须具有使用 Azure RBAC 在订阅中分配角色的权限。例如，订阅的 Owner、Role Based Access Control Administrator 或 User Access Administrator。
- 用于身份验证的帐户必须是订阅目录的成员。需要注意两种类型的帐户：“工作或学校”帐户和“个人 Microsoft 帐户”。有关详细信息，请参阅 CTX219211。

- 尽管您可以通过将现有 Microsoft 帐户添加为订阅目录的成员来使用它，但如果用户之前被授予对目录某个资源的来宾访问权限，则可能会出现并发症。在这种情况下，他们可能在目录中有一个占位符条目，该条目未授予他们必要的权限，并且会返回错误。

  通过从目录中删除资源并将其显式添加回来进行纠正。但是，请谨慎使用此选项，因为它会对该帐户可以访问的其他资源产生意外影响。
- 存在一个已知问题，即某些帐户在实际上是成员时被检测为目录访客。此类配置通常发生在较旧的已建立的目录帐户中。解决方法：将帐户添加到目录，该帐户将采用正确的成员身份值。
- 资源组只是资源的容器，它们可以包含来自其自身区域以外区域的资源。如果您期望资源组区域中显示的资源可用，这可能会造成混淆。
- 确保您的网络和子网足够大，可以容纳您所需的计算机数量。这需要一些远见，但 Microsoft 会帮助您指定正确的值，并提供有关地址空间容量的指导。

您可以通过两种方式建立到 Azure 的主机连接：

- 向 Azure 进行身份验证以创建服务主体。
- 使用先前创建的服务主体的详细信息连接到 Azure。

**创建服务主体**

> **重要提示：**
>
> 此功能尚不适用于 Azure 中国和 Azure 德国订阅。

开始之前，请向 Azure 进行身份验证。请确保：

- 您在订阅的 Azure Active Directory 租户中拥有一个用户帐户。
- 用于身份验证的帐户必须具有使用 Azure RBAC 在订阅中分配角色的权限。例如，订阅的 Owner、Role Based Access Control Administrator 或 User Access Administrator。
- 您拥有用于身份验证的全局管理员、应用程序管理员或应用程序开发人员权限。这些权限可以在创建主机连接后撤销。有关角色的更多信息，请参阅Azure AD 内置角色。

当您向 Azure 进行身份验证以创建服务主体时，Azure 中会注册一个应用程序。为注册的应用程序创建了一个密钥（客户端密钥）。注册的应用程序使用客户端密钥向 Azure AD 进行身份验证。请务必在客户端密钥过期之前更改它。在密钥过期之前，您会在控制台上收到警报。

要向 Azure 进行身份验证以创建服务主体，请在“**添加连接和资源**”向导中完成以下步骤：

1. 在“**连接**”页面上，选择“**创建新连接**”、“**Microsoft Azure**”连接类型和您的 Azure 环境。
2. 选择用于创建虚拟机的工具，然后选择“**下一步**”。
3. 在**连接详细信息**页面上，输入您的 Azure 订阅 ID 和连接名称。输入订阅 ID 后，**新建**按钮将启用。

> **注意：**
>
> 连接名称可以包含 1–64 个字符，并且不能仅包含空格或字符 `\/;:#.*?=<>|[]{}"'()'`。

4. 选择**新建**，然后输入 Azure Active Directory 帐户用户名和密码。
5. 选择“**登录**”。
6. 选择“**接受**”以授予 Citrix Virtual Apps and Desktops 列出的权限。Citrix Virtual Apps and Desktops 会创建一个服务主体，该主体允许它代表指定用户管理 Azure 资源。
7. 选择 **接受** 后，您将返回向导中的“**连接**”页面。

> **注意：**
>
> 成功通过 Azure 身份验证后，“**新建**”和“**使用现有**”按钮将消失。“**连接成功**”文本将显示，并带有一个绿色复选标记，表示已成功连接到您的 Azure 订阅。

8. 在“**连接详细信息**”页面上，选择“**下一步**”。

> **注意：**
>
> 在成功向 Azure 进行身份验证并同意授予所需权限之前，您无法继续访问下一页。

9. 配置连接的资源。资源包括区域和网络。
   - 在**区域**页面上，选择一个区域。
   - 在**网络**页面上，执行以下操作：
     - 键入 1–64 个字符的资源名称，以帮助识别区域和网络组合。资源名称不能只包含空格，也不能包含字符 `\/;:#.*?=<>|[]{}"'()'`。

- 选择一个虚拟网络/资源组对。（如果存在多个同名虚拟网络，将网络名称与资源组配对可提供唯一组合。）如果您在上一页选择的区域没有任何虚拟网络，请返回该页面并选择一个具有虚拟网络的区域。

10. 在**摘要**页面上，查看设置摘要，然后选择**完成**以完成设置。

**使用先前创建的服务主体的详细信息连接到 Azure**

要手动创建服务主体，请连接到您的 Azure Resource Manager 订阅并使用以下部分中提供的 PowerShell cmdlet。

先决条件：

- **SubscriptionId**：Azure Resource Manager `SubscriptionID` 用于要预配 VDA 的订阅。
- **ActiveDirectoryID**：您在 Azure AD 中注册的应用程序的租户 ID。
- **ApplicationName**：要在 Azure AD 中创建的应用程序的名称。

要创建服务主体：

1. 连接到您的 Azure Resource Manager 订阅。

   ```
   Connect-AzAccount
   ```

2. 选择要在其中创建服务主体的 Azure Resource Manager 订阅。

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
   ```

3. 在您的 AD 租户中创建应用程序。

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

4. 创建服务主体。

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

5. 为服务主体分配角色。

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

6. 从 PowerShell 控制台的输出窗口中，记下 ApplicationId。在创建主机连接时提供该 ID。

在 **添加连接和资源** 向导中：

1. 在“**连接**”页面上，选择“**创建新连接**”、“**Microsoft Azure**”连接类型和您的 Azure 环境。
2. 选择用于创建虚拟机的工具，然后选择“**下一步**”。

3. 在“**连接详细信息**”页面上，输入您的 Azure 订阅 ID 和连接名称。

> **注意：**
>
> 连接名称可以包含 1–64 个字符，并且不能仅包含空格或字符 `\/;:#.*?=<>|[]{}"'()'` 。

4. 选择 **使用现有**。在 **现有服务主体详细信息** 窗口中，输入现有服务主体的以下设置。输入详细信息后，**保存** 按钮将启用。选择 **保存**。在提供有效详细信息之前，您无法继续此页面。

   - **订阅 ID**。输入您的 Azure 订阅 ID。要获取您的订阅 ID，请登录 Azure 门户并导航到 **订阅 > 概述**。
   - **Active Directory ID**（租户 ID）。输入您在 Azure AD 中注册的应用程序的目录（租户）ID。
   - **应用程序 ID**。输入您在 Azure AD 中注册的应用程序的应用程序（客户端）ID。
   - **应用程序密钥**。创建密钥（客户端密钥）。注册的应用程序使用该密钥向 Azure AD 进行身份验证。建议您定期更改密钥以确保安全。请务必保存密钥，因为以后无法检索该密钥。
   - **密钥过期日期**。输入应用程序密钥的过期日期。在密钥过期之前，您会在控制台上收到警报。但是，如果密钥过期，您将收到错误。

     > **注意：**
     >
     > 出于安全考虑，过期期限不能超过两年。

   - **身份验证 URL**。此字段会自动填充且不可编辑。
   - **管理 URL**。此字段会自动填充且不可编辑。
   - **存储后缀**。此字段会自动填充且不可编辑。

     在 Azure 中创建 MCS 目录需要访问以下终结点。访问这些终结点可优化您的网络与 Azure 门户及其服务之间的连接。

     - 身份验证 URL: `<https://login.microsoftonline.com/>`
     - 管理 URL: `<https://management.azure.com/>`。这是 Azure Resource Manager 提供程序 API 的请求 URL。管理终结点取决于环境。例如，对于 Azure Global，它是

`<https://management.azure.com/>`；对于 Azure US Government，它是 `<https://management.usgovcloudapi.net/>`。

- 存储后缀: `<https://*.core.windows.net./>`。此 (*) 是存储后缀的通配符。例如，`<https://demo.table.core.windows.net/>`。

5. 选择“**保存**”后，您将返回到“**连接详细信息**”页面。选择“**下一步**”以继续到下一页。
6. 配置连接的资源。资源包括区域和网络。
   - 在**区域**页面上，选择一个区域。
   - 在**网络**页面上，执行以下操作：
     - 键入 1–64 个字符的资源名称，以帮助识别区域和网络组合。资源名称不能只包含空格，也不能包含字符 `\/;:#.*?=<>|[]{}"'()'`。
     - 选择一个虚拟网络/资源组对。（如果存在多个同名虚拟网络，将网络名称与资源组配对可提供唯一组合。）如果您在上一页选择的区域没有任何虚拟网络，请返回该页面并选择一个具有虚拟网络的区域。
7. 在**摘要**页面上，查看设置摘要，然后选择**完成**以完成设置。

### 使用 Azure Resource Manager 映像创建计算机目录

映像可以是磁盘、快照，也可以是 Azure 计算库中映像定义的映像版本，用于在计算机目录中创建 VM。有关映像的常规信息，请参阅创建计算机目录。

### Azure 限制

Azure Resource Manager 会限制订阅和租户的请求，根据定义的限制路由流量，这些限制是根据提供商的特定需求量身定制的。有关详细信息，请参阅 Microsoft 网站上的限制 Resource Manager 请求。订阅和租户存在限制，管理大量计算机可能会出现问题。例如，包含许多计算机的订阅可能会遇到与电源操作相关的性能问题。

> **提示：**
>
> 有关详细信息，请参阅使用 Machine Creation Services 提高 Azure 性能。
>
> 为帮助缓解这些问题，您可以删除 MCS 内部限制，以使用 Azure 提供的更多可用请求配额。

在大型订阅（例如包含 1,000 个 VM 的订阅）中打开或关闭 VM 时，我们建议使用以下最佳设置：

- 绝对同时操作数：500

- 每分钟最大新操作数：2000
- 最大并发操作数：500

MCS 默认支持 500 个最大并发操作。或者，您可以使用远程 PowerShell SDK 设置最大并发操作数。

使用 **PowerShell** 属性 `MaximumConcurrentProvisioningOperations` 指定 Azure 预配操作的最大并发数。使用此属性时，请考虑：

- `MaximumConcurrentProvisioningOperations` 的默认值为 500。
- 使用 PowerShell 命令 `Set-item` 配置 `MaximumConcurrentProvisioningOperations` 参数。

### Azure 资源组

Azure 预配资源组提供了一种预配虚拟机的方式，这些虚拟机为用户提供应用程序和桌面。您可以在创建 MCS 计算机目录时添加现有的空 Azure 资源组，或者让系统为您创建新的资源组。有关 Azure 资源组的信息，请参阅 Microsoft 文档。

#### Azure 资源组使用情况

每个 Azure 资源组的虚拟机、托管磁盘、快照和映像的数量没有限制。（每个 Azure 资源组 240 个 VM 和 800 个托管磁盘的限制已取消。）

- 当使用完全范围的服务主体创建计算机目录时，MCS 只创建一个 Azure 资源组，并将该组用于目录。
- 使用窄范围的服务主体创建计算机目录时，必须为该目录提供一个空的、预先创建的 Azure 资源组。

#### Azure 临时磁盘

通过 Azure 临时磁盘，您可以重新利用缓存磁盘或临时磁盘来存储支持 Azure 的虚拟机的操作系统磁盘。此功能对于需要高性能 SSD 磁盘而非标准 HDD 磁盘的 Azure 环境非常有用。要使用临时磁盘，您必须在运行 `New-ProvScheme` 时将自定义属性 `UseEphemeralOsDisk` 设置为 **true**。

> **注意：**
>
> 如果自定义属性 `UseEphemeralOsDisk` 设置为 **false** 或未指定值，则所有预配的 VDA 将继续使用预配的操作系统磁盘。
>
> 以下是用于预配方案的自定义属性示例集：

```
"CustomProperties": [
            {
                "Name": "UseManagedDisks",
                "Value": "true"
            },
            {
                "Name": "StorageType",
                "Value": "Standard_LRS"
            },
            {
                "Name": "UseSharedImageGallery",
                "Value": "true"
            },
            {
                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
            },
            {
                "Name": "SharedImageGalleryReplicaMaximum",
                "Value": "10"
            },
            {
```

```
                "Name": "LicenseType",
                "Value": "Windows_Server"
            },
            {
                "Name": "UseEphemeralOsDisk",
                "Value": "true"
            }
        ],
```

#### 如何使用临时 OS 磁盘创建计算机

临时 OS 磁盘根据 `CustomProperties` 参数中的 `UseEphemeralOsDisk` 属性进行控制。

#### 临时磁盘的重要注意事项

要使用 `New-ProvScheme` 预配临时操作系统磁盘，请考虑以下限制：

- 用于目录的 VM 大小必须支持临时操作系统磁盘。
- 与 VM 大小关联的缓存或临时磁盘的大小必须大于或等于操作系统磁盘的大小。
- 临时磁盘大小必须大于缓存磁盘大小。

此外，在以下情况下也要考虑这些问题：

- 创建预配方案时。
- 修改预配方案时。
- 更新映像时。

### AZURE 临时磁盘和 MACHINE CREATION SERVICES (MCS) 存储优化 (MCS I/O)

Azure 临时 OS 磁盘和 MCS I/O 不能同时启用。

重要注意事项如下：

- 不能同时启用临时 OS 磁盘和 MCS I/O 来创建计算机目录。
- 在 `New-ProvScheme` 或 `Set-ProvScheme` 中设置为 **true** 的 PowerShell 参数 (`UseWriteBackCache` 和 `UseEphemeralOsDisk`) 将失败并显示相应的错误消息。

- 对于已启用这两种功能而创建的现有计算机目录，您仍然可以：
  - 更新计算机目录。
  - 添加或删除 VM。
  - 删除计算机目录。

### Azure 服务器端加密

Citrix Virtual Apps and Desktops 和 Citrix DaaS 通过 Azure Key Vault 支持 Azure 托管磁盘的客户管理加密密钥。借助此支持，您可以使用自己的加密密钥加密计算机目录的托管磁盘，从而管理您的组织和合规性要求。有关详细信息，请参阅Azure 磁盘存储的服务器端加密。

将此功能用于托管磁盘时：

- 要更改磁盘加密所用的密钥，请在 `DiskEncryptionSet` 中更改当前密钥。与该 `DiskEncryptionSet` 关联的所有资源都将更改为使用新密钥进行加密。
- 当您禁用或删除密钥时，使用该密钥的任何虚拟机（VM）的磁盘都会自动关闭。关闭后，除非重新启用密钥或分配新密钥，否则虚拟机将无法使用。任何使用该密钥的目录都无法开机，并且您无法向其中添加虚拟机。

#### 使用客户管理加密密钥时的重要注意事项

使用此功能时，请考虑以下事项：

- 与客户管理密钥相关的所有资源（Azure Key Vault、磁盘加密集、VM、磁盘和快照）必须位于同一订阅和区域中。
- 启用客户管理加密密钥后，以后无法将其禁用。如果要禁用或删除客户管理加密密钥，请将所有数据复制到不使用客户管理加密密钥的其他托管磁盘。
- 使用服务器端加密和客户管理密钥从加密自定义映像创建的磁盘必须使用相同的客户管理密钥进行加密。这些磁盘必须位于同一订阅中。
- 从使用服务器端加密和客户管理密钥加密的磁盘创建的快照必须使用相同的客户管理密钥进行加密。
- 使用客户管理密钥加密的磁盘、快照和映像无法移动到其他资源组和订阅。
- 当前或以前使用 Azure 磁盘加密加密的托管磁盘不能使用客户管理密钥进行加密。
- 有关每个区域的磁盘加密集限制，请参阅 Microsoft 网站。

> **注意：**

> 有关配置 Azure 服务器端加密的信息，请参阅快速入门：使用 Azure 门户创建 Key Vault。

#### Azure 客户管理的加密密钥

创建计算机目录时，可以选择是否加密目录中预配的计算机上的数据。使用客户管理的加密密钥进行服务器端加密，可让您在托管磁盘级别管理加密并保护目录中计算机上的数据。磁盘加密集 (DES) 表示客户管理的密钥。要使用此功能，您必须首先在 Azure 中创建 DES。DES 采用以下格式：

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

从列表中选择一个 DES。您选择的 DES 必须与您的资源位于同一订阅和区域中。如果您的映像使用 DES 加密，则在创建计算机目录时请使用相同的 DES。创建目录后，您无法更改 DES。

如果您使用加密密钥创建目录，然后禁用 Azure 中相应的 DES，则您将无法再启动目录中的计算机或向其中添加计算机。

### Azure 专用主机

您可以使用 MCS 在 Azure 专用主机上预配 VM。在 Azure 专用主机上预配 VM 之前：

- 创建主机组。
- 在该主机组中创建主机。
- 确保有足够的宿主容量用于创建目录和虚拟机。

您可以通过以下 PowerShell 脚本创建具有主机租用定义的计算机目录：

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

使用 MCS 在 Azure 专用主机上预配虚拟机时，请考虑：

- *专用主机*是目录属性，目录创建后无法更改。Azure 目前不支持专用租用。

- 使用 `HostGroupId` 参数时，需要一个在托管单元区域中预配置的 Azure 主机组。
- Azure 自动放置是必需的。此功能会发出请求以载入与主机组关联的订阅。有关详细信息，请参阅 Azure 专用主机上的 VM 规模集 - 公共预览版。如果未启用自动放置，MCS 将在目录创建期间引发错误。

### Azure 共享映像库

使用 Azure 共享映像库作为 Azure 中 MCS 预配计算机的已发布映像存储库。您可以在库中存储已发布的映像，以加速 OS 磁盘的创建和填充，从而缩短非持久性 VM 的启动和应用程序启动时间。共享映像库包含以下三个元素：

- *库*：映像存储在此处。MCS 为每个计算机目录创建一个库。
- *库映像定义*：此定义包含有关已发布映像的信息（操作系统类型和状态、Azure 区域）。MCS 为为目录创建的每个映像创建一个映像定义。
- *库映像版本*：共享映像库中的每个映像可以有多个版本，每个版本可以在不同区域有多个副本。每个副本都是已发布映像的完整副本。

> **注意：**
>
> 共享映像库功能仅适用于托管磁盘。它不适用于旧版计算机目录。

> 有关详细信息，请参阅Azure 共享映像库概述。

#### 配置共享映像库

使用 `New-ProvScheme` 命令创建支持共享映像库的预配方案。使用 `Set-ProvScheme` 命令为预配方案启用或禁用此功能，并更改副本比率和最大副本值。

已向预配方案添加了三个自定义属性，以支持共享映像库功能：

`UseSharedImageGallery`

- 定义是否使用共享映像库存储已发布的映像。如果设置为 **True**，则映像存储为共享映像库映像，否则映像存储为快照。
- 有效值为 **True** 和 **False**。
- 如果未定义该属性，则默认值为 **False**。

`SharedImageGalleryReplicaRatio`

- 定义机器与图库映像版本副本的比率。

- 有效值为大于 0 的整数。
- 如果未定义该属性，则使用默认值。持久性操作系统磁盘的默认值为 1000，非持久性操作系统磁盘的默认值为 40。

`SharedImageGalleryReplicaMaximum`

- 定义每个图库映像版本的最大副本数。
- 有效值为大于 0 的整数。
- 如果未定义该属性，则默认值为 10。
- Azure 目前支持一个库映像单个版本最多 10 个副本。如果属性设置为大于 Azure 支持的值，MCS 会尝试使用指定值。Azure 会生成一个错误，MCS 会记录该错误，然后保持当前副本计数不变。

> **提示：**
>
> 当使用共享映像库存储 MCS 预配目录的已发布映像时，MCS 会根据目录中的计算机数量、副本比率和最大副本数设置库映像版本副本计数。副本计数是通过将目录中的计算机数量除以副本比率（向上舍入到最接近的整数值），然后将该值限制为最大副本计数来计算的。例如，如果副本比率为 20，最大值为 5，则 0-20 台计算机创建一个副本，21-40 台计算机创建 2 个副本，41-60 台计算机创建 3 个副本，61-80 台计算机创建 4 个副本，81 台以上计算机创建 5 个副本。

#### 用例：更新共享映像库副本比率和最大副本数

现有计算机目录使用共享映像库。使用 `Set-ProvScheme` 命令更新目录中所有现有计算机和未来计算机的自定义属性：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

#### 用例：将快照目录转换为共享映像库目录

对于此用例：

1. 运行 `Set-ProvScheme`，并将 `UseSharedImageGallery` 标志设置为 **True**。可以选择包含 `SharedImageGalleryReplicaRatio` 和 `SharedImageGalleryReplicaMaximum` 属性。
2. 更新目录。
3. 对计算机进行电源循环以强制更新。

例如：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

**提示：**

参数 `SharedImageGalleryReplicaRatio` 和 `SharedImageGalleryReplicaMaximum` 不是必需的。`Set-ProvScheme` 命令完成后，共享映像库映像尚未创建。目录配置为使用库后，下一次目录更新操作会将已发布的映像存储在库中。目录更新命令会创建库、库映像和映像版本。对计算机进行电源循环会更新它们，此时（如果适用）副本计数也会更新。从那时起，所有现有的非持久性计算机都将使用共享映像库映像进行重置，所有新预配的计算机都将使用该映像创建。旧快照将在几小时内自动清理。

#### 用例：将共享映像库目录转换为快照目录

对于此用例：

1. 运行 `Set-ProvScheme`，并将 `UseSharedImageGallery` 标志设置为 **False** 或未定义。
2. 更新目录。
3. 对计算机进行电源循环以强制更新。

例如：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

**提示：**

与从快照更新到共享映像库目录不同，每台计算机的自定义数据尚未更新以反映新的自定义属性。运行以下命令以查看原始共享映像库自定义属性：`Get-ProvVm -ProvisioningSchemeName catalog-name`。在 `Set-ProvScheme` 命令完成后，映像快照尚未创建。一旦目录配置为不使用库，下一次目录更新操作会将发布的映像存储为快照。从那时起，所有现有的非持久性计算机都将使用快照进行重置，所有新预配的计算机都将从快照创建。对计算机进行电源循环会更新它们，此时自定义计算机数据会更新以反映 `UseSharedImageGallery` 设置为 **False**。旧的共享映像库资产（库、映像和版本）将在几小时内自动清理。

### 将计算机预配到指定的可用性区域

您可以将计算机预配到 Azure 环境中的特定可用性区域。您可以使用 PowerShell 实现此目的。

**注意：**

如果未指定区域，MCS 会让 Azure 将计算机放置在该区域内。如果指定了多个区域，MCS 会将计算机随机分布在这些区域中。

#### 通过 PowerShell 配置可用性区域

使用 PowerShell，您可以通过 `Get-Item` 查看产品库存项。例如，要查看 *美国东部区域* `Standard_B1ls` 服务产品：

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

要查看区域，请使用该项的 `AdditionalData` 参数：

`$serviceOffering.AdditionalData`

如果未指定可用性区域，则计算机的预配方式不会改变。

要通过 PowerShell 配置可用性区域，请使用 `New-ProvScheme` 操作中可用的 **区域** 自定义属性。**区域** 属性定义了用于预配计算机的可用性区域列表。这些区域可以包括一个或多个可用性区域。例如，`<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>` 用于区域 1 和 3。

使用 `Set-ProvScheme` 命令更新预配方案的区域。

如果提供了无效区域，则预配方案不会更新，并且会显示一条错误消息，提供有关如何修复无效命令的说明。

> **提示：**
>
> 如果您指定了无效的自定义属性，则预配方案不会更新，并显示相关错误消息。

### Azure 临时磁盘

Azure 临时磁盘 允许您重新利用缓存或临时磁盘来存储已启用 Azure 的虚拟机的 OS 磁盘。此功能对于需要高性能 SSD 磁盘而非标准 HDD 磁盘的 Azure 环境非常有用。

> **注意：**
>
> 持久性目录不支持临时操作系统磁盘。
>
> 临时 OS 磁盘要求您的预配方案使用托管磁盘和共享映像库。有关详细信息，请参阅Azure 共享映像库。

#### 使用 PowerShell 配置临时磁盘

要为目录配置 Azure 临时操作系统磁盘，请在 `Set-ProvScheme` 中使用 `UseEphemeralOsDisk` 参数。将 `UseEphemeralOsDisk` 参数的值设置为 **true**。

> **注意：**
>
> 要使用此功能，您还必须启用参数 `UseManagedDisks` 和 `UseSharedImageGallery`。

例如：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

#### 存储临时操作系统临时磁盘

您可以选择将临时操作系统磁盘存储在虚拟机临时磁盘或资源磁盘上。此功能使您能够将临时操作系统磁盘与没有缓存或缓存不足的虚拟机配合使用。此类虚拟机具有临时磁盘或资源磁盘来存储临时操作系统磁盘，例如 `Ddv4`。

请考虑以下事项：

- 临时磁盘存储在虚拟机缓存磁盘或虚拟机的临时（资源）磁盘中。缓存磁盘优先于临时磁盘，除非缓存磁盘不足以容纳操作系统磁盘的内容。
- 对于更新，如果新映像大于缓存磁盘但小于临时磁盘，则会导致用 VM 的临时磁盘替换临时 OS 磁盘。

### 在电源循环时保留已预配的虚拟机

选择在电源循环时是否保留已预配的虚拟机。使用 PowerShell 参数 `New-ProvScheme CustomProperties`。此参数支持一个额外属性 `PersistVm`，用于确定已预配的虚拟机在电源循环时是否持久存在。将 `PersistVm` 属性设置为 **true** 以在关机时保留虚拟机，或将该属性设置为 **false** 以确保在关机时不保留虚拟机。

**注意：**

`PersistVm` 属性仅适用于启用了 `CleanOnBoot` 和 `UseWriteBackCache` 属性的预配方案。如果未为非持久性虚拟机指定 `PersistVm` 属性，则它们在关机时会从 Azure 环境中删除。

在以下示例中，`New-ProvScheme CustomProperties` 参数将 `PersistVm` 属性设置为 **true**：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>
```

在以下示例中，`New-ProvScheme CustomProperties` 参数通过将 `PersistVM` 设置为 **true** 来保留回写缓存：

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
```

```
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache

 -WriteBackCacheDiskSize 127

 -WriteBackCacheMemorySize 256
```

**提示：**

`PersistVm` 属性确定是否保留预配的虚拟机。`PersistOsdisk` 属性确定是否持久保存操作系统磁盘。要保留预配的虚拟机，请首先保留操作系统磁盘。您无法在不先删除虚拟机的情况下删除操作系统磁盘。您可以使用 `PersistOsdisk` 属性，而无需指定 `PersistVm` 参数。

### 存储类型

为使用 MCS 的 Azure 环境中的虚拟机选择不同的存储类型。对于目标 VM，MCS 支持：

- 操作系统磁盘：高级 SSD、SSD 或 HDD
- 回写缓存盘：高级 SSD、SSD 或 HDD

使用这些存储类型时，请考虑以下事项：

- 确保您的 VM 支持所选的存储类型。
- 如果您的配置使用 Azure 临时磁盘，则不会获得回写缓存磁盘设置选项。

> **提示：**
>
> `StorageType` 配置用于 OS 类型和存储帐户。`WBCDiskStorageType` 配置用于回写缓存存储类型。对于普通目录，`StorageType` 是必需的。如果未配置 `WBCDiskStorageType`，则 `StorageType` 将用作 `WBCDiskStorageType` 的默认值。

> 如果未配置 WBCDiskStorageType，则 StorageType 将用作 WBCDiskStorageType 的默认值

**配置存储类型**

要为 VM 配置存储类型，请在 `New-ProvScheme` 中使用 `StorageType` 参数。将 `StorageType` 参数的值设置为受支持的存储类型之一。

以下是预配方案中 `CustomProperties` 参数的示例集：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

### 检索 Azure VM、快照、操作系统磁盘和库映像定义的信息

您可以显示 Azure VM 的信息，包括操作系统磁盘和类型、快照和库映像定义。分配计算机目录时，此信息将显示在主映像上的资源中。使用此功能可以查看和选择 Linux 或 Windows 映像。PowerShell 属性 `TemplateIsWindowsTemplate` 已添加到 `AdditionDatafield` 参数。此字段包含 Azure 特定信息：VM 类型、操作系统磁盘、库映像信息和操作系统类型信息。将 `TemplateIsWindowsTemplate` 设置为 **True** 表示操作系统类型为 Windows；将 `TemplateIsWindowsTemplate` 设置为 **False** 表示操作系统类型为 Linux。

**提示：**

由 `TemplateIsWindowsTemplate` PowerShell 属性显示的信息来源于 Azure API。在某些情况下，此字段可能为空。例如，数据磁盘的快照不包含 `TemplateIsWindowsTemplate` 字段，因为无法从快照中检索操作系统类型。

例如，使用 PowerShell 将 Azure VM `AdditionData` 参数设置为 **True** 以表示 Windows 操作系统类型：

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192

ServiceOfferingCores 2

TemplateIsWindowsTemplate True

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

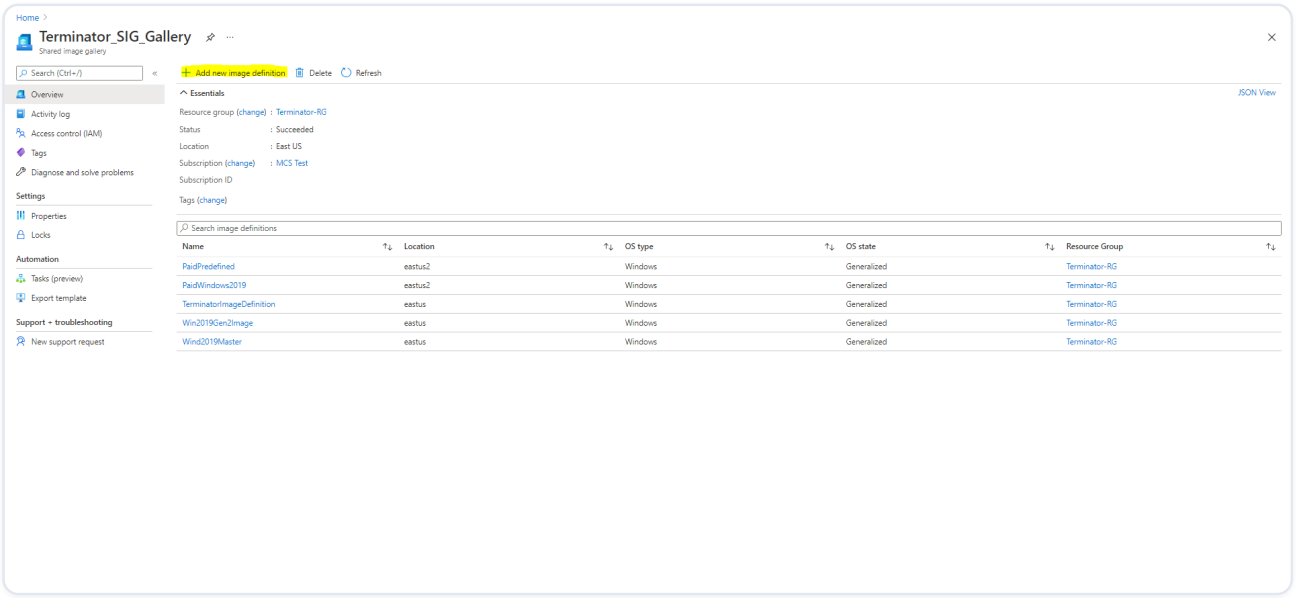
### Azure 应用商店

Citrix Virtual Apps and Desktops 和 Citrix DaaS 支持在 Azure 上使用包含计划信息的主映像来创建计算机目录。有关详细信息，请参阅 Microsoft Azure Marketplace。

> **提示：**
>
> Azure Marketplace 上的一些映像（例如标准 Windows Server 映像）不附加计划信息。Citrix DaaS™ 功能适用于付费映像。

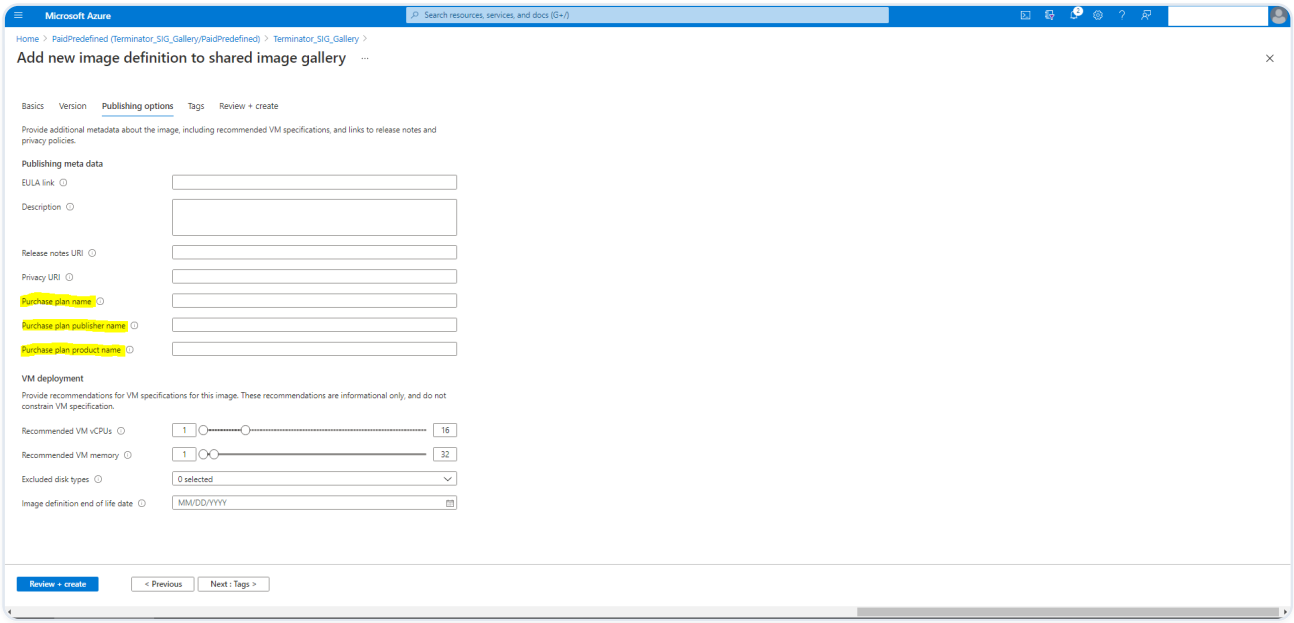
#### 确保在共享映像库中创建的映像包含 Azure 计划信息

使用本节中的过程在 Citrix Studio 中查看共享映像库映像。这些映像可以选择用作主映像。要将映像放入共享映像库，请在库中创建映像定义。




在**发布选项**页面中，验证购买计划信息。

购买计划信息字段最初为空。使用用于镜像的购买计划信息填充这些字段。未能填充购买计划信息可能导致计算机目录创建过程失败。




验证购买计划信息后，在定义中创建镜像版本。此版本用作主镜像。单击**添加版本**：

Azure Marketplace 添加 VDA 版本(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-marketplace-add-vda-version.png)

在**版本详细信息**部分中，选择镜像快照或托管磁盘作为源：

Azure Marketplace 选择 VDA 选项(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-marketplace-add-vda-version-info.png)

## 关于 Azure 权限

本节包含 Azure 所需的最低和一般权限。

### 最低权限

最低权限可提供更好的安全控制。但是，由于仅使用最低权限，需要额外权限的新功能将无法运行。

#### 创建主机连接

使用从 Azure 获取的信息添加新的主机连接。

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/disks/read",
```

#### 虚拟机电源管理

启动或关闭计算机实例。

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",
```

#### 创建、更新或删除虚拟机

创建计算机目录，然后添加、删除、更新计算机，并删除计算机目录。

以下是当主映像是托管磁盘或快照与托管连接位于同一区域时所需的最低权限列表。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",
```

```
"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",
```

对于以下功能，您需要在最低权限的基础上额外授予以下权限：

- 如果主映像是位于与托管连接相同区域的存储帐户中的 VHD：

  ```
  "Microsoft.Storage/storageAccounts/read",

  "Microsoft.Storage/storageAccounts/listKeys/action",
  ```

- 如果主映像是来自共享映像库的 ImageVersion：

  ```
  "Microsoft.Compute/galleries/read",

  "Microsoft.Compute/galleries/images/read",
  ```

```
"Microsoft.Compute/galleries/images/versions/read",
```

- 如果主映像是托管磁盘。快照或 VHD 位于与托管连接区域不同的区域：

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/delete",
```

- 如果您使用 Citrix 管理的资源组：

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- 如果您将主映像放入共享映像库：

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/versions/delete",
```

- 如果您使用 Azure 专用主机支持：

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

- 如果您使用带客户管理密钥 (CMK) 的服务器端加密 (SSE)：

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- 如果您使用 ARM 模板（计算机配置文件）部署 VM：

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/delete",
```

- 如果您使用 Azure 模板规范作为计算机配置文件：

```
"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

#### 创建、更新和删除具有非托管磁盘的计算机

以下是主映像为 VHD 且使用管理员提供的资源组时所需的最低权限列表：

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Compute/virtualMachines/deallocate/action",
```

```
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action"
```

**一般权限**

参与者角色拥有管理所有资源的完全访问权限。这组权限不会阻止您获取新功能。

以下权限集提供了最佳的未来兼容性，尽管它包含的权限比当前功能集所需的权限更多：

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/endGetAccess/action",
```

```
"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/write",

"Microsoft.Compute/hostGroups/hosts/read",

"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",
```

```
"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

```
"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

### 更多信息

- 连接和资源
- 创建计算机目录
- CTX219211: 设置 微软 Azure 活动目录 帐户
- CTX219243: 授予 XenApp 和 XenDesktop 访问您的 Azure 订阅的权限
- CTX219271: 使用站点到站点 VPN 部署混合云

## Microsoft System Center 虚拟机管理器 虚拟化环境

如果您使用 Hyper-V 和 Microsoft System Center Virtual Machine Manager (VMM) 来提供虚拟机，请遵循此指导。

此版本支持 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html) 中列出的 VMM 版本。

> **注意：**

> 不支持混合 Hyper-V 群集（包含运行不同 Hyper-V 版本的服务器）。

> 您可以使用 Citrix Provisioning（以前称为 Provisioning Services）和 Machine Creation Services™ 来预配：

- 第 1 代支持的桌面或服务器操作系统 VM。
- 第 2 代支持的桌面或服务器操作系统 VM，包括安全启动支持。

### 安装和配置管理程序

> **重要提示：**
>
> 所有 Delivery Controller 必须与 VMM 服务器位于同一林中。

1. 在服务器上安装 Microsoft Hyper-V 服务器和 VMM。
2. 在所有 Controller 上安装 System Center Virtual Machine Manager 控制台。控制台版本必须与管理服务器版本匹配。尽管较早的控制台可以连接到管理服务器，但如果版本不同，则预配 VDA 将失败。
3. 验证以下帐户信息：

   您在 Studio 中指定主机时使用的帐户是相关 Hyper-V 计算机的 VMM 管理员或 VMM 委派管理员。如果此帐户在 VMM 中仅具有委派管理员角色，则在主机创建过程中，存储数据不会在 Studio 中列出。

   > **提示：**
   >
   > 当使用 VMM 委派管理员时，您需要定义一个顶级主机组，并仅授予该委派管理员对该组的完全权限。多个主机组需要多个 VMM 委派管理员。每个主机组配置一个委派管理员。
   >
   > 用于 Studio 集成的用户帐户还必须是每个 Hyper-V 服务器上管理员本地安全组的成员。此配置支持 VM 生命周期管理，例如 VM 创建、更新和删除。

   不支持在运行 Hyper-V 的服务器上安装 Controller。

### 创建主 VM

1. 在主 VM 上安装 VDA，并选择优化桌面以提高性能的选项。
2. 为主 VM 创建快照以用作备份。

### 创建虚拟桌面

如果您使用 MCS 创建 VM，则在创建站点或连接时：

1. 选择 Microsoft 虚拟化主机类型。
2. 输入主机服务器的完全限定域名作为地址。

3. 输入您之前设置的、具有创建 VM 权限的管理员帐户的凭据。
4. 在 **主机详细信息** 中，选择创建 VM 时要使用的群集或独立主机。

   即使您使用的是单个 Hyper-V 主机部署，也要浏览并选择一个群集或独立主机。

### SMB 3 文件共享上的 MCS

对于使用 MCS 在 SMB 3 文件共享上创建的用于 VM 存储的计算机目录，请确保凭据满足以下要求。这些要求可确保来自 Controller 的 Hypervisor 通信库 (HCL) 的调用成功连接到 SMB 存储：

- VMM 用户凭据必须包含对 SMB 存储的完全读写访问权限。
- VM 生命周期事件期间的存储虚拟磁盘操作通过 Hyper-V 服务器使用 VMM 用户凭据执行。

使用 SMB 存储时，请从 Controller 到各个 Hyper-V 计算机启用身份验证凭据安全支持提供程序 (CredSSP)。对于在 Windows Server 2012 上运行 Hyper-V 的 VMM 2012 SP1，请使用此过程。有关详细信息，请参阅 CTX137465。

HCL 使用 `CredSSP` 打开与 Hyper-V 计算机的连接。此功能将 Kerberos 加密的用户凭据传递给 Hyper-V 计算机。远程 Hyper-V 计算机上的会话中的 **PowerShell** 命令使用提供的凭据运行。在这种情况下，使用 VMM 用户的凭据，以便与存储的通信命令正常工作。

以下任务使用源自 HCL 的 PowerShell 脚本，然后将这些脚本发送到 Hyper-V 计算机以对 SMB 3.0 存储执行操作。

- **整合主映像**：主映像创建 MCS 预配方案（计算机目录）。它克隆并平展主 VM，以便从新创建的磁盘创建 VM（并删除对原始主 VM 的依赖）。

  root\\virtualization\\v2 命名空间上的 ConvertVirtualHardDisk

  示例：

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

- **创建差异磁盘**：从通过整合主映像生成的主映像创建差异磁盘。然后将差异磁盘附加到新的 VM。

  root\\virtualization\\v2 命名空间上的 CreateVirtualHardDisk

  示例：

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

- **上载身份磁盘**：HCL 无法直接将身份磁盘上载到 SMB 存储。因此，Hyper-V 计算机必须将身份磁盘上载并复制到存储。由于 Hyper-V 计算机无法从 Controller 读取磁盘，因此 HCL 必须首先通过 Hyper-V 计算机复制身份磁盘，如下所示。

  HCL 通过管理员共享将身份上载到 Hyper-V 计算机。

  Hyper-V 计算机通过在 PowerShell 远程会话中运行的 PowerShell 脚本将磁盘复制到 SMB 存储。在 Hyper-V 计算机上创建一个文件夹，并且该文件夹的权限仅锁定给 VMM 用户（通过远程 PowerShell 连接）。

  HCL 从管理员共享中删除文件。

  当 HCL 完成将身份磁盘上载到 Hyper-V 计算机后，远程 PowerShell 会话会将身份磁盘复制到 SMB 存储。然后将其从 Hyper-V 计算机中删除。

  如果身份磁盘文件夹被删除，则会重新创建该文件夹，以便可以重复使用。

- **下载身份磁盘**：与上载一样，身份磁盘通过 Hyper-V 计算机传递到 HCL。以下过程会在 Hyper-V 服务器上创建一个仅具有 VMM 用户权限的文件夹（如果该文件夹不存在）。

  Hyper-V 计算机通过 PowerShell 脚本将磁盘从 SMB 存储复制到本地 Hyper-V 存储。此脚本在 PowerShell V3 远程会话中运行。

  HCL 将磁盘从 Hyper-V 计算机的管理员共享读取到内存中。

  HCL 从管理员共享中删除文件。

## Citrix Hypervisor™ 虚拟化环境

### 创建到 Citrix Hypervisor 的连接

创建到 Citrix Hypervisor（以前称为 XenServer®）的连接时，必须提供 VM Power Admin 或更高级别用户的凭据。

Citrix 建议使用 HTTPS 保护与 Citrix Hypervisor 的通信。要使用 HTTPS，必须替换 Citrix Hypervisor 上安装的默认 SSL 证书；请参阅 CTX128656。

如果 Citrix Hypervisor 服务器上启用了高可用性，则可以配置高可用性。Citrix 建议您选择池中的所有服务器（通过“编辑高可用性”），以便在池主服务器发生故障时允许与 Citrix Hypervisor 服务器通信。

如果 Citrix Hypervisor 支持 vGPU，则可以选择 GPU 类型和组，或直通。显示屏会指示所选内容是否具有专用 GPU 资源。

当在一个或多个 Citrix Hypervisor 主机上使用本地存储进行临时数据存储时，请确保池中的每个存储位置都具有唯一的名称。（要在 XenCenter® 中更改名称，请右键单击存储并编辑名称属性。）

您可以使用 Citrix Provisioning（以前称为 Provisioning Services）和 Machine Creation Services™ (MCS) 来预配：

- 受支持的桌面或服务器操作系统 VM 的传统 BIOS。
- 受支持的桌面或服务器操作系统 VM 的 UEFI，包括安全启动。

> **注意：**
>
> 配置 MCS 时需要池操作员权限或更高级别的权限。

#### 将 IntelliCache™ 用于 Citrix Hypervisor 连接

使用 IntelliCache，托管 VDI 部署更具成本效益，因为您可以结合使用共享存储和本地存储。这可以提高性能并减少网络流量。本地存储会缓存共享存储中的主映像，从而减少对共享存储的读取次数。对于共享桌面，对差异磁盘的写入会写入到主机上的本地存储，而不是共享存储。

- 使用 IntelliCache 时，共享存储必须是 NFS。
- Citrix® 建议您使用高性能本地存储设备，以确保最快的数据传输速度。

要使用 IntelliCache，必须在此产品和 Citrix Hypervisor 中都启用它。

- 安装 Citrix Hypervisor 时，选择 **Enable thin provisioning (Optimized storage for Virtual Desktops)**（启用精简预配（针对虚拟桌面优化的存储））。Citrix 不支持 IntelliCache 已启用和未启用服务器的混合池。有关详细信息，请参阅 Citrix Hypervisor 文档。
- 在 Citrix Virtual Apps and Desktops™ 中，IntelliCache 默认处于禁用状态。您只能在创建 Citrix Hypervisor 连接时更改此设置；之后无法禁用 IntelliCache。添加 Citrix Hypervisor 连接时：
  - 选择**共享**作为存储类型。
  - 选中**使用 IntelliCache**复选框。

## 所需的 Citrix Hypervisor 权限

Citrix Hypervisor 权限是基于角色的 (RBAC)。

有关详细信息，请参阅 基于角色的访问控制。

角色层次结构（按权限递增顺序）为：只读 → VM 操作员 → VM 管理员 → VM 电源管理员 → 池操作员 → 池管理员。

以下部分总结了每个预配任务所需的最低角色。

### 创建主机连接

| 任务 | 所需的最低角色 |
| --- | --- |
| 使用从 XenServer 获取的信息添加主机连接 | 只读 |
| 查看用户及其分配的角色 | 只读 |

### 虚拟机电源管理

| 任务 | 所需的最低角色 |
| --- | --- |
| 启动或关闭虚拟机 | 虚拟机操作员 |

### 创建、更新或删除虚拟机

| 任务 | 所需的最低角色 |
| --- | --- |
| 将虚拟机添加到现有快照计划或从中删除虚拟机 | 虚拟机电源管理员 |
| 添加、修改、删除快照计划 | 池操作员 |
| 发布主映像 | 池操作员（需要交换机端口锁定） |
| 创建计算机目录 | 池操作员：需要交换机端口锁定 |
| 添加或删除 VM（非 GPU 启用的 VM） | VM 管理员 |
| 添加或删除 VM（GPU 启用的 VM） | 池操作员 |
| 添加、删除或配置虚拟磁盘或 CD 设备 | VM 管理员 |
| 管理标签 | 虚拟机操作员 |

有关 RBAC 角色和权限的更多信息，请参阅 RBAC 角色和权限。

有关交换机端口锁定的信息，请参阅 使用交换机端口锁定。

### 使用 Citrix Hypervisor 连接创建计算机目录

支持 GPU 的计算机需要专用的主映像。这些 VM 需要支持 GPU 的显卡驱动程序。配置支持 GPU 的计算机，以允许 VM 运行使用 GPU 进行操作的软件。

1. 在 XenCenter 中，创建一台具有标准 VGA、网络和 vCPU 的虚拟机。
2. 更新 VM 配置以启用 GPU 使用（直通或 vGPU）。
3. 安装受支持的操作系统并启用 RDP。
4. 安装 Citrix VM Tools 和 NVIDIA 驱动程序。
5. 清除虚拟网络计算 (VNC) 管理控制台以优化性能，然后重新启动 VM。
6. 系统会提示您使用 RDP。使用 RDP 安装 VDA，然后重新启动 VM。
7. （可选）为 VM 创建快照，作为其他 GPU 主映像的基线模板。
8. 使用 RDP 安装在 XenCenter 中配置并使用 GPU 功能的客户特定应用程序。

### 更多信息

- 连接和资源
- 创建计算机目录

## 微软系统中心配置管理器 环境

使用 Microsoft System Center Configuration Manager (Configuration Manager) 管理应用程序和桌面访问的站点，可以通过以下选项将该用途扩展到 Citrix Virtual Apps and Desktops™：

- 使用 SCCM 安装 VDA。
- **Configuration Manager 唤醒代理功能：** 远程 PC 访问的局域网唤醒功能受 Configuration Manager 支持。有关详细信息，请参阅 局域网唤醒 - SCCM 集成。
- **Citrix Virtual Apps and Desktops 属性：** 属性 使您能够识别 Citrix Virtual Desktops™ 以通过 Configuration Manager 进行管理。（在某些版本中，Configuration Manager 使用 Citrix Virtual Apps and Desktops 的旧名称：XenApp and XenDesktop。）

### 属性

Microsoft System Center Configuration Manager 可使用属性来管理虚拟桌面。

在 Configuration Manager 中显示的布尔属性显示为 `1` 或 `0`，而不是 true 或 false。

这些属性在 `Root\Citrix\DesktopInformation` 命名空间中的 `Citrix_virtualDesktopInfo` 类中可用。属性名称来自 Windows Management Instrumentation (WMI) 提供程序。

| 属性 | 描述 |
| --- | --- |
| `AssignmentType` | 设置 IsAssigned 的值。有效值包括：`ClientIP`、`ClientName`、`None` 和 `User`（将 `IsAssigned` 设置为 `True`） |
| `BrokerSiteName` | 返回与 `HostIdentifier` 相同的值 |
| `DesktopCatalogName` | 与桌面关联的计算机目录。 |
| `DesktopGroupName` | 与桌面关联的交付组。 |
| `HostIdentifier` | 返回与 `BrokerSiteName` 相同的值。 |
| `IsAssigned` | `True` 用于将桌面分配给用户，对于随机桌面，设置为 `False` |
| `IsMasterImage` | 允许对环境做出决策。例如，将应用程序安装在映像上而不是预配的计算机上。有效值为：`True` 在用作映像的 VM 上。此值在安装期间根据选择设置，或在从该映像预配的 VM 上清除。 |
| `IsVirtualMachine` | `True` 用于虚拟机，`false` 用于物理机。 |
| `OSChangesPersist` | 如果桌面操作系统映像在每次重新启动时都重置为干净状态，则为 `False`；否则为 `true`。 |
| `PersistentDataLocation` | Configuration Manager 存储持久数据的位置。用户无法访问此位置。 |
| `BrokerSiteName`、`DesktopCatalogName`、`DesktopGroupName`、`HostIdentifier` | 在桌面向 Controller 注册时确定。对于尚未完全注册的桌面，它们为空。 |

要收集属性，请在 Configuration Manager 中运行硬件清单。要查看属性，请使用 Configuration Manager 资源管理器。在这些情况下，名称包含空格或与属性名称略有不同。例如，`BrokerSiteName` 显示为 `Broker Site Name`。

- 配置 Configuration Manager 以从 Citrix VDA 收集 Citrix WMI 属性

- 使用 Citrix WMI 属性创建基于查询的设备集合
- 基于 Citrix WMI 属性创建全局条件
- 使用全局条件定义应用程序部署类型要求

您还可以在 `Root\ccm_vdi` 命名空间中的 Microsoft 类 `CCM_DesktopMachine` 中使用 Microsoft 属性。有关详细信息，请参阅 Microsoft 文档。

## VMware 虚拟化环境

如果您使用 VMware 提供虚拟机，请遵循此指南。

安装 vCenter Server 和相应的管理工具。（不支持 vSphere vCenter Linked Mode 操作。）

如果您计划使用 MCS，请勿禁用 vCenter Server 中的 Datastore Browser 功能（如 `<https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2101567>` 中所述）。禁用此功能后，MCS 将无法正常工作。

您可以使用 Citrix Provisioning（以前称为 Provisioning Services）和 Machine Creation Services™ 来预配：

- 受支持的桌面或服务器操作系统 VM 的传统 BIOS。
- 受支持的桌面或服务器操作系统 VM 的 UEFI，包括安全启动。

### 所需权限

创建一个 VMware 用户帐户和一个或多个 VMware 角色，并授予本文列出的部分或所有权限。角色创建应基于用户权限所需的特定粒度级别，以便随时请求各种 Citrix DaaS™ 操作。要在任何时候授予用户特定权限，请将这些权限与相应的角色关联，至少在数据中心级别，并选中“**传播到子项**”选项。但是，对于 `StorageProfile` 权限和特定的 `Tags` 权限，请在 Root vCenter Server 级别应用权限，而不选中“**传播到子项**”。请参阅每个表中的注释。

下表显示了 Citrix Virtual Apps and Desktops™ 操作与最低所需 VMware 权限之间的映射。

> **注意：**

> 权限列表显示名称，特别是*用户界面*，在某些 vSphere 版本中有所不同。例如，在 vSphere 6.7 中，*用户界面*权限是“**更改内存**”和“**更改设置**”，而不是本页所述的所需权限中的“**设置**”和“**内存**”。

### 添加连接和资源

| SDK | 用户界面 |
| --- | --- |
| System.Anonymous、System.Read 和 System.View | 自动添加。可以使用内置的只读角色。 |

### 电源管理

| SDK | 用户界面 |
| --- | --- |
| VirtualMachine.Interact.PowerOff | 虚拟机 > 交互 > 关闭电源 |
| VirtualMachine.Interact.PowerOn | 虚拟机 > 交互 > 打开电源 |
| VirtualMachine.Interact.Reset | 虚拟机 > 交互 > 重置 |
| VirtualMachine.Interact.Suspend | 虚拟机 > 交互 > 暂停 |
| Datastore.Browse | 数据存储 > 浏览数据存储 |

### 预配计算机（Machine Creation Services）

要使用 MCS 预配计算机，需要以下权限：

| SDK | 用户界面 |
| --- | --- |
| Datastore.AllocateSpace | 数据存储 > 分配空间 |
| Datastore.Browse | 数据存储 > 浏览数据存储 |
| Datastore.FileManagement | 数据存储 > 低级别文件操作 |
| Network.Assign | 网络 > 分配网络 |
| Resource.AssignVMToPool | 资源 > 将虚拟机分配到资源池 |
| VirtualMachine.Config.AddExistingDisk | 虚拟机 > 配置 > 添加现有磁盘 |
| VirtualMachine.Config.AddNewDisk | 虚拟机 > 配置 > 添加新磁盘 |
| 虚拟机.配置.添加或移除设备 | 虚拟机 > 配置 > 添加或移除设备 |
| VirtualMachine.Config.AdvancedConfig | 虚拟机 > 配置 > 高级 |

| SDK | 用户界面 |
| --- | --- |
| VirtualMachine.Config.RemoveDisk | 虚拟机 > 配置 > 移除磁盘 |
| VirtualMachine.Config.CPUCount | 虚拟机 > 配置 > 更改 CPU 计数 |
| VirtualMachine.Config.Memory | 虚拟机 > 配置 > 更改内存 |
| 虚拟机.配置.设置 | 虚拟机 > 配置 > 更改设置 |
| VirtualMachine.Interact.PowerOff | 虚拟机 > 交互 > 关闭电源 |
| VirtualMachine.Interact.PowerOn | 虚拟机 > 交互 > 打开电源 |
| VirtualMachine.Interact.Reset | 虚拟机 > 交互 > 重置 |
| VirtualMachine.Interact.Suspend | 虚拟机 > 交互 > 暂停 |
| 虚拟机.清单.从现有创建 | 虚拟机 > 清单 > 从现有创建 |
| 虚拟机.清单.创建 | 虚拟机 > 清单 > 创建新项 |
| 虚拟机.清单.删除 | 虚拟机 > 清单 > 移除 |
| VirtualMachine.Provisioning.Clone | 虚拟机 > 置备 > 克隆虚拟机 |
| VirtualMachine.State.CreateSnapshot | vSphere 5.0 Update 2、vSphere 5.1 Update 1 和 vSphere 6.x Update 1：虚拟机 > 状态 > 创建快照；vSphere 5.5：虚拟机 > 快照管理 > 创建快照 |

**映像更新和回滚**

| SDK | 用户界面 |
| --- | --- |
| Datastore.AllocateSpace | 数据存储 > 分配空间 |
| Datastore.Browse | 数据存储 > 浏览数据存储 |
| Datastore.FileManagement | 数据存储 > 低级别文件操作 |
| Network.Assign | 网络 > 分配网络 |
| Resource.AssignVMToPool | 资源 > 将虚拟机分配到资源池 |

| SDK | 用户界面 |
| --- | --- |
| VirtualMachine.Config.AddExistingDisk | 虚拟机 > 配置 > 添加现有磁盘 |
| VirtualMachine.Config.AddNewDisk | 虚拟机 > 配置 > 添加新磁盘 |
| VirtualMachine.Config.AdvancedConfig | 虚拟机 > 配置 > 高级 |
| VirtualMachine.Config.RemoveDisk | 虚拟机 > 配置 > 移除磁盘 |
| VirtualMachine.Interact.PowerOff | 虚拟机 > 交互 > 关闭电源 |
| VirtualMachine.Interact.PowerOn | 虚拟机 > 交互 > 打开电源 |
| VirtualMachine.Interact.Reset | 虚拟机 > 交互 > 重置 |
| 虚拟机.清单.从现有创建 | 虚拟机 > 清单 > 从现有创建 |
| 虚拟机.清单.创建 | 虚拟机 > 清单 > 创建新项 |
| 虚拟机.清单.删除 | 虚拟机 > 清单 > 移除 |
| VirtualMachine.Provisioning.Clone | 虚拟机 > 置备 > 克隆虚拟机 |

### 删除已置备的计算机

| SDK | 用户界面 |
| --- | --- |
| Datastore.Browse | 数据存储 > 浏览数据存储 |
| Datastore.FileManagement | 数据存储 > 低级别文件操作 |
| VirtualMachine.Config.RemoveDisk | 虚拟机 > 配置 > 移除磁盘 |
| VirtualMachine.Interact.PowerOff | 虚拟机 > 交互 > 关闭电源 |
| 虚拟机.清单.删除 | 虚拟机 > 清单 > 移除 |

### 存储配置文件 (vSAN)

要在 vSAN 数据存储上创建目录时查看、创建或删除存储策略，需要以下权限：

| SDK | 用户界面 |
| --- | --- |
| StorageProfile.Update | 配置文件驱动的存储 > 配置文件驱动的存储更新。对于 vSphere 8：VM 存储策略 > 更新 VM 存储策略 |
| StorageProfile.View | 配置文件驱动的存储 > 配置文件驱动的存储视图。对于 vSphere 8：VM 存储策略 > 查看 VM 存储策略 |

**注意：**

在 Root vCenter Server 级别应用存储配置文件权限，不勾选**传播到子对象**。

### 标签和自定义属性

标签和自定义属性允许您将元数据附加到 vSphere 清单中创建的 VM，并使其更容易搜索和筛选这些对象。要创建、编辑、分配和删除标签或类别，需要以下权限：

| SDK | 用户界面 |
| --- | --- |
| InventoryService.Tagging.CreateTag | vSphere 标记 > 创建 vSphere 标签 |
| InventoryService.Tagging.CreateCategory | vSphere 标记 > 创建 vSphere 标签类别 |
| InventoryService.Tagging.EditTag | vSphere 标记 > 编辑 vSphere 标签 |
| InventoryService.Tagging.EditCategory | vSphere 标记 > 编辑 vSphere 标签类别 |
| InventoryService.Tagging.DeleteTag | vSphere 标记 > 删除 vSphere 标记 |
| InventoryService.Tagging.DeleteCategory | vSphere 标记 > 删除 vSphere 标记类别 |
| InventoryService.Tagging.AttachTag | vSphere 标记 > 分配或取消分配 vSphere 标记 |
| InventoryService.Tagging.ObjectAttachable | vSphere 标记 > 在对象上分配或取消分配 vSphere 标记 |
| Global.ManageCustomFields | 全局 > 管理自定义属性 |
| Global.SetCustomField | 全局 > 设置自定义属性 |

**注意：**

- 当 MCS 创建计算机目录时，它会使用特殊名称标记来标记目标 VM。这些标记将主映像与 MCS 创建的 VM 区分开来，并防止使用 MCS 创建的 VM 进行映像准备。您可以通过 vCenter 中 `XdProvisioned` 属性的值来识别差异。如果 MCS 创建 VM，则该属性设置为 **True**。
- 在根 vCenter Server 级别应用 `InventoryService.Tagging.AttachTag` 权限，不带“**传播到子对象**”选项。

### 加密操作

加密操作权限控制谁可以在哪种类型的对象上执行哪种类型的加密操作。vSphere 本机密钥提供程序使用 `Cryptographer.*` 权限。加密操作需要以下最低权限：

| SDK | 用户界面 |
| --- | --- |
| Cryptographer.Access | 权限 > 所有权限 > 加密操作 > 直接访问 |
| Cryptographer.AddDisk | 权限 > 所有权限 > 加密操作 > 添加磁盘 |
| Cryptographer.Clone | 权限 > 所有权限 > 加密操作 > 克隆 |
| Cryptographer.Encrypt | 权限 > 所有权限 > 加密操作 > 加密 |
| Cryptographer.EncryptNew | 权限 > 所有权限 > 加密操作 > 加密新内容 |
| Cryptographer.Decrypt | 权限 > 所有权限 > 加密操作 > 解密 |
| Cryptographer.Migrate | 权限 > 所有权限 > 加密操作 > 迁移 |
| Cryptographer.ReadKeyServersInfo | 权限 > 所有权限 > 加密操作 > 读取 KMS 信息 |

### 预配计算机 (Citrix Provisioning™)

通过 Citrix Provisioning 控制台使用 Citrix Virtual Apps and Desktops 安装向导和导出设备向导预配 VM 需要这些克隆和部署模板的权限。在创建主机连接时设置权限。您需要预配计算机（Machine Creation Services）中的所有权限以及以下权限。

| SDK | 用户界面 |
| --- | --- |
| VirtualMachine.Config.AddRemoveDevice | 虚拟机 > 配置 > 添加或移除设备 |
| VirtualMachine.Config.CPUCount | 虚拟机 > 配置 > 更改 CPU 计数 |
| VirtualMachine.Config.Memory | 虚拟机 > 配置 > 内存 |
| 虚拟机.配置.设置 | 虚拟机 > 配置 > 设置 |
| VirtualMachine.Provisioning.CloneTemplate | 虚拟机 > 置备 > 克隆模板 |
| VirtualMachine.Provisioning.DeployTemplate | 虚拟机 > 置备 > 部署模板 |
| VApp.Export | vApp > 导出 |

**注意：**

使用计算机配置文件创建 MCS 计算机目录需要 `VApp.Export`。

### 获取并导入证书

为保护 vSphere 通信，Citrix® 建议使用 HTTPS 而非 HTTP。

HTTPS 需要数字证书。请使用符合贵组织安全策略的证书颁发机构颁发的数字证书。

如果无法使用证书颁发机构颁发的数字证书，则可以使用 VMware 安装的自签名证书。仅当贵组织的安全策略允许时才使用此方法。将 VMware vCenter 证书添加到每个 Delivery Controller。

1. 将运行 vCenter Server 的计算机的完全限定域名 (FQDN) 添加到该服务器上的 hosts 文件中，路径为 `%SystemRoot%/WINDOWS/system32/Drivers/etc/`。仅当运行 vCenter Server 的计算机的 FQDN 尚未存在于域名系统中时，才需要执行此步骤。
2. 使用以下三种方法之一获取 vCenter 证书：

   **从 vCenter 服务器。**

   a. 将文件 rui.crt 从 vCenter 服务器复制到您的 Delivery Controllers 可访问的位置。

   b. 在控制器上，导航到导出的证书所在的位置并打开 rui.crt 文件。

   **使用 Web 浏览器下载证书。** 如果您使用的是 Internet Explorer，请右键单击 Internet Explorer 并选择**以管理员身份运行**以下载或安装证书。

a. 打开 Web 浏览器并与 vCenter 服务器建立安全的 Web 连接（例如 `<https://server1.domain1.com)>`）。
b. 接受安全警告。
c. 单击显示证书错误的地址栏。
d. 查看证书并单击“详细信息”选项卡。
e. 选择**复制到文件并以 .CER 格式导出**，并在出现提示时提供名称。
f. 保存导出的证书。
g. 导航到导出的证书所在的位置并打开 .CER 文件。

**直接从以管理员身份运行的 Internet Explorer 导入。**

- 打开 Web 浏览器并与 vCenter 服务器建立安全的 Web 连接（例如 `<https://server1.domain1.com)>`）。
- 接受安全警告。
- 单击显示证书错误的地址栏。
- 查看证书。

3. 将证书导入到每个 Controller 上的证书存储中。

a. 单击“**安装证书**”选项，选择“**本地计算机**”，然后单击“**下一步**”。
b. 选择“**将所有证书放入以下存储**”，然后单击“**浏览**”。选择“**受信任的个人**”，然后单击“**确定**”。单击“**下一步**”，然后单击“**完成**”。

如果在安装后更改 vSphere 服务器的名称，则必须在该服务器上生成新的自签名证书，然后才能导入新证书。

## 配置注意事项

**创建主 VM：**

使用主 VM 在计算机目录中提供用户桌面和应用程序。在您的虚拟机管理程序上：

1. 在主 VM 上安装 VDA，选择优化桌面的选项，这可以提高性能。
2. 为主 VM 创建快照以用作备份。

**创建连接：**

在连接创建向导中：

- 选择 VMware 连接类型。

- 指定 vCenter SDK 访问点的地址。
- 指定您之前设置的具有创建 VM 权限的 VMware 用户帐户的凭据。以 domain/username 形式指定用户名。

### VMware SSL 指纹

VMware SSL 指纹功能消除了手动创建到 VMware vSphere 管理程序的宿主连接的需要。在创建连接之前，不再需要手动在站点中的 Delivery Controller 与管理程序证书之间建立信任关系。

VMware SSL 指纹功能将不受信任证书的指纹存储在站点数据库中。此配置可确保管理程序可被 Citrix Virtual Apps and Desktops 持续识别为受信任，即使控制器不识别。

在 Studio 中创建 vSphere 宿主连接时，对话框允许您查看要连接的计算机的证书。然后，您可以选择是否信任它。

### 故障排除

如果目录创建失败，请参阅 CTX294978。

## VMware 云和合作伙伴解决方案

Citrix Virtual Apps and Desktops™ 支持以下 VMware 云和合作伙伴解决方案：

- Azure VMware 解决方案 (AVS)
- 谷歌云 VMware 引擎
- 在 Amazon Web Services (AWS) 上运行的 VMware Cloud

### Azure VMware 解决方案 (AVS) 集成

Citrix Virtual Apps and Desktop 服务支持 AVS。AVS 提供包含由 Azure 基础架构创建的 vSphere 群集的云基础架构。利用 Citrix Virtual Apps and Desktop 服务使用 AVS 预配 VDA 工作负载，其方式与在本地环境中使用 vSphere 相同。

#### 设置 AVS 集群

要使 Citrix Virtual Apps™ and Desktop 服务能够使用 AVS，请在 Azure 中执行以下步骤：

- 请求主机配额
- 注册 Microsoft.AVS 资源提供程序
- 网络清单
- 创建 Azure VMware Solution 私有云
- 访问 Azure VMware Solution 私有云

- 在 Azure 中为您的 VMware 私有云配置网络
- 配置适用于 Azure VMware Solution 的 DHCP
- 在 Azure VMware Solution 中添加网络段
- 验证 Azure VMware Solution 环境

### 为 AZURE 企业协议客户请求主机配额

在 Azure 门户的“**帮助 + 支持**”页面中，选择“**新建支持请求**”，并包含以下信息：

- 问题类型:技术
- 订阅:选择您的订阅
- 服务:所有服务 > Azure VMware Solution
- 资源:一般问题
- 摘要:需要容量
- 问题类型:容量管理问题
- 问题子类型:客户请求额外主机配额/容量

在支持票证的 **Description** 中，在 **Details** 选项卡中包含以下信息：

- POC 或生产
- 区域名称
- 主机数量
- 任何其他详细信息

> **注意：**

> AVS 最少需要三台主机，并建议您使用 N+1 主机冗余。

> 指定支持票证的详细信息后，选择 **Review + Create** 以将请求提交到 Azure。

### 注册 MICROSOFT.AVS 资源提供程序

请求主机配额后，注册资源提供程序：

1. 登录 Azure 门户。
2. 在 Azure 门户菜单上，选择 **所有服务**。
3. 在 **所有服务** 菜单中，输入订阅，并选择 **订阅**。

4. 从订阅列表中选择订阅。
5. 选择 **资源提供程序** 并在搜索栏中输入 **Microsoft.AVS**。
6. 如果资源提供程序未注册，请选择 **注册**。

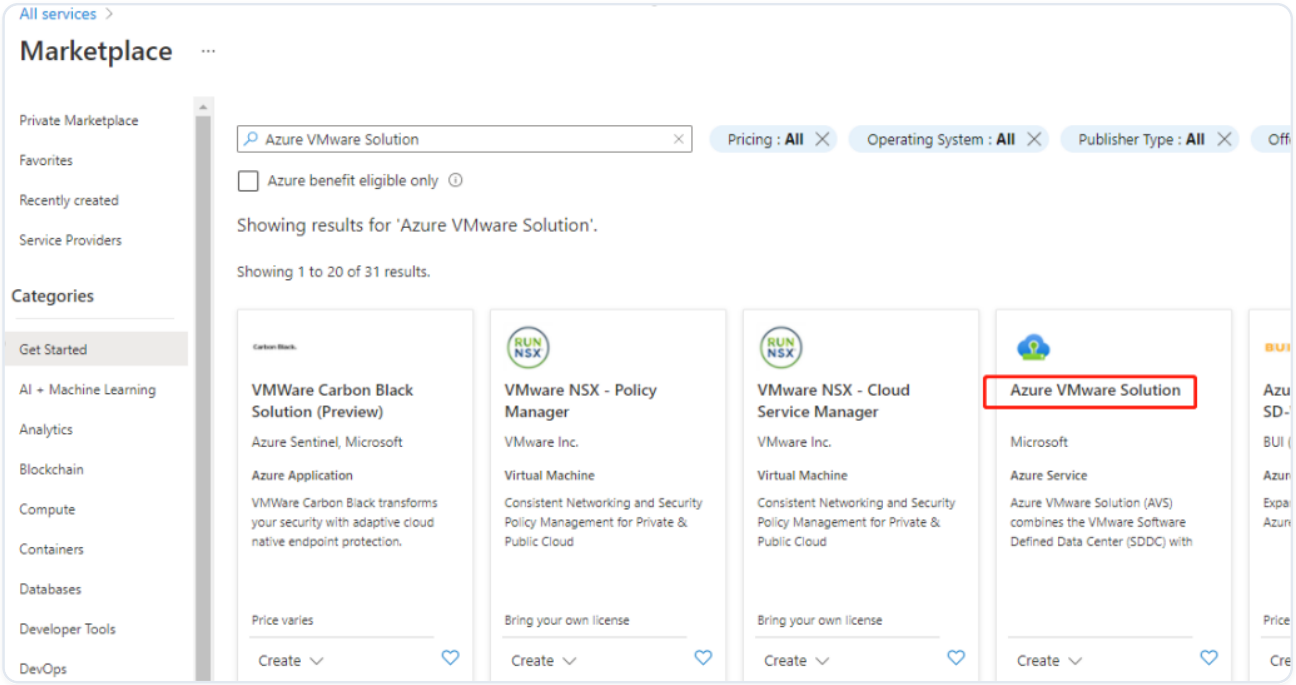
### 网络注意事项

AVS 提供需要特定网络地址范围和防火墙端口的网络服务。有关详细信息，请参阅 Azure VMware Solution 的网络规划清单。

### 创建 AZURE VMWARE SOLUTION 私有云

在考虑了环境的网络要求后，创建一个 ASV 私有云：

1. 登录 Azure 门户。
2. 选择 **创建新资源**。
3. 在 **搜索市场** 文本框中键入 *Azure VMware Solution*，然后从列表中选择 **Azure VMware Solution**。



图像

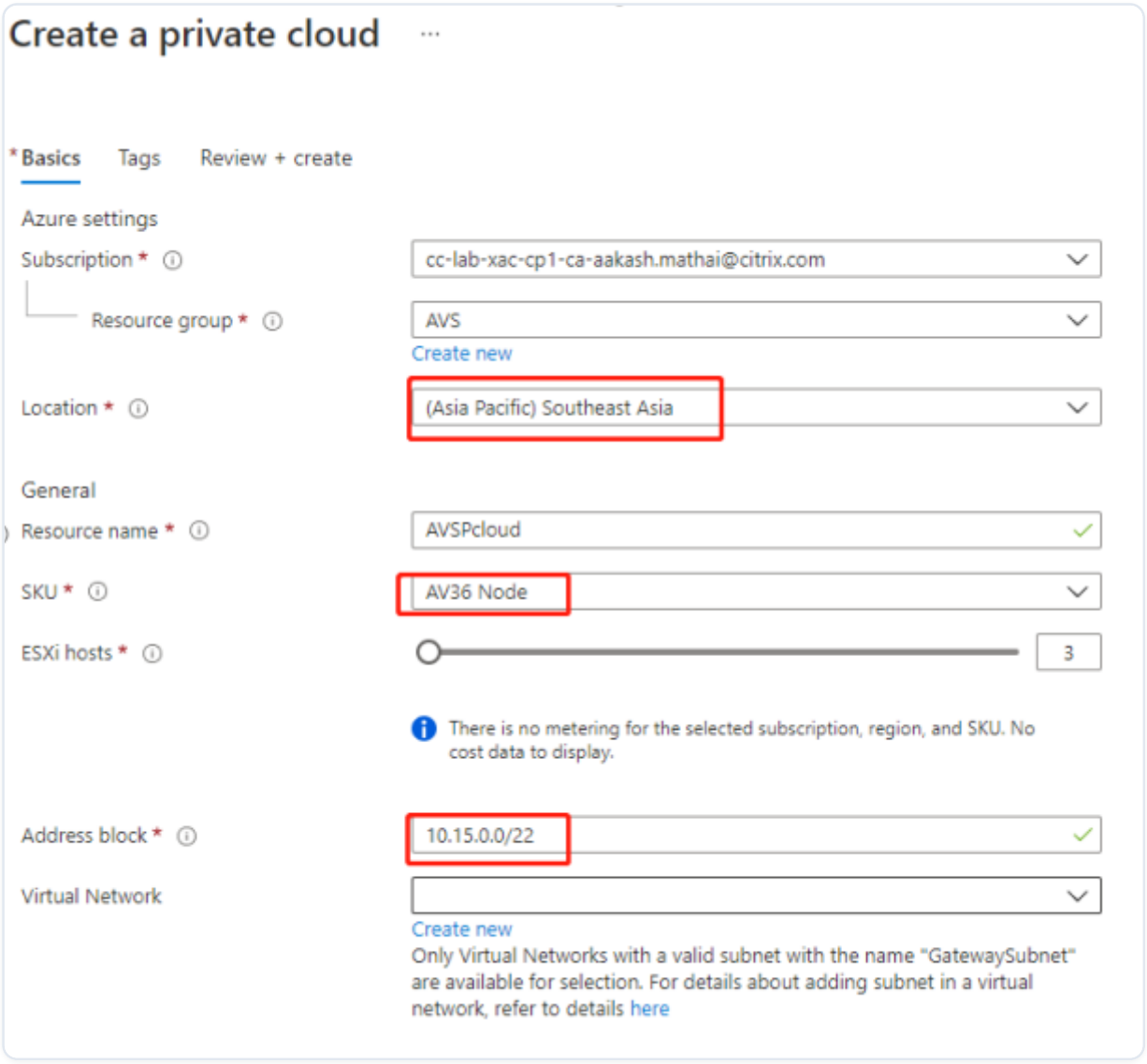
在 **Azure VMware Solution** 窗口中：

1. 选择 **创建**。
2. 单击**基本信息**选项卡。
3. 使用下表中的信息，输入字段的值：

| 字段 | 值 |
| --- | --- |
| 订阅 | 选择您计划用于部署的订阅。Azure 订阅中的所有资源将一起计费。 |
| 资源组 | 选择您的私有云的资源组。Azure 资源组是一个逻辑容器，Azure 资源部署和管理于其中。或者，您可以为您的私有云创建一个新的资源组。 |
| 位置 | 选择一个位置，例如美国东部。这是您在规划阶段定义的区域。 |
| 资源名称 | 提供您的 Azure VMware Solution 私有云的名称。 |
| SKU | 选择 AV36。 |
| 主机 | 显示为私有云集群分配的主机数量。默认值为 3，部署后可以增加或减少。 |
| 地址块 | 为私有云提供一个 IP 地址块。CIDR 代表私有云管理网络，将用于集群管理服务，例如 vCenter Server 和 NSX-T Manager。使用 /22 地址空间，例如 10.175.0.0/22。该地址应是唯一的，并且不与其他的 Azure 虚拟网络以及本地网络重叠。 |
| 虚拟网络 | 将其留空，因为 Azure VMware Solution ExpressRoute 线路是在部署后步骤中建立的。 |

在“**创建私有云**”屏幕中：

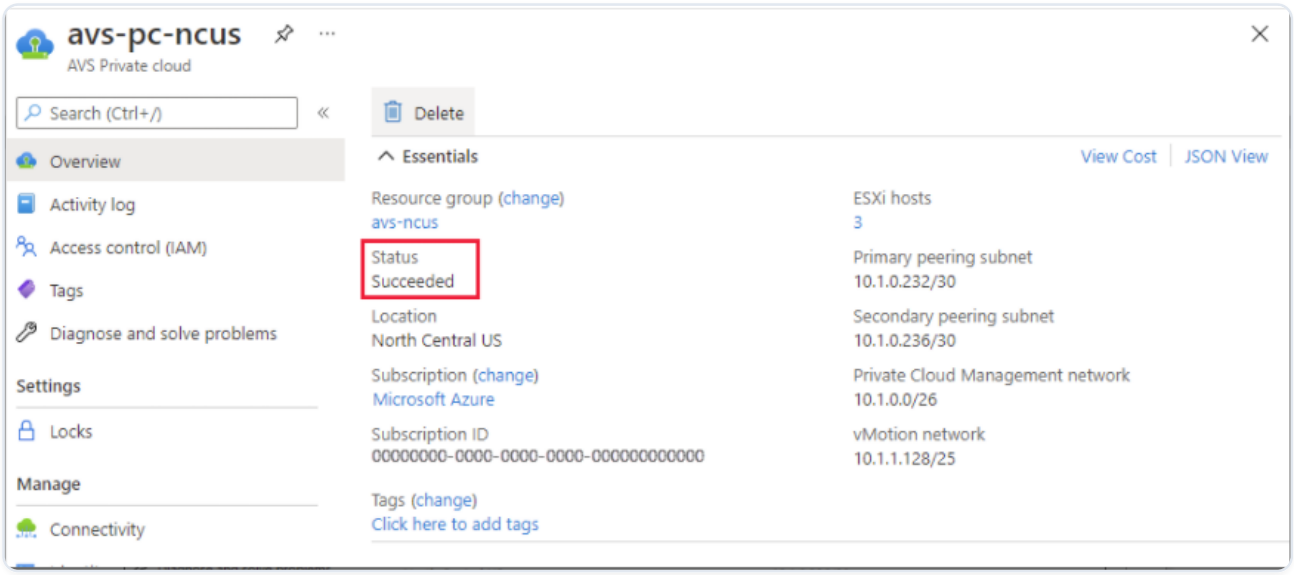
1. 在**位置**字段中，选择具有 AVS 的区域；资源组区域与 AVS 区域相同。
2. 在 **SKU** 字段中，选择 **AV36 Node**。
3. 在 **地址块** 字段中指定一个 IP 地址。例如，10.15.0.0/22。
4. 选择“**审查 + 创建**”。
5. 审查信息后，单击“**创建**”。




**提示：**

创建私有云可能需要 3-4 小时。向集群添加单个主机可能需要 30-45 分钟。

验证部署是否成功。导航到您创建的资源组并选择您的私有云。一旦 **状态** 为 **成功**，部署即完成。




### 访问 AZURE VMWARE SOLUTION 私有云

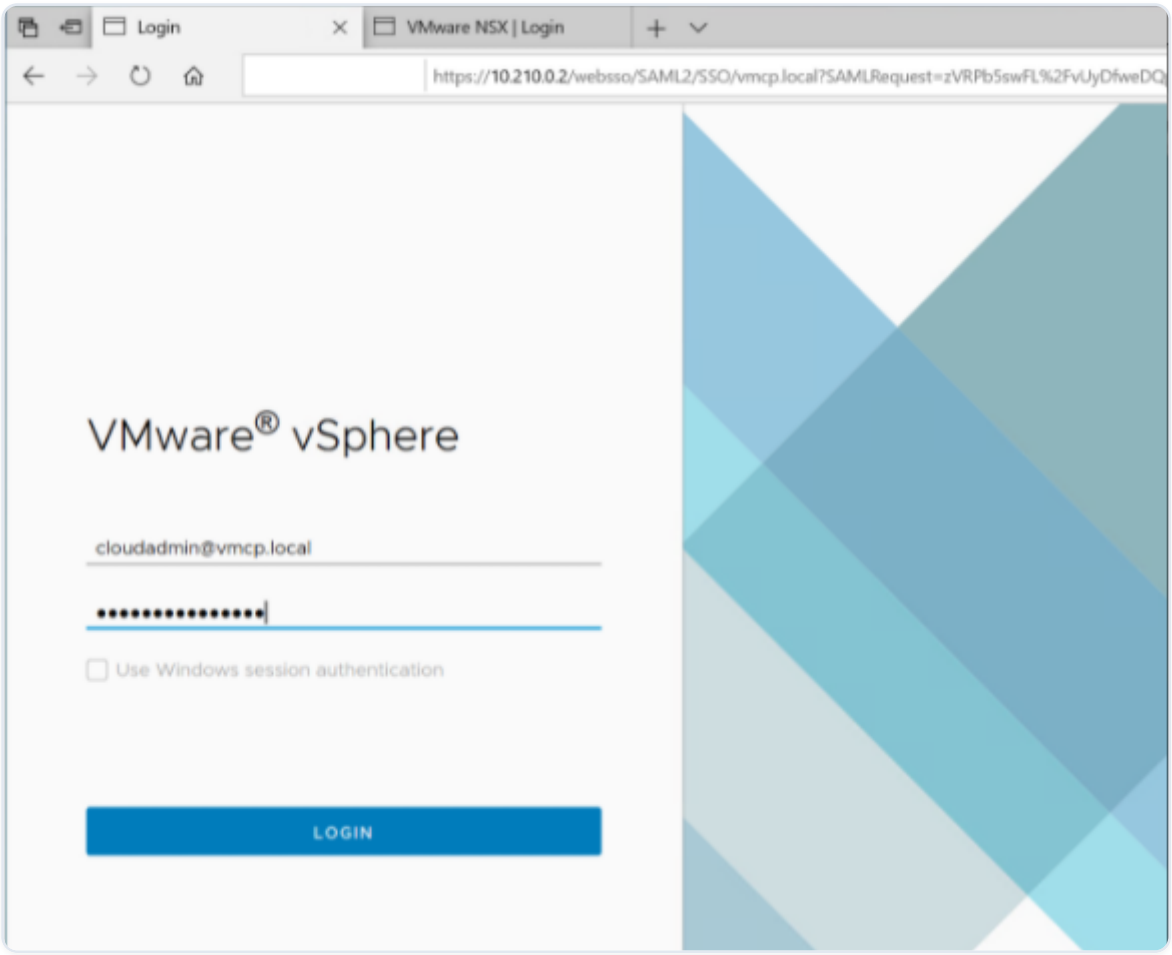
创建私有云后，创建 Windows VM 并连接到私有云的本地 vCenter。

创建新的 Windows 虚拟机

1. 在资源组中，选择 **+ 添加**，然后搜索并选择 **Microsoft Windows 10/2016/2019**。
2. 单击**创建**。
3. 输入所需信息，然后选择“**审查 + 创建**”。
4. 验证通过后，选择“**创建**”以开始虚拟机创建过程。

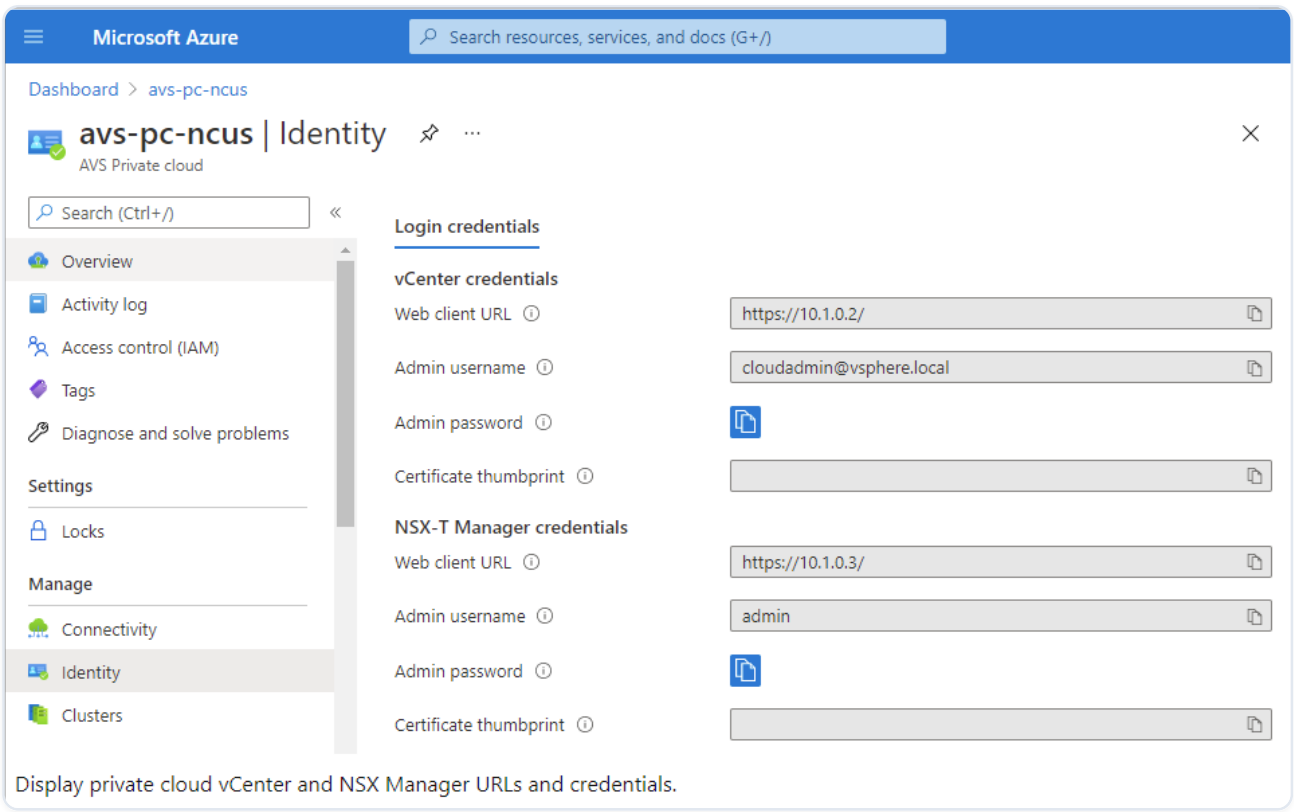
连接到私有云的本地 vCenter

1. 以云管理员身份登录 **vSphere Client with VMware vCenter SSO**。




2. 在 Azure 门户中，选择您的私有云，然后选择 **管理 > 身份**。

私有云 vCenter 和 NSX-T Manager 的 URL 和用户凭据显示如下：



确认 URL 和用户凭据后：

1. 导航到您在上一步中创建的 VM 并连接到该虚拟机。
2. 在 Windows VM 中，打开浏览器并在两个浏览器选项卡中导航到 vCenter 和 NSX-T Manager URL。在 vCenter 选项卡中，输入上一步中的 *cloudadmin@vmcp.local* 用户凭据。

### 在 AZURE 中为您的 VMWARE 私有云配置网络

访问 ASV 私有云后，通过创建虚拟网络和网关来配置网络。
创建虚拟网络

1. 登录 Azure 门户。
2. 导航到之前创建的资源组。
3. 选择 **+ 添加** 以定义新资源。
4. 在 **搜索市场** 文本框中，键入 *虚拟网络*。找到虚拟网络资源并选择它。
5. 在**虚拟网络**页面上，选择**创建**以设置您的私有云的虚拟网络。
6. 在**创建虚拟网络**页面上，输入您的虚拟网络的详细信息。
7. 在**基本信息**选项卡上，输入虚拟网络的名称，选择相应的区域，然后单击**下一步：IP 地址。**
8. 在**IP 地址**选项卡上，在 IPv4 地址空间下，输入之前创建的地址。

> **重要提示：**

> 使用的地址不得与您创建私有云时使用的地址空间重叠。

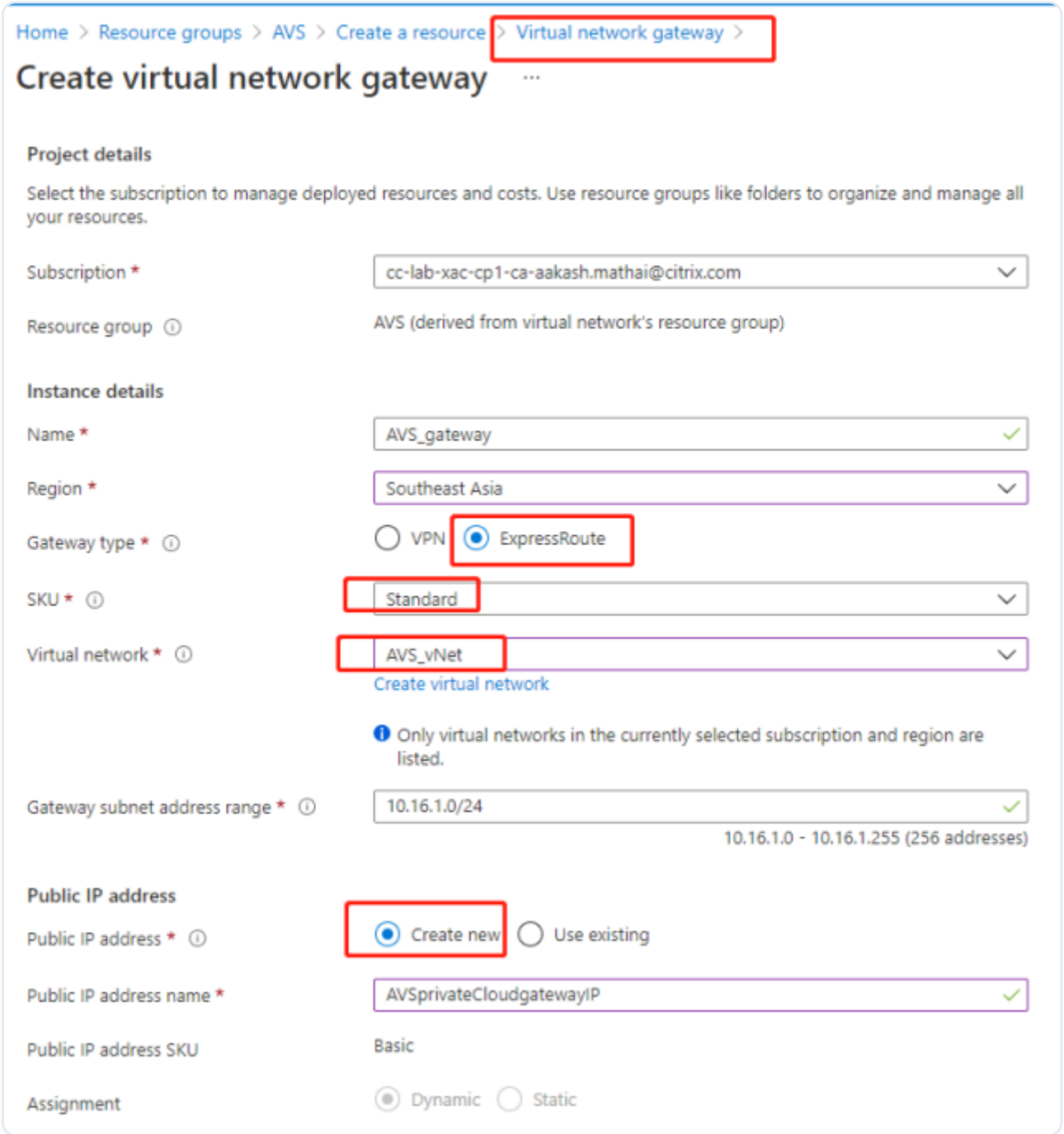
> 输入地址空间后：

1. 选择**+ 添加子网**。
2. 在**添加子网**页面上，为子网指定名称和适当的地址范围。
3. 单击**添加。**
4. 选择**审核 + 创建**。
5. 验证信息并单击**创建**。部署完成后，虚拟网络将显示在资源组中。

创建虚拟网络网关
创建虚拟网络后，创建虚拟网络网关。

1. 在您的资源组中，选择**+ 添加**以添加新资源。
2. 在“**搜索市场**”文本框中，键入 *虚拟网络网关*。找到虚拟网络资源并选择它。

3. 在“**虚拟网络网关**”页面上，单击“**创建**”。
4. 在“**创建虚拟网络网关**”页面上的“**基本信息**”选项卡中，为字段提供值。
5. 单击“**审查 + 创建**”。



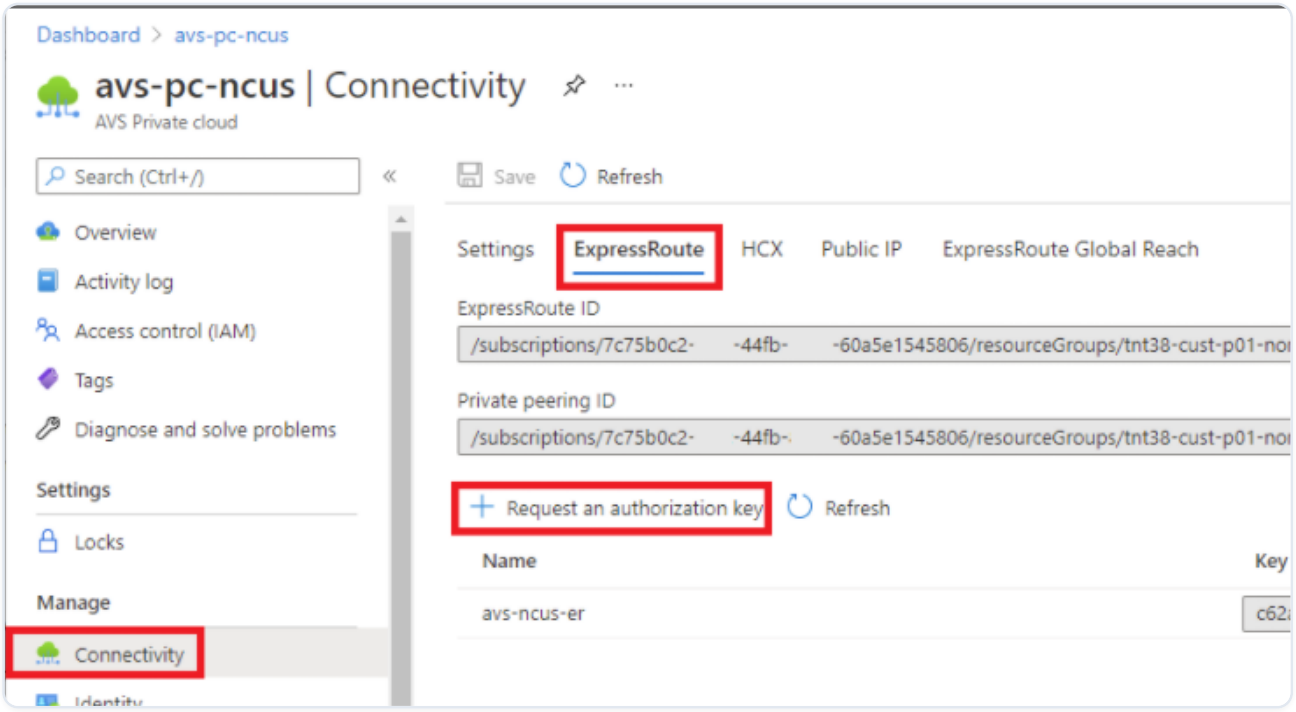

审查虚拟网络网关配置后，单击“**创建**”以部署虚拟网络网关。 部署完成后，将您的 **ExpressRoute** 连接连接到包含 Azure AVS 私有云的虚拟网络网关。

### 将 EXPRESSROUTE 连接到虚拟网络网关

部署虚拟网络网关后，在其与 Azure AVS 私有云之间添加连接：

1. 请求 ExpressRoute 授权密钥。

2. 在 Azure 门户中，导航到“**Azure VMware Solution 私有云**”。选择“**管理 > 连接 > ExpressRoute**”，然后选择“**+ 请求授权密钥**”。




请求授权密钥后：

1. 输入密钥名称，然后单击“**创建**”。创建密钥可能需要大约 30 秒。创建后，新密钥将显示在私有云的授权密钥列表中。
2. 复制 **授权密钥** 和 **ExpressRoute ID**。您将需要它们来完成对等过程。授权密钥会在一段时间后消失，因此请在它出现后立即复制。
3. 导航到您计划使用的**虚拟网络网关**，并选择“**连接 > + 添加**”。
4. 在“**添加连接**”页面上，提供字段值，然后选择“**确定**”。

Azure ASV 添加连接(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-avs-add-connection-v2.png)

连接已在您的 ExpressRoute 线路和您的虚拟网络之间建立：

Azure ASV 连接成功(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-avs-connection-succeeded.png)

### 配置适用于 AZURE VMWARE SOLUTION 的 DHCP

将 ExpressRoute 连接到虚拟网关后，配置 DHCP。
使用 NSX-T 托管您的 DHCP 服务器
在 NSX-T Manager 中：

1. 选择“**网络 > DHCP**”，然后选择“**添加服务器**”。

2. 对于“**服务器类型**”，选择“**DHCP**”，提供服务器名称和 IP 地址。
3. 单击 **保存**。
4. 选择“**第 1 层网关**”，选择第 1 层网关上的垂直省略号，然后选择“**编辑**”。
5. 选择“**未设置 IP 分配**”以添加子网。
6. 对于“**类型**”，选择“**DHCP 本地服务器**”。
7. 对于“**DHCP 服务器**”，选择“**默认 DHCP**”，然后单击“**保存**”。
8. 再次点击“**保存**”，然后选择“**关闭编辑**”。

Azure ASV 添加 NSX-T 服务器(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-avs-nsx-t-add-server.png)

### 在 AZURE VMWARE SOLUTION 中添加网络段

设置 DHCP 后，添加网络段。

要添加网络分段，请在 NSX-T Manager 中选择“**网络 > 分段**”，然后点击“**添加分段**”。

Azure ASV 添加 NSX-T 分段(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-avs-nsx-t-add-segment.png)

在“**分段配置文件**”屏幕中：

1. 输入该分段的**名称**。
2. 选择“**Tier-1 网关 (TNTxx-T1)**”作为“**连接的网关**”，并将“**类型**”保留为“**灵活**”。
3. 选择预配置的覆盖**传输区域 (TNTxx-OVERLAY-TZ)**。
4. 点击“**设置子网**”。

Azure ASV 添加 NSX-T 分段配置文件(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-avs-nsx-t-segment-profiles.png)

在“**子网**”部分中：

1. 输入网关 IP 地址。
2. 选择“**添加**”。

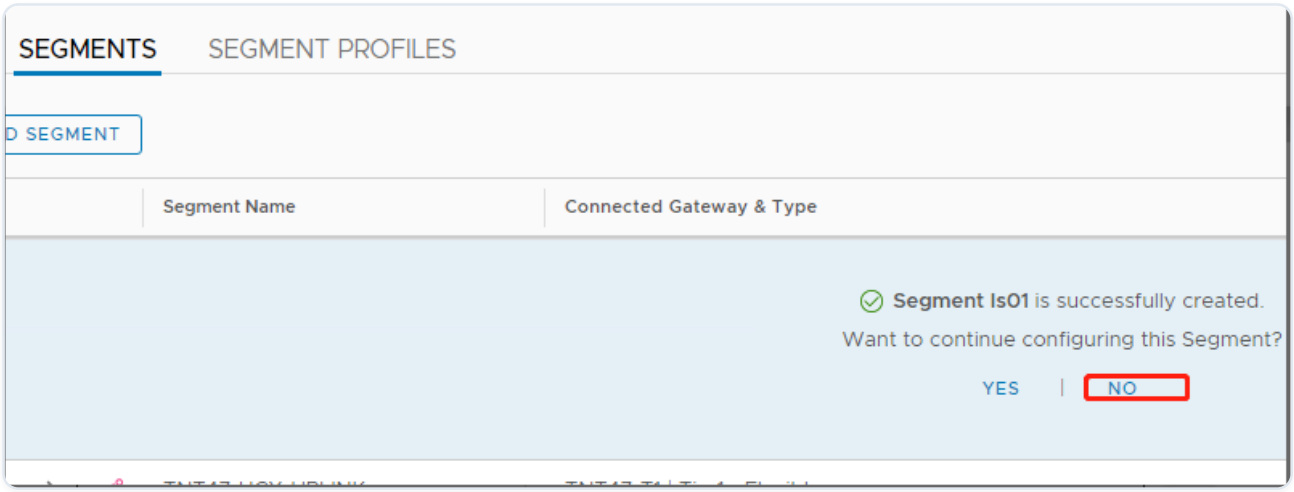
> **重要提示：**

> 此分段 IP 地址必须属于 Azure 网关 IP 地址，10.15.0.0/22。

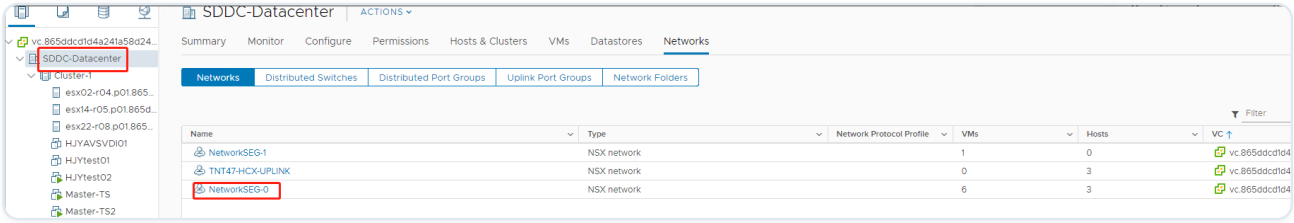
> DHCP 范围应属于网段 IP 地址：




选择 **否** 以拒绝继续配置分段的选项：




在 vCenter 中，选择 **网络 > SDDC-数据中心**：

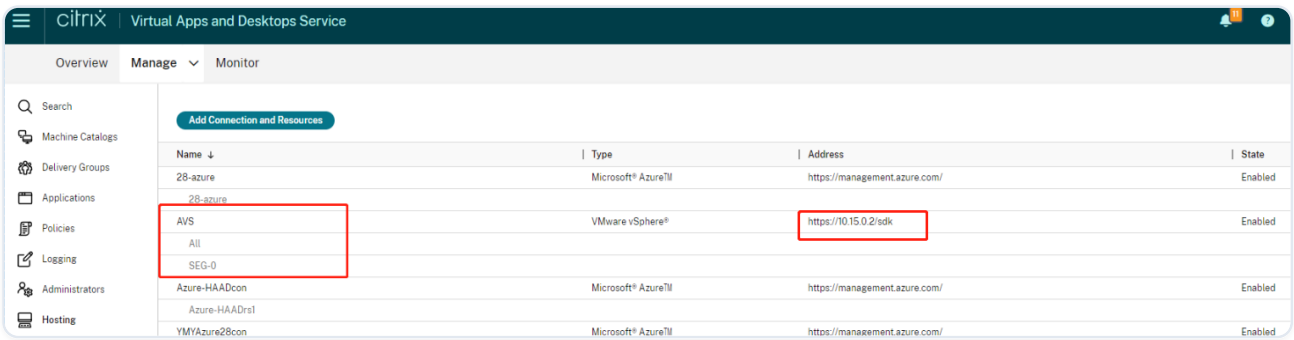



### 验证 AZURE AVS 环境

在 Azure 资源组中设置直接连接和连接器：

Azure ASV ASV 验证连接(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-avs-verify-connection-create-dc-v2.png)

使用 vCenter 凭据验证连接：



## 谷歌云 VMware 引擎

Citrix Virtual Apps and Desktops 允许您将基于 VMware 的本地 Citrix 工作负载迁移到 Google Cloud VMware Engine。

### 配置 谷歌云 VMware 引擎

以下过程介绍了如何在 Google Cloud VMware 引擎上获取和设置集群。

#### 访问 VMWARE ENGINE 门户

1. 在 **Google Cloud Console** 中，单击导航菜单。
2. 在 **计算** 部分中，单击 **VMware Engine** 以在新浏览器选项卡中打开 VMware Engine。

#### 创建第一个私有云的要求

您必须拥有 Google Cloud VMware Engine 的访问权限、可用的 VMware Engine 节点配额以及适当的 IAM 角色。在继续创建私有云之前，请准备以下要求：

1. 请求 API 访问权限和节点配额。有关详细信息，请参阅 请求 API 访问权限和配额。
2. 记下您要用于 VMware 管理设备和 HCX 部署网络的地址范围。有关详细信息，请参阅 网络要求。
3. 获取 VMware Engine Service 管理员 IAM 角色。

#### 创建您的第一个私有云

1. 访问 VMware Engine 门户。
2. 在 VMware Engine 主页上，单击 **创建私有云**。将列出托管位置和硬件节点类型。
3. 选择私有云的节点数。至少需要三个节点。
4. 为 VMware 管理网络输入一个无类别域间路由 (CIDR) 范围。
5. 为 HCX 部署网络输入一个 CIDR 范围。

> **重要提示：**
>
> CIDR 范围不得与您的任何本地或云子网重叠。CIDR 范围必须为 /27 或更高。

6. 选择 **审核并创建**。
7. 查看设置。要更改任何设置，请单击 **Back**。
8. 单击 **Create** 开始创建私有云。

当 VMware Engine 创建您的新私有云时，它会部署多个 VMware 组件并为私有云中的集群设置初始 Autoscale™ 策略。私有云创建可能需要 30 分钟到 2 小时。预配完成后，您会收到一封电子邮件。

### 设置 谷歌云 VMWARE ENGINE VPN 网关

要与 Google Cloud VMware Engine 建立初始连接，您可以使用 VPN 网关。这是一个基于 OpenVPN 的客户端 VPN，您可以使用它连接到您的 VMware 软件定义数据中心 (SDDC) vCenter 并执行任何所需的初始配置。

在部署 VPN 网关之前，请配置部署 SDDC 的区域的 **Edge Services** 范围。为此：

1. 登录 **Google Cloud VMware Engine** 门户，然后转到 **Network > Regional Settings**。单击 **Add Region**。
2. 选择部署 SDDC 的区域，并启用 **Internet Access** 和 **Public IP Service**。
3. 提供规划期间记录的 Edge Services 范围，然后单击 **Submit**。启用这些服务需要 10-15 分钟。

   完成后，Edge Services 在“区域设置”页面上显示为 **Enabled**。启用这些设置允许将公共 IP 分配给您的 SDDC，这是部署 VPN 网关的要求。

要部署 VPN 网关：

1. 在 **Google Cloud VMware Engine** 门户中，转到 **网络 > VPN 网关**。单击 **创建新的 VPN 网关**。
2. 提供 VPN 网关的名称以及规划期间保留的客户端子网。单击“**下一步**”。
3. 选择要授予 VPN 访问权限的用户。单击“**下一步**”。
4. 指定必须通过 VPN 访问的网络。单击“**下一步**”。
5. 将显示摘要屏幕。验证选择，然后单击“**提交**”以创建 VPN 网关。将显示 VPN 网关页面，其中新 VPN 网关的状态为“**正在创建**”。
6. 状态变为“**运行中**”后，单击新的 VPN 网关。
7. 单击“**下载我的 VPN 配置**”以下载包含 VPN 网关预配置 OpenVPN 配置文件的 ZIP 文件。提供了通过 UDP/1194 和 TCP/443 连接的配置文件。选择您的首选项并将其导入 Open VPN，然后连接。
8. 转到“**资源**”并选择您的 SDDC。

### 连接 VPN

1. 通过 VPN 网关设置在本地网络和私有云之间建立点到站点连接。请参阅 设置 Google Cloud VMware Engine VPN 网关。
2. 上传在 设置 Google Cloud VMware Engine VPN 网关 中下载的 VPN 配置。

3. 导入到您的 VPN 客户端，例如 OpenVPN Connect。

有关详细信息，请参阅 使用 VPN 连接。

#### 创建第一个子网

从 VMware Engine 门户访问 NSX-T Manager
创建子网的过程在 NSX-T 中进行，您可以通过 VMware Engine 访问 NSX-T。请执行以下操作以访问 NSX-T Manager。

1. 登录到 **Google Cloud VMware Engine** 门户。
2. 从主导航中，转到 **资源**。
3. 单击与要创建子网的私有云对应的 **私有云名称**。
4. 在私有云的详细信息页面上，单击 **vSphere Management Network** 选项卡。
5. 单击与 NSX-T Manager 对应的 **FQDN**。
6. 出现提示时，输入您的登录凭据。如果您已设置 vIDM 并将其连接到身份源（例如 Active Directory），请改用您的身份源凭据。

> **提醒：**
>
> 您可以从私有云详细信息页面检索生成的凭据。

为子网设置 DHCP 服务
在创建子网之前，请设置 DHCP 服务：

在 NSX-T Manager 中：

1. 转到 **网络 > DHCP**。网络仪表板显示 DHCP 服务创建了一个 Tier-0 和一个 Tier-1 网关。
2. 要开始预配 DHCP 服务器，请单击 **添加服务器**。
3. 对于“**服务器类型**”，选择“**DHCP**”，提供服务器名称和 IP 地址。
4. 单击 **保存** 以创建 DHCP 服务。

执行以下操作以将此 DHCP 服务附加到相关的 Tier-1 网关。DHCP 服务已预配了一个默认的 Tier-1 网关：

1. 选择“**第 1 层网关**”，选择第 1 层网关上的垂直省略号，然后选择“**编辑**”。
2. 在 **IP 地址管理** 字段中，选择 **未设置 IP 分配**。
3. 对于“**类型**”，选择“**DHCP 本地服务器**”。

4. 为 **DHCP 服务器** 选择您创建的 DHCP 服务器。
5. 单击 **保存**。
6. 单击 **关闭编辑**。

您现在可以在 NSX-T 中创建网络分段。有关 NSX-T 中 DHCP 的更多信息，请参阅 VMware DHCP 文档。

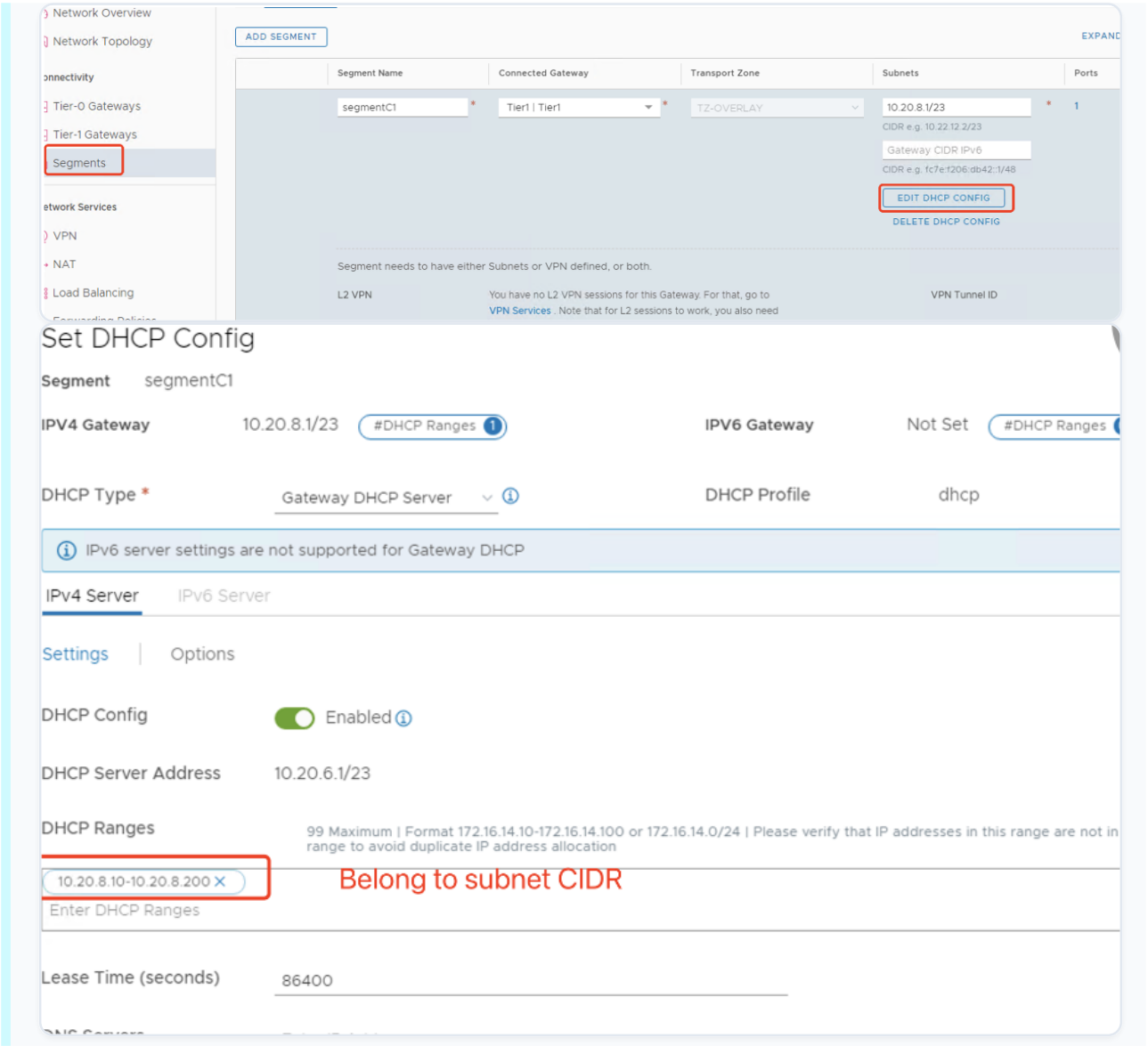
在 NSX-T 中创建网络分段

对于工作负载 VM，您可以为私有云创建作为 NSX-T 网络分段的子网：

1. 在 NSX-T Manager 中，转到 **网络 > 分段**。
2. 单击 **添加分段**。
3. 输入分段的名称。
4. 选择 **Tier-1** 作为 **连接的网关**，并将类型保留为 **灵活**。
5. 点击“**设置子网**”。
6. 单击 **添加子网**。
7. 在 **网关 IP/前缀长度** 中输入子网范围。将子网范围指定为以 **.1** 作为最后一个八位字节。例如，**10.12.2.1/24**。
8. 指定 DHCP 范围，然后单击 **添加**。
9. 在 **传输区域** 中，从下拉列表中选择 **TZ-OVERLAY**。
10. 单击 **保存**。现在，您可以在 vCenter 中创建 VM 时选择此网络段。

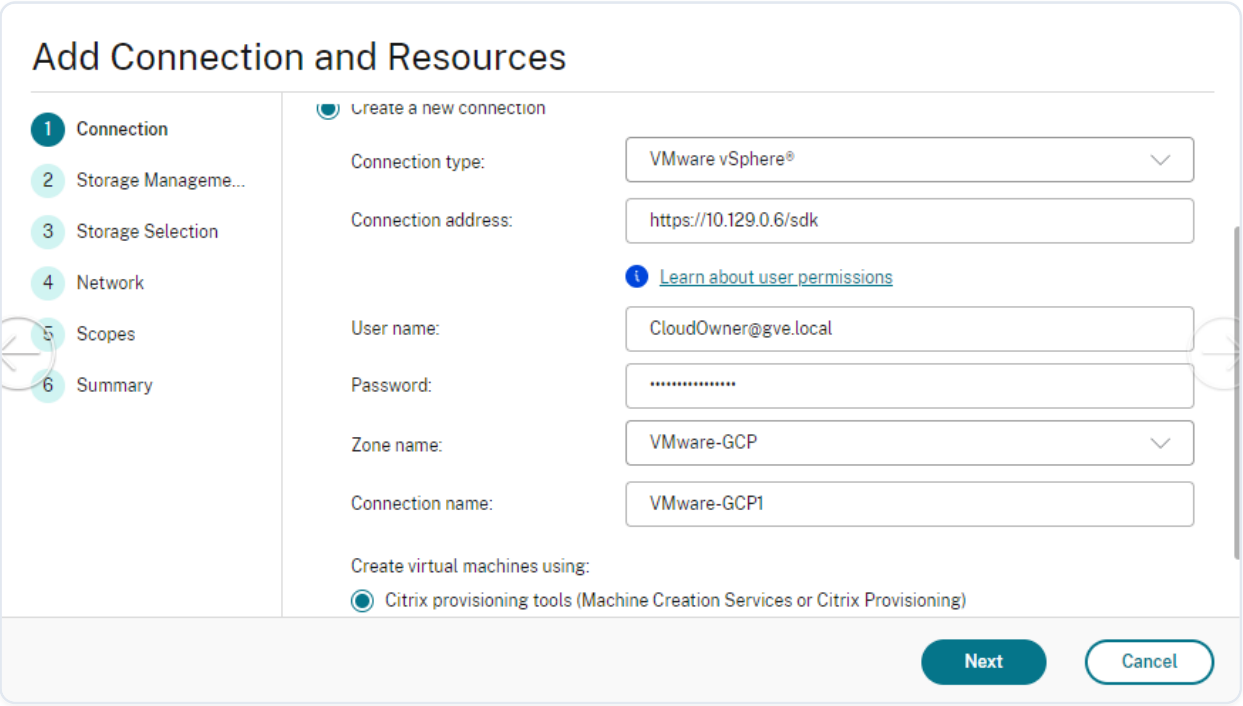
在给定区域中，您最多可以使用私有服务访问从 VMware Engine 设置 100 条到 VPC 网络的唯一路由。这包括（例如）私有云管理 IP 地址范围、NSX-T 工作负载网络段和 HCX 网络 IP 地址范围。此限制包括该区域中的所有私有云。

> **注意：**
>
> 存在一个 Google Cloud 配置问题，因此您需要多次配置 DHCP 范围设置。因此，请务必在 Google Cloud 配置后配置 DHCP 范围设置。单击 **编辑 DHCP 配置** 以配置 DHCP 范围。




## 在 CITRIX STUDIO 中创建 GOOGLE CLOUD VMWARE 连接

1. 在 vCenter 中创建计算机。
2. 启动 Citrix Studio 应用程序。
3. 选择托管节点，然后单击 **添加连接和资源**。
4. 在 **连接** 屏幕上，选择 **创建新连接**，并填写以下详细信息：




a. 选择 **连接类型** 为 **VMware vSphere**。

b. 在 **连接地址** 中，输入 vCenter 私有 IP 地址。

c. 输入 vCenter 凭据。

d. 输入连接名称。

e. 选择用于创建虚拟机的工具。

5. 在“**网络**”屏幕上，选择在 NSX-T 服务器中创建的子网。

6. 完成向导。

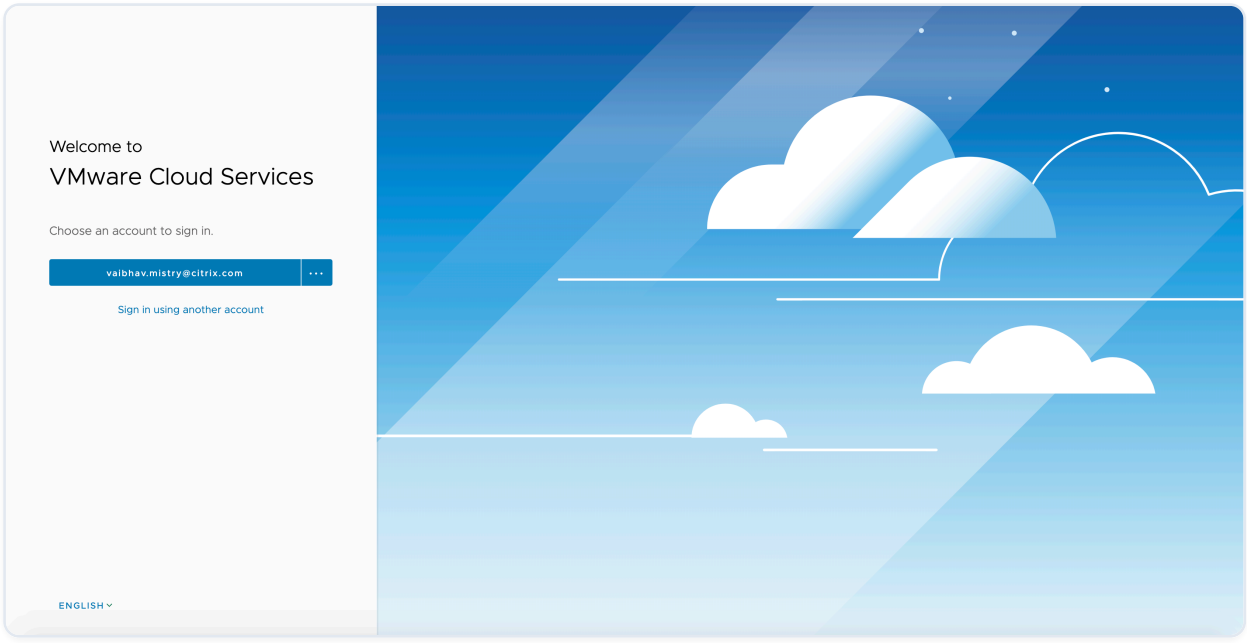
## 亚马逊网络服务 (AWS) 上的 VMware 云

Amazon Web Services (AWS) 上的 VMware Cloud 使您能够将基于 VMware 的本地 Citrix 工作负载迁移到 AWS Cloud。

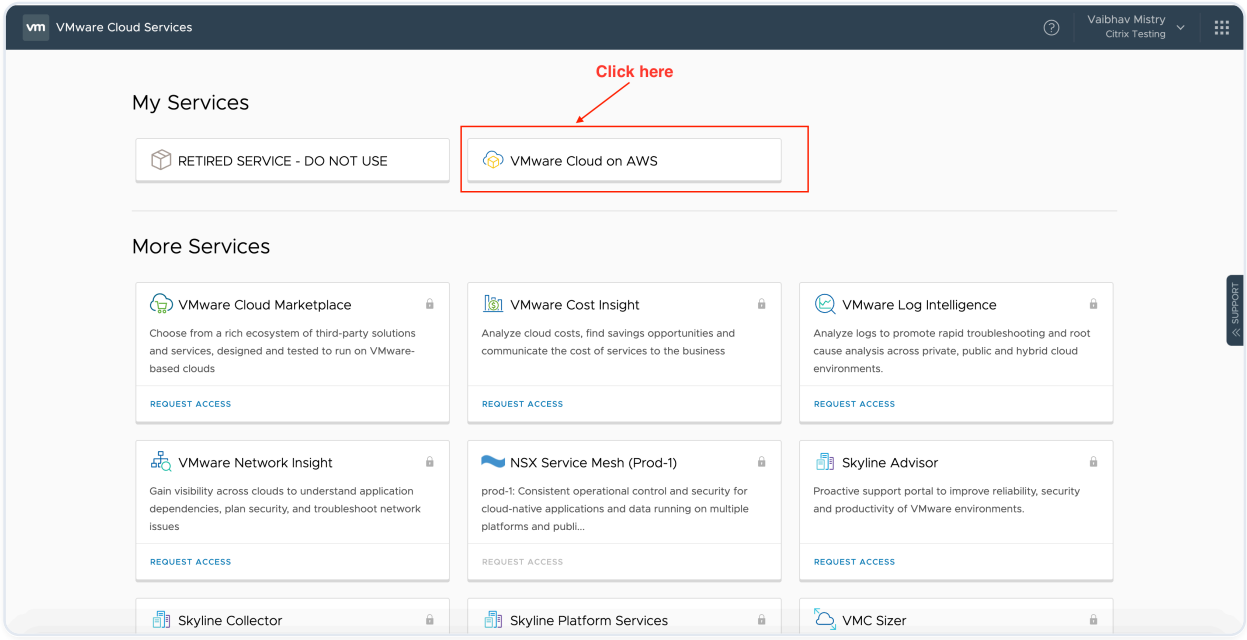
本文介绍了在 AWS 上设置 VMware Cloud 的过程。

### 访问 VMware Cloud 环境

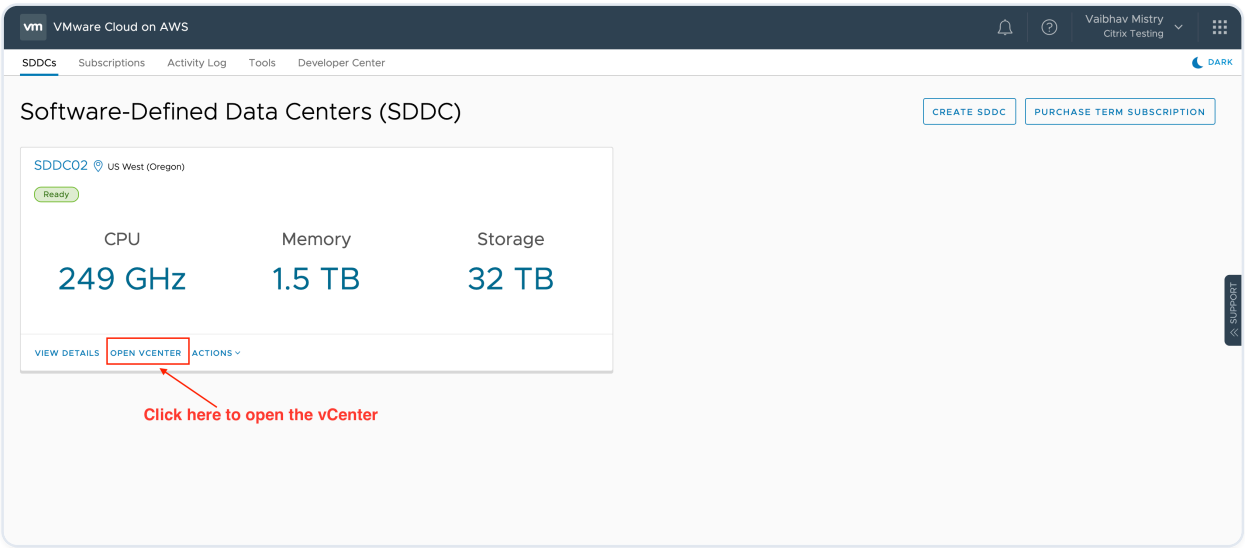
1. 使用 URL `<https://console.cloud.vmware.com/>` 登录到 VMware Cloud 服务。

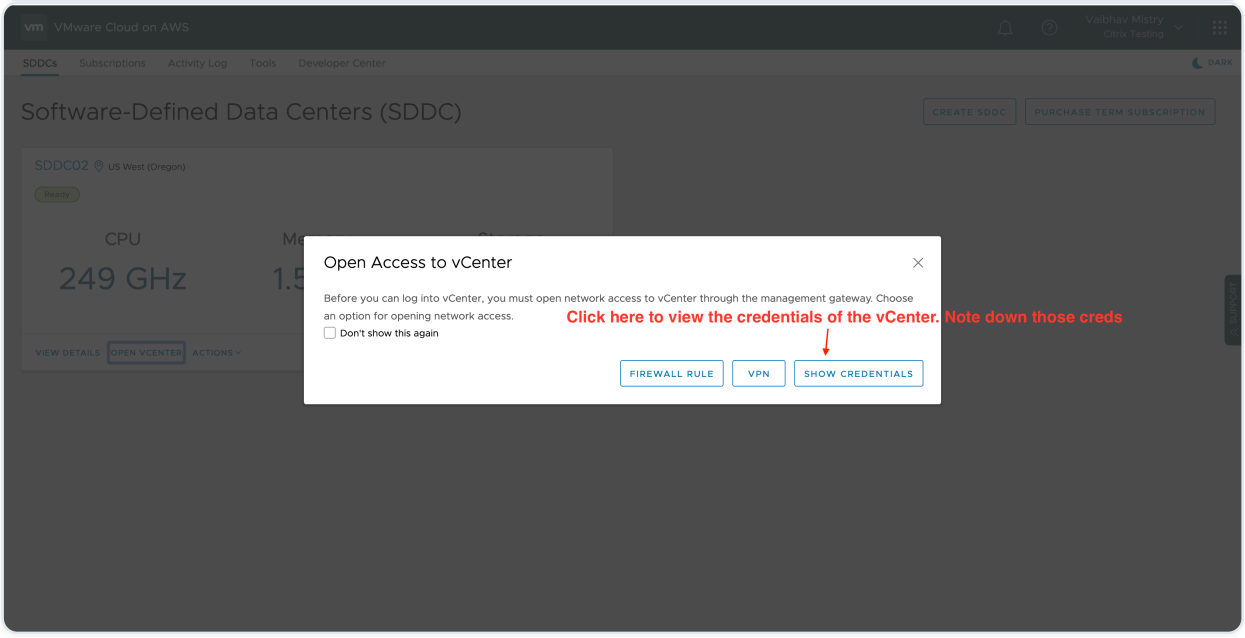



2. 单击**Amazon Web Services 上的 VMware Cloud**。将显示“软件定义数据中心 (SDDC)”页面。

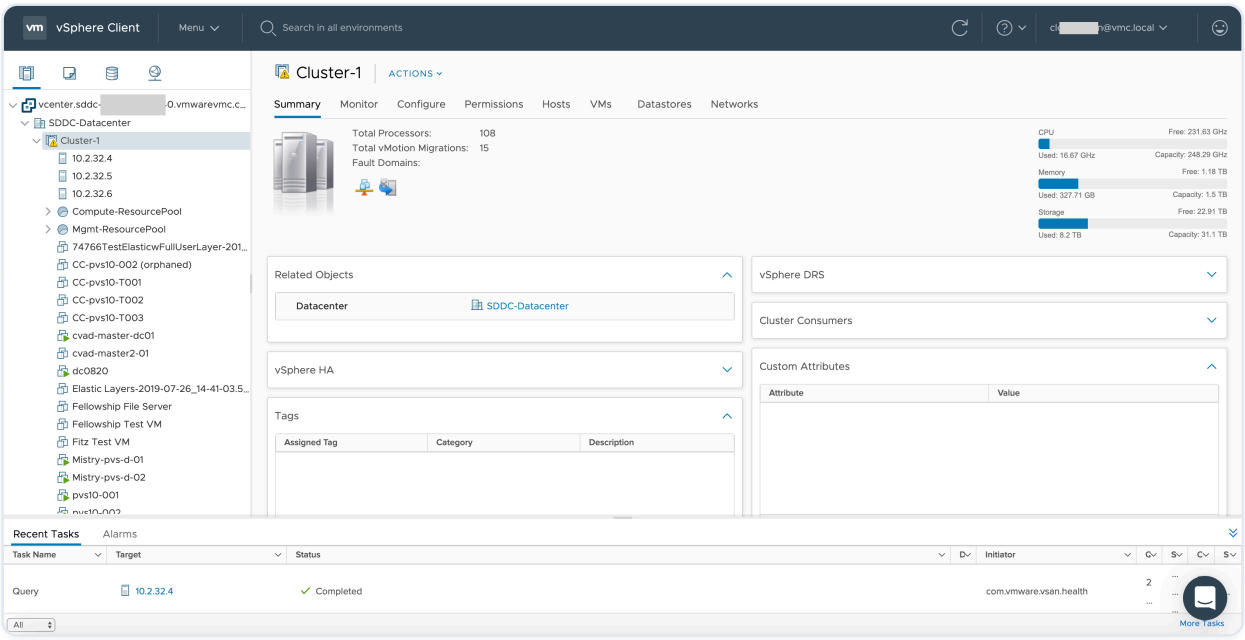



3. 单击**打开 VCENTER**，然后单击**显示凭据**。记下凭据以供以后使用。



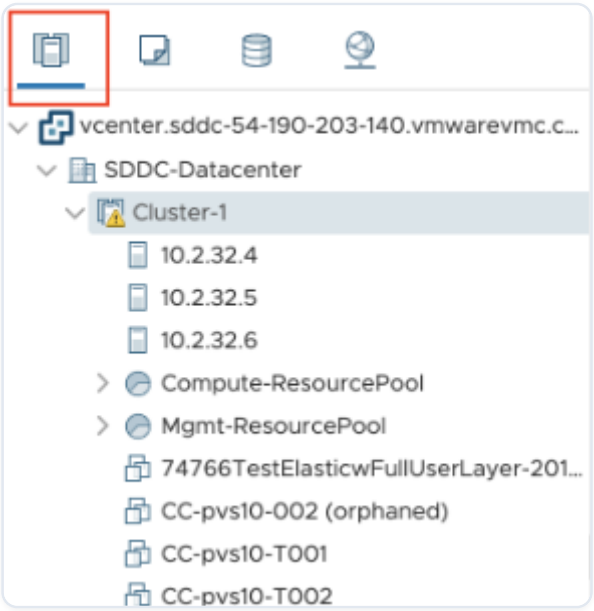

4. 打开 Web 浏览器并输入 vSphere Web Client 的 URL。
5. 输入所记录的凭据，然后单击“**登录**”。vSphere 客户端网页与本地环境类似。



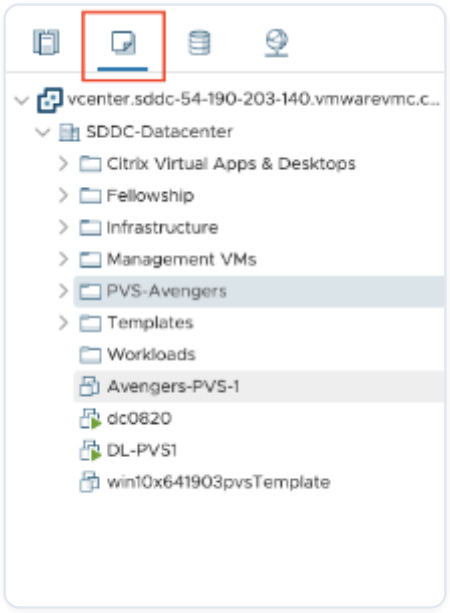

## 关于 VMware 云环境

vSphere 客户端网页上有四种视图。

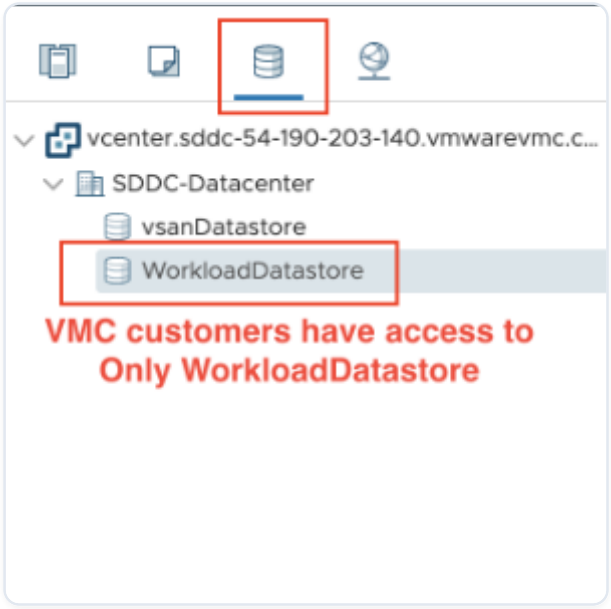
- 主机和群集视图：您无法创建新的群集，但云管理员可以创建多个资源池。



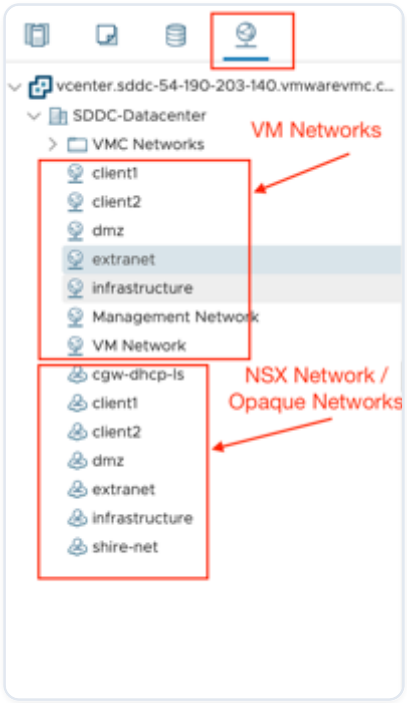

- VM 和模板视图：云管理员可以创建许多文件夹。




- 存储视图：在 Citrix Studio 中添加托管单元时，请选择 **WorkloadDatastore** 存储，因为您只能访问 Workload Datastore。




- 网络视图：VMware 云网络和不透明网络的图标不同。




设置群集后，请参阅 VMware 虚拟化环境 以添加连接和资源。

## AWS 云环境

本文将引导您设置 AWS 账户作为可与 Citrix Virtual Apps and Desktops 配合使用的资源位置。该资源位置包含一组基本组件，非常适合概念验证或其他不需要资源分散在多个可用区中的部署。完成这些任务后，您可以安装 VDA、预配计算机、创建计算机目录和创建交付组。

完成本文中的任务后，您的资源位置将包含以下组件：

- 一个虚拟私有云 (VPC)，其中包含单个可用区内的公共子网和私有子网。
- 一个实例，在 VPC 的私有子网中运行，既作为 Active Directory 域控制器又作为 DNS 服务器。
- 在 VPC 的公共子网中充当堡垒主机的实例。此实例用于启动到私有子网中实例的 RDP 连接，以进行管理。完成资源位置设置后，您可以关闭此实例，使其不再易于访问。当您必须管理私有子网中的其他实例（例如 VDA 实例）时，可以重新启动堡垒主机实例。

### 限制

从 Citrix Virtual Apps and Desktops 2203 LTSR 及更高版本开始，MCS AWS 插件进行 `DescribeInstanceTypes` AWS API 调用，如果成功，则 MCS 使用从 API 响应创建的清单名称。

因此，当您从 CVAD 1912 升级到 2203 或更高版本时，请禁用 AWS 上的 `DefineInstanceType` 权限，然后使用 `Set-ProvScheme` 命令更新现有目录以匹配 AWS 命名方案。然后，在目录更新完成且服务产品与 AWS 命名方案匹配后，重新添加 `DescribeInstanceType` 权限。

### 任务概述

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

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

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

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

### 任务 1：设置 VPC

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

### 任务 2：配置安全组

此任务为您的 VPC 创建并配置以下安全组：

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

要创建安全组：

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

### 配置公共安全组

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

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

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

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

5. 完成后，选择**保存**。

### 配置私有安全组

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

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

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

| 类型 | 目标 |
| --- | --- |
| 所有流量 | 选择私有安全组。 |
| 所有流量 | 0.0.0.0/0 |
| ICMP | 0.0.0.0/0 |
| UDP 53 (DNS) | 0.0.0.0/0 |

5. 完成后，选择**保存**。

### 任务 3：启动实例

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

1. 在 AWS 管理控制台中，选择 **EC2**。
2. 在 EC2 控制面板中，选择 **启动实例**。
3. 选择 Windows Server 计算机映像和实例类型。
4. 在“**配置实例详细信息**”页面上，为实例输入名称并选择您之前设置的 VPC。
5. 在 **子网** 中，为每个实例进行以下选择：
   - 堡垒主机：选择公共子网
   - 域控制器：选择私有子网
6. 在 **自动分配公有 IP 地址** 中，为每个实例进行以下选择：
   - 堡垒主机：选择“**启用**”。
   - 域控制器：选择“**使用默认设置**”或“**禁用**”。
7. 在 **网络接口** 中，输入您的私有子网 IP 范围内的主 IP 地址，供域控制器使用。
8. 如有必要，在 **添加存储** 页面上，修改磁盘大小。
9. 在 **标记实例** 页面上，为每个实例输入一个易记的名称。
10. 在 **配置安全组** 页面上，选择 **选择现有安全组**，然后为每个实例进行以下选择：
    - 堡垒主机：选择公有安全组。
    - 域控制器：选择私有安全组。
11. 查看您的选择，然后选择 **启动**。
12. 创建新的密钥对或选择现有密钥对。如果您创建新的密钥对，请下载您的私钥 (.pem) 文件并将其保存在安全位置。在获取实例的默认管理员密码时，您必须提供您的私钥。
13. 选择 **启动实例**。选择 **查看实例** 以显示您的实例列表。请等待新启动的实例通过所有状态检查后再访问它。
14. 获取每个实例的默认管理员密码：
    a. 从实例列表中，选择实例，然后选择 **连接**。
    b. 转到 **RDP 客户端** 选项卡，选择 **获取密码**，并在出现提示时上传您的私钥 (`.pem`) 文件。
    c. 选择 **Decrypt Password** 以获取人类可读的密码。AWS 会显示默认密码。

15. 重复步骤 2 中的步骤，直到您创建了两个实例：

    - 一个位于公共子网中的堡垒主机实例
    - 您的私有子网中的一个实例，用作域控制器。

### 任务 4：创建 DHCP 选项集

1. 在 VPC 控制面板中，选择 **DHCP Options Sets**。
2. 输入以下信息：

    - 名称标签：为该集输入一个易记的名称。
    - 域名：输入配置域控制器实例时使用的完全限定域名。
    - 域名服务器：输入分配给域控制器实例的私有 IP 地址和字符串 **AmazonProvidedDNS**，用逗号分隔。
    - NTP 服务器：将此字段留空。
    - NetBIOS 名称服务器：输入域控制器实例的私有 IP 地址。
    - NetBIOS 节点类型：输入 **2**。

3. 选择 **是，创建。**
4. 将新集与您的 VPC 关联：

    a. 在 VPC 控制面板中，选择 **您的 VPC**，然后选择您之前设置的 VPC。
    b. 选择 **操作 > 编辑 DHCP 选项集**。
    c. 出现提示时，选择您创建的新集，然后选择 **保存**。

### 任务 5：配置实例

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

    a. 选择 **开始 > 控制面板 > 网络和 Internet > 网络和共享中心 > 更改适配器设置**。双击显示的网络连接。
    b. 选择 **属性 > Internet 协议版本 4 (TCP/IPv4) > 属性**。
    c. 选择 **高级 > DNS**。确保以下设置已启用，然后选择 **确定**：

        - 在 DNS 中注册此连接的地址

- 在 DNS 注册中使用此连接的 DNS 后缀

4. 要配置域控制器：

   a. 使用服务器管理器，添加具有所有默认功能的 Active Directory 域服务角色。

   b. 将实例提升为域控制器。在提升过程中，启用 DNS 并使用创建 DHCP 选项集时指定的域名。出现提示时，重新启动实例。

### 创建连接

从 Studio 创建连接时：

- 您必须提供 API 密钥和秘密密钥值。您可以从 AWS 导出包含这些值的密钥文件，然后将其导入。您还必须提供区域、可用区、VPC 名称、子网地址、域名、安全组名称和凭据。
- 根 AWS 账户的凭据文件（从 AWS 控制台检索）的格式与为标准 AWS 用户下载的凭据文件不同。因此，Citrix Virtual Apps and Desktops 管理无法使用该文件填充 API 密钥和秘密密钥字段。确保您使用的是 AWS Identity Access Management (IAM) 凭据文件。

> **注意：**
>
> 创建连接后，更新 API 密钥和秘密密钥的尝试可能会失败。要解决此问题，请检查您的代理服务器或防火墙限制，并确保以下地址可访问：`https://*.amazonaws.com`。

#### 主机连接默认值

在 AWS 云环境中创建主机连接时，将显示以下默认值：

| 选项 | 绝对值 | 百分比 |
| --- | --- | --- |
| 并发操作（所有类型） | 125 | 100 |
| 每分钟最大新增操作数 | 125 | |

MCS 默认支持 100 个最大并发预配操作。

### 服务终结点 URL

#### 标准区域服务终端节点 URL

使用 MCS 时，将添加一个包含 API 密钥和 API 秘密的新 AWS 连接。借助此信息以及经过身份验证的帐户，MCS 使用 AWS DescribeRegions EC2 API 调用查询 AWS 以获取支持的区域。查询是使

用通用 EC2 服务端点 URL `https://ec2.amazonaws.com/` 进行的。使用 MCS 从支持的区域列表中为连接选择区域。首选的 AWS 服务端点 URL 会自动为该区域选择。但是，创建服务端点 URL 后，您将无法再设置或修改该 URL。

### AWS 租用

AWS 提供以下租用选项：共享租用（默认类型）和专用租用。共享租用意味着来自不同客户的多个 Amazon EC2 实例可能驻留在同一物理硬件上。专用租用意味着您的 EC2 实例仅在您部署的其他实例所在的硬件上运行。其他客户不使用同一块硬件。

您可以使用 MCS 通过 PowerShell 预配 AWS 专用主机。

#### 使用 PowerShell 配置 AWS 专用主机租用

您可以通过 PowerShell 创建具有主机租用定义的计算机目录。

Amazon 专用主机是具有 实例容量的物理服务器，该容量完全专用，允许您使用现有的按插槽或按 VM 软件许可证。

专用主机具有基于实例类型的预设利用率。例如，单个分配的 C4 Large 实例类型的专用主机仅限于运行 16 个实例。有关详细信息，请参阅 AWS 站点。

预配到 AWS 主机的要求包括：

- 导入的 BYOL（自带许可证）映像 (AMI)。对于专用主机，请使用和管理您现有的许可证。
- 具有足够利用率的专用主机分配，以满足预配请求。
- 启用 **自动放置**。

要使用 PowerShell 预配到 AWS 中的专用主机，请使用 **New-ProvScheme** cmdlet，并将 TenancyType 参数设置为 *Host*。

有关详细信息，请参阅 Citrix 开发人员文档。

### AWS 实例属性捕获

在 AWS 中使用 Machine Creation Services (MCS) 创建目录以预配计算机时，您需要选择一个 AMI 来表示该目录的主/黄金映像。MCS 会从该 AMI 使用磁盘快照。在以前的版本中，如果您希望在计算机上设置角色或标签，则需要使用 AWS 控制台单独进行设置。此功能默认启用。

> **提示：**
>
> 要使用 AWS 实例属性捕获，您必须有一个与 AMI 关联的 VM。

> 为了改进此过程，**MCS 会读取**从中获取 AMI 的实例的属性，并将该计算机的 Identity Access Management (IAM) 角色和标签应用于为给定目录预配的计算机。使用此可选功能时，目录创建过程会查找选定的 AMI 源实例，读取一组有限的属性。然后，这些属性存储在 AWS 启动模板中，该模板用于为该目录预配计算机。目录中的任何计算机都将继承捕获的实例属性。

捕获的属性包括：

- IAM 角色 – 应用于预配的实例。
- 标签 - 应用于预配的实例、其磁盘和 NIC。这些标签应用于瞬态 Citrix® 资源，包括：S3 存储桶和对象、卷和辅助资源，以及 AMI、快照和启动模板。

> **提示：**

> 瞬态 Citrix 资源的标记是可选的，可以使用自定义属性 `AwsOperationalResourcesTagging` 进行配置。

#### 捕获 AWS 实例属性

您可以通过在为 AWS 托管连接创建预配方案时指定自定义属性 `AwsCaptureInstanceProperties` 来使用此功能：

```
New-ProvScheme -CustomProperties “AwsCaptureInstanceProperties,true” …<standard provscheme parameters
```

有关详细信息，请参阅 Citrix 开发人员文档。

### 应用 AWS 实例属性并标记操作资源

在 AWS 中使用 MCS 创建目录以预配计算机时，您可以控制是否将 IAM 角色和标签属性应用于这些计算机。您还可以控制是否将计算机标签应用于操作资源。

### AWS 操作资源标记

Amazon Machine Image (AMI) 表示一种虚拟设备类型，用于在 Amazon 云环境（通常称为 EC2）中创建虚拟机。您可以使用 AMI 部署使用 EC2 环境的服务。当您创建目录以使用 MCS for AWS 预配计算机时，您选择 **AMI** 作为该目录的黄金映像。

> **重要提示：**

> 要使用操作资源标记，需要通过捕获实例属性和启动模板来创建目录。

> 要创建 AWS 目录，您必须首先为您希望作为黄金映像的实例创建 AMI。MCS 从该实例读取标签并将其合并到启动模板中。然后，启动模板标签将应用于在您的 AWS 环境中创建的所有 Citrix 资源，包括：

- 虚拟机
- VM 磁盘
- VM 网络接口
- S3 存储桶
- S3 对象
- 启动模板
- AMI

#### 标记操作资源

要使用 PowerShell 标记资源，请执行以下操作：

1. 从 DDC 主机打开 PowerShell 窗口。
2. 运行命令 `asnp citrix` 以加载 Citrix 特定的 PowerShell 模块。

要为预配的 VM 标记资源，请使用新的自定义属性 `AwsOperationalResourcesTagging`。此属性的语法为：

```
New-ProvScheme -CustomProperties “AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true” …<standard provscheme parameters>
```

### 定义 IAM 权限

使用本节中的信息定义 Citrix DaaS 在 AWS 上的 IAM 权限。Amazon 的 IAM 服务允许拥有多个用户的账户，这些用户可以进一步组织成组。这些用户可以拥有不同的权限来控制其执行与账户相关的操作的能力。有关 IAM 权限的更多信息，请参阅 IAM JSON policy reference。

要将 IAM 权限策略应用于新的用户组：

1. 登录 AWS 管理控制台，然后从下拉列表中选择 **IAM service**。
2. 选择 **创建新的用户组**。
3. 为新的用户组键入名称，然后选择 **继续**。
4. 在“**权限**”页面上，选择“**自定义策略**”。选择“**选择**”。
5. 为“**权限策略**”键入名称。

6. 在“**策略文档**”部分中，输入相关权限。

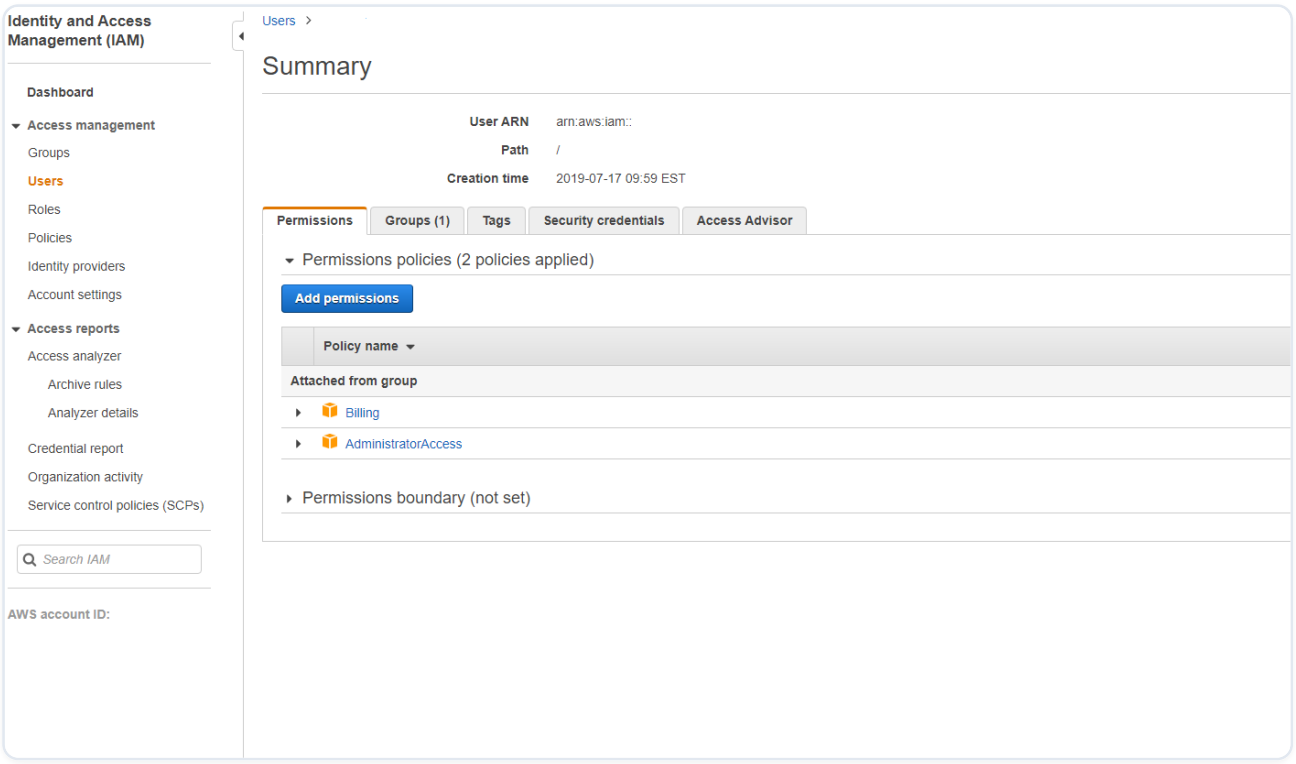
输入策略信息后，选择**Continue**以完成用户组。组中的用户被授予权限，只能执行 Citrix DaaS 所需的操作。

> **重要提示：**
>
> 使用上面示例中提供的策略文本列出 Citrix DaaS 用于在 AWS 账户中执行操作而无需将这些操作限制到特定资源的那些操作。Citrix 建议您将此示例用于测试目的。对于生产环境，您可能选择对资源添加进一步的限制。

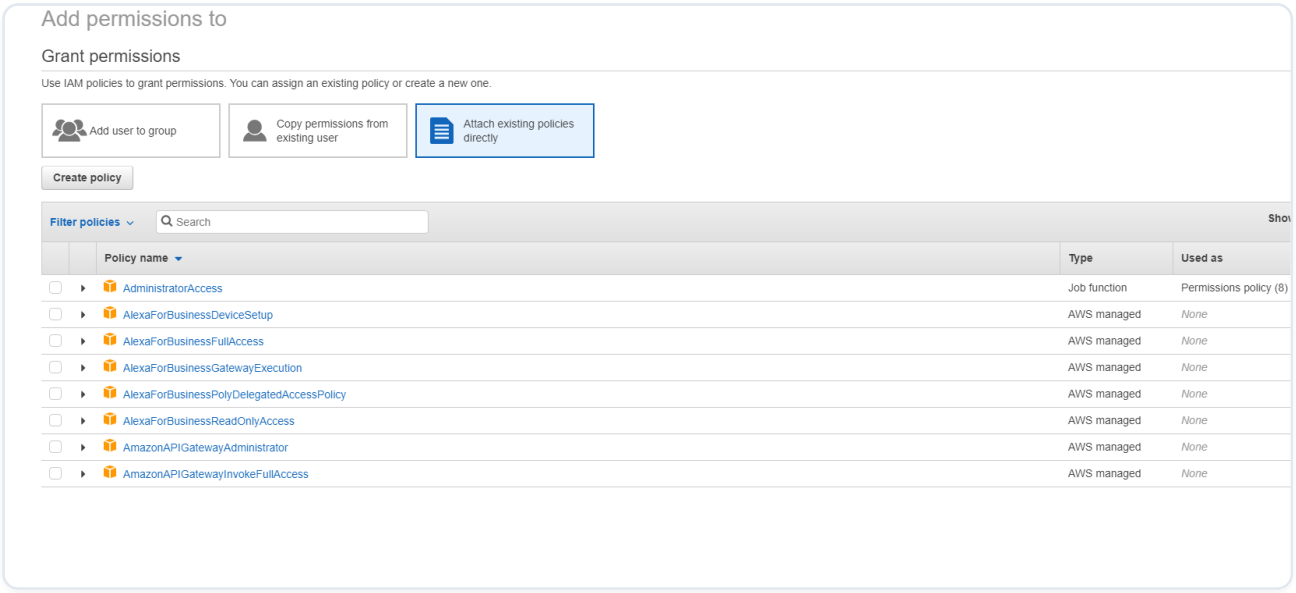
### 添加 IAM 权限

在 AWS Management Console 的“**IAM**”部分中设置权限：

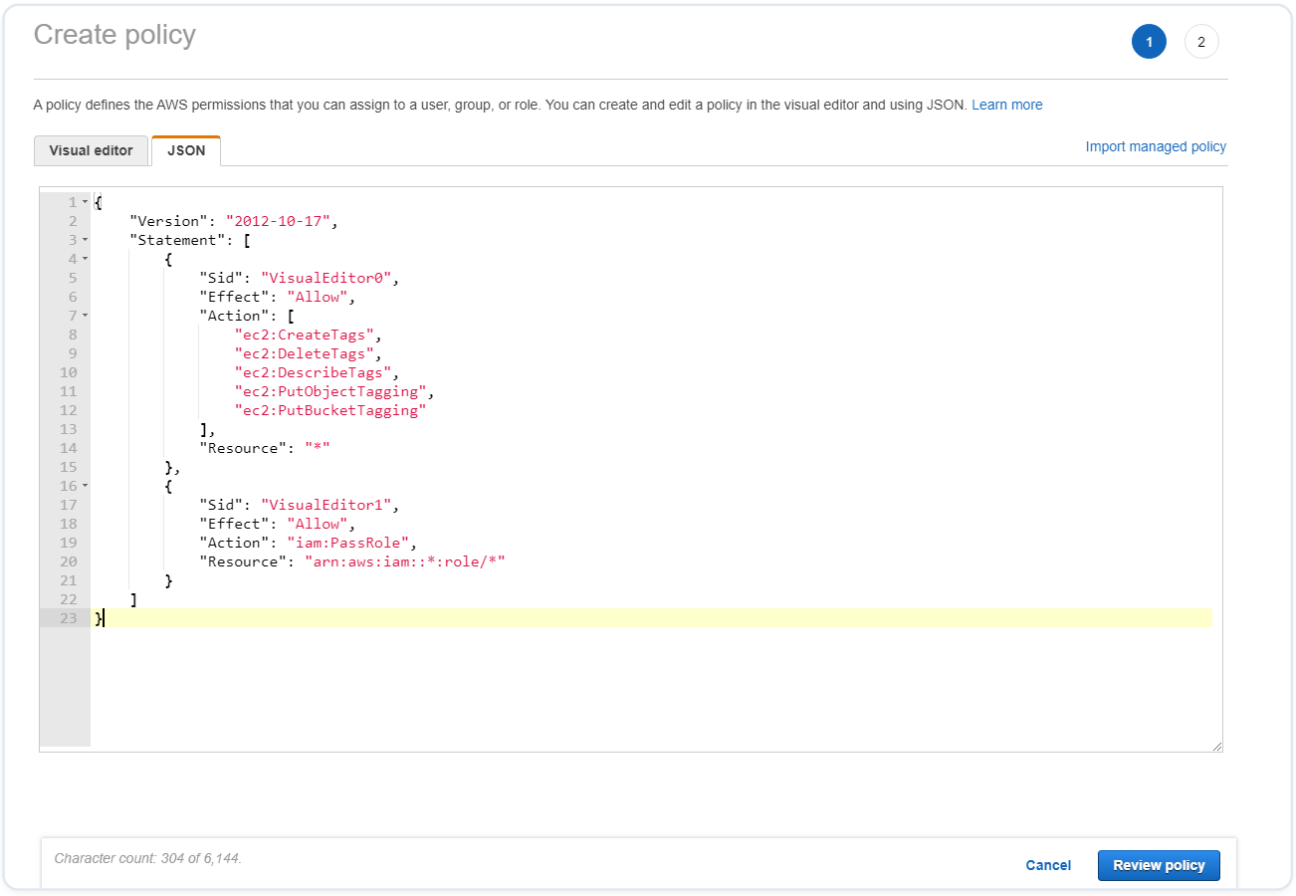
1. 在“**摘要**”面板中，选择“**权限**”选项卡。
2. 选择“**添加权限**”。




在 **添加权限到** 屏幕中，授予权限：




在 **JSON** 选项卡中，使用以下内容作为示例：




**提示：**

所提及的 JSON 示例可能不包含您的环境所需的所有权限。有关详细信息，请参阅 如何在 AWS 上运行 Citrix Virtual Apps and Desktops 时定义身份和访问管理权限。

## 关于 AWS 权限

本节包含 AWS 权限的完整列表。

> **注意：**
>
> *iam:PassRole* 权限仅在 **role_based_auth** 中需要。

### 创建主机连接

使用从 AWS 获取的信息添加新的主机连接。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeLaunchTemplates"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

**虚拟机电源管理**

虚拟机实例已开机或关机。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DetachVolume",
                "ec2:StartInstances",
                "ec2:StopInstances"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

**创建、更新或删除虚拟机**

创建、更新或删除计算机目录，其中 VM 作为 AWS 实例进行预配。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
```

```
                "ec2:CreateVolume",

                "ec2:DeleteVolume",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                “ec2:DescribeIamInstanceProfileAssociations”,

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",

                "ec2:RunInstances",

                "ec2:StartInstances",
```

```
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
```

```
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
```

```
        }

    ]

}
```

**注意：**

仅当在目录创建期间必须为准备 VM 创建隔离安全组时，才需要与 SecurityGroups 相关的 EC2 部分。完成此操作后，不再需要这些权限。

#### 直接磁盘上传和下载

直接磁盘上传消除了计算机目录预配对卷工作程序的要求，而是使用 AWS 提供的公共 API。此功能降低了与额外存储帐户相关的成本以及维护卷工作程序操作的复杂性。

必须将以下权限添加到策略中：

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

**重要提示：**

- 您可以将新 VM 添加到现有计算机目录，而无需任何卷工作程序操作，例如卷工作程序 AMI 和卷工作程序 VM。
- 如果删除以前使用卷工作程序的现有目录，则所有工件（包括与卷工作程序相关的工件）都将被删除。

### EBS 加密已创建的卷

如果 AMI 已加密，或者 EBS 配置为加密所有新卷，则 EBS 可以自动加密新创建的卷。但是，要实现此功能，IAM 策略中必须包含以下权限。

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
    ]
}
```

**注意：**

用户可以自行决定通过包含资源和条件块来将权限限制为特定密钥。例如，**带条件的 KMS 权限**：

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
```

```
                }

            }

        }

    ]

}
```

以下密钥策略语句是 KMS 密钥的整个默认密钥策略，它允许帐户使用 IAM 策略委托 KMS 密钥上的所有操作 (kms:*) 权限。

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",

"Resource": ""

}
```

有关详细信息，请参阅 AWS Key Management Service 官方文档。

**基于 IAM 角色的身份验证**

添加以下权限以支持基于角色的身份验证。

```
{

     "Version": "2012-10-17",

     "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
    ]
}
```

**最小 IAM 权限策略**

以下 JSON 可用于所有当前支持的功能。您可以使用此策略创建主机连接、创建、更新或删除 VM 以及执行电源管理。 该策略可以按照 定义 IAM 权限 部分中的说明应用于用户，或者您也可以使用 **role_based_auth** 安全密钥和秘密密钥进行基于角色的身份验证。

**重要提示：**

要使用 **role_based_auth**，请在设置云连接器时，首先在云连接器 EC2 实例上配置所需的 IAM 角色。使用 Citrix Studio 添加托管连接，并为身份验证密钥和秘密提供 role_based_auth。具有这些设置的托管连接随后将使用基于角色的身份验证。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
```

```
                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateNetworkInterface",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteLaunchTemplate",

                "ec2:DeleteNetworkInterface",

                "ec2:DeleteSecurityGroup",

                "ec2:DeleteSnapshot",

                "ec2:DeleteTags",

                "ec2:DeleteVolume",

                "ec2:DeregisterImage",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",
```

```
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
```

```
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:CreateSecurityGroup",
            "ec2:DeleteSecurityGroup",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupIngress"
        ],
        "Effect": "Allow",
        "Resource": "*"
    },
    {
        "Action": [
            "s3:CreateBucket",
            "s3:DeleteBucket",
            "s3:DeleteObject",
            "s3:GetObject",
            "s3:PutBucketAcl",
            "s3:PutObject",
            "s3:PutBucketTagging",
            "s3:PutObjectTagging"
        ],
        "Effect": "Allow",
        "Resource": "arn:aws:s3:::citrix*"
```

```
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
```

```
                "kms:ReEncryptFrom"

            ],

            "Resource": "*"

        },

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

**注意：**

- 仅当在目录创建期间必须为准备 VM 创建隔离安全组时，才需要与 SecurityGroups 相关的 EC2 部分。完成此操作后，不再需要这些权限。
- 仅在使用 EBS 卷加密时才需要 KMS 部分。
- iam:PassRole 权限部分仅在 **role_based_auth** 中需要。
- 可以根据您的要求和环境添加特定的资源级权限，而不是完全访问权限。有关更多详细信息，请参阅 AWS 文档 揭秘 EC2 资源级权限 和 AWS 资源访问管理。

### 更多信息

- 连接和资源
- 创建计算机目录

# Google Cloud 环境

Citrix Virtual Apps and Desktops™ 允许您在 Google Cloud 上预配和管理计算机。本文将引导您使用 Machine Creation Services (MCS) 在 Citrix Virtual Apps 或 Citrix Virtual Desktops 服务部署中预配虚拟机。

## 要求

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

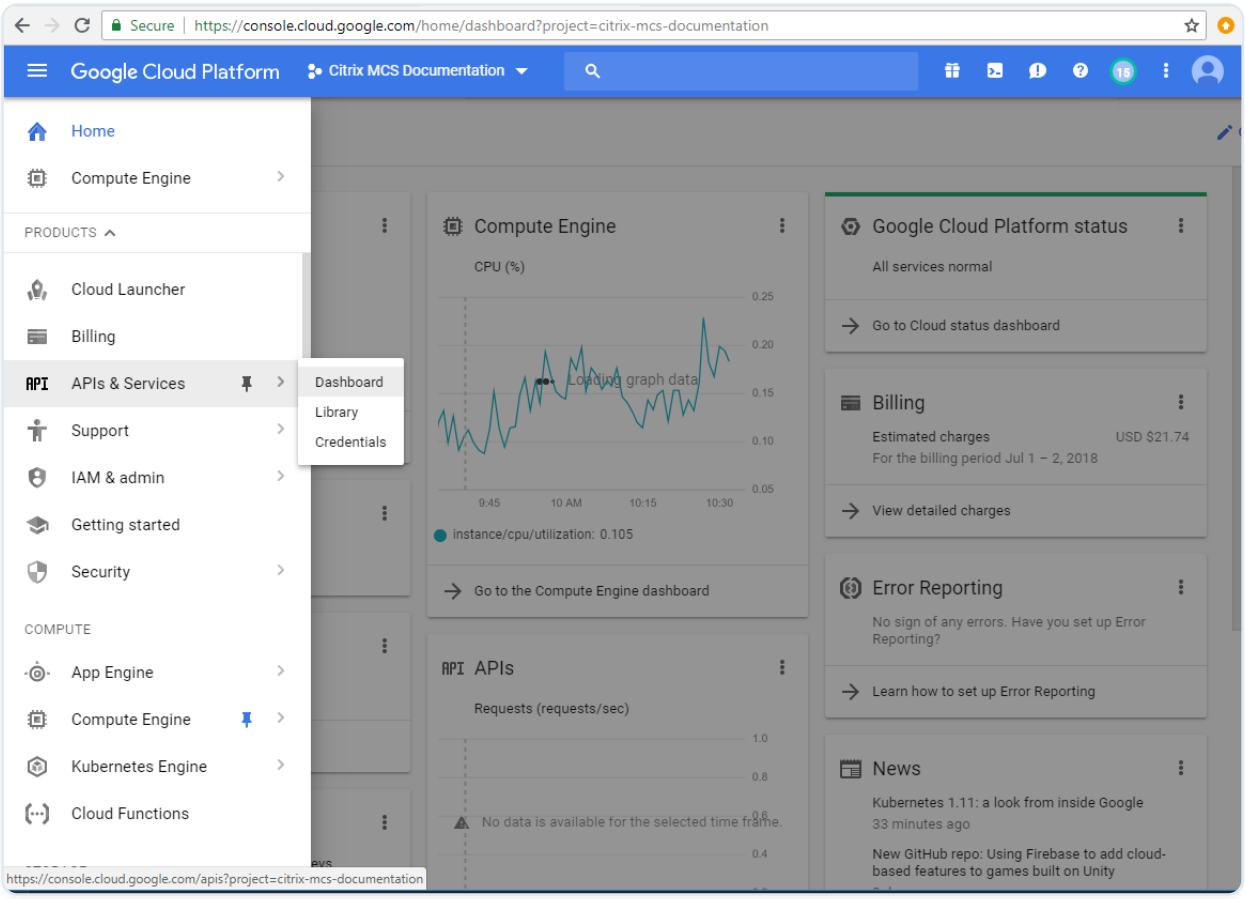
## 启用 Google Cloud API

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

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

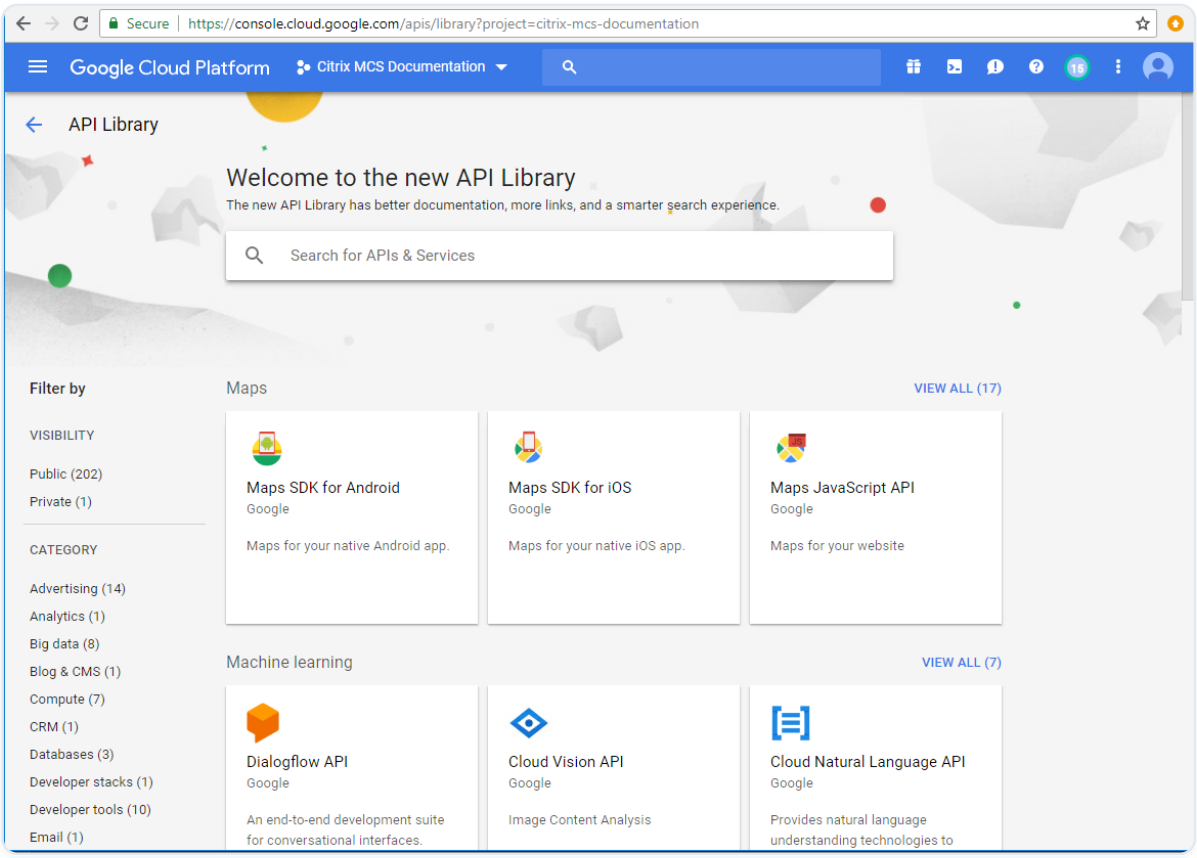
在 Google Cloud 控制台中，完成以下步骤：

1. 在左上角菜单中，选择 **API 和服务 > 控制面板**。




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

   a. 导航到**API 和服务 > 库**。



b. 在搜索框中，键入 *Compute Engine*。

c. 从搜索结果中，选择**Compute Engine API**。

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

3. 启用云资源管理器 API。

a. 导航到**API 和服务 > 库**。

b. 在搜索框中，键入 *Cloud Resource Manager*。

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

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

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

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

1. 打开 Google 控制台并加载 Cloud Shell。
2. 在 Cloud Shell 中运行以下四个命令：

- 启用计算服务：gcloud services enable compute.googleapis.com
- 启用云资源管理器服务：gcloud services enable cloudresourcemanager.googleapis.com
- gcloud 服务 启用 iam.googleapis.com
- gcloud 服务 启用 cloudbuild.googleapis.com

3. 如果 Cloud Shell 提示，请单击**授权**。

### 配置和更新服务帐号

> **注意：**
>
> CP 正在引入对 Cloud Build Service 默认行为和服务帐户使用方式的更改，这些更改将于 April 29, 2024 之后生效。有关详细信息，请参阅 Cloud Build Service Account Change。您在 April 29, 2024 之前启用了 Cloud Build API 的现有 Google 项目不受此更改的影响。但是，如果您希望在 April 29 之后仍保留现有的 Cloud Build Service 行为，则可以在启用 Cloud Build API 之前创建或应用组织策略以禁用约束实施。因此，以下内容分为两部分：Before April 29, 2024 和 After April 29, 2024。如果您设置了新的组织策略，请遵循 Before April 29, 2024 部分。

**April 29, 2024 之前**

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

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

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

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

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

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

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

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

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

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

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

#### 创建 CITRIX CLOUD 服务帐号

要创建 Citrix Cloud 服务帐号，请执行以下步骤：

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

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

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

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

   Cloud KMS 加密操作员需要以下权限：

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

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

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

**注意事项：**

创建服务帐户时，请考虑以下事项：

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

#### CITRIX CLOUD 服务帐户密钥

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

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

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

#### 向 CITRIX CLOUD 服务帐号添加角色

要向 Citrix Cloud 服务帐号添加角色，请执行以下操作：

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

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

#### 向 CLOUD BUILD 服务帐号添加角色

要向 Cloud Build 服务帐号添加角色，请执行以下操作：

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

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

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

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

> **注意：**
>
> 启用所有 API 以获取完整的角色列表。

**April 29, 2024 之后**

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

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

  您必须手动创建此服务帐号。

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

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

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

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

  验证是否已向服务帐号授予以下角色。

- Cloud Build 服务帐户
- 计算实例管理员
- 服务帐号用户

### 创建 CITRIX CLOUD 服务帐号

要创建 Citrix Cloud 服务帐号，请执行以下步骤：

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

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

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

   Cloud KMS 加密操作员需要以下权限：

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

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

5. 单击“**继续**”

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

**注意事项：**

创建服务帐户时，请考虑以下事项：

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

### CITRIX CLOUD 服务帐户密钥

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

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

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

### 向 CITRIX CLOUD 服务帐号添加角色

要向 Citrix Cloud 服务帐号添加角色，请执行以下操作：

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

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

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

#### 向 CLOUD COMPUTE 服务帐号添加角色

要向 Cloud Compute 服务帐号添加角色，请执行以下操作：

1. 在 Google Cloud 控制台中，导航到 **IAM 和管理 > IAM**。
2. 在 **IAM** 页面上，找到 Cloud Compute 服务帐号，该帐号可通过以 **项目 ID** 和单词 **compute** 开头的电子邮件地址进行识别。

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

> **注意：**
>
> 启用所有 API 以获取完整的角色列表。

#### 存储权限和存储桶管理

Citrix DaaS 改进了 Google Cloud 服务 的云构建失败报告流程。此服务在 Google Cloud 上运行构建。Citrix DaaS 创建一个名为 `citrix-mcs-cloud-build-logs-{region}-{5 random characters}` 的存储桶，Google Cloud 服务在此存储桶中捕获构建日志信息。此存储桶上设置了一个选项，可在 30 天后删除内容。此过程要求用于连接的服务帐号具有设置为 `storage.buckets.update` 的 Google Cloud 权限。如果服务帐号没有此权限，Citrix DaaS 将忽略错误并继续执行目录创建过程。如果没有此权限，构建日志的大小会增加，并且需要手动清理。

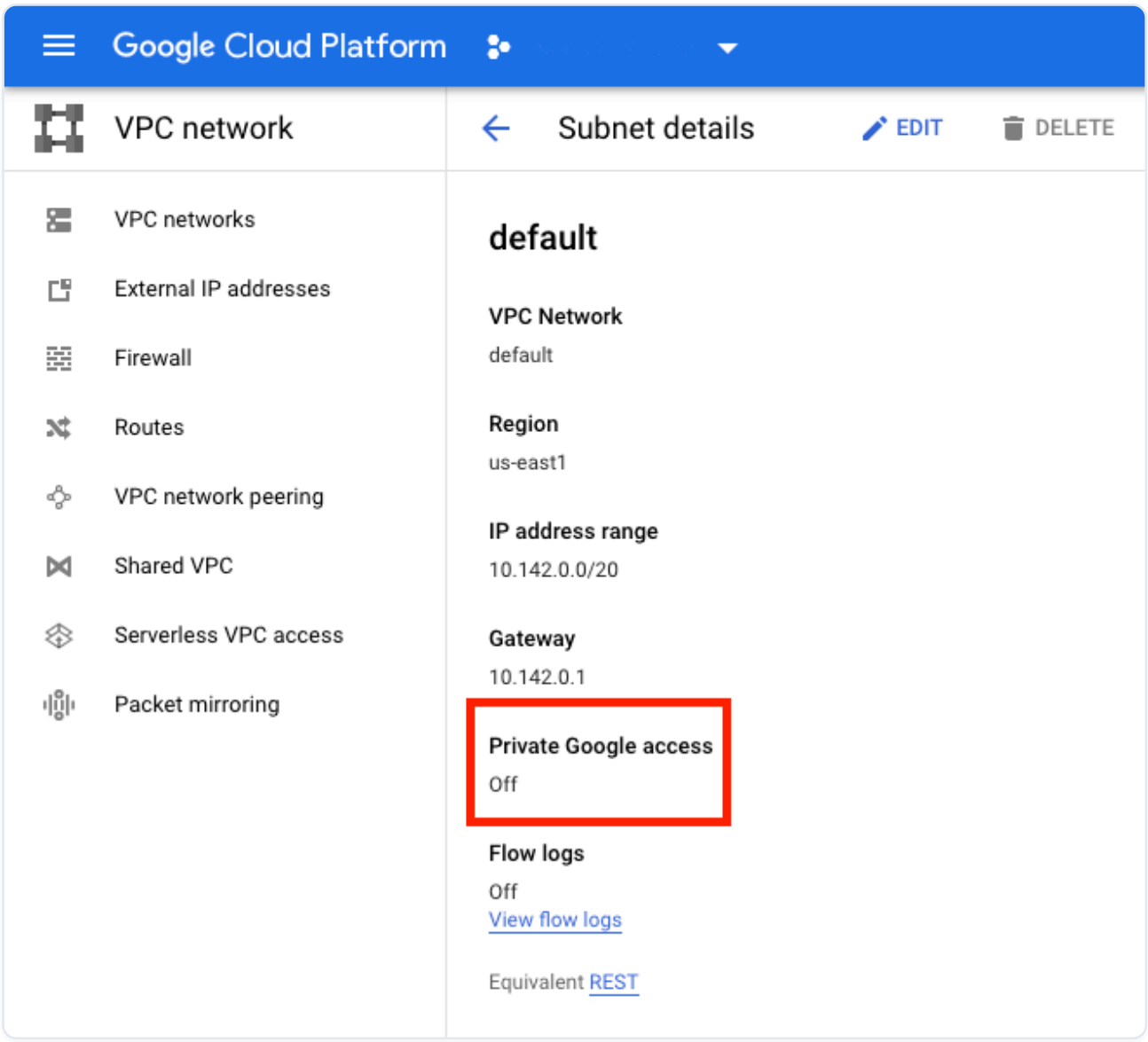
### 启用私有 Google 访问

当虚拟机缺少分配给其网络接口的外部 IP 地址时，数据包只会发送到其他内部 IP 地址目标。启用私有访问后，虚拟机将连接到 Google API 和相关服务使用的外部 IP 地址集。

> **注意：**
>
> 无论是否启用私有 Google 访问，所有具有和不具有公共 IP 地址的虚拟机都必须能够访问 Google 公共 API，尤其是在环境中安装了第三方网络设备的情况下。

为确保子网中的 VM 可以在没有公共 IP 地址的情况下访问 Google API 以进行 MCS 预配：

1. 在 Google Cloud 中，访问 **VPC 网络配置**。
2. 在“子网详细信息”屏幕中，启用 **Private Google access**。




有关详细信息，请参阅配置 Private Google Access。

**重要提示：**

如果您的网络配置为阻止 VM 访问 Internet，请确保您的组织承担为 VM 连接的子网启用 Private Google access 所带来的风险。

### 添加连接

请遵循 Create a connection and resources 中的指导。以下说明将指导您设置托管连接：

1. 在左侧窗格中，从 **Manage > Configuration** 中选择 **Hosting**。
2. 在操作栏中选择 **Add Connection and Resources**。
3. 在 **Connection** 页面上，选择 **Create a new Connection** 和 **Citrix provisioning™ tools**，然后选择 **Next**。
   - **连接类型**。从菜单中选择 **Google Cloud**。
   - **连接名称**。键入连接的名称。
4. 在**区域**页面上，从菜单中选择一个项目名称，选择包含要使用的资源的区域，然后选择**下一步**。
5. 在**网络**页面上，键入资源的名称，从菜单中选择一个虚拟网络，选择一个子集，然后选择**下一步**。资源名称有助于识别区域和网络组合。名称后附加 *(Shared)* 后缀的虚拟网络表示共享 VPC。如果您为共享 VPC 配置了子网级 IAM 角色，则共享 VPC 的特定子网才会显示在子网列表中。

> **注意：**
>
> - 资源名称可以包含 1–64 个字符，并且不能只包含空格或字符 `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`。

6. 在**摘要**页面上，确认信息，然后选择**完成**以退出**添加连接和资源**窗口。

创建连接和资源后，将列出您创建的连接和资源。要配置连接，请选择该连接，然后在操作栏中选择适用的选项。

同样，您可以删除、重命名或测试在连接下创建的资源。为此，请选择连接下的资源，然后在操作栏中选择适用的选项。

### 准备主 VM 实例和永久性磁盘

> **提示：**

> 永久性磁盘是 Google Cloud 中虚拟磁盘的术语。

> 要准备主 VM 实例，请创建并配置一个 VM 实例，其属性应与您计划的计算机目录中克隆的 VDA 实例所需的配置相匹配。此配置不仅适用于实例大小和类型，还包括元数据、标签、GPU 分配、网络标签和服务帐户属性等实例属性。

作为主映像创建过程的一部分，MCS 使用您的主 VM 实例来创建 Google Cloud *实例模板*。然后，该实例模板用于创建构成计算机目录的克隆 VDA 实例。克隆实例继承了创建实例模板所用的主 VM 实例的属性（VPC、子网和永久性磁盘属性除外）。

根据您的具体要求配置主 VM 实例的属性后，启动该实例，然后为该实例准备永久性磁盘。

建议您手动创建磁盘快照。这样做可以让您使用有意义的命名约定来跟踪版本，为您提供更多选项来管理主映像的早期版本，并节省创建计算机目录的时间。如果您不创建自己的快照，MCS 会为您创建一个临时快照（该快照将在预配过程结束时删除）。

### 创建计算机目录

> **注意：**
>
> 在创建计算机目录之前，请先创建您的资源。配置计算机目录时，请使用 Google Cloud 建立的命名约定。有关详细信息，请参阅 存储桶和对象命名准则。

> 请遵循 Create machine catalogs 中的指导。目前，Studio 不支持创建 Google Cloud 目录。请改用 PowerShell。

### 管理计算机目录

要将计算机添加到目录、更新计算机以及回滚更新，请参阅 Manage machine catalogs。

### 电源管理

Citrix DaaS 允许您对 Google Cloud 计算机进行电源管理。使用导航窗格中的“**搜索**”节点查找要进行电源管理的计算机。提供以下电源操作：

- 删除
- 启动
- 重新启动
- 强制重新启动
- 关机
- 强制关机

- 添加到交付组
- 管理标签
- 启用维护模式

您还可以使用 Autoscale 对 Google Cloud 计算机进行电源管理。为此，请将 Google Cloud 计算机添加到交付组，然后为该交付组启用 Autoscale。有关 Autoscale 的详细信息，请参阅 Autoscale。

### 防止意外删除计算机

Citrix DaaS 允许您保护 Google Cloud 上的 MCS 资源，以防止意外删除。通过将 `deletionProtection` 标志设置为 TRUE 来配置预配的 VM。

默认情况下，通过 MCS 或 Google Cloud 插件预配的 VM 会在启用 InstanceProtection 的情况下创建。此实现适用于持久和非持久目录。当实例从模板重新创建时，非持久目录会更新。对于现有持久计算机，您可以在 Google Cloud 控制台中设置该标志。有关设置标志的详细信息，请参阅 Google 文档站点。添加到持久目录的新计算机是在启用 `deletionProtection` 的情况下创建的。

如果您尝试删除已设置 `deletionProtection` 标志的 VM 实例，则请求将失败。但是，如果您被授予权限 `compute.instances.setDeletionProtection` 或分配了 IAM **Compute Admin** 角色，则可以重置该标志以允许删除资源。

### 导入手动创建的 Google Cloud 机器

您可以*创建与 Google Cloud 的连接，然后创建包含 Google Cloud 计算机的目录*。然后，您可以通过 Citrix DaaS 手动重启 Google Cloud 计算机。借助此功能，您可以：

- 将手动创建的 Google Cloud 多会话操作系统计算机导入 Citrix Virtual Apps and Desktops 计算机目录。
- 从 Citrix Virtual Apps and Desktops 目录中删除手动创建的 Google Cloud 多会话操作系统计算机。
- 使用现有的 Citrix Virtual Apps and Desktops 电源管理功能来管理 Google Cloud Windows 多会话操作系统计算机的电源。例如，为这些计算机设置重启计划。

此功能不需要更改现有 Citrix Virtual Apps and Desktops 预配工作流，也不需要删除任何现有功能。建议您使用 MCS 在 Web Studio 中预配计算机，而不是导入手动创建的 Google Cloud 计算机。

### 共享虚拟私有云

共享虚拟私有云 (VPC) 包含一个主机项目（从中提供共享子网）以及一个或多个使用该资源的服务项目。共享 VPC 是大型安装的理想选择，因为它们提供对共享企业 Google 云资源的集中控制、使用和管理。有关详细信息，请参阅 Google 文档站点。

借助此功能，Machine Creation Services™ (MCS) 支持预配和管理部署到共享 VPC 的计算机目录。此支持在功能上等同于当前在本地 VPC 中提供的支持，但在两个方面有所不同：

1. 您必须向用于创建主机连接的服务帐户授予额外权限。此过程允许 MCS 访问和使用共享 VPC 资源。
2. 您必须创建两条防火墙规则，一条用于入站，一条用于出站。这些防火墙规则在映像主控过程中使用。

### 所需的新权限

创建主机连接时需要具有特定权限的 Google Cloud 服务帐户。必须将这些额外权限授予用于创建基于共享 VPC 的主机连接的任何服务帐户。

> **提示：**
>
> 这些额外权限对于 Citrix DaaS 而言并非新功能。它们用于促进本地 VPC 的实施。对于共享 VPC，这些额外权限允许访问其他共享 VPC 资源。
>
> 最多需要向与主机连接关联的服务帐户授予四个额外权限，以支持共享 VPC：

1. **compute.firewalls.list** - 此权限是强制性的。它允许 MCS 检索共享 VPC 上存在的防火墙规则列表。
2. **compute.networks.list** - 此权限是强制性的。它允许 MCS 识别服务帐户可用的共享 VPC 网络。
3. **compute.subnetworks.list** – 此权限是可选的，具体取决于您如何使用 VPC。它允许 MCS 识别可见共享 VPC 中的子网。在使用本地 VPC 时已需要此权限，但它也必须分配给共享 VPC 主机项目。
4. **compute.subnetworks.use** - 此权限是可选的，具体取决于您如何使用 VPC。在预配的计算机目录中使用子网资源时，此权限是必需的。在使用本地 VPC 时已需要此权限，但它也必须分配给共享 VPC 主机项目。

使用这些权限时，请考虑根据用于创建计算机目录的权限类型，有不同的方法：

- 项目级权限：
  - 允许访问主机项目中的所有共享 VPC。
  - 要求将权限 #3 和 #4 分配给服务帐户。
- 子网级权限：

- 允许访问共享 VPC 中的特定子网。
- 权限 #3 和 #4 是子网级别分配固有的，因此无需直接分配给服务帐户。

选择符合您的组织需求和安全标准的方法。

> **提示：**
>
> 有关项目级别和子网级别权限之间差异的更多信息，请参阅 Google Cloud 文档。

### 防火墙规则

在准备计算机目录期间，会准备一个计算机映像，用作目录的主映像系统磁盘。在此过程发生时，磁盘会临时附加到虚拟机。此虚拟机必须在隔离环境中运行，以防止所有入站和出站网络流量。这通过一对拒绝所有防火墙规则来实现；一个用于入站流量，一个用于出站流量。使用 Google Cloud 本地 VCP 时，MCS 会在本地网络中创建此防火墙，并将其应用于用于主映像的计算机。主映像完成后，防火墙规则将从映像中删除。

我们建议将使用共享 VPC 所需的新权限数量保持在最低限度。共享 VPC 是更高级别的企业资源，通常具有更严格的安全协议。因此，请在主机项目中的共享 VPC 资源上创建一对防火墙规则，一个用于入站，一个用于出站。为它们分配最高优先级。使用以下值将新的目标标记应用于每个规则：

`citrix-provisioning-quarantine-firewall`

当 MCS 创建或更新计算机目录时，它会搜索包含此目标标记的防火墙规则。然后，它会检查规则的正确性，并将其应用于用于为目录准备主映像的计算机。如果未找到防火墙规则，或者找到了规则但规则或其优先级不正确，则会出现类似以下内容的消息：

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."
```

### 配置共享 VPC

在 Web Studio 中将共享 VPC 添加为主机连接之前，请完成以下步骤以添加您打算预配到的项目中的服务帐户：

1. 创建 IAM 角色。
2. 将用于创建 CVAD 主机连接的服务帐户添加到共享 VPC 主机项目 IAM 角色。
3. 将您打算预配到的项目中的 Cloud Build 服务帐户添加到共享 VPC 主机项目 IAM 角色。

4. 创建防火墙规则。

#### 创建 IAM 角色

确定角色的访问级别 — *项目级别访问*或使用*子网级别访问*的更受限模型。

**IAM 角色的项目级别访问**。对于项目级别的 IAM 角色，请包含以下权限：

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

要创建项目级别的 IAM 角色：

1. 在 Google Cloud 控制台中，导航到 **IAM 和管理 > 角色**。
2. 在 **角色** 页面上，选择 **创建角色**。
3. 在 **创建角色** 页面上，指定角色名称。选择 **添加权限**。
    a. 在“**添加权限**”页面上，单独向角色添加权限。要添加权限，请在“**筛选表**”字段中键入权限名称。选择权限，然后选择“**添加**”。
    b. 选择 **创建**。

**子网级别 IAM 角色**。此角色在选择“**创建角色**”后省略了权限 `compute.subnetworks.list` 和 `compute.subnetworks.use` 的添加。对于此 IAM 访问级别，必须将权限 `compute.firewalls.list` 和 `compute.networks.list` 应用于新角色。

要创建子网级别的 IAM 角色：

1. 在 Google Cloud 控制台中，导航到 **VPC 网络** > **共享 VPC**。“**共享 VPC**”页面随即显示，其中显示了宿主项目包含的共享 VPC 网络的子网。
2. 在 **共享 VPC** 页面上，选择您要访问的子网。
3. 在右上角，选择 **添加成员** 以添加服务帐户。
4. 在 **添加成员** 页面上，完成以下步骤：
    a. 在 **新成员** 字段中，键入您的服务帐户名称，然后从菜单中选择您的服务帐户。
    b. 选择 **选择角色** 字段，然后选择 **计算网络用户**。
    c. 选择 **保存**。
5. 在 Google Cloud 控制台中，导航到 **IAM 和管理** > **角色**。

6. 在 **角色** 页面上，选择 **创建角色**。
7. 在 **创建角色** 页面上，指定角色名称。选择 **添加权限**。
    a. 在 **添加权限** 页面上，单独为角色添加权限。要添加权限，请在 **筛选表** 字段中键入权限名称。选择该权限，然后选择 **添加**。
    b. 选择 **创建**。

#### 将服务帐户添加到主机项目 IAM 角色

创建 IAM 角色后，执行以下步骤为主机项目添加服务帐户：

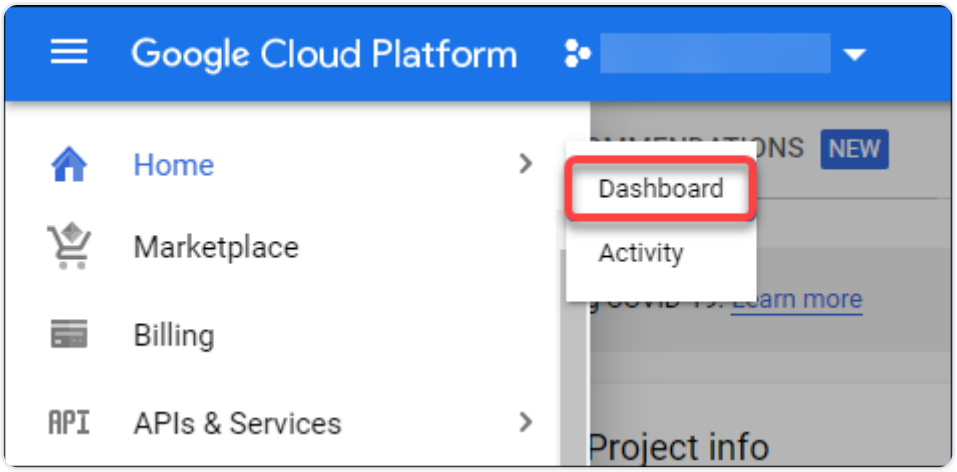
1. 在 Google Cloud 控制台中，导航到主机项目，然后导航到 **IAM 和管理 > IAM**。
2. 在 **IAM** 页面上，选择 **添加** 以添加服务帐户。
3. 在“**添加成员**”页面上：
    a. 在 **新成员** 字段中，键入您的服务帐户名称，然后从菜单中选择您的服务帐户。
    b. 选择一个角色字段，键入您创建的 IAM 角色，然后从菜单中选择该角色。
    c. 选择 **保存**。

服务帐户现已为主机项目配置。

#### 将云构建服务帐户添加到共享 VPC

每个 Google Cloud 订阅都有一个服务帐户，其名称是项目 ID 号，后跟 `cloudbuild.gserviceaccount`。例如：`705794712345@cloudbuild.gserviceaccount`。

您可以通过在 Google Cloud 控制台中选择 **Home** 和 **Dashboard** 来确定您的项目 ID 号：




在屏幕的 **Project Info** 区域下方找到 **Project Number**。

执行以下步骤将 Cloud Build 服务帐户添加到共享 VPC：

1. 在 Google Cloud 控制台中，导航到主机项目，然后导航到“**IAM 和管理**”>“**IAM**”。

2. 在“**权限**”页面上，选择“**添加**”以添加帐户。
3. 在 **添加成员** 页面上，完成以下步骤：
    a. 在“**新成员**”字段中，键入 Cloud Build 服务帐户的名称，然后从菜单中选择您的服务帐户。
    b. 选择“**选择角色**”字段，键入 `Computer Network User`，然后从菜单中选择该角色。
    c. 选择 **保存**。

#### 创建防火墙规则

作为主映像过程的一部分，MCS 会复制选定的计算机映像，并用它来准备目录的主映像系统磁盘。在主映像期间，MCS 会将磁盘附加到临时虚拟机，然后该虚拟机运行准备脚本。此虚拟机必须在禁止所有入站和出站网络流量的隔离环境中运行。为了创建隔离环境，MCS 需要两条 *拒绝所有* 防火墙规则（一条入站规则和一条出站规则）。因此，请在 *主机项目* 中创建两条防火墙规则，如下所示：

1. 在 Google Cloud 控制台中，导航到主机项目，然后转到 **VPC network > Firewall**。
2. 在 **Firewall** 页面上，选择 **CREATE FIREWALL RULE**。
3. 在 **Create a firewall rule** 页面上，完成以下操作：
    - **名称**。键入规则的名称。
    - **网络**。选择入站防火墙规则适用的共享 VPC 网络。
    - **优先级**。值越小，规则的优先级越高。我们建议使用较小的值（例如，10）。
    - **流量方向**。选择 **Ingress**。
    - **匹配操作**。选择 **Deny**。
    - **目标**。使用默认值 **Specified target tags**。
    - **目标标记**。键入 `citrix-provisioning-quarantine-firewall`。
    - **源筛选器**。使用默认值 **IP ranges**。
    - **源 IP 范围**。键入与所有流量匹配的范围。键入 `0.0.0.0/0`。
    - **协议和端口**。选择**拒绝所有**。
4. 选择**创建**以创建规则。
5. 重复步骤 1–4 以创建另一条规则。对于 **Direction of traffic**，选择 **Egress**。

#### 添加连接

添加与 Google 云环境的连接。请参阅 添加连接。

## 启用区域选择

Citrix Virtual Apps and Desktops 支持区域选择。通过区域选择，您可以指定要创建 VM 的区域。通过区域选择，管理员可以将独占租户节点放置在他们选择的区域中。要配置独占租用，您必须在 Google Cloud 上完成以下操作：

- 预留 Google Cloud 单租户节点
- 创建 VDA 主映像

### 预留 Google Cloud 独占租户节点

要预留单租户节点，请参阅 Google Cloud 文档。

> **重要提示：**
>
> 节点模板用于指示在节点组中预留的系统的性能特征。这些特征包括 vGPU 的数量、分配给节点的内存量以及在节点上创建的计算机所使用的计算机类型。有关详细信息，请参阅 Google Cloud 文档。

### 创建 VDA 主映像

要在单租户节点上成功部署计算机，您需要在创建主 VM 映像时采取额外的步骤。Google Cloud 上的计算机实例具有一个名为 *节点亲和性标签* 的属性。用作部署到单租户节点的目录的主映像的实例需要一个与 **目标节点组** 名称匹配的 *节点亲和性标签*。为此，请记住以下几点：

- 对于新实例，请在创建实例时在 Google Cloud 控制台中设置标签。有关详细信息，请参阅 创建实例时设置节点亲和性标签。
- 对于现有实例，请使用 **gcloud** 命令行设置标签。有关详细信息，请参阅 为现有实例设置节点亲和性标签。

> **注意：**
>
> 如果您打算将单租户与共享 VPC 结合使用，请参阅 共享虚拟私有云。

#### 创建实例时设置节点亲和性标签

要设置节点亲和性标签：

1. 在 Google Cloud 控制台中，导航到 **Compute Engine > VM instances**。
2. 在 **VM instances** 页面上，选择 **Create instance**。

3. 在 **Instance creation** 页面上，键入或配置所需信息，然后选择 **management, security, disks, networking, sole tenancy** 以打开设置面板。
4. 在 **Sole tenancy** 选项卡上，选择 **Browse** 以查看当前项目中的可用节点组。此时将显示 **Sole-tenant node** 页面，其中列出了可用节点组。
5. 在 **Sole-tenant node** 页面上，从列表中选择适用的节点组，然后选择 **Select** 返回到 **Sole tenancy** 选项卡。节点亲和性标签字段将填充您选择的信息。此设置可确保从该实例创建的计算机目录将部署到所选的节点组。
6. 选择 **Create** 以创建实例。

#### 为现有实例设置节点亲和性标签

要设置节点亲和性标签：

1. 在 Google Cloud Shell 终端窗口中，使用 *gcloud compute instances* 命令设置节点亲和性标签。在 **gcloud** 命令中包含以下信息：

   - **VM 名称**。例如，使用名为 `s*2019-vda-base`.* 的现有 VM。
   - **节点组名称**。使用您之前创建的节点组名称。例如，`mh-sole-tenant-node-group-1`。
   - **实例所在的区域**。例如，VM 位于 `*us-east-1b* zone`。

   例如，在终端窗口中键入以下命令：

   - `gcloud compute instances set-scheduling "s2019-vda-base" --node-group="mh-sole-tenant-node-group-1" --zone="us-east1-b"`

   有关 *gcloud compute instances* 命令的更多信息，请参阅 `<https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling>` 处的 Google Developer Tools 文档。

2. 导航到实例的**VM 实例详细信息**页面，并验证**节点亲和性**字段是否已填充标签。

#### 创建计算机目录

设置节点亲和性标签后，配置计算机目录。

### 预览：使用客户管理的加密密钥 (CMEK)

您可以将客户管理的加密密钥 (CMEK) 用于 MCS 目录。使用此功能时，您需要将 Google Cloud Key Management Service `CryptoKey Encrypter/Decrypter` 角色分配给 Compute Engine Service Agent。Citrix DaaS 帐户必须在存储密钥的项目中具有正确的权限。有关详细信息，请参阅使用 Cloud KMS 密钥帮助保护资源。

您的 Compute Engine 服务代理采用以下形式：`service-<Project _Number>@compute-system.iam.gserviceaccount.com`。此形式不同于默认的 Compute Engine 服务帐户。

> **注意：**
>
> 此 Compute Engine 服务帐户可能不会显示在 Google Console **IAM 权限**显示中。在这种情况下，请使用 `gcloud` 命令，如通过使用 Cloud KMS 密钥帮助保护资源 中所述。

### 向 Citrix DaaS 帐户分配权限

Google Cloud KMS 权限可以通过多种方式配置。您可以提供*项目级* KMS 权限或*资源级* KMS 权限。有关详细信息，请参阅权限和角色。

#### 项目级权限

一种选择是向 Citrix DaaS 帐户提供项目级权限以浏览 Cloud KMS 资源。为此，请创建一个自定义角色，并添加以下权限：

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

将此自定义角色分配给您的 Citrix DaaS 帐户。这允许您在清单中浏览相关项目中的区域密钥。

#### 资源级权限

对于另一个选项，即资源级权限，在 Google Cloud 控制台中，浏览到您用于 MCS 预配的 `cryptoKey`。将 Citrix DaaS 帐户添加到您用于目录预配的密钥环或密钥。

> **提示：**
>
> 使用此选项，您无法在清单中浏览项目的区域密钥，因为 Citrix DaaS 帐户没有 Cloud KMS 资源的项级列表权限。但是，您仍然可以通过在下面描述的 `ProvScheme` 自定义属性中指定正确的 `cryptoKeyId` 来使用 CMEK 预配目录。

### 使用自定义属性通过 CMEK 进行预配

通过 PowerShell 创建预配方案 时，请在 `ProvScheme CustomProperties` 中指定 `CryptoKeyId` 属性。例如：

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

`cryptoKeyId` 必须按以下格式指定：

`projectId:location:keyRingName:cryptoKeyName`

例如，如果您想在区域 `us-east1` 的密钥环 `my-example-key-ring` 中使用密钥 `my-example-key`，并且项目 ID 为 `my-example-project-1`，则您的 `ProvScheme` 自定义设置将类似于：

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />

</CustomProperties>'
```

与此预配方案相关的所有 MCS 预配磁盘和映像都使用此客户管理的加密密钥。

**提示：**

如果您使用全局密钥，客户属性位置必须显示 `global`，而不是 **region** 名称（在上面的示例中为 **us-east1**）。例如：`<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`。

### 轮换客户管理的密钥

Google Cloud 不支持轮换现有持久性磁盘或映像上的密钥。一旦预配了计算机，它就与创建时使用的密钥版本绑定。但是，可以创建新版本的密钥，并且该新密钥将用于新预配的计算机或在目录使用新主映像更新时创建的资源。

#### 关于密钥环的重要注意事项

密钥环无法重命名或删除。此外，配置它们时可能会产生不可预见的费用。删除或移除密钥环时，Google Cloud 会显示错误消息：

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
nor key rings are billed for, just the active key versions within the
keys.
```

**提示：**

有关详细信息，请参阅从控制台编辑或删除密钥环。

### 统一存储桶级访问兼容性

Citrix DaaS 与 Google Cloud 上的统一存储桶级访问控制策略兼容。此功能增强了 IAM 策略的使用，该策略授予服务帐户权限以允许操作资源，包括存储桶。借助统一存储桶级访问控制，Citrix DaaS 允许您使用访问控制列表 (ACL) 来控制对存储桶或其中存储的对象的访问。有关 Google Cloud 统一存储桶级访问的概述信息，请参阅 统一存储桶级访问。有关配置信息，请参阅 要求统一存储桶级访问。

### 服务端点 URL

您必须有权访问以下 URL：

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

### Google Cloud 项目

Google Cloud 项目主要有两种类型：

- 预配项目：在这种情况下，当前管理员帐户拥有项目中预配的计算机。此项目也称为本地项目。
- 共享 VPC 项目：在其中，预配项目中创建的计算机使用来自共享 VPC 项目的 VPC 的项目。用于预配项目的管理员帐户在此项目中具有有限的权限，具体来说，仅具有使用 VPC 的权限。

### 所需的 GCP 权限

本节包含 GCP 权限的完整列表。请使用本节中提供的完整权限集，以确保功能正常运行。

> **注意：**
>
> GCP 将在 April 29, 2024 之后对 Cloud Build Services 的默认行为和服务账户的使用引入更改。有关详细信息，请参阅 Cloud Build Service Account Change。您在 April 29, 2024 之前启用了 Cloud Build API 的现有 Google 项目不受此更改影响。但是，如果您希望在 April 29 之后仍保留现有的 Cloud Build Service 行为，则可以在启用 API 之前创建或应用组织策略以禁用约束强制执行。如果您设置了新的组织策略，则仍可以遵循本节中现有的权限以及标记为 **Before Cloud Build Service Account Change** 的项目。否则，请遵循标记为 **After Cloud Build Service Account Change** 的现有权限和项目。

#### 创建主机连接

- 预配项目中 Citrix Cloud 服务账户所需的最低权限：

```
compute.instanceTemplates.list

compute.instances.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list
```

```
resourcemanager.projects.get
```

以下 Google 定义的角色具有上述权限：

- 计算管理员
- 云数据存储用户

- Citrix Cloud 服务帐户在共享 VPC 项目中共享 VPC 所需的额外权限：

```
compute.networks.list

compute.subnetworks.list

resourcemanager.projects.get
```

以下 Google 定义的角色具有上述权限：

- 计算网络用户

**虚拟机电源管理**

在仅电源管理的目录中，Citrix Cloud 服务帐户在预配项目中所需的最低权限：

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.networks.list

compute.projects.get
```

```
compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

以下 Google 定义的角色具有上述权限：

- 计算管理员
- 云数据存储用户

**创建、更新或删除虚拟机**

- 预配项目中 Citrix Cloud 服务账户所需的最低权限：

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels
```

```
compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get
```

```
compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list
```

```
compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

compute.networks.get
```

```
compute.resourcePolicies.use
```

以下 Google 定义的角色具有上述权限：

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

- Citrix Cloud 服务帐户在共享 VPC 项目中创建托管单元时，使用共享 VPC 项目中的 VPC 和子网所需的共享 VPC 附加权限：

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

以下 Google 定义的角色具有上述权限：

- 计算网络用户
- 云数据存储用户

- （在 Cloud Build 服务帐户更改之前）：Google Cloud Build 服务在将准备说明磁盘下载到 MCS 时，预配项目中 Cloud Build 服务帐户所需的最低权限：

- （在 Cloud Build 服务帐户更改之后）：Google Cloud Compute 服务在将准备说明磁盘下载到 MCS 时，预配项目中 Cloud Compute 服务帐户所需的最低权限：

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.machineTypes.list

compute.networks.get
```

```
compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list
```

以下 Google 定义的角色具有上述权限：

  - Cloud Build 服务帐户（在 Cloud Build 服务帐户更改后，它是 Cloud Compute 服务帐户）
  - 计算实例管理员
  - 服务帐号用户

- 将准备说明磁盘下载到 MCS 时，Google Cloud Build 服务在预配项目中为 Cloud Compute 服务帐户所需的最低权限：

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get

storage.objects.list
```

  以下 Google 定义的角色具有上述权限：

  - 计算网络用户
  - 存储账户用户
  - 云数据存储用户

- （在 Cloud Build 服务帐户更改之前）：Google Cloud Build 服务在将准备说明磁盘下载到 MCS 时，预配项目中 Cloud Build 服务帐户的共享 VPC 所需的额外权限：
- （在 Cloud Build 服务帐户更改之后）：Google Cloud Compute 服务在将准备说明磁盘下载到 MCS 时，预配项目中 Cloud Compute 服务帐户的共享 VPC 所需的额外权限：

```
compute.firewalls.list

compute.networks.list

compute.subnetworks.list

compute.subnetworks.use

resourcemanager.projects.get
```

  以下 Google 定义的角色具有上述权限：

  - 计算网络用户

  - 存储账户用户
  - 云数据存储用户

- 预配项目中 Citrix Cloud 服务帐户的 Cloud Key Management Service (KMS) 所需的额外权限：

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

  以下 Google 定义的角色具有上述权限：

  - 计算 KMS 查看者

**一般权限**

以下是预配项目中 Citrix Cloud 服务帐户在 MCS 中支持的所有功能的权限。这些权限可提供最佳的未来兼容性：

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get
```

```
compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk
```

```
compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig

compute.instances.updateShieldedVmConfig

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list
```

```
compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list
```

```
storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs

compute.resourcePolicies.use
```

### 更多信息

- 连接和资源
- 创建计算机目录

## Nutanix 虚拟化环境

在您的 Citrix Virtual Apps and Desktops™ 部署中使用 Nutanix Acropolis 提供虚拟机时，请遵循本指南。设置过程包括以下任务：

- 在您的 Citrix Virtual Apps and Desktops 环境中安装并注册 Nutanix 插件。
- 创建与 Nutanix Acropolis 管理程序的连接。
- 创建计算机目录，该目录使用您在 Nutanix 管理程序上创建的主映像的快照。

有关详细信息，请参阅 Nutanix 支持门户 上提供的 Nutanix Acropolis MCS 插件安装指南。

### 安装并注册 Nutanix 插件

完成以下过程，在所有 Delivery Controller 上安装并注册 Nutanix 插件。使用 Citrix Studio 创建与 Nutanix 的连接。然后，创建计算机目录，该目录使用您在 Nutanix 环境中创建的主映像的快照。

> **提示：**
>
> 我们建议您在安装或更新 Nutanix 插件时停止并重新启动 Citrix Host Service、Citrix Broker Service 和 Machine Creation Services™。
>
> 有关安装 Nutanix 插件的信息，请参阅 Nutanix 文档站点。

### 创建 Nutanix 连接

以下信息是对 连接和资源 的补充。要创建 Nutanix 连接，请遵循该文章中的一般指导，同时注意 Nutanix 特有的详细信息。

在**添加连接和资源**向导中，在**连接**页面上选择 Nutanix 连接类型，然后指定地址和凭据，以及连接名称。在**网络**页面上，为托管单元选择一个网络。

以下连接类型可供选择：**Nutanix AHV**、**Nutanix AHV Xi** 和 **Nutanix AHV PC**。

- 对于 **Nutanix AHV**，请指定 Prism Element (PE) 群集地址和凭据。
- 对于 **Nutanix AHV PC**，请指定 Prism Central (PC) 地址和凭据。

  > **注意：**
  >
  > 目前，Nutanix AHV PC 连接类型仅用于创建到 Azure 上的 Nutanix Cloud Cluster (NC2) 的连接。此外，计算机目录只能托管在 Azure 连接上的 NC2 中的单个群集上。

- 对于 **Nutanix AHV DRaaS**，请指定 DRaaS 租户地址和用户名。导入您的私有和公共 Nutanix DRaaS 凭据文件 (`.pem`)。

> **提示：**
>
> 如果使用 Nutanix AHV (Prism Element) 作为资源部署计算机，请选择虚拟机磁盘所在的容器。

### 使用 Nutanix 快照创建计算机目录

以下信息是对 创建计算机目录 中指南的补充。要创建目录，请遵循该文章中的一般指南，同时注意 Nutanix 特有的详细信息。

您选择的快照是用于在目录中创建 VM 的模板。在创建目录之前，请在 Nutanix 中创建映像和快照。有关详细信息，请参阅 Nutanix 文档。

在目录创建向导中：

- **操作系统**和**计算机管理**页面不包含 Nutanix 特定的信息。
- **Container**（容器）或 **Cluster and Container**（群集和容器）页面是 Nutanix 独有的。

  如果您使用 Nutanix AHV XI 作为资源部署计算机，您会看到**容器**页面。选择一个容器来放置 VM 的身份磁盘。

  如果您使用 Nutanix AHV Prism Central (PC) 作为资源部署计算机，您会看到**群集和容器**页面。选择用于部署 VM 的群集，然后选择一个容器。
- 在**主映像**页面上，选择映像快照。Acropolis 快照名称必须以“XD_”为前缀才能在 Citrix Virtual Apps and Desktops 中使用。如果需要，请使用 Acropolis 控制台重命名快照。如果重命名快照，请重新启动目录创建向导以查看刷新后的列表。
- 在 **Virtual Machines**（虚拟机）页面上，指示虚拟 CPU 的数量和每个 vCPU 的核心数。
- 在“**网卡**”页面上，选择网卡类型以筛选关联的网络。有两种网卡类型：**VLAN** 和 **OVERLAY**。选择主映像包含的一个或多个网卡，然后为每个网卡选择一个关联的虚拟网络。
- **Machine Identities**（计算机身份）、**Domain Credentials**（域凭据）、**Scopes**（范围）和 **Summary**（摘要）页面不包含 Nutanix 特定的信息。

## Nutanix 云和合作伙伴解决方案

Citrix Virtual Apps and Desktops™ 支持以下 Nutanix 云和合作伙伴解决方案：

- AWS 上的 Nutanix 云集群

### AWS 上的 Nutanix 云集群

Citrix Virtual Apps and Desktops 支持 AWS 上的 Nutanix 云集群。Nutanix 集群简化了应用程序在私有云或多个公共云上的运行方式。有关 AWS 上的 Nutanix 云集群的更多信息，请参阅 AWS 上的 Nutanix 云集群部署和用户指南。

> **提示：**
>
> 此支持提供与 Nutanix 本地集群相同的功能。仅支持单个集群，即 *Prism Element*。有关更多信息，请参阅 此处。

#### 要求

要在 AWS 上使用 Nutanix 集群，您需要满足以下条件：

- 一个 Nutanix 帐户。
- 具有以下权限的 AWS 帐户：
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

#### 创建 Nutanix 集群

要创建 Nutanix 集群：

1. 登录您的 Nutanix 帐户。
2. 找到 **Nutanix 集群**选项，然后单击**启动**。**Nutanix 控制台**随即打开。有关更多信息，请参阅 AWS 上的 Nutanix 集群入门。
3. 选择创建**新的 VPC**。

集群创建过程可能会因以下错误而失败：

- 集群未能在给定时间内创建。正在删除集群。
- 主机 Nutanix 集群 - 节点 `XXXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`.
- 主机 Nutanix 集群 - 节点 `XXXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxxx network interface info.`.

如果集群创建失败：

- 尝试在其他区域重新创建一个。
- 在重试之前，请务必删除 Nutanix CloudFormation 堆栈 (CFS)。

除了其他资源，Nutanix CFS 还会创建：

- 一个名为 *Nutanix Cluster xxxxxxxxxxxx* 的 VPC，地址为 10.0.0.0/16
- 2 个子网 10.0.128.0/24 和 10.0.129.0/24
- 1 个互联网网关
- 1 个 NAT 网关

集群创建完成后，检索 **Nutanix Prism** 的地址：

1. 转到 **Nutanix 控制台**。
2. 在控制台的右上角，将鼠标悬停在链接 **启动 Prism Element** 上并复制 URL。

### 连接到 Nutanix Prism

创建 Nutanix 集群后，连接到 Nutanix Prism。

要连接到 Nutanix Prism：

1. 在 10.0.129.0/24 子网中创建一个堡垒虚拟机。
2. RDP 到堡垒虚拟机，访问您在上一节中复制的 **Prism Element** 的 URL。
3. 使用默认凭据登录：`admin:nutanix/4u`。记得更改密码。

### 在 Nutanix 集群上创建虚拟机

连接到 **Nutanix Prism** 后，创建 Nutanix 集群上的虚拟机。

#### 如果虚拟机需要 Internet 访问

1. 转到 AWS 控制台。
2. 在与 Nutanix CFS 创建的 VPC 相同的 VPC 中创建一个新子网 10.0.130.0/24。
3. 向此子网的路由表添加路由，以将所有非本地流量定向到上面的 NAT 网关。
4. RDP 到堡垒虚拟机，访问您在上一节中复制的 **Prism Element** 的 URL 并登录。
5. 添加新网络。转到 **设置>网络配置>创建子网**。使用与 AWS 中相同的子网 10.0.130.0/24。
6. 在该新子网中创建所有 VM（AD、CC、VDA 等）。

#### 如果 VM 不需要 Internet 访问

1. RDP 到堡垒虚拟机，访问您在上一节中复制的 **Prism Element** 的 URL 并登录。

2. 添加新网络。转到 **设置>网络配置>创建子网**。使用子网 10.0.129.0/24。
3. 在该子网中创建所有 VM（AD、CC、VDA 等）。

> **提示：**
>
> 确保 VM 中的时间和时区信息设置正确。对于 AD 尤其如此。

### 创建主机连接

1. 启动 Web Studio。
2. 选择托管节点，然后单击 **添加连接和资源**。
3. 在 **连接** 屏幕上，选择 **创建新连接**，并在 **连接地址** 中输入 `https://xxx.xxx.xxx.xxx:9440`。
4. 按照 UI 完成向导。

> **注意：**
>
> 要在 Web Studio 中看到 Nutanix 选项，所有连接器 VM 都必须安装 nutanix 插件，即使它们未在 nutanix 区域中使用。

# 安装核心组件

> **重要提示：**
>
> Citrix 会收集必要的许可基本数据，以满足其合法利益，包括许可证合规性。有关详细信息，请参阅 Citrix 许可数据。 确保许可证服务器运行的最低版本为 11.17.2 build 53100。未能满足此先决条件可能会在站点升级和创建期间导致错误或建议。

> 核心组件包括 思杰 Delivery Controller™、思杰 Studio、思杰 Director 和 思杰 License Server。

（在 2003 之前的版本中，核心组件包括 Citrix StoreFront。您仍然可以通过单击**Citrix StoreFront** 磁贴或运行安装介质上提供的命令来安装 StoreFront。）

在开始安装之前，请查看本文和准备安装。

本文介绍了安装核心组件时的安装向导顺序。提供了命令行等效项。有关详细信息，请参阅使用命令行安装。

## 步骤 1. 下载产品软件并启动向导

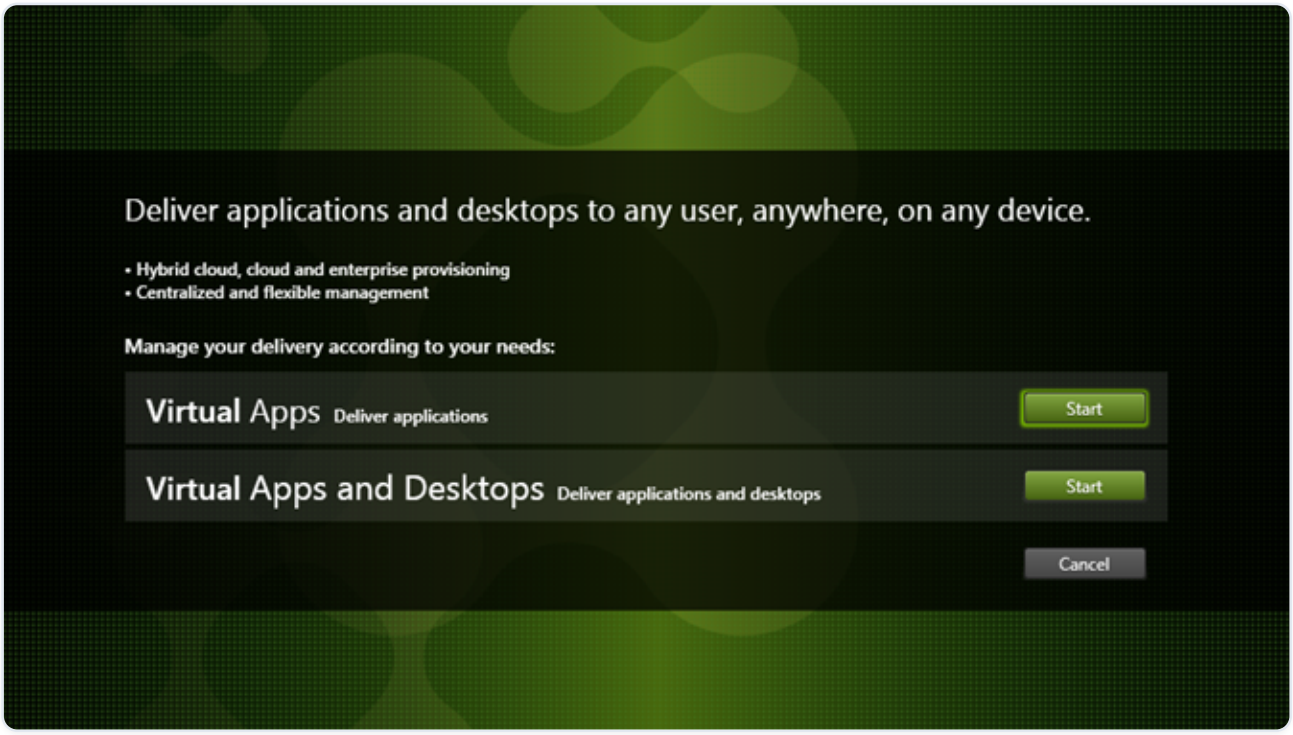
使用您的 Citrix 帐户凭据访问 Citrix Virtual Apps and Desktops™ 下载页面。下载产品 ISO 文件。

解压缩文件。或者，刻录 ISO 文件的 DVD。

使用本地管理员帐户登录到要安装核心组件的计算机。

将 DVD 插入驱动器或装载 ISO 文件。如果安装程序未自动启动，请双击 **AutoSelect** 应用程序或装载的驱动器。

## 步骤 2. 选择要安装的产品

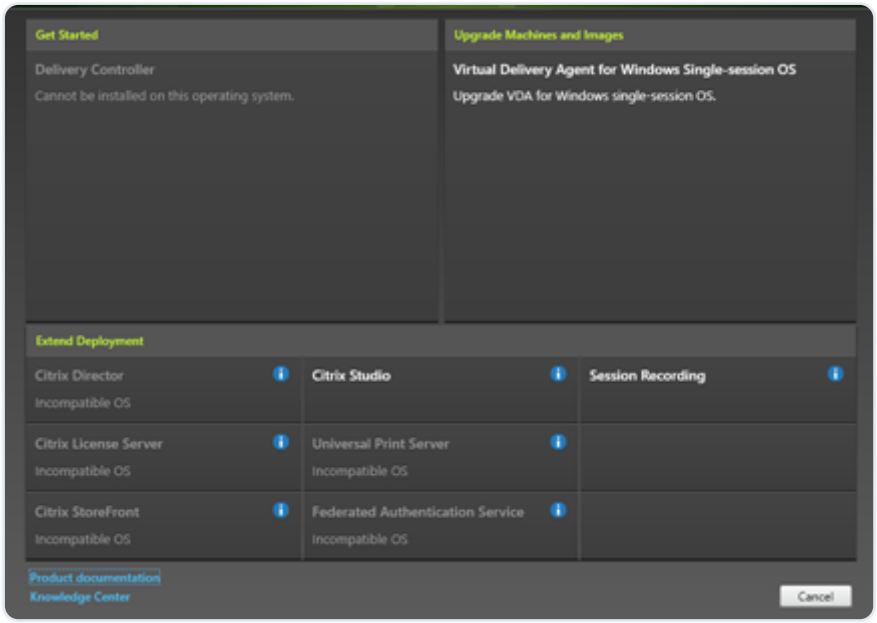



点击要安装的产品旁边的 **开始**：Virtual Apps 或 Virtual Apps and Desktops。

(如果计算机上已安装 Citrix Virtual Apps and Desktops 组件，则此页面不会出现。)

命令行选项：`/xenapp` 以安装 Citrix Virtual Apps。如果省略该选项，则安装 Citrix Virtual Apps and Desktops。

## 步骤 3. 选择要安装的内容

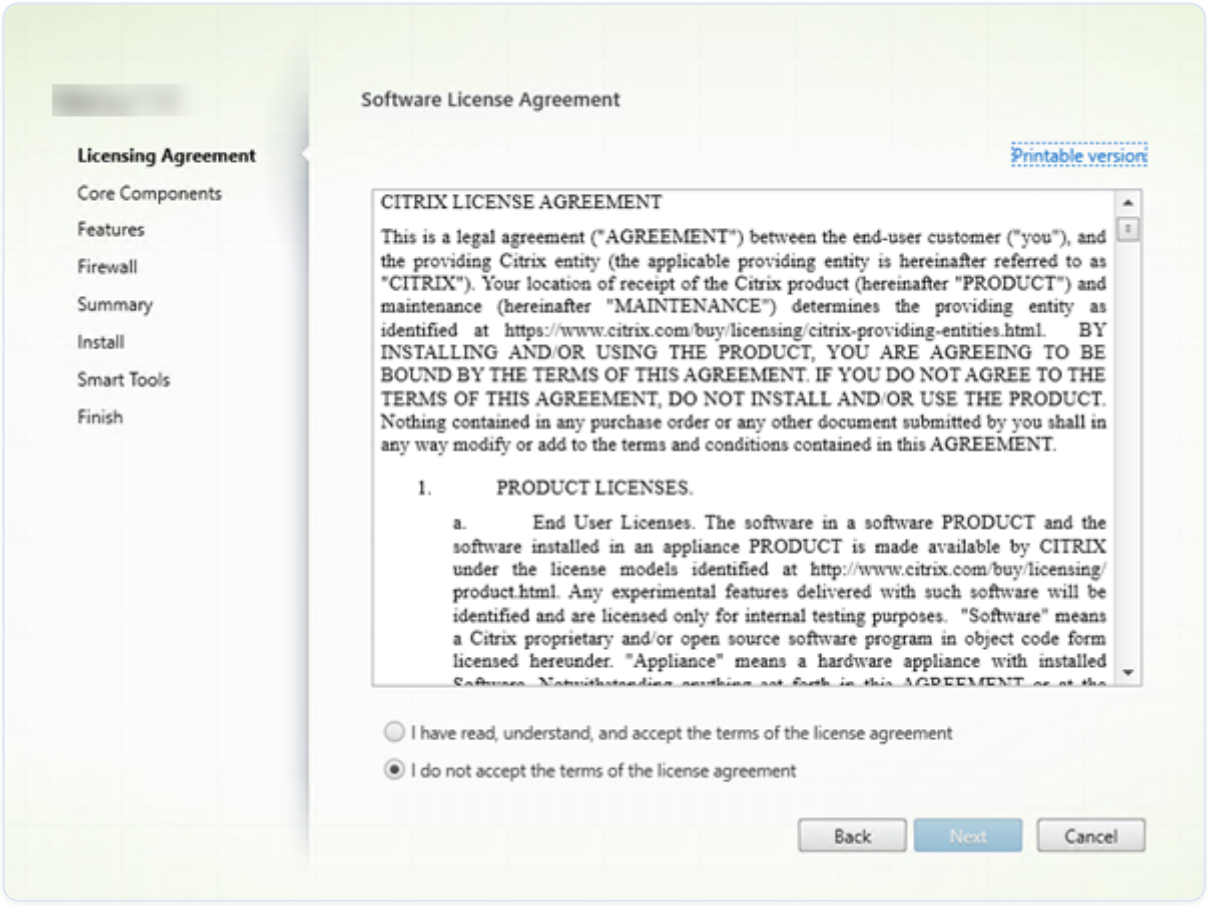



如果您是初次使用，请选择 **Delivery Controller**。（在后续页面上，您将选择要在此计算机上安装的特定组件。）

如果您已安装 Controller（在此计算机上或在其他计算机上），并且想要安装其他组件，请从 **Extend Deployment** 部分选择该组件。

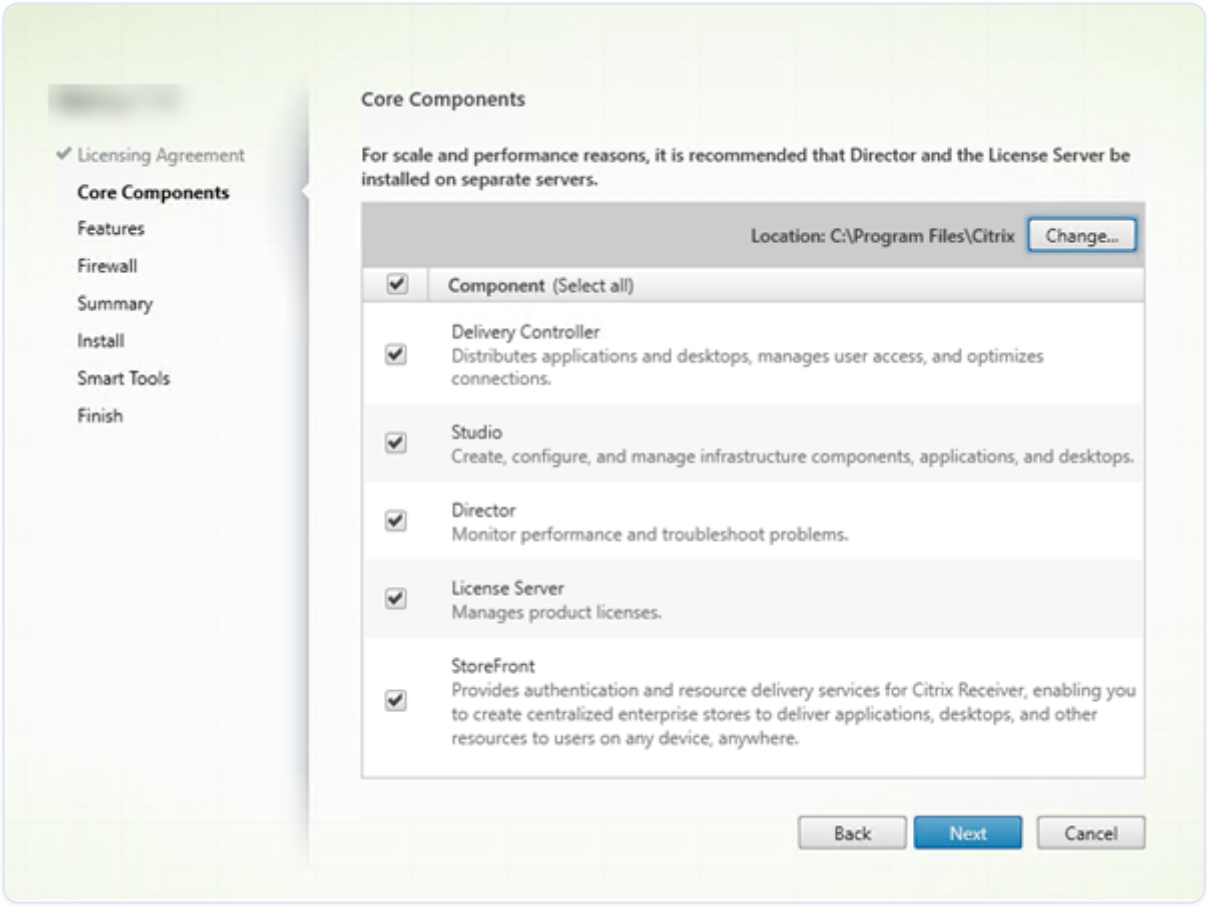
命令行选项：`/components`

## 步骤 4. 阅读并接受许可协议




在 **许可协议** 页面上，阅读许可协议后，请指明您已阅读并接受该协议。然后单击 **下一步**。

## 步骤 5. 选择要安装的组件和安装位置




在 **核心组件** 页面上：

- **位置：** 默认情况下，组件安装在 `C:\Program Files\Citrix` 中。对于大多数部署而言，默认位置即可。如果您指定了不同的位置，则该位置必须对网络服务具有执行权限。
- **组件：** 默认情况下，所有核心组件的复选框均已选中。将所有核心组件安装在一台服务器上适用于概念验证、测试或小型生产部署。对于大型生产环境，Citrix 建议将 Director、StoreFront 和 License Server 安装在单独的服务器上。

> **注意：**
>
> 如果您要在多台服务器上安装组件，请先安装 Citrix License Server 和许可证，然后再在其他服务器上安装其他组件。有关指导，请参阅 (/zh-cn/licensing/licensing-guide-for-citrix-virtual-apps-desktops.html#automatic-installation) 的“自动安装”部分。

> 当您选择不在此计算机上安装所需的某个核心组件时，会出现一个图标提醒您。该提醒会提示您安装该组件，但并非必须在此计算机上安装。

单击**下一步**。

命令行选项：`/installdir`、`/components`、`/exclude`

### 硬件检查

安装或升级 Delivery Controller 时，系统会检查硬件。如果计算机的 RAM 小于建议量 (5 GB)，安装程序会发出警报，这可能会影响站点的稳定性。有关详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#hardware-requirements)。

**图形界面：** 将出现一个对话框。

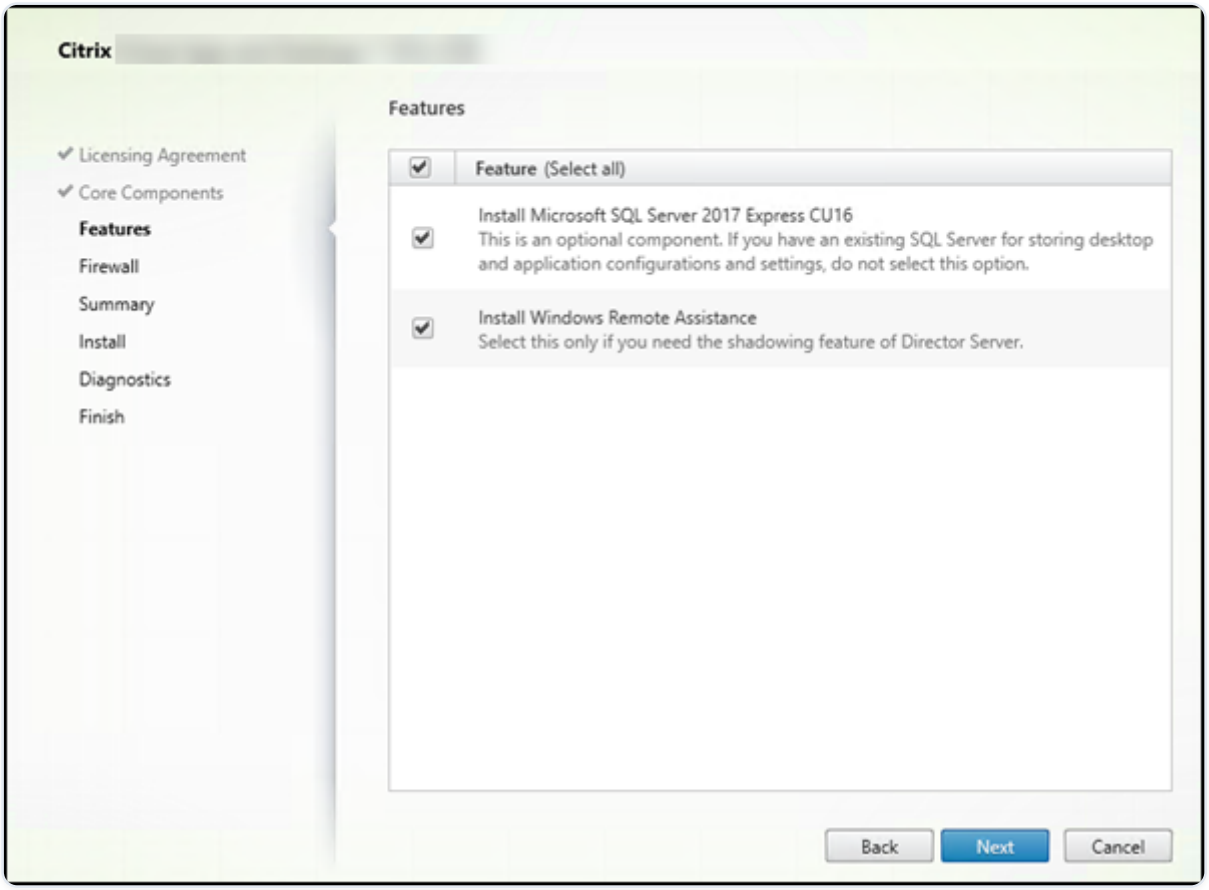
- 建议：单击 **取消** 以停止安装。向计算机添加更多 RAM，然后重新开始安装。
- 或者，单击 **下一步** 以继续安装。站点可能存在稳定性问题。

**命令行界面：** 安装/升级结束。安装日志包含一条消息，描述了发现的问题和可用选项。

- 建议：向计算机添加更多 RAM，然后再次运行该命令。
- 或者，使用 `/ignore_hw_check_failure` 选项再次运行该命令以覆盖警告。您的站点可能存在稳定性问题。

升级时，如果操作系统或 SQL Server 版本不再受支持，您也会收到通知。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/upgrade-migrate/upgrade.html)。

## 步骤 6. 启用或禁用功能



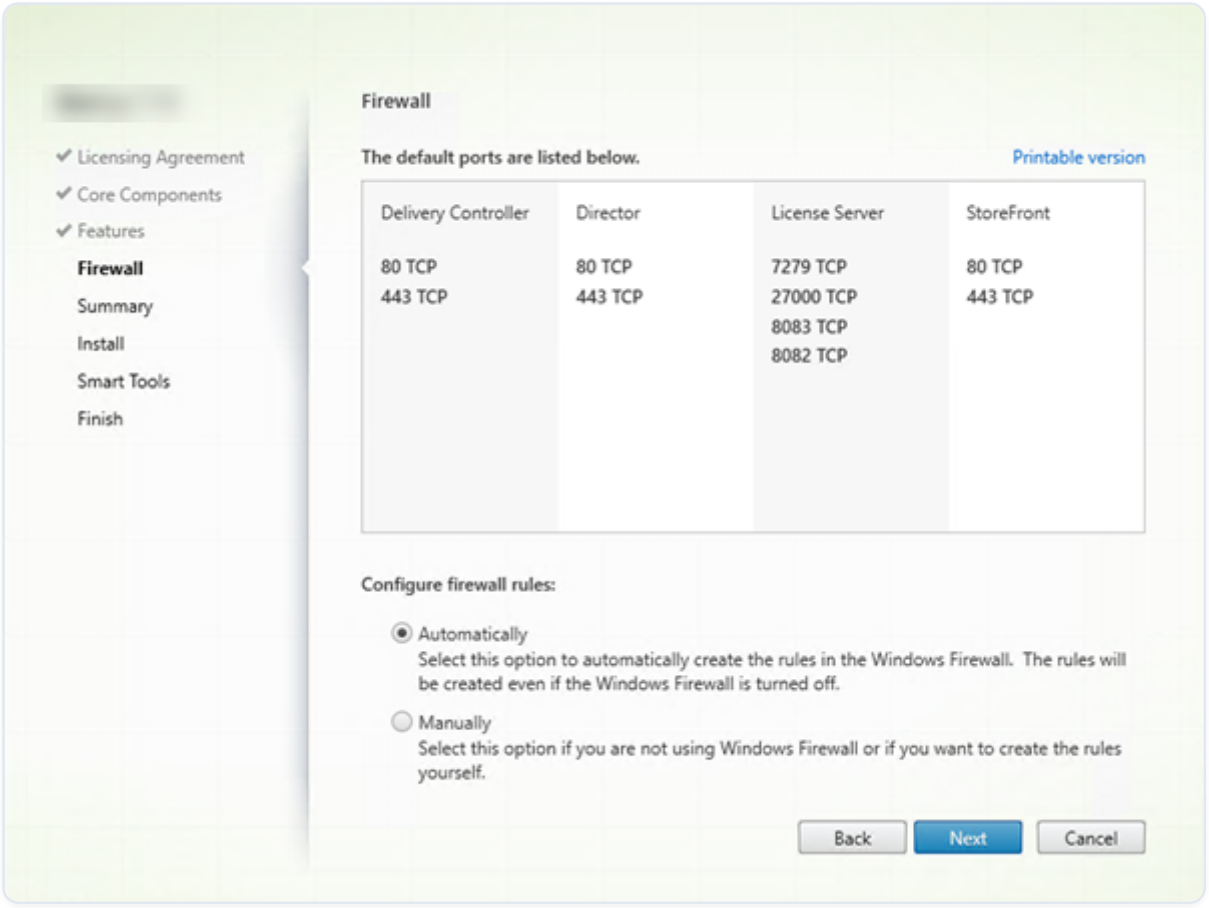

在“**功能**”页面上：

- 选择是否安装 Microsoft SQL Server Express 作为站点数据库。默认情况下，此选项处于启用状态。如果您不熟悉 Citrix Virtual Apps and Desktops 数据库，请查看数据库。
- 安装 Director 时，Windows 远程协助会自动安装。您可以选择是否在 Windows 远程协助中启用影子功能，以用于 Director 用户影子。启用影子功能会打开 TCP 端口 3389。默认情况下，此功能处于启用状态。默认设置适用于大多数部署。此功能仅在安装 Director 时显示。

单击**下一步**。

命令行选项：`/nosql`（阻止安装），`/no_remote_assistance`（阻止启用）

## 步骤 7. 打开 Windows 防火墙端口



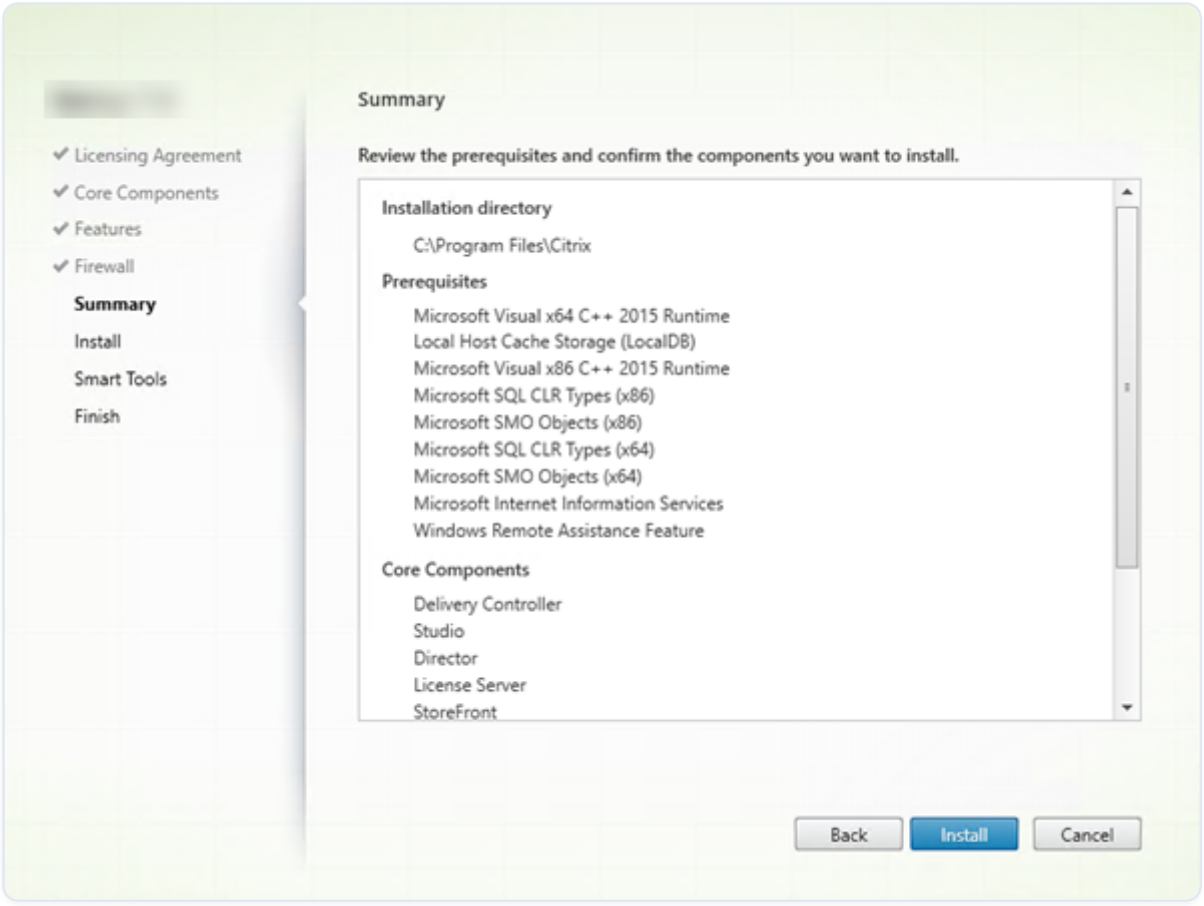

默认情况下，如果 Windows 防火墙服务正在运行，即使防火墙未启用，**防火墙**页面上的端口也会自动打开。默认设置适用于大多数部署。有关端口信息，请参阅网络端口。

单击**下一步**。

（该图显示了在此计算机上安装所有核心组件时的端口列表。此类安装通常仅用于测试部署。）

命令行选项：`/configure_firewall`

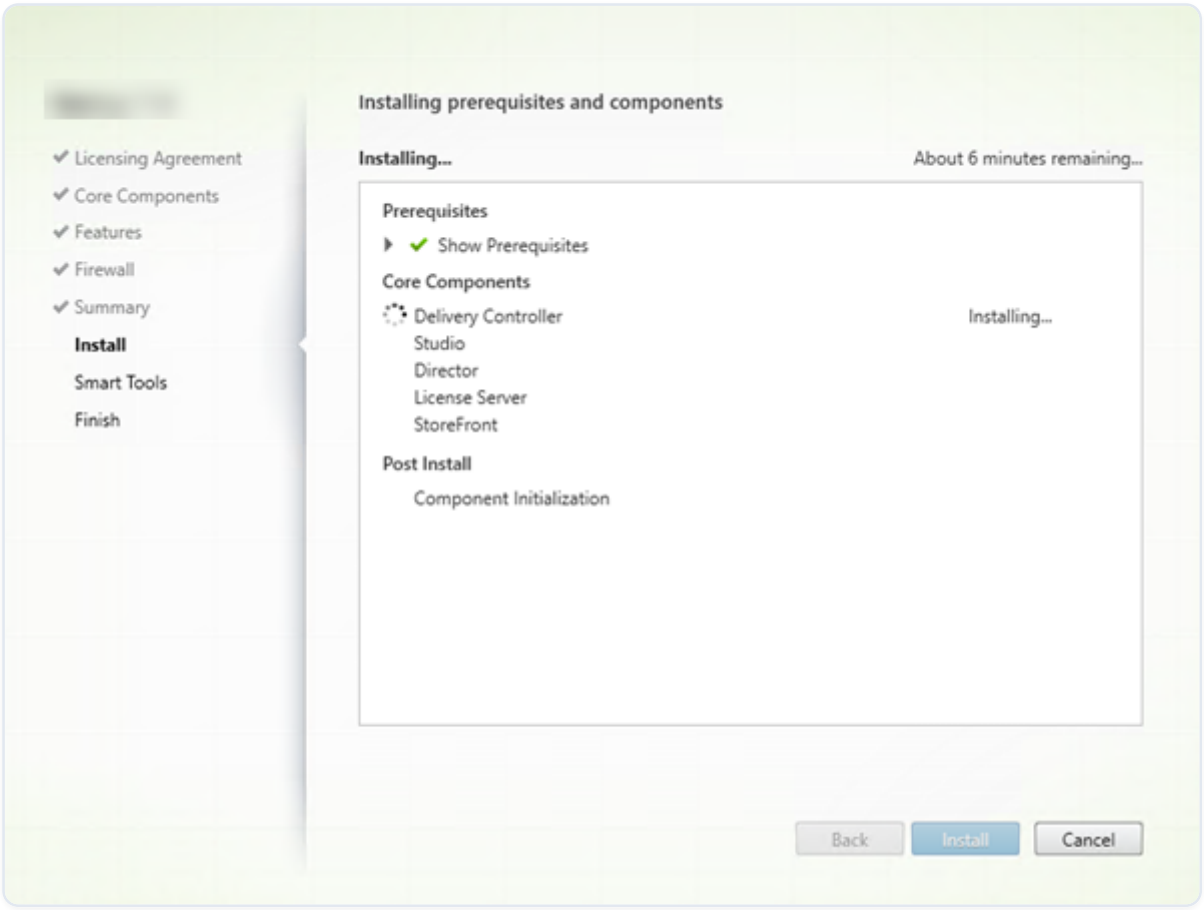
## 步骤 8. 查看必备项并确认安装




**摘要**页面列出了将要安装的内容。使用“**返回**”按钮返回到之前的向导页面并根据需要更改选择。

准备就绪后，单击“**安装**”。

显示屏显示安装进度：




## 步骤 9. 诊断

组件安装程序中的诊断页面(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/controller-diagnostic-1.png)

在**诊断**页面上，选择是否参与 Citrix Call Home。

使用图形界面安装 Delivery Controller 时，将显示此页面。安装 StoreFront（但不是 Controller）时，向导会显示此页面。安装其他核心组件（但不是 Controller 或 StoreFront）时，向导不会显示此页面。

在升级过程中，如果 Call Home 已启用，或者如果安装程序遇到与 Citrix Telemetry Service 相关的错误，则不会显示此页面。

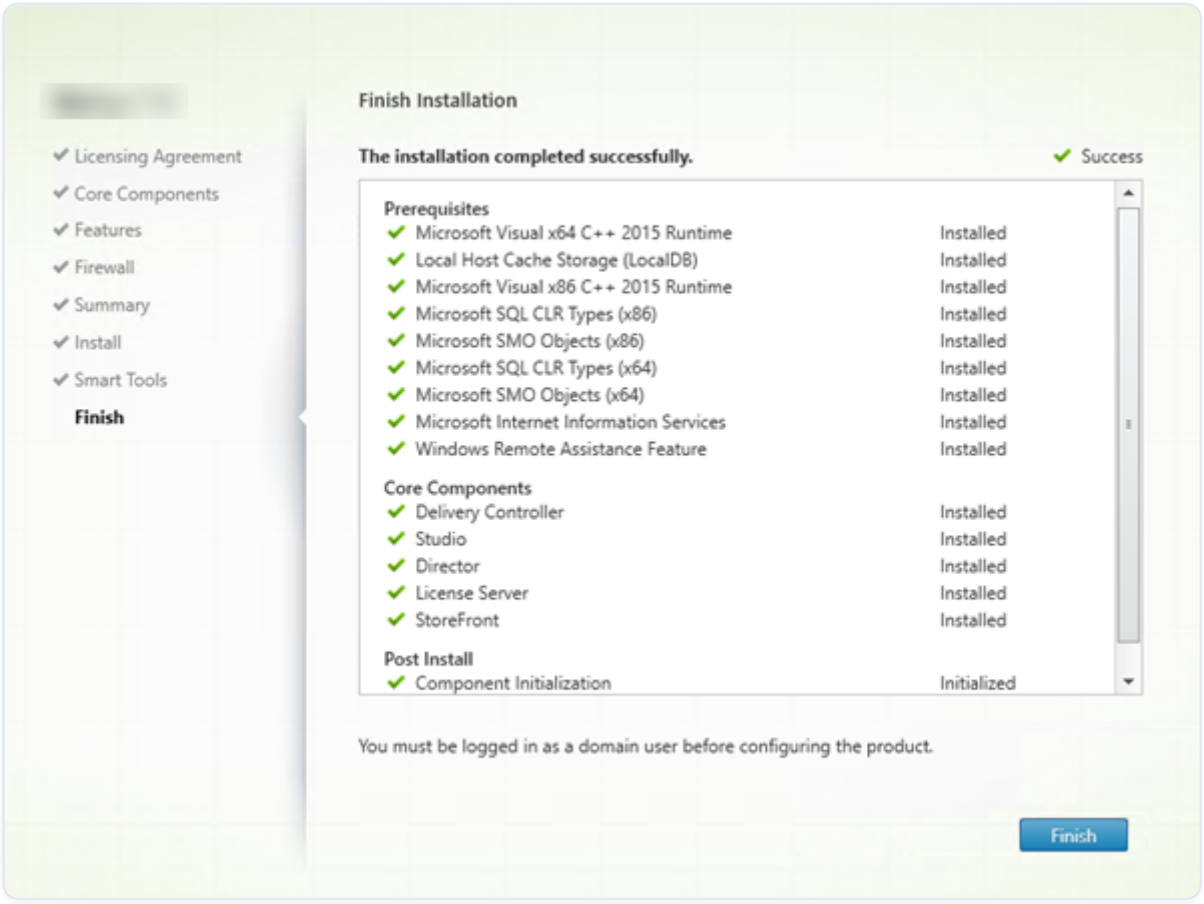
如果您选择参与（默认），请单击**连接**。出现提示时，输入您的 Citrix 帐户凭据。您可以在安装后更改您的注册选择。

凭据验证后（或者如果您选择不参与），单击**下一步**。

如果您在**诊断**页面上单击**连接**而未首先选择**收集诊断信息**，则在关闭**连接到 Citrix Insight Services** 对话框后，**下一步**按钮将禁用。您无法移动到下一页。要重新启用**下一步**按钮，请选择并立即取消选择**收集诊断信息**。

有关详细信息，请参阅Call Home。

## 步骤 10. 完成此安装




**完成**页面包含所有已成功安装和初始化的先决条件和组件的绿色复选标记。

单击“**完成**”。

## 步骤 11. 在其他计算机上安装剩余的核心组件

如果您已在一台计算机上安装所有核心组件，请继续执行后续步骤。否则，请在其他计算机上运行安装程序以安装其他组件。您还可以在其他服务器上安装更多 Controller。

## 后续步骤

安装所有必需组件后，使用 Studio 创建站点。

创建站点后，安装 VDA。

您可以随时使用完整产品安装程序通过以下组件扩展部署：

- **Universal Print Server 服务器组件：** 在打印服务器上启动安装程序。

  a. 在**扩展部署**部分中选择 **Universal Print Server**。

b. 接受许可协议。

c. 在**防火墙**页面上，如果 Windows 防火墙服务正在运行，即使防火墙未启用，默认情况下也会在防火墙中打开 TCP 端口 7229 和 8080。如果您想手动打开端口，可以禁用此默认操作。

要从命令行安装此组件，请参阅安装通用打印服务器的命令行选项。

- 联合身份验证服务。
- 会话录制。

# 安装 VDA

> **重要提示：**
>
> 如果您正在升级，并且当前版本安装了 Personal vDisk 或 AppDisks 软件，请参阅 删除 PvD、AppDisks 和不受支持的主机。
>
> Windows 计算机有两种类型的 VDA：适用于多会话操作系统的 VDA 和适用于单会话操作系统的 VDA。（有关适用于 Linux 计算机的 VDA 的信息，请参阅 Linux Virtual Delivery Agent 文档。）

在开始安装之前，请查看准备安装 并完成所有准备任务。

在安装 VDA 之前，请先安装核心组件。您也可以在安装 VDA 之前创建站点。

本文介绍了安装 VDA 时的安装向导序列。提供了命令行等效项。有关详细信息，请参阅使用命令行安装。

## 步骤 1. 下载产品软件并启动向导

如果您使用的是完整产品安装程序：

1. 如果您尚未下载产品 ISO：
   - 使用您的 Citrix 帐户凭据访问 Citrix Virtual Apps and Desktops™ 下载页面。下载产品 ISO 文件。
   - 解压缩文件。或者，刻录 ISO 文件的 DVD。
2. 在安装 VDA 的映像或计算机上使用本地管理员帐户。将 DVD 插入驱动器或装载 ISO 文件。如果安装程序未自动启动，请双击 **AutoSelect** 应用程序或装载的驱动器。

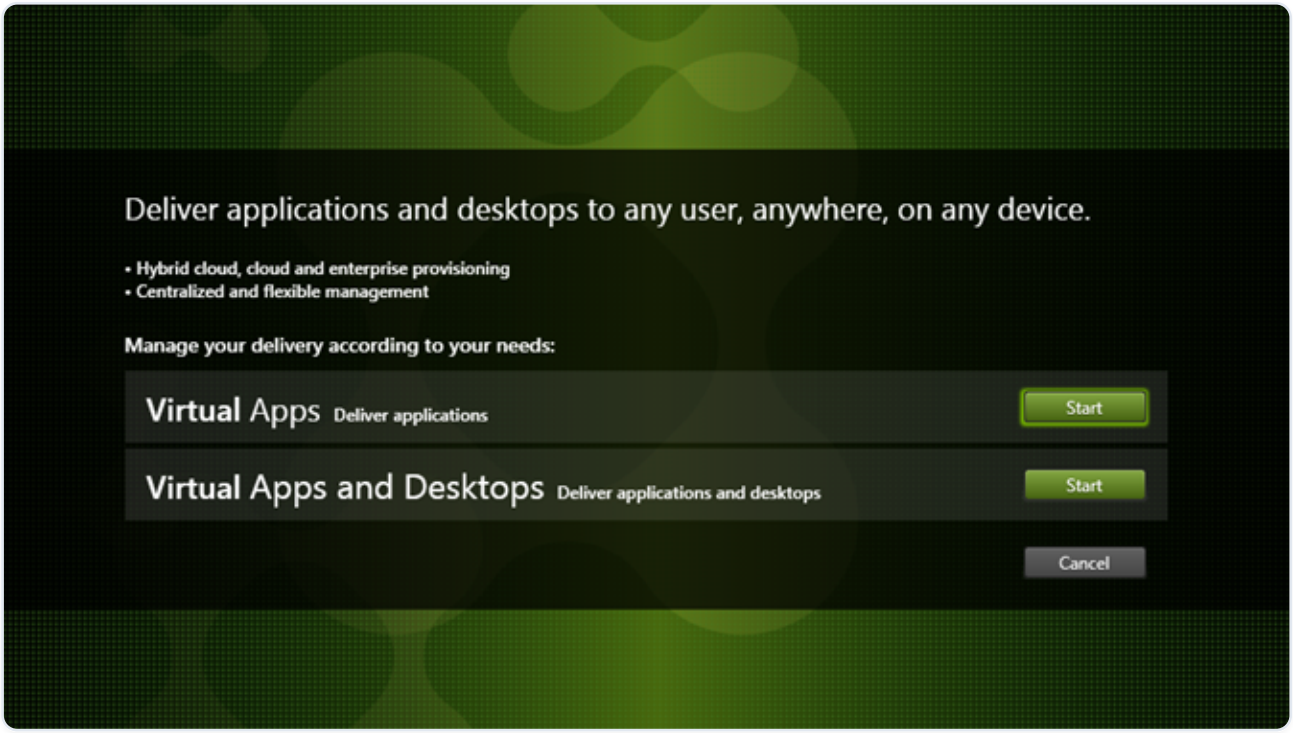
安装向导启动。

如果您使用的是独立软件包：

1. 使用您的 Citrix 帐户凭据访问 Citrix Virtual Apps and Desktops 下载页面。下载相应的软件包：
   - `VDAServerSetup.exe`：多会话操作系统 VDA *版本*
   - `VDAWorkstationSetup.exe`：单会话操作系统 VDA *版本*
   - `VDAWorkstationCoreSetup.exe`：单会话操作系统核心服务 VDA *版本*
2. 右键单击软件包并选择**以管理员身份运行**。

   安装向导启动。

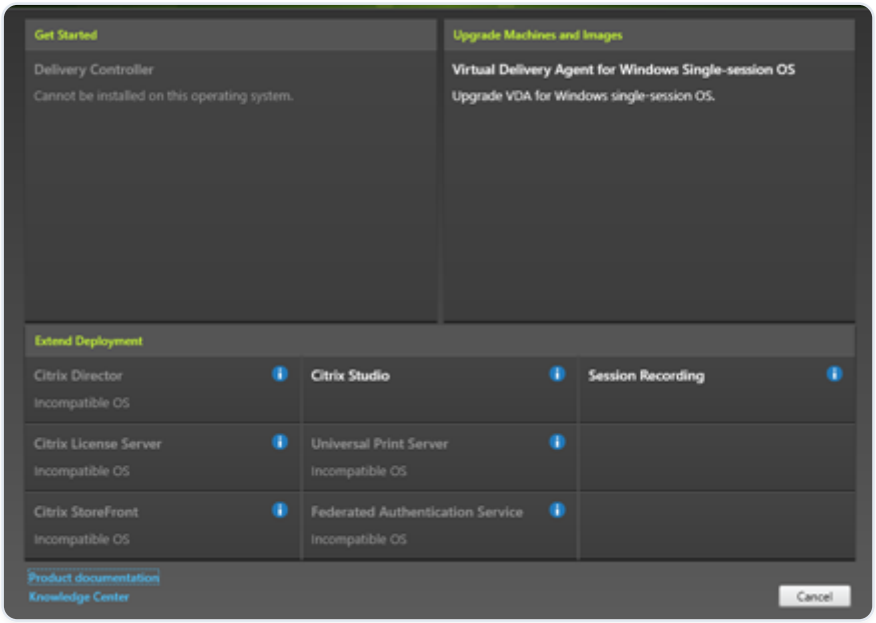
## 步骤 2. 选择要安装的产品




单击要安装的产品旁边的**开始**：Citrix Virtual Apps 或 Citrix Virtual Desktops。（如果计算机已安装 Citrix Virtual Apps 或 Citrix Virtual Desktops 组件，则此页面不会出现。）

命令行选项：`/xenapp` 以安装 Citrix Virtual Apps。如果省略此选项，则安装 Citrix Virtual Desktops。

## 步骤 3. 选择 VDA

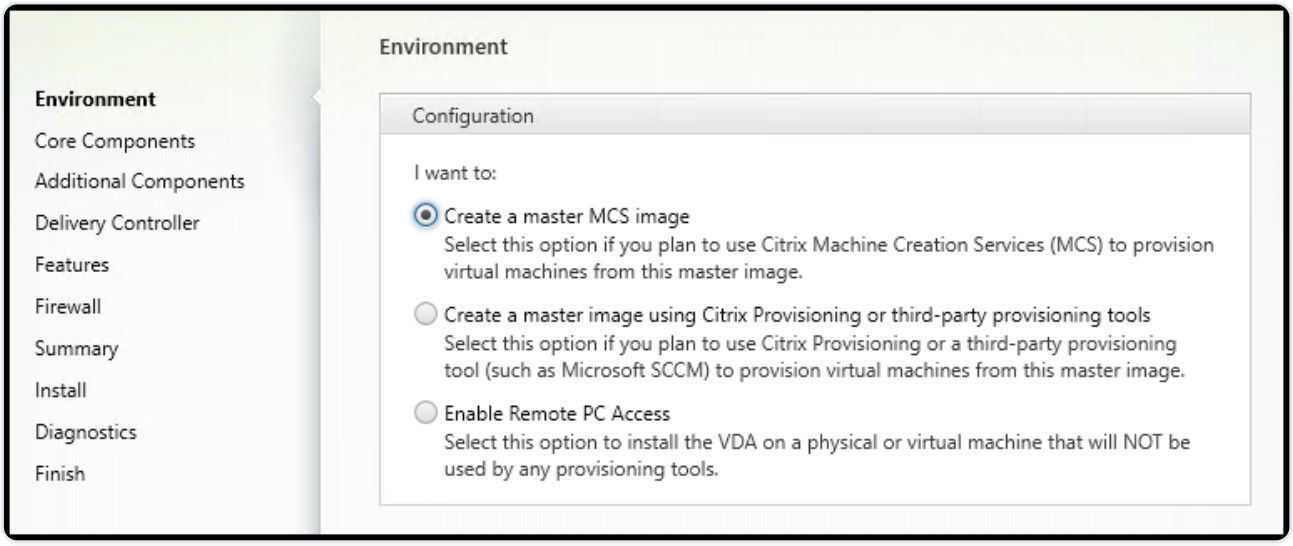



选择**虚拟投递代理**条目。安装程序知道它是在单会话还是多会话操作系统上运行，因此它只提供适当的 VDA 类型。

例如，当您在 Windows Server 2016 计算机上运行安装程序时，多会话操作系统 VDA 选项可用。不提供单会话操作系统 VDA 选项。

如果您尝试在不支持此 Citrix Virtual Apps and Desktops 版本的操作系统上安装（或升级到）Windows VDA，将显示一条消息，引导您了解有关选项的信息。

## 步骤 4. 指定 VDA 的使用方式




在**环境**页面上，指定您计划如何使用 VDA，指示您是否将此计算机用作预配更多计算机的映像。

您选择的选项会影响自动安装哪些 Citrix provisioning™ 工具（如果有），以及 VDA 安装程序“附加组件”页面上的默认值。

安装 VDA 时，会自动安装多个 MSI（预配和其他）。防止其安装的唯一方法是在命令行安装中使用 `/exclude` 选项。

请选择以下选项之一：

- **创建主 MCS 映像：** 如果您计划使用 Machine Creation Services™ 预配 VM，请选择此选项以在 VM 映像上安装 VDA。此选项将安装 Machine Identity Service。这是默认选项。

  命令行选项：`/mastermcsimage` 或 `/masterimage`

> **重要提示：**
>
> 安装介质或 ISO 映像必须在本地装载。不支持从网络驱动器装载 ISO 映像以安装软件。

- **使用 Citrix Provisioning 或第三方预配工具创建主映像：** 如果您计划使用 Citrix Provisioning 或第三方预配工具（例如 Microsoft System Center Configuration Manager）预配 VM，请选择此选项以在 VM 映像上安装 VDA。

  命令行选项：`/masterpvsimage`

- （仅在多会话操作系统计算机上显示）**启用与服务器的代理连接：** 选择此选项可在不作为映像预配其他计算机的物理或虚拟机上安装 VDA。

  命令行选项：`/remotepc`

- （仅在单会话操作系统计算机上显示）**启用远程电脑访问：** 选择此选项可在物理计算机上安装 VDA，以用于远程电脑访问。

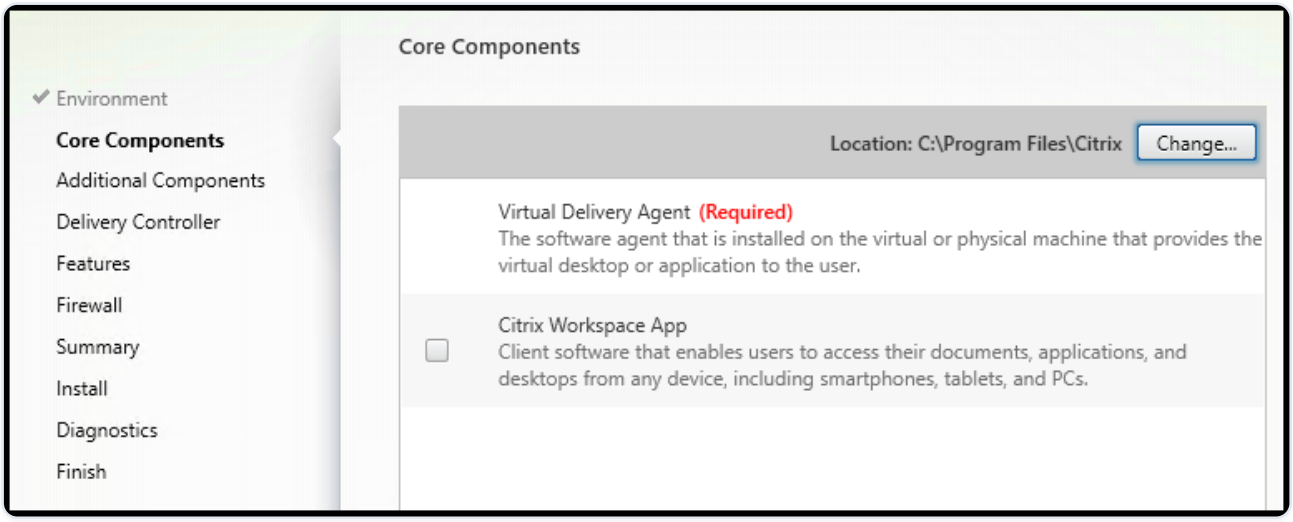
  命令行选项：`/remotepc`

单击**下一步**。

此页面不显示：

- 如果您正在升级 VDA
- 如果您正在使用 `VDAWorkstationCoreSetup.exe` 安装程序

## 步骤 5. 选择要安装的组件和安装位置



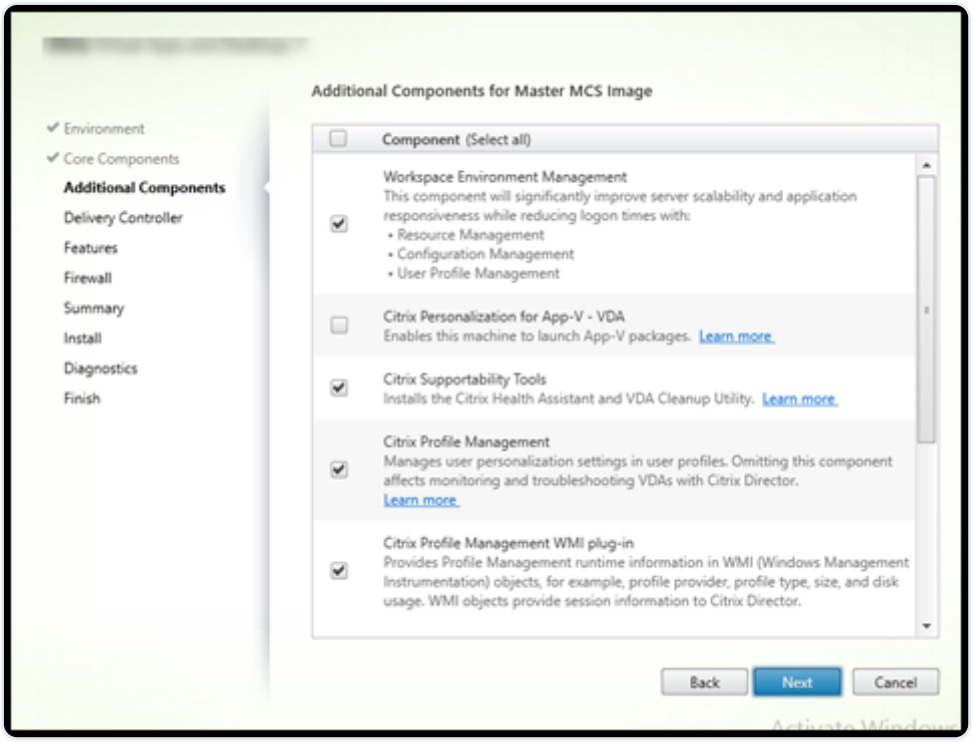

在“**核心组件**”页面上：

- **位置：** 默认情况下，组件安装在 `C:\Program Files\Citrix` 中。此默认设置适用于大多数部署。如果您指定不同的位置，该位置必须具有网络服务的执行权限。
- **组件：** 默认情况下，Citrix Workspace app for Windows 不随 VDA 一起安装。如果您使用的是 `VDAWorkstationCoreSetup.exe` 安装程序，则 Citrix Workspace app for Windows 永远不会安装，因此不显示此复选框。

单击**下一步**。

命令行选项：`/installdir`、`/components vda,plugin` 用于安装 VDA 和 Citrix Workspace app for Windows

## 步骤 6. 安装附加组件




“**其他组件**”页面包含用于启用或禁用随 VDA 安装其他功能和技术的复选框。在命令行安装中，您可以使用 `/exclude` 或 `/includeadditional` 选项明确省略或包含一个或多个可用组件：

- **/includeadditional** "*组件*"\[,"*组件*"\] ...
- **/排除** "*组件*"\[,"*组件*"\] ...

下表指示此页面上项目的默认设置。默认设置取决于您在**环境**页面上选择的选项。

| 附加组件页面 | 环境页面：“带有 MCS 的主映像”或“带有 CITRIX PROVISIONING 的主映像”已选择 | 环境页面：“启用与服务器的代理连接”（适用于多会话操作系统）或“远程电脑访问”（适用于单会话操作系统）已选择 |
| --- | --- | --- |
| 工作区环境管理™ | 未选择 | 未选择 |
| 适用于 App-V 的 Citrix 个性化 | 未选择 | 未选择 |
| 用户个性化层 | 未选择 | 未显示，因为它不适用于此用例。 |
| Citrix 可支持性工具 | 已选择 | 未选择 |
| Citrix 配置文件管理 | 已选择 | 未选择 |
| Citrix 配置文件管理 WMI 插件 | 已选择 | 未选择 |

| 附加组件页面 | 环境页面：“带有 MCS 的主映像”或“带有 CITRIX PROVISIONING 的主映像”已选择 | 环境页面：“启用与服务器的代理连接”（适用于多会话操作系统）或“远程电脑访问”（适用于单会话操作系统）已选择 |
| --- | --- | --- |
| Citrix VDA 升级代理 | 未选择 | 未选择 |
| 适用于 Windows 的 Citrix Files | 未选择 | 未选择 |
| 适用于 Outlook 的 Citrix Files | 未选择 | 未选择 |
| MCSIO 写入缓存以优化存储 | 未选择 | 未选择 |
| Rendezvous 协议配置 | 未选择 | 未选择 |

如果出现以下情况，此页面将不显示：

- 您正在使用 `VDAWorkstationCoreSetup.exe` 安装程序。此外，附加组件的命令行选项不适用于该安装程序。
- 您正在升级 VDA 并且所有附加组件均已安装。如果某些附加组件已安装，则此页面仅列出未安装的组件。

选择或清除以下复选框。（组件在安装程序中显示的顺序可能不同。）

- **Workspace Environment Management：** 如果您的部署使用 Citrix Workspace Environment Management，请安装此组件。有关详细信息，请参阅 Workspace Environment Management。

  命令行选项：`/includeadditional "Citrix WEM Agent"` 启用组件安装，`/exclude "Citrix WEM Agent"` 阻止组件安装

- **Citrix Personalization for App-V：** 如果您使用 Microsoft App-V 软件包中的应用程序，请安装此组件。有关详细信息，请参阅 App-V。

  命令行选项：`/includeadditional "Citrix Personalization for App-V – VDA"` 启用组件安装，`/exclude "Citrix Personalization for App-V – VDA"` 阻止组件安装

- **Citrix 用户个性化层：** 安装用户个性化层的 MSI。有关详细信息，请参阅用户个性化层。

  此组件仅在单会话 Windows 10 计算机上安装 VDA 时显示。

  命令行选项：`/includeadditional "User Personalization Layer"` 启用组件安装，`/exclude "User Personalization Layer"` 阻止组件安装

- **Citrix 可支持性工具** 安装包含 Citrix 可支持性工具（例如 Citrix Health Assistant）的 MSI。

  命令行选项：`/includeadditional "Citrix Supportability Tools"` 启用组件安装，`/exclude "Citrix Supportability Tools"` 阻止组件安装

- **Citrix 配置文件管理：** 此组件管理用户配置文件中的用户个性化设置。有关详细信息，请参阅配置文件管理。

  在安装中排除 Citrix Profile Management 会影响使用 Citrix Director 对 VDA 进行监视和故障排除。在“**用户详细信息**”和“**端点**”页面上，“**个性化**”面板和“**登录持续时间**”面板将失败。在“**控制板**”和“**趋势**”页面上，“**平均登录持续时间**”面板仅显示已安装 Profile Management 的计算机的数据。

  即使您正在使用第三方用户配置文件管理解决方案，Citrix 仍建议您安装并运行 Citrix Profile Management Service。不需要启用 Citrix Profile Management Service。

  命令行选项：`/includeadditional "Citrix Profile Management"` 启用组件安装，`/exclude "Citrix Profile Management"` 阻止组件安装

- **Citrix Profile Management WMI 插件：** 此插件在 WMI (Windows Management Instrumentation) 对象中提供 Profile Management 运行时信息（例如，配置文件提供程序、配置文件类型、大小和磁盘使用情况）。WMI 对象向 Director 提供会话信息。

  命令行选项：`/includeadditional "Citrix Profile Management WMI Plugin"` 启用组件安装，`/exclude "Citrix Profile Management WMI Plugin"` 阻止组件安装

- **VDA 升级代理：** 仅适用于 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）部署。使 VDA 能够参与VDA 升级功能。您可以使用该功能从管理控制台立即或在计划时间升级目录的 VDA。如果未安装此代理，您可以通过在计算机上运行 VDA 安装程序来升级 VDA。

  命令行选项：`/includeadditional "Citrix VDA Upgrade Agent"` 启用组件安装，`/exclude "Citrix VDA Upgrade Agent"` 阻止组件安装

- **适用于 Windows 的 Citrix Files：** 此组件使用户能够连接到其 Citrix Files 帐户。然后，他们可以通过 Windows 文件系统中的映射驱动器与 Citrix Files 交互（无需完全同步其内容）。有关详细信息，请参阅 Content Collaboration。

  命令行选项：`/includeadditional "Citrix Files for Windows"` 启用组件安装，`/exclude "Citrix Files for Windows"` 阻止组件安装

- **适用于 Outlook 的 Citrix Files：** 适用于 Outlook 的 Citrix Files 允许您通过 Citrix Files 发送附件或电子邮件，从而绕过文件大小限制并增加安全性。您可以直接在电子邮件中为同事、客户和合作伙伴提供安全的 文件上传请求。有关详细信息，请参阅 Content Collaboration。

命令行选项：`/includeadditional "Citrix Files for Outlook"` 启用组件安装，`/exclude "Citrix Files for Outlook"` 阻止组件安装

- **用于存储优化的 MCSIO 写入缓存：** 安装 Citrix MCS IO 驱动程序。有关详细信息，请参阅 Storage shared by hypervisors 和 Configure cache for temporary data。

  命令行选项：`/includeadditional "Citrix MCS IODriver"` 启用组件安装，`/exclude "Citrix MCS IODriver"` 阻止组件安装

- **Rendezvous 代理配置：** 如果您计划在您的环境中使用 Rendezvous 协议和 Citrix Gateway Service，并且您的网络中存在用于出站连接的非透明代理，请安装此组件。仅支持 HTTP 代理。

  如果安装此组件，请在“**Rendezvous 代理配置**”页面上指定代理地址或 PAC 文件路径。有关功能详细信息，请参阅Rendezvous 协议。

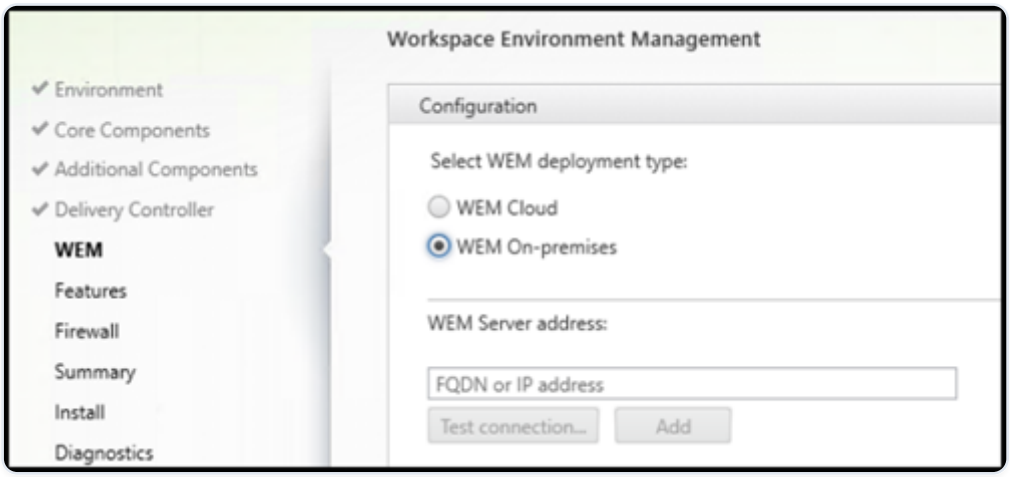
  命令行选项：`/includeadditional "Citrix Rendezvous V2"` 启用组件安装，`/exclude "Citrix Rendezvous V2"` 阻止组件安装

## 步骤 7. 工作区环境管理

**Workspace Environment Management** (WEM) 页面仅在您在**附加组件**页面上启用相应的复选框时显示。

1. 选择您是拥有 WEM 本地部署还是 WEM 云（服务）部署。
2. 添加 FQDN 或 IP 地址。特殊字符将被忽略。

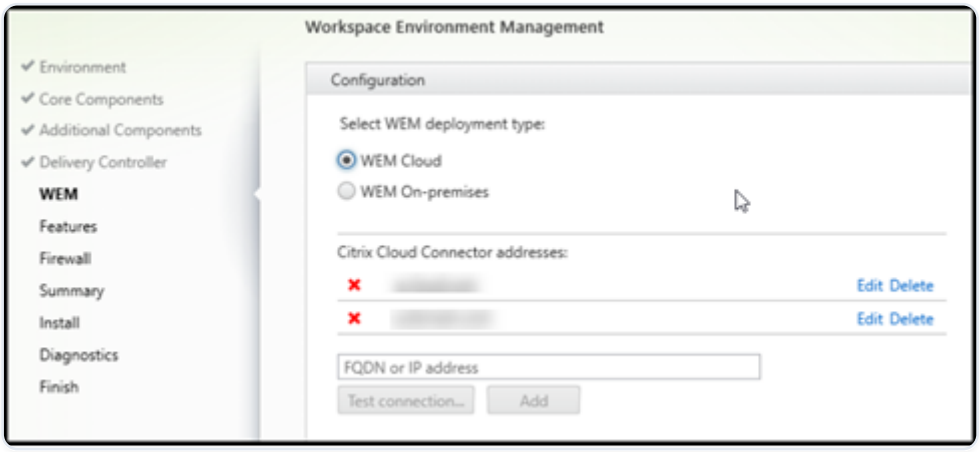
   - 对于 WEM 本地部署：WEM 基础架构服务器地址




> **注意：**

> 当您测试 WEM 服务器连接时，可能会看到以下错误消息：`Unable to establish connection with "<the address you entered>"`。如果地址正确且服务器可访问，则可以忽略此消息。

- 对于 WEM 服务：Cloud Connector 地址

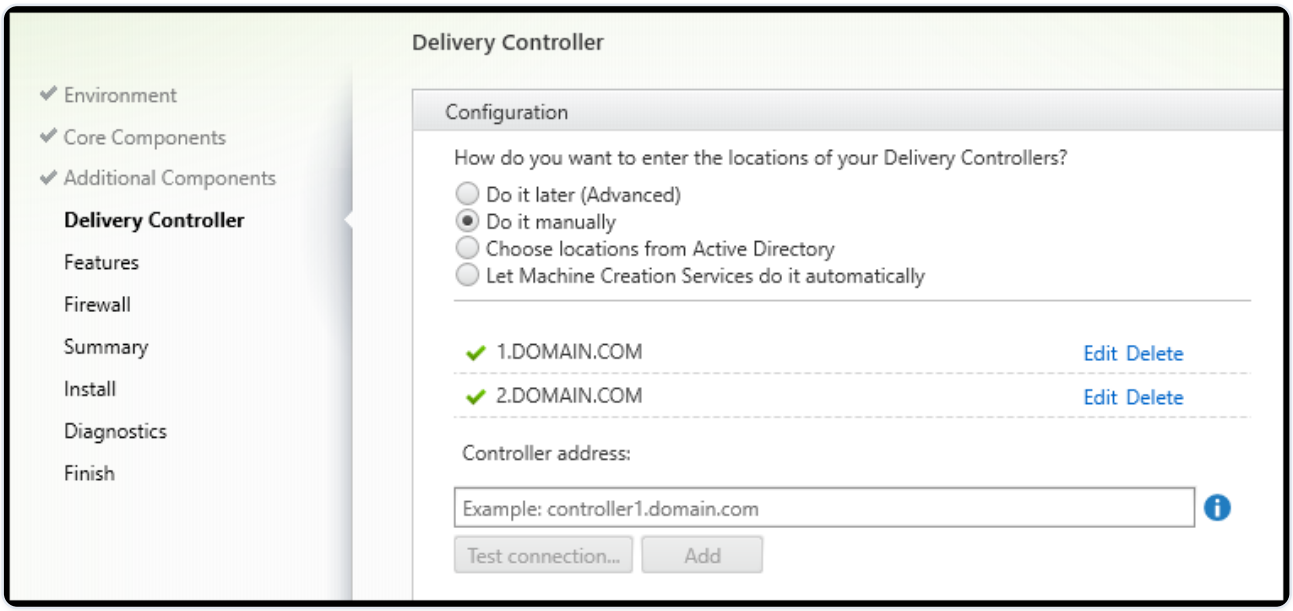



3. 单击**测试连接**。防火墙中必须打开该端口。
4. 连接测试成功后，单击**添加**。
5. 对于 WEM 服务部署，对其他 Cloud Connector 重复步骤 2-4。
6. 单击**下一步**。

命令行选项：`/wem_server`、`/wem_cloud_connectors`

命令行界面中提供了更多 WEM 代理配置选项。请参阅命令行安装选项。

## 步骤 8. Delivery Controller™ 地址



在“**Delivery Controller**”页面上，选择输入已安装 Controller 地址的方式。Citrix 建议您在安装 VDA 时指定地址（**手动执行**）。VDA 必须拥有此信息才能向 Controller 注册。如果 VDA 无法注册，用户将无法访问该 VDA 上的应用程序和桌面。

- **手动执行：**（默认）输入已安装 Controller 的 FQDN，然后单击“**添加**”。如果您安装了更多 Controller，请添加它们的地址。
- **稍后执行 (高级)：** 如果选择此选项，向导会要求您确认是否要继续。要稍后指定地址，可以重新运行安装程序或使用 Citrix 组策略。向导也会在**摘要**页面上提醒您。
- **从 Active Directory 中选择位置：** 仅当计算机已加入域且用户是域用户时有效。
- **让 Machine Creation Services 自动执行：** 仅在使用 MCS 预配计算机时有效。

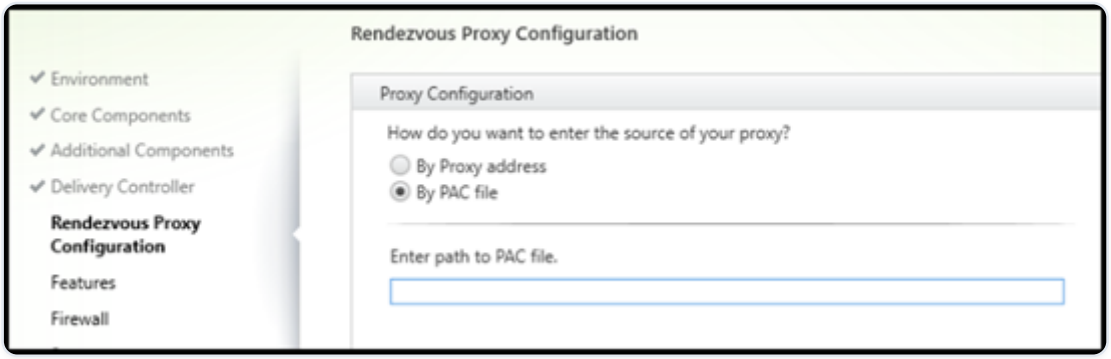
单击“**下一步**”。如果您选择了“**稍后执行（高级）**”，系统会提示您确认稍后指定 Controller 地址。

其他注意事项：

- 地址不能包含非字母数字字符。
- 如果您在 VDA 安装期间和组策略中指定了地址，则策略设置将覆盖安装期间提供的设置。
- VDA 成功注册要求用于与 Controller 通信的防火墙端口处于打开状态。此操作在向导的“**防火墙**”页面上默认启用。
- 指定 Controller 位置后（在 VDA 安装期间或之后），您可以使用自动更新功能在添加或删除 Controller 时更新 VDA。有关 VDA 如何发现 Controller 并向其注册的详细信息，请参阅VDA 注册。

命令行选项：`/controllers`

## 步骤 9. Rendezvous 代理配置




仅当您在**附加组件**页面上启用了**Rendezvous 代理配置**复选框时，才会显示**Rendezvous 代理配置**页面。

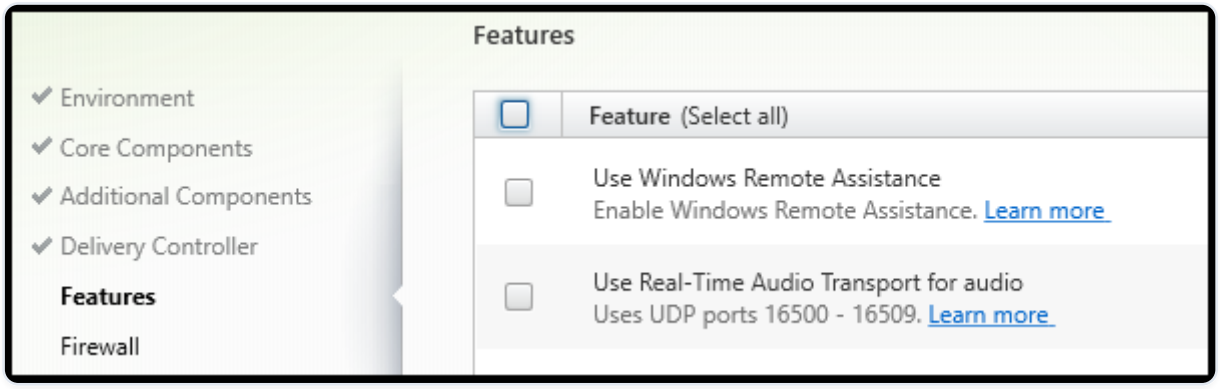
1. 选择您将通过代理地址还是 PAC 文件路径指定代理源。
2. 指定代理地址或 PAC 文件路径。

- 代理地址格式：`http://<url-or-ip>:<port>`
- PAC 文件格式：`http://<url-or-ip>:<port>/<path>/<filename>.pac`

代理端口的防火墙必须打开，连接测试才能成功。如果无法连接到代理，您可以选择是否继续 VDA 安装。

命令行选项：`/proxyconfig`

## 步骤 10. 启用或禁用功能




在“**功能**”页面上，使用复选框启用或禁用您要使用的功能。

- **使用 Windows 远程协助：** 启用此功能后，Windows 远程协助将与 Director 的用户影子功能一起使用。Windows 远程协助会在防火墙中打开动态端口。（默认 = 禁用）

  命令行选项：`/enable_remote_assistance`

- **使用实时音频传输进行音频传输**：如果您的网络中广泛使用 IP 语音，请启用此功能。此功能可降低延迟并提高音频在有损网络中的弹性。它允许使用 RTP 通过 UDP 传输音频数据。（默认 = 禁用）

  命令行选项：`/enable_real_time_transport`

- **使用屏幕共享**：启用后，屏幕共享使用的端口将在 Windows 防火墙中打开。（默认 = 禁用）

  命令行选项：`/enable_ss_ports`

- **此 VDA 是否安装在云中的 VM 上**：此设置有助于 Citrix 正确识别本地和服务 (Citrix Cloud™) VDA 部署的资源位置，以用于遥测目的。此功能对客户侧利用率没有影响。如果您的部署使用 Citrix DaaS，请启用此设置（默认 = 禁用）。

  命令行选项：`/xendesktopcloud`

如果此页面包含名为 **MCS I/O** 的功能，请勿使用它。MCS IO 功能在**附加组件**页面上配置。

单击**下一步**。

## 步骤 11. 防火墙端口

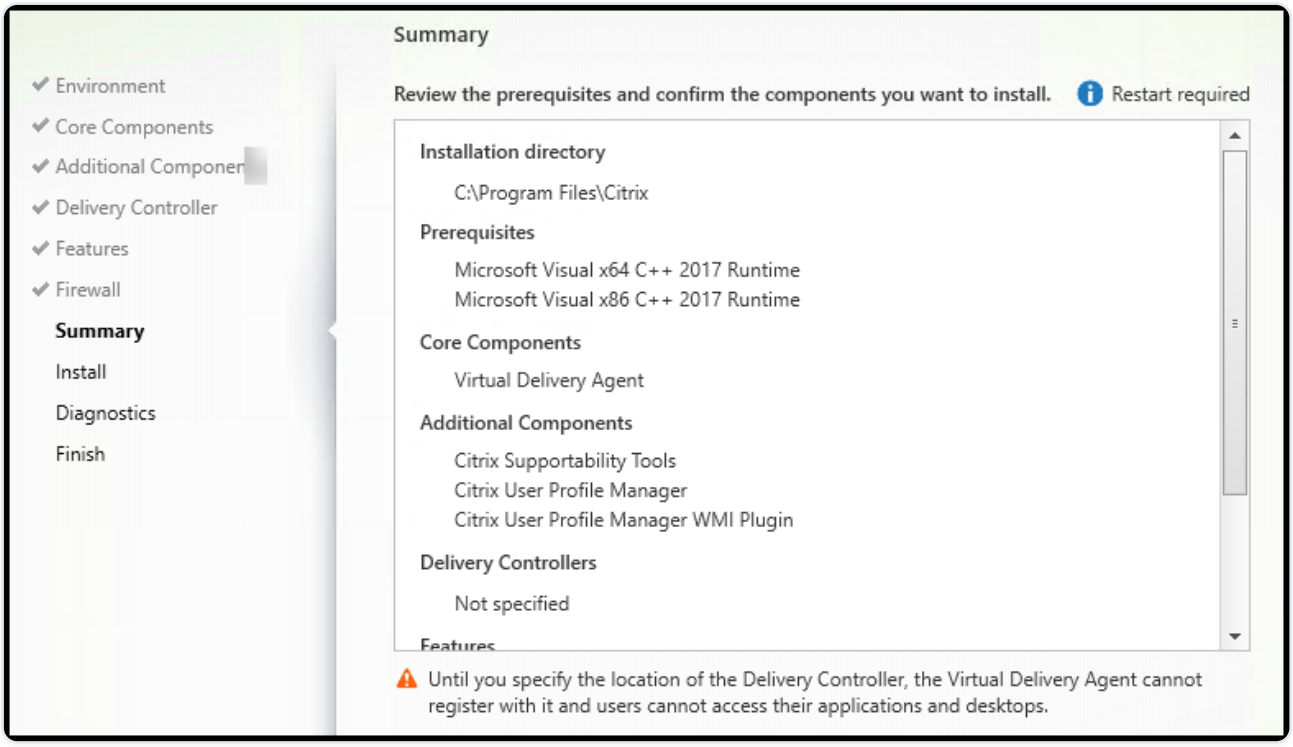



在**防火墙**页面上，如果 Windows 防火墙服务正在运行，即使防火墙未启用，端口也会默认自动打开。此默认设置适用于大多数部署。有关端口信息，请参阅网络端口。

单击**下一步**。

命令行选项：`/enable_hdx_ports`

## 步骤 12. 查看先决条件并确认安装



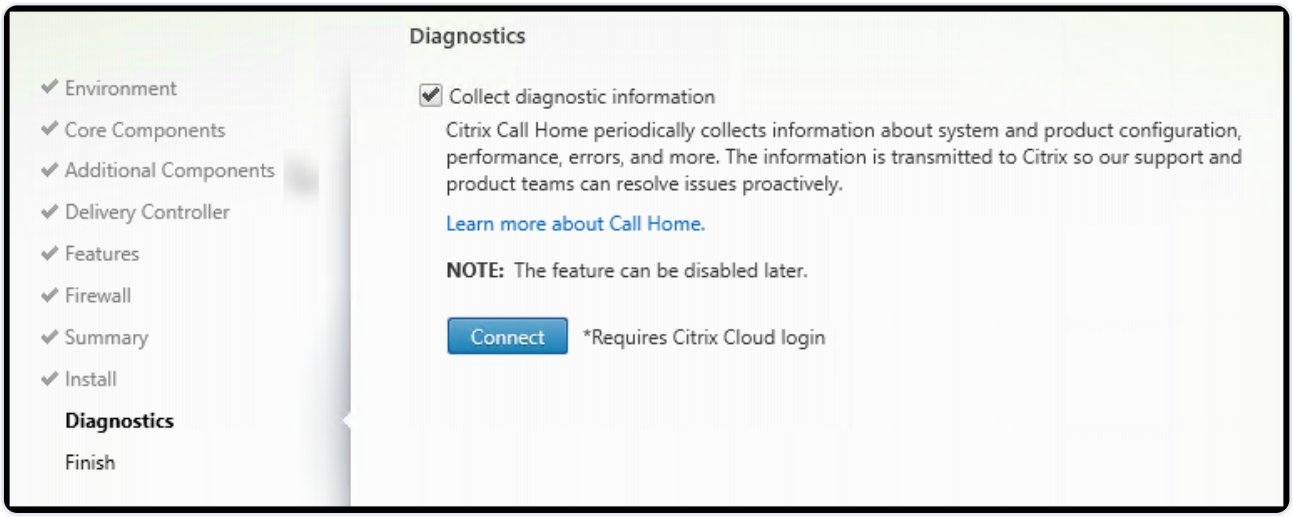

**摘要**页面列出了将要安装的内容。使用**返回**按钮返回到之前的向导页面并更改选择。

(仅限单会话 VDA) 选中**如果更新失败则启用自动还原**复选框以启用失败时还原功能。有关详细信息，请参阅安装或升级失败时还原。

准备就绪后，单击**安装**。

如果先决条件尚未安装或启用，计算机可能会重启一次或多次。请参阅准备安装。

## 步骤 13. 诊断



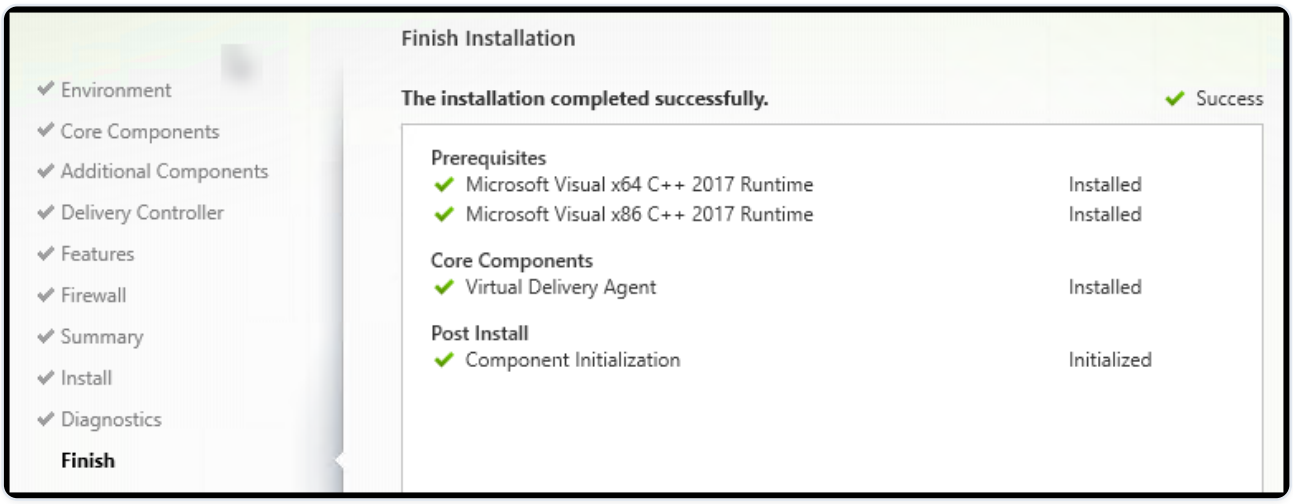

在**诊断**页面上，选择是否参与 Citrix Call Home。如果您选择参与（默认），请单击**连接**。出现提示时，输入您的 Citrix 帐户凭据。

凭据验证成功后（或者如果您选择不参与），请单击**下一步**。

使用完整产品安装程序时，如果您在**诊断**页面上单击**连接**而未首先选择**收集诊断信息**，则在关闭**连接到 Citrix Insight Services**对话框后，**下一步**按钮将处于禁用状态。您无法移动到下一页。要重新启用**下一步**按钮，请选择并立即取消选择**收集诊断信息**。

有关详细信息，请参阅Call Home。

## 步骤 14. 完成此安装




**完成**页面包含所有已成功安装和初始化的必备项和组件的绿色复选标记。

单击**完成**。默认情况下，计算机将自动重启。尽管您可以禁用此自动重启，但在计算机重启之前，VDA 无法使用。

## 后续步骤

根据需要，重复上述过程在其他计算机或映像上安装 VDA。

安装所有 VDA 后，启动 Studio。如果您尚未创建站点，Studio 会自动引导您完成该任务。完成该任务后，Studio 会引导您创建计算机目录，然后创建交付组。请参阅：

- 创建站点
- 创建计算机目录
- 创建交付组

## Citrix 优化器

Citrix Optimizer 是一款适用于 Windows 操作系统的工具，可帮助 Citrix 管理员通过删除和优化各种组件来优化 VDA。

安装 VDA 并完成最终重新启动后，下载并安装 Citrix Optimizer。请参阅 CTX224676。该 CTX 文章包含下载包以及有关安装和使用 Citrix Optimizer 的说明。

### 自定义 VDA

要自定义已安装的 VDA：

1. 在 Windows 的“删除或更改程序”功能中，选择“**Citrix Virtual Delivery Agent**”或“**Citrix Remote PC Access/VDI Core Services VDA**”。然后右键单击并选择“**更改**”。
2. 选择**自定义 Virtual Delivery Agent 设置**。安装程序启动后，您可以更改：
   - Controller 地址
   - 用于向 Controller 注册的 TCP/IP 端口（默认值 = 80）
   - 是否自动打开 Windows 防火墙端口

### 故障排除

- 有关 Citrix 如何报告组件安装结果的信息，请参阅 Citrix 安装返回代码。
- 在交付组的 Studio 显示中，**详细信息**窗格中的**已安装 VDA 版本**条目可能不是计算机上安装的版本。计算机的 Windows 程序和功能显示屏会显示实际的 VDA 版本。
- VDA 安装后，必须先向 Delivery Controller 注册，然后才能向用户交付应用程序或桌面。

  要了解 VDA 注册方法以及如何排查注册问题，请参阅VDA 注册。

## 使用命令行安装

> **重要提示：**
>
> 如果您正在升级，并且当前版本使用或安装了 Personal vDisk 或 AppDisks 软件，请参阅 删除 PvD、AppDisks 和不受支持的主机。

### 简介

本文适用于在安装了 Windows 操作系统的计算机上安装组件。有关适用于 Linux 操作系统的 VDA 的信息，请参阅 Linux Virtual Delivery Agents。

本文介绍了如何发出产品安装命令。在开始任何安装之前，请查看 准备安装。该文章包含可用安装程序的说明。

要查看命令执行进度和返回值，您必须是原始管理员或使用**以管理员身份运行**。有关详细信息，请参阅 Microsoft 命令文档。

作为直接使用安装命令的补充，产品 ISO 上提供了示例脚本，用于在 Active Directory 中的计算机上安装、升级或删除 VDA。有关详细信息，请参阅 使用脚本安装 VDA。

如果您尝试在不受此 Citrix Virtual Apps and Desktops 版本支持的 Windows 操作系统版本上安装或升级，则会显示一条消息，引导您了解相关选项。请参阅 早期操作系统。

有关 Citrix 如何报告组件安装结果的信息，请参阅 Citrix 安装返回代码。

## 使用完整产品安装程序

要访问完整产品安装程序的命令行界面：

1. 从 Citrix 下载产品包。访问下载站点需要 Citrix 帐户凭据。
2. 解压缩文件。或者，刻录 ISO 文件的 DVD。
3. 使用本地管理员帐户登录到要安装组件的服务器。
4. 将 DVD 插入驱动器或装载 ISO 文件。
5. 从介质上的 `\x64\XenDesktop Setup` 目录中，运行相应的命令。

   **要安装核心组件：** 运行 `XenDesktopServerSetup.exe`，并使用 安装核心组件的命令行选项 中列出的选项。

   **要安装 VDA：** 运行 `XenDesktopVDASetup.exe`，并使用 安装 VDA 的命令行选项 中列出的选项。

   **要安装 StoreFront：** 在安装介质的 `x64 > StoreFront` 文件夹中运行 `CitrixStoreFront-x64.exe`。

   **要安装 Universal Print Server：** 请遵循 安装 Universal Print Server 的命令行选项 中的指导。

   **要安装 Federated Authentication Service：** Citrix 建议使用图形界面。

   **要安装 Session Recording：** 请遵循 Session Recording 中的指导。

## 安装核心组件的命令行选项

使用 `XenDesktopServerSetup.exe` 命令安装核心组件时，以下选项有效。有关选项的更多详细信息，请参阅 安装核心组件。

> **注意：**

- 在使用命令行选项安装核心组件时，请勿使用 `/exclude`。
- 如果您使用 `/components` 升级一个组件，则其他组件也可能会升级。这是为了避免不同组件之间潜在的兼容性问题。
- 如果您只想升级一个组件，请使用该组件的独立安装程序。请参阅 升级部署。

- **/components** *组件 ...*

  逗号分隔的用于安装或删除的组件列表。有效值为：

  - `CONTROLLER`: 控制器
  - `DESKTOPSTUDIO`: 管理控制台
  - `DESKTOPDIRECTOR`: 监控器
  - `LICENSESERVER`: Citrix 许可证服务器

  如果省略此选项，则会安装所有组件（如果也指定了 `/remove` 选项，则会将其删除）。

  (在 2003 之前的版本中，有效值包括 `STOREFRONT`。对于 2003 及更高版本，请使用 中提及的专用 StoreFront 安装命令 (#use-the-full-product-installer))。

- **/configure_firewall**

  如果 Windows 防火墙服务正在运行，即使防火墙未启用，也会打开 Windows 防火墙中供正在安装的组件使用的所有端口。如果您使用的是第三方防火墙或没有防火墙，则必须手动打开端口。

- **禁用体验指标**

  阻止在安装、升级或删除期间收集的分析数据自动上传到 Citrix。

- **/help 或 /h**

  显示命令帮助。

- **/ignore_hw_check_failure**

  允许 Delivery Controller 安装或升级继续进行，即使硬件检查失败（例如，由于 RAM 不足）。有关详细信息，请参阅 硬件检查。

- **/ignore_site_test_failure**

仅在 Controller 升级期间有效。通常，任何站点测试失败都会被忽略，升级会继续进行。如果省略（或设置为 false），任何站点测试失败都会导致安装程序失败，而不会执行升级。默认值 = false

在升级期间，如果检测到不受支持的 SQL Server 版本，此选项将被忽略。有关详细信息，请参阅 SQL Server 版本检查。

- **/installdir *目录***

  现有空目录，组件将安装在此处。默认值 = `c:\Program Files\Citrix`。

- **/logpath *路径***

  日志文件位置。指定的文件夹必须存在。安装程序不会创建它。默认值 = `TEMP%\Citrix\XenDesktop Installer`

- **/no_pending_reboot_check**

  在安装或升级核心组件时，阻止检查计算机上以前的 Windows 安装是否存在待处理的重新启动。

- **/no_remote_assistance**

  仅在安装 Director 时有效。禁用使用 Windows 远程协助的用户影子功能。

- **/noreboot**（禁止重新启动）

  阻止安装后重新启动。（对于大多数核心组件，默认情况下不启用重新启动。）

- **/noresume**（禁止恢复）

  默认情况下，如果在安装过程中需要重新启动计算机，安装程序会在重新启动完成后自动恢复。要覆盖默认设置，请指定 `/noresume`。如果您必须重新装载介质或希望在自动化安装期间捕获信息，这会很有帮助。

- **/无SQL**

  阻止在安装 Controller 的服务器上安装 Microsoft SQL Server Express。如果省略此选项，则会安装 SQL Server Express 作为站点数据库。

  此选项对用于本地主机缓存的 SQL Server Express LocalDB 的安装没有影响。

- **/quiet** 或 **/passive**

  安装过程中不会出现用户界面。安装过程的唯一证据在 Windows 任务管理器中。如果省略此选项，则会启动图形界面。

- **/删除**

删除使用 `/components` 选项指定的核心组件。

- **/删除所有**

  删除所有已安装的核心组件。

- **/发送体验指标**

  自动将安装、升级或删除期间收集的分析数据发送给 Citrix。如果省略此选项（或指定 `/disableexperiencemetrics`），则分析数据将在本地收集，但不会自动发送。

- **/临时目录** *目录*

  安装期间用于存放临时文件的目录。默认值 = `c:\Windows\Temp`。

- **/XenApp**

  安装 Citrix Virtual Apps。如果省略此选项，则安装 Citrix Virtual Apps and Desktops™。

## 安装核心组件的示例

以下命令在服务器上安装 Delivery Controller™、Studio、Citrix Licensing 和 SQL Server Express。组件通信所需的防火墙端口将自动打开。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall
```

以下命令在服务器上安装 Citrix Virtual Apps™ Controller、Studio 和 SQL Server Express。组件通信所需的防火墙端口将自动打开。

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall
```

## 使用独立 VDA 安装程序

访问下载站点需要 Citrix 帐户凭据。您必须在开始安装之前拥有提升的管理权限，或者使用**以管理员身份运行**。

1. 从 Citrix 下载相应的软件包：
   - 多会话操作系统虚拟投递代理：`VDAServerSetup.exe`
   - 单会话操作系统虚拟投递代理：`VDAWorkstationSetup.exe`
   - 单会话操作系统核心服务虚拟投递代理：`VDAWorkstationCoreSetup.exe`
2. 可以先将文件从软件包中提取到现有目录，然后运行安装命令，或者直接运行软件包。

要在安装文件之前提取文件，请使用 `/extract` 和绝对路径，例如 `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`。目录必须存在。否则，提取将失败。然后，在单独的命令中，使用本文中列出的有效选项运行相应的命令。

- 对于 `VDAServerSetup_XXXX.exe`，运行 `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
- 对于 `VDAWorkstationCoreSetup_XXXX.exe`，运行 `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
- 对于 `VDAWorkstationSetup_XXXX.exe`，运行 `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

要运行下载的软件包，请运行其名称：`VDAServerSetup.exe`、`VDAWorkstationSetup.exe` 或 `VDAWorkstationCoreSetup.exe`。使用本文中列出的有效选项。

如果您熟悉完整产品安装程序：

- 运行独立的 `VDAServerSetup.exe` 或 `VDAWorkstationSetup.exe` 安装程序，就像它是 `XenDesktopVdaSetup.exe` 命令一样，只是名称不同。
- `VDAWorkstationCoreSetup.exe` 安装程序有所不同，因为它支持其他安装程序可用选项的子集。

## 用于安装 VDA 的命令行选项

以下选项适用于以下一个或多个命令（安装程序）：`VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe` 和 `VDAWorkstationCoreSetup_xxxx.exe`。

有关选项的更多详细信息，请参阅 安装 VDA。

- **/components** *组件*\[,*组件*\]

  逗号分隔的用于安装或删除的组件列表。有效值为：

  - `VDA`：虚拟投递代理
  - `PLUGINS`：适用于 Windows 的 Citrix Workspace™ 应用程序

  要安装 VDA 和适用于 Windows 的 Citrix Workspace 应用程序，请指定 `/components vda,plugins`。

  如果省略此选项，则仅安装 VDA（不安装 Citrix Workspace 应用程序）。

使用 `VDAWorkstationCoreSetup_xxxx.exe` 安装程序时，此选项无效。该安装程序无法安装 Citrix Workspace 应用程序。

- **/controllers** "*控制器* \[*控制器*\]"

  用直引号括起来的、VDA 可与之通信的 Controller 的 FQDN（以空格分隔）。请勿同时指定 `/site_guid` 和 `/controllers` 选项。

- **禁用体验指标**

  阻止自动上传在安装、升级或删除期间收集到 Citrix 的分析数据。

- **/enable_hdx_ports**

  如果检测到 Windows 防火墙服务，即使防火墙未启用，也会打开 VDA 和已启用功能（Windows 远程协助除外）所需的 Windows 防火墙中的端口。如果您使用的是其他防火墙或没有防火墙，则必须手动配置防火墙。有关端口信息，请参阅网络端口。

  要打开 HDX 自适应传输使用的 UDP 端口，除了此 `/enable_hdx_ports` 选项外，还要指定 `/enable_hdx_udp_ports` 选项。

- **/enable_hdx_udp_ports**

  如果检测到 Windows 防火墙服务，则在 Windows 防火墙中打开 HDX 自适应传输使用的 UDP 端口，即使防火墙未启用也是如此。如果您使用的是其他防火墙或没有防火墙，则必须手动配置防火墙。有关端口信息，请参阅 网络端口。

  要打开 VDA 使用的额外端口，除了此 `/enable_hdx_udp_ports` 选项之外，还要指定 `/enable_hdx_ports` 选项。

- **/enable_real_time_transport**

  启用或禁用将 UDP 用于音频数据包（用于音频的实时音频传输）。启用此功能可以提高音频性能。如果您希望在检测到 Windows 防火墙服务时自动打开 UDP 端口，请包含 `/enable_hdx_ports` 选项。

- **/enable_remote_assistance**

  启用 Windows 远程协助中的影子功能，以便与 Director 结合使用。如果指定此选项，Windows 远程协助将在防火墙中打开动态端口。

- **/enablerestore** 或 **/enablerestorecleanup**

  （仅适用于单会话 VDA）如果 VDA 安装或升级失败，则启用自动返回到还原点。

  如果安装/升级成功完成：

- `/enablerestorecleanup` 指示安装程序删除还原点。
- `/enablerestore` 指示安装程序保留还原点，即使该还原点未使用。

有关详细信息，请参阅安装或升级失败时恢复。

- **/enable_ss_ports**

  如果在检测到 Windows 防火墙服务时，即使防火墙未启用，也会打开 Windows 防火墙中屏幕共享所需的端口。如果您使用不同的防火墙或不使用防火墙，则必须手动配置防火墙。

- **/排除** “*组件*”

  阻止安装一个或多个以逗号分隔的可选组件，每个组件都用直引号括起来。例如，在不受 MCS 管理的映像上安装或升级 VDA 不需要计算机身份服务组件。有效值如下所示：

| 多会话操作系统 | 单会话操作系统 | 单会话操作系统核心服务 |
| --- | --- | --- |
| `Citrix Authentication Identity Assertion VDA Plug-in` | `Citrix Authentication Identity Assertion VDA Plug-in` | `Citrix Authentication Identity Assertion VDA Plug-in` |
| `Citrix Backup and Restore` | `Citrix Backup and Restore` | `Citrix Browser Content Redirection` |
| `Citrix Browser Content Redirection` | `Citrix Browser Content Redirection` | `Citrix Personalization for App-V - VDA` |
| `Citrix MCS IODriver` | `Citrix MCS IODriver` | `Citrix Telemetry Service` |
| `Citrix Personalization for App-V - VDA` | `Citrix Personalization for App-V - VDA` | `Citrix Universal Print Client` |
| `Citrix Profile Management` | `Citrix Profile Management` | `Citrix Vda Log Capture Service` |
| `Citrix Profile Management WMI Plug-in` | `Citrix Profile Management WMI Plug-in` | `CSE Component` |
| `Citrix Rendezvous V2` | `Citrix Rendezvous V2` | `Director VDA Plug-in` |
| `Citrix Supportability Tools` | `Citrix Supportability Tools` | `Machine Management Provider` |

| 多会话操作系统 | 单会话操作系统 | 单会话操作系统核心服务 |
| --- | --- | --- |
| `Citrix Telemetry Service` | `Citrix Telemetry Service` | `VDA Monitor Plug-in` |
| `Citrix Universal Print Client` | `Citrix Universal Print Client` | `VDA WMI Proxy Plug-in` |
| `Citrix Vda Log Capture Service` | `Citrix Vda Log Capture Service` | |
| `Citrix VDA Upgrade Agent` | `Citrix VDA Upgrade Agent` | |
| `Citrix WEM Agent` | `Citrix WEM Agent` | |
| `CSE Component` | `CSE Component` | |
| `Director VDA Plug-in` | `Director VDA Plug-in` | |
| `Machine Identity Service` | `Machine Identity Service` | |
| `Machine Management Provider` | `Machine Management Provider` | |
| `VDA Monitor Plug-in` | `User Personalization Layer` | |
| `VDA WMI Proxy Plug-in` | `VDA Monitor Plug-in` | |
| | `VDA WMI Proxy Plug-in` | |

从安装中排除 Citrix Profile Management ( `/exclude "Citrix Profile Management"` ) 会影响使用 Citrix Director 对 VDA 进行监视和故障排除。在**用户详细信息**和**端点**页面上，个性化面板和登录持续时间面板将失败。在**控制板**和**趋势**页面上，平均登录持续时间面板仅显示已安装 Profile Management 的计算机的数据。

即使您正在使用第三方用户配置文件管理解决方案，Citrix 仍建议您安装并运行 Citrix Profile Management Service。无需启用 Citrix Profile Management Service。

如果同时指定 `/exclude` 和 `/includeadditional` 并使用相同的组件名称，则不会安装该组件。

使用 `VDAWorkstationCoreSetup.exe` 安装程序时，此选项无效。该安装程序会自动排除其中许多项目。

- **/h** 或 **/help**

  显示命令帮助。

- **/includeadditional** "*组件*"\[,"*组件*"\]

  包括安装一个或多个以逗号分隔的可选组件，每个组件都用直引号括起来。当您创建远程 PC 访问部署并希望安装默认不包含的其他组件时，此选项会很有帮助。有效值如下所示：

| 多会话操作系统 | 单会话操作系统 |
| --- | --- |
| `Citrix Backup and Restore` | `Citrix Backup and Restore` |
| `Citrix MCS IODriver` | `Citrix MCS IODriver` |
| `Citrix Personalization for App-V - VDA` | `Citrix Personalization for App-V - VDA` |
| `Citrix Profile Management` | `Citrix Profile Management` |
| `Citrix Profile Management WMI Plug-in` | `Citrix Profile Management WMI Plug-in` |
| `Citrix Rendezvous V2` | `Citrix Rendezvous V2` |
| `Citrix Supportability Tools` | `Citrix Supportability Tools` |
| `Citrix VDA Upgrade Agent` | `Citrix VDA Upgrade Agent` |
| `Citrix WEM Agent` | `Citrix WEM Agent` |
| `Machine Identity Service` | `Machine Identity Service` |
| | `User Personalization Layer` |

  如果同时指定 `/exclude` 和 `/includeadditional` 并使用相同的组件名称，则不会安装该组件。

- **/installdir** *目录*

将安装组件的现有空目录。默认值 = `c:\Program Files\Citrix`。

- **/install_mcsio_driver**

  请勿使用。请改用 `/includeadditional "Citrix MCS IODriver"` 或 `/exclude "Citrix MCS IODriver"`。

- **/logpath** *路径*

  日志文件位置。指定的文件夹必须存在。安装程序不会创建它。默认值 = "`%TEMP%\Citrix\XenDesktop Installer`"

  此选项在图形界面中不可用。

- **/主映像**

  仅在虚拟机上安装 VDA 时有效。将 VDA 设置为用于创建其他计算机的映像。此选项等效于 `/mastermcsimage`。

  使用 `VDAWorkstationCoreSetup_xxxx.exe` 安装程序时，此选项无效。

- **/MCS主映像**

  指定此计算机将用作 Machine Creation Services 的映像。此选项等同于 `/masterimage`。

- **/PVS主映像**

  指定此计算机将用作映像，与 Citrix Provisioning™ 或第三方预配工具（例如 Microsoft System Center Configuration Manager）一起用于预配 VM。

- **/no_mediafoundation_ack**

  确认未安装 Microsoft Media Foundation，并且多个 HDX™ 多媒体功能将不会安装且无法工作。如果省略此选项且未安装 Media Foundation，则 VDA 安装将失败。大多数受支持的 Windows 版本都已安装 Media Foundation，N 版本除外。

- **/nodesktopexperience**（不安装桌面体验）

  增强桌面体验功能不再可用。如果指定此选项（和策略设置），则会将其忽略。

  仅在安装适用于多会话操作系统的 VDA 时有效。阻止启用增强桌面体验功能。此功能也通过增强桌面体验 Citrix 策略设置进行控制。

- **/noreboot**（禁止重新启动）

  阻止安装后重新启动。VDA 必须在重新启动后才能使用。

- **/noresume**（禁止恢复）

默认情况下，如果在安装过程中需要重新启动计算机，安装程序会在重新启动完成后自动恢复。要覆盖默认设置，请指定 `/noresume`。如果您必须重新装载介质或希望在自动化安装期间捕获信息，这会很有帮助。

- **/portnumber** *端口*

  仅当指定了 `/reconfig` 选项时有效。用于启用 VDA 与 Controller 之间通信的端口号。除非是端口 80，否则以前配置的端口将被禁用。

- **/proxyconfig** "*地址或 PAC 文件路径*"

  仅当命令包含 `/includeadditional "Citrix Rendezvous V2"` 时有效。用于 Rendezvous 协议的代理地址或 PAC 文件路径。有关功能详细信息，请参阅Rendezvous 协议。

  - 代理地址格式：`http://<url-or-ip>:<port>`
  - PAC 文件格式：`http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** 或 **/passive**

  安装期间不会出现用户界面。安装和配置过程的唯一证据在 Windows 任务管理器中。如果省略此选项，则会启动图形界面。

- **/重新配置**

  与 `/portnumber`、`/controllers` 或 `/enable_hdx_ports` 选项一起使用时，自定义以前配置的 VDA 设置。如果指定此选项但未同时指定 `/quiet` 选项，则会启动用于自定义 VDA 的图形界面。

- **/远程电脑**

  仅适用于远程电脑访问部署（单会话操作系统）或代理连接（多会话操作系统）。排除安装任何附加组件（请参阅 `/exclude` 和 `/includeadditional` 选项的组件列表）。

  使用 `VDAWorkstationCoreSetup.exe` 安装程序时，此选项无效。该安装程序会自动排除这些组件的安装。

  `/remotepc` 与 `/servervdi` 选项不兼容。

- **/删除**

  删除使用 `/components` 选项指定的组件。

- **/remove_appdisk_ack**

  授权 VDA 安装程序卸载 AppDisks™ VDA 插件（如果已安装）。

- **/remove_pvd_ack**

授权 VDA 安装程序卸载 Personal vDisk（如果已安装）。

- **/删除所有**

  删除 VDA。它不会删除 Citrix Workspace 应用程序（如果已安装）。

- **/发送体验指标**

  在安装、升级或删除过程中自动将收集到的分析数据发送给 Citrix。如果省略此选项（或指定了 `/disableexperiencemetrics` 选项），则分析数据将在本地收集，但不会自动发送。

- **/服务器VDI**

  在受支持的 Windows 多会话计算机上安装适用于单会话操作系统的 VDA。在 Windows 多会话计算机上安装适用于多会话操作系统的 VDA 时，请省略此选项。

  使用此选项之前，请参阅 Server VDI。

  仅将此选项与完整产品 VDA 安装程序一起使用。

- **/站点GUID** *GUID*

  站点的 Active Directory 组织单位 (OU) 的全局唯一标识符。当您使用 Active Directory 进行发现时（自动更新是推荐的默认发现方法），这会将虚拟桌面与站点关联。站点 GUID 是 Studio 中显示的站点属性。请勿同时指定 `/site_guid` 和 `/controllers` 选项。

- **/临时目录** *目录*

  安装期间用于存放临时文件的目录。默认值 = `c:\Windows\Temp`。

  此选项在图形界面中不可用。

- **/虚拟机**

  仅在 VM 上安装 VDA 时有效。覆盖安装程序对物理机的检测，因为传递给 VM 的 BIOS 信息使其显示为物理机。

  此选项在图形界面中不可用。

- **/wem_add_firewall_rules**

  添加 WEM 代理防火墙规则。

- **/wem_agent_cache_location**

  备用 WEM 代理缓存位置。

- **/wem_agent_port**

  WEM 代理用于与 WEM 基础架构服务器通信的端口。

- **/wem_cached_data_sync_port**

  WEM 代理用于与 WEM 基础架构服务器同步缓存的端口。

- **/wem_cloud_connectors**

  包含 WEM 部署的资源位置中 Citrix Cloud™ Connector 的逗号分隔列表。

- **/wem_server**

  WEM 基础架构服务器的 FQDN 或 IP 地址。

- **/XenDesktop云**

  指示 VDA 安装在 Citrix DaaS™ (Citrix Cloud) 部署中。

## 安装 VDA 的示例

**使用完整产品安装程序安装 VDA：**

以下命令将为单会话操作系统和 Citrix Workspace 应用程序安装 VDA 到 VM 上的默认位置。此 VDA 将用作映像，并使用 MCS 预配 VM。VDA 将首先在域 `mydomain` 中名为 `Contr-Main` 的服务器上向 Controller 注册。VDA 将使用用户个性化层和 Windows 远程协助。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /
controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional
"user personalization layer" /mastermcsimage /enable_remote_assistance
```

**使用 VDAWorkstationCoreSetup 独立安装程序安装单会话操作系统 VDA：**

以下命令在单会话操作系统上安装核心服务 VDA，用于远程 PC 访问或 VDI 部署。Citrix Workspace 应用程序和其他非核心服务未安装。指定了 Controller 的地址，Windows 防火墙服务中的端口将自动打开。管理员将处理重新启动。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /
enable_hdx_ports /noreboot
```

## 自定义 VDA

安装 VDA 后，您可以自定义多项设置。从产品介质上的 `\x64\XenDesktop Setup` 目录中，运行 `XenDesktopVdaSetup.exe`，使用以下一个或多个选项，这些选项在 安装 VDA 的命令行选项 中进行了描述。

- `/reconfigure`（自定义 VDA 时必需）
- `/h` 或 `/help`

- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

## VDA 故障排除

- 在交付组的 Studio 显示中，**详细信息**窗格中的**已安装的 VDA 版本**条目可能不是计算机上安装的版本。计算机的 Windows 程序和功能显示会显示实际的 VDA 版本。
- VDA 安装后，必须先向 Delivery Controller 注册，然后才能向用户交付应用程序或桌面。

  要了解 VDA 注册方法以及如何排查注册问题，请参阅 VDA 注册。

## 安装 Universal Print Server 的命令行选项

以下选项对 `XenDesktopPrintServerSetup.exe` 命令有效。

- **/enable_upsserver_port**

| 软件 | 文件夹 | 文件名 |
| --- | --- | --- |
| | | |
| Citrix 诊断工具 | x64 > 虚拟桌面组件 | `cdf_x64.msi` |
| Universal Print Server 服务器组件 | x64 > 通用打印服务器 | `UpsServer_x64.msi` |

如果未指定此选项，安装程序将从图形界面显示**防火墙**页面。选择**自动**以让安装程序自动添加 Windows 防火墙规则，或选择**手动**以让管理员手动配置防火墙。

在打印服务器上安装软件后，请按照预配打印机中的指导配置通用打印服务器。

## 更多信息

有关 Citrix 如何报告组件安装结果的信息，请参阅Citrix 安装返回代码。

# 使用脚本安装 VDA

> **注意：**
>
> Citrix 不对因适应客户生产环境而修改的脚本引起的问题负责。对于任何与安装相关的 Citrix 问题，请使用 Citrix 支持门户 并附上相关安装日志来开具技术支持案例。

> 本文适用于在 Windows 操作系统计算机上安装 VDA。有关适用于 Linux 操作系统的 VDA 的信息，请参阅 Linux Virtual Delivery Agent 文档。

安装介质包含用于在 Active Directory 中安装、升级或删除 Virtual Delivery Agent (VDA) 的示例脚本。您还可以使用这些脚本来维护 Machine Creation Services™ 和 Citrix Provisioning（以前称为 Provisioning Services）所用的主映像。

所需访问权限：

- 脚本需要对 VDA 安装命令所在的网络共享具有“所有人读取”访问权限。在完整产品 ISO 中，安装命令为 `XenDesktopVdaSetup.exe`；在独立安装程序中，安装命令为 `VDAWorkstationSetup.exe` 或 `VDAServerSetup.exe`。
- 日志详细信息存储在每台本地计算机上。要集中记录结果以供审查和分析，脚本需要对相应的网络共享具有“所有人读取和写入”访问权限。

要检查运行脚本的结果，请查看中央日志共享。捕获的日志包括脚本日志、安装程序日志和 MSI 安装日志。每次安装或删除尝试都记录在一个带时间戳的文件夹中。文件夹标题以 PASS 或 FAIL 前缀指示操作结果。您可以使用标准目录搜索工具在中央日志共享中查找失败的安装或删除。这些工具提供了在目标计算机上本地搜索的替代方法。

在开始任何安装之前，请阅读并完成 准备安装 中的任务。

## 使用脚本安装或升级 VDA

1. 从安装介质上的 `\Support\AdDeploy\` 获取示例脚本 **InstallVDA.bat**。Citrix 建议您在自定义脚本之前备份原始脚本。
2. 编辑脚本：
   - 指定要安装的 VDA 版本：`SET DESIREDVERSION`。例如，版本 7 可以指定为 7.0。完整值可在安装介质的 ProductVersion.txt 文件中找到。但是，不需要完全匹配。
   - 指定将调用安装程序的网络共享。指向布局的根目录（树的最高点）。脚本运行时会自动调用相应版本的安装程序（32 位或 64 位）。例如：`SET DEPLOYSHARE=\\fileserver1\share1`。

- （可选）指定用于存储集中式日志的网络共享位置。例如：`SET LOGSHARE=\\fileserver1\log1)`。
- 按照使用命令行安装中所述指定 VDA 配置选项。`/quiet` 和 `/noreboot` 选项默认包含在脚本中，并且是必需的：`SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT`。

3. 使用组策略启动脚本，将脚本分配给包含您的计算机的组织单位 (OU)。此 OU 应仅包含您要安装 VDA 的计算机。当该 OU 中的计算机重新启动时，脚本将在所有这些计算机上运行。VDA 将安装在每台具有受支持操作系统的计算机上。

## 使用脚本删除 VDA

1. 从安装介质上的 `\Support\AdDeploy\` 获取示例脚本 UninstallVDA.bat。Citrix 建议您在自定义脚本之前备份原始脚本。
2. 编辑脚本。
   - 指定要删除的 VDA 版本：`SET CHECK\_VDA\_VERSION`。例如，版本 7 可以指定为 7.0。完整值可在安装介质的 ProductVersion.txt 文件中找到（例如 7.0.0.3018）。但是，不需要完全匹配。
   - （可选）指定用于存储集中式日志的网络共享位置。
3. 使用组策略启动脚本，将脚本分配给包含您的计算机的组织单位 (OU)。此 OU 应仅包含您要从中删除 VDA 的计算机。当该 OU 中的计算机重新启动时，脚本将在所有这些计算机上运行。VDA 将从每台计算机中删除。

## 故障排除

- 脚本生成描述脚本执行进度的内部日志文件。脚本在部署启动后的几秒钟内将 `Kickoff_VDA_Startup_Script` 日志复制到中央日志共享。您可以验证整个过程是否正常运行。如果此日志未按预期复制到中央日志共享，请通过检查本地计算机进一步排查故障。脚本在每台计算机的 `%temp%` 文件夹中放置两个调试日志文件：
  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  查看这些日志以确保脚本：
  - 按预期运行。
  - 正确检测目标操作系统。
  - 已正确配置为指向 `DEPLOYSHARE` 共享的 `ROOT`（包含名为 `AutoSelect.exe` 的文件）。

  - 能够对 `DEPLOYSHARE` 和 `LOG` 共享进行身份验证。

- 有关 Citrix 如何报告组件安装结果的信息，请参阅Citrix 安装返回代码。
- 在 Studio 的交付组显示中，**已安装的 VDA 版本**条目在**详细信息**窗格中可能不是计算机上安装的版本。计算机的程序和功能显示会显示实际的 VDA 版本。
- VDA 安装后，必须先向 Delivery Controller 注册，然后才能向用户交付应用程序或桌面。

  要了解 VDA 注册方法以及如何解决注册问题，请参阅VDA 注册。

# 使用 SCCM 安装 VDA

> **注意：**
>
> Citrix 不对因使用 Microsoft System Center Configuration Manager (SCCM) 等软件分发工具部署虚拟投递代理 (VDA) 而引起的问题负责，这些工具已调整以匹配客户生产环境。对于任何与安装相关的 Citrix 问题，请使用 Citrix 支持门户 提交技术支持案例并附上相关安装日志。

## 概述

为了使用 Microsoft System Center Configuration Manager (SCCM) 或类似软件分发工具成功部署虚拟投递代理 (VDA)，Citrix® 建议按一系列步骤使用 VDA 安装程序。

Citrix 不建议将 VDA 清理实用程序作为 VDA 安装或升级的一部分使用。仅当 VDA 安装程序之前失败时，才可在有限情况下使用 VDA 清理实用程序。

### 重启

VDA 安装期间所需的重新启动次数取决于环境。例如：

- 可能需要重新启动以应用挂起的更新或完成早期软件安装的重新启动。
- 以前被其他进程锁定的文件可能需要更新，从而强制进行额外重新启动。
- VDA 安装程序中的某些可选组件（例如 Citrix Profile Management 和 Citrix Files）可能需要重新启动。

SCCM 任务序列器管理所有必需的重启。

## 定义任务序列

确定所有先决条件和重启后，使用 SCCM 任务序列器完成以下操作：

- VDA 可以从安装介质的可访问副本或从以下 VDA 独立安装程序之一进行安装：
  - `VDAWorkstationSetup_XXXX.exe`
  - `VDAServerSetup_XXXX.exe`
  - `VDAWorkstationCoreSetup_XXXX.exe`

  有关 VDA 安装程序的详细信息，请参阅安装程序。
- 升级 VDA 时，安装 VDA 的计算机必须处于维护模式，且没有会话。
- 当 VDA 安装首次在计算机上运行时，所使用的 VDA 安装程序会复制到该计算机上。
  - 当使用 `VDAWorkstationCoreSetup_XXXX.exe` 以外的 VDA 安装程序时，VDA 安装程序将复制到 `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`。
  - 当使用 `VDAWorkstationCoreSetup_XXXX.exe` 时，VDA 安装程序将复制到 `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe`。 `
- VDA 安装程序的目录位置也存储在注册表 `“HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall” “MetaInstallerInstallLocation”` 中。
- 将命令行选项 `/NOREBOOT`、`/NORESUME` 和 `/QUIET` 添加到您的命令行选项中。
  - `/QUIET`：安装期间不显示用户界面，以便 SCCM 控制安装过程。
  - `/NOREBOOT`：禁止 VDA 安装程序自动重新启动。SCCM 会在需要时触发重新启动。
  - `/NORESUME`：通常，当安装期间需要重启时，VDA 安装程序会设置一个 `runonce` 注册表项 (`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`)。当计算机重启时，Windows 使用该注册表项启动 VDA 安装程序。这对于 SCCM 来说是一个问题，因为 SCCM 无法监控安装并捕获退出代码。

## 使用 SCCM 的安装序列示例

以下示例显示了安装序列。

1. **SCCM 任务 1：** 通过重启计算机来准备计算机。
2. **SCCM 任务 2：** 开始 VDA 安装。
   a. 将 `/quiet`、`/noreboot` 和 `/noresume` 选项添加到您的命令行选项中。
   b. 运行您选择的 VDA 安装程序（本地映像或其中一个最小安装程序）。
   c. SCCM 必须捕获返回代码。

- 如果返回代码为 0 或 8，则安装完成，需要重新启动。
- 如果返回代码为 3，请重新启动计算机，然后将控制权传递给 SCCM TASK3。

3. **SCCM TASK3：** 继续 VDA 安装。

   a. 如果 SCCM TASK2 未返回 0 或 8，则必须在重新启动完成后继续安装。

   b. SCCM TASK3 会重复执行，直到 VDA 安装程序返回 0 或 8（表示安装成功），或 3（表示必须重复执行 SCCM TASK3）。将任何其他返回代码视为错误，SCCM TASK3 应报告错误并停止。

   c. 通过运行适当的 VDA 安装程序（大多数情况下为 `XenDesktopVdaSetup.exe`，如果使用了 `VDAWorkstationCoreSetup_XXXX.exe` 则为 `XenDesktopRemotePCSetup.exe`），从复制它的位置（如 定义任务序列 中所述）恢复 VDA 安装，不带任何命令行参数。（VDA 安装程序使用它在首次运行安装程序时保存的参数。）

   d. 注意 VDA 安装程序返回的代码。

      - 0 或 8：成功，安装完成，需要重启。
      - 3：安装未完成。重新启动计算机并重复 SCCM TASK3，直到返回 0 或 8。将任何其他返回代码视为错误，SCCM TASK3 应报告错误并结束。

有关返回代码的更多信息，请参阅Citrix 安装返回代码。

## VDA 安装命令示例

可用的安装选项因所使用的安装程序而异。有关命令行选项的详细信息，请参阅以下文章。

- 安装 VDA
- 使用命令行安装

### 远程电脑访问的安装命令

- 以下命令使用单会话核心 VDA 安装程序 (`VDAWorkstationCoreSetup.exe`)：

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /
  enable_hdx_ports /noresume /noreboot
  ```

- 以下命令使用单会话完整 VDA 安装程序 (`VDAWorkstationSetup.exe`)：

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /controllers “control.domain.com” /
  enable_hdx_ports /noresume /noreboot
  ```

### 专用 VDI 的安装命令

- 以下命令使用单会话完整 VDA 安装程序 ( `VDAWorkstationSetup.exe` )：

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers
  “control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /
  noreboot
  ```

# 创建站点

站点是您为 Citrix Virtual Apps and Desktops™ 部署指定的名称。它包含 Delivery Controller 和其他核心组件、Virtual Delivery Agent (VDA)、到主机的连接、计算机目录和交付组。您在安装核心组件之后、创建第一个计算机目录和交付组之前创建站点。

如果您的 Controller 安装在 Server Core 上，请使用 Citrix Virtual Apps and Desktops SDK 中的 PowerShell cmdlet 创建站点。

创建站点时，您将自动加入 Citrix 客户体验改善计划 (CEIP)。CEIP 会收集匿名统计信息和使用情况信息，然后将其发送给 Citrix。第一个数据包将在您创建站点后大约七天发送给 Citrix。您可以在站点创建后的任何时间更改您的注册。在 Studio 导航窗格中选择**配置**，然后选择**产品支持**选项卡，并按照指导操作。有关详细信息，请参阅 `<http://more.citrix.com/XD-CEIP>` 。

创建站点的用户将成为完全管理员；有关详细信息，请参阅委派管理。

在创建站点之前，请查看本文，以便了解预期情况。

## 步骤 1. 打开 Studio 并启动站点创建向导

如果 Studio 尚未打开，请将其打开。系统会自动引导您执行启动站点创建向导的操作。选择该操作。

## 步骤 2. 站点类型和名称

在**简介**页面上，选择站点类型：

- **应用程序和桌面交付站点**。创建应用程序和桌面交付站点时，您可以进一步选择创建完整部署站点（推荐）或空站点。空站点仅部分配置，通常由高级管理员创建。
- **远程电脑访问站点**。远程电脑访问站点允许指定用户通过安全连接远程访问其办公电脑。

如果您现在创建应用程序和桌面交付部署，则以后可以添加远程电脑访问部署。相反，如果您现在创建远程电脑访问部署，则以后可以添加完整部署。

键入站点的名称。站点创建后，其名称将显示在 Studio 导航窗格的顶部：**Citrix Studio** (*站点名称*)。

## 步骤 3. 数据库

**数据库**页面包含用于设置站点、监视和配置日志记录数据库的选项。有关数据库设置选择和要求的详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/technical-overview/databases.html)。

> **注意：**

> 如果 SQL Server Always On 侦听器配置为 TLS 加密，系统可能会提示您输入具有数据库创建权限的凭据。即使您输入有效的管理员凭据，创建数据库的尝试仍然会失败。请验证 SQL Server 证书是否在主题备用名称 (SAN) 中包含侦听器 DNS 名称。有关详细信息，请参阅 `<https://docs.microsoft.com/zh-cn/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates>` 。

> 如果您选择安装 SQL Server Express 作为站点数据库（默认），则在该软件安装后会发生重启。如果您选择不安装 SQL Server Express 软件作为站点数据库，则不会发生重启。

如果您不使用默认的 SQL Server Express，请确保在创建站点之前已在计算机上安装 SQL Server 软件。(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html) 列出了支持的版本。

如果您想向站点添加更多 Delivery Controller，并且已在其他服务器上安装了 Controller 软件，则可以从此页面添加这些 Controller。如果您还计划生成用于设置数据库的脚本，请在生成脚本之前添加 Controller。

## 步骤 4. 许可

> **注意：**

> 确保许可证服务器运行的最低版本为 11.17.2 build 53100 及更高版本。未能满足此先决条件可能会在站点升级和创建过程中导致错误或建议

> 在**许可**页面上，指定许可证服务器地址，然后指示要使用（安装）哪个许可证。

- 以 `name:[port]` 形式指定许可证服务器地址。*名称*必须是 FQDN、NetBIOS 或 IP 地址。建议使用 FQDN。如果省略端口号，则默认值为 27000。单击**连接**。在成功连接到许可证服务器之前，您无法继续到下一页。
- 建立连接后，**使用现有许可证**默认处于选中状态。显示屏列出了此产品可配置为的兼容产品，具体取决于当前安装的许可证。
  - 如果您想将此产品配置为列出的产品之一（例如，Citrix Virtual Apps Premium 或 Citrix Virtual Desktops™ Premium），并使用其中一个许可证，请选择该条目。
  - 如果您已分配并下载了要与此产品一起使用的许可证（使用 Citrix 许可证管理工具），但尚未安装该许可证：
    - 单击**浏览许可证文件**。
    - 在文件资源管理器中，找到并选择您下载的许可证。关联产品现在显示在站点创建向导的**许可**页面上。选择您要使用的条目。
  - 如果未显示您想要的产品，或者您没有已分配和下载的许可证，则可以分配、下载并安装许可证。为此，许可证服务器必须具有 Internet 访问权限。您必须拥有您想要的产品对应的许可证访问代码。Citrix 会将该代码通过电子邮件发送给您。
    - 单击**分配并下载**。
    - 在**分配许可证**对话框中，输入 Citrix 发送的许可证访问代码。单击**分配许可证**。
    - 与新许可证关联的产品将显示在站点创建向导的**许可**页面上。选择要使用的条目。

    或者，选择**使用免费 30 天试用版**，稍后安装许可证。有关详细信息，请参阅许可文档。

## 步骤 5. 电源管理（仅限远程电脑访问）

请参阅步骤 8. 远程电脑访问。

## 步骤 6. 主机连接、网络和存储

如果您正在虚拟机管理程序或其他服务上使用 VM 来交付应用程序和桌面，则可以选择创建与该主机的第一个连接。您还可以为该连接指定存储和网络资源。创建站点后，您可以修改此连接和资源，并创建更多连接。有关详细信息，请参阅连接和资源。

- 有关**连接**页面上指定的信息，请参阅连接和资源。
  - 如果您未在虚拟机管理程序或其他服务上使用 VM（或者如果您使用 Studio 管理专用刀片式电脑上的桌面），请选择连接类型**无**。

- 如果您正在配置远程电脑访问站点并计划使用局域网唤醒功能，请选择 **Microsoft System Center Configuration Manager** 类型。

除了连接类型之外，还要指定是使用 Citrix 工具（例如 Machine Creation Services™）还是其他工具来创建 VM。

- 有关**存储**和**网络**页面上指定的信息，请参阅主机存储、存储管理和存储选择。
- 如果您拥有混合权利许可证并已添加公共云主机连接（例如 AWS），则这些连接将在此处列出。重新启动 Citrix Studio 以查看这些公共云主机连接。

## 步骤 7. 附加功能

在**附加功能**页面上，您可以选择功能来自定义您的站点。当您选中需要信息的项目的复选框时，将出现一个配置框。

- **App-V 发布：** 如果您使用 App-V 服务器上 Microsoft App-V 软件包中的应用程序，请选择此功能。提供 App-V 管理服务器的 URL 以及 App-V 发布服务器的 URL 和端口号。

  如果您仅使用网络共享位置上的 App-V 软件包中的应用程序，则无需选择此功能。

  您也可以稍后在 Studio 中启用/禁用和配置此功能。有关详细信息，请参阅 App-V。

## 步骤 8. 远程电脑访问

有关远程电脑访问部署的信息，请参阅远程电脑访问。

如果您使用局域网唤醒功能，请在创建站点之前完成 Microsoft System Center Configuration Manager 上的配置步骤。有关详细信息，请参阅Configuration Manager 和远程电脑访问局域网唤醒。

创建远程电脑访问站点时：

- 如果您正在使用局域网唤醒功能，请在**电源管理**页面上指定 Microsoft System Center Configuration Manager 地址、凭据和连接信息。
- 在**用户**页面上指定用户或用户组。没有自动添加所有用户的默认操作。此外，在**计算机帐户**页面上指定计算机帐户（域和 OU）信息。

  要添加用户信息，请单击**添加用户**。选择用户和用户组，然后单击**添加用户**。

  要添加计算机帐户信息，请单击**添加计算机帐户**。选择计算机帐户，然后单击**添加计算机帐户**。单击**添加 OU**。选择域和组织单位，并指明是否包含子文件夹中的项目。单击**添加 OU**。

将自动创建名为 `Remote PC User Machine Accounts` 的计算机目录。该目录包含您在站点创建向导中添加的所有计算机帐户。将自动创建名为 `Remote PC User Desktops` 的交付组。该组包含您添加的所有用户和用户组。

### 步骤 9. 摘要

“**摘要**”页面列出了您指定的信息。如果要更改任何内容，请使用“**返回**”按钮。完成后，单击“**创建**”，站点创建即开始。

### 测试站点配置

创建站点后，若要运行测试，请在导航窗格顶部选择 **Citrix Studio（站点** *site-name***）**。然后单击中心窗格中的 **测试站点**。您可以查看站点测试结果的 HTML 报告。

对于安装在 Windows Server 2016 上的 Controller，站点测试功能可能会失败。当本地 SQL Server Express 用于站点数据库且 SQL Server Browser 服务未启动时，会发生此故障。为避免此故障，请完成以下任务。

1. 启用 SQL Server Browser 服务（如果需要），然后启动它。
2. 重新启动 SQL Server (SQLEXPRESS) 服务。

升级早期部署时，站点测试会自动运行。有关详细信息，请参阅初步站点测试。

### 故障排除

配置站点后，您可以安装 Studio 并通过 MMC 将其作为管理单元添加到远程计算机上。如果以后尝试删除该管理单元，MMC 可能会停止响应。作为一种解决方法，请重新启动 MMC。

## 创建计算机目录

> **重要提示：**

> 自 Citrix Virtual Apps and Desktops™ 7 2006 起，如果您的当前部署使用了以下任何技术，则只有在移除使用这些技术的生命周期结束 (EOL) 项目后，才能将部署升级到当前版本。

> - 个人虚拟磁盘 (PvD)
> - AppDisks™
> - 公有云主机类型：Citrix CloudPlatform、Microsoft Azure Classic

> 有关详细信息，请参阅移除 PVD、AppDisks 和不受支持的主机。

> 如果您想在部署中使用公有云主机连接，则需要混合权利许可证才能完成全新安装或升级到当前版本。

当安装程序检测到一个或多个不受支持的技术或没有混合权利许可证的主机连接时，升级会暂停或停止。此时会显示一条解释性消息。安装程序日志中包含详细信息。有关详细信息，请参阅升级部署。

## 混合权利许可证对主机连接的影响

根据混合权利许可证的授权，主机与公有云主机的连接会受到影响，共有以下三种情况：

- 要创建与公有云主机的连接，您必须拥有混合权利许可证。
- 如果您拥有混合权利许可证但许可证已过期，则与公有云主机的现有连接将被标记为未授权并进入维护模式。当现有主机连接处于维护模式时，您无法执行以下操作：
  - 添加或修改主机连接
  - 创建目录和更新映像
  - 执行电源操作
- 当未授权的主机连接变为授权状态时，现有主机连接将重新启用。

## 简介

物理机或虚拟机集合作为称为计算机目录的单个实体进行管理。目录中的计算机具有相同类型的操作系统：多会话操作系统或单会话操作系统。包含多会话操作系统计算机的目录可以包含 Windows 或 Linux 计算机，但不能同时包含两者。

创建站点后，Citrix Studio 会指导您创建第一个计算机目录。创建第一个目录后，Studio 会指导您创建第一个交付组。之后，您可以更改已创建的目录，并创建更多目录。

> **提示：**

> 升级现有部署可启用 Machine Creation Services (MCS) 存储优化 (MCS I/O) 功能，无需额外配置。Virtual Delivery Agent (VDA) 和 Delivery Controller 升级会处理 MCS I/O 升级。

# 概述

创建 VM 目录时，您需要指定如何预配这些 VM。您可以使用 Citrix 工具，例如 Machine Creation Services™ (MCS) 或 Citrix Provisioning（以前称为 Provisioning Services）。或者，您可以使用自己的工具来提供计算机。

请考虑：

- MCS 支持来自虚拟机映像的单个系统磁盘。它会忽略附加到该映像的其余数据磁盘。
- 如果您使用 Citrix Provisioning 创建计算机，请参阅 Citrix Provisioning 文档以获取说明。
- 如果您使用 MCS 预配 VM，则需要提供主映像（或映像快照）以在目录中创建相同的 VM。在创建目录之前，您首先使用工具创建和配置主映像。此过程包括在映像上安装 Virtual Delivery Agent (VDA)。然后，您在 Studio 中创建计算机目录。您选择该映像（或快照），指定要在目录中创建的 VM 数量，并配置其他信息。
- 如果您的计算机已可用，您仍然必须为这些计算机创建一个或多个计算机目录。
- 如果您直接使用 PowerShell SDK 创建目录，则可以指定管理程序模板 (VMTemplates)，而不是映像或快照。
- 使用模板预配目录被视为实验性功能。使用此方法时，虚拟机准备可能会失败。因此，无法使用该模板发布目录。

使用 MCS 或 Citrix Provisioning™ 创建第一个目录时，您将使用在创建站点时配置的主机连接。之后（在创建第一个目录和交付组之后），您可以更改有关该连接的信息或创建更多连接。

完成目录创建向导后，测试会自动运行以确保其配置正确。测试完成后，您可以查看测试报告。随时从 Studio 运行测试。

> **注意：**
>
> MCS 不支持 Windows 10 IoT Core 和 Windows 10 IoT Enterprise。有关详细信息，请参阅 Microsoft 站点。

> 有关 Citrix Provisioning 工具的技术详细信息，请参阅 Citrix Virtual Apps and Desktops 映像管理。

## RDS 许可证检查

Citrix Studio 目前在创建包含 Windows 多会话操作系统计算机的计算机目录时，不执行对有效 Microsoft RDS 许可证的检查。要查看 Windows **多会话操作系统计算机**的 Microsoft RDS 许可证状

态，请转至 Citrix Director。在**计算机详细信息**面板中查看 Microsoft RDS 许可证的状态。此面板位于**计算机详细信息和用户详细信息**页面中。有关详细信息，请参阅 Microsoft RDS 许可证运行状况。

### VDA 注册

启动代理会话时，VDA 必须向 Delivery Controller™ 注册。未注册的 VDA 可能会导致原本可用的资源利用不足。VDA 未注册的原因有很多，其中许多原因管理员都可以进行故障排除。Studio 在目录创建向导中以及将计算机从目录添加到交付组后提供故障排除信息。

使用向导添加现有计算机后，计算机帐户名称列表会指示每台计算机是否适合添加到目录。将鼠标悬停在每台计算机旁边的图标上，可显示有关该计算机的信息性消息。

如果消息识别出有问题的计算机，请移除该计算机，或添加该计算机。例如，如果消息指示可能无法获取有关计算机的信息，无论如何都添加该计算机。

有关详细信息，请参阅：

- CTX136668 用于 VDA 注册故障排除指南
- VDA 版本和功能级别
- VDA 注册方法

### MCS 目录创建摘要

以下是您在目录创建向导中提供信息后，默认 MCS 操作的简要概述。

- 如果您选择的是主映像（而不是快照），MCS 会创建一个快照。
- MCS 会创建快照的完整副本，并将该副本放置在主机连接中定义的每个存储位置。
- MCS 将计算机添加到 Active Directory，从而创建唯一的身份。
- MCS 会创建向导中指定的虚拟机数量，并为每个虚拟机定义两个磁盘。除了每个虚拟机的两个磁盘外，主副本也存储在同一存储位置。如果您定义了多个存储位置，则每个位置都会获得以下磁盘类型：
  - 快照的完整副本，该副本是只读的，并在刚创建的虚拟机之间共享。
  - 一个唯一的 16 MB 身份磁盘，为每个 VM 提供唯一的身份。每个 VM 都会获得一个身份磁盘。
  - 一个唯一的差异磁盘，用于存储对虚拟机进行的写入。此磁盘是精简预配的（如果主机存储支持），并在必要时增加到主映像的最大大小。每个虚拟机都会获得一个差异磁盘。差异磁盘保存会话期间所做的更改。对于专用桌面，它是永久性的。对于池化桌面，它会在每次通过交付控制器重新启动后删除并创建一个新的。

或者，在创建用于交付静态桌面的 VM 时，您可以在目录创建向导的**计算机**页面上指定厚（完整副本）VM 克隆。完整克隆不需要在每个数据存储上保留主映像。每个 VM 都有自己的文件。

### MCS 存储注意事项

在决定 MCS 的存储解决方案、配置和容量时，有许多因素需要考虑。以下信息提供了存储容量的适当注意事项：

*容量注意事项:*

- 磁盘

  在大多数 MCS 部署中，Delta 或差异 (Diff) 磁盘为每个 VM 消耗最大的空间。MCS 创建的每个 VM 在创建时至少会获得 2 个磁盘。

  - Disk0 = 差异磁盘：从主基础映像复制时包含操作系统。
  - Disk1 = 身份磁盘：16 MB - 包含每个 VM 的 Active Directory 数据。

  随着产品的演进，您可能需要添加更多磁盘以满足某些用例和功能消耗。例如：

  - MCS 存储优化 为每个 VM 创建一个写入缓存式磁盘。在 XenServer、VMware 和 SCVMM 虚拟化环境中，如果您在创建主机连接时将可用操作系统存储列表配置为与可用临时存储列表相同，则 MCS 会将回写缓存 (WBC) 磁盘放置在与操作系统磁盘相同的存储位置。
  - MCS 增加了使用 完整克隆 的能力，而不是上一节中描述的 Delta 磁盘方案。

  管理程序功能也可能纳入考虑范围。例如：

  - Citrix Hypervisor IntelliCache 为每个 Citrix Hypervisor 在本地存储上创建一个读取磁盘。此选项可节省针对主映像的 IOPS，主映像可能保存在共享存储位置。

- 管理程序开销

  不同的管理程序使用特定文件，这些文件会为虚拟机创建开销。管理程序还使用存储进行管理和一般日志记录操作。计算空间以包含以下开销：

  - 日志文件
  - 管理程序特定文件。例如：
    - VMware 会将更多文件添加到 **VM 存储**文件夹。请参阅 VMware 最佳实践。
    - 计算您的虚拟机总大小要求。考虑一个虚拟机，其中包含 20 GB 虚拟磁盘、16 GB 交换文件和 100 MB 日志文件，总共占用 36.1 GB。
  - XenServer 快照；VMware 快照。

- 进程开销

  创建目录、添加计算机和更新目录具有独特的存储影响。例如：

  - 初始目录创建 需要将基本磁盘的副本复制到每个存储位置。
    - 它还要求您临时创建一个 准备虚拟机。
  - 向目录添加计算机 不需要将基本磁盘复制到每个存储位置。目录创建因所选功能而异。
  - 更新目录 以在每个存储位置创建额外的基本磁盘。目录更新还会经历一个临时存储峰值，在此期间，目录中的每个 VM 在一定时间内都有 2 个差异磁盘。

*更多注意事项：*

- **RAM 大小调整：** 影响某些管理程序文件和磁盘的大小，包括 I/O 优化磁盘、写入缓存和快照文件。
- **精简/厚置备：** 由于精简置备功能，NFS 存储是首选。

### 机器创建服务 (MCS) 存储优化

借助 Machine Creation Services (MCS) 存储优化功能（称为 MCS I/O）：

- 写入缓存容器是*基于文件的*，与 Citrix Provisioning 中的功能相同。例如，Citrix Provisioning 写入缓存文件名是 `D:\vdiskdif.vhdx`，MCS I/O 写入缓存文件名是 `D:\mcsdif.vhdx`。
- 通过支持写入到写入缓存磁盘的 Windows 崩溃转储文件来改进诊断。
- MCS I/O 保留了*RAM 中缓存并溢出到硬盘*的技术，以提供最优的多层写入缓存解决方案。此功能允许管理员在每个层（RAM 和磁盘）的成本与性能之间进行平衡，以满足所需的工作负载预期。

将写入缓存方法从*基于磁盘*更新为*基于文件*需要进行以下更改：

1. MCS I/O 不再支持仅限 RAM 的缓存。在创建计算机目录期间，在 Citrix Studio 中指定磁盘大小。
2. 虚拟机写入缓存磁盘在首次启动虚拟机时自动创建和格式化。虚拟机启动后，写入缓存文件 `mcsdif.vhdx` 将写入到格式化的卷 `MCSWCDisk` 中。
3. 页面文件将重定向到此格式化的卷 `MCSWCDisk`。因此，此磁盘大小会考虑总磁盘空间量。它包括磁盘大小与生成的工作负载之间的差值以及页面文件大小。这通常与虚拟机 RAM 大小相关。

#### 启用 MCS 存储优化更新

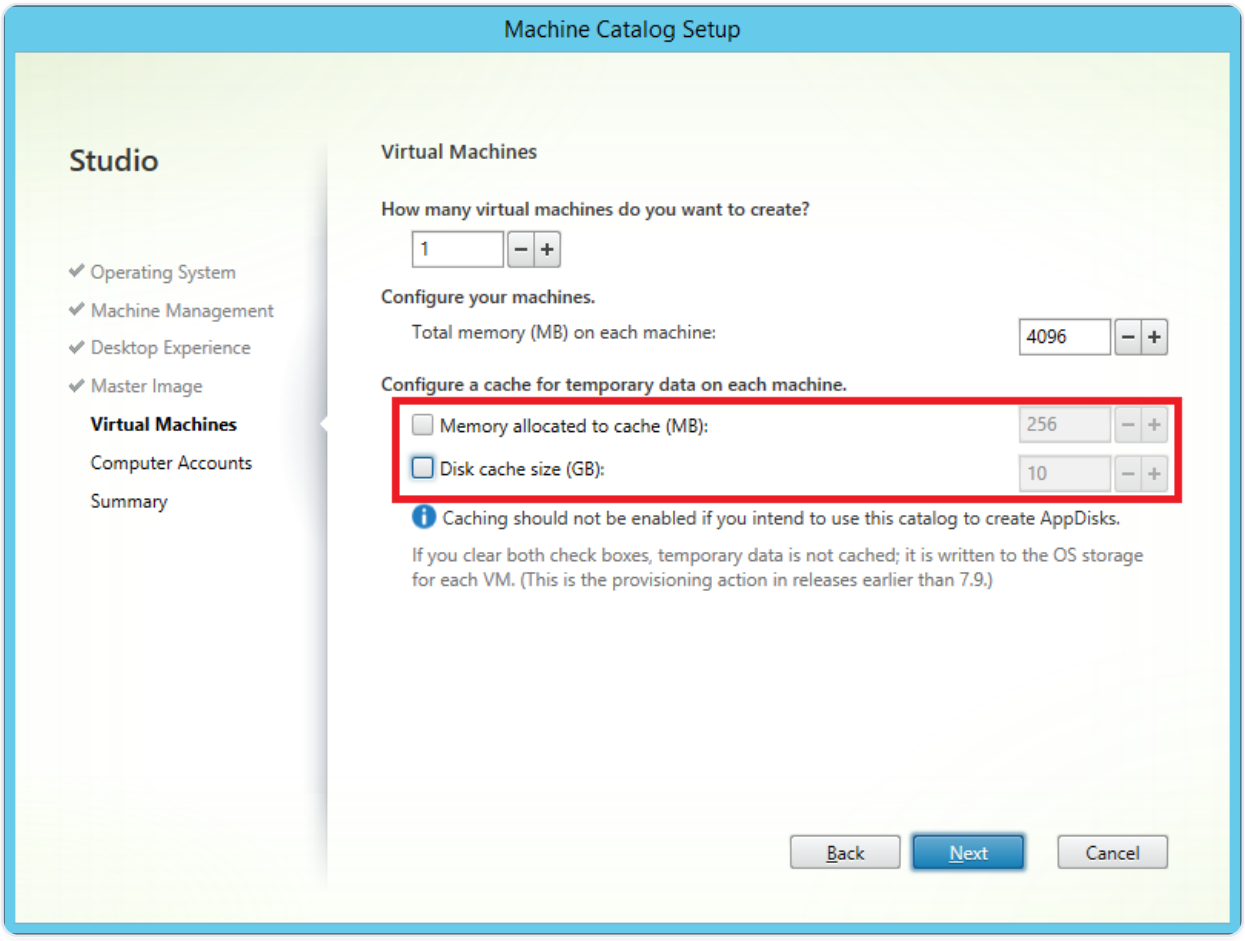
要启用 MCS I/O 存储优化功能，请将 Delivery Controller 和 VDA 升级到最新版本的 Citrix Virtual Apps and Desktops。

**注意：**

如果您升级已启用 MCS I/O 的现有部署，则无需进行额外配置。VDA 和 Delivery Controller 升级会处理 MCS I/O 升级。

启用 MCS 存储优化更新时，请考虑以下事项：

- 创建计算机目录时，管理员可以配置 RAM 和磁盘大小。




- 将现有计算机目录更新到包含为版本 1903 配置的 VDA 的新 VM 快照会导致以下行为：新快照继续使用现有目录的 MCS I/O RAM 和磁盘大小设置。现有原始磁盘将被格式化。

**重要提示：**

Citrix Virtual Apps and Desktops 1903 版本更改了 MCS 存储优化。此版本支持基于文件的写入缓存技术，可提供更好的性能和稳定性。与以前的 Citrix Virtual Apps and Desktops 版本相比，MCS I/O 提供的新功能可能需要更高的写入缓存存储要求。Citrix 建议您重新评估磁盘大小，以确保其具有足够的磁盘空间来满足分配的工作流和额外的页面文件大小。页面文件大小

> 通常与系统 RAM 量相关。如果现有目录磁盘大小不足，请创建计算机目录并分配更大的写入缓存磁盘。

### 使用 PowerShell 创建具有持久回写缓存磁盘的目录

要配置具有持久回写缓存磁盘的目录，请使用 PowerShell 参数 `New-ProvScheme` `CustomProperties`。此参数支持一个额外的属性 `PersistWBC`，用于确定回写缓存磁盘如何为 MCS 预配的计算机持久保存。`PersistWBC` 属性仅在指定 `UseWriteBackCache` 参数且 `WriteBackCacheDiskSize` 参数设置为指示已创建磁盘时使用。

在支持 `PersistWBC` 之前，`CustomProperties` 参数中找到的属性示例包括：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

使用这些属性时，请注意，如果 `CustomProperties` 参数中省略了这些属性，它们将包含默认值。`PersistWBC` 属性有两个可能的值：**true** 或 **false**。

将 `PersistWBC` 属性设置为 **true** 时，Citrix Virtual Apps and Desktops 管理员使用 Citrix Studio 关闭计算机不会删除回写缓存磁盘。

将 `PersistWBC` 属性设置为 **false** 时，Citrix Virtual Apps and Desktops 管理员使用 Citrix Studio 关闭计算机将删除回写缓存磁盘。

> **注意：**

> 如果省略 `PersistWBC` 属性，则该属性默认为 **false**，并且在使用 Citrix Studio 关闭计算机时，回写缓存将被删除。

例如，使用 `CustomProperties` 参数将 `PersistWBC` 设置为 true：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

**重要提示：**

`PersistWBC` 属性只能使用 `New-ProvScheme` PowerShell cmdlet 进行设置。在创建后尝试更改预配方案的 `CustomProperties` 对计算机目录以及计算机关闭时回写缓存磁盘的持久性没有影响。

例如，设置 `New-ProvScheme` 以使用回写缓存，同时将 `PersistWBC` 属性设置为 true：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"
```

```
-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

## 准备主映像

有关创建连接主机的详细信息，请参阅连接和资源。

主映像包含操作系统、非虚拟化应用程序、VDA 和其他软件。

须知：

- 主映像也可能被称为克隆映像、黄金映像、基础虚拟机或基础映像。主机供应商使用不同的术语。
- 使用 Citrix Provisioning 时，可以将主映像或物理计算机用作主目标设备。Citrix Provisioning 使用与 MCS 不同的术语来指代映像。有关详细信息，请参阅 Citrix Provisioning 文档。
- 确保主机具有足够的处理器、内存和存储空间，以容纳所创建的计算机数量。
- 配置桌面和应用程序所需的正确硬盘空间量。此值以后无法更改，也无法在计算机目录中更改。
- 远程电脑访问计算机目录不使用主映像。
- 使用 MCS 时的 Microsoft KMS 激活注意事项：如果您的部署包含 7.x VDA 以及 XenServer 6.1 或 6.2、vSphere 或 Microsoft System Center Virtual Machine Manager 主机，则无需手动重新激活 Microsoft Windows 或 Microsoft Office。

在主映像上安装并配置以下软件：

- 适用于您的管理程序的集成工具（例如 Citrix VM Tools、Hyper-V Integration Services 或 VMware tools）。如果省略此步骤，应用程序和桌面可能无法正常运行。
- VDA。Citrix 建议安装最新版本以访问最新功能。如果未在主映像上安装 VDA，则会导致目录创建失败。
- 根据需要安装第三方工具，例如防病毒软件或电子软件分发代理。使用适合用户和计算机类型（例如更新功能）的设置来配置服务。
- 您未虚拟化的第三方应用程序。Citrix 建议虚拟化应用程序。虚拟化通过消除在添加或重新配置应用程序后更新主映像的需要来降低成本。此外，安装的应用程序越少，主映像硬盘的大小就越小，从而节省了存储成本。
- 如果您计划发布 App-V 应用程序，请安装具有推荐设置的 App-V 客户端。App-V 客户端可从 Microsoft 获取。
- 使用 MCS 时，如果您本地化 Microsoft Windows，请安装区域设置和语言包。在预配期间，创建快照时，预配的 VM 将使用已安装的区域设置和语言包。

> **重要提示：**
>
> 如果您正在使用 Citrix Provisioning 或 MCS，请勿在主映像上运行 Sysprep。

> 准备主映像：

1. 使用您的虚拟机管理程序管理工具创建主映像，然后安装操作系统以及所有服务包和更新。指定 vCPU 的数量。如果您使用 PowerShell 创建计算机目录，也可以指定 vCPU 值。使用 Studio 创建目录时，无法指定 vCPU 的数量。配置桌面和应用程序所需的硬盘空间量。该值以后无法更改，也无法在目录中更改。
2. 确保硬盘连接到设备位置 0。大多数标准主映像模板默认配置此位置，但某些自定义模板可能不会。
3. 在主映像上安装并配置上面列出的软件。
4. 使用 Citrix Provisioning 时，在将主目标设备加入域之前，请从主目标设备为虚拟磁盘创建 VHD 文件。有关详细信息，请参阅 Citrix Provisioning 文档。
5. 如果您不使用 MCS，请将主映像加入到应用程序和桌面所属的域中。确保主映像在创建计算机的主机上可用。如果您正在使用 MCS，则无需将主映像加入域。预配的计算机将加入到目录创建向导中指定的域。

6. Citrix 建议您创建并命名主映像的快照。如果在创建目录时指定主映像而不是快照，Studio 将创建一个快照。您无法为其命名。

## 使用 Studio 创建计算机目录

在启动目录创建向导之前，请查看本节。

如果您正在使用主映像，请确保在创建目录之前已在该映像上安装 VDA。

在 Studio 中：

- 如果您已创建站点但尚未创建计算机目录，Studio 会引导您到正确的起始位置来创建目录。
- 如果您已创建目录并想创建另一个目录，请在 **Studio** 导航窗格中选择 **Machine Catalogs**。然后，在 **Actions** 窗格中选择 **Create Machine Catalog**。

向导将引导您完成以下各项。您看到的向导页面会因您所做的选择而异。

## 操作系统

每个目录仅包含一种类型的计算机。请选择一种。

- **多会话操作系统：** 多会话操作系统目录提供托管共享桌面。计算机可以运行受支持的 Windows 或 Linux 操作系统版本，但目录不能同时包含这两种操作系统。（有关该操作系统的详细信息，请参阅 Linux VDA 文档。）
- **单会话操作系统：** 单会话操作系统目录提供可分配给不同用户的 VDI 桌面。
- **远程电脑访问：** 远程电脑访问目录为用户提供对其物理办公桌面计算机的远程访问。远程电脑访问不需要 VPN 来提供安全性。

## 计算机管理

创建远程电脑访问目录时，此页面不会显示。

**计算机管理**页面指示计算机的管理方式以及用于部署计算机的工具。

选择目录中的计算机是否通过 Studio 进行电源管理。

- 计算机通过 Studio 进行电源管理，例如虚拟机或刀片式 PC。此选项仅在您已配置到主机的连接时可用。
- 计算机不通过 Studio 进行电源管理，例如物理机。

如果您指示计算机通过 Studio 进行电源管理，请选择用于创建虚拟机的工具。

- **Citrix Machine Creation Services (MCS)：** 使用主映像创建和管理虚拟机。MCS 不适用于物理机。
- **Citrix Provisioning：**（以前称为 Provisioning Services。）将目标设备作为设备集合进行管理。从主目标设备映像的 Citrix Provisioning 虚拟磁盘可交付桌面和应用程序。

> **注意：**
>
> 此选项不再受支持。要将 Citrix Provisioning 目标设备导入 Citrix Virtual Apps and Desktops 目录，请使用 **Citrix Provisioning Export Devices Wizard**。

- **其他：**一种管理数据中心中已有计算机的工具。Citrix 建议您使用 Microsoft System Center Configuration Manager 或其他第三方应用程序，以确保目录中的计算机保持一致。

## 桌面类型（桌面体验）

此页面仅在您创建包含单会话操作系统计算机的目录时显示。

“**桌面体验**”页面决定了用户每次登录时发生的情况。请选择以下选项之一：

- 用户每次登录时都连接到新的（随机）桌面。
- 用户每次登录时都连接到相同的（静态）桌面。

如果您选择第二个选项并使用 MCS 预配计算机，则可以配置如何处理用户对桌面的更改：

- 将用户对桌面的更改保存到本地磁盘。
- 丢弃用户更改并在用户注销时清除虚拟桌面。如果您正在使用用户个性化层，请选择此选项。

## 主映像

此页面仅在您使用 MCS 创建 VM 时显示。

在“**主映像**”页面上，选择与主机的连接，然后选择之前创建的快照或 VM。如果您正在创建第一个目录，则唯一可用的连接是您在创建站点时配置的连接。

请记住：

- 当您使用 MCS 或 Citrix Provisioning 时，请勿在主映像上运行 Sysprep。
- 如果您指定主映像而不是快照，Studio 会创建一个快照，但您无法为其命名。

为了启用最新产品功能，请确保主映像已安装最新 VDA 版本。请勿更改默认的最低 VDA 选择。但是，如果您必须使用较早的 VDA 版本，请参阅VDA 版本和功能级别。

如果您选择的快照或 VM 与您之前在向导中选择的计算机管理技术不兼容，则会显示错误消息。

## 设备集合

此页面仅在使用 Citrix Provisioning 创建 VM 时显示。

**设备集合**页面显示设备集合以及尚未添加到目录的设备。

选择要使用的设备集合。

## 计算机

创建远程电脑访问目录时，此页面不显示。

此页面的标题取决于您在**计算机管理**页面上选择的内容：**计算机**、**虚拟机**或**VM 和用户**。

**使用 MCS 时：**

- 指定要创建的虚拟机数量。
- 选择每个 VM 的内存量（以 MB 为单位）。
- 每个创建的 VM 都有一个硬盘。其大小在主映像中设置。您无法在目录中更改硬盘大小。
- 如果您的部署包含多个区域，则可以为目录选择一个区域。
- 如果要创建静态桌面 VM，请选择虚拟机复制模式。请参阅虚拟机复制模式。
- 如果要创建不使用 vDisk 的随机桌面 VM，可以配置一个缓存，用于存储每台计算机上的临时数据。请参阅配置临时数据缓存。

**使用 Citrix 预配时：**

**设备**页面列出了您在上一向导页面上选择的设备集合中的计算机。您无法在此页面上添加或删除计算机。

**使用其他工具时：**

添加（或导入列表）Active Directory 计算机帐户名称。添加/导入虚拟机后，可以更改其 Active Directory 帐户名称。如果在**桌面体验**页面上指定了静态计算机，则可以选择为添加的每个虚拟机指定 Active Directory 用户名。

添加或导入名称后，在此页面上，可以使用**删除**按钮从列表中删除名称。

**使用 Citrix Provisioning 或其他工具（但不是 MCS）时：**

为添加（或导入，或来自 Citrix Provisioning 设备集合）的每台计算机提供一个图标和工具提示，以帮助识别可能不符合添加到目录条件或无法向 Delivery Controller 注册的计算机。有关详细信息，请参阅(#vda-versions-and-functional-levels)。

### 虚拟机复制模式

在**计算机**页面上指定的复制模式决定了 MCS 是从主映像创建精简（快速复制）克隆还是完整（完全复制）克隆。（默认 = 精简克隆）

- 使用快速复制克隆可实现更高效的存储利用和更快的计算机创建。
- 使用完整复制克隆可获得更好的数据恢复和迁移支持，并且在计算机创建后可能降低 IOPS。

### VDA 版本和功能级别

目录的功能级别控制目录中计算机可用的产品功能。使用新产品版本中引入的功能需要新的 VDA。设置功能级别可使该版本中引入的所有功能（如果功能级别未更改，则包括更高版本的功能）可用于目录中的计算机。但是，该目录中具有早期 VDA 版本的计算机无法注册。

**计算机**（或**设备**）页面底部附近的菜单允许您选择最低 VDA 级别。这会设置目录的最低功能级别。默认情况下，本地部署会选择最新的功能级别。如果您遵循 Citrix 建议，始终安装 VDA 和核心组件并将其升级到最新版本，则无需更改此选择。但是，如果必须继续使用旧版 VDA，请选择正确的值。

Citrix Virtual Apps and Desktops 版本可能不包含新的 VDA 版本，或者新的 VDA 不会影响功能级别。在这种情况下，功能级别可能指示早于已安装或已升级组件的 VDA 版本。例如，尽管版本 7.17 包含 7.17 VDA，但默认功能级别（“7.9 或更高版本”）仍为最新。因此，在将组件 7.9–7.16 安装或升级到 7.17 后，您无需更改默认功能级别。每个版本的(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/whats-new.html)文章都指出了默认功能级别的任何更改。

所选功能级别会影响其上方的计算机列表。在列表中，每个条目旁边的工具提示指示计算机的 VDA 是否与该功能级别的目录兼容。

如果每台计算机上的 VDA 未达到或超过所选的最低功能级别，则页面上会发布消息。您可以继续执行向导。这些计算机以后可能无法向 Controller 注册。或者，您可以执行以下操作：

- 从列表中删除包含旧版 VDA 的计算机，升级其 VDA，然后将其重新添加到目录中。
- 选择较低的功能级别，以阻止访问最新的产品功能。

如果计算机未添加到目录中，因为它是错误的计算机类型，也会发布消息。示例包括尝试将服务器添加到单会话操作系统目录，或将最初为随机分配创建的单会话操作系统计算机添加到静态计算机目录。

**重要提示：**

在版本 1811 中，添加了一个额外功能级别：**1811（或更高版本）**。该级别旨在用于未来的 Citrix Virtual Apps and Desktops 功能。**7.9（或更高版本）**选择仍为默认值。该默认值现在适用于所有部署。

如果您选择 **1811（或更高版本）**，则该目录中任何更早的 VDA 版本都无法向 Controller 注册。但是，如果目录中仅包含版本 1811 或更高受支持版本的 VDA，则它们都符合注册条件。这包括包含为更高版本的 Citrix Virtual Apps and Desktops 版本（包括 1903 版和当前版本之前的其他 19XX 版本）配置的 VDA 的目录。

### 配置临时数据缓存

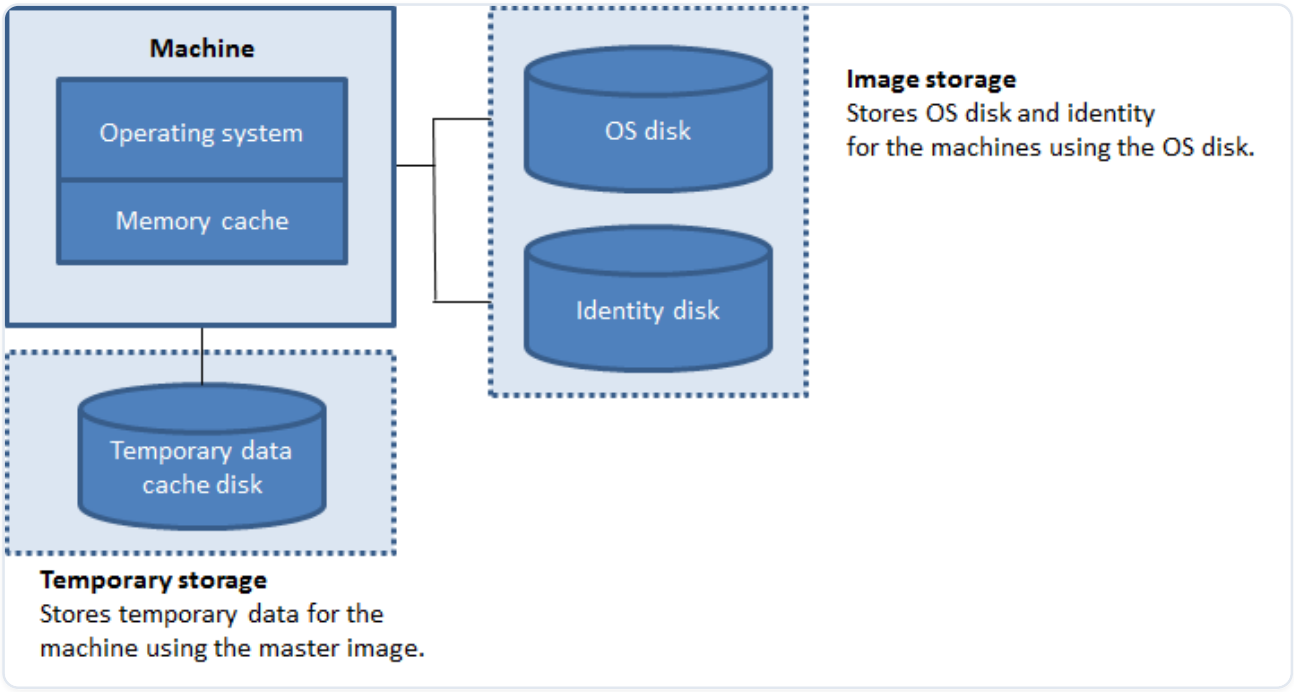
在 VM 上本地缓存临时数据是可选的。当您使用 MCS 管理目录中的池化（非专用）计算机时，可以启用在计算机上使用临时数据缓存。如果目录使用的连接指定了临时数据存储，则可以在创建目录时启用并配置临时数据缓存信息。

**重要提示：**

此功能需要当前的 MCS I/O 驱动程序。安装此驱动程序是安装或升级 VDA 时的可选操作。默认情况下，该驱动程序未安装。

在创建目录使用的连接时，您可以指定临时数据是使用共享存储还是本地存储。有关详细信息，请参阅连接和资源。要为每台计算机配置临时数据缓存，可以使用以下两个选项：**分配给缓存的内存 (MB)** 和 **磁盘缓存大小 (GB)**。默认情况下，这两个选项处于未选中状态。要启用“分配给缓存的内存 (MB)”选项，请选中“磁盘缓存大小 (GB)”复选框。如果未选中“**磁盘缓存大小**”复选框，“分配给缓存的内存”选项将灰显。根据连接类型，这些选项的默认值可能有所不同。通常，默认值足以满足大多数情况。但是，请考虑以下所需的空间：

- Windows 自身创建的临时数据文件，包括 Windows 页面文件。
- 用户配置文件数据。
- 同步到用户会话的 ShareFile 数据。
- 会话用户可能创建或复制的数据，或者用户可能在会话中安装的任何应用程序。




要为每台计算机配置临时数据缓存，请注意以下三种情况：

- 如果未选中“磁盘缓存大小”复选框和“分配给缓存的内存”复选框，则临时数据不会被缓存。它会直接写入每台 VM 的差异磁盘（位于操作系统存储中）。（这是 7.8 及更早版本中的预配操作。）
- 如果选中“磁盘缓存大小”复选框但未选中“分配给缓存的内存”复选框，则临时数据会直接写入缓存磁盘，使用最少量的内存缓存。
- 如果选中“磁盘缓存大小”复选框和“分配给缓存的内存”复选框，则临时数据最初会写入内存缓存。当内存缓存达到其配置的限制（“分配给缓存的内存”值）时，最旧的数据会移动到临时数据缓存磁盘。

**重要提示：**

- 如果磁盘缓存空间不足，用户的会话将变得不可用。
- 使用 Nutanix 主机连接时，此功能不可用。
- 计算机创建后，您无法更改计算机目录中的缓存值。

**注意：**

- 内存缓存是每台计算机总内存的一部分。因此，如果启用“分配给缓存的内存”选项，请考虑增加每台计算机的总内存量。

- 更改“磁盘缓存大小”的默认值可能会影响性能。大小必须与用户要求以及计算机上的负载相匹配。

## NIC

在创建远程电脑访问目录时，此页面不会显示。

在“**网络接口卡**”页面上，如果您计划使用多个 NIC，请将虚拟网络与每张卡关联。例如，您可以将一张卡分配给访问特定的安全网络，将另一张卡分配给访问更常用的网络。您还可以从此页面添加或删除 NIC。

## 计算机帐户

此页面仅在创建远程电脑访问目录时显示。

在“**计算机帐户**”页面上，指定要添加的与用户或用户组对应的 Active Directory 计算机帐户或组织单位 (OU)。OU 名称中请勿使用正斜杠 (/)。

您可以选择以前配置的电源管理连接，也可以选择不使用电源管理。如果您想使用电源管理但尚未配置合适的连接，您可以稍后创建该连接，然后编辑计算机目录以更新电源管理设置。

## 计算机帐户

此页面仅在使用 MCS 创建 VM 时显示。

目录中的每台计算机都必须具有相应的 Active Directory 计算机帐户。在“**计算机帐户**”页面上，指明是创建帐户还是使用现有帐户，以及这些帐户的位置。

- 如果您创建帐户，则必须具有在计算机所在的 OU 中创建计算机帐户的权限。

  指定计算机的帐户命名方案，使用井号标记指示序列号或字母出现的位置。OU 名称中请勿使用正斜杠 (/)。名称不能以数字开头。例如，命名方案 PC-Sales-##（选择 0-9）将生成名为 PC-Sales-01、PC-Sales-02、PC-Sales-03 等的计算机帐户。
- 如果您使用现有帐户，请浏览到这些帐户，或单击“**导入**”并指定包含帐户名称的 .csv 文件。导入的文件内容必须使用以下格式：

```
[ADComputerAccount]

ADcomputeraccountname.domain
```

> ...

确保有足够的帐户用于您要添加的所有计算机。Studio 管理这些帐户，因此请允许 Studio 重置所有帐户的密码，或指定帐户密码（所有帐户的密码必须相同）。

对于包含物理计算机或现有计算机的目录，请选择或导入现有帐户。将每台计算机分配给 Active Directory 计算机帐户和用户帐户。

对于使用 Citrix Provisioning 创建的计算机，目标设备的计算机帐户管理方式不同；请参阅 Citrix Provisioning 文档。

## 摘要、名称和说明

在**摘要**页面上，检查您指定的设置。输入目录的名称和描述。此信息将显示在 Studio 中。

完成后，单击 **完成** 以开始创建目录。

## 故障排除

> **重要提示：**

> 使用 Citrix Studio 创建计算机目录后，您将无法再使用 `Get-ProvTask` PowerShell 命令检索与计算机目录创建相关的任务。此限制是由于 Studio 在创建计算机目录后会删除这些任务，无论目录是否成功创建。

> Citrix 建议收集日志以帮助支持团队提供解决方案。使用 Citrix Provisioning 时，请按照以下过程生成日志文件：

1. 在主映像上，创建以下注册表项，其值为 1（作为 DWORD（32 位）值）：`HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. 关闭主映像并创建快照。
3. 在 Delivery Controller 上，运行以下 PowerShell 命令：`Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
4. 基于该快照创建目录。
5. 在虚拟机管理程序上创建准备 VM 后，登录并从 `C:\` 的根目录中提取以下文件：Image-prep.log 和 PvsVmAgentLog.txt。
6. 关闭计算机，此时它会报告故障。

7. 运行以下 PowerShell 命令以重新启用映像准备计算机的自动关机：`Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`。

## 下一步操作

如果这是创建的第一个目录，Studio 会引导您创建交付组。

# 管理计算机目录

## 简介

您可以从计算机目录中添加或删除计算机、重命名、更改描述或管理目录的 Active Directory 计算机帐户。

维护目录还可以包括确保每台计算机都具有最新的操作系统更新。包括防病毒更新、操作系统升级或配置更改。

- 包含使用 Machine Creation Services™ (MCS) 创建的随机池化计算机的目录通过更新目录中使用的主映像，然后更新计算机来维护计算机。此方法使您能够有效地更新大量用户计算机。
- 对于使用 Citrix Provisioning™ 创建的计算机，计算机更新通过虚拟磁盘传播。有关详细信息，请参阅 Citrix Provisioning 文档。
- 对于包含静态、永久分配计算机的目录以及远程电脑访问计算机目录，您可以在 Studio 外部管理用户计算机的更新。可以使用第三方软件分发工具单独或集体执行此任务。

有关创建和管理到主机管理程序的连接的信息，请参阅连接和资源。

> **注意：**
>
> MCS 不支持 Windows 10 IoT Core 和 Windows 10 IoT Enterprise。有关详细信息，请参阅 Microsoft 站点。

### 关于持久性实例

更新使用持久或专用实例创建的 MCS 目录时，为该目录创建的任何新计算机都将使用更新后的映像。现有实例将继续使用原始实例。更新映像的过程与任何其他类型的目录相同。请考虑以下事项：

- 对于持久性磁盘目录，现有计算机不会更新到新映像，但添加到目录中的任何新计算机都使用新映像。

- 对于非持久性磁盘目录，计算机映像将在下次计算机重置时更新。
- 对于持久性计算机目录，更新映像也会更新使用该映像的目录实例。
- 对于非持久性目录，如果您希望不同计算机使用不同的映像，则这些映像必须位于单独的目录中。

## 将计算机添加到目录

开始之前：

- 确保虚拟化主机具有足够的处理器、内存和存储空间来容纳额外的计算机。
- 确保您有足够的未使用的 Active Directory 计算机帐户。如果您使用现有帐户，则可以添加的计算机数量受可用帐户数量的限制。
- 如果您使用 Studio 为其他计算机创建 Active Directory 计算机帐户，则必须具有相应的域管理员权限。

要将计算机添加到目录：

1. 在 **Studio** 导航窗格中选择**计算机目录**。
2. 选择一个计算机目录，然后在**操作**窗格中选择**添加计算机**。
3. 选择要添加的虚拟机数量。
4. 如果现有 Active Directory 帐户不足以满足您要添加的 VM 数量，请选择创建帐户的域和位置。指定帐户命名方案，使用井号标记指示连续数字或字母出现的位置。OU 名称中不要使用正斜杠 (/)。名称不能以数字开头。例如，命名方案 PC-Sales-##（选择 0-9）将生成名为 PC-Sales-01、PC-Sales-02、PC-Sales-03 等的计算机帐户。
5. 如果使用现有 Active Directory 帐户，请浏览到这些帐户，或单击**导入**并指定包含帐户名称的 .csv 文件。确保有足够的帐户用于您要添加的所有计算机。Studio 管理这些帐户。可以允许 Studio 重置所有帐户的密码，也可以指定帐户密码，该密码必须对所有帐户都相同。

计算机以后台进程的形式创建，并且在创建大量计算机时可能需要很长时间。即使关闭 Studio，计算机创建也会继续。

## 从目录中删除计算机

从计算机目录中删除计算机后，用户将无法再访问它，因此在删除计算机之前，请确保：

- 用户数据已备份或不再需要。
- 所有用户均已注销。启用维护模式可阻止新连接连接到计算机。
- 计算机已关机。

要从目录中删除计算机，请执行以下操作：

1. 在 **Studio** 导航窗格中选择**计算机目录**。
2. 选择一个目录，然后在**操作**窗格中选择**查看计算机**。
3. 选择一台或多台计算机，然后在**操作**窗格中选择**删除**。

选择是否删除正在移除的计算机。如果选择删除计算机，请指明这些计算机的 Active Directory 帐户是保留、禁用还是删除。

## 更改目录描述或更改远程电脑访问设置

1. 在 **Studio** 导航窗格中选择**计算机目录**。
2. 选择一个目录，然后在**操作**窗格中选择**编辑计算机目录**。
3. 对于远程电脑访问目录，使用**电源管理**页面更改电源管理设置并选择电源管理连接。在**组织单位**页面上，添加或移除 Active Directory OU。
4. 在**描述**页面上，更改目录描述。

## 重命名目录

1. 在 **Studio** 导航窗格中选择**计算机目录**。
2. 选择一个目录，然后在**操作**窗格中选择**重命名计算机目录**。
3. 输入新名称。

## 将目录移动到其他区域

如果您的部署有多个区域，可以将目录从一个区域移动到另一个区域。

将目录移动到不同于包含该目录中 VM 的管理程序的区域会影响性能。

1. 在 **Studio** 导航窗格中选择 **计算机目录**。
2. 选择一个目录，然后在 **操作** 窗格中选择 **移动**。
3. 选择要将目录移动到的区域。

## 删除目录

删除目录之前，请确保：

- 所有用户均已注销，并且没有断开连接的会话正在运行。
- 目录中的所有计算机均已启用维护模式，以便无法建立新连接。
- 目录中的所有计算机均已关机。

- 目录未关联交付组。换句话说，交付组不包含来自该目录的计算机。

要删除目录，请执行以下操作：

1. 在 **Studio** 导航窗格中选择 **计算机目录**。
2. 选择一个目录，然后在 **操作** 窗格中选择 **删除计算机目录**。
3. 指示是否删除目录中的计算机。如果您选择删除计算机，请指示是保留、禁用还是删除这些计算机的 Active Directory 计算机帐户。

## 管理目录中的 Active Directory 计算机帐户

要管理计算机目录中的 Active Directory 帐户，您可以：

- 通过从单会话操作系统和多会话操作系统目录中删除 Active Directory 计算机帐户来释放未使用的计算机帐户。然后，这些帐户可用于其他计算机。
- 添加帐户，以便在向目录添加更多计算机时，计算机帐户已就位。请勿在 OU 名称中使用正斜杠 (/)。

要管理 Active Directory 帐户：

1. 在 **Studio** 导航窗格中选择 **计算机目录**。
2. 选择一个目录，然后在 **操作** 窗格中选择 **管理 AD 帐户**。
3. 选择是添加还是删除计算机帐户。如果添加帐户，请指定如何处理帐户密码：要么全部重置，要么输入一个适用于所有帐户的密码。

   如果您不知道当前帐户密码，则可以重置密码；您必须具有执行密码重置的权限。输入密码时，导入帐户后会更改其密码。删除帐户时，请选择是保留、禁用还是删除 Active Directory 中的帐户。

指示从目录中删除计算机或删除目录时，是保留、禁用还是删除 Active Directory 帐户。

## 更新目录

建议您在更新目录中的计算机之前保存主映像的副本或快照。数据库会保留每个计算机目录所用主映像的历史记录。回滚或还原目录中的计算机以使用主映像的先前版本。如果用户遇到您部署到其桌面的更新问题，请执行此任务。这可最大程度地减少用户停机时间。请勿删除、移动或重命名主映像。您无法还原目录以使用它们。

对于使用 Citrix Provisioning（以前称为 Provisioning Services）的目录，您必须发布新的虚拟磁盘才能将更改应用到目录。有关详细信息，请参阅 Citrix Provisioning 文档。

计算机更新后，会自动重新启动。

### 更新或创建主映像

在更新计算机目录之前，请更新现有主映像或在主机管理程序上创建主映像。

1. 在您的管理程序上，为当前 VM 创建快照并为该快照指定一个有意义的名称。如果需要，此快照可用于还原（回滚）目录中的计算机。
2. 如有必要，请启动主映像并登录。
3. 安装更新或对主映像进行任何必要的更改。
4. 关闭 VM。
5. 创建 VM 的快照。为其指定一个有意义的名称，以便在 Studio 中更新目录时能够识别。尽管 Studio 可以创建快照，但 Citrix 建议您使用管理程序管理控制台创建快照。然后在 Studio 中选择该快照。此过程使您能够提供有意义的名称和描述，而不是自动生成的名称。对于 GPU 主映像，您只能通过 Citrix Hypervisor™ 控制台更改主映像。

### 更新目录

要准备更新并将其推广到目录中的所有计算机，请执行以下操作：

1. 在 **Studio** 导航窗格中选择 **计算机目录**。
2. 选择一个目录，然后在 **操作** 窗格中选择 **更新计算机**。
3. 在 **主映像** 页面上，选择要部署的主机和映像。
4. 在**推出策略**页面上，选择计算机目录中的计算机何时使用新主映像进行更新：在下次关机时或立即更新。
5. 验证**摘要**页面上的信息，然后单击**完成**。每台计算机更新后会自动重新启动。

当直接使用 PowerShell SDK 而非 Studio 更新目录时，请指定一个管理程序模板（VM 模板）。将其用作映像或映像快照的替代方案。

**推出策略：**

在下次关机时更新映像将立即影响所有当前未使用的计算机，即没有活动用户会话的计算机。正在使用的系统将在当前活动会话结束时接收更新。请考虑以下事项：

- 在适用的计算机上完成更新之前，无法启动新会话。
- 对于单会话操作系统计算机，当计算机未使用或用户未登录时，计算机将立即更新。
- 对于具有子计算机的多会话操作系统，不会自动重新启动。要应用更新的主映像，请使用 Studio、PowerShell 或 Workspace 重新启动计算机。从计算机或管理程序重新启动不会应用更新。

> **提示：**
>
> 通过使用主机连接的高级设置来限制正在重新启动的计算机数量。使用这些设置可以修改给定目录所采取的操作；高级设置因虚拟机管理程序而异。

> 如果您选择立即更新映像，请配置分发时间和通知。

- **分发时间：** 选择同时更新所有计算机，或指定开始更新目录中所有计算机的总时长。内部算法会确定在此间隔内每台计算机何时更新和重新启动。
- **通知：** 在左侧通知下拉菜单中，选择是否在更新开始前在计算机上显示通知消息。默认情况下，不显示任何消息。选择在更新开始前 15 分钟显示消息。或者，选择在初始消息后每五分钟重复一次消息。默认情况下，消息不重复。除非您选择同时更新所有计算机，否则通知消息会在更新开始前的适当时间显示在每台计算机上。

### 回滚更新

推出更新/新主映像后，您可以将其回滚。如果新更新的计算机出现问题，则可能需要此过程。回滚时，目录中的计算机将回滚到上次正常工作的映像。需要较新映像的任何新功能将不再可用。与推出一样，回滚计算机也包括重新启动。

1. 在 **Studio** 导航窗格中选择 **Machine Catalogs**。
2. 选择目录，然后在 **Actions** 窗格中选择 **Rollback machine update**。
3. 按照上一节中关于推出操作的说明，指定何时将较早的主映像应用于计算机。

回滚仅应用于需要恢复的计算机。尚未通过新/更新主映像进行更新的计算机不会收到通知消息，也不会被强制注销。

## 升级目录或恢复升级

将计算机上的 VDA 升级到较新版本后，升级计算机目录。Citrix® 建议将所有 VDA 升级到最新版本，以启用对所有最新功能的访问。

升级目录之前：

- 如果您正在使用 Citrix Provisioning，请升级 VDA 版本。预配控制台不保留 VDA 版本。Citrix Provisioning 直接与 Citrix Virtual Apps and Desktops™ 安装向导通信，以在创建的目录中设置 VDA 版本。
- 启动已升级的计算机，使其向 Controller 注册。此过程使 Studio 能够确定目录中的计算机需要升级。

要升级目录：

1. 在 **Studio** 导航窗格中选择 **计算机目录**。
2. 选择目录。下部窗格中的**详细信息**选项卡显示版本信息。
3. 选择 **升级目录**。如果 Studio 检测到目录需要升级，它会显示一条消息。按照提示操作。如果一台或多台计算机无法升级，将显示一条消息解释原因。Citrix 建议您在升级目录之前解决计算机问题，以确保所有计算机正常运行。

目录升级完成后，您可以通过选择目录，然后在 **操作** 窗格中选择 **撤消**，将计算机恢复到以前的 VDA 版本。

## 更改现有预配方案的网络设置

您可以更改现有预配方案的网络设置，以便在新子网上创建新的 VM。使用 `Set-ProvScheme` 命令中的 `-NetworkMapping` 参数更改网络设置。

> **注意：**
>
> 此功能在 Citrix Virtual Apps and Desktops 2203 LTSR CU3 及更高版本中受支持。

> 要更改现有预配方案的网络设置，请执行以下操作：

1. 在 PowerShell 窗口中，运行命令 `asnp citrix*` 以加载 PowerShell 模块。
2. 运行 `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` 以获取要更改的网络路径。
3. 为新的网络设置分配一个变量。例如：

   ```
   $NewNetworkMap = @{“0”= “XDHYP:\HostingUnits\MyNetworks\Network 0.network”}
   ```

4. 运行 `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap`。
5. 运行 `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` 以验证现有预配方案的新网络设置。

## 故障排除

- 对于状态为“电源状态未知”的计算机，请参阅 CTX131267 获取指导。

- 要修复持续显示未知电源状态的 VM，请参阅 如何修复持续显示未知电源状态的 VM。

# 创建交付组

交付组是从一个或多个计算机目录中选择的计算机集合。交付组指定哪些用户可以使用这些计算机，以及这些用户可用的应用程序和桌面。

创建交付组是在创建站点和创建计算机目录之后配置部署的下一步。稍后，您可以更改第一个交付组中的初始设置并创建其他交付组。还有一些功能和设置只能在编辑交付组时配置，而不能在创建时配置。

对于远程电脑访问，当您创建站点时，会自动创建一个名为“远程电脑访问桌面”的交付组。

要创建交付组，请执行以下操作：

1. 如果您已创建站点和计算机目录，但没有交付组，Studio 会指导您到正确的起始位置来创建一个。如果您已创建交付组并想创建另一个，请选择**交付组**。在“操作”窗格中选择**创建交付组**。
2. 向导将启动一个**简介**页面，您可以选择在此向导的未来启动中将其删除。
3. 然后，向导将指导您完成以下部分中描述的页面。完成每个页面后，单击**下一步**，直到到达最后一页。

## 步骤 1. 计算机

在**计算机**页面上，选择一个目录并选择要从该目录使用的计算机数量。

须知：

- 所选目录中至少有一台计算机必须保持未使用状态。
- 一个目录可以在多个交付组中指定。一台计算机只能在一个交付组中使用。
- 一个交付组可以使用来自多个目录的计算机；但是，这些目录必须包含相同的计算机类型（多会话操作系统、单会话操作系统或远程电脑访问）。换句话说，您不能在交付组中混合计算机类型。同样，如果您的部署包含 Windows 计算机目录和 Linux 计算机目录，则交付组可以包含来自任一操作系统类型的计算机，但不能同时包含两者。
- Citrix 建议您安装或升级所有计算机，使其使用最新的 VDA 版本。根据需要升级目录和交付组。创建交付组时，如果您选择安装了不同 VDA 版本的计算机，则交付组与最早的 VDA 版本兼容。这称为组的*功能级别*。例如，如果其中一台计算机的 VDA 版本为 7.1，而其他计算机的版本为当前版本，则组中的所有计算机只能使用 VDA 7.1 中支持的功能。这意味着某些需要较新 VDA 版本的功能可能在该交付组中不可用。

- 远程电脑访问目录中的每台计算机都会自动与一个交付组关联。当您创建远程电脑访问站点时，会自动创建一个名为“远程电脑访问计算机”的目录和一个名为“远程电脑访问桌面”的交付组。
- 执行以下兼容性检查：
  - MinimumFunctionalLevel 必须兼容
  - SessionSupport 必须兼容
  - SingleSession 的 AllocationType 必须兼容
  - ProvisioningType` 必须兼容
  - PersistChanges 必须与 MCS 和 Citrix Provisioning™ 兼容
  - RemotePC 目录仅与 RemotePC 目录兼容
  - AppDisk 相关检查

## 步骤 2. 交付类型

此页面仅在您选择的目录包含静态（分配的）单会话操作系统计算机时显示。

在**交付类型**页面上，选择**应用程序**或**桌面**。不能同时启用两者。

如果您从多会话操作系统或单会话操作系统随机（池化）目录中选择了计算机，则交付类型假定为应用程序和桌面：您可以交付应用程序、桌面或两者。

## 步骤 3. 用户

指定可以使用交付组中的应用程序和桌面的用户和用户组。

### 指定用户列表的位置

在创建或编辑以下内容时指定 Active Directory 用户列表：

- 站点的用户访问列表，该列表不是通过 Studio 配置的。默认情况下，应用程序授权策略规则包括所有人。有关详细信息，请参阅 PowerShell SDK `BrokerAppEntitlementPolicyRule` cmdlet。
- 应用程序组（如果已配置）。
- 交付组。
- 应用程序。

可以通过 StoreFront™ 访问应用程序的用户列表由上述用户列表的交集形成。例如，要将应用程序 A 的使用配置给特定部门，而不过度限制对其他组的访问：

- 使用包含所有人的默认应用程序授权策略规则。

- 配置交付组用户列表，以允许所有总部用户使用交付组中指定的任何应用程序。
- (如果配置了应用程序组) 配置应用程序组用户列表，以允许管理和财务业务部门的成员访问应用程序 A 到 L。
- 配置应用程序 A 的属性，以将其可见性限制为仅限管理和财务部门的应收账款员工。

### 已验证用户和未验证用户

有两种类型的用户：已验证用户和未验证用户（未验证用户也称为匿名用户）。您可以在交付组中配置其中一种或两种类型。

- **已验证用户：** 要访问应用程序和桌面，您按名称指定的这些用户和组成员必须向 StoreFront 或 Citrix Workspace™ 应用程序提供凭据，例如智能卡或用户名和密码。对于包含单会话操作系统计算机的交付组，您可以通过编辑交付组稍后导入用户数据（用户列表）。
- **未验证用户（匿名用户）：** 对于包含多会话操作系统计算机的交付组，您可以允许用户访问应用程序和桌面，而无需向 StoreFront 或 Citrix Workspace 应用程序提供凭据。例如，在信息亭中，应用程序可能需要凭据，但 Citrix 访问门户和工具不需要。安装第一个 Delivery Controller 时会创建一个匿名用户组。

  要授予未验证用户访问权限，交付组中的每台计算机都必须安装适用于 Windows Server OS 的 VDA（最低版本 7.6）。启用未验证用户时，您必须拥有一个未验证的 StoreFront 商店。

  未验证用户帐户在会话启动时按需创建，并命名为 Anon*XYZ*，其中 *XYZ* 是一个唯一的三位数值。

  未经身份验证的用户会话的默认空闲超时为 10 分钟，并且在客户端断开连接时会自动注销。不支持重新连接、客户端之间漫游和 Workspace Control。

下表描述了您在**用户**页面上的选择：

| 启用访问权限 | 添加/分配用户和用户组？ | 启用“授予未验证用户访问权限”复选框？ |
|---|---|---|
| 仅限经过身份验证的用户 | 是 | 否 |
| 仅限未经身份验证的用户 | 否 | 是 |
| 已验证和未验证用户 | 是 | 是 |

## 步骤 4. 应用程序

须知：

- 您无法将应用程序添加到远程电脑访问交付组。
- 默认情况下，您添加的新应用程序会放置在名为“应用程序”的文件夹中。您可以指定其他文件夹。有关详细信息，请参阅“管理应用程序”一文。
- 您可以在将应用程序添加到交付组时或之后更改其属性。有关详细信息，请参阅“管理应用程序”一文。
- 如果您尝试添加一个应用程序，并且该文件夹中已存在同名应用程序，系统会提示您重命名要添加的应用程序。如果您拒绝，则会为该应用程序添加一个后缀，使其在该应用程序文件夹中是唯一的。
- 当您将应用程序添加到多个交付组时，如果您没有足够的权限在所有这些交付组中查看该应用程序，则可能会出现可见性问题。在这种情况下，请咨询具有更高权限的管理员，或者扩展您的范围以包括添加了该应用程序的所有交付组。
- 如果您向同一用户发布两个同名应用程序，请在 Studio 中更改“应用程序名称（面向用户）”属性；否则，用户将在 Citrix Workspace 应用程序中看到重复的名称。

单击**添加**以显示应用程序源。

- **从“开始”菜单”：** 在所选目录中从主映像创建的计算机上发现的应用程序。选择此源时，将启动一个新页面，其中包含发现的应用程序列表；选择要添加的应用程序，然后单击 **“确定”**。
- **手动定义：** 位于站点或网络中其他位置的应用程序。选择此源时，将启动一个新页面，您可以在其中键入可执行文件的路径、工作目录、可选命令行参数以及管理员和用户的显示名称。输入此信息后，单击 **“确定”**。
- **现有：** 以前添加到站点的应用程序，可能位于另一个交付组中。选择此源时，将启动一个新页面，其中包含发现的应用程序列表。添加应用程序，然后单击 **“确定”**。
- **App-V：** App-V 软件包中的应用程序。选择此源时，将启动一个新页面，您可以在其中选择 App-V 服务器或应用程序库。从结果显示中选择要添加的应用程序，然后单击 **“确定”**。有关详细信息，请参阅 App-V。

如果应用程序源或应用程序不可用或无效，则它不可见或无法选择。例如，如果尚未向站点添加任何应用程序，则 **“现有”** 源不可用。或者，应用程序可能与所选目录中计算机上支持的会话类型不兼容。

## 步骤 5. 桌面

此页面的标题取决于您在 **“计算机”** 页面上选择的目录：

- 如果您选择的目录包含池化计算机，则此页面的标题为 **“桌面”**。
- 如果您选择的目录包含分配的计算机，并且在 **“交付类型”** 页面上指定了“桌面”，则此页面的标题为 **“桌面用户分配”**。

- 如果您选择的目录包含分配的计算机，并且在 **“交付类型”** 页面上指定了“应用程序”，则此页面的标题为 **“应用程序计算机用户分配”**。

单击 **“添加”**。在对话框中：

- 在“显示名称”和“描述”字段中，键入要在 Citrix Workspace 应用程序中显示的信息。
- 要向桌面添加标记限制，请选择 **“将启动限制为具有此标记的计算机”**，然后从下拉列表中选择标记。有关详细信息，请参阅 标记。
- 使用单选按钮启动桌面或在启动桌面时分配计算机。用户可以是所有可以访问此交付组的用户，也可以是特定的用户和用户组。
- 如果组包含已分配的计算机，请指定每个用户的最大桌面数。此值必须大于或等于一。
- 启用或禁用桌面（对于池化计算机）或桌面分配规则（对于已分配的计算机）。禁用桌面会停止桌面交付。禁用桌面分配规则会停止向用户自动分配桌面。
- 完成对话框后，单击 **确定**。

### 站点中桌面的最大实例数（仅限 PowerShell）

要配置站点中桌面的最大实例数（仅限 PowerShell），请执行以下操作：

- 在 PowerShell 中，将相应的 BrokerEntitlementPolicyRule cmdlet 与 MaxPerEntitlementInstances 参数结合使用。例如，以下 cmdlet 修改 `tsvda-desktop` 规则，将站点中允许的桌面最大并发实例数设置为两个。当有两个桌面实例正在运行时，如果第三个订阅者尝试启动桌面，则会发生错误。

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
  -MaxPerEntitlementInstances 2
  ```

- 有关指导，请使用 Get-Help cmdlet。例如，`Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`。

## 步骤 6. 摘要

输入交付组的名称。您还可以（可选）输入说明，该说明将显示在 Citrix Workspace 应用程序和 Studio 中。

查看摘要信息，然后单击**完成**。

# 管理交付组

## 简介

本文介绍了通过管理控制台管理交付组的步骤。除了更改创建组时指定的设置外，您还可以配置创建交付组时不可用的其他设置。

过程类别包括：常规、用户、计算机和会话。某些任务跨越多个类别。例如，“阻止用户连接到计算机”在计算机类别中描述，但它也影响用户。如果在一个类别中找不到任务，请检查相关类别。

其他文章也包含相关信息：

- 应用程序 包含有关管理交付组中应用程序的信息。
- 管理交付组需要交付组管理员内置角色权限。有关详细信息，请参阅 委派管理。

## 常规

- 更改交付类型
- 更改 StoreFront™ 地址
- 升级交付组
- 管理远程电脑访问交付组

### 更改交付组的交付类型

交付类型指示组可以交付的内容：应用程序、桌面或两者。

在将**仅应用程序**或**桌面和应用程序**类型更改为**仅桌面**类型之前，请从组中删除所有应用程序。

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后在“操作”窗格中单击**编辑交付组**。
3. 在 **交付类型** 页面上，选择所需的交付类型。
4. 单击**应用**以应用所做的任何更改并保持窗口打开。或者，单击**确定**以应用更改并关闭窗口。

### 更改 StoreFront 地址

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后在“操作”窗格中单击**编辑交付组**。
3. 在**StoreFront**页面上，选择或添加 StoreFront URL。这些 URL 由 Citrix Workspace™ 应用程序使用，该应用程序安装在交付组中的每台计算机上。
4. 单击**应用**以应用所做的任何更改并保持窗口打开。或者，单击**确定**以应用更改并关闭窗口。

您还可以通过在导航窗格中选择**配置 > StoreFront**来指定 StoreFront 服务器地址。

### 升级交付组或回滚升级

在升级交付组中的计算机上的 Virtual Delivery Agent (VDA) 以及包含交付组中所用计算机的计算机目录后，升级交付组。

在开始交付组升级之前：

- 如果您使用 Citrix Provisioning™（以前称为 Provisioning Services），请在 Citrix Provisioning 控制台中升级 VDA 版本。
- 启动包含已升级 VDA 的计算机，以便它们可以向 Delivery Controller 注册。此过程会告知控制台交付组中需要升级的内容。
- 如果继续使用早期 VDA 版本，则无法使用较新的产品功能。有关详细信息，请参阅升级文档。

要升级交付组：

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后在“操作”窗格中单击**升级交付组**。仅当检测到已升级的 VDA 时，才会显示**升级交付组**操作。

显示屏会指示您哪些计算机（如果有）无法升级以及原因。然后，您可以取消升级，解决计算机问题，然后再次开始升级。

升级完成后，您可以通过选择交付组，然后在**操作**窗格中单击**撤消**来将计算机恢复到以前的状态。

### 管理远程电脑访问交付组

如果远程电脑访问计算机目录中的计算机未分配，则该计算机将临时分配给与该目录关联的交付组。此临时分配使计算机以后可以分配给用户。

交付组到计算机目录的关联具有优先级值。优先级决定了计算机在注册到系统时或用户需要分配计算机时所分配的交付组。值越低，优先级越高。如果远程电脑访问计算机目录具有多个交付组分配，则软件会选择优先级最高的匹配项。使用 PowerShell SDK 设置此优先级值。

首次创建时，远程电脑访问计算机目录与交付组关联。稍后添加到目录的计算机帐户或组织单位可以添加到交付组。此关联可以关闭或打开。

要添加或删除远程电脑访问计算机目录与交付组的关联：

1. 在导航窗格中选择 **交付组**。
2. 选择一个远程电脑访问组。

3. 在 **详细信息** 部分中，单击 **计算机目录** 选项卡，然后选择一个远程电脑访问目录。
4. 要添加或恢复关联，请单击 **添加桌面**。要删除关联，请单击 **删除关联**。

## 用户

- 更改用户设置
- 添加或删除用户

### 更改交付组中的用户设置

此页面的名称显示为**用户设置**或**基本设置**。

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后在“操作”窗格中单击**编辑交付组**。
3. 在**用户设置**（或**基本设置**）页面上，更改下表中的任何设置。
4. 点击 **应用** 以应用所做的任何更改并保持窗口打开。或者，点击 **确定** 以应用更改并关闭窗口。

| 设置 | 描述 |
| --- | --- |
| 描述 | Citrix Workspace（或 StoreFront）使用的文本，也是用户看到的文本。 |
| 启用交付组 | 交付组是否已启用。 |
| 时区 | 此交付组中的计算机必须驻留的时区。该选项列出了站点支持的时区。 |
| 启用 Secure ICA® | 使用 SecureICA 保护交付组中计算机之间的通信，SecureICA 会加密 ICA 协议。默认级别为 128 位。可以使用 SDK 更改级别。Citrix® 建议在遍历公共网络时使用更多加密方法，例如 TLS 加密。此外，SecureICA 不会检查数据完整性。 |

### 在交付组中添加或删除用户

有关用户的详细信息，请参阅用户。

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后点击“操作”窗格中的 **编辑交付组**。
3. 在**用户**页面上：

- 要添加用户，请点击“**添加**”，然后指定要添加的用户。
- 要删除用户，请选择一个或多个用户，然后点击“**删除**”。
- 选中或清除复选框以允许未经身份验证的用户访问。

4. 点击 **应用** 以应用所做的任何更改并保持窗口打开。或者，点击 **确定** 以应用更改并关闭窗口。

#### 导入或导出用户列表

对于包含物理单会话操作系统计算机的交付组，您可以在创建交付组后从 .csv 文件导入用户信息。您还可以将用户信息导出到 .csv 文件。.csv 文件可以包含来自以前产品版本的数据。

CSV 文件中的第一行必须包含两个列标题，以逗号分隔。确保第一个标题是 `Machine Account`，第二个标题是 `User Names`。（您可以包含其他标题，但不支持这些标题。）文件中的后续行包含逗号分隔的数据。`Machine Account` 条目可以是计算机 SID、FQDN 或域与计算机名称对。

要导入或导出用户信息：

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后点击“操作”窗格中的 **编辑交付组**。
3. 在“**计算机分配**”页面上，选择“**导入**”列表或“**导出**”列表，然后浏览到文件位置。
4. 点击 **应用** 以应用所做的任何更改并保持窗口打开。或者，点击 **确定** 以应用更改并关闭窗口。

## 计算机

- 更改计算机到用户的分配
- 更改每个用户的最大计算机数
- 更新计算机(#update-a-machine-in-a-delivery-group)
- 添加、更改或删除桌面的标签限制(#add-change-or-remove-a-tag-restriction-for-a-desktop)
- 删除计算机(#remove-a-machine-from-a-delivery-group)
- 限制对计算机的访问
- 阻止用户连接到计算机（维护模式）(#prevent-users-from-connecting-to-a-machine-maintenance-mode-in-a-delivery-group)
- 关闭并重新启动计算机(#shut-down-and-restart-machines-in-a-delivery-group)
- 创建和管理计算机的重新启动计划(#create-and-manage-restart-schedules-for-machines-in-a-delivery-group)
- 加载受管计算机
- 电源受管计算机

### 更改交付组中计算机到用户的分配

您可以更改使用 MCS 预配的单会话操作系统计算机的分配。您无法更改多会话操作系统计算机或使用 Citrix Provisioning 预配的计算机的分配。

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后点击“操作”窗格中的 **编辑交付组**。
3. 在 **桌面** 或 **桌面分配规则** 页面上（页面标题取决于交付组使用的计算机目录类型），指定新用户。
4. 点击 **应用** 以应用所做的任何更改并保持窗口打开。或者，点击 **确定** 以应用更改并关闭窗口。

### 更改交付组中每个用户的最大计算机数

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后点击“操作”窗格中的 **编辑交付组**。
3. 在“**桌面分配规则**”页面上，设置每个用户的最大桌面数。
4. 点击 **应用** 以应用所做的任何更改并保持窗口打开。或者，点击 **确定** 以应用更改并关闭窗口。

### 更新交付组中的计算机

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后点击“操作”窗格中的 **查看计算机**。
3. 选择一台计算机，然后点击“操作”窗格中的 **更新计算机**。

要选择其他映像，请选择 **主映像**，然后选择一个快照。

要应用更改并通知计算机用户，请选择**向最终用户推出通知**。然后指定：

- 何时更新主映像：立即或在下次重新启动时
- 重新启动分发时间（开始更新组中所有计算机的总时间）
- 是否通知用户重新启动
- 用户收到的消息

### 添加、更改或删除桌面的标签限制

添加、更改和删除标签限制可能会对考虑启动的桌面产生意想不到的影响。请参阅标签中的注意事项和警告。

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后点击“操作”窗格中的 **编辑交付组**。

3. 在“**桌面**”页面上，选择桌面并点击“**编辑**”。
4. 要添加标签限制，请选择 **将启动限制到具有此标签的计算机**，然后选择该标签。
5. 要更改或删除标签限制，请执行以下操作之一：
   - 选择其他标签。
   - 通过清除 **将启动限制到具有此标签的计算机** 来删除标签限制。
6. 点击 **应用** 以应用您所做的任何更改并保持窗口打开。或者，点击 **确定** 以应用更改并关闭窗口。

### 从交付组中删除计算机

删除计算机会将其从交付组中删除。它不会将其从交付组使用的计算机目录中删除。因此，该计算机可用于分配给另一个交付组。

计算机必须先关闭才能删除。要在删除计算机时暂时阻止用户连接到该计算机，请在关闭计算机之前将其置于维护模式。

计算机可能包含个人数据，因此在将计算机分配给其他用户之前请务必谨慎。请考虑重新映像计算机。

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后点击“操作”窗格中的 **查看计算机**。
3. 确保计算机已关闭。
4. 选择计算机，然后点击“操作”窗格中的 **从交付组中删除**。

您还可以通过计算机使用的连接从交付组中删除计算机。

### 限制对交付组中计算机的访问

您对限制交付组中计算机访问所做的任何更改都将覆盖以前的设置，无论您使用何种方法。您可以：

- **使用委派管理范围限制管理员访问：**创建并分配一个允许管理员访问所有应用程序的范围，以及另一个仅提供对某些应用程序访问的范围。有关详细信息，请参阅委派管理。
- **通过 SmartAccess 策略表达式限制用户访问：** 使用策略表达式筛选通过 Citrix Gateway 建立的用户连接。

  a. 在导航窗格中选择 **交付组**。

  b. 选择一个组，然后点击“操作”窗格中的 **编辑交付组**。

  c. 在**访问策略**页面上，选择**通过 NetScaler® Gateway 的连接**。

d. 要选择这些连接的子集，请选择**符合以下任何筛选器的连接**。然后定义 Citrix Gateway 站点，并添加、编辑或删除允许的用户访问方案的 SmartAccess 策略表达式。有关详细信息，请参阅 Citrix Gateway 文档。

e. 点击 **应用** 以应用您所做的任何更改并保持窗口打开。或者，点击 **确定** 以应用更改并关闭窗口。

- **通过排除筛选器限制用户访问：** 对在 SDK 中设置的访问策略使用排除筛选器。访问策略应用于交付组以优化连接。例如，您可以将计算机访问权限限制为部分用户，并且可以指定允许的用户设备。排除筛选器进一步优化访问策略。例如，出于安全考虑，您可以拒绝部分用户或设备的访问。默认情况下，排除筛选器处于禁用状态。

  例如，公司网络子网上的教学实验室可阻止从该实验室访问特定交付组。无论谁在使用实验室中的计算机，请使用以下命令：`Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`。

  使用星号 (*) 通配符匹配所有以相同策略表达式开头的标记。例如，如果您将标记 `VPDesktops_Direct` 添加到一台计算机，将 `VPDesktops_Test` 添加到另一台计算机，则在 `Set-BrokerAccessPolicy` 脚本中将标记设置为 `VPDesktops_*` 会将筛选器应用于这两台计算机。

  如果您使用 Web 浏览器连接，或者在应用商店中启用了 Citrix Workspace 应用程序用户体验功能，则无法使用客户端名称排除筛选器。

### 阻止用户连接到交付组中的计算机（维护模式）

当您需要暂时停止与计算机建立新连接时，可以为交付组中的一台或所有计算机启用维护模式。您可以在应用修补程序或使用管理工具之前执行此操作。

- 当多会话操作系统计算机处于维护模式时，用户可以连接到现有会话，但无法启动新会话。
- 当单会话操作系统计算机（或使用远程电脑访问的电脑）处于维护模式时，用户无法连接或重新连接。当前连接将保持连接状态，直到用户断开连接或注销。

要启用或禁用维护模式：

1. 在导航窗格中选择 **交付组**。
2. 选择一个组。
3. 要为交付组中的所有计算机开启维护模式，请点击“操作”窗格中的 **开启维护模式**。

   要为一台计算机开启维护模式，请点击“操作”窗格中的 **查看计算机**。选择一台计算机，然后点击“操作”窗格中的 **开启维护模式**。

4. 要为交付组中的一台或所有计算机关闭维护模式，请按照之前的说明操作，但点击“操作”窗格中的 **关闭维护模式**。

Windows 远程桌面连接 (RDC) 设置也会影响多会话操作系统计算机是否处于维护模式。在以下任何一种情况下，维护模式都处于启用状态：

- 维护模式已设置为启用，如前所述。
- RDC 设置为 **不允许连接到此计算机**。
- RDC 未设置为 **不允许连接到此计算机**。**远程主机配置用户登录模式** 设置为 **允许重新连接，但阻止新登录** 或 **允许重新连接，但阻止新登录直到服务器重新启动**。

您还可以为以下各项启用或禁用维护模式：

- 连接，这会影响使用该连接的计算机。
- 计算机目录，这会影响该目录中的计算机。

### 关闭并重新启动交付组中的计算机

远程电脑访问计算机不支持此过程。

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后点击“操作”窗格中的 **查看计算机**。
3. 选择计算机，然后点击“操作”窗格中的以下某个条目：
    - **强制关机：** 强制关闭计算机电源并刷新计算机列表。
    - **重新启动：** 请求操作系统关闭然后再次启动计算机。如果操作系统无法执行此操作，则计算机将保持其当前状态。
    - **强制重新启动：** 强制关闭操作系统，然后重新启动计算机。
    - **暂停：** 暂停计算机而不将其关闭，并刷新计算机列表。
    - **关机：** 请求操作系统关机。

对于非强制操作，如果计算机在 10 分钟内未关机，则会将其关闭电源。如果在关机期间 Windows 尝试安装更新，则存在计算机在更新完成前断电的风险。

Citrix 建议您阻止单会话操作系统计算机用户在会话中选择**关机**。有关详细信息，请参阅 Microsoft 策略文档。

您还可以在 连接 上关闭和重新启动计算机。

## 创建和管理交付组中计算机的重新启动计划

重新启动计划指定交付组中的计算机何时定期重新启动。您可以为一个交付组创建一个或多个计划。计划可以影响：

- 组中的所有计算机。
- 组中的一台或多台（但不是全部）计算机。计算机通过您应用于计算机的标签进行标识。这称为标签限制，因为标签将操作限制为仅具有该标签的项目。

例如，假设您的所有计算机都在一个交付组中。您希望每周重新启动每台计算机一次，并希望每天重新启动会计团队使用的计算机。为此，请为所有计算机设置一个计划，并为会计部门的计算机设置另一个计划。

计划包括重新启动开始的日期和时间以及持续时间。

您可以启用或禁用计划。禁用计划在测试期间、特殊时间间隔期间或在需要之前准备计划时会很有帮助。

您不能使用计划从管理控制台进行自动开机或关机，只能用于重新启动。

> **注意：**
>
> Citrix Studio 不支持为桌面操作系统配置重新启动计划。

### 计划重叠

多个计划可以重叠。在上面的示例中，两个计划都影响会计机器。这些机器可能在周日重新启动两次。调度代码旨在避免比预期更频繁地重新启动同一台机器，但这无法保证。

- 如果计划在开始时间和持续时间上精确一致，则计算机很可能只重新启动一次。
- 计划在开始时间和持续时间上的差异越大，则越有可能发生多次重新启动。
- 受计划影响的机器数量也会影响重叠的可能性。在此示例中，影响所有机器的每周计划可能会比会计机器的每日计划更快地启动重新启动，具体取决于为每个计划指定的持续时间。

有关重新启动计划的深入了解，请参阅重新启动计划内部机制。

### 查看重新启动计划

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后点击“操作”窗格中的 **编辑交付组**。
3. 选择 **重新启动计划** 页面。

**重新启动计划** 页面包含每个已配置计划的以下信息：

- 计划名称。
- 使用的标签限制（如果有）。
- 机器重新启动的频率。
- 机器用户是否收到通知。
- 计划是否已启用。

### 添加（应用）标签

当您配置使用标签限制的重新启动计划时，请确保已将标签添加到受计划影响的计算机。在上面的示例中，会计团队使用的每台计算机都应用了一个标签。有关详细信息，请参阅 标签。

尽管您可以将多个标签应用到一台计算机，但重新启动计划只能指定一个标签。

1. 在导航窗格中选择 **交付组**。
2. 选择包含由计划控制的计算机的组。
3. 点击“**查看计算机**”，然后选择要添加标记的计算机。
4. 在“操作”窗格中，单击**管理标记**。
5. 如果标记已存在，请启用标记名称旁边的复选框。如果标记不存在，请点击“**创建**”，然后指定标记的名称。创建标记后，启用新创建的标记名称旁边的复选框。
6. 在“**管理标记**”对话框中点击“**保存**”。

### 创建重新启动计划

> **注意：**
>
> 重新启动计划可应用于所有电源管理和非电源管理的多会话计算机。

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后在“操作”窗格中单击**编辑交付组**。
3. 在“**重新启动计划**”页面上，点击“**添加**”。
4. 在**添加重新启动计划**页面上：
   - 键入计划名称和描述。
   - 如果使用标记限制，请选择该标记。

- 在**重新启动频率**中，选择重新启动发生的频率：每天、工作日、周末或每周的特定某天。
- 使用 24 小时制，指定开始重新启动的时间。
- 对于**重新启动持续时间**，选择是同时重新启动所有计算机，还是开始重新启动所有受影响计算机的总时长。内部算法将确定在此间隔内何时重新启动每台计算机。

  > **注意：**
  >
  > 使用 PowerShell 时，可以使用其他重新启动持续时间选项。请参阅耗尽后重新启动。

- 在**向用户发送通知**中，选择是否在重新启动开始前在受影响的计算机上显示通知消息。默认情况下，不显示任何消息。
- 如果选择在重新启动开始前 15 分钟显示消息，则可以选择（在“通知频率”中）在初始消息之后每五分钟重复一次消息。默认情况下，不重复该消息。
- 输入通知标题和文本。没有默认文本。

  如果希望消息中包含重新启动前的分钟数，请包含变量 **%m%**。例如：“警告：您的计算机将在 %m% 分钟后自动重新启动。”在每个重复消息中，该值递减五分钟。除非您选择同时重新启动所有计算机，否则消息将在重新启动前在每台计算机上以适当的时间显示，该时间由内部算法计算。
- 要启用计划，请选中该复选框。要禁用计划，请清除该复选框。

5. 单击**应用**以应用所做的更改并保持窗口打开。或者，单击**确定**以应用更改并关闭窗口。

### 耗尽后重新启动

使用 PowerShell 创建或更新计算机重启计划时，可以使用另一个重启持续时间值（`New-BrokerRebootSchedulev2` 或 `Set-BrokerRebootSchedulev2`）。

使用 `-UseNaturalReboot <Boolean>` 参数启用耗尽后重启功能时，所有计算机将在耗尽所有会话后重启。当达到重启时间时，计算机将进入耗尽状态，并在所有会话注销后重启。

此功能支持包含单会话或多会话计算机的交付组。计算机必须进行电源管理。

在本地环境中，此功能仅在使用 PowerShell 时受支持。Studio 中不提供此功能。

### 编辑、删除、启用或禁用重新启动计划

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后在“操作”窗格中单击**编辑交付组**。

3. 在 **重新启动计划** 页面上，选中计划对应的复选框。

   - 要编辑计划，请单击**编辑**。根据创建重启计划 中的指导更新计划配置。
   - 要启用或禁用计划，请单击**编辑**。选中或清除**启用重启计划**复选框。
   - 要删除计划，请单击**删除**。确认删除。删除计划不会影响应用于受影响计算机中的任何标记。

**由于数据库中断，计划的重新启动延迟**

> **注意：**
>
> 此功能仅在 PowerShell 中可用。
>
> 如果在交付组中计算机 (VDA) 的计划重启开始之前发生站点数据库中断，则重启将在中断结束时开始。这可能会导致意外结果。

例如，假设您已将交付组的重启计划在非生产时间（从 03:00 开始）进行。在计划重启开始前一小时（02:00）发生站点数据库中断。中断持续六小时（直到 08:00）。当 Delivery Controller 与站点数据库之间的连接恢复时，重启计划开始。VDA 重启现在比原定计划晚了五个小时，导致 VDA 在生产时间重启。

为避免这种情况，您可以将 `MaxOvertimeStartMins` 参数用于 `New-BrokerRebootScheduleV2` 和 `Set-BrokerRebootScheduleV2` cmdlet。该值指定重启计划可以在计划开始时间之后开始的最大分钟数。

- 如果在此时间（计划时间 + `MaxOvertimeStartMins`）内恢复数据库连接，则 VDA 重启开始。
- 如果在此时间内未恢复数据库连接，则 VDA 重启不会开始。
- 如果省略此参数或其值为零，则无论中断持续时间如何，计划重启都会在数据库连接恢复时开始。

有关详细信息，请参阅 cmdlet 帮助。此功能仅在 PowerShell 中可用。在 Studio 中配置重新启动计划时，无法设置此值。

**维护模式下计算机的计划重启**

> **注意：**

> 此功能仅在 PowerShell 中可用。

> 要指示重启计划是否影响处于维护模式的计算机，请将 `IgnoreMaintenanceMode` 选项与 `BrokerRebootScheduleV2` cmdlet 结合使用。

例如，以下 cmdlet 创建一个计划，该计划重启处于维护模式的计算机（以及未处于维护模式的计算机）。

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup> -IgnoreMaintenanceMode $true
```

以下 cmdlet 修改现有重启计划。

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

有关详细信息，请参阅 cmdlet 帮助。此功能仅在 PowerShell 中可用。

### 在交付组中负载管理计算机

您只能对多会话操作系统计算机进行负载管理。

负载管理衡量服务器负载并根据当前环境条件确定要选择的服务器。此选择基于：

- **服务器维护模式状态：** 只有当维护模式关闭时，多会话操作系统计算机才会被考虑用于负载均衡。
- **服务器负载指数：** 确定提供多会话操作系统计算机的服务器接收连接的可能性。该指数是负载评估器（会话数以及 CPU、磁盘和内存使用等性能指标的设置）的组合。负载评估器在负载管理策略设置中指定。

  服务器负载指数为 10000 表示服务器已满载。如果没有其他可用服务器，用户在启动会话时可能会收到桌面或应用程序不可用的消息。

  您可以在 Director（监视）、Studio（管理）搜索和 SDK 中监视负载指数。

  在控制台显示中，要显示“**服务器负载指数**”列（默认情况下隐藏），请选择一台计算机，右键单击列标题，然后选择“**选择列**”。在“**计算机类别**”中，选择“**负载指数**”。

  在 SDK 中，使用 `Get-BrokerMachine` cmdlet。有关详细信息，请参阅 CTX202150。
- **并发登录容忍策略设置**：登录到服务器的最大并发请求数。（此设置等同于 XenApp 6.x 版本中的负载限制。）

当所有服务器都达到或高于并发登录容忍设置时，下一个登录请求将分配给待处理登录数最少的服务器。如果有多个服务器满足这些条件，则选择负载指数最低的服务器。

### 交付组中进行电源管理的计算机

只能对虚拟单会话操作系统计算机进行电源管理，不能对物理计算机（包括远程电脑访问计算机）进行电源管理。具有 GPU 功能的单会话操作系统计算机无法挂起，因此关机操作会失败。对于多会话操作系统计算机，可以创建重新启动计划。

在包含池化计算机的交付组中，虚拟单会话操作系统计算机可以处于以下状态之一：

- 随机分配且正在使用
- 未分配且未连接

在包含静态计算机的交付组中，虚拟单会话操作系统计算机可以处于以下状态：

- 永久分配且正在使用
- 永久分配且未连接（但已就绪）
- 未分配且未连接

在正常使用期间，静态交付组通常包含永久分配和未分配的计算机。最初，所有计算机都未分配，除非在创建交付组时手动分配。随着用户连接，计算机将永久分配。您可以对这些交付组中的未分配计算机进行完全电源管理，但只能对永久分配的计算机进行部分管理。

- **池和缓冲区：** 对于池化交付组和具有未分配计算机的静态交付组，池（在此处）是一组处于开机状态的未分配或临时分配的计算机，可供用户连接。用户登录后会立即获得一台计算机。池大小（保持开机状态的计算机数量）可按一天中的时间进行配置。对于静态交付组，请使用 SDK 配置池。

  缓冲区是额外的备用未分配计算机集，当池中的计算机数量低于阈值时，这些计算机将开机。阈值是交付组大小的百分比。对于大型交付组，当超过阈值时，可能会开启大量计算机。因此，请仔细规划交付组大小，或使用 SDK 调整默认缓冲区大小。
- **电源状态计时器：** 您可以使用电源状态计时器在用户断开连接指定时间后暂停计算机。例如，如果用户断开连接至少 10 分钟，则计算机在办公时间之外会自动暂停。

  您可以为工作日和周末以及高峰和非高峰时段配置计时器。
- **永久分配计算机的部分电源管理：** 对于永久分配的计算机，您可以设置电源状态计时器，但不能设置池或缓冲区。计算机在每个高峰期开始时开机，并在每个非高峰期开始时关机。您无法像管理未分配计算机那样对可用计算机的数量进行精细控制，以补偿已使用的计算机。

**电源管理虚拟单会话操作系统计算机**

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后在“操作”窗格中单击“**编辑交付组**”。
3. 在**电源管理**页面上，在**电源管理计算机**中选择**工作日**。默认情况下，工作日为星期一至星期五。
4. 对于随机交付组，在**要开机的计算机**中，单击**编辑**，然后指定工作日期间的池大小。然后，选择要开机的计算机数量。
5. 在**高峰时段**中，设置每天的高峰和非高峰时段。
6. 设置工作日期间高峰和非高峰时段的电源状态计时器：在**高峰时段 > 断开连接时**，指定在暂停交付组中任何断开连接的计算机之前的延迟（以分钟为单位），然后选择**暂停**。在**非高峰时段 > 断开连接时**，指定在关闭交付组中任何已注销的计算机之前的延迟，然后选择**关机**。此计时器不适用于具有随机计算机的交付组。
7. 在**电源管理计算机**中选择**周末**，然后配置周末的高峰时段和电源状态计时器。
8. 单击“**应用**”以应用所做的任何更改并保持窗口打开。或者，单击“**确定**”以应用更改并关闭窗口。

使用 SDK 执行以下操作：

- 在响应电源状态计时器时关闭计算机而不是挂起计算机，或者如果您希望计时器基于注销而不是断开连接。
- 更改默认的工作日和周末定义。
- 禁用电源管理。请参阅 CTX217289。

**对会话已断开连接且正在转换为不同时间段的 VDI 计算机进行电源管理**

> **重要提示：**
>
> 此增强功能仅适用于会话已断开连接的 VDI 计算机。它不适用于会话已注销的 VDI 计算机。
>
> 在早期版本中，VDI 计算机在需要执行操作（断开连接操作=“**挂起**”或“**关机**”）的时间段内转换时，会保持开机状态。如果计算机在不需要执行任何操作（断开连接操作=“**无**”）的时间段（高峰或非高峰时段）内断开连接，则会出现此情况。

从 Citrix Virtual Apps and Desktops™ 7 1909 开始，当指定的断开连接时间到期时，计算机将根据为目标时间段配置的断开连接操作而挂起或关机。

例如，为 VDI 交付组配置以下电源策略：

- 将 `PeakDisconnectAction` 设置为“无”
- 将 `OffPeakDisconnectAction` 设置为“关机”
- 将 `OffPeakDisconnectTimeout` 设置为“10”

有关电源策略中断开连接操作的详细信息，请参阅 `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>` 和 `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`。

在早期版本中，会话在高峰时段断开连接的 VDI 计算机在从高峰时段转换为非高峰时段时仍保持开机状态。从 Citrix Virtual Apps and Desktops 7 1909 开始，`OffPeakDisconnectAction` 和 `OffPeakDisconnectTimeout` 策略操作在时段转换时应用于 VDI 计算机。因此，计算机在转换为非高峰时段 10 分钟后关机。

如果要恢复到以前的行为（即，对从高峰时段转换为非高峰时段或从非高峰时段转换为高峰时段且会话已断开连接的计算机不执行任何操作），请执行以下操作之一：

- 将 `LegacyPeakTransitionDisconnectedBehaviour` 注册表值设置为 `1`，这相当于 *true*，可启用以前的行为。默认情况下，该值为 `0` 或 *false*，这会在时段转换时触发断开连接电源策略操作。
  - 路径：`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - 名称: `LegacyPeakTransitionDisconnectedBehaviour`
  - 类型: `REG_DWORD`
  - 数据: `0x00000001 (1)`
- 使用 `Set-BrokerServiceConfigurationData` PowerShell 命令配置设置。例如：
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

在周期转换时对其应用电源策略操作之前，计算机必须满足以下条件：

- 具有断开连接的会话。
- 没有待处理的电源操作。
- 属于转换到不同时间段的 VDI（单会话）交付组。
- 会话在特定时间段（高峰或非高峰时段）断开连接，并转换到已分配电源操作的时间段。

### 更改目录中处于通电状态的 VDA 百分比

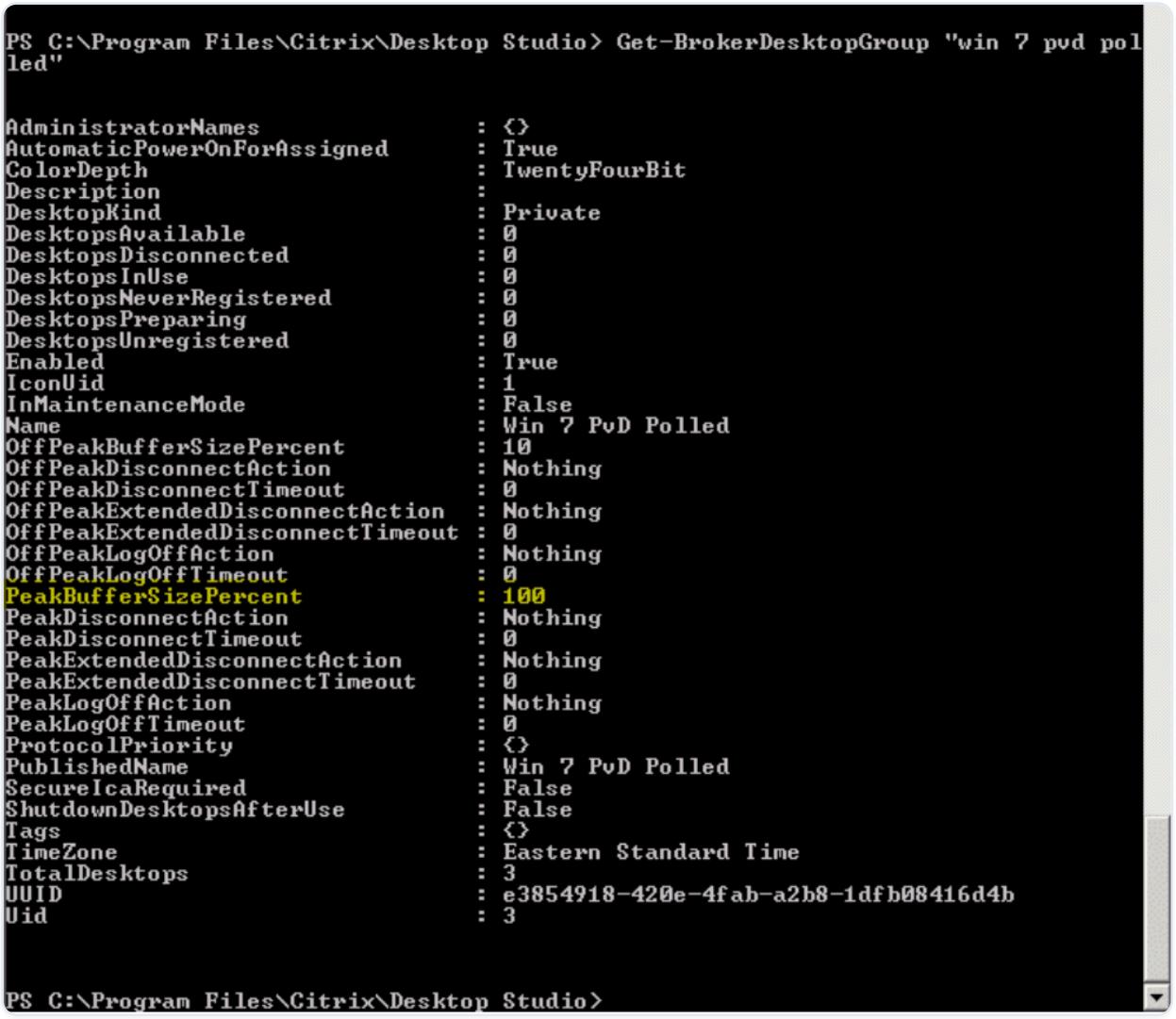
1. 从交付组的**电源管理**部分调整交付组的高峰时段。
2. 记下桌面组名称。
3. 使用管理员权限启动 PowerShell 并运行以下命令。将“Desktop Group Name”替换为已更改 VDA 运行百分比的桌面组的名称。

   ```
   asnp Citrix*
   ```

   ```
   # Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100
   ```

   值为 100 表示 100% 的 VDA 处于就绪状态。
4. 通过运行以下命令验证解决方案：

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```




更改最多可能需要一小时才能生效。

在用户注销后关闭 VDA，请输入：

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

在高峰时段重新启动 VDA，以便在用户注销后它们可供用户使用，请输入：

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

## 会话

- 注销或断开会话，或向用户发送消息
- 配置会话预启动和会话保留
- 控制维护模式下从计算机断开连接时的会话重新连接

### 注销或断开会话

1. 在 Studio 导航窗格中，选择“**交付组**”。
2. 选择一个交付组，然后在“**操作**”窗格中选择“**查看计算机**”。
3. 在中间窗格中，选择计算机，在“**操作**”窗格中选择“**查看会话**”，然后选择一个会话。
   - 或者，在中间窗格中，选择 **会话** 选项卡，然后选择一个会话。
4. 要注销会话，请在“**操作**”窗格中选择“**注销**”。会话关闭，用户注销。除非计算机分配给特定用户，否则它将可供其他用户使用。
5. 要断开会话，请在“**操作**”窗格中选择“**断开连接**”。应用程序在会话中继续运行，并且计算机仍分配给该用户。用户可以重新连接到同一台计算机。

您可以为单会话操作系统计算机配置电源状态计时器，以自动处理未使用的会话。有关详细信息，请参阅电源管理计算机。

### 向交付组发送消息

1. 在 Studio 导航窗格中，选择 **交付组**。
2. 选择一个交付组，然后在 **操作** 窗格中选择 **查看计算机**。
3. 在中间窗格中，选择要向其发送消息的计算机。
4. 在 **操作** 窗格中，选择 **查看会话**。
5. 在中间窗格中，选择所有会话，然后在 **操作** 窗格中选择 **发送消息**。
6. 键入您的消息，然后单击 **确定**。如果需要，可以指定严重性级别。选项包括 **严重**、**问题**、**警告** 和 **信息**。

或者，您可以使用 Citrix Director 发送消息。有关详细信息，请参阅 向用户发送消息。

### 在交付组中配置会话预启动和会话保持

这些功能仅在多会话操作系统计算机上受支持。

会话预启动和会话保持功能通过在请求会话之前启动会话（会话预启动）以及在用户关闭所有应用程序后保持应用程序会话处于活动状态（会话保持），帮助指定用户快速访问应用程序。

默认情况下，不使用会话预启动和会话保持。当用户启动应用程序时，会话会启动，并保持活动状态，直到会话中最后一个打开的应用程序关闭。

注意事项：

- 交付组必须支持应用程序，并且计算机必须运行适用于多会话操作系统的 VDA，最低版本为 7.6。
- 这些功能仅在使用适用于 Windows 的 Citrix Workspace 应用程序时受支持，并且还需要额外的 Citrix Workspace 应用程序配置。有关说明，请在适用于 Windows 的 Citrix Workspace 应用程序版本的产品文档中搜索会话预启动。
- 不支持适用于 HTML5 的 Citrix Workspace 应用程序。
- 使用会话预启动时，如果用户的计算机进入挂起或休眠模式，则预启动不起作用（无论会话预启动设置如何）。用户可以锁定其计算机/会话。但是，如果用户从 Citrix Workspace 应用程序注销，则会话将结束，并且预启动不再适用。
- 使用会话预启动时，物理客户端计算机无法使用挂起或休眠电源管理功能。客户端计算机用户可以锁定其会话，但不应注销。
- 预启动和保持的会话会占用并发许可证，但仅在连接时占用。如果使用用户/设备许可证，则许可证有效期为 90 天。默认情况下，未使用的预启动和保持的会话会在 15 分钟后断开连接。此值可以在 PowerShell 中配置（`New/Set-BrokerSessionPreLaunch` cmdlet）。
- 精心规划和监控用户活动模式对于调整这些功能以使其相互补充至关重要。最佳配置需要在用户更早获得应用程序可用性所带来的好处与保持许可证使用和资源分配的成本之间取得平衡。
- 您还可以在 Citrix Workspace 应用程序中为预定时间配置会话预启动。

#### 未使用的预启动和会话保留会话保持活动状态的时长

有多种方法可以指定如果用户未启动应用程序，未使用的会话保持活动状态的时长：配置的超时和服务器负载阈值。您可以配置所有这些。首先发生的事件会导致未使用的会话结束。

- **超时：** 配置的超时指定未使用的预启动或会话保留会话保持活动状态的分钟数、小时数或天数。如果配置的超时时间过短，预启动会话将在为用户提供更快应用程序访问的优势之前结束。如果配置的超时时间过长，则传入的用户连接可能会被拒绝，因为服务器没有足够的资源。

您只能通过 SDK 启用此超时 (`New/Set-BrokerSessionPreLaunch` cmdlet)，而不能通过管理控制台启用。如果禁用超时，则它不会显示在该交付组的控制台显示中或“**编辑交付组**”页面中。

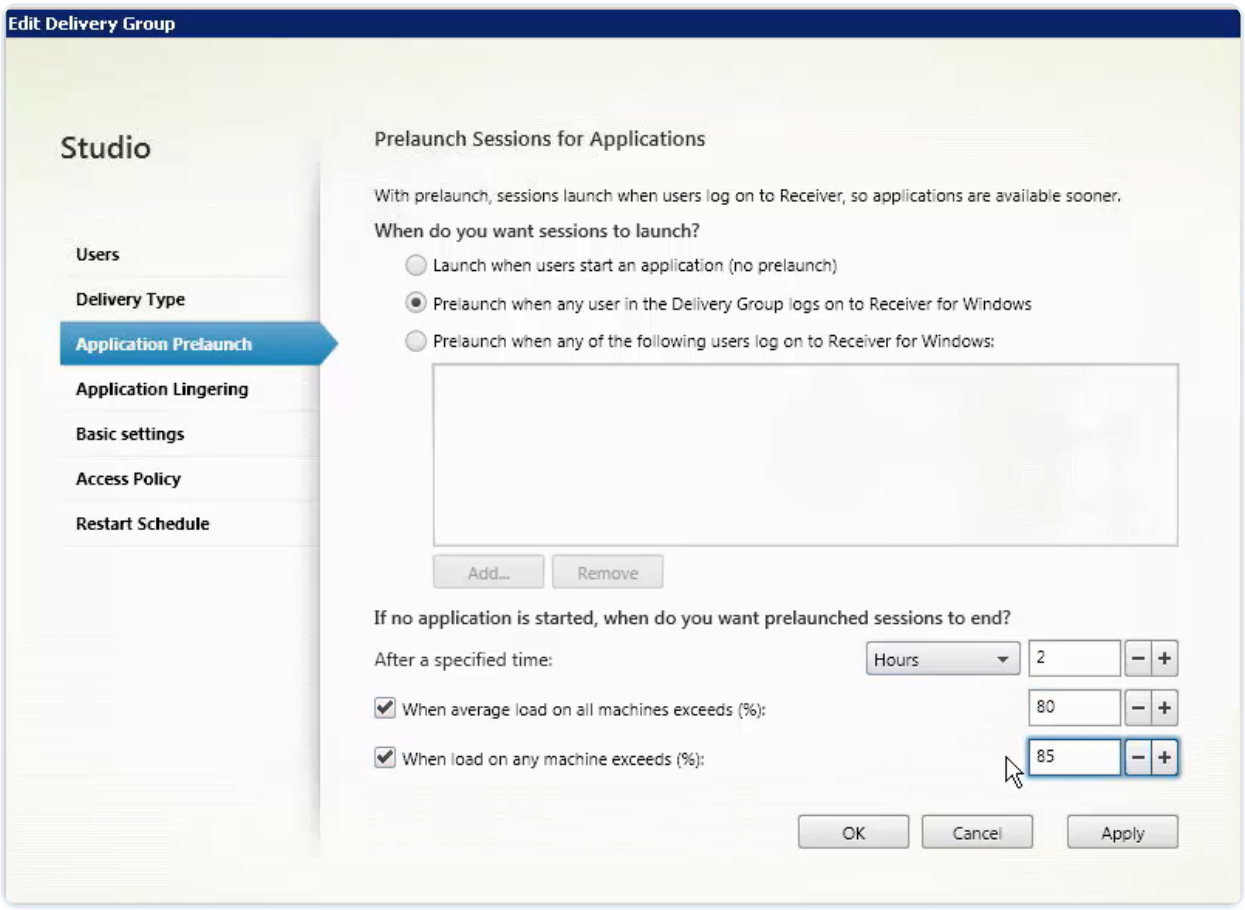
- **阈值：** 根据服务器负载自动结束预启动和会话保留会话可确保会话尽可能长时间保持打开状态，前提是服务器资源可用。未使用的预启动和会话保留会话不会导致连接被拒绝，因为当新用户会话需要资源时，它们会自动结束。

  您可以配置两个阈值：交付组中所有服务器的平均负载百分比，以及组中单个服务器的最大负载百分比。当超过阈值时，处于预启动或会话保留状态时间最长的会话将结束。会话将以分钟为间隔逐个结束，直到负载降至阈值以下。当超过阈值时，不会启动新的预启动会话。

未向 Controller 注册 VDA 的服务器以及处于维护模式的服务器被视为已满载。计划外中断会导致预启动和会话保留会话自动结束以释放容量。

### 启用会话预启动

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后在操作窗格中单击 **编辑交付组**。
3. 在**应用程序预启动**页面上，通过选择会话启动时间来启用会话预启动：
   - 当用户启动应用程序时。这是默认设置。会话预启动已禁用。
   - 当交付组中的任何用户登录到适用于 Windows 的 Citrix Workspace 应用程序时。
   - 当用户和用户组列表中的任何人登录到适用于 Windows 的 Citrix Workspace 应用程序时。如果选择此选项，请务必同时指定用户或用户组。



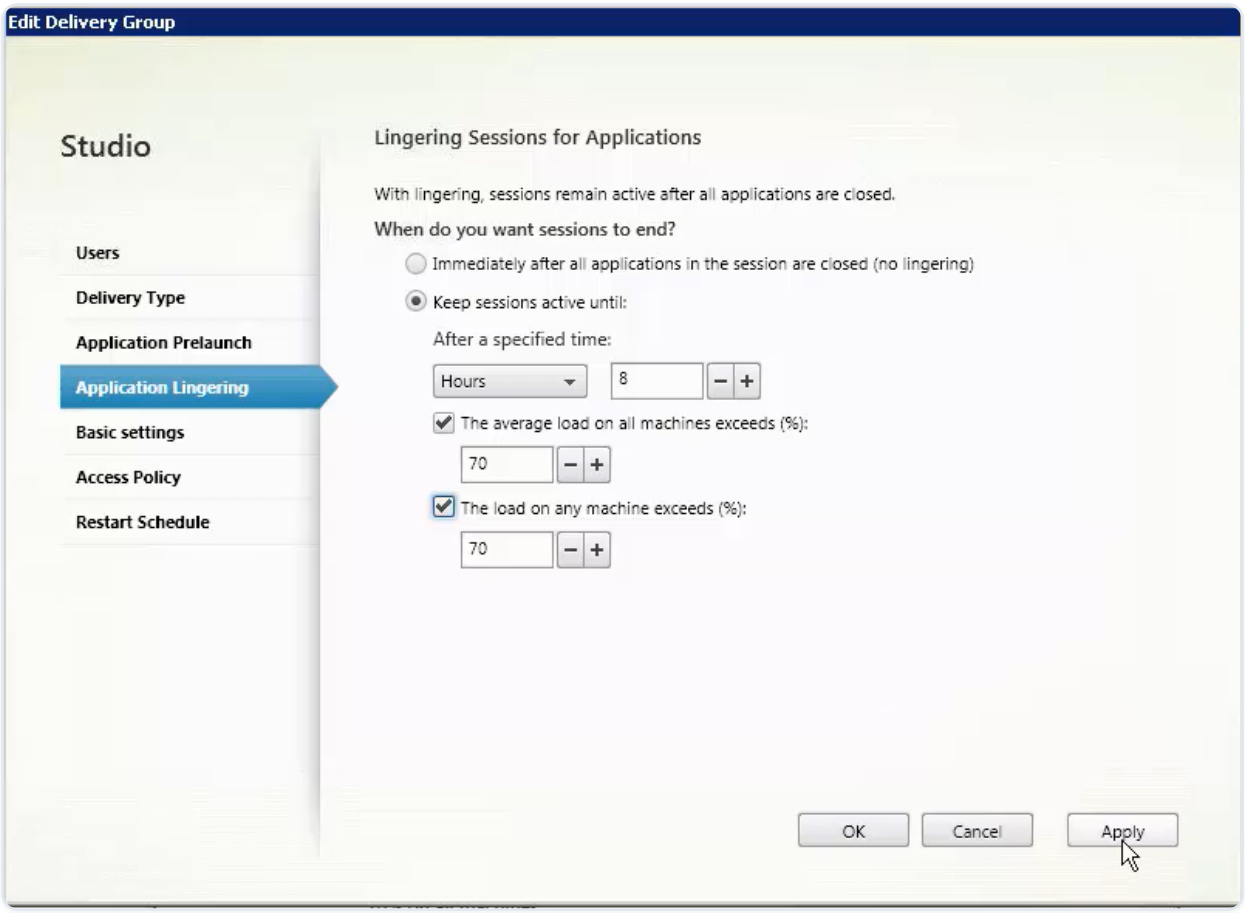

4. 当用户启动应用程序时，预启动会话将替换为常规会话。如果用户未启动应用程序（预启动会话未使用），则以下设置会影响该会话保持活动状态的时间。

   - 当指定的时间间隔过去时。您可以更改时间间隔（1-99 天、1-2376 小时或 1-142,560 分钟）。
   - 当交付组中所有计算机的平均负载超过指定百分比（1-99%）时。
   - 当交付组中任何计算机的负载超过指定百分比（1-99%）时。

   总结：预启动会话将保持活动状态，直到发生以下事件之一：用户启动应用程序、指定时间过去或超过指定的负载阈值。

### 启用会话延迟

1. 在导航窗格中选择 **交付组**。
2. 选择一个组，然后在操作窗格中单击 **编辑交付组**。
3. 在**应用程序延迟**页面上，通过选择**保持会话活动直到**来启用会话延迟。




4. 如果用户未启动其他应用程序，则有多个设置会影响滞留会话保持活动状态的时长。

   - 当指定的时间间隔过去时。您可以更改时间间隔：1–99 天、1–2376 小时或 1–142,560 分钟。
   - 当交付组中所有计算机的平均负载超过指定百分比时：1–99%。
   - 当交付组中任何计算机的负载超过指定百分比时：1–99%。

   总结：滞留会话保持活动状态，直到发生以下事件之一：用户启动应用程序、指定时间过去或超过指定负载阈值。

### 控制维护模式下从计算机断开连接时的会话重新连接

> **注意：**
>
> 此功能仅在 PowerShell 中可用。

您可以控制在维护模式下从计算机断开连接的会话是否允许重新连接到交付组中的计算机。

在版本 2106 之前，不允许重新连接已从维护模式下的计算机断开连接的单会话池桌面会话。从版本 2106 开始，您可以配置交付组以允许或禁止在从维护模式下的计算机断开连接后重新连接（无论会话类型如何）。

创建或编辑交付组时（`New-BrokerDesktopGroup`，`Set-BrokerDesktopGroup`），使用 `-AllowReconnectInMaintenanceMode <boolean>` 参数来允许或禁止从维护模式下的计算机断开连接的计算机重新连接。

- 当设置为 true 时，会话可以重新连接到组中的计算机。
- 当设置为 false 时，会话无法重新连接到组中的计算机。

默认值：

- 单会话：已禁用
- 多会话：已启用

## 故障排除

- 未向 Delivery Controller 注册的 VDA 在启动代理会话时不会被考虑。这会导致原本可用的资源未得到充分利用。VDA 未注册的原因有很多，其中许多管理员都可以进行故障排除。详细信息显示在目录创建向导中以及将目录添加到交付组后提供故障排除信息。

  创建交付组后，交付组的详细信息窗格会指示可以注册但未注册的计算机数量。例如，一台或多台计算机已开机且未处于维护模式，但当前未向控制器注册。查看“未注册但应注册”的计算机时，请查看详细信息窗格中的 **故障排除** 选项卡，以了解可能的原因和建议的纠正措施。

  有关功能级别消息，请参阅VDA 版本和功能级别。

  有关 VDA 注册故障排除的信息，请参阅CTX136668。
- 在交付组的显示中，详细信息窗格中的 **已安装的 VDA 版本** 可能与计算机上安装的实际版本不同。计算机的 Windows 程序和功能显示屏会显示实际的 VDA 版本。
- 对于状态为 **电源状态未知** 的计算机，请参阅 CTX131267 以获取指导。

# 创建应用程序组

## 简介

应用程序组允许您管理应用程序集合。为跨不同交付组共享的应用程序创建应用程序组。或者，为交付组中由部分用户使用的应用程序创建应用程序组。应用程序组是可选的；它们提供了一种替代

方法，无需将相同的应用程序添加到多个交付组。将交付组与多个应用程序组关联，并将应用程序组与多个交付组关联。

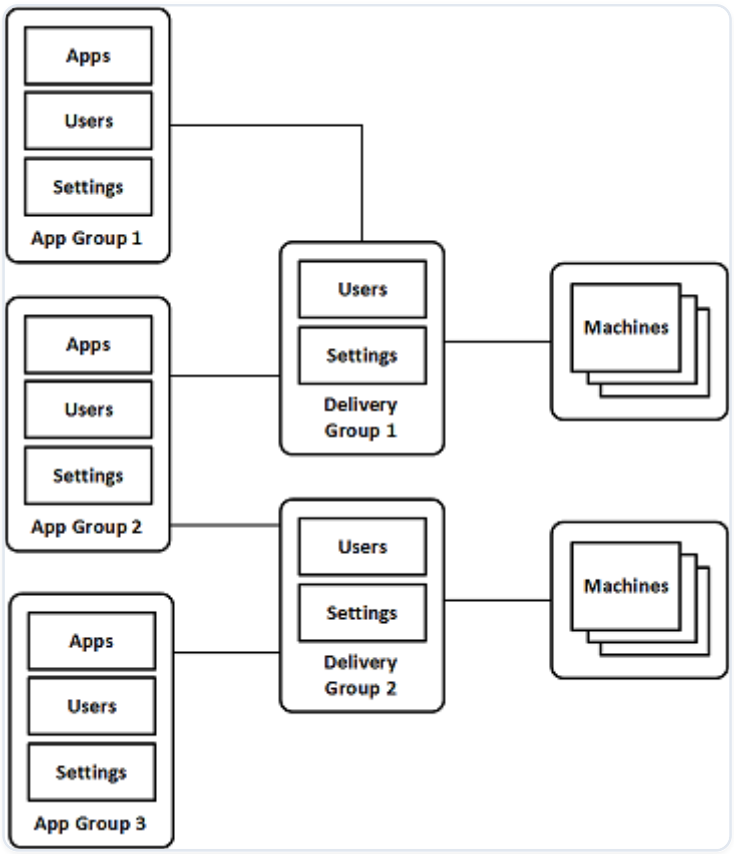
与使用更多交付组相比，使用应用程序组可以在应用程序管理和资源控制方面提供优势：

- 应用程序及其设置的逻辑分组使您可以将这些应用程序作为一个单元进行管理。例如，您不必一次一个地将相同的应用程序添加到各个交付组。
- 应用程序组之间的会话共享可以节省资源消耗。在其他情况下，禁用应用程序组之间的会话共享可能是有益的。
- 您可以使用标记限制功能从应用程序组发布应用程序，仅考虑所选交付组中的一部分计算机。通过标记限制，您可以将现有计算机用于多个发布任务，从而节省部署和管理额外计算机的成本。标记限制可以看作是对交付组中的计算机进行细分（或分区）。在使用标记限制的应用程序组或桌面时，有助于隔离和排查交付组中的一部分计算机。

## 示例配置

**示例 1：**

下图显示了包含应用程序组的 Citrix Virtual Apps and Desktops™ 部署：



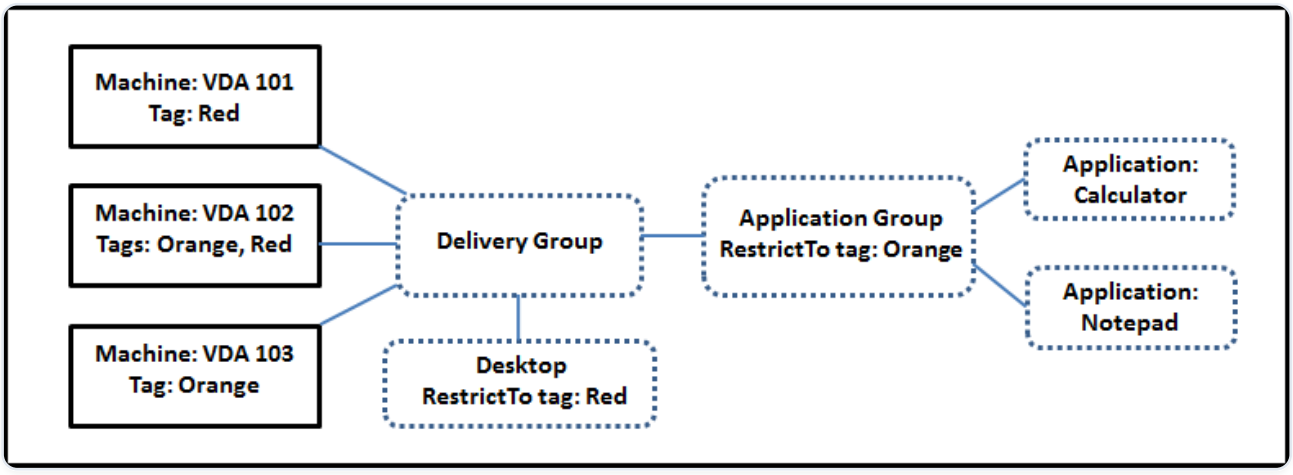

在此配置中，应用程序被添加到应用程序组，而不是交付组。交付组指定使用哪些计算机。（尽管未显示，但这些计算机位于计算机目录中。）

应用程序组 1 与交付组 1 关联。应用程序组 1 中的应用程序由应用程序组 1 中指定的用户访问。这些组仅在它们也位于交付组 1 的用户列表中时才显示。此配置遵循以下指导原则：应用程序组的用户列表是关联交付组用户列表的子集（一种限制）。应用程序组 1 中的设置（例如应用程序组之间的应用程序会话共享、关联的交付组）适用于该组中的应用程序和用户。交付组 1 中的设置适用于应用程序组 1 和 2 中的用户，因为这些应用程序组已与该交付组关联。

应用程序组 2 与两个交付组（1 和 2）关联。这些交付组中的每一个都在应用程序组 2 中分配了一个优先级，指示在启动应用程序时检查交付组的顺序。优先级相同的交付组会进行负载平衡。应用程序组 2 中的应用程序由应用程序组 2 中指定的用户访问。但是，他们还必须出现在交付组 1 和交付组 2 的用户列表中。

**示例 2：**

此简单布局使用标记限制来限制哪些计算机被考虑用于某些桌面和应用程序启动。该站点有一个共享交付组、一个已发布的桌面和一个配置了两个应用程序的应用程序组。




已将标记添加到三台计算机（VDA 101–103）中的每一台。

应用程序组是使用“Orange”标记限制创建的。它的每个应用程序都只在该交付组中具有“Orange”标记的计算机（VDA 102 和 103）上启动。

有关在应用程序组（以及桌面）中使用标签限制的更全面的示例和指导，请参阅标签。

## 指导和注意事项

Citrix® 建议将应用程序添加到应用程序组或交付组，但不要同时添加到两者。否则，在两种组类型中都包含应用程序会增加复杂性，从而使其更难管理。

默认情况下，应用程序组处于启用状态。创建应用程序组后，您可以编辑该组以更改此设置。请参阅管理应用程序组。

默认情况下，应用程序组之间的应用程序会话共享处于启用状态。请参阅应用程序组之间的会话共享。

Citrix 建议将交付组升级到当前版本。此过程需要：

1. 升级交付组中使用的计算机上的 VDA。
2. 升级包含这些计算机的计算机目录。
3. 升级交付组。

有关详细信息，请参阅管理交付组。

要使用应用程序组，您的核心组件最低版本必须为 7.9。

创建应用程序组需要交付组管理员内置角色的委派管理权限。有关详细信息，请参阅委派管理。

本文指的是将应用程序“关联”到多个应用程序组。它将此操作与从可用源添加该应用程序的实例区分开来。同样，交付组与应用程序组关联，而不是彼此的添加项或组件。

## 与应用程序组的会话共享

启用应用程序会话共享后，所有应用程序都在同一应用程序会话中启动。这节省了启动更多应用程序会话的成本，并允许使用涉及剪贴板的应用程序功能，例如复制粘贴操作。但是，在某些情况下，您可以清除会话共享。

使用应用程序组时，您可以通过以下三种方式配置应用程序会话共享，这些方式扩展了仅使用交付组时可用的标准会话共享行为：

- 应用程序组之间启用会话共享。
- 仅在同一应用程序组中的应用程序之间启用会话共享。
- 会话共享已禁用。

### 应用程序组之间的会话共享

您可以在应用程序组之间启用应用程序会话共享，也可以禁用它，将应用程序会话共享仅限于同一应用程序组中的应用程序。

- **启用应用程序组之间会话共享的有用示例：**

  应用程序组 1 包含 Microsoft Office 应用程序，例如 Word 和 Excel。应用程序组 2 包含其他应用程序，例如记事本和计算器，并且这两个应用程序组都附加到同一个交付组。有权访问这两个应用程序组的用户通过启动 Word 来启动应用程序会话，然后启动记事本。如果控制器发现用户运行 Word 的现有会话适合运行记事本，则记事本将在现有会话中启动。如果记事本无法从现有

会话中运行（例如，如果标记限制排除了会话正在运行的计算机），则会在合适的计算机上创建新会话，而不是使用会话共享。

- **禁用应用程序组之间会话共享的有用示例：**

  一种配置，其中包含一组与安装在同一计算机上的其他应用程序无法很好地互操作的应用程序。例如，同一软件套件的两个不同版本或同一 Web 浏览器的两个不同版本。您不希望允许用户在同一会话中启动这两个版本。

  为软件套件的每个版本创建一个应用程序组，并将软件套件每个版本的应用程序添加到相应的应用程序组。如果这些应用程序组中的每个组都禁用了组间会话共享，则这些组中指定的用户可以在同一会话中运行相同版本的应用程序。用户仍然可以同时运行其他应用程序，但不能在同一会话中运行。当启动其中一个不同版本的应用程序，或任何不包含在应用程序组中的应用程序时，该应用程序将在新会话中启动。

此应用程序组之间的会话共享功能不是安全沙盒功能。它并非万无一失，也无法阻止用户通过其他方式（例如，通过 Windows 资源管理器）在其会话中启动应用程序。

如果计算机已达到容量，则不会在其上启动新会话。新应用程序会根据需要使用会话共享在计算机上的现有会话中启动。

您只能将预启动会话提供给允许应用程序会话共享的应用程序组。（使用会话延迟功能的会话可用于所有应用程序组。）这些功能必须在与应用程序组关联的每个交付组中启用和配置。您无法在应用程序组中配置它们。

默认情况下，在创建应用程序组时，应用程序组之间的应用程序会话共享处于启用状态。创建组时无法更改此设置。创建应用程序组后，您可以编辑该组以更改此设置。请参阅管理应用程序组。

### 禁用应用程序组内的会话共享

您可以阻止同一应用程序组中的应用程序之间进行应用程序会话共享。

- **禁用应用程序组内的会话共享有帮助的示例：**

  您希望用户在单独的显示器上访问应用程序的多个同时全屏会话。

  您创建一个应用程序组并将应用程序添加到其中。

默认情况下，创建应用程序组时会启用应用程序会话共享。创建组时无法更改此设置。创建应用程序组后，您可以编辑该组以更改此设置。请参阅管理应用程序组。

## 创建应用程序组

要创建应用程序组，请执行以下操作：

1. 在 Studio 导航窗格中选择 **应用程序**，然后在“操作”窗格中选择 **创建应用程序组**。
2. 向导将启动并显示“**简介**”页面，您可以选择在以后启动此向导时不再显示此页面。
3. 向导将引导您完成以下部分中描述的页面。完成每个页面后，单击“**下一步**”，直到到达“摘要”页面。

### 步骤 1. 交付组

“**交付组**”页面列出了所有交付组，以及每个组包含的计算机数量。

- “**兼容的交付组**”列表包含您可以选择的交付组。兼容的交付组包含随机（非永久或静态分配）多会话或单会话操作系统计算机。
- “**不兼容的交付组**”列表包含您无法选择的交付组。每个条目都解释了其不兼容的原因，例如包含静态分配的计算机。

应用程序组可以与包含可交付应用程序的共享（非专用）计算机的交付组关联。

如果满足以下两个条件，您还可以选择包含仅交付桌面的共享计算机的交付组：

- 交付组包含共享计算机，并且是使用早于 7.9 版本的 XenDesktop 创建的。
- 您具有“编辑交付组”权限。

提交应用程序组创建向导时，交付组类型会自动转换为“桌面和应用程序”。

尽管您可以创建不带关联交付组的应用程序组（可能用于组织应用程序或用作当前未使用的应用程序的存储），但应用程序组必须指定至少一个交付组才能用于交付应用程序。此外，如果未指定交付组，则无法从“**从‘开始’菜单**”源向应用程序组添加应用程序。

您选择的交付组指定用于交付应用程序的计算机。选中要与应用程序组关联的交付组旁边的复选框。

要添加标记限制，请选择“**将启动限制到具有该标记的计算机**”，然后从下拉列表中选择该标记。

### 步骤 2. 用户

在应用程序组中指定应用程序用户。可以允许上一页中选择的交付组中的所有用户和用户组，也可以从这些交付组中选择特定的用户和用户组。如果将使用限制为指定用户，则只有在交付组中指定的那些用户（即应用程序组）才能访问此组中的应用程序。本质上，应用程序组中的用户列表对交付组中的用户列表提供了筛选。

启用或禁用未经身份验证的用户使用应用程序仅在交付组中可用，而不在应用程序组中可用。

有关部署中指定用户列表的位置的信息，请参阅 指定用户列表的位置。

### 步骤 3. 应用程序

须知：

- 默认情况下，您添加的新应用程序将放置在名为“**应用程序**”的文件夹中。您可以指定其他文件夹。如果您尝试添加应用程序，并且该文件夹中已存在同名应用程序，系统会提示您重命名要添加的应用程序。如果您同意建议的唯一名称，则应用程序将以该新名称添加。否则，您必须自行重命名才能添加。有关详细信息，请参阅管理应用程序文件夹。
- 您可以在添加应用程序时或之后更改其属性（设置）。请参阅更改应用程序属性。如果您向同一用户发布两个同名应用程序，请在 Studio 中更改“**应用程序名称（面向用户）**”属性。否则，用户将在 Citrix Workspace 应用程序中看到重复的名称。
- 当您将应用程序添加到多个应用程序组时，如果您没有足够的权限在所有这些组中查看该应用程序，则可能会出现可见性问题。在这种情况下，请咨询具有更高权限的管理员，或者扩展您的范围以包括添加了该应用程序的所有组。

单击下拉菜单中的“**添加**”以显示应用程序源。

- **从“开始”菜单：** 在所选交付组中的计算机上发现的应用程序。选择此源时，将启动一个新页面，其中包含发现的应用程序列表。选中要添加的应用程序的复选框，然后单击“**确定**”。

  如果选择了以下任何一项，则无法选择此源：

  - 没有关联交付组的应用程序组。
  - 关联交付组中不包含任何计算机的应用程序组。
  - 不包含任何计算机的交付组。

- **手动定义：** 位于站点或网络中其他位置的应用程序。选择此源时，将启动一个新页面，您可以在其中键入可执行文件的路径、工作目录、可选命令行参数以及管理员和用户的显示名称。输入此信息后，单击“**确定**”。
- **现有：** 以前添加到站点的应用程序。选择此源时，将启动一个新页面，其中包含发现的应用程序列表。选中要添加的应用程序的复选框，然后单击“**确定**”。如果站点没有应用程序，则无法选择此源。
- **App-V**：App-V 软件包中的应用程序。选择此源时，将启动一个新页面，您可以在其中选择 **App-V 服务器**或**应用程序库**。在结果显示中，选中要添加的应用程序的复选框，然后单击“**确定**”。有关详细信息，请参阅 App-V。如果未为站点配置 App-V，则无法选择此源（或可能不显示）。

如前所述，如果不存在该类型的有效源，则“**添加**”下拉菜单中的某些条目将不可选。不兼容的源根本不会列出（例如，您不能将应用程序组添加到应用程序组，因此在创建应用程序组时不会列出该源）。

### 步骤 4. 作用域

此页面仅在您之前创建了自定义作用域时显示。默认情况下，将选择**所有**作用域。有关详细信息，请参阅委派管理。

### 步骤 5. 摘要

输入应用程序组的名称。您还可以（可选）输入描述。

查看摘要信息，然后单击**完成**。

# 管理应用程序组

## 简介

本文介绍如何管理您创建的应用程序组。

有关在应用程序组或交付组中管理应用程序的信息，包括如何执行以下操作，请参阅应用程序：

- 在应用程序组中添加或删除应用程序。
- 更改应用程序组关联。

管理应用程序组需要交付组管理员内置角色的委派管理权限。有关详细信息，请参阅委派管理。

## 启用或禁用应用程序组

启用应用程序组后，它可以交付已添加到其中的应用程序。禁用应用程序组会禁用该组中的每个应用程序。但是，如果这些应用程序也与其他已启用的应用程序组关联，则可以从其他组交付这些应用程序。如果应用程序已明确添加到与应用程序组关联的交付组，则禁用应用程序组不会影响这些交付组中的应用程序。

创建应用程序组时，该组处于启用状态。创建组时无法更改此配置。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**编辑应用程序组**。
3. 在**设置**页面上，选中或清除**启用应用程序组**复选框。
4. 单击**应用**以保持窗口打开，或单击**确定**以应用更改并关闭窗口。

## 启用或禁用应用程序组之间的应用程序会话共享

应用程序组之间的会话共享在创建应用程序组时启用。创建组时无法更改此配置。有关详细信息，请参阅与应用程序组共享会话。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**编辑应用程序组**。
3. 在 **设置** 页面上，选中或清除 **启用应用程序组之间的应用程序会话共享** 复选框。
4. 单击**应用**以保持窗口打开，或单击**确定**以应用更改并关闭窗口。

## 禁用应用程序组内的应用程序会话共享

在创建应用程序组时，同一应用程序组中应用程序之间的会话共享默认启用。如果禁用应用程序组之间的应用程序会话共享，则同一应用程序组中应用程序之间的会话共享仍保持启用状态。

您可以使用 PowerShell SDK 配置应用程序组，使其包含的应用程序之间禁用应用程序会话共享。在某些情况下，此选项是可取的。例如，您可能希望用户在单独的显示器上以全尺寸应用程序窗口启动非无缝应用程序。

当您禁用应用程序组内的应用程序会话共享时，该组中的每个应用程序都会在新应用程序会话中启动。如果有正在运行相同应用程序的合适断开连接会话可用，则会重新连接该会话。例如，当启动记事本时，如果存在一个正在运行记事本的断开连接会话，则会重新连接该会话，而不是创建一个新会话。当有多个合适的断开连接会话可用时，会以随机但确定性的方式选择其中一个会话进行重新连接。当在相同情况下再次发生此情况时，会选择相同的会话，但除此之外，该会话不一定可预测。

使用 PowerShell SDK 禁用现有应用程序组中所有应用程序的应用程序会话共享，或创建禁用应用程序会话共享的组。

### PowerShell cmdlet 示例

要禁用会话共享，请使用 Broker PowerShell cmdlet `New-BrokerApplicationGroup` 或 `Set-BrokerApplicationGroup`，并将参数 `SessionSharingEnabled` 设置为 `False`，将参数 `SingleAppPerSession` 设置为 `True`。

- 例如，要创建一个应用程序组，其中禁用该组中所有应用程序的应用程序会话共享：

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

- 例如，要禁用现有应用程序组中所有应用程序之间的应用程序会话共享：

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

### 注意事项

- 要启用 `SingleAppPerSession` 属性，您必须将 `SessionSharingEnabled` 属性设置为 False。这两个属性不能同时启用。`SessionSharingEnabled` 参数指的是应用程序组之间的会话共享。
- 应用程序会话共享仅适用于与应用程序组关联但未与交付组关联的应用程序。所有直接与交付组关联的应用程序默认共享会话。
- 如果一个应用程序分配给多个应用程序组，请确保这些组没有冲突的设置。例如，一个组的选项设置为 `True`，而另一个组的选项设置为 `False` 会导致不可预测的行为。

## 重命名应用程序组

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**重命名应用程序组**。
3. 指定新的唯一名称，然后单击**确定**。

## 添加、删除或更改交付组与应用程序组关联的优先级

应用程序组可以与包含可交付应用程序的共享（非专用）计算机的交付组关联。

如果满足以下两个条件，您还可以选择包含仅交付桌面的共享计算机的交付组：

- 交付组包含共享计算机，并且是使用早于 7.9 的版本创建的。
- 您具有“编辑交付组”权限。

提交**编辑应用程序组**对话框时，交付组类型会自动转换为“桌面和应用程序”。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**编辑应用程序组**。
3. 选择**交付组**页面。
4. 要添加交付组，请单击**添加**。选中可用交付组的复选框。（无法选择不兼容的交付组。）完成选择后，单击**确定**。
5. 要删除交付组，请选中要删除的组的复选框，然后单击**删除**。出现提示时确认删除。
6. 要更改交付组的优先级，请选中交付组的复选框，然后单击**编辑优先级**。输入优先级（0 = 最高），然后单击**确定**。
7. 点击“**应用**”以应用您所做的任何更改并保持窗口打开，或点击“**确定**”以应用更改并关闭窗口。

## 在应用程序组中添加、更改或删除标记限制

添加、更改和删除标记限制可能会对哪些计算机被考虑用于启动应用程序产生意想不到的影响。请查看 标记 中的注意事项和警告。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**编辑应用程序组**。
3. 选择“**交付组**”页面。
4. 要添加标记限制，请选择“**将启动限制到具有此标记的计算机**”，然后从下拉列表中选择标记。
5. 要更改或删除标记限制，请选择其他标记，或通过清除“**将启动限制到具有此标记的计算机**”来完全删除标记限制。
6. 点击“**应用**”以应用您所做的任何更改并保持窗口打开，或点击“**确定**”以应用更改并关闭窗口。

## 在应用程序组中添加或删除用户

有关用户的详细信息，请参阅 创建应用程序组。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**编辑应用程序组**。
3. 选择“**用户**”页面。指明是允许关联交付组中的所有用户使用应用程序组中的应用程序，还是只允许特定用户和组使用。要添加用户，请点击“**添加**”，然后指定要添加的用户。要删除用户，请选择一个或多个用户，然后点击“**删除**”。
4. 点击“**应用**”以应用您所做的任何更改并保持窗口打开，或点击“**确定**”以应用更改并关闭窗口。

## 更改应用程序组中的作用域

只有在您创建了作用域后才能更改作用域（您无法编辑“所有”作用域）。有关详细信息，请参阅委派管理。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**编辑应用程序组**。
3. 选择**作用域**页面。选中或清除作用域旁边的复选框。
4. 点击“**应用**”以应用您所做的任何更改并保持窗口打开，或点击“**确定**”以应用更改并关闭窗口。

## 删除应用程序组

应用程序必须至少与一个交付组或应用程序组关联。如果删除应用程序组导致一个或多个应用程序不再属于任何组，系统会警告您删除该组也会删除这些应用程序。然后您可以确认或取消删除。

删除应用程序不会从其原始源中删除它。但是，如果您想再次使其可用，则必须再次添加它。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**删除组**。
3. 出现提示时确认删除。

# 远程电脑访问

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

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

此功能包含类型为 **远程电脑访问** 的计算机目录，该目录提供以下功能：

- 能够通过指定组织单位 (OU) 添加计算机。此功能有助于批量添加电脑。
- 基于登录到办公室 Windows PC 的用户进行自动用户分配。我们支持单用户和多用户分配。

Citrix Virtual Apps and Desktops 可以通过使用其他类型的计算机目录来适应物理电脑的更多用例。这些用例包括：

- 物理 Linux 电脑
- 池化物理电脑（即随机分配，而非专用）

> **注意：**
>
> 有关支持的操作系统版本的详细信息，请参阅 单会话操作系统 和 Linux VDA 的 VDA 系统要求。

> 对于本地部署，远程电脑访问仅对 Citrix Virtual Apps and Desktops Advanced 或 Premium 许可证有效。会话消耗许可证的方式与其他 Citrix Virtual Desktops™ 会话相同。对于 Citrix

> Cloud，远程电脑访问对 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）和 Workspace Premium Plus 有效。

## 注意事项

虽然适用于 Citrix Virtual Apps and Desktops 的所有技术要求和注意事项通常也适用于远程电脑访问，但有些可能与物理 PC 用例更相关或专属于物理 PC 用例。

> **重要提示：**

> Windows 11 物理系统（以及一些运行 Windows 10 的系统）包含基于虚拟化的安全功能，导致 VDA 软件错误地将其检测为虚拟机。为缓解此问题，您有以下选项：

> - 在 VDA 命令行安装中，将“/physicalmachine”选项与“/remotepc”选项一起使用
> - 如果在 VDA 安装后未曾使用上述选项，请添加以下注册表值 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>   - 名称: ForceEnableRemotePC
>   - 类型: DWORD
>   - 数据: 1

## 部署注意事项

在规划远程电脑访问的部署时，需要做出一些一般性决定。

- 您可以将远程电脑访问添加到现有 Citrix Virtual Apps and Desktops 部署中。在选择此选项之前，请考虑以下事项：
  - 当前的 Delivery Controller 或 Cloud Connector 的大小是否合适，以支持与远程电脑访问 VDA 相关的额外负载？
  - 本地站点数据库和数据库服务器的大小是否合适，以支持与远程电脑访问 VDA 相关的额外负载？
  - 现有 VDA 和新的远程电脑访问 VDA 是否会超过每个站点支持的最大 VDA 数量？
- 您必须通过自动化过程将 VDA 部署到办公电脑。以下是可用选项：
  - 电子软件分发 (ESD) 工具（例如 SCCM）：使用 SCCM 安装 VDA。

  - 部署脚本：使用脚本安装 VDA。

- 查看远程电脑访问安全注意事项。

## 计算机目录注意事项

所需的计算机目录类型取决于用例：

- 远程电脑访问计算机目录
  - Windows 专用电脑
  - Windows 专用多用户电脑。此用例适用于多个用户可以在不同班次远程访问的物理办公电脑。
  - 池化 Windows 电脑。此用例适用于多个随机用户可以访问的物理电脑，例如计算机实验室。
- 单会话 OS 计算机目录
  - 静态 - 专用 Linux 电脑
  - 随机 - 池化 Linux PC

确定计算机目录类型后，请考虑以下事项：

- 一台计算机一次只能分配给一个计算机目录。
- 为了方便委派管理，请考虑根据地理位置、部门或任何其他分组创建计算机目录，以便于将每个目录的管理委派给相应的管理员。
- 在选择计算机帐户所在的 OU 时，请选择较低级别的 OU 以获得更高的粒度。如果不需要这种粒度，可以选择较高级别的 OU。例如，在 Bank/Officers/Tellers 的情况下，选择 **Tellers** 以获得更高的粒度。否则，您可以根据需要选择 **Officers** 或 **Bank**。
- 将 OU 分配给远程电脑访问计算机目录后，移动或删除 OU 会影响 VDA 关联并导致未来分配出现问题。因此，请务必进行相应规划，以便在 Active Directory 更改计划中考虑计算机目录的 OU 分配更新。
- 如果由于 OU 结构的原因，选择 OU 将计算机添加到计算机目录不方便，则无需选择任何 OU。您可以在之后使用 PowerShell 将计算机添加到目录。如果桌面分配在交付组中配置正确，则用户自动分配将继续有效。一个用于将计算机和用户分配添加到计算机目录的示例脚本可在 GitHub 中找到。
- 集成的局域网唤醒功能仅适用于 **Remote PC Access** 类型的计算机目录。

## Linux VDA 注意事项

以下注意事项特定于 Linux VDA：

- 仅在非 3D 模式下在物理机上使用 Linux VDA。由于 NVIDIA 驱动程序的限制，当启用 HDX™ 3D 模式时，电脑的本地屏幕无法黑屏，并会显示会话活动。显示此屏幕存在安全风险。
- 对物理 Linux 计算机使用单会话操作系统类型的计算机目录。
- Linux 计算机不支持自动用户分配。
- 如果用户已在本地登录其 PC，则从 StoreFront™ 启动 PC 的尝试将失败。
- Linux 计算机不支持电源节省选项。

## 技术要求和注意事项

本节包含物理 PC 的技术要求和注意事项。

- 不支持以下各项：
  - KVM 切换器或其他可能断开会话的组件。
  - 混合型 PC，包括一体机和 NVIDIA Optimus 笔记本电脑及 PC。
  - 双启动计算机。
- 将键盘和鼠标直接连接到 PC。连接到显示器或其他可能关闭或断开连接的组件，可能会导致这些外围设备不可用。如果必须将输入设备连接到显示器等组件，请勿关闭这些组件。
- PC 必须加入 Active Directory 域服务域。
- 安全启动仅在 Windows 10 和 Windows 11 上受支持。
- PC 必须具有活动的网络连接。有线连接更可靠，带宽更高，因此是首选。
- 如果使用 Wi-Fi，请执行以下操作：
  a. 将电源设置配置为保持无线适配器开启。
  b. 配置无线适配器和网络配置文件，以允许在用户登录前自动连接到无线网络。否则，VDA 不会注册，直到用户登录。在用户登录之前，PC 无法用于远程访问。
  c. 确保可以从 Wi-Fi 网络访问 Delivery Controller 或 Cloud Connector。
- 您可以在笔记本电脑上使用远程电脑访问。请确保笔记本电脑连接到电源，而不是使用电池运行。将笔记本电脑的电源选项配置为与台式电脑的选项匹配。例如：
  a. 禁用休眠功能。
  b. 禁用睡眠功能。

c. 将合盖操作设置为 **不执行任何操作**。

d. 将“按下电源按钮”操作设置为 **关机**。

e. 禁用显卡和网卡节能功能。

- 远程电脑访问支持运行 Windows 10 的 Surface Pro 设备。请遵循前面提到的笔记本电脑相同准则。
- 如果使用扩展坞，可以对笔记本电脑进行取消坞接和重新坞接操作。当您取消坞接笔记本电脑时，VDA 会通过 Wi-Fi 重新向 Delivery Controller 或 Cloud Connector 注册。但是，当您重新坞接笔记本电脑时，除非您断开无线适配器，否则 VDA 不会切换到使用有线连接。某些设备提供内置功能，可在建立有线连接时断开无线适配器。其他设备需要自定义解决方案或第三方实用程序来断开无线适配器。请查看前面提到的 Wi-Fi 注意事项。

  要为远程电脑访问设备启用坞接和取消坞接，请执行以下操作：

  a. 在“**开始**”菜单中，选择“**设置 > 系统 > 电源和睡眠**”，然后将“**睡眠**”设置为“**从不**”。

  b. 在 **设备管理器 > 网络适配器 > 以太网适配器** 下，转到 **电源管理** 并取消选中 **允许计算机关闭此设备以节约电源**。确保选中 **允许此设备唤醒计算机**。

- 有权访问同一办公 PC 的多个用户在 Citrix Workspace 中看到相同的图标。当用户登录 Citrix Workspace 时，如果该资源已被其他用户使用，则该资源将显示为不可用。
- 在每个访问办公电脑的客户端设备（例如，家用电脑）上安装 Citrix Workspace 应用程序。

## 配置顺序

本节概述了在使用 **远程电脑访问** 类型计算机目录时如何配置远程电脑访问。有关如何创建其他类型计算机目录的信息，请参阅 创建计算机目录。

1. 仅限本地站点 - 要使用集成的局域网唤醒功能，请配置 局域网唤醒 中概述的先决条件。
2. 如果为远程电脑访问创建了新的 Citrix Virtual Apps and Desktops 站点：

   a. 选择 **Remote PC Access** 站点类型。

   b. 在 **电源管理** 页面上，选择为默认的远程电脑访问计算机目录启用或禁用电源管理。您可以通过编辑计算机目录属性稍后更改此设置。有关配置局域网唤醒的详细信息，请参阅 局域网唤醒。

   c. 填写 **用户** 和 **计算机帐户** 页面上的信息。

   完成这些步骤将创建一个名为 **Remote PC Access Machines** 的计算机目录和一个名为 **Remote PC Access Desktops** 的交付组。
3. 如果添加到现有 Citrix Virtual Apps and Desktops 站点：

a. 创建 **远程电脑访问** 类型的计算机目录（向导的操作系统页面）。有关如何创建计算机目录的详细信息，请参阅 创建计算机目录。请务必分配正确的 OU，以便目标电脑可用于远程电脑访问。

b. 创建交付组以向用户提供对计算机目录中 PC 的访问权限。有关如何创建交付组的详细信息，请参阅 创建交付组。请务必将交付组分配给包含需要访问其 PC 的用户的 Active Directory 组。

4. 将 VDA 部署到办公电脑。

   - 我们建议使用单会话操作系统核心 VDA 安装程序 (VDAWorkstationCoreSetup.exe)。
   - 您也可以使用带 `/remotepc` 选项的单会话完整 VDA 安装程序 (VDAWorkstationSetup.exe)，这与使用核心 VDA 安装程序的效果相同。
   - 考虑启用 Windows 远程协助，以允许技术支持团队通过 Citrix Director 提供远程支持。为此，请使用 `/enable_remote_assistance` 选项。有关详细信息，请参阅 使用命令行安装。
   - 要在 Director 中查看登录持续时间信息，您必须使用单会话完整 VDA 安装程序并包含 **Citrix User Profile Management WMI Plugin** 组件。通过使用 `/includeadditional` 选项包含此组件。有关详细信息，请参阅 使用命令行安装。
   - 有关使用 SCCM 部署 VDA 的信息，请参阅 使用 SCCM 安装 VDA。
   - 有关通过部署脚本部署 VDA 的信息，请参阅 使用脚本安装 VDA。

   成功完成步骤 2-4 后，用户在本地登录 PC 时将自动分配到其自己的计算机。

5. 指示用户在其用于远程访问办公电脑的每个客户端设备上下载并安装 Citrix Workspace 应用程序。Citrix Workspace 应用程序可从 `https://www.citrix.com/downloads/` 或支持的移动设备的应用商店获取。

## 通过注册表管理的功能

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

### 禁用多用户自动分配

在每个 Delivery Controller™ 上，添加以下注册表设置：

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- 名称: AllowMultipleRemotePCAssignments
- 类型: DWORD
- 数据: 0

### 睡眠模式（最低版本 7.16）

要允许远程电脑访问计算机进入睡眠状态，请在 VDA 上添加此注册表设置，然后重新启动计算机。重新启动后，操作系统电源节省设置将生效。计算机在预配置的空闲计时器到期后进入睡眠模式。计算机唤醒后，它会重新向 Delivery Controller 注册。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名称: DisableRemotePCSleepPreventer
- 类型: DWORD
- 数据: 1

### 会话管理

默认情况下，当本地用户在该计算机上启动会话（通过按 CTRL+ATL+DEL）时，远程用户的会话会自动断开连接。为防止此自动操作，请在办公室 PC 上添加以下注册表项，然后重新启动计算机。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名称: SasNotification
- 类型: DWORD
- 数据: 1

默认情况下，如果在超时期限内未确认连接消息，则远程用户优先于本地用户。要配置此行为，请使用以下设置：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名称: RpcaMode
- 类型: DWORD
- 数据:
  - 1 - 如果远程用户在指定的超时期限内未响应消息 UI，则远程用户始终具有优先权。如果未配置此设置，则此行为是默认行为。
  - 2 - 本地用户具有优先权。

默认情况下，强制执行远程电脑访问模式的超时时间为 30 秒。您可以配置此超时时间，但不要将其设置为低于 30 秒。要配置超时，请使用此注册表设置：

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 名称: RpcaTimeout
- 类型: DWORD
- 数据: 超时秒数（十进制值）

当用户想要强制获取控制台访问权限时：本地用户可以在 10 秒内两次按下 Ctrl+Alt+Del，以获取对远程会话的本地控制权并强制断开连接事件。

注册表更改并重新启动计算机后，如果本地用户在远程用户使用该电脑时按下 Ctrl+Alt+Del 登录，远程用户将收到提示。该提示询问是否允许或拒绝本地用户的连接。允许连接会断开远程用户的会话。

## 会话管理日志记录

远程电脑访问现在具有日志记录功能，可在有人尝试访问具有活动 ICA® 会话的电脑时进行记录。这使您能够监控环境中的不必要或意外活动，并在需要调查任何事件时能够审计此类事件。

事件使用 Windows 事件查看器记录，位于 **应用程序和服务 > Citrix > HostCore > ICA 服务 > 管理员** 中。

使用远程电脑访问时，会记录三个不同的事件。

### Ctrl+Alt+Del 事件

当本地用户在具有活动远程会话的控制台键盘上按下 Ctrl+Alt+Del 时，会出现此事件。

#### 事件详细信息

- 日志名称: 应用程序和服务
- 事件 ID: 43, 44, 45
- 来源：ICA 服务

#### 事件 ID 43

当 SasNotification 注册表值不存在或 SasNotification 注册表值为 0 时，将显示此事件 ID。

- 消息：

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to automatically disconnect the
remote session.
```

**事件 ID 44**

当 SasNotification 注册表值为 1 且 RpcaMode 注册表值为 1 或 RpcaMode 注册表值不存在时，将显示此事件 ID。

- 消息：

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user. The
user preference is set to remote user.
```

**事件 ID 45**

当 SasNotification 注册表值为 1 且 RpcaMode 注册表值为 2 时，将显示此事件 ID。

- 消息：

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user.

The user preference is set to local user.
```

### 远程会话断开连接事件

当远程会话因各种原因断开连接时，将显示此事件。

### 事件详细信息

- 日志名称：应用程序和服务
- 事件 ID：46、47、48
- 来源: ICA Service

**事件 ID 46**

当远程会话已断开连接，并且 SasNotification 注册表值不存在或 SasNotification 注册表值为 0 时，将显示此事件 ID。

- 消息:

```
The remote session for &lt;remoteUserName> has been disconnected.
```

**事件 ID 47**

当远程用户同意断开会话连接，并且 SasNotification 注册表值为 1 且 RpcaMode 注册表值为 1，或者 RpcaMode 注册表值为 2，或者 RpcaMode 注册表值不存在时，将显示此事件 ID。

- 消息:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user accepted the request to disconnect the session.
```

**事件 ID 48**

当远程用户未在特定超时期限内拒绝断开连接请求，并且 SasNotification 注册表值为 1 且 RpcaMode 注册表值为 2 时，将显示此事件 ID。

- 消息:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user did not decline the disconnection request within the
configured timeout period (&lt;timeout period>).
```

**Ctrl+Alt+Del 两次按下事件**

当在 10 秒内两次按下 Ctrl+Alt+Del 时，将显示此事件。

**事件详细信息**

- 日志名称: 应用程序和服务
- 事件 ID: 49
- 来源：ICA 服务

**事件 ID 49**

当在 10 秒内两次按下 Ctrl+Alt+Del 时，会出现此事件 ID。

- 消息：

```
The remote session for &lt;remoteUserName> has been forcibly
disconnected.
```

## 局域网唤醒

远程电脑访问支持局域网唤醒，这使用户能够远程打开物理 PC。此功能使用户在不使用办公室 PC 时可以将其关闭，从而节省能源成本。当计算机意外关闭时，它还可以实现远程访问。

借助局域网唤醒 (Wake on LAN) 功能，当交付控制器发出指令时，魔术包会直接从在 PC 上运行的 VDA 发送到 PC 所在的子网。这使得该功能无需依赖额外的基础架构组件或第三方解决方案即可发送魔术包。

局域网唤醒 (Wake on LAN) 功能与旧版基于 SCCM 的局域网唤醒功能不同。有关基于 SCCM 的局域网唤醒的信息，请参阅 局域网唤醒 – SCCM 集成。

### 限制

带局域网唤醒功能的远程电脑访问不支持在高峰时段自动开机。

### 系统要求

以下是使用局域网唤醒功能的系统要求：

- 控制平面：
  - 思杰 DaaS™
  - Citrix Virtual Apps and Desktops 2009 或更高版本
- 物理 PC：
  - VDA 2009 或更高版本
  - Windows 10 或 Windows 11。有关支持性详细信息，请参阅 VDA 系统要求。
  - 在 BIOS/UEFI 中启用 Wake on LAN
  - 在 Windows 配置中，网卡属性中启用了局域网唤醒。

### 配置 Wake on LAN

如果您使用的是本地部署的 Citrix Virtual Apps and Desktops，则仅支持使用 PowerShell 配置集成式局域网唤醒。

要配置局域网唤醒：

1. 如果您还没有远程电脑访问计算机目录，请创建一个。
2. 如果您还没有 Wake on LAN 主机连接，请创建一个。

> **注意：**
>
> 要使用局域网唤醒功能，如果您有“Microsoft Configuration Manager Wake on LAN”类型的主机连接，请创建新的主机连接。

3. 检索局域网唤醒主机连接的唯一标识符。
4. 将 Wake on LAN 主机连接与计算机目录关联。

要创建 Wake on LAN 主机连接：

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `

                -PluginId VdaWOLMachineManagerFactory `
```

```
                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid



# Wait for the connection to be ready before trying to use it

while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

}
```

当主机连接准备就绪时，运行以下命令以检索主机连接的唯一标识符：

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

检索到连接的唯一标识符后，运行以下命令以将连接与远程电脑访问计算机目录关联：

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

### 设计注意事项

当您计划将局域网唤醒 (Wake on LAN) 与远程电脑访问 (Remote PC Access) 结合使用时，请考虑以下事项：

- 多个计算机目录可以使用相同的局域网唤醒主机连接。
- 要使一台电脑唤醒另一台电脑，两台电脑必须位于同一子网中并使用相同的局域网唤醒主机连接。电脑是否在相同或不同的计算机目录中无关紧要。
- 主机连接分配给特定的区域。如果您的部署包含多个区域，则每个区域都需要一个局域网唤醒主机连接。这同样适用于计算机目录。
- 魔术包使用全局广播地址 255.255.255.255 进行广播。请确保该地址未被阻止。
- 对于每个局域网唤醒连接，子网中必须至少有一台电脑处于开机状态，才能唤醒该子网中的计算机。

### 操作注意事项

以下是使用局域网唤醒功能时的注意事项：

- VDA 必须至少注册一次，然后才能使用集成的局域网唤醒功能唤醒电脑。
- 局域网唤醒只能用于唤醒电脑。它不支持其他电源操作，例如重新启动或关机。
- 创建局域网唤醒连接后，它在 Studio 中可见。但是，如果使用本地部署的 Citrix Virtual Apps and Desktops，则不支持在 Studio 中编辑其属性。
- 魔术包通过以下两种方式之一发送：

  a. 当用户尝试启动其电脑会话且 VDA 未注册时

  b. 当管理员从 Studio 或 PowerShell 手动发送开机命令时

- 由于交付控制器不知道 PC 的电源状态，Studio 在电源状态下显示 **不支持**。交付控制器使用 VDA 注册状态来确定 PC 是开机还是关机。

## 局域网唤醒 – SCCM 集成

SCCM 集成式局域网唤醒是远程电脑访问的一种替代局域网唤醒选项，仅适用于本地部署的 Citrix Virtual Apps and Desktops。

### 系统要求

以下是使用 SCCM 集成式局域网唤醒功能的系统要求：

- Citrix Virtual Apps and Desktops 1912 或更高版本
- 物理 PC：
  - VDA 版本 1912 或更高版本
  - Windows 10。有关支持详细信息，请参阅 VDA 系统要求。

  - 在 BIOS/UEFI 中启用 Wake on LAN
  - 在 Windows 配置中，网卡属性中启用了局域网唤醒。
- 系统中心配置管理器 (SCCM) 2012 R2 或更高版本

### 配置 SCCM 集成的局域网唤醒

完成以下先决条件：

1. 在组织内配置 SCCM 2012 R2、2016 或 2019。然后将 SCCM 客户端部署到所有远程电脑访问计算机，留出时间让计划的 SCCM 清单周期运行，或者在必要时手动强制运行。
2. 要支持唤醒代理，请在 SCCM 中启用该选项。对于组织中包含使用远程电脑访问局域网唤醒功能的电脑的每个子网，请确保有三台或更多计算机可以充当哨兵计算机。
3. 要支持魔术包，请配置网络路由器和防火墙以允许发送魔术包，可以使用子网定向广播或单播。
4. 在每台 PC 的 BIOS/UEFI 设置中配置局域网唤醒。
5. 如果尚未部署，请将 VDA 部署到物理 PC。

解决先决条件后，完成以下步骤以允许 Delivery Controller 与 SCCM 通信：

1. 为 SCCM 创建主机连接。有关详细信息，请参阅 连接和资源。
   - 选择 **Microsoft Configuration Manager Wake on LAN** 作为连接类型。
   - 输入的凭据必须有权访问范围内的集合，并且必须具有 **Remote Tools Operator** 角色。
2. 在 Studio 中选择连接，然后选择 **编辑连接**，并单击 **高级**。
3. 选择处理局域网唤醒的相应选项：
   - 如果您使用的是唤醒代理，请选择第一个选项：**Microsoft System Center Configuration Manager 唤醒代理**。
   - 如果您使用的是魔术包，请选择第二个选项：**由 Delivery Controller 传输的局域网唤醒数据包**。
     - 选择相应的传输方法：**子网定向广播** 或 **单播**。

创建主机连接后，将该连接与远程电脑访问目录关联：

- 如果您要创建新的远程电脑访问目录，请在目录创建向导的**操作系统**页面中，选择**远程电脑访问**作为目录类型，然后从下拉列表中选择相应的连接。
- 要将局域网唤醒添加到现有远程电脑访问目录：

  a. 在 Studio 中转到 **计算机目录** 节点，选择计算机目录，然后选择 **编辑计算机目录**。

b. 选择**电源管理**选项卡，然后选择**是**以启用计算机目录的电源管理。

c. 从下拉列表中选择相应的连接，然后单击**确定**。

## 故障排除

### 显示器消隐不起作用

如果 Windows PC 的本地显示器在活动 HDX 会话期间未空白（本地显示器显示会话中发生的情况），则很可能是由于 GPU 供应商的驱动程序问题。要解决此问题，请通过设置以下注册表值，使 Citrix 间接显示驱动程序 (IDD) 具有比显卡供应商驱动程序更高的优先级：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名称：CitrixIDD
- 类型: DWORD
- 数据: 3

有关显示适配器优先级和显示器创建的更多详细信息，请参阅知识中心文章 CTX237608。

### 在启用了会话管理通知的计算机上选择 Ctrl+Alt+Del 时会话断开连接

由 **SasNotification** 注册表值控制的会话管理通知仅在 VDA 上启用远程电脑访问模式时才有效。如果物理 PC 启用了 Hyper-V 角色或任何基于虚拟化的安全功能，则该 PC 会报告为虚拟机。如果 VDA 检测到它正在虚拟机上运行，它会自动禁用远程电脑访问模式。要启用远程电脑访问模式，请添加以下注册表值：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名称: ForceEnableRemotePC
- 类型: DWORD
- 数据: 1

重新启动 PC 以使设置生效。

### 诊断信息

有关远程电脑访问的诊断信息将写入 Windows 应用程序事件日志。信息性消息不受限制。错误消息通过丢弃重复消息来限制。

- 3300 (信息): 计算机已添加到目录
- 3301 (信息): 计算机已添加到交付组
- 3302 (信息): 计算机已分配给用户

- 3303 (错误): 异常

### 电源管理

如果启用了远程电脑访问的电源管理，则子网定向广播可能无法启动与 Controller 位于不同子网上的计算机。如果您需要使用子网定向广播进行跨子网电源管理，并且 AMT 支持不可用，请尝试唤醒代理或单播方法。请确保在电源管理连接的高级属性中启用了这些设置。

### 活动远程会话记录本地触摸屏输入

当 VDA 启用远程电脑访问模式时，计算机在活动会话期间会忽略本地触摸屏输入。如果物理 PC 启用了 Hyper-V 角色或任何基于虚拟化的安全功能，则该 PC 会报告为虚拟机。如果 VDA 检测到它正在虚拟机上运行，它会自动禁用远程电脑访问模式。要启用远程电脑访问模式，请添加以下注册表设置：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名称: ForceEnableRemotePC
- 类型: DWORD
- 数据: 1

重新启动电脑以使设置生效。

## 更多资源

以下是远程电脑访问的其他资源：

- 解决方案设计指南：远程电脑访问设计决策。
- 远程电脑访问架构示例：Citrix 远程电脑访问解决方案参考架构。

# 应用程序虚拟化

## 将 App-V 与 Citrix Virtual Apps and Desktops™ 结合使用

Microsoft Application Virtualization (App-V) 允许您将应用程序作为服务进行部署、更新和支持。用户无需在其设备上安装应用程序即可访问。App-V 和 Microsoft User State Virtualization (USV) 提供对应用程序和数据的访问，无论位置和互联网连接如何。 下表列出了支持的版本。

| 应用程序虚拟化 | CITRIX VIRTUAL APPS AND DESKTOPS 交付控制器 | CITRIX 虚拟应用和桌面 VDA |
|---|---|---|
| 5.0 和 5.0 SP1 | XenDesktop 7 到当前版本，XenApp 7.5 到当前版本 | 7.0 到当前版本 |
| 5.0 SP2 | XenDesktop 7 到当前版本，XenApp 7.5 到当前版本 | 7.1 到当前版本 |
| 5.0 SP3 和 5.1 | XenDesktop 7.6 到当前版本，XenApp 7.6 到当前版本 | 7.6.300 到当前版本 |
| Windows 服务器 2016 中的 App-V | XenDesktop 7.12 到当前版本，XenApp 7.12 到当前版本 | 7.12 到当前版本 |

App-V 客户端不支持对应用程序进行离线访问。App-V 集成支持包括将 SMB 共享用于应用程序。不支持 HTTP 协议。 如果您不熟悉 App-V，请参阅 Microsoft 文档。以下是本文中提到的 App-V 组件概述：

- **管理服务器**。提供一个集中式控制台来管理 App-V 基础结构，并将虚拟应用程序交付给 App-V 桌面客户端和远程桌面服务客户端。App-V 管理服务器进行身份验证、请求并提供管理员所需的安全、计量、监视和数据收集。该服务器使用 Active Directory 和支持工具来管理用户和应用程序。
- **发布服务器**。为 App-V 客户端提供面向特定用户的应用程序，并托管用于流式传输的虚拟应用程序包。它从管理服务器获取软件包。
- **客户端**。检索虚拟应用程序，在客户端上发布应用程序，并在 Windows 设备上自动设置和管理运行时虚拟环境。您可以在 VDA 上安装 App-V 客户端，它会在每个用户配置文件中存储用户特定的虚拟应用程序设置，例如注册表和文件更改。

应用程序可无缝使用，无需任何预配置或操作系统设置更改。您可以从服务器操作系统和桌面操作系统交付组启动 App-V 应用程序：

- 通过 Citrix Workspace™ 应用
- 通过 App-V 客户端和 Citrix Workspace app
- 多个用户在多个设备上同时使用
- 通过 Citrix StoreFront™

修改后的 App-V 应用程序属性在应用程序启动时实施。例如，对于显示名称已修改或图标已自定义的应用程序，当用户启动应用程序时，修改会显示出来。保存在动态配置文件中的应用程序自定义项也会在应用程序启动时应用。

### 管理方法

您可以使用 App-V sequencer 创建的 App-V 软件包和动态配置文件，然后将其放置在 App-V 服务器或网络共享上。

- **App-V 服务器：** 从 App-V 服务器上的程序包使用应用程序，需要 Studio 与 App-V 服务器之间持续通信，以进行发现、配置和下载到 VDA。这会产生硬件、基础架构和管理开销。Studio 和 App-V 服务器必须保持同步，尤其是对于用户权限。

  这称为*双管理员*管理方法，因为 App-V 程序包和应用程序访问需要 Studio 和 App-V 服务器控制台。此方法最适用于紧密耦合的 App-V 和 Citrix 部署。在此方法中，管理服务器处理动态配置文件。当您使用双管理员管理方法时，Citrix App-V 组件会管理应用程序启动所需的相应发布服务器的注册。这可确保发布服务器在适当时间与用户同步。发布服务器使用其配置的设置来维护程序包生命周期的其他方面（例如登录时刷新和连接组）。

- **网络共享：** 放置在网络共享上的程序包和 XML 部署配置文件消除了 Studio 对 App-V 服务器和数据库基础架构的依赖，从而降低了开销。（您必须在每个 VDA 上安装 Microsoft App-V 客户端。）

  这称为*单管理员*管理方法，因为 App-V 程序包和应用程序的使用只需要 Studio 控制台。您可以浏览到网络共享，并将该位置的一个或多个 App-V 程序包添加到站点级应用程序库 。在此方法中，Citrix App-V 组件在应用程序启动时处理部署配置文件。（不支持用户配置文件。）当您使用单管理员管理方法时，Citrix App-V 组件会管理主机上程序包生命周期的所有方面。程序包在代理启动时或检测到配置更改时（也可以在会话启动时）添加到计算机。当从 Citrix Workspace 应用程序收到启动请求时，程序包会首先按需“即时”发布给单个用户。

  单管理员还管理连接组的生命周期，这些连接组需要满足 Studio 中制定的隔离组配置定义。

  *应用程序库*是 Citrix 的一个术语，指用于存储 App-V 程序包信息的缓存存储库。应用程序库还存储有关其他 Citrix 应用程序交付技术的信息。

在这两种管理方法中，如果 VDA 配置为丢弃用户数据，则必须在下次会话启动时重新进行发布（或同步）。

您可以同时使用一种或两种管理方法。换句话说，当您将应用程序添加到交付组时，这些应用程序可以来自 App-V 服务器或网络共享上的 App-V 包。

> **注意：**
>
> 如果您同时使用两种管理方法，并且 App-V 包在两个位置都有动态配置文件，则将使用 App-V 服务器中的文件（双重管理）。

> 在 Studio 导航窗格中选择 **Configuration > App-V Publishing** 时，显示屏会显示 App-V 程序包名称和源。源列指示程序包是位于 App-V 服务器上还是缓存在应用程序库中。选择程序包时，详细信息窗格会列出程序包中的应用程序和快捷方式。

## 动态配置文件

### 概述

App-V 程序包可以使用动态配置文件进行自定义，这些文件应用于程序包后，可用于更改其特性。例如，您可以使用它们来定义额外的应用程序快捷方式和行为。Citrix App-V 支持这两种类型的动态配置文件。文件设置在应用程序启动时应用：

- 部署配置文件为所有用户提供计算机范围的配置。这些文件应命名为 \<*packageFileName*>_DeploymentConfig.xml，并位于其所应用的 App-V 程序包所在的文件夹中。受单管理员和双管理员管理支持。
- 用户配置文件提供用户特定的配置，支持对程序包进行按用户自定义。单管理员支持以下格式命名的用户配置文件：\<*packageFileName*>_UserConfig.xml，并位于其所应用的 App-V 程序包所在的文件夹中。

当特定程序包存在多个用户配置文件时，它们按以下优先级应用：

1. 用户 SID
2. 用户名
3. AD 组 SID（第一个找到的获胜）
4. AD 组名称（第一个找到的获胜）
5. 默认值

### 例如

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml

MyAppVPackage_joeblogs_UserConfig.xml

MyAppVPackage_S-1-5-32-547_UserConfig.xml

MyAppVPackage_Power Users_UserConfig.xml

MyAppVPackage_UserConfig.xml
```

> **注意：**

文件名的用户特定部分也可以选择性地出现在末尾（例如 MyAppVPackage_UserConfig_**joeblogs**.xml）。

### 动态配置文件位置

在单管理员管理中，Citrix App-V 组件仅处理与其 App-V 程序包位于同一文件夹中的动态配置文件。当程序包中的应用程序启动时，对相应动态配置文件的任何更改都将重新应用。如果您的动态配置文件与其程序包位于不同的位置，请使用映射文件将程序包映射到其部署配置文件。

### 创建映射文件

1. 打开一个新文本文件。
2. 对于每个动态配置文件，添加一行，使用格式 \<PackageGuid> : path 指定包的路径。

   例如：

   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
3. 将文件保存为 ctxAppVDynamicConfigurations.cfg，与包位于同一文件夹中。每次启动包中的应用程序时，都会在与 App-V 包相同的 UNC 共享上向上递归搜索整个目录层次结构以查找此文件。

**注意：**

当存在打开了包中应用程序的用户会话时，您无法应用对动态部署配置的更改。如果其他用户（*但不是当前用户*）打开了包中的应用程序，则可以应用对动态用户配置文件的更改。

### 配置 IIS 以使用动态配置文件

VDA 上的 Citrix App-V 组件可以利用放置在包旁边的 App-V 部署配置文件和用户配置文件，遵循与 UNC 托管包相同的规则。 为此，VDA 组件需要权限来浏览 IIS 目录结构以确定要使用的文件。与 UNC 托管包不同，VDA 必须首先将配置文件从服务器下载到主机上的临时位置，然后才能在发布中使用它们。这是一个可选功能，如果未启用目录浏览，则动态配置文件将被忽略。

执行以下步骤为您的站点启用目录浏览：

1. 在 IIS 管理器控制台中，选择网站节点，然后双击中央窗格中的 **目录浏览**。
2. 单击右侧窗格中的 **启用**，然后选择 *时间*、*大小*、*扩展名* 和 *日期*。（不要选择长日期。）这允许 VDA 上的 Citrix App-V 组件判断是否已应用最新版本的配置文件，或者是否需要更新。

### 隔离组

当您使用 App-V 单一管理员方法时，创建隔离组允许您指定必须在沙盒中运行的相互依赖的应用程序组。此功能与 App-V 连接组类似，但并不完全相同。App-V 管理服务器使用强制和可选包术语，而 Citrix 则对包部署选项使用自动和显式。

- 当用户启动 App-V 应用程序（主应用程序）时，系统会搜索隔离组中标记为自动包含的其他应用程序包。这些包会自动下载并包含在隔离组中。您无需将它们添加到包含主应用程序的交付组中。
- 隔离组中标记为显式包含的应用程序包仅在您已将该应用程序显式添加到包含主应用程序的同一交付组时才会被下载。

这允许您创建隔离组，其中包含可供所有用户全局使用的自动包含应用程序的混合。此外，该组还可以包含一组插件和其他应用程序（可能具有特定的许可限制），您可以将其限制为特定用户集（通过交付组识别），而无需创建更多隔离组。

例如，应用程序“app-a”需要 JRE 1.7 才能运行。您可以创建一个隔离组，其中包含 app-a（具有显式部署类型）和 JRE 1.7（具有自动部署类型）。然后，将这些 App-V 软件包添加到一个或多个交付组。当用户启动 app-a 时，JRE 1.7 会随之自动部署。

您可以将一个应用程序添加到多个 App-V 隔离组。但是，当用户启动该应用程序时，始终使用添加该应用程序的第一个隔离组。您无法对包含该应用程序的其他隔离组进行排序或设置优先级。

### 负载平衡 App-V 服务器

如果使用双管理员管理方法，则支持使用 DNS 循环 (Round-Robin) 对管理服务器和发布服务器进行负载平衡。不支持在 Netscaler、F5（或类似）虚拟 IP 后面对管理服务器进行负载平衡，因为 Studio 需要通过远程 PowerShell 与管理服务器通信。有关详细信息，请参阅这篇 Citrix 博客文章。

### 配置 IIS 以托管和流式传输 App-V 软件包

要使 IIS 服务器能够托管和流式传输 App-V 软件包，请执行以下步骤：

1. 打开 IIS 管理器控制台。有关说明，请参阅 `<https://docs.microsoft.com/zh-cn/previous-versions/iis/6.0-sdk/ms525920(v%3Dvs.90)>`。
2. 右键单击要使用的网站实例，然后选择 **Add Virtual directory**（添加虚拟目录）。
3. 键入别名以及软件包在网络上物理存储的路径。
4. 双击中央窗格中的 **MIME Types**（MIME 类型），然后右键单击窗口中的任意位置并选择 **Add**（添加）。
5. 对于文件扩展名类型 `.appv`，选择 MIME 类型 `application/app-v`，然后单击 **OK**（确定）。

### 将 HTTP 流式传输的 App-V 软件包导入 Citrix DaaS™（以前称为 Citrix Virtual Apps and Desktops 服务）

> **注意：**
>
> 此功能仅在 2009 及更高版本的 Virtual Delivery Agents (VDA) 上受支持。如果将具有 HTTP(S) 路径的 App-V 软件包中的应用程序添加到功能级别为 2003 或更高版本的交付组，则这些应用程序将发布到 Citrix DaaS，但除非 VDA 为 2009 或更高版本，否则用户无法从 Citrix Cloud 启动它们。交付组功能级别在创建交付组中进行了解释。

1. 下载并安装/解压缩最新版本的 *CVAD 远程 PowerShell SDK* 和 *Citrix App-V 包发现模块*。请参阅 Citrix DaaS SDK 和 API。
2. 使用 Package Discovery Module 将 App-V 软件包从 IIS 服务器导入到 Citrix DaaS。例如：

```
Import-Module <Download
Directory>\Citrix.Cloud.AppLibrary.Admin.v1.psm1

Import-AppVPackageToCloud

–PackagePath "https://My.AppVServer.net/Packages/Notepad++.appv"
```

3. 登录您的 Citrix Cloud™ 帐户。
4. 软件包将下载到您计算机上的临时位置，从中提取相关信息并上传到 Citrix DaaS 实例中的应用程序库。

## 设置

下表总结了在 Citrix Virtual Apps and Desktops 中使用单管理员和双管理员管理方法使用 App-V 的设置任务序列。

| 单管理员 | 双管理员 | 任务 |
| --- | --- | --- |
| X | X | 部署 App-V |
| X | X | 打包和放置 |
| | X | 在 Studio 中配置 App-V 服务器地址 |

| 单管理员 | 双管理员 | 任务 |
| --- | --- | --- |
| X | X | 在 VDA 计算机上安装软件 |
| X | | 将 App-V 软件包添加到应用程序库 |
| X | | 添加 App-V 隔离组（可选） |
| X | X | 将 App-V 应用程序添加到交付组 |

### 部署 微软 App-V

有关 App-V 部署说明，请参阅 `<https://docs.microsoft.com/zh-cn/microsoft-desktop-optimization-pack/>`。

（可选）更改 App-V 发布服务器设置。Citrix 建议在 Controller 上使用 SDK cmdlet。有关详细信息，请参阅 SDK 文档。

- 要查看发布服务器设置，请输入 **Get-CtxAppvServerSetting -AppVPublishingServer \<*pubServer*>**。
- 为确保 App-V 应用程序正常启动，请输入 **Set-CtxAppvServerSetting –UserRefreshonLogon 0**。

如果您以前使用 GPO 策略设置来管理发布服务器设置，则 GPO 设置会覆盖所有 App-V 集成设置，包括 cmdlet 设置。这可能导致 App-V 应用程序启动失败。Citrix 建议您删除所有 GPO 策略设置，然后使用 SDK 配置这些设置。

### 打包和放置

对于任一管理方法，请使用 App-V sequencer 创建应用程序包。有关详细信息，请参阅 Microsoft 文档。

- 对于单一管理员管理，请在 UNC 或 SMB 共享网络位置上提供软件包及其对应的动态配置文件。确保将应用程序添加到交付组的 Studio 管理员至少具有该位置的读取权限。
- 对于双管理员管理，请从 UNC 路径在 App-V 管理服务器上发布软件包。（不支持从 HTTP URL 发布。）

无论软件包位于 App-V 服务器上还是网络共享上，请确保软件包具有适当的安全权限，以允许 Studio 管理员访问它们。网络共享必须与“经过身份验证的用户”共享，以确保 VDA 和 Studio 默认都具有读取权限。

### 在 Studio 中配置 App-V 服务器地址

> **重要提示：**
>
> 如果 App-V 服务器使用非默认属性值，Citrix 建议在 Controller 上使用 PowerShell cmdlet 指定 App-V 服务器地址。有关详细信息，请参阅 SDK 文档。如果在 Studio 中更改 App-V 服务器地址，您指定的某些服务器连接属性可能会重置为默认值。这些属性用于 VDA 连接到 App-V 发布服务器。如果发生这种情况，请重新配置服务器上任何已重置属性的非默认值。

> 此过程仅适用于双管理员管理方法。

在站点创建期间或之后，为双管理员管理方法指定 App-V 管理和发布服务器地址。您可以在创建站点期间或之后执行此操作。

在站点创建期间：

- 在向导的 **App-V** 页面上，输入 Microsoft App-V 管理服务器的 URL，以及 App-V 发布服务器的 URL 和端口号。
- 在继续向导之前测试连接。如果测试失败，请参阅下面的“故障排除”部分。

创建站点后：

1. 在 Studio 导航窗格中，选择 **Configuration > App-V Publishing**。
2. 如果您之前未指定 App-V 服务器地址，请在“操作”窗格中选择 **Add Microsoft Server**。
3. 要更改 App-V 服务器地址，请在“操作”窗格中选择 **Edit Microsoft Server**。
4. 输入 Microsoft App-V 管理服务器的 URL，以及 App-V 发布服务器的 URL 和端口号。
5. 在关闭对话框之前测试与这些服务器的连接。如果测试失败，请参阅下面的“故障排除”部分。

稍后，如果您想删除与 App-V 管理和发布服务器的所有链接，并阻止 Studio 从这些服务器发现 App-V 软件包，请在“操作”窗格中选择 **Remove Microsoft Server**。仅当这些服务器上的软件包中没有应用程序当前发布到任何交付组时，才允许执行此操作。如果存在，则必须先从交付组中删除这些应用程序，然后才能删除 App-V 服务器。

### 在 VDA 计算机上安装软件

包含 VDA 的计算机必须安装两套软件才能支持 App-V：一套来自 Microsoft，另一套来自 Citrix。

### Microsoft App-V 客户端

此软件检索虚拟应用程序，在客户端上发布应用程序，并在 Windows 设备上运行时自动设置和管理虚拟环境。App-V 客户端将用户特定的虚拟应用程序设置（例如注册表和文件更改）存储在每个用户的配置文件中。

App-V 客户端可从 Microsoft 获取。在包含 VDA 的每台计算机上，或在用于计算机目录创建 VM 的主映像上安装客户端。**注意**：Windows 10（1607 或更高版本）和 Windows Server 2016 已包含 App-V 客户端。仅在这些操作系统上，通过运行 PowerShell **Enable-AppV** cmdlet（无参数）来启用 App-V 客户端。**Get-AppVStatus** cmdlet 检索当前的启用状态。

> **提示：**
>
> 安装 App-V 客户端后，使用管理员权限运行 PowerShell **Get-AppvClientConfiguration** cmdlet，并确保 EnablePackageScripts 设置为 1。如果未设置为 1，请运行 **Set-AppvClientConfiguration -EnablePackageScripts $true**。

### Citrix App-V 组件

默认情况下，在安装 VDA 时，Citrix App-V 组件软件会被排除。

您可以在 VDA 安装期间控制此默认行为。在图形界面中，在**附加组件**页面上选择 **Citrix Personalization for App-V - VDA** 复选框。在命令行界面中，使用 **/includeadditional "Citrix Personalization for App-V – VDA"** 选项。

如果在 VDA 安装期间未包含 Citrix App-V 组件，但之后想使用 App-V 应用程序：在 Windows 计算机的“程序和功能”列表中，右键单击 **Citrix Virtual Delivery Agent** 条目，然后选择**更改**。此时将启动一个向导。在该向导中，启用安装并启用 App-V 发布组件的选项。

## 在应用程序库中添加或删除 App-V 程序包

这些过程仅适用于单一管理员管理方法。

您必须至少具有包含 App-V 程序包的网络共享的读取访问权限。

### 将 App-V 程序包添加到应用程序库

1. 在 Studio 导航窗格中选择**配置 > App-V 发布**。
2. 在“操作”窗格中选择**添加程序包**。
3. 浏览到包含 App-V 程序包的共享，然后选择一个或多个程序包。
4. 单击“**添加**”。

### 从应用程序库中删除 App-V 程序包

从应用程序库中删除 App-V 程序包会将其从 Studio App-V 发布节点显示中删除。但是，它不会从交付组中删除其应用程序，并且这些应用程序仍然可以启动。该程序包仍保留在其物理网络位置。（此效果与从交付组中删除 App-V 应用程序不同。）

1. 在 Studio 导航窗格中选择**配置 > App-V 发布**。
2. 选择一个或多个要删除的程序包。
3. 在“操作”窗格中选择“**删除包**”。

## 添加、编辑或删除 App-V 隔离组

### 添加 App-V 隔离组

1. 在 Studio 导航窗格中选择“**App-V 发布**”。
2. 在“操作”窗格中选择“**添加隔离组**”。
3. 在“**添加隔离组设置**”对话框中，键入隔离组的名称和描述。
4. 从“可用包”列表中，选择要添加到隔离组的应用程序，然后单击右箭头。选定的应用程序现在应显示在“隔离组中的包”列表中。在每个应用程序旁边的“**部署**”下拉列表中，选择“**显式**”或“**自动**”。您还可以使用向上和向下箭头更改列表中的应用程序顺序。
5. 完成后，单击“**确定**”。

### 编辑 App-V 隔离组

1. 在 Studio 导航窗格中选择“**App-V 发布**”。
2. 在中间窗格中选择“**隔离组**”选项卡，然后选择要编辑的隔离组。
3. 在“操作”窗格中选择“**编辑隔离组**”。
4. 在“**编辑隔离组设置**”对话框中，更改隔离组名称或描述、添加或删除应用程序、更改其部署类型或更改应用程序顺序。
5. 完成后，单击“**确定**”。

### 删除 App-V 隔离组

移除隔离组不会移除应用程序包。它只会移除分组。

1. 从 Studio 导航窗格中选择 **App-V Publishing**。
2. 在中间窗格中选择 **Isolation Groups** 选项卡，然后选择要移除的隔离组。
3. 从“操作”窗格中选择 **Remove Isolation Group**。
4. 确认删除。

### 将 App-V 应用程序添加到交付组

以下过程重点介绍如何将 App-V 应用程序添加到交付组。有关创建交付组的完整详细信息，请参阅创建交付组。

**步骤 1：** 选择是要创建新的交付组，还是将 App-V 应用程序添加到现有交付组：

要创建包含 App-V 应用程序的交付组：

1. 在 Studio 导航窗格中选择 **交付组**。
2. 在“操作”窗格中选择 **Create Delivery Group**。
3. 在向导的后续页面上，指定计算机目录和用户。

要将 App-V 应用程序添加到现有交付组：

1. 在 Studio 导航窗格中选择 **Applications**。
2. 在“操作”窗格中选择 **Add Applications**。
3. 选择一个或多个将添加 App-V 应用程序的交付组。

**步骤 2：** 在向导的“**应用程序**”页面上，单击“**添加**”下拉列表以显示应用程序源。选择 **App-V**。

**步骤 3：** 在“**添加 App-V 应用程序**”页面上，选择 App-V 源：App-V 服务器或应用程序库。结果显示包括应用程序名称及其程序包名称和程序包版本。选中要添加的应用程序或应用程序快捷方式旁边的复选框。然后单击“**确定**”。

**步骤 4：** 完成向导。

须知：

- 如果在将 App-V 应用程序添加到交付组时更改其属性，则这些更改会在应用程序启动时生效。例如，如果在将应用程序添加到组时修改其显示名称或图标，则当用户启动该应用程序时，更改会显示。
- 如果使用动态配置文件自定义 App-V 应用程序的属性，则这些属性将覆盖在将应用程序添加到交付组时所做的任何更改。
- 如果以后编辑包含 App-V 应用程序的交付组，并且将组的交付类型从桌面和应用程序更改为仅应用程序，则 App-V 应用程序的性能不会发生变化。
- 从交付组中删除以前发布的（单一管理员）App-V 程序包时，Citrix App-V 客户端组件会尝试清理、取消发布和删除单一管理员管理方法不再使用的任何程序包。

- 如果您正在使用混合部署（通过单一管理员管理方法和 App-V 发布服务器交付程序包，由双管理员或通过其他机制（例如组策略）进行管理），则无法确定哪些（现在可能冗余的）程序包来自哪个源。在这种情况下，不会尝试清理。
- 如果在单个交付组中发布超过 100 个 App-V 应用程序，则应用程序可能无法启动。如果是这样，请使用相应绑定元素上的 MaxReceivedMessageSize 属性来增加交付控制器和/或 VDA 上的 Broker Agent 配置中的最大可接收消息大小。

## 故障排除

仅在使用双管理员方法时可能出现的问题标记为 (DUAL)。

(DUAL) 在 Studio 导航窗格中选择“**配置 > App-V 发布**”时，出现 PowerShell 连接错误。

- Studio 管理员也是 App-V 服务器管理员吗？Studio 管理员必须属于 App-V 管理服务器上的“administrators”组，才能与其通信。

(DUAL) 在 Studio 中指定 App-V 服务器地址时，“测试连接”操作返回错误。

- App-V 服务器是否已开机？可以发送 Ping 命令或检查 IIS 管理器；每个 App-V 服务器都应处于“已启动”和“正在运行”状态。
- App-V 服务器上是否启用了 PowerShell 远程处理？如果没有，请参阅 `<https://docs.microsoft.com/zh-cn/previous-versions/technet-magazine/ff700227(v=msdn.10)>`。
- Studio 管理员也是 App-V 服务器管理员吗？Studio 管理员必须属于 App-V 管理服务器上的 *administrators* 组，才能与其通信。
- App-V 服务器上是否启用了文件共享？在 Windows 资源管理器中或使用“运行”命令输入 `\\<App-V server FQDN>`。
- App-V 服务器是否具有与 App-V 管理员相同的文件共享权限？在 App-V 服务器上，在“存储的用户名和密码”中为 `\\<App-V server FQDN>` 添加一个条目，指定在 App-V 服务器上具有管理员权限的用户的凭据。有关指导，请参阅 `<http://support.microsoft.com/kb/306541>`。
- App-V 服务器是否在 Active Directory 中？

  如果 Studio 计算机和 App-V 服务器位于没有信任关系的不同 Active Directory 域中，请在 Studio 计算机上的 PowerShell 控制台中运行 **winrm s winrm/Config/client '@(TrustedHosts="\<*App-V server FQDN*>")'**。

  如果 TrustedHosts 由 GPO 管理，则会显示以下错误消息：“*无法更改配置设置 TrustedHosts，因为其使用受策略控制。需要将策略设置为“未配置”才能更改配置设置。*”在这种情况下，请将

App-V 服务器名称的条目添加到 GPO 中的 TrustedHosts 策略（管理模板 > Windows 组件 > Windows 远程管理 (WinRM) > WinRM 客户端）。

(DUAL) 将 App-V 应用程序添加到交付组时发现失败。

- Studio 管理员是否也是 App-V 管理服务器管理员？Studio 管理员必须属于 App-V 管理服务器上的 *administrators* 组，以便能够与其通信。
- App-V 管理服务器是否正在运行？可以发送 Ping 命令或检查 IIS 管理器；每个 App-V 服务器都应处于“已启动”和“正在运行”状态。
- 两个 App-V 服务器上是否都启用了 PowerShell 远程处理？如果未启用，请参阅 `<https://docs.microsoft.com/zh-cn/previous-versions/technet-magazine/ff700227(v=msdn.10)>`。
- 程序包是否具有 Studio 管理员访问所需的相应安全权限？

App-V 应用程序只能在一个浏览器版本中启动。

- 如果您发布同一浏览器应用程序的多个序列化版本，则每个用户在 VDA 上一次只能启动一个版本的应用程序。即使不涉及 Citrix 组件，并且用户从指向不同路径的桌面快捷方式启动序列化应用程序，也会发生同样的情况。

  用户首次启动的浏览器版本决定了后续运行的浏览器版本。当 Firefox 检测到第二次启动时，它倾向于创建已运行进程的一个实例，而不是创建一个新进程。其他浏览器也可能以相同的方式运行。

  您可以通过将命令行参数 **-no-remote** 添加到快捷方式的启动命令中，使应用程序在预期的 Firefox 浏览器版本中启动。其他浏览器也提供相同或类似的功能。

  > **注意：**
  >
  > 您必须使用 XenApp 7.17 或更高版本才能利用快捷方式枚举功能。您还必须更改应用程序两个版本中的程序包才能获得此双向行为。

App-V 应用程序无法启动。

- (DUAL) 发布服务器是否正在运行？
- (DUAL) App-V 软件包是否具有适当的安全权限，以便用户可以访问它们？
- (DUAL) 在 VDA 上，确保 Temp 指向正确的位置，并且 Temp 目录中有足够的可用空间。

- (DUAL) 在 App-V 发布服务器上，运行 `Get-AppvPublishingServer *` 以显示发布服务器列表。
- (DUAL) 在 App-V 发布服务器上，确保 UserRefreshonLogon 设置为 False。
- (DUAL) 在 App-V 发布服务器上，以管理员身份运行 **Set-AppvPublishingServer** 并将 UserRefreshonLogon 设置为 False。
- VDA 上是否安装了受支持的 App-V 客户端版本？VDA 是否启用了 **enable package scripts** 设置？
- 在包含 App-V 客户端和 VDA 的计算机上，从注册表编辑器 (regedit) 中，转到 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV。确保 AppVServers 键具有以下值格式：AppVManagementServer+metadata;PublishingServer（例如：`http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082)`。
- 在包含 App-V 客户端和 VDA 的计算机或主映像上，检查 PowerShell ExecutionPolicy 是否设置为 RemoteSigned。Microsoft 提供的 App-V 客户端未签名，此 ExecutionPolicy 允许 PowerShell 运行未签名的本地脚本和 cmdlet。使用以下两种方法之一设置 ExecutionPolicy：(1) 作为管理员，输入 cmdlet：**Set-ExecutionPolicy RemoteSigned**，或 (2) 从组策略设置中，转到“计算机配置”>“策略”>“管理模板”>“Windows 组件”>“Windows PowerShell”>“启用脚本执行”。
- 如果出现错误“RegistrationManager.AttemptRegistrationWithSingleDdc: Failed to register”，请使用相应绑定元素上的 MaxReceivedMessageSize 属性来增加 Delivery Controller 和/或 VDA 上 Broker Agent 配置中的最大可接收消息大小。

如果这些步骤无法解决问题，请启用并检查日志。

## 日志

App-V 配置相关日志位于 C:\CtxAppvLogs。应用程序启动日志位于：%LOCALAPPDATA%\Citrix\CtxAppvLogs。LOCALAPPDATA 解析为登录用户的本地文件夹。检查应用程序启动失败的用户的本地文件夹。

要启用用于 App-V 的 Studio 和 VDA 日志，您必须具有管理员权限。您还需要一个文本编辑器，例如记事本。

要启用 Studio 日志：

1. 创建文件夹 C:\CtxAppvLogs。
2. 转到 C:\Program Files\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1。使用文本编辑器打开 CtxAppvCommon.dll.config 并取消注释以下行：\<add key ="LogFileName" value="C:\CtxAppvLogs\log.txt"/>
3. 重新启动 Broker 服务以开始记录日志。

要启用 VDA 日志：

1. 创建文件夹 C:\CtxAppvLogs。
2. 转到 C:\Program Files\Citrix\ Virtual Desktop Agent。使用文本编辑器打开 CtxAppvCommon.dll.config 并取消注释以下行：\<add key ="LogFileName" value="C:\CtxAppvLogs\log.txt"/>
3. 取消注释该行并将值字段设置为 1：\<add key ="EnableLauncherLogs" value="1"/>
4. 重新启动计算机以开始记录日志。

# 发布内容

您可以发布一个应用程序，该应用程序只是指向资源的 URL 或 UNC 路径，例如 Microsoft Word 文档或 Web 链接。此功能称为发布内容。发布内容的能力增加了向用户交付内容的灵活性。您可以受益于现有的应用程序访问控制和管理。您还可以指定是使用本地应用程序还是已发布的应用程序来打开内容。

发布的内容在 StoreFront™ 和 Citrix Workspace™ 应用程序中与其他应用程序一样显示。用户访问它的方式与访问应用程序的方式相同。在客户端上，资源照常打开。

- 如果本地安装的应用程序合适，则会启动它来打开资源。
- 如果已定义文件类型关联，则会启动已发布的应用程序来打开资源。

您可以使用 PowerShell SDK 发布内容。您不能使用 Studio 发布内容。但是，您可以在内容发布后使用 Studio 编辑应用程序属性。

## 配置概述和准备

发布内容使用 `New-BrokerApplication` cmdlet，并具有以下关键属性。（有关所有 cmdlet 属性的说明，请参阅 cmdlet 帮助。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType` 属性必须为 `PublishedContent`。

`CommandLineExecutable` 属性指定发布内容的位置。支持以下格式，限制为 255 个字符。

- HTML 网站地址（例如，`<http://www.citrix.com>`）
- Web 服务器上的文档文件（例如，`https://www.citrix.com/press/pressrelease.doc`）

- FTP 服务器上的目录（例如，`ftp://ftp.citrix.com/code`）
- FTP 服务器上的文档文件（例如，`ftp://ftp.citrix.com/code/Readme.txt`>）
- UNC 目录路径（例如，`file://myServer/myShare or \\\\myServer\\myShare`）
- UNC 文件路径（例如，`file://myServer/myShare/myFile.asf` 或 `\\myServer\myShare\myFile.asf`）

确保您拥有正确的 SDK。

- 对于 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）部署，下载 并安装 Citrix Virtual Apps and Desktops 远程 PowerShell SDK。
- 对于本地 Citrix Virtual Apps and Desktops 部署，请使用随 Delivery Controller 安装的 PowerShell SDK。添加已发布的内容应用程序需要最低版本为 7.11 的 Delivery Controller。

以下过程使用示例。在示例中：

- 已创建计算机目录。
- 已创建名为 `PublishedContentApps` 的交付组。该组使用目录中的多会话操作系统计算机。WordPad 应用程序已添加到该组。
- 已为交付组名称、`CommandLineExecutable` 位置和应用程序名称进行分配。

## 入门

在包含 PowerShell SDK 的计算机上，打开 PowerShell。

以下 cmdlet 添加相应的 PowerShell SDK 管理单元，并分配返回的交付组记录。

`Add-PsSnapin Citrix* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

如果您使用的是 Citrix DaaS，请通过输入您的 Citrix Cloud™ 凭据进行身份验证。如果存在多个客户，请选择一个。

### 发布 URL

分配位置和应用程序名称后，以下 cmdlet 将 Citrix® 主页发布为应用程序。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"
```

```
New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

验证成功：

- 打开 StoreFront 并以可以访问 PublishedContentApps 交付组中应用程序的用户身份登录。显示屏包含新创建的带有默认图标的应用程序。要了解如何自定义图标，请参阅 `<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`。
- 单击 **Citrix 主页**应用程序。URL 将在本地运行的默认浏览器实例的新选项卡中启动。

## 发布位于 UNC 路径的资源

在此示例中，管理员已创建了一个名为 `PublishedResources` 的共享。分配位置和应用程序名称后，以下 cmdlet 将该共享中的 RTF 和 DOCX 文件发布为资源。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName
```

```
-DesktopGroup $dg.Uid
```

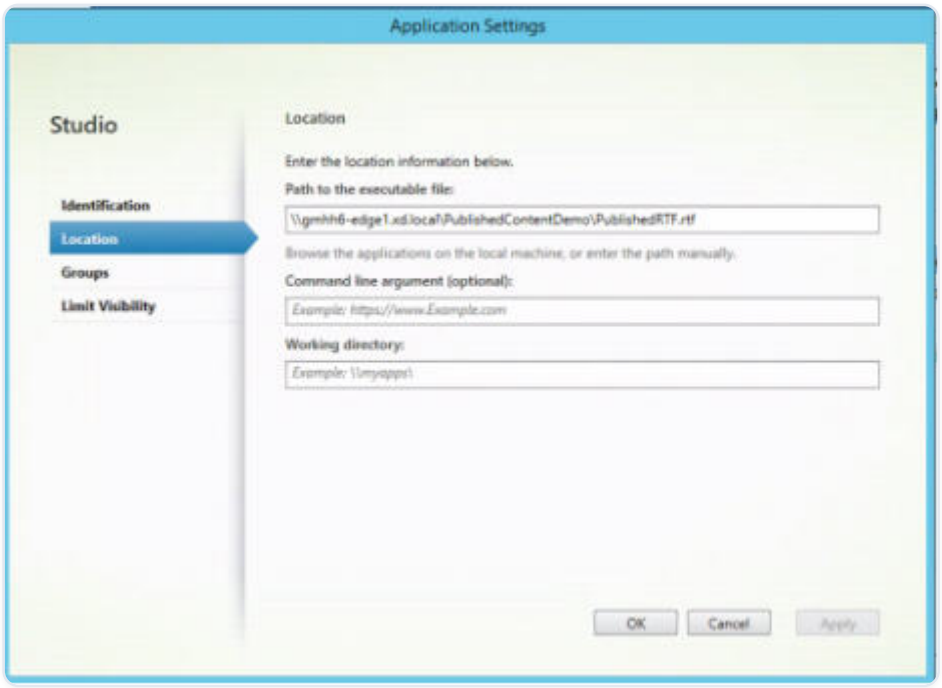
验证成功：

- 刷新 StoreFront 窗口以查看新发布的文档。
- 单击 **PublishedRTF** 和 **PublishedDOCX** 应用程序。每个文档都会在本地运行的写字板中打开。

## 查看和编辑 PublishedContent 应用程序

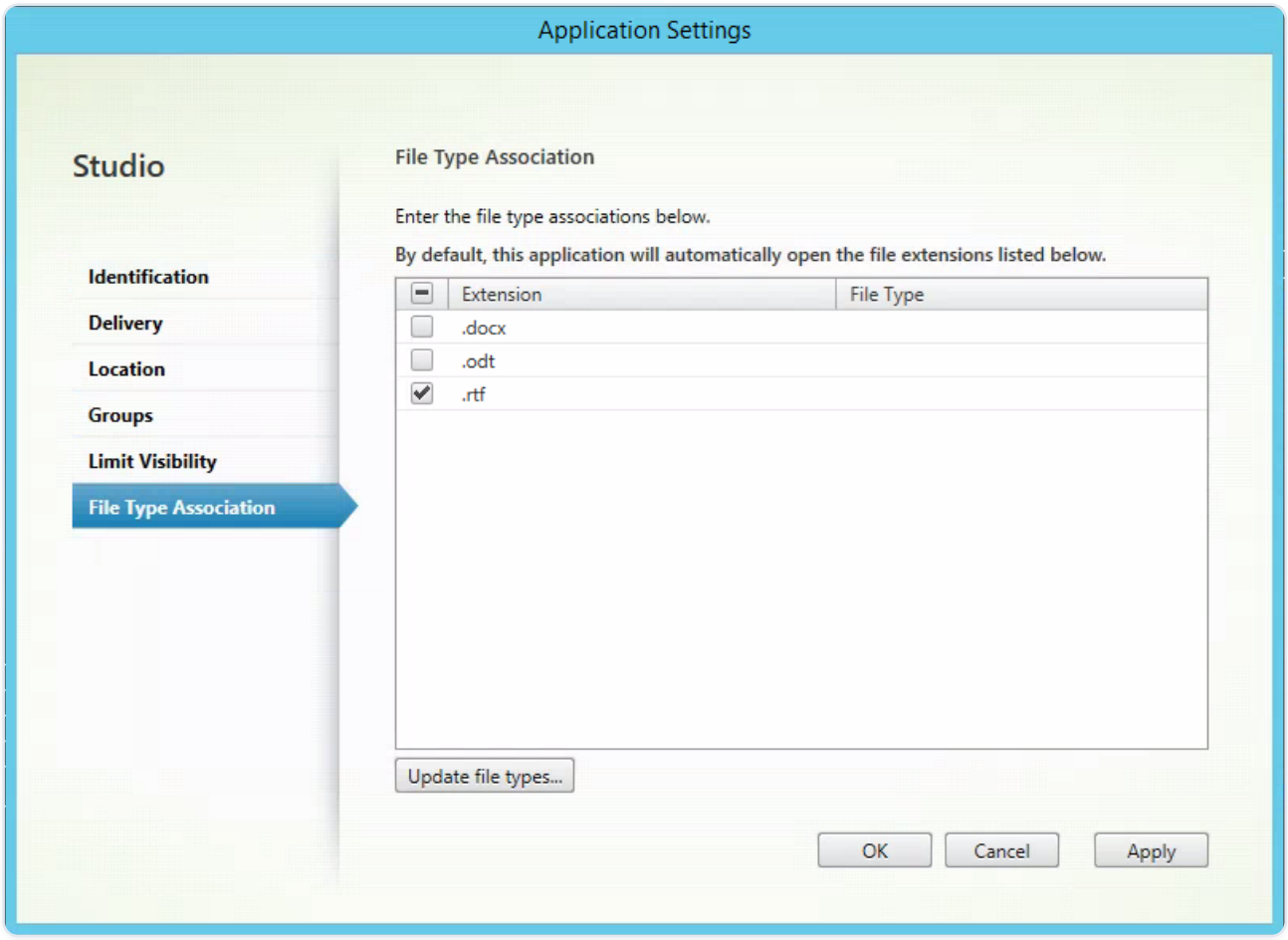
您可以使用管理其他应用程序类型的方法来管理已发布内容。已发布内容项显示在 Studio 的“**应用程序**”列表中，并且可以在 Studio 中进行编辑。

应用程序属性（例如用户可见性、组关联和快捷方式）适用于已发布内容。但是，您不能更改“**位置**”页面上的命令行参数或工作目录属性。要更改资源，请修改该页面上的“**可执行文件路径**”字段。

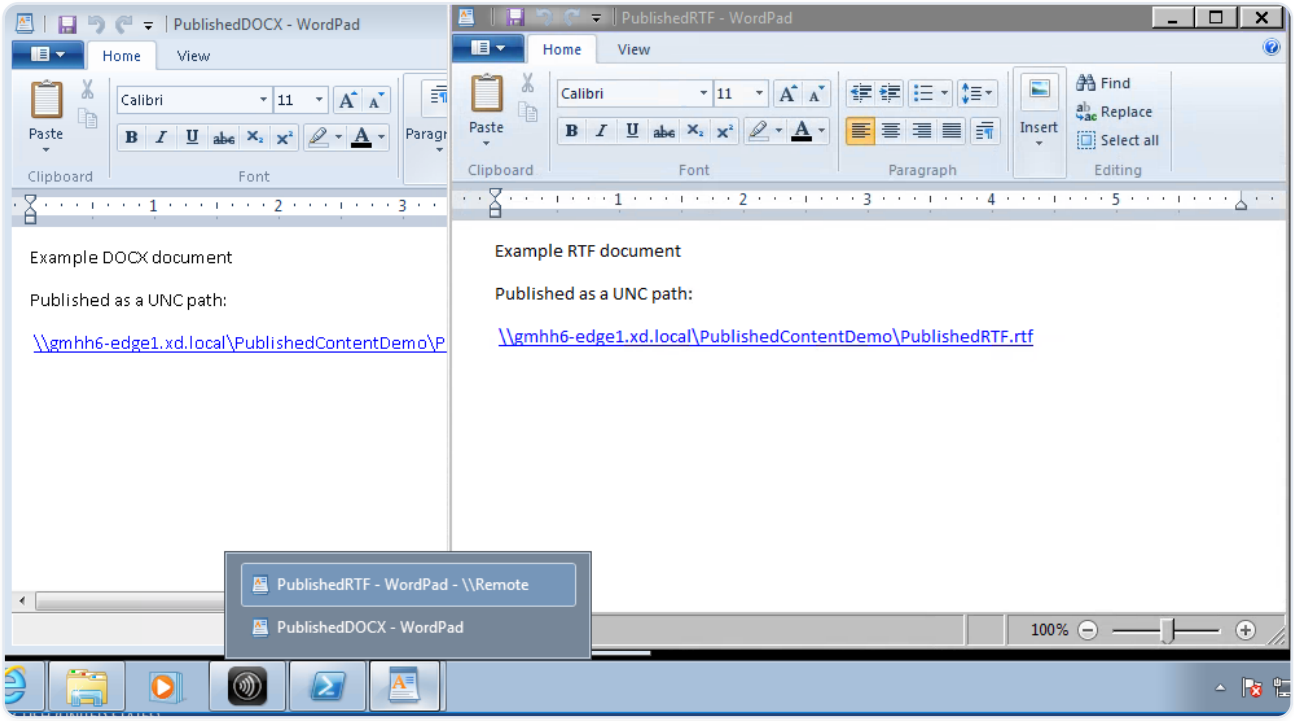



要使用已发布的应用程序打开 `PublishedContent` 应用程序（而不是本地应用程序），请编辑已发布应用程序的“**文件类型关联**”属性。在此示例中，已发布的写字板应用程序经过编辑，为 .rtf 文件创建了文件类型关联。

在编辑文件类型关联之前，请为交付组启用维护模式。完成后请记住关闭维护模式。




刷新 StoreFront 以加载文件类型关联更改，然后单击“**PublishedRTF**”和“**PublishedDOCX**”应用程序。请注意区别。“**PublishedDOCX**”仍将在本地写字板中打开。但是，由于文件类型关联，“**PublishedRTF**”现在将在已发布的写字板中打开。



## 更多信息

- 创建计算机目录
- 创建交付组
- 更改应用程序属性

# 服务器 VDI

使用服务器 VDI（虚拟桌面基础结构）功能，从服务器操作系统为单个用户交付桌面。

- 企业管理员可以将服务器操作系统作为 VDI 桌面交付，这对于工程师和设计师等用户来说非常有价值。
- 服务提供商可以从云端提供桌面。这些桌面符合 Microsoft 服务提供商许可协议 (SPLA)。

支持：

- 在 Citrix Virtual Apps and Desktops™ 和 Citrix DaaS（其前身为 Citrix Virtual Apps and Desktops 服务）的部署中，服务器 VDI 支持 Windows Server 2022、Windows Server 2019 和 Windows Server 2016。
- 所有服务器 VDI 部署都支持用户个性化层技术。
- 要使服务器 VDI 与扫描仪等 TWAIN 设备配合使用，必须安装 Windows Server 桌面体验功能。
- 以下功能不能与服务器 VDI 一起使用：
  - 托管应用程序
  - 本地应用访问
  - 直接（非代理）桌面连接
  - 远程电脑访问

## 安装和配置服务器 VDI

1. 准备 Windows 服务器以进行安装。
   - 使用 Windows Server Manager 确保未安装远程桌面服务角色服务。如果以前安装过，请将其删除。如果安装了这些角色服务，VDA 安装将失败。
   - 确保**将每个用户限制为单个会话**属性已启用。在 Windows 服务器上，编辑终端服务器设置的注册表：

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

`DWORD fSingleSessionPerUser = 1`

2. 使用 Citrix Virtual Apps and Desktops 安装程序的命令行界面在受支持的服务器或服务器主映像上安装 VDA，并指定 `/servervdi` 选项。（默认情况下，安装程序的图形界面会阻止在服务器操作系统上安装 Windows 单会话 OS VDA。使用命令行可覆盖此行为。）使用以下命令之一：

   - 思杰虚拟应用和桌面部署：
     - `XenDesktopVdaSetup.exe /servervdi`
     - `VDAWorkstationSetup.exe /servervdi`
   - Citrix DaaS™ 部署：
     - `VDAWorkstationSetup.exe /servervdi`

   其他选项：

   - 使用 `/controllers` 指定交付控制器或云连接器。
   - 使用 `/enable_hdx_ports` 在防火墙中打开端口，除非防火墙要手动配置。
   - 如果您要在映像上安装 VDA，并且将使用 MCS 从该映像创建服务器 VM，请使用 `/mastermcsimage`（或 `/masterimage`）。
   - 有关所有选项的详细信息，请参阅使用命令行安装。

3. 为 Server VDI 创建计算机目录。在目录创建向导中：

   - 在**操作系统**页面上，选择**单会话操作系统**。
   - 在**摘要**页面上，为管理员指定一个计算机目录名称和描述，以清楚地将其标识为 Server VDI。这是 Studio 中指示目录支持 Server VDI 的唯一标志。

   在 Studio 中使用搜索时，Server VDI 目录会显示在**单会话操作系统计算机**选项卡上，即使 VDA 是安装在多会话计算机上。

4. 创建交付组并选择您创建的 Server VDI 目录。

如果在 VDA 安装期间未指定 Delivery Controller 或 Cloud Connector，请记住稍后指定它们。有关详细信息，请参阅VDA 注册。

# 用户个性化层

Citrix Virtual Apps and Desktops™ 的用户个性化层功能扩展了非持久性计算机目录的功能，以在会话之间保留用户数据和本地安装的应用程序。用户个性化层功能由底层 Citrix App Layering 技术提供支持，在非持久性计算机目录中支持 Citrix Provisioning 和 Machine Creation Services (MCS)。

您在主映像中与 Virtual Delivery Agent 一起安装用户个性化层组件。VHD 文件存储本地用户安装的应用程序。挂载在映像上的 VHD 充当用户自己的虚拟硬盘。

> **重要提示：**
>
> 您可以在 Citrix Virtual Apps and Desktops 中部署用户个性化层，或者在映像模板中启用 App Layering 用户层，但不能同时部署两者。请勿在 App Layering 中的层上安装用户个性化层功能。
>
> 此功能取代了 Personal vDisk (PvD)，同时还在非持久性、池化桌面环境中为用户提供持久的工作区体验。

要部署用户个性化层功能，请按照文章中详述的步骤进行安装和配置。在此之前，该功能不可用。

## 应用程序支持

除以下例外情况外，用户在桌面上本地安装的所有应用程序都受用户个性化层支持。

### 例外情况

以下应用程序是例外，用户个性化层不支持这些应用程序：

- 企业应用程序，例如 MS Office 和 Visual Studio。
- 修改网络堆栈或硬件的应用程序。示例：VPN 客户端。
- 具有启动级别驱动程序的应用程序。示例：病毒扫描程序。
- 驱动程序使用驱动程序存储的应用程序。示例：打印机驱动程序。

> **注意：**
>
> 您可以使用 Windows 组策略对象 (GPO) 使打印机可用。

*不要*允许用户在本地安装任何不受支持的应用程序。相反，请将这些应用程序直接安装在主映像上。

### 需要本地用户或管理员帐户的应用程序

当用户在本地安装应用程序时，该应用程序会进入其用户层。如果用户随后添加或编辑本地用户或组，则这些更改在会话结束后不会保留。

**重要提示：**

在主映像中添加任何所需的本地用户或组。

## 要求

用户个性化层功能需要以下组件：

- Citrix Virtual Apps and Desktops 7 1909 或更高版本
- 虚拟投递代理 (VDA)，版本 1912
- Citrix Provisioning™，版本 1909 或更高版本
- Windows 文件共享 (SMB)，或启用了本地 AD 身份验证的 Azure 文件

当操作系统部署为单会话时，您可以在以下 Windows 版本上部署用户个性化层功能。支持仅限于单个会话上的单个用户。

- Windows 10 Enterprise x64，版本 1607 或更高版本
- Windows 10 多会话（支持 Azure 文件）
- Windows Server 2016（支持 Azure 文件）
- Windows Server 2019（支持 Azure 文件）

对于 Citrix Virtual Apps and Desktops 7，在 Windows Server 2019、Windows Server 2016v 和 Windows 10 客户端上支持将 Azure 文件与用户个性化层结合使用。

**注意：**

用户个性化层仅支持作为服务器 VDI 部署。有关部署详细信息，请参阅 服务器 VDI 文章。

用户个性化层每台计算机一次仅支持一个用户，然后计算机必须重新启动才能重置磁盘。您不能将用户个性化层与多会话服务器操作系统一起使用，只能与单会话服务器系统一起使用。用户个性化层仅适用于非持久性桌面。

如果已安装用户个性化层功能，请将其卸载。在安装最新版本之前，请重新启动主映像。

## 设置文件共享

用户个性化层功能需要 Windows 服务器消息块 (SMB) 存储。要创建 Windows 文件共享，请按照您所用 Windows 操作系统的常规步骤操作。

有关将 Azure 文件与基于 Azure 的目录结合使用的更多信息，请参阅 为用户个性化层设置 Azure 文件存储。

## 建议

请遵循本节中的建议，以成功部署用户个性化层。

### 配置文件管理解决方案

用户个性化层存储用户对单个计算机目录映像所做的所有更改。为了增加增强功能，例如跨多个目录映像漫游配置文件数据，Citrix 建议同时使用 Profile Management。有关更多详细信息，请参阅 Profile Management 文档。

将 Profile Management 与用户个性化层功能结合使用时，请在注销时清除用户的删除信息。您可以使用组策略对象 (GPO) 或 Delivery Controller™ (DDC) 上的策略来清除删除。

有关可用配置文件管理策略的详细信息，请参阅 Profile Management policy descriptions and defaults。

### Microsoft 系统中心配置管理器 (SCCM)

如果您将 SCCM 与用户个性化层功能结合使用，请遵循 Microsoft 关于在 VDI 环境中准备映像的准则。有关详细信息，请参阅这篇 Microsoft TechNet 文章。

### 用户层大小

用户层是精简预配磁盘，会随着磁盘空间的使用而扩展。用户层允许的默认大小为 10 GB，这是我们建议的最小值。

> **注意：**
>
> 在安装过程中，如果该值设置为零 (0)，则默认用户层大小设置为 10 GB。
>
> 如果要更改用户层大小，可以为 **用户层大小** Studio 策略输入不同的值。请参阅 **步骤 5：创建交付组自定义策略**，在 **可选：单击“用户层大小(GB)”旁边的“选择”** 下。

### 覆盖用户层大小的工具（可选）

您可以使用 Windows 工具在用户层文件共享上定义配额，从而覆盖用户层大小。

使用以下 Microsoft 配额工具之一，为名为 **Users** 的用户层目录设置硬配额：

- 文件服务器资源管理器 (FSRM)
- 配额管理器

> **注意：**
>
> 增加配额会影响新的用户层并扩展现有用户层。减少配额仅影响新的用户层。现有用户层的大小永远不会减小。

## 部署用户个性化层

部署用户个性化功能时，您可以在 Studio 中定义策略。然后，将策略分配给绑定到部署该功能的计算机目录的交付组。

如果主映像没有用户个性化层配置，则服务将保持空闲状态，并且不会干扰创作活动。

如果在主映像中设置策略，服务将尝试在主映像中运行并装载用户层。主映像将表现出意外行为和不稳定。

要部署用户个性化层功能，请按以下顺序完成以下步骤：

- 步骤 1：验证 Citrix Virtual Apps and Desktops 环境的可用性。
- 步骤 2：准备主映像。
- 步骤 3：创建计算机目录。
- 步骤 4：创建交付组。
- 步骤 5：创建交付组自定义策略。

### 步骤 1: 验证 Citrix Virtual Apps and Desktops 环境是否可用

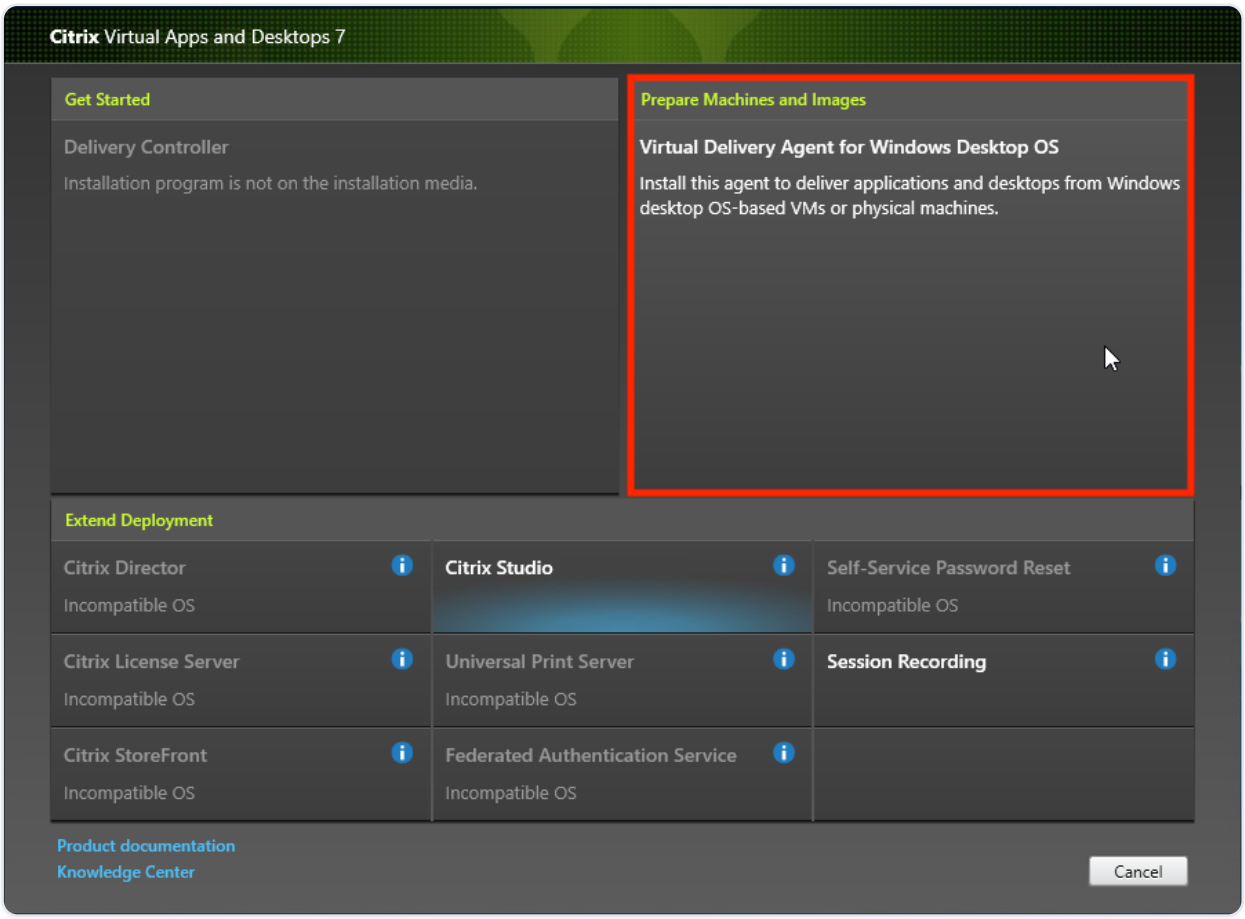
请确保您的 Citrix Virtual Apps and Desktops 环境可用于此新功能。有关设置详细信息，请参阅安装和配置 Citrix Virtual Apps and Desktops。

### 步骤 2: 准备主映像

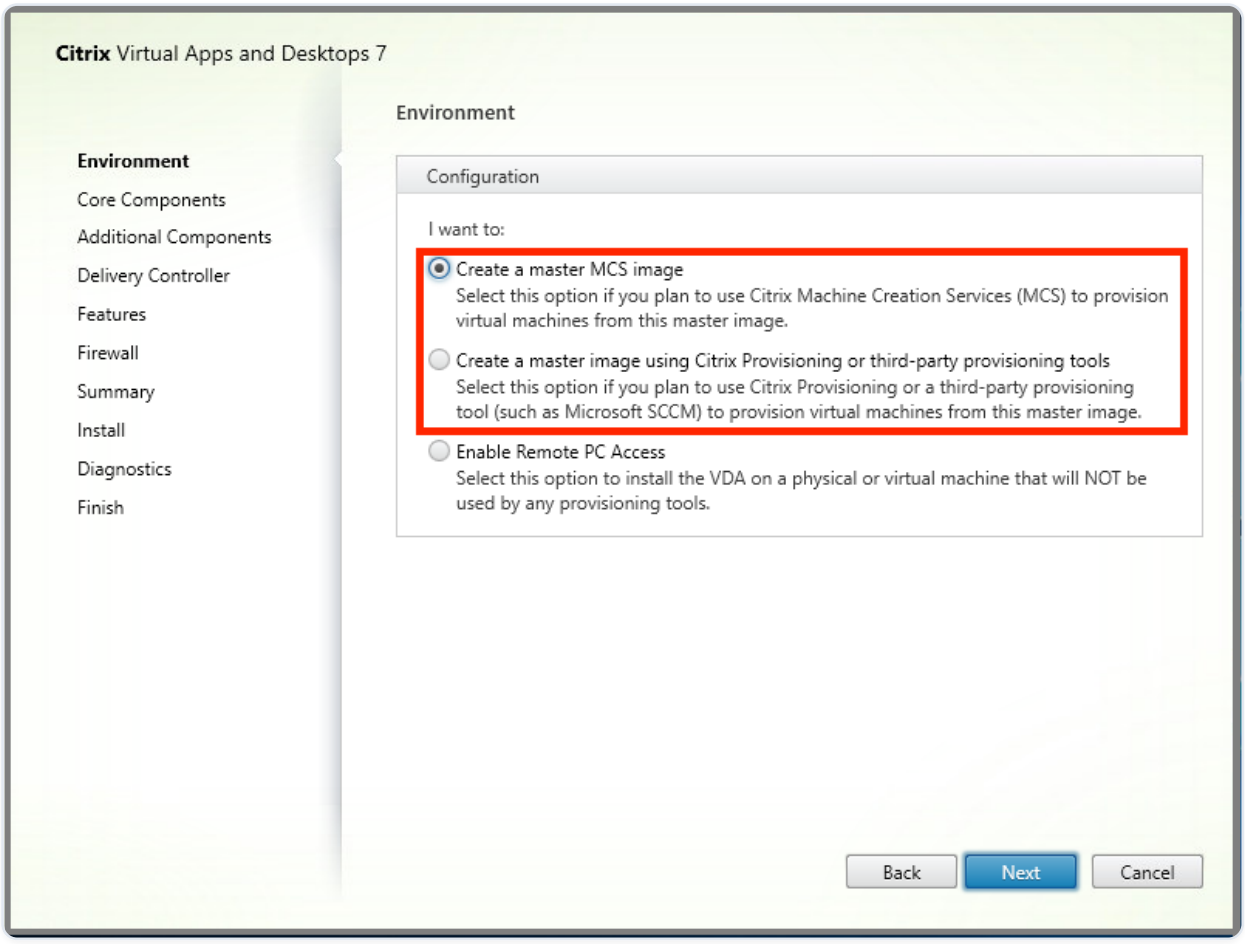
准备主映像的步骤如下：

1. 找到主映像。安装您组织的业务应用程序以及用户通常认为有用的任何其他应用程序。
2. 如果您正在部署 Server VDI，请按照 Server VDI 文章中的步骤操作。务必包含可选组件 **用户个性化层**。有关详细信息，请参阅 安装 VDA 的命令行选项。
3. 如果您使用的是 Windows 10，请安装 Virtual Delivery Agent (VDA) 1912。如果已安装旧版本的 VDA，请先卸载旧版本。安装新版本时，请务必选择并安装可选组件 **Citrix 用户个性化层**，如下所示：

   a. 单击磁贴 **适用于 Windows 桌面操作系统的 Virtual Delivery Agent**：

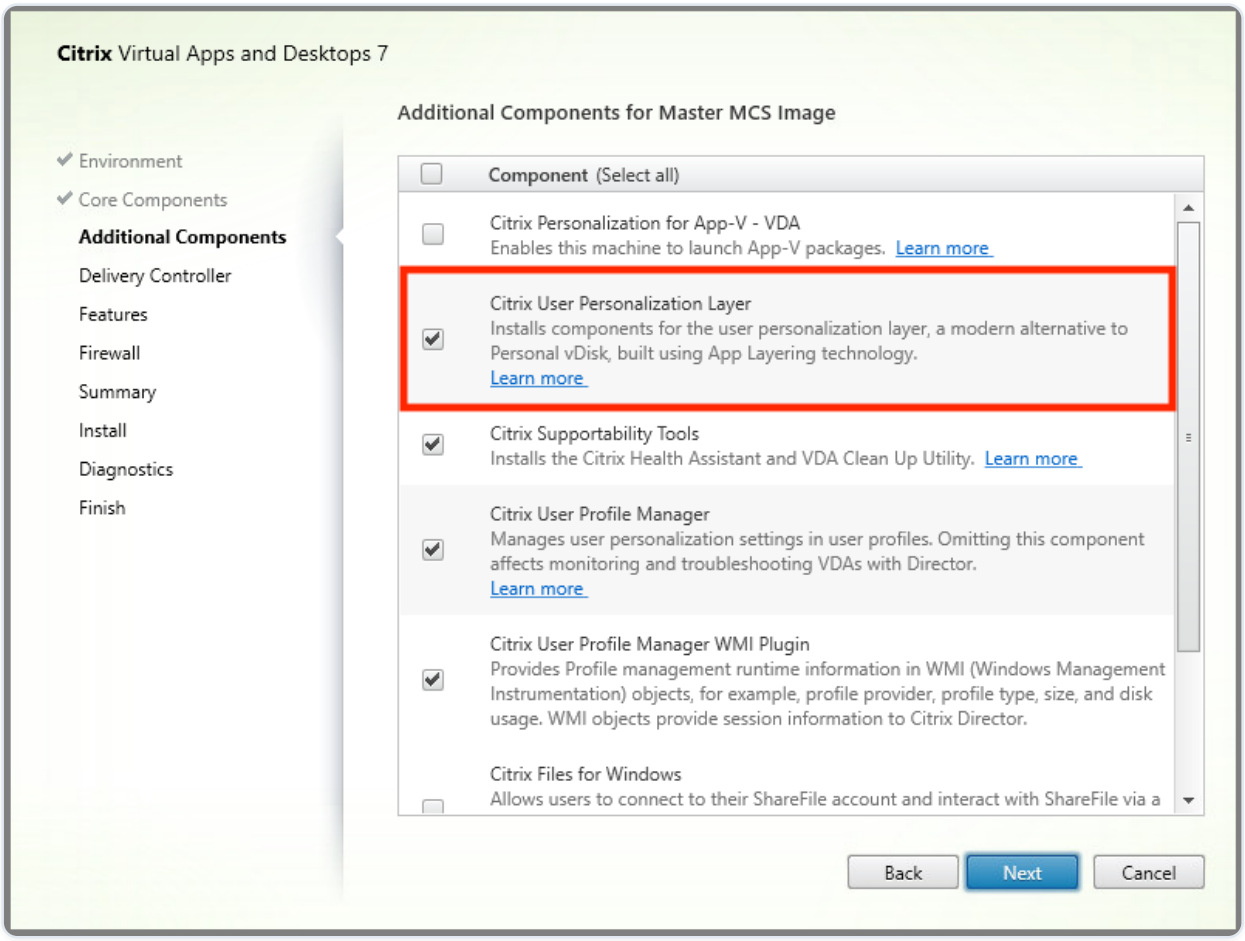



   a. **环境：** 选择“创建 MCS 主映像”或“使用 Citrix Provisioning 或第三方预配工具创建主映像”。




a. **核心组件：** 单击**下一步**。

b. **附加组件：** 选中**Citrix 用户个性化层**。




a. 单击其余安装屏幕，根据需要配置 VDA，然后单击“安装”。映像在安装过程中会重启一次或多次。

4. 保持 **Windows 更新** 禁用。用户个性化层安装程序会禁用映像上的 Windows 更新。保持更新禁用。

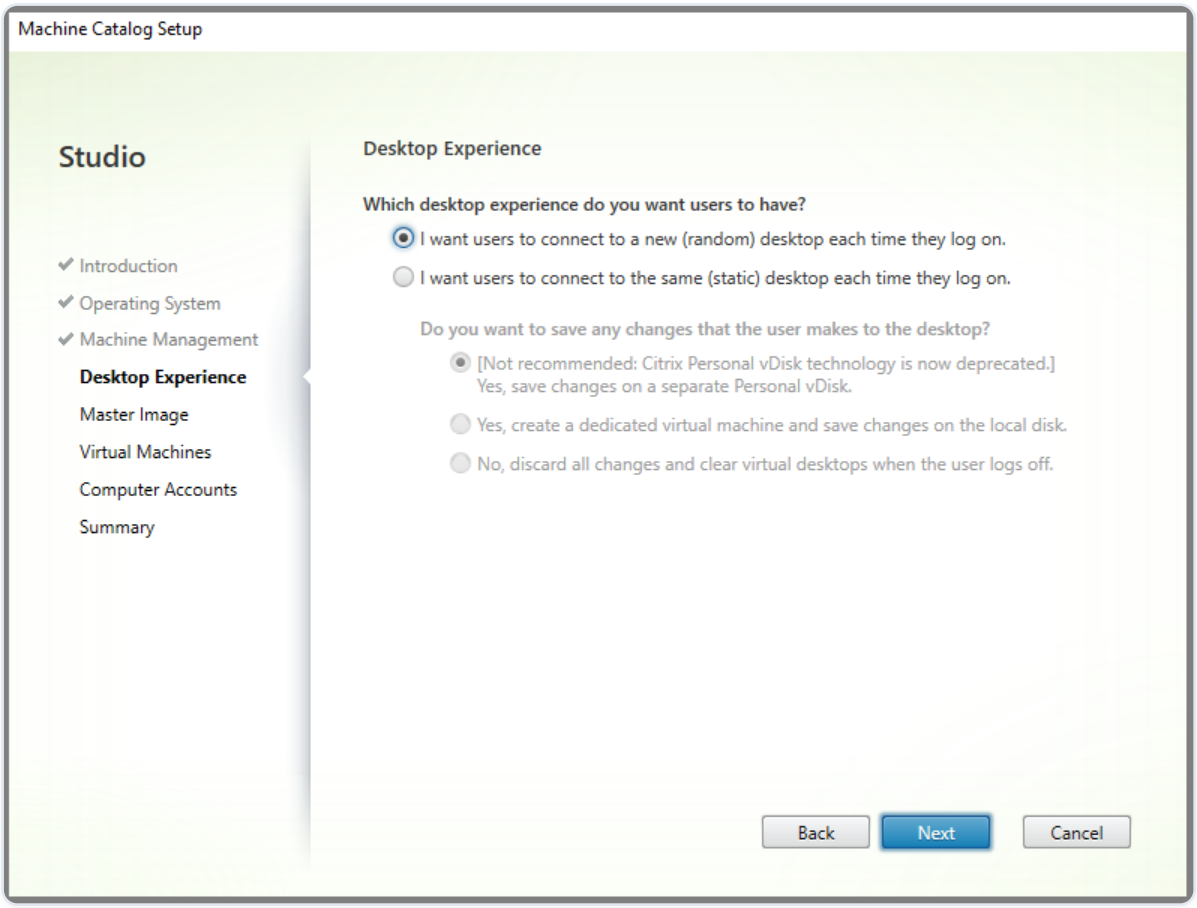
映像已准备好供您上传到 Studio。

### 步骤 3：创建计算机目录

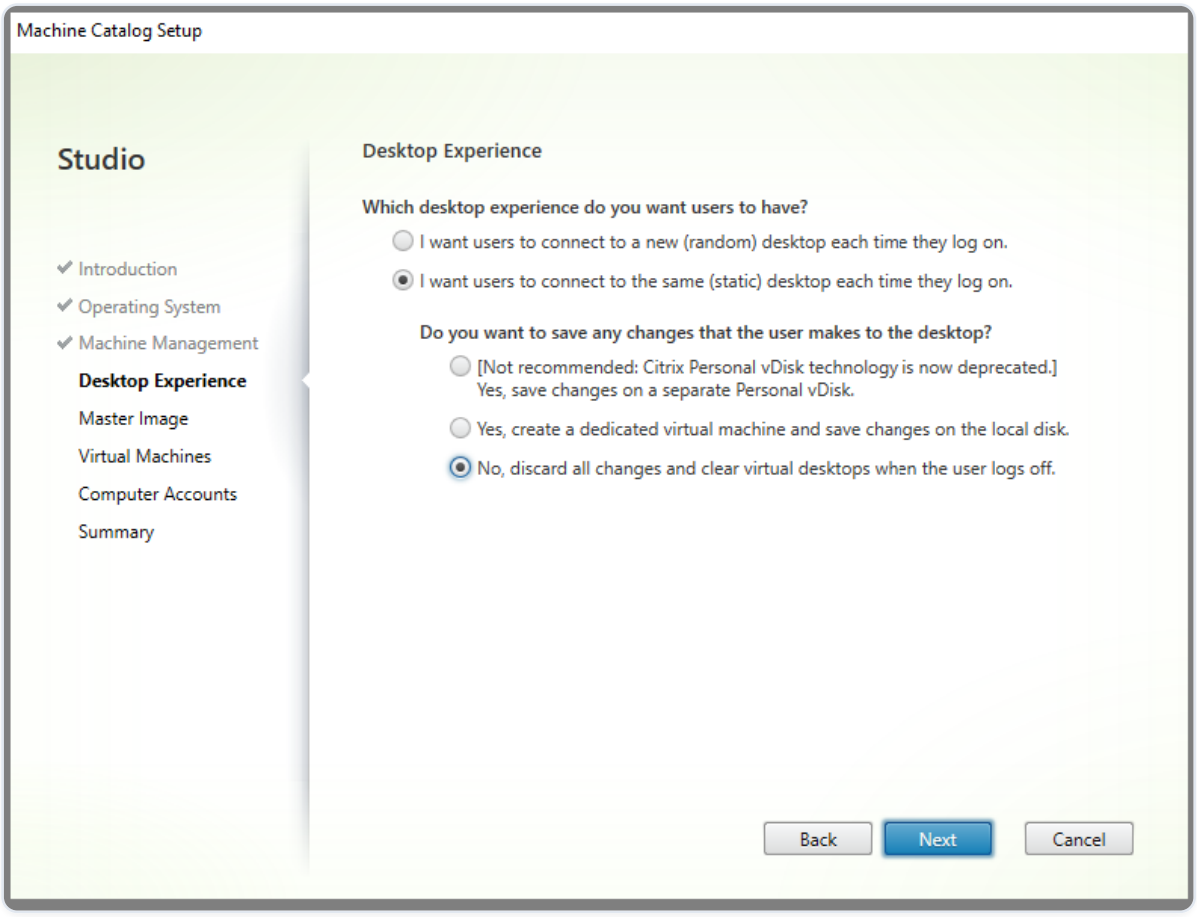
在 Studio 中，按照步骤创建计算机目录。在目录创建过程中使用以下选项：

1. 选择 **操作系统** 并将其设置为 **单会话操作系统**。
2. 选择 **计算机管理** 并将其设置为 **已进行电源管理的计算机**。例如，虚拟机或刀片式 PC。
3. 选择 **桌面体验** 并将其设置为 **随机池** 或 **静态池** 目录类型，如下例所示：

   - **随机池：**




- **静态池：** 如果选择静态池，请将桌面配置为在用户注销时丢弃所有更改并清除虚拟桌面，如以下屏幕截图所示：




> **注意：**
>
> 用户个性化层不支持配置为使用 Citrix Personal vDisk 或分配为专用虚拟机的静态池目录。

4. 如果您使用的是 MCS，请选择 **主映像** 和上一节中创建的映像的快照。
5. 根据您的环境需要配置其余目录属性。

### 步骤 4：创建交付组

创建并配置**交付组**，包括您创建的计算机目录中的计算机。有关详细信息，请参阅创建交付组。

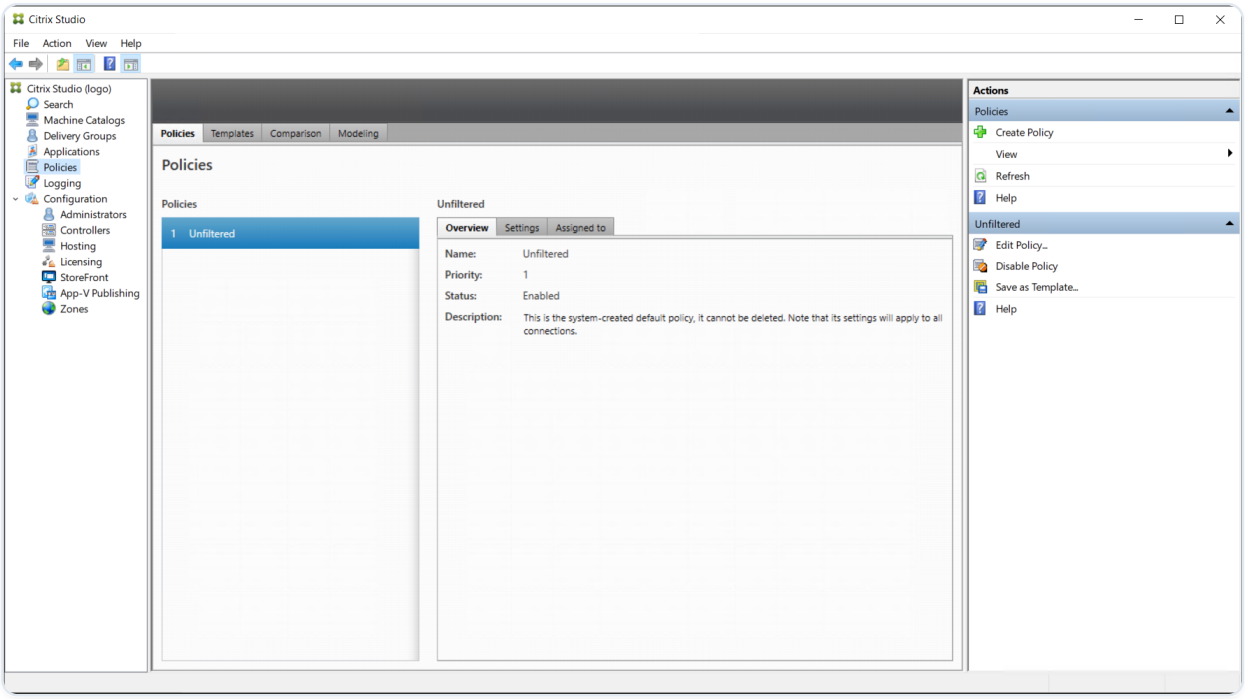
### 步骤 5：创建交付组自定义策略

为了在虚拟投递代理中启用用户层挂载，您可以使用配置参数来指定：

- 在网络上的何处访问用户层。
- 允许用户层磁盘增长到多大。

在 Studio 中将参数定义为自定义 Citrix 策略，并将其分配给您的交付组。

1. 在 Studio 中，在导航窗格中选择“策略”：

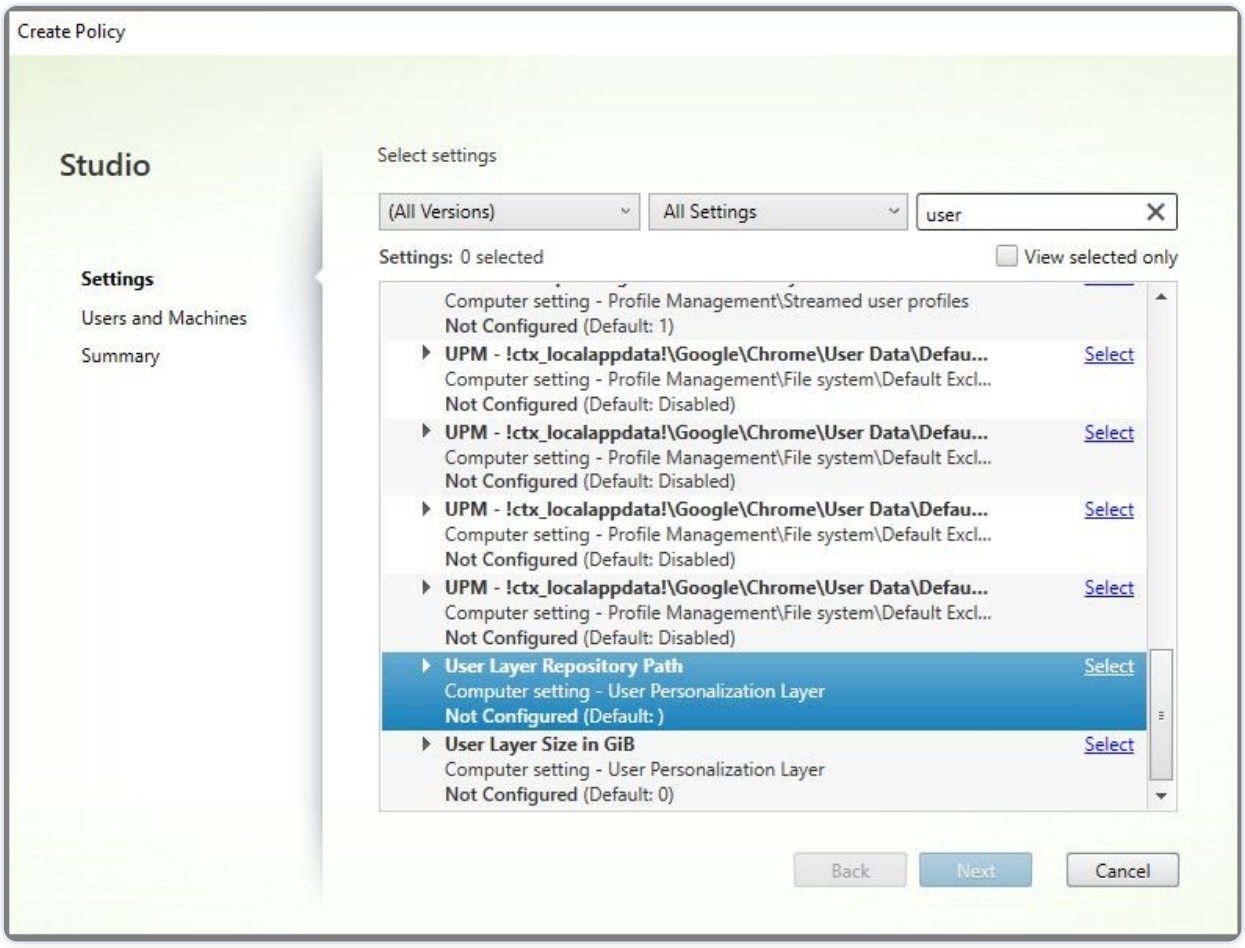



2. 在“操作”窗格中选择“创建策略”。“创建策略”窗口随即出现。
3. 在搜索字段中键入“用户层”。以下两个策略将显示在可用策略列表中：

   - 用户层存储库路径
   - 用户层大小 (GB)

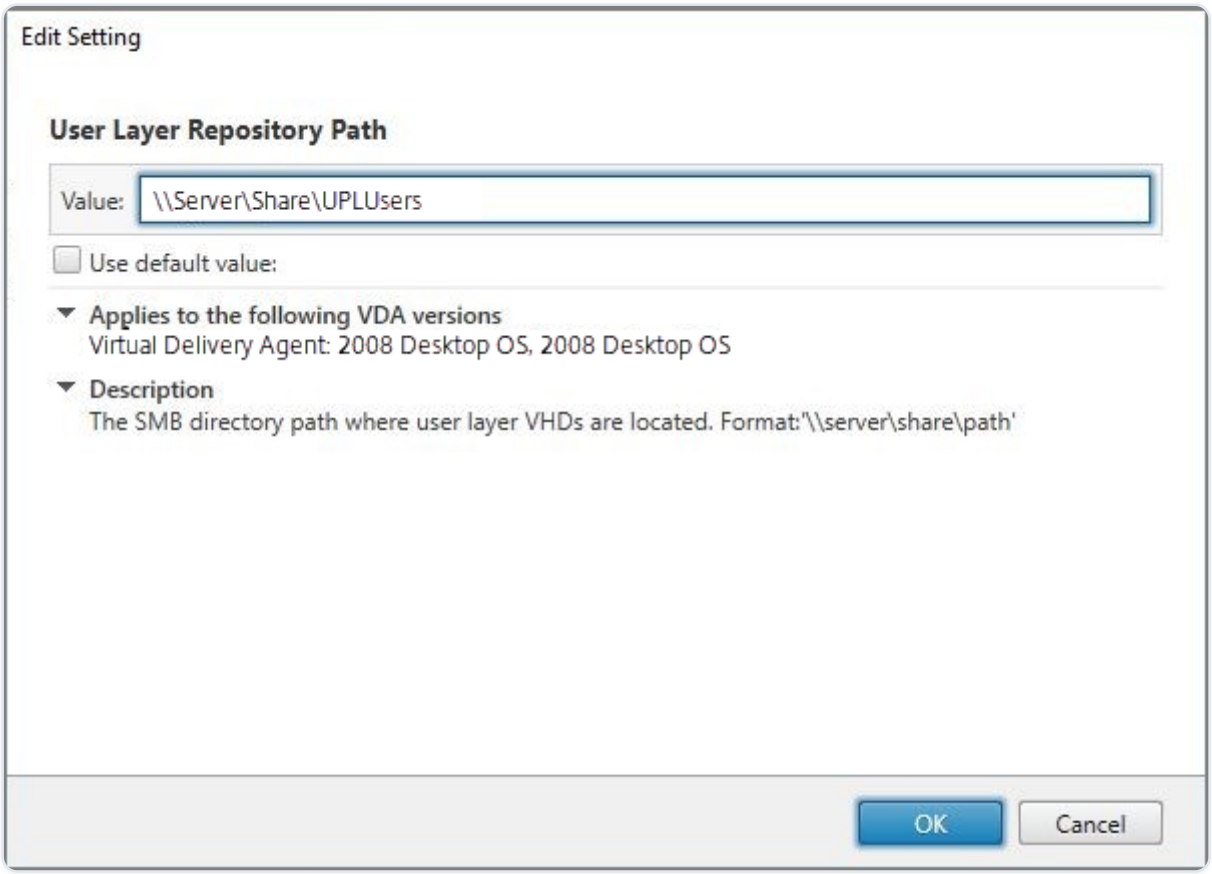
   > **注意：**
   >
   > 增大大小会影响新的用户层并扩展现有用户层。减小大小仅影响新的用户层。现有用户层的大小永远不会减小。

4. 单击“用户层存储库路径”旁边的“**选择**”。“编辑设置”窗口随即出现。



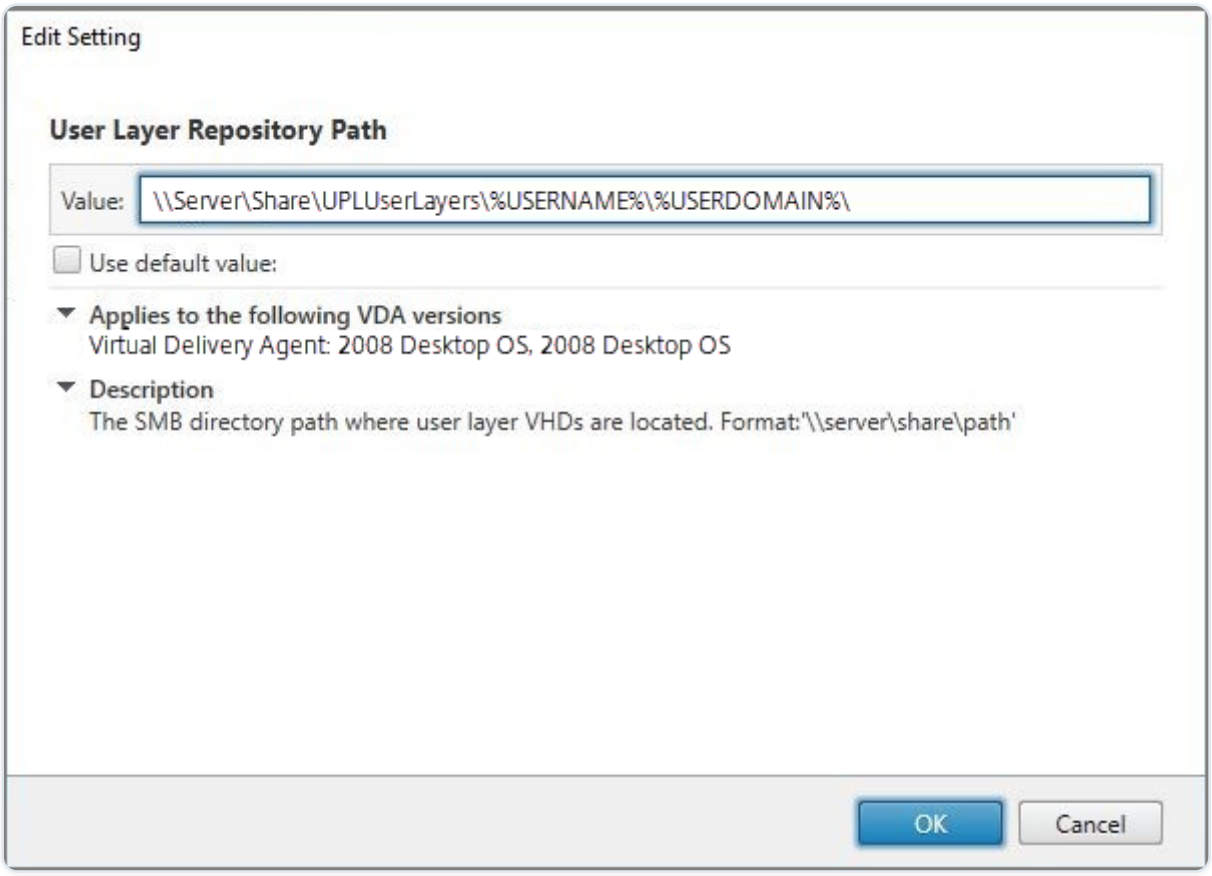

5. 在“值”字段中输入路径，然后单击“**确定**”：

   - **路径格式：** `\\server-name-or-address\share-name\folder`
   - **路径示例：** `\\Server\Share\UPLUsers`
   - **结果路径示例：** 对于 **CoolCompanyDomain** 中名为 **Alex** 的用户，路径将为：`\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

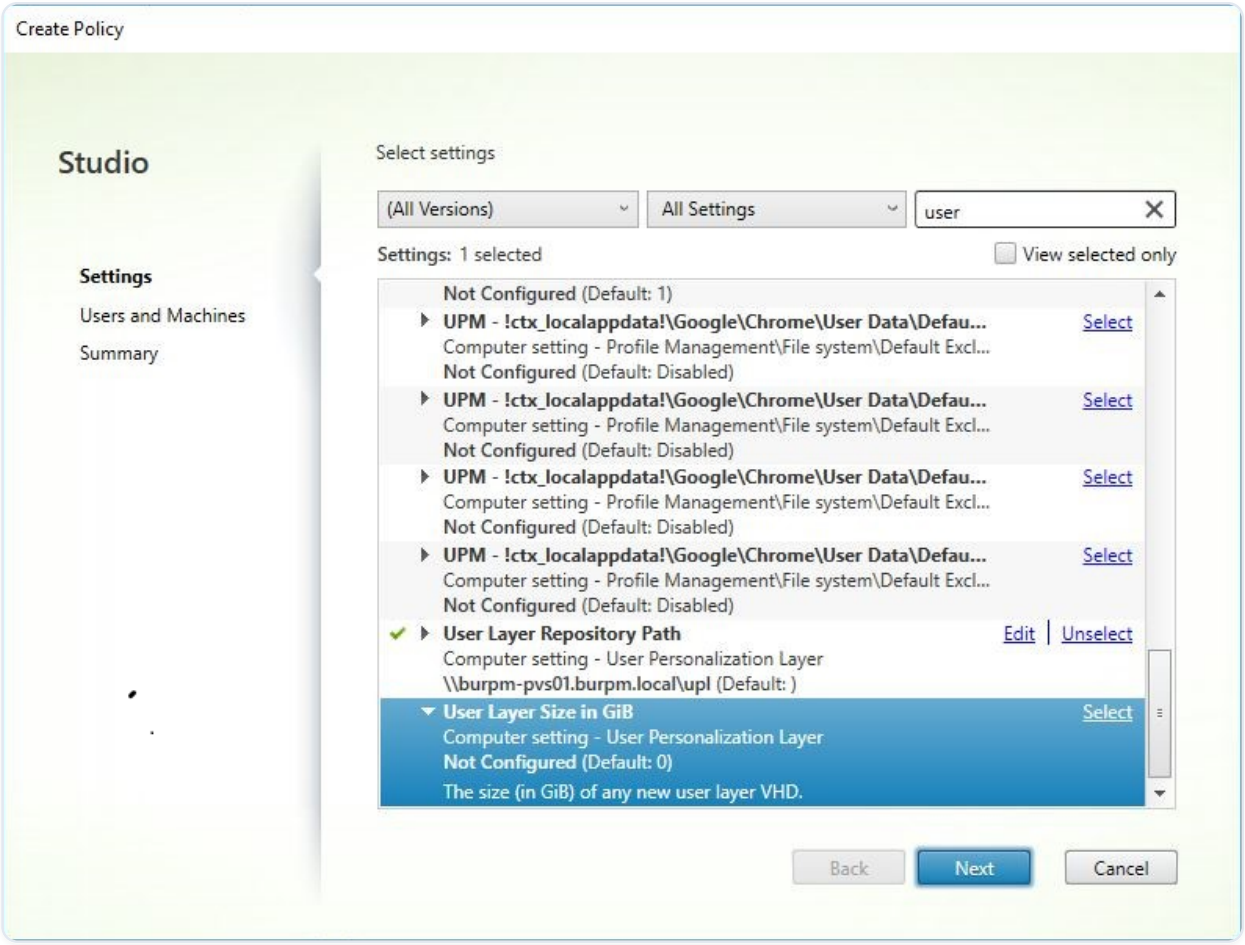



您可以使用变量 `%USERNAME%`、`%USERDOMAIN%` 以及计算机环境变量来自定义路径。展开后，这些变量将生成显式路径。

- **路径格式：** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **路径示例：** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **结果路径示例：** 对于 **CoolCompanyDomain** 中名为 **Alex** 的用户，路径将为：`\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

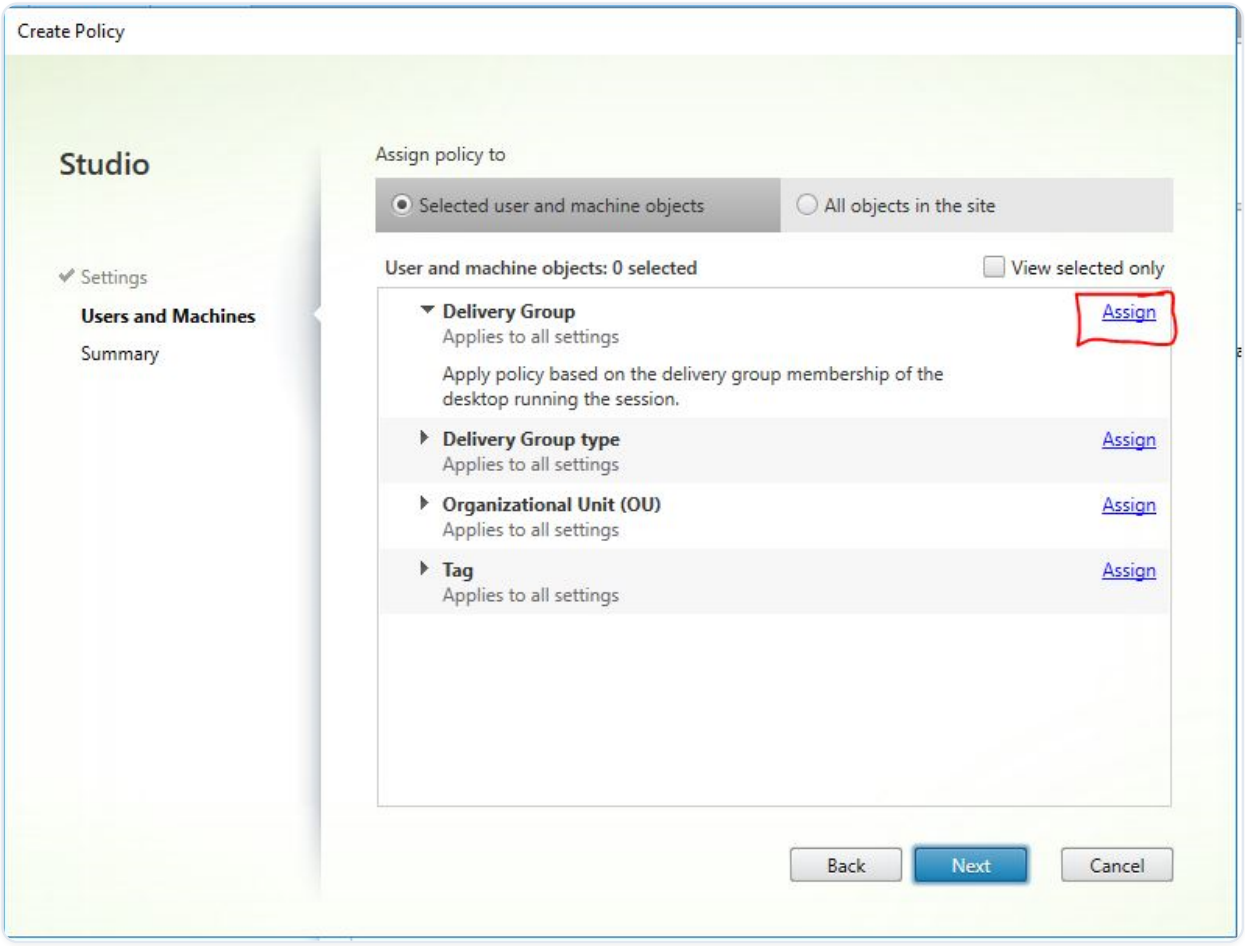



6. 可选：单击“用户层大小(GB)”旁边的“**选择**”：

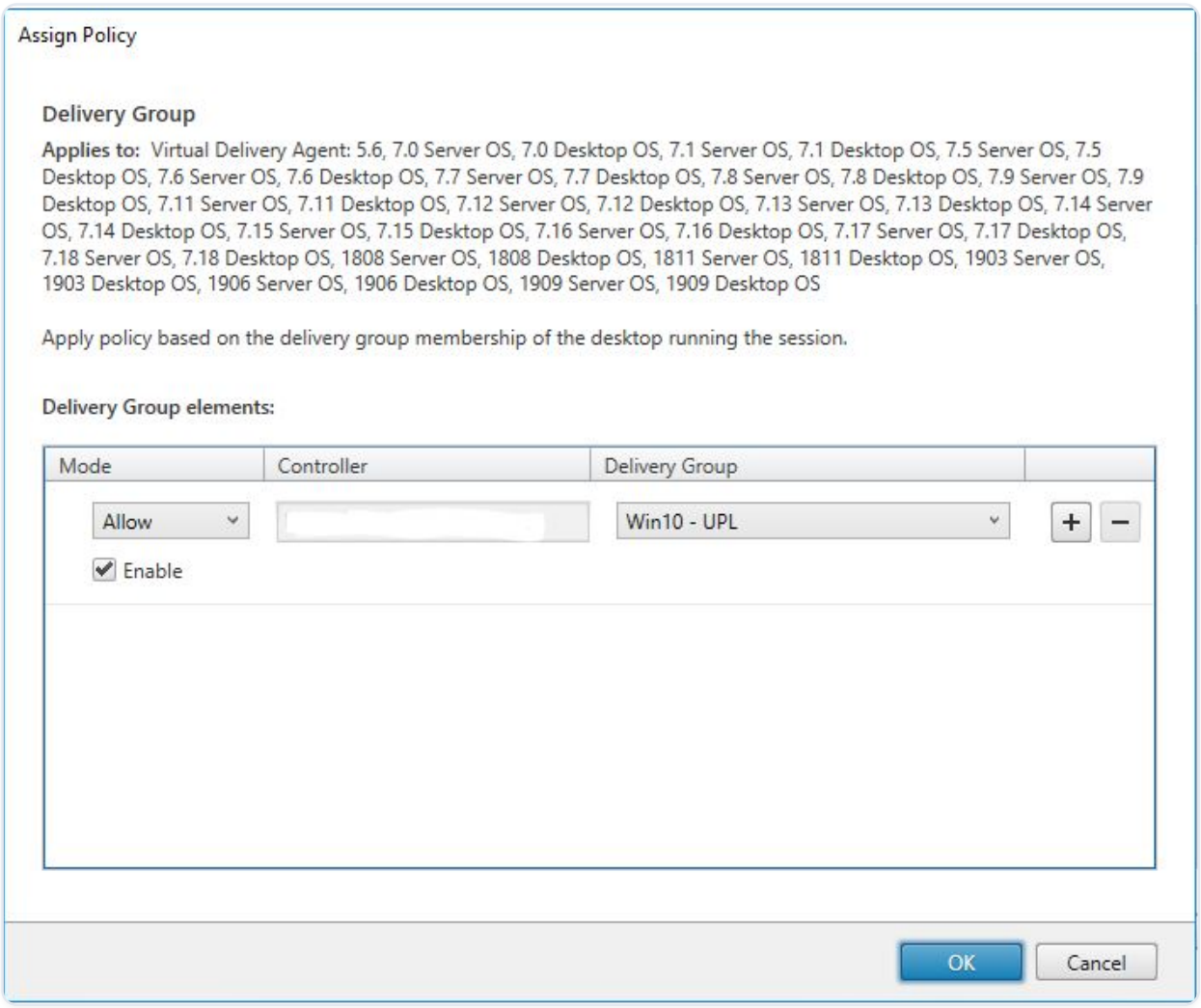


将显示“编辑设置”窗口。

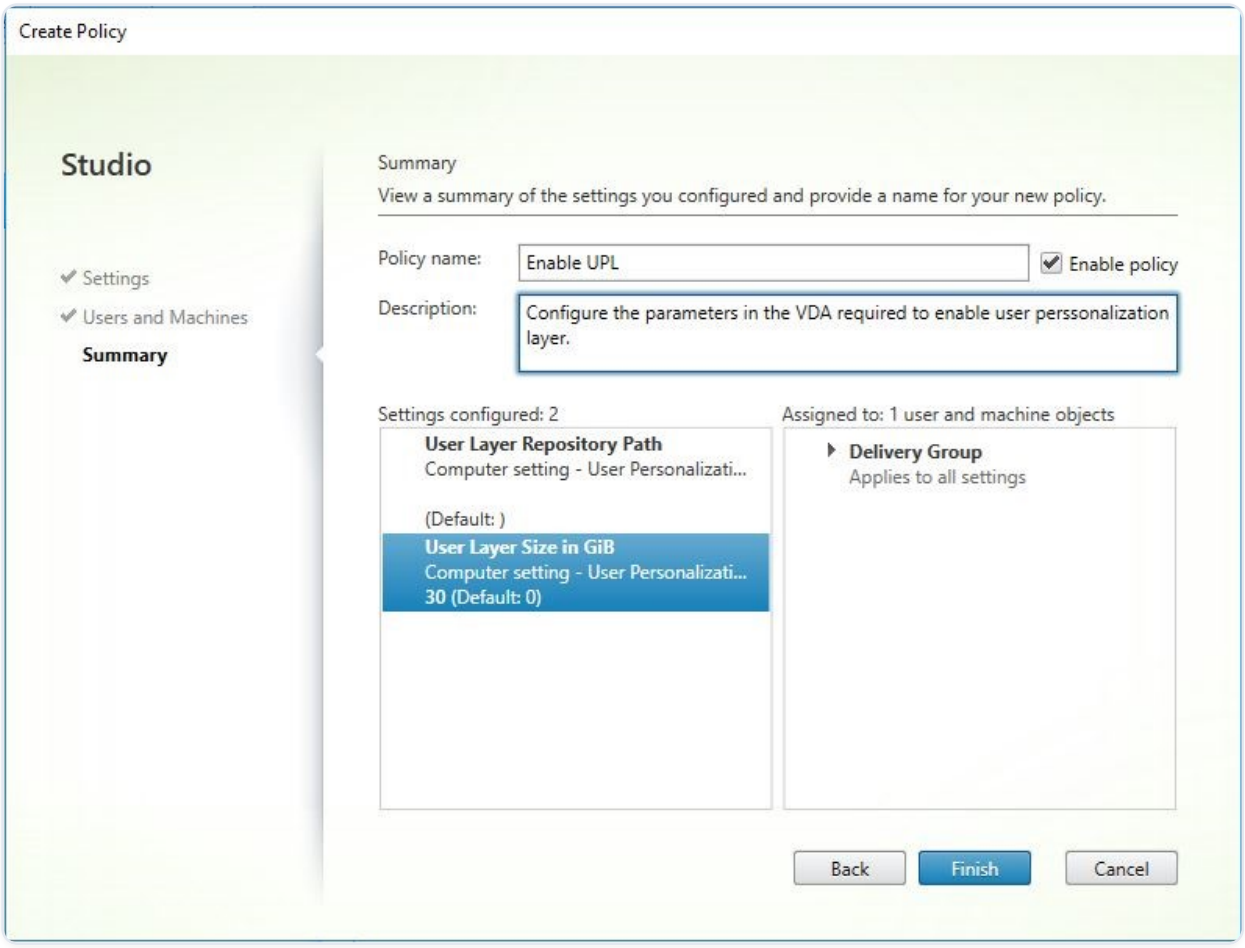
7. 可选：将默认值 **10 GB** 更改为每个用户层可增长的最大大小。单击“**确定**”。
8. 单击“**下一步**”以配置用户和计算机。单击此图像中突出显示的“交付组分配”链接：




9. 在“交付组”菜单中，选择上一节中创建的交付组。单击“确定”。




10. 输入策略名称。选中复选框以启用策略，然后单击 **完成**。




## 配置用户层文件夹上的安全设置

作为域管理员，您可以为用户层指定多个存储位置。为每个存储位置（包括默认位置）创建一个 `\Users` 子文件夹。使用以下设置保护每个位置。

| 设置名称 | 值 | 应用于 | |
|---|---|---|---|
| 创建者所有者 | 修改 | 仅子文件夹和文件 | |
| 所有者权限 | 修改 | 仅子文件夹和文件 | |
| 用户或组： | 创建文件夹/追加数据；遍历文件夹/执行文件；列出文件夹/读取数据；读取属性 | 仅选定文件夹 | |
| 系统 | 完全控制 | 选定的文件夹、子文件夹和文件 | |
| 域管理员和选定的管理员组 | 完全控制 | 选定的文件夹、子文件夹和文件 | |

## 用户层消息

当用户无法访问其用户层时，他们会收到以下通知消息之一。

- **用户层正在使用中**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **用户层不可用**

  `We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **用户注销后系统未重置**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`.

## 故障排除时使用的日志文件

日志文件 ulayersvc.log 包含用户个性化层软件的输出，其中记录了更改。

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

## 限制

在安装和使用用户个性化层功能时，请记住以下限制。

- *不要*尝试在 App Layering 中的层上部署用户个性化层软件。要么在 Citrix Virtual Apps and Desktops 中部署用户个性化层，要么在 App Layering 映像模板中启用用户层，两者不可兼得。任一过程都会生成您所需的用户层。
- *请勿*将用户个性化层功能与持久性计算机目录一起配置。
- 请 *勿* 使用会话主机。
- *不要*使用运行新操作系统安装的映像更新计算机目录（即使是相同版本的 Windows 10）。最佳实践是在创建计算机目录时使用的同一主映像中应用操作系统更新。
- *不要*使用启动时驱动程序，也不要使用任何其他早期启动个性化设置。
- 请 *勿* 将 PvD 数据迁移到用户个性化层功能。
- 请 *勿* 将现有用户层从完整的 App Layering 产品迁移到用户个性化层功能。

- 请 *勿* 更改用户层 SMB 路径以访问使用不同主操作系统映像创建的用户层。
- 当用户从会话注销并再次登录时，新会话将在池中的另一台计算机上运行。在 VDI 环境中，Microsoft Software Center 将应用程序在第一台计算机上列为“**已安装**”，但在第二台计算机上显示为“**不可用**”。

  要查找应用程序的真实状态，请指示用户在 Software Center 中选择该应用程序，然后单击 **安装**。SCCM 随后会将状态更新为真实值。
- 在启用了用户个性化层功能的 VDA 中，Software Center 偶尔会在启动后立即停止。为避免此问题，请遵循 Microsoft 关于 在 XenDesktop VDI 环境中实施 SCCM 的建议。此外，请确保在启动 Software Center 之前 `ccmexec` 服务正在运行。
- 在组策略（计算机设置）中，用户层设置会覆盖应用于主映像的设置。因此，您使用 GPO 在计算机设置中所做的更改并非总是在用户下次会话登录时出现。

  要解决此问题，请创建一个用户登录脚本，该脚本发出以下命令：

  ```
  gpupdate /force
  ```

  例如，一位客户将以下命令设置为在每次用户登录时运行：

  ```
  gpudate /Target:Computer /force
  ```

  为获得最佳结果，请在用户登录后，直接在用户层上应用对计算机设置的更改。
- 域用户帐户不得是最后登录到主映像的用户。否则，从该映像预配的计算机将出现问题。

# 删除组件

要删除组件，Citrix® 建议使用 Windows 的“程序和功能”功能。或者，您可以使用命令行或安装介质上的脚本删除组件。

删除组件时，不会删除先决条件，也不会更改防火墙设置。例如，当您删除 Delivery Controller™ 时，SQL Server 软件和数据库不会被删除。

如果您从包含 Web Interface 的早期部署升级了控制器，则必须单独删除 Web Interface 组件。您不能使用安装程序删除 Web Interface。

有关删除未在下面提及的功能的信息，请参阅该功能的文档。

## 准备工作

在删除控制器之前，请将其从站点中删除。有关详细信息，请参阅 删除控制器。

在删除 Studio 和 Director 之前，请关闭它们。

## 使用 Windows 的删除或更改程序功能删除组件

从 Windows 的删除或更改程序功能中：

- 要删除 Controller、Studio、Director、License Server 或 StoreFront，请右键单击 **Citrix Virtual Apps *version*** 或 **Citrix Virtual Apps and Desktops™ *version***，然后选择**卸载**。安装程序将启动。选择要删除的组件。

  或者，您可以通过右键单击 **Citrix StoreFront** 并选择**卸载**来删除 StoreFront™。
- 要删除 VDA，请右键单击 **Citrix Virtual Delivery Agent *version*** 并选择**卸载**。安装程序将启动，您可以选择要删除的组件。默认情况下，删除后计算机将自动重启。
- 要删除 Universal Print Server，请右键单击 **Citrix Universal™ Print Server** 并选择**卸载**。

## 使用命令行删除核心组件

在 `\x64\XenDesktop Setup` 目录中，运行 `XenDesktopServerSetup.exe` 命令。

- 要删除一个或多个组件，请指定 `/remove` 和 `/components` 选项。
- 要删除所有组件，请指定 `/removeall` 选项。

有关命令和参数的详细信息，请参阅 使用命令行安装。

例如，以下命令将删除 Studio。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```

## 使用命令行删除 VDA

从 `\x64\XenDesktop Setup` 目录运行 `XenDesktopVdaSetup.exe` 命令。

- 要删除一个或多个组件，请使用 `/remove` 和 `/components` 选项。例如，要删除 VDA 和 Citrix Workspace 应用程序，请使用 `/remove /components vda,plugin`。
- `/removeall` 选项仅删除 VDA。它不会删除 Citrix Workspace 应用程序。

有关命令和参数的详细信息，请参阅使用命令行安装。

默认情况下，计算机在删除后会自动重新启动。

要使用 Active Directory 中的脚本删除 VDA，请参阅使用脚本安装或删除 VDA。

# 升级和迁移

**注意：**

基于文件的许可系统，传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于 Citrix 产品套件中产品激活的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 Citrix 本地组件的唯一方式。为了保持受支持，您的 Citrix Virtual Apps and Desktops 部署必须是 LAS 兼容版本。LAS 兼容的最低所需 CVAD 版本为：

- CVAD 2203 LTSR CU7
- CVAD 2402 LTSR CU3
- CVAD 2507 LTSR
- CVAD 2411

如果您有任何疑问或疑虑，请联系客户服务。对于不遵守这些要求的行为，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法上的任何其他补救措施。这些要求不适用于法律或法规禁止的情况。

**注意：**

- **“版本交叉”警告**

  请注意，不同的 LTSR 版本通常在维护周期上存在重叠。在启动升级之前，您必须验证当前累积更新 (CU) 和目标 LTSR（或其后续 CU）的**发布日期**。如果当前环境的发布日期**晚于**目标 LTSR 或 LTSR CU 的发布日期，Citrix 强烈建议等待较新 LTSR 的下一个 CU。否则，可能会导致旧代码覆盖现有的安全更新、稳定性补丁和功能增强。

- **“不受支持状态”条款**

> 尝试升级到发布日期较早的版本在技术上被视为**核心组件的降级**。这种特定配置可能会导致**“部分成功”**状态。

# 简介

升级会将您的部署更改为 Citrix Virtual Apps and Desktops 7 当前版本 (CR)，而无需设置新计算机或站点。这种升级称为就地升级。

升级可让您访问符合条件的最新功能和技术。升级还可以包含早期版本中的修复、澄清和增强功能。

## 升级概述

1. 在开始升级之前，请查看升级部署文章。该文章是了解如何准备和实施升级的主要信息来源。
2. 完成准备指南。
3. 运行安装程序以升级核心组件。
4. 升级系统数据库和站点。
5. 升级映像上的 VDA（或直接在计算机上升级）。
6. 升级其他组件。

每个准备和升级步骤都在 升级部署 中详细说明。

# 可升级的版本

您可以从以下版本升级到 Citrix Virtual Apps and Desktops™ 2203 LTSR：

- XenApp and XenDesktop 7.15 LTSR CU5 到最新的 CU
- Virtual Apps and Desktops 1912（无论是否包含 CU，直至并包括最新的 CU）
- 当前支持的 Citrix Virtual Apps and Desktops CR 版本

Citrix Virtual Apps and Desktops 当前版本支持可在 升级部署 中找到。

# 常见问题

本节回答了一些关于升级 Citrix Virtual Apps and Desktops 的常见问题。

- **升级 Virtual Apps and Desktops 环境的正确顺序是什么？**

  有关推荐升级顺序的图示和说明，请参阅升级顺序和升级过程。

- **我的站点有多个交付控制器（位于不同区域）。如果我只升级其中一部分，会发生什么？我是否必须在同一维护时段内升级站点中的所有控制器？**

  最佳做法是在同一维护时段内升级所有交付控制器，因为每个控制器上的各种服务会相互通信。保留不同版本可能会导致问题。在维护时段内，我们建议您升级一半的控制器，然后升级站点，再升级剩余的控制器。（有关详细信息，请参阅升级过程。）

- **我可以直接升级到最新版本，还是必须进行增量升级？**

  您几乎总是可以直接升级到最新版本并跳过中间版本，除非您要升级到的版本的**新增功能**文章中明确说明。请参阅升级指南。

- **客户能否从长期服务版本 (LTSR) 环境升级到当前版本？**

  可以。客户无需长时间停留在长期服务版本上。客户可以根据业务需求和功能，将 LTSR 环境迁移到当前版本。

- **是否允许混合使用不同版本的组件？**

  在每个站点中，Citrix 建议将所有组件升级到同一版本。尽管您可以使用某些组件的早期版本，但最新版本中的所有功能可能无法使用。有关详细信息，请参阅混合环境注意事项。

- **当前版本必须多久升级一次？**

  当前版本在发布日期后 6 个月达到维护终止 (EOM)。Citrix 建议客户采用最新的当前版本。当前版本在发布日期后 18 个月达到生命周期终止 (EOL)。有关详细信息，请参阅当前版本生命周期。

- **建议：升级到 LTSR 还是 CR？**

  当前版本 (CR) 提供最新、最具创新性的应用程序、桌面和服务器虚拟化功能。这使您能够保持领先技术并超越竞争对手。

  长期服务版本 (LTSR) 非常适合希望长时间保留相同基础版本的大型企业生产环境。

  有关详细信息，请参阅服务选项。

- **我需要升级我的许可证吗？**

  确保当前许可证日期未过期，并且对您要升级到的版本有效。请参阅 CTX111618。有关续订的信息，请参阅 客户成功服务续订许可证。

- **升级需要多长时间？**

  升级部署所需的时间因基础结构和网络而异。因此，我们无法提供确切的时间。

- **最佳实践是什么？**

确保您理解并遵循 准备指南。

- **支持哪些操作系统？**

  您要升级到的版本的 系统要求 文章列出了受支持的操作系统。

  如果您当前的部署使用不再受支持的操作系统，请参阅 早期操作系统。

- **支持哪些版本的 VMware vSphere (vCenter + ESXi)？**

  CTX131239 列出了受支持的主机和版本，以及已知问题的链接。

- **我的版本何时终止生命周期 (EOL)？**

  查看 产品矩阵。

- **最新版本有哪些已知问题？**

  - Citrix 虚拟应用和桌面
  - StoreFront
  - Citrix 预配
  - Citrix 许可证服务器
  - 适用于 Windows 的 Citrix Workspace 应用程序

# 更多信息

长期服务版本 (LTSR) 部署更新使用累积更新 (CU)。CU 会更新 LTSR 的基线组件，并且每个 CU 都包含其自己的元安装程序。

每个 CU 都有专门的文档。例如，对于 7.15 LTSR，请在该 LTSR 的“**新增功能**”页面上查找最新 CU 的链接。每个 CU 页面都包含支持的版本信息、说明以及 CU 下载包的链接。

# 迁移

## 迁移到云

您可以使用适用于 Citrix Virtual Apps and Desktops 的自动配置工具将本地部署迁移到云。有关详细信息，请参阅迁移到云。

## 旧版迁移

迁移是将数据从早期部署移动到较新版本。此过程包括安装较新的组件并创建新站点、从旧场导出数据，然后将数据导入新站点。

没有支持的工具或脚本可用于迁移 XenApp 和 XenDesktop® 版本，或迁移早期 Citrix Virtual Apps and Desktops 版本。

有关早期 XenApp 6.x 迁移内容，请参阅以下内容。这些脚本不受支持或维护。

- XenApp 6.x 版本的开源迁移脚本可在 `<https://github.com/citrix/xa65migrationtool>` 获取。Citrix 不支持或维护这些迁移脚本。
- 有关“**7.x 中的更改**”、“**将 XenApp 6.5 工作程序升级到新 VDA**”和“**迁移 XenApp 6.x**”，请参阅 `<https://docs.citrix.com/zh-cn/legacy-archive/citrix-virtual-apps-and-desktops.html>` 处的 Citrix Virtual Apps and Desktops 旧版存档。

# 升级部署

> **注意：**

> 传统上用于激活各种本地组件的基于文件的许可系统将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活 Citrix 产品套件的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 Citrix 本地组件的唯一方式。为了获得支持，您的 Citrix Virtual Apps and Desktops 部署必须是 LAS 兼容版本。兼容 LAS 的最低所需 CVAD 版本为：

> - CVAD 2203 LTSR CU7
> - CVAD 2402 LTSR CU3
> - CVAD 2507 LTSR
> - CVAD 2411

> 如果您有任何疑问或疑虑，请联系客户服务。如果不遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法上的任何其他补救措施。这些要求不适用于法律或法规禁止的情况。

## 简介

您可以将某些部署升级到更新版本，而无需首先设置新计算机或站点。这称为就地升级。

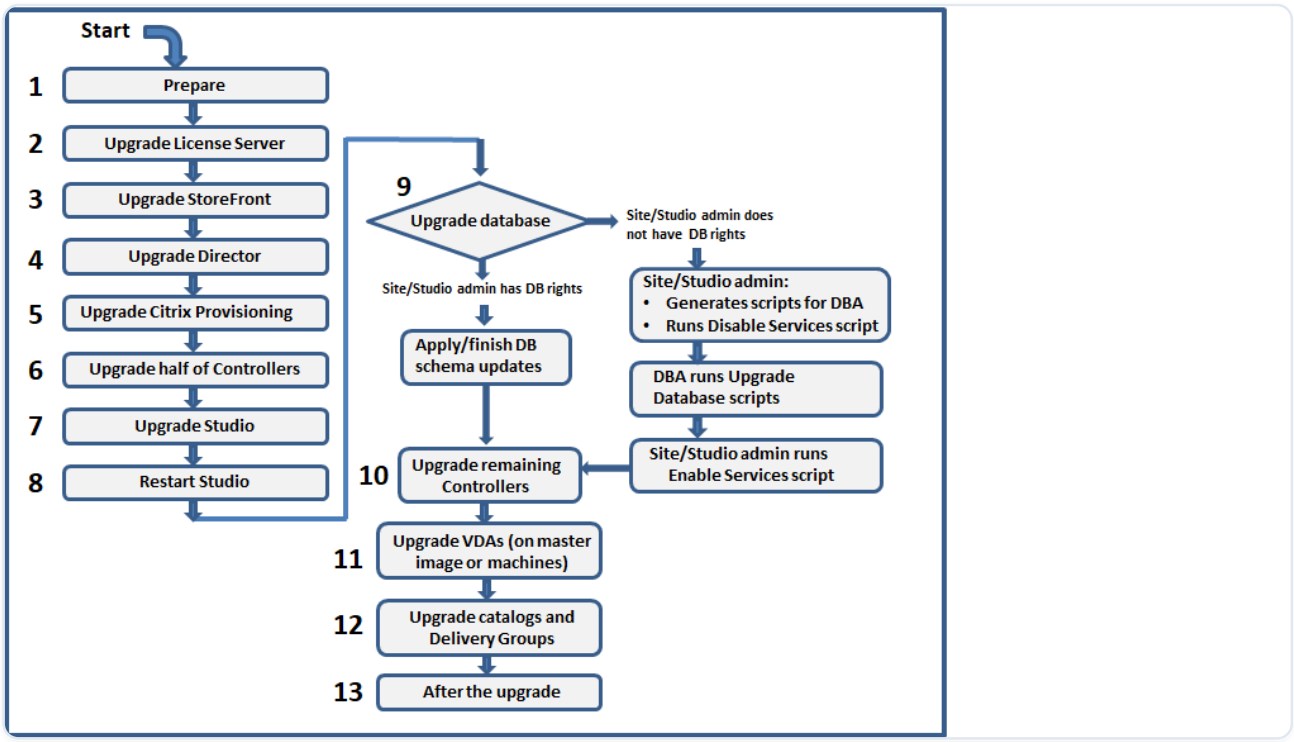
要开始升级，请运行新版本的安装程序以升级以前安装的核心组件、VDA 和某些其他组件。然后升级数据库和站点。

如果提供了更新版本，您可以升级任何可以使用完整产品安装程序（以及独立 VDA 安装程序）安装的组件。对于未使用完整产品安装程序安装的其他组件（例如 Citrix Provisioning™ 和 Profile Management），请参阅该组件的文档以获取指导。有关主机升级，请参阅相应的文档。

在开始升级之前，请查看本文中的所有信息。

## 升级顺序

下图显示了升级序列的步骤。升级过程 包含图中每个步骤的详细信息。




**注意：**

为避免故障，您必须在执行任何与预配和交付组相关的任务（例如创建新计算机目录、删除计算机目录、更新交付组中的计算机等）之前升级所有 Delivery Controller 和数据库。

## 混合权利许可证

混合权利许可证是基于期限的订阅许可证，当客户从永久许可证过渡或升级到云服务订阅时，除了云服务订阅之外，还会提供此类许可证。您还可以随 DaaS 订阅购买混合权利附加组件。

如果您拥有具有 SaaS 属性的混合权利许可证，当您升级到 Citrix Virtual Apps and Desktops™ LTSR 2203 及更高版本时，您将有资格访问 Citrix Virtual Apps and Desktops LTSR 1912 不具备的功能。这些功能包括在公共云（例如 Microsoft Azure、AWS EC2 和 Google Cloud）中预配和托管

工作负载。在部署新的许可证文件之前，请将您的许可证服务器更新到最新版本，未能满足此先决条件可能会在站点升级和创建期间导致错误或建议

如果您从 Citrix Virtual Apps and Desktops LTSR 1912 升级到 LTSR 2203，并且有权获得具有 Azure、AWS 或 Google Cloud 连接的新混合权利许可证，请务必遵循以下步骤。否则，您的 2203 元安装程序将阻止您的升级：

> **注意：**
>
> - 您会收到一封包含新许可证代码的电子邮件。有关详细信息，请参阅使用许可证访问代码。
> - 您现有的许可证将被撤销。必须从许可证服务器中删除已撤销的许可证，然后安装新许可证。有关详细信息，请参阅删除许可证文件。

1. 转到 citrix.com 管理许可证门户，并下载启用了云预配权限（SaaS 属性）的新混合权利许可证文件。有关详细信息，请参阅下载许可证。下图显示了“增量”部分中具有 SaaS 属性的混合权利许可证文件。

```
INCREMENT XDT_PLT_CCS CITRIX 2022.1201 01-dec-2022 5 \
    VENDOR_STRING=;LT=RetailS;GP=720;PSL=10;CL=VDS,VDA,VDE,VDP,SaaS:SA=0;ODP=0;NUDURMIN=2880;NUDURMAX=525600;AP=ADMIN/INT/14
    OVERDRAFT=1 DUP_GROUP=V ISSUED=18-dec-2005 NOTICE="Citrix \
    Systems Inc." SN=RetailSSaaS SIGN="..."
```

2. 在许可证服务器上安装混合权利许可证文件。有关详细信息，请参阅安装许可证。
3. 如果许可证版本或模型发生更改，请务必运行 broker 命令来设置版本和模型，然后开始就地升级。有关 Broker 命令的详细信息，请参阅Broker PowerShell SDK 部分。

有关 Citrix Virtual Apps and Desktops 当前版本和长期服务版本对公共云支持的更多信息，请参阅 CTX270373。

## 升级过程

大多数主要产品组件可以通过在包含组件的计算机上运行产品安装程序进行升级。

如果一台计算机包含多个组件（例如 Studio 和许可证服务器），则如果产品介质包含其软件的较新版本，该计算机上的所有组件都将升级。

要使用安装程序：

- 要运行完整产品安装程序的图形界面，请登录到计算机，然后插入介质或装载新版本的 ISO 驱动器。双击 **AutoSelect**。

- 要使用命令行界面，请发出相应的命令。请参阅使用命令行安装。

### 步骤 1：准备

在开始升级之前，请确保您已做好准备。阅读并完成所有必要的任务：

- 删除 PVD、AppDisks™ 和不受支持的主机
- 具有 PvD 或 AppDisk 组件的 VDA
- 限制
- 混合环境注意事项
- 早期操作系统
- 准备工作
- 初步站点测试
- SQL Server 版本检查

### 步骤 2：升级许可证服务器

如果安装包含新版本的 Citrix 许可证服务器软件，请先升级此组件，然后再升级任何其他组件。

如果您尚未确定您的许可证服务器是否与新版本兼容，则必须在升级任何其他核心组件之前在许可证服务器上运行安装程序。

### 步骤 3：升级 StoreFront™

如果安装介质包含新版本的 StoreFront 软件，请在包含 StoreFront 服务器的计算机上运行安装程序。

- 在图形界面中，从“**扩展部署**”部分选择“**Citrix StoreFront**”。
- 从命令行运行 `CitrixStoreFront-x64.exe`，该文件位于 Citrix Virtual Apps and Desktops 安装介质的 `x64` 文件夹中。

### 步骤 4：升级 Director

如果安装介质包含新版本的 Director 软件，请在包含 Director 的计算机上运行安装程序。

### 步骤 5：升级 Citrix Provisioning

Citrix Provisioning 安装介质独立于 Citrix Virtual Apps and Desktops 安装介质提供。要了解如何安装和升级 Citrix Provisioning 服务器和目标设备软件，请参阅 Citrix Provisioning 产品文档。

### 步骤 6：升级一半的 Delivery Controller

例如，如果您的站点有四个 Controller，请在其中两个上运行安装程序。

保持一半的 Controller 处于活动状态可让用户访问站点。VDA 可以向剩余的 Controller 注册。有时，由于可用的 Controller 较少，站点的容量可能会降低。升级仅在最终数据库升级步骤中导致建立新客户端连接的短暂中断。在整个站点升级完成之前，已升级的 Controller 无法处理请求。

如果您的站点只有一个 Controller，则在升级期间它将无法运行。

在实际升级开始之前，将在第一个 Controller 上运行初步站点测试。有关详细信息，请参阅 初步站点测试。

### 步骤 7：升级 Studio

如果您尚未升级 Studio（因为它与另一个组件位于同一台计算机上），请在包含 Studio 的计算机上运行安装程序。

### 步骤 8：重新启动 Studio

重新启动已升级的 Studio。升级过程将自动恢复。

### 步骤 9：升级数据库和站点

> **注意：**
>
> 为避免故障，您必须在执行任何预配和交付组相关任务（例如创建新计算机目录、删除计算机目录、更新交付组中的计算机等）之前，升级所有 Delivery Controller 和数据库。

> 检查 (#preparation) 以了解更新 SQL Server 数据库架构所需的权限。

- 如果您有足够的权限更新 SQL Server 数据库架构，则可以启动自动数据库升级。继续执行 (#upgrade-the-database-and-site-automatically)。
- 如果您没有足够的数据库权限，则可以启动使用脚本的手动升级，并在数据库管理员（具有所需权限的人员）的帮助下进行。对于手动升级，Studio 用户生成脚本，然后运行启用和禁用服务的脚本。数据库管理员使用 SQLCMD 实用程序或 SQLCMD 模式下的 SQL Server Management Studio 运行其他更新数据库架构的脚本。继续执行 (#upgrade-the-database-and-site-manually)。
- 如果您有多区域部署并希望自动升级数据库和站点，Citrix 建议在托管站点 SQL Server 数据库的同一区域中执行 dbschema 升级。否则，自动升级数据库和站点可能会失败。

Citrix 强烈建议您在升级前备份数据库。请参阅 CTX135207。在数据库升级期间，产品服务将被禁用。在此期间，Controller 无法为站点代理新连接，因此请仔细规划。

#### 自动升级数据库和站点

1. 启动新升级的 Studio。
2. 指示您要自动启动站点升级并确认您已准备就绪。

数据库和站点升级正在进行中。

#### 手动升级数据库和站点

1. 启动新升级的 Studio。
2. 指示您要手动升级站点。向导会检查许可证服务器兼容性并请求确认。
3. 确认您已备份数据库。

   向导会生成并显示脚本以及升级步骤清单。如果自产品版本升级以来数据库的架构未发生更改，则不会生成该脚本。例如，如果日志记录数据库架构未更改，则不会生成 `UpgradeLoggingDatabase.sql` 脚本。
4. 按所示顺序运行以下脚本。

   - `DisableServices.ps1`：Studio 用户在 Controller 上运行此 PowerShell 脚本以禁用产品服务。
   - `UpgradeSiteDatabase.sql`：数据库管理员在包含站点数据库的服务器上运行此 SQL 脚本。
   - `UpgradeMonitorDatabase.sql`：数据库管理员在包含 Monitor 数据库的服务器上运行此 SQL 脚本。
   - `UpgradeLoggingDatabase.sql`：数据库管理员在包含配置日志记录数据库的服务器上运行此 SQL 脚本。仅当此数据库发生更改时（例如，应用修补程序后）才运行此脚本。
   - `EnableServices.ps1`：Studio 用户在 Controller 上运行此 PowerShell 脚本以启用产品服务。

   数据库升级完成且产品服务启用后，Studio 会自动测试环境和配置，然后生成 HTML 报告。如果发现问题，可以还原数据库备份。解决问题后，可以再次升级数据库。
5. 完成清单任务后，单击 **Finish upgrade**。

### 步骤 10：升级剩余的 Delivery Controller

在新升级的 Studio 中，在导航窗格中选择 **Citrix Studio** *site-name*。在**常见任务**选项卡上，选择 **Upgrade remaining Delivery Controllers**。

完成升级并确认完成后，关闭然后重新打开 Studio。Studio 可能会提示进行额外的站点升级，以将 Controller 的服务注册到站点，或者在区域 ID 不存在时创建该 ID。

### 步骤 11：升级 VDA

> **重要提示：**

> 如果要将 VDA 升级到版本 1912 或更高版本，请参阅将 VDA 升级到 1912 或更高版本。

> 在包含 VDA 的计算机上运行产品安装程序。

如果您使用 Machine Creation Services™ 和主映像创建计算机，请转到主机并升级主映像上的 VDA。您可以使用任何可用的 VDA 安装程序。

- 有关图形界面指导，请参阅安装 VDA。
- 有关命令行指导，请参阅使用命令行安装。

如果您使用 Citrix Provisioning 创建计算机，请参阅Citrix Provisioning 产品文档 以获取有关升级的指导。

### 步骤 12：更新计算机目录和交付组

- 更新使用已升级 VDA 的计算机的目录。
- 升级使用已升级 VDA 的计算机的目录。
- 升级使用已升级 VDA 的计算机的交付组。

### 步骤 13：升级后

完成升级后，您可以测试新升级的站点。在 Studio 中，在导航窗格中选择 **Citrix Studio site-name**。在**“常见任务”**选项卡上，选择**“测试站点”**。这些测试在您升级数据库后会自动运行，但您可以随时再次运行它们。

如果未启动 SQL Server Browser Service，则当本地 Microsoft SQL Server Express 用于站点数据库时，Windows Server 2016 上的 Controller 的测试可能会失败。为避免此问题：

- 启用 SQL Server Browser Service（如果需要），然后启动它。
- 重新启动 SQL Server (SQLEXPRESS) 服务。

升级部署中的其他组件。有关指导，请参阅以下产品文档：

- StoreFront
- AppDNA
- Citrix 应用分层
- HDX RealTime 优化包
- 配置文件管理
- Citrix 预配
- 会话录制
- 工作区环境管理

如果您需要将 Microsoft SQL Server Express LocalDB 软件替换为更高版本，请参阅 替换 SQL Server Express LocalDB。

## 数据库架构升级

更新部署时，可以升级多个数据库架构。下表列出了在此过程中升级的数据库架构：

| From/To | 1912 CU1 | 1912 CU2 | 1912 CU3 | 1912 CU4 | 1912 CU5 | 2203 RTM | 2203 CU1 | 2203 CU2 | 2203 CU3 |
|---|---|---|---|---|---|---|---|---|---|
| 7.15 RTM/CU | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 RTM | Config | Site; Config | Site; Config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU1 | | Site | Site; Config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU2 | | | Site; Config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU3 | | | | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU4 | | | | | Site; Config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU5 | | | | | | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU6 | | | | | | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU7 | | | | | | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 2203 RTM | | | | | | | Config | Config | Config |
| 2203 CU1 | | | | | | | | Config | Config |
| 2203 CU2 | | | | | | | | | Config |

术语定义：

- 站点：站点数据存储。数据库架构更新应用于站点数据存储。
- 监视器：监视器数据存储。数据库架构更新应用于监视器数据存储。
- 配置：配置表。Desktop Studio 版本、许可信息或两者都在配置表中更新。
- 日志记录：日志记录数据存储。Dbschema 更新已应用于日志记录数据存储。

## 将 VDA 升级到 2203 或更高版本

如果 VDA 上曾安装过 Personal vDisk (PvD) 组件，则该 VDA 无法升级到 2203 或更高版本。要使用新的 VDA，必须卸载当前 VDA，然后安装新的 VDA。

即使您从未使用过 PvD，此说明也适用。

PvD 组件在早期版本中可能通过以下方式安装：

- 在 VDA 安装程序的图形界面中，PvD 是“**附加组件**”页面上的一个选项。7.15 LTSR 和更早的 7.x 版本默认启用此选项。因此，如果您接受了默认设置（或在任何版本中明确启用了该选项），则会安装 PvD。
- 在命令行中，`/baseimage` 选项安装了 PvD。如果您指定了此选项，或使用了包含此选项的脚本，则会安装 PvD。

如果您不确定 VDA 是否安装了 PvD，请在该计算机或映像上运行新 VDA（2203 或更高版本）的安装程序。

- 如果安装了 PvD，则会显示一条消息，指示存在不兼容的组件。
  - 在图形界面中，单击包含该消息的页面上的“**取消**”，然后确认要关闭安装程序。
  - 从 CLI 中，命令将直接失败并显示消息。
- 如果未安装 PvD，则升级将继续进行。

### 操作方法

如果 VDA 未安装 PvD，请按照常规升级过程进行操作。

如果 VDA 已安装 PvD：

1. 卸载当前 VDA。
2. 安装新的 VDA。

如果您想在 Windows 10（1607 及更早版本，未更新）计算机上继续使用 PvD，VDA 7.15 LTSR 是最新支持的版本。

> **注意：**

> *我可以在 XenApp and XenDesktop 7.15 LTSR 中将 Personal vDisk 与 Windows 7 桌面结合使用吗？*

> Citrix 于 2016 年 1 月宣布将 Personal vDisk (PvD) 从 XenApp and XenDesktop 7.6 LTSR 中排除。此外，Citrix 已宣布弃用 PvD 技术，并建议客户今后开始使用 Citrix App Layering。Citrix App Layering（版本 4.4 及更高版本）是 XenApp and XenDesktop 7.15 LTSR 的兼容组件。但是，为了帮助在 Windows 7 上现有 PvD 部署的客户迁移到 Citrix App Layering 技术，Citrix 决定通过 XenApp and XenDesktop 7.15 LTSR 累积更新 (CU) 为 Windows 7 桌面的 PvD 部署提供限时支持，直至 Jan 14, 2020。PvD 组件将从 LTSR CU 中移除，并且在 Jan 14, 2020 之后将不再受支持。此外，在 Jan 14, 2020 之后继续将 PvD 用于 Windows 7 将导

> 致 LTSR 站点不合规。此外，适用于 Windows 10 的 PvD 仍被排除在 7.15 LTSR 之外。因此，客户不应将其与 7.15 LTSR 站点一起使用。

## 移除 PvD、AppDisks 和不受支持的主机

Citrix Virtual Apps and Desktops 7 Current Release 部署不支持以下技术和主机类型：

- **Personal vDisks (PvD)**：用于在目录中存储用户 VM 旁边的数据。用户个性化层功能现在处理用户持久性。
- **AppDisks**：用于管理交付组中使用的应用程序。
- **主机类型**：Azure Classic、CloudPlatform（原始 Citrix 产品）。
  - 有关此版本中支持的主机类型，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#hosts--virtualization-resources)。
  - 有关继续使用 ARM 和 AWS 的替代方法的信息，请参阅 CTX270373。

如果您的当前部署使用 PvDs 或 AppDisks，或者连接到不受支持的主机类型（例如 Microsoft Azure Classic），则只有在移除使用这些技术的项目后，才能升级到版本 2006（或更高版本支持的版本）。如果您的当前部署使用公共云主机连接（例如 AWS），请确保在升级前拥有 Hybrid Rights License。当安装程序检测到一个或多个不受支持的技术或没有 Hybrid Rights License 的主机连接时，升级将暂停或停止，并显示一条解释性消息。安装程序日志中包含详细信息。

为确保成功升级，请查看并遵循有关移除不受支持项目的适用指南。

- (#remove-pvd)
- (#remove-appdisks)
- 删除不支持的主机项

即使您未在部署中使用 PvD 或 AppDisks，相关的 MSI 也可能已包含在较早的 VDA 安装或升级中。在将 VDA 升级到版本 2006（或更高受支持版本）之前，您必须删除该软件，即使您从未使用过它。使用图形界面时，可以为您完成此删除操作，或者在使用 CLI 时可以包含删除选项。有关详细信息，请参阅 (#vdas-that-have-pvd-or-appdisks-components)。

### 删除 PvD

在删除所有配置为使用 PvD 的计算机之前，部署升级无法成功。这会影响目录和交付组。

要从组和目录中删除 PvD：

1. 在 Studio 中，如果交付组包含来自使用 PvD 的目录的计算机，请 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/install-configure/delivery-groups-manage.html#remove-a-machine-from-a-delivery-group)。
2. 在 Studio 中，(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/install-configure/machine-catalogs-manage.html#delete-a-catalog) 包含使用 PvD 的计算机的所有目录。

**VDA 升级：** 部署升级不会检测 VDA 是否安装了 AppDisk 或 PvD 组件。但是，VDA 安装程序会检测。有关详细信息，请参阅 (#vdas-that-have-pvd-or-appdisks-components)。

### 删除 AppDisks

在从所有使用 AppDisks 的交付组中删除 AppDisks，然后删除 AppDisks 本身之前，部署升级无法继续。

1. 在 Studio 导航窗格中选择 **交付组**。
2. 选择一个组，然后在“操作”窗格中单击“**管理 AppDisks**”。
3. 单击从组中删除 AppDisk 的操作。
4. 对每个使用 AppDisks 的交付组重复步骤 2 和 3。
5. 在 Studio 导航窗格中选择“**AppDisks**”。
6. 选择一个 AppDisk，然后单击删除该 AppDisk 的操作。
7. 对每个 AppDisk 重复步骤 5 和 6。

**VDA 升级：** 部署升级不会检测 VDA 是否安装了 AppDisk 或 PvD 组件。但是，VDA 安装程序会检测。有关详细信息，请参阅 具有 PvD 或 AppDisks 组件的 VDA。

### 删除不受支持的主机项

如果站点连接到不受支持的主机类型（例如 Citrix CloudPlatform 或 Microsoft Azure Classic），则无法将部署升级到版本 2006（或更高版本支持的版本）。在尝试升级之前，请完成以下任务。

在 Studio 中：

- 删除所有连接 到不受支持的主机。
- 如果交付组包含使用不受支持的主机中的主映像创建的目录中的计算机，请从该组中删除这些计算机。
- 删除所有目录，这些目录是使用不受支持的主机中的主映像创建的。

### 具有 PvD 或 AppDisks 组件的 VDA

如果 VDA 上安装了启用 PvD 和 AppDisks 技术的组件，则在删除这些组件之前无法升级该 VDA。

> **注意：**
>
> 升级到版本 1912 时，您必须卸载当前 VDA，然后安装新的 VDA。在此版本中，系统会询问您是否希望 Citrix 删除该组件，然后继续升级。

> 即使您从未使用过这些技术，AppDisk 和 PvD 组件也可能已在早期 VDA 版本中安装：

- 图形界面：在 VDA 安装程序中，**附加组件**页面包含 **Citrix AppDisk / Personal vDisk** 选项。7.15 LTSR 和更早的 7.x 版本默认启用此选项。因此，如果您接受了默认设置（或在任何提供此选项的版本中明确启用了此选项），则会安装该组件。
- CLI：指定 `/baseimage` 选项会安装该组件。

### 操作方法

如果 VDA 安装程序未检测到当前安装的 VDA 中的 AppDisks 或 PvD 组件，则升级将照常进行。

如果安装程序在当前安装的 VDA 中检测到 AppDisks 或 PvD 组件：

- 图形界面：升级暂停。一条消息询问您是否要自动删除不受支持的组件。如果单击 **确定**，组件将自动删除，然后升级继续进行。
- 命令行界面：为避免命令失败，请在命令中包含以下选项：
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

## 限制

以下限制适用于升级：

- **选择性组件安装：** 如果您将任何组件安装或升级到新版本，但选择不升级需要升级的其他组件（在不同的计算机上），Studio 会提醒您。例如，假设升级包括新版本的 Controller 和 Studio。您升级了 Controller，但未在安装 Studio 的计算机上运行安装程序。在您升级 Studio 之前，Studio 将不允许您继续管理站点。

  您不必升级 VDA，但 Citrix 建议升级所有 VDA，以便您可以使用所有可用功能。
- **早期版本或技术预览版本：** 您无法从早期版本、技术预览版或预览版进行升级。
- **早期操作系统上的组件：** 您无法在 Microsoft 或 Citrix 不再支持的操作系统上安装当前 VDA。有关详细信息，请参阅早期操作系统。

- **混合环境/站点：** 如果您必须继续运行早期版本站点和当前版本站点，请参阅混合环境注意事项。
- **产品选择：** 从早期版本升级时，您无需选择或指定在安装过程中设置的产品（Citrix Virtual Apps 或 Citrix Virtual Apps and Desktops）。

## 混合环境注意事项

升级时，Citrix 建议您升级所有组件和 VDA，以便您可以访问您的版本和版本中的所有新增和增强功能。

例如，尽管您可以在包含早期 Controller 版本的部署中使用当前 VDA，但当前版本中的新功能可能不可用。使用非当前版本时，也可能出现 VDA 注册问题。

在某些环境中，您可能无法将所有 VDA 升级到最新版本。在这种情况下，当您创建计算机目录时，可以指定安装在计算机上的 VDA 版本。（这称为功能级别。）默认情况下，此设置指定建议的最低 VDA 版本。默认值足以满足大多数部署的需求。仅当目录包含早于默认版本的 VDA 时，才考虑将设置更改为早期版本。不建议在计算机目录中混合使用 VDA 版本。

如果使用默认的最低 VDA 版本设置创建目录，并且一台或多台计算机的 VDA 版本早于默认版本，则这些计算机将无法向 Controller 注册，并且无法正常工作。

有关详细信息，请参阅 VDA 版本和功能级别。

### 具有不同版本的多个站点

当您的环境包含具有不同产品版本的站点（例如，XenDesktop 7.18 站点和 Citrix Virtual Apps and Desktops 1909 站点）时，Citrix 建议使用 StoreFront 聚合来自不同产品版本的应用程序和桌面。有关详细信息，请参阅 StoreFront 文档。

在混合环境中，请继续使用每个版本的 Studio 和 Director 版本，但请确保将不同版本安装在单独的计算机上。

## 早期操作系统

假设您在运行受支持的操作系统 (OS) 版本的计算机上安装了某个组件的早期版本。现在，您想使用较新的组件版本，但该操作系统不再受当前组件版本的支持。

例如，假设您在 Windows Server 2008 R2 计算机上安装了服务器 VDA。现在您想将该 VDA 升级到当前版本，但 Windows Server 2008 R2 不受您要升级到的当前版本的支持。

如果您尝试在不再允许的操作系统上安装或升级组件，则会显示错误消息，例如“无法在此操作系统上安装”。

这些注意事项适用于升级当前版本和长期服务版本。(它不影响将 CU 应用于 LTSR 版本。)

请单击以下链接以了解支持哪些操作系统：

- Citrix 虚拟应用和桌面（当前版本）：
  - Delivery Controller、Studio、Director、VDA、通用打印服务器
  - 联合身份验证服务
  - 对于 StoreFront、自助密码重置 和 会话录制，请参阅当前版本的系统要求文章。
- 对于 LTSR，请参阅您的 LTSR 版本和 CU 的组件列表。（从主要的 Citrix Virtual Apps and Desktops 产品文档页面中选择您的 LTSR 版本。）

### 无效的操作系统

下表列出了当前版本中安装/升级组件无效的早期操作系统。它指出了每个列出的操作系统支持的最新有效组件版本，以及安装和升级变得无效的组件版本。

表中的操作系统包括 Service Pack 和更新。

| 操作系统 | 组件/功能 | 最新有效版本 | 从该版本起无法安装/升级 |
|---|---|---|---|
| 视窗 7 和 视窗 8 | VDA | 7.15 LTSR | 7.16 |
| 视窗 7 和 视窗 8 | 其他安装程序组件 | 7.17 | 7.18 |
| 早于 1607 的 Windows 10 版本 | VDA | 7.15 LTSR | 7.16 |
| Windows 10 x86 版本 | VDA | 1906.2.0 | 1909 |
| Windows 服务器 2008 R2 | VDA | 7.15 LTSR | 7.16 |
| Windows 服务器 2008 R2 | 其他安装程序组件 | 7.17 | 7.18 |
| Windows 服务器 2012 | VDA | 7.15 LTSR | 7.16 |
| Windows 服务器 2012 | 其他安装程序组件 | 7.17 | 7.18 |

| 操作系统 | 组件/功能 | 最新有效版本 | 从该版本起无法安装/升级 |
| --- | --- | --- | --- |
| Windows Server 2012 R2 服务器 | 其他安装程序组件 * | 1912 LTSR | 2003 |
| Windows Server 2012 R2 服务器 | 服务器 VDI | 7.15 LTSR | 7.16 |

Windows XP 和 Windows Vista 不适用于任何 7.x 组件或技术。

* 适用于交付控制器、Studio、Director 和 VDA。

## 您可以执行的操作

您有多种选择。您可以：

- 继续使用当前操作系统
- 重新映像或升级计算机
- 添加新计算机，然后移除旧计算机

### 继续使用当前操作系统

这些方法适用于 VDA。如果您想继续使用旧版操作系统的计算机，可以选择以下方法之一：

- 继续使用已安装的组件版本。
- 下载最新的有效组件版本，然后将组件升级到该版本。（这假设尚未安装最新的有效组件版本。）

例如，您的 Windows 7 SP1 计算机上有一个 7.14 VDA。Windows 7 操作系统计算机上最新的有效 VDA 版本是 XenApp and XenDesktop 7.15 LTSR。您可以继续使用 7.14，也可以下载 7.15 LTSR VDA，然后将您的 VDA 升级到该版本。这些较早的 VDA 版本可在包含较新版本 Delivery Controller 的部署中运行。例如，7.15 LTSR VDA 可以连接到 Citrix Virtual Apps and Desktops 7 1808 Controller。

### 重新创建映像或升级计算机

这些方法适用于 VDA 和未安装核心组件（例如 Delivery Controller）的其他计算机。请选择以下方法之一：

- 将计算机停止服务（启用维护模式并允许所有会话关闭）后，您可以将其重新创建映像为受支持的 Windows 操作系统版本，然后安装最新版本的组件。

- 要在不重新创建映像的情况下升级 VDA 计算机中的操作系统，您必须首先安装您要升级到的操作系统上支持的 VDA 版本，或者在升级操作系统后升级 VDA。否则，Citrix 软件将不受支持。在不卸载 VDA 的情况下执行就地升级时，您可以升级到以下最低操作系统版本：
  - 已安装 2023-07 Cumulative Update for Windows 11 (KB5028185) 或更高版本（内部版本 22621.1992 或更高版本）的 Windows 11。
  - 已安装 2023 年 7 月适用于 Windows 10 的动态更新 (KB5028311) 的 Windows 10。
- 如果您计划升级到的 Windows 版本与上述指南不符，则必须在升级操作系统之前卸载 VDA，然后在操作系统升级完成后安装受支持的 VDA 版本。

#### 添加新计算机，然后删除旧计算机

如果必须升级包含 Delivery Controller™ 或其他核心组件的计算机上的操作系统，此方法是可行的。

Citrix 建议站点中的所有 Controller 都使用相同的操作系统。以下升级顺序可最大程度地缩短不同 Controller 使用不同操作系统的时间间隔。

1. 对站点中的所有 Delivery Controller 进行快照，然后备份站点数据库。
2. 在支持的操作系统上，在全新服务器上安装新的 Delivery Controller。例如，在两台 Windows Server 2016 计算机上安装一个 Controller。
3. 将新的 Controller 添加到站点。
4. 移除在当前版本不支持的操作系统上运行的 Controller。例如，移除两台 Windows Server 2008 R2 计算机上的两个 Controller。请遵循 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/manage-deployment/delivery-controllers.html) 中有关移除 Controller 的建议。

## 准备工作

在开始升级之前，请查看以下信息并完成必要的任务。

> **注意：**
>
> 尽管 VDA 升级在 (#upgrade-sequence) 中稍后进行，但最好在开始升级之前选择一个安装程序并查看该过程，以便您了解预期结果。

#### 选择安装程序和界面

使用产品 ISO 中的完整产品安装程序升级组件。您可以使用完整产品安装程序或其中一个独立 VDA 安装程序升级 VDA。所有安装程序都提供图形界面和命令行界面。

有关详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-prepare.html#installers)。

**安装详情：** 完成所有准备工作并准备好启动安装程序后，安装文章将向您展示您将看到的内容（如果您使用的是图形界面）或要键入的内容（如果您使用的是命令行界面）。

- 使用图形界面安装/升级核心组件(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-core.html)
- 使用命令行安装/升级核心组件(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-command.html)
- (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-vdas.html)
- (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-command.html)

如果您最初使用 `VDAWorkstationCoreSetup.exe` 安装程序安装了单会话 VDA，Citrix 建议使用该安装程序进行升级。如果您使用完整产品 VDA 安装程序或 `VDAWorkstationSetup.exe` 安装程序升级 VDA，则除非您明确从升级中省略/排除这些组件，否则最初排除的组件可能会被安装。

升级 VDA 到当前版本时，升级过程中会发生计算机重启。（此要求始于 7.17 版本。）这是无法避免的。重启后升级会自动恢复（除非您在命令行中指定 `/noresume`）。

### 数据库操作

备份站点、监视和配置日志数据库。请按照 CTX135207 中的说明进行操作。如果在升级后发现任何问题，可以还原备份。

有关升级不再受支持的 SQL Server 版本的信息，请参阅 SQL Server 版本检查。（这指的是用于站点、监视和配置日志数据库的 SQL Server。）

Microsoft SQL Server Express LocalDB 会自动安装，以用于本地主机缓存。如果需要替换早期版本，新版本必须是 SQL Server Express LocalDB 2019。有关在升级组件和站点后用新版本替换 SQL Server Express LocalDB 的详细信息，请参阅 替换 SQL Server Express LocalDB。

### 确保您的 Citrix 许可为最新版本

有关管理 Citrix 许可的全面信息，请参阅 激活、升级和管理 Citrix 许可证。

您可以使用完整产品安装程序升级许可证服务器。或者，您可以单独下载和升级许可证组件。请参阅 升级。

升级之前，请确保您的客户成功服务/软件维护/订阅优势日期对新产品版本有效。该日期必须至少为 2021.11.15。

### 确保您的 Citrix 许可证服务器兼容

确保您的 Citrix 许可证服务器与新版本兼容。有两种方法可以执行此操作：

- 在升级任何其他 Citrix 组件之前，请在包含 Delivery Controller 的计算机上从 ISO 布局运行 `XenDesktopServerSetup.exe` 安装程序。如果存在任何不兼容问题，安装程序会报告并提供建议的解决步骤。
- 在安装介质的 `XenDesktop Setup` 目录中，运行命令：`.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`。显示内容指示许可证服务器是否兼容。如果许可证服务器不兼容，请升级许可证服务器。

### 备份所有 StoreFront 修改

在开始升级之前，如果您已修改 `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data` 中的文件（例如 *default.ica* 和 *usernamepassword.tfrm*），请为每个应用商店备份这些文件。升级后，您可以还原它们以恢复您的修改。

### 关闭应用程序和控制台

在开始升级之前，请关闭所有可能导致文件锁定的程序，包括管理控制台和 PowerShell 会话。

重新启动计算机可确保清除所有文件锁定，并且没有待处理的 Windows 更新。

在开始升级之前，请停止并禁用所有第三方监控代理服务。

### 确保您拥有适当的权限

除了是域用户之外，您还必须是正在升级产品组件的计算机上的本地管理员。

站点数据库和站点可以自动或手动升级。对于自动数据库升级，Studio 用户的权限必须包括更新 SQL Server 数据库架构的能力（例如，`db_securityadmin` 或 `db_owner` 数据库角色）。有关详细信息，请参阅 数据库。

如果 Studio 用户没有这些权限，则启动手动数据库升级会生成脚本。Studio 用户从 Studio 运行部分脚本。数据库管理员使用 SQL Server Management Studio 等工具运行其他脚本。

### 其他准备任务

- 如有需要，备份模板并升级管理程序
- 完成业务连续性计划中规定的任何其他准备任务。

## 站点初步测试

升级 Delivery Controller 和站点时，在实际升级开始之前会运行站点初步测试。这些测试验证：

- 站点数据库可访问且已备份
- 与关键 Citrix 服务的连接正常工作
- Citrix 许可证服务器地址可用
- 可以访问配置日志数据库
- 如果要添加公共云主机连接（例如 AWS），请确保您拥有混合权利许可证。否则，初步站点测试将暂停或停止，并显示一条解释性消息。

测试运行后，您可以查看结果报告。然后，您可以修复检测到的任何问题，并再次运行测试。未能运行初步站点测试并解决任何问题可能会影响站点的运行方式。

包含测试结果的报告是一个 HTML 文件 (`PreliminarySiteTestResult.html`)，位于与安装日志相同的目录中。如果该文件不存在，则会创建该文件。如果文件存在，则其内容将被覆盖。

### 运行测试

- 当您使用安装程序的图形界面进行升级时，向导会包含一个页面，您可以在其中启动测试并显示报告。测试运行后，查看报告并解决发现的任何问题后，您可以重新运行测试。测试成功完成后，单击“下一步”继续向导。
- 当您使用命令行界面进行升级时，测试会自动运行。默认情况下，如果测试失败，则不执行升级。查看报告并解决问题后，重新运行命令。

Citrix 建议在继续 Controller 和站点升级之前，始终运行初步站点测试并解决任何问题。运行测试所花费的几分钟时间非常值得。但是，您可以覆盖此建议操作。

- 使用图形界面升级时，您可以选择跳过测试并继续升级。
- 从命令行升级时，无法跳过测试。默认情况下，失败的站点测试会导致安装程序失败，而不执行升级。在大多数情况下，如果您包含 `/ignore_site_test_failure` 选项，则会忽略任何测试失败，并继续升级。（有关例外情况，请参阅 SQL Server 版本检查。）

### 升级多个 Controller 时

当您在一个 Controller 上启动升级，然后在同一站点中的另一个 Controller 上启动升级时（在第一个升级完成之前）：

- 如果初步站点测试已在第一个 Controller 上完成，则初步站点测试页面不会出现在另一个 Controller 的向导中。
- 如果在您在另一个 Controller 上启动升级时，第一个 Controller 上的测试正在进行，则站点测试页面会出现在另一个 Controller 的向导中。但是，如果第一个 Controller 上的测试完成，则仅保留第一个 Controller 的测试结果。

### 与站点运行状况无关的测试失败

- 如果初步站点测试因内存不足而失败，请提供更多内存，然后重新运行测试。
- 如果您有权升级，但无权运行站点测试，则初步站点测试将失败。要解决此问题，请使用有权运行测试的用户帐户重新运行安装程序。

## SQL Server 版本检查

成功的 Citrix Virtual Apps and Desktops 部署需要受支持的 Microsoft SQL Server 版本来支持站点、监视和配置日志记录数据库。使用不再受支持的 SQL Server 版本升级 Citrix 部署可能会导致功能问题，并且站点将不受支持。

要了解您要升级到的 Citrix 版本支持哪些 SQL Server 版本，请参阅该版本的系统要求文章。

升级 Controller 时，Citrix 安装程序会检查用于站点、监视和配置日志记录数据库的当前安装的 SQL Server 版本。

- 如果检查确定当前安装的 SQL Server 版本不是您要升级到的 Citrix 版本中支持的版本：
  - 图形界面：升级将暂停并显示一条消息。单击**我理解**，然后单击**取消**以关闭 Citrix 安装程序。（您无法继续升级。）
  - 命令行界面：命令失败（即使您在命令中包含了 `/ignore_db_check_failure` 选项）。

  升级 SQL Server 版本，然后再次启动 Citrix 升级。
- 如果检查无法确定当前安装的 SQL Server 版本，请查看您当前安装的版本在您要升级到的版本中是否受支持（系统要求）。
  - 图形界面：升级将暂停并显示一条消息。
    - 如果当前安装的 SQL Server 版本受支持，请单击**我理解**以关闭消息，然后单击**下一步**以继续 Citrix 升级。
    - 如果当前安装的 SQL Server 版本不受支持，请单击**我理解**以关闭消息，然后单击**取消**以结束 Citrix 升级。将 SQL Server 升级到受支持的版本，然后再次启动 Citrix 升级。
  - 命令行界面：命令失败并显示一条消息。关闭该消息后：
    - 如果当前安装的 SQL Server 版本受支持，请使用 `/ignore_db_check_failure` 选项再次运行该命令。
    - 如果当前安装的 SQL Server 版本不受支持，请将 SQL Server 升级到受支持的版本。再次运行该命令以启动 Citrix 升级。

### 升级 SQL Server

如果您启动新的 SQL Server 服务器并迁移站点数据库，则必须更新连接字符串。

如果站点当前将 SQL Server Express 用于站点数据库（Citrix 在站点创建期间自动安装）：

1. 安装最新版本的 SQL Server Express。
2. 分离数据库。
3. 将数据库附加到新的 SQL Server Express。
4. 迁移连接字符串。

有关详细信息，请参阅配置连接字符串和 Microsoft SQL Server 产品文档。

## 替换 SQL Server Express 本地数据库

Microsoft SQL Server Express LocalDB 是 SQL Server Express 的一项功能，本地主机缓存独立使用它。本地主机缓存不需要 SQL Server Express 的任何组件，只需要 SQL Server Express LocalDB。

Citrix 不会自动更新 SQL Server Express LocalDB。要更新 SQL Server Express LocalDB 版本，请遵循本节中的指导。

- 将 Delivery Controller 升级到 Citrix Virtual Apps and Desktops 2203 LTSR 版或更高版本时，支持的版本是 SQL Server Express LocalDB 2019 或 SQL Server Express LocalDB 2022。

> **注意：**
>
> SQL Server Express LocalDB 2022 在 Citrix Virtual Apps and Desktops 2203 LTSR CU5 及更高版本中受支持。

> 所需条件：

- Citrix Virtual Apps and Desktops 的安装介质。
- 来自 Windows Sysinternals 工具箱的 PsExec 工具。

步骤：

1. 完成 Citrix Virtual Apps and Desktops 组件、数据库和站点的升级。（这些数据库升级会影响站点、监视和配置日志记录数据库。它们不影响使用 SQL Server Express LocalDB 的本地主机缓存数据库。）

2. 登录到要更新 SQL Server Express LocalDB 的 Delivery Controller。
3. 从 Microsoft 下载 PsExec 并将其放置在该 Delivery Controller 上易于访问的位置，例如 C:\Temp。
4. 从 Windows 系统服务中停止 Delivery Controller 上的 Citrix High Availability Service。
5. 在 Delivery Controller 上打开命令提示符，导航到 PsExec 所在的位置（例如，`C:\Temp`），然后运行以下命令以使用网络服务帐户提升命令提示符权限：

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
   ```

6. 运行 `whoami` 以确认命令提示符以网络服务帐户身份运行。您必须获得以下输出：`nt authority\networkservice`。
7. 使用命令提示符导航到 SQL LocalDB 实例：
   - 如果从 SQL LocalDB 2014 升级：

     ```
     cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
     ```

   - 如果从 SQL LocalDB 2017 升级：

     ```
     cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
     ```

   - 如果从 SQL LocalDB 2019 升级：

     ```
     cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
     ```

8. 停止并删除 SQL LocalDB 实例：`CitrixHA`。

   ```
   SqlLocalDB stop CitrixHA



   SqlLocalDB delete CitrixHA
   ```

9. 从 Delivery Controller 中删除以下文件：

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*

C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if
exists)

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.*
(if exists)
```

10. 使用 Windows 本机程序删除功能，从 Delivery Controller 中卸载现有的 SQL LocalDB SQL Server Express。
11. 卸载完成后，重新启动 Delivery Controller。
12. 从 Windows 系统服务中停止 Delivery Controller 上的 Citrix High Availability Service。
13. 将 Citrix Virtual Apps and Desktops 安装介质装载到您的 Delivery Controller。
14. 以管理员身份在 Delivery Controller 上安装 SQL Server Express LocalDB 2019。
    a. 使用 Citrix Virtual Apps and Desktops 安装介质的 `Support > SQLLocalDB` 文件夹中的 `sqllocaldb.msi` 文件。例如，如果安装介质装载到 `E drive` 盘符，则可以在 `E:\Support\SQLLocalDB\sqllocaldb.msi` 找到该文件。需要重新启动才能完成安装。
    b. 新的 SQL LocalDB 必须位于 `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` 中。
15. 从 Windows 系统服务中启动 Delivery Controller 上的 Citrix High Availability Service。
16. 在 Delivery Controller 的命令提示符中，导航到 `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` 并运行 `SqlLocalDB i` 以确认已创建 CitrixHA 实例。返回的实例列表中必须包含 `CitrixHA`。

> **注意：**
>
> 启动 Citrix High Availability Service 后，可能需要长达 15 分钟才能创建 CitrixHA 数据库。

17. 确保已创建本地主机缓存数据库文件，以确认高可用性服务（辅助代理）可在需要时接管。
    a. 在 Delivery Controller 上，浏览到 `C:\Windows\ServiceProfiles\NetworkService`。
    b. 验证 `HaDatabaseName.mdf` 和 `HaDatabaseName_log.ldf` 已创建。

18. 在其余 Delivery Controller 上重复这些步骤。

# 安全

Citrix Virtual Apps and Desktops™ 提供了一种安全设计解决方案，可让您根据安全需求定制环境。

IT 面临的移动办公人员安全问题之一是数据丢失或被盗。通过托管应用程序和桌面，Citrix Virtual Apps and Desktops 将所有数据保留在数据中心，从而将敏感数据和知识产权与终端设备安全地分离。当启用策略以允许数据传输时，所有数据都将加密。

Citrix Virtual Apps and Desktops 数据中心还通过集中式监控和管理服务简化了事件响应。Director 允许 IT 监控和分析网络中正在访问的数据，而 Studio 允许 IT 在数据中心修补和修复大多数漏洞，而不是在每个最终用户设备上本地解决问题。

Citrix Virtual Apps and Desktops 还简化了审计和法规遵从性，因为调查人员可以使用集中式审计跟踪来确定谁访问了哪些应用程序和数据。Director 通过访问配置日志和 OData API 收集有关系统更新和用户数据使用情况的历史数据。

委派管理允许您设置管理员角色，以精细控制对 Citrix Virtual Apps and Desktops 的访问。这使您的组织能够灵活地为某些管理员提供对任务、操作和范围的完全访问权限，而其他管理员则具有有限的访问权限。

Citrix Virtual Apps and Desktops 允许管理员通过在网络的各个级别（从本地级别到组织单位级别）应用策略，对用户进行精细控制。这种策略控制决定了用户、设备或用户和设备组是否可以连接、打印、复制/粘贴或映射本地驱动器，从而最大程度地减少了与第三方临时工作人员相关的安全问题。管理员还可以使用桌面锁定功能，以便最终用户只能使用虚拟桌面，同时阻止对最终用户设备的本地操作系统的任何访问。

管理员可以通过将站点配置为使用控制器或最终用户与虚拟投递代理 (VDA) 之间的传输层安全 (TLS) 协议来增强 Citrix Virtual Apps 或 Citrix Virtual Desktops 的安全性。该协议还可以在站点上启用，以提供服务器身份验证、数据流加密和 TCP/IP 连接的消息完整性检查。

Citrix Virtual Apps and Desktops 还支持 Windows 或特定应用程序的多重身份验证。多重身份验证还可用于管理 Citrix Virtual Apps and Desktops 交付的所有资源。这些方法包括：

- 令牌
- 智能卡
- RADIUS

- Kerberos (科尔贝罗斯)
- 生物识别

Citrix Virtual Desktops 可以与许多第三方安全解决方案集成，从身份管理到防病毒软件。支持的产品列表可在 `<http://www.citrix.com/ready>` 找到。

Citrix Virtual Apps and Desktops 的部分版本已通过通用准则标准认证。有关这些标准的列表，请访问 `<https://www.commoncriteriaportal.org/cc/>`。

# 安全注意事项和最佳实践

> **注意：**
>
> 您的组织可能需要满足特定的安全标准以符合法规要求。本文档不涵盖此主题，因为此类安全标准会随时间变化。有关安全标准和 Citrix 产品的最新信息，请查阅 `<http://www.citrix.com/security/>`。

## 安全最佳实践

确保环境中的所有计算机都安装了最新的安全补丁。一个优点是，您可以将瘦客户端用作终端，这简化了此任务。

使用防病毒软件保护环境中的所有计算机。

考虑使用特定于平台的反恶意软件。

安装软件时，请安装到提供的默认路径。

- 如果您将软件安装到提供的默认路径以外的文件位置，请考虑为您的文件位置添加额外的安全措施，例如受限权限。

所有网络通信都应根据您的安全策略进行适当的安全保护和加密。您可以使用 IPSec 保护 Microsoft Windows 计算机之间的所有通信；有关如何执行此操作的详细信息，请参阅您的操作系统文档。此外，用户设备和桌面之间的通信通过 Citrix SecureICA 进行保护，该协议默认配置为 128 位加密。您可以在创建或更新交付组时配置 SecureICA。

> **注意：**

Citrix SecureICA 是 ICA/HDX 协议的一部分，但它不是像传输层安全性 (TLS) 那样符合标准的网络安全协议。您还可以使用 TLS 保护用户设备和桌面之间的网络通信。要配置 TLS，请参阅 传输层安全性 (TLS)。

应用 Windows 帐户管理最佳实践。在通过 Machine Creation Services 或 Provisioning Services 复制模板或映像之前，请勿在其中创建帐户。请勿使用存储的特权域帐户安排任务。请勿手动创建共享的 Active Directory 计算机帐户。这些做法将有助于防止计算机攻击获取本地持久帐户密码，然后使用这些密码登录到属于其他用户的 MCS/PVS 共享映像。

### 防火墙

使用外围防火墙保护环境中的所有计算机，包括在适当的隔离区边界处。

环境中的所有计算机都应受到个人防火墙的保护。安装核心组件和 VDA 时，如果检测到 Windows 防火墙服务（即使防火墙未启用），您可以选择自动打开组件和功能通信所需的端口。您也可以选择手动配置这些防火墙端口。如果您使用不同的防火墙，则必须手动配置。

如果您要将传统环境迁移到此版本，可能需要重新定位现有外围防火墙或添加新的外围防火墙。例如，假设数据中心中传统客户端和数据库服务器之间存在外围防火墙。使用此版本时，必须放置该外围防火墙，以便虚拟桌面和用户设备位于一侧，而数据中心中的数据库服务器和 Delivery Controller 位于另一侧。因此，请考虑在数据中心内创建一个隔离区以包含数据库服务器和 Controller。此外，还应考虑在用户设备和虚拟桌面之间提供保护。

**注意：**

TCP 端口 1494 和 2598 用于 ICA 和 CGP，因此很可能在防火墙上打开，以便数据中心外的用户可以访问它们。Citrix 建议您不要将这些端口用于其他任何用途，以避免无意中将管理界面暴露于攻击的可能性。端口 1494 和 2598 已在 Internet 号码分配机构 (http://www.iana.org/) 正式注册。

### 应用程序安全性

为防止非管理员用户执行恶意操作，我们建议您在 VDA 主机和本地 Windows 客户端上为安装程序、应用程序、可执行文件和脚本配置 Windows AppLocker 规则。

## 管理用户权限

仅授予用户所需的权限。Microsoft Windows 权限仍以常规方式应用于桌面：通过用户权限分配配置权限，通过组策略配置组成员身份。此版本的一个优点是，可以授予用户对桌面的管理权限，而无需同时授予对存储桌面的计算机的物理控制权。

规划桌面权限时请注意以下事项：

- 默认情况下，当非特权用户连接到桌面时，他们看到的是运行桌面的系统时区，而不是其自身用户设备的本地时区。有关如何允许用户在使用桌面时查看其本地时间的信息，请参阅“管理交付组”文章。
- 作为桌面管理员的用户对该桌面拥有完全控制权。如果桌面是池桌面而非专用桌面，则必须信任该用户，以确保其不会对该桌面的所有其他用户（包括未来用户）造成影响。该桌面的所有用户都需要了解这种情况对其数据安全可能造成的永久性风险。此注意事项不适用于专用桌面，因为专用桌面只有一个用户；该用户不应是任何其他桌面的管理员。
- 作为桌面管理员的用户通常可以在该桌面上安装软件，包括潜在的恶意软件。该用户还可能监视或控制连接到桌面的任何网络上的流量。

## 管理登录权限

用户帐户和计算机帐户都需要登录权限。与 Microsoft Windows 权限一样，登录权限仍以常规方式应用于桌面：通过用户权限分配配置登录权限，通过组策略配置组成员身份。

Windows 登录权限包括：本地登录、通过远程桌面服务登录、通过网络登录（从网络访问此计算机）、作为批处理作业登录以及作为服务登录。

对于计算机帐户，仅授予计算机所需的登录权限。需要“从网络访问此计算机”登录权限：

- 在 VDA 上，针对交付控制器的计算机帐户
- 在交付控制器上，针对 VDA 的计算机帐户。请参阅 基于 Active Directory OU 的控制器发现。
- 在 StoreFront™ 服务器上，对于同一 StoreFront 服务器组中其他服务器的计算机帐户

对于用户帐户，仅授予用户所需的登录权限。

根据 Microsoft 的说法，默认情况下，远程桌面用户组被授予“允许通过远程桌面服务登录”的登录权限（域控制器除外）。

您的组织安全策略可能明确规定应从该登录权限中删除此组。请考虑以下方法：

- 适用于多会话操作系统的虚拟投递代理 (VDA) 使用 Microsoft 远程桌面服务。您可以将远程桌面用户组配置为受限组，并通过 Active Directory 组策略控制该组的成员身份。有关详细信息，请参阅 Microsoft 文档。

- 对于 Citrix Virtual Apps and Desktops™ 的其他组件，包括适用于单会话操作系统的 VDA，不需要远程桌面用户组。因此，对于这些组件，远程桌面用户组不需要“允许通过远程桌面服务登录”的登录权限；您可以将其删除。此外：
  - 如果您通过远程桌面服务管理这些计算机，请确保所有此类管理员都已是 Administrators 组的成员。
  - 如果您不通过远程桌面服务管理这些计算机，请考虑在这些计算机上禁用远程桌面服务本身。

尽管可以将用户和组添加到登录权限“拒绝通过远程桌面服务登录”，但通常不建议使用拒绝登录权限。有关更多信息，请参阅 Microsoft 文档。

## 配置用户权限

Delivery Controller™ 安装会创建以下 Windows 服务：

- Citrix AD 身份服务 (NT SERVICE\CitrixADIdentityService)：管理虚拟机的 Microsoft Active Directory 计算机帐户。
- Citrix 分析服务 (NT SERVICE\CitrixAnalytics)：如果站点管理员已批准此收集，则收集站点配置使用信息供 Citrix 使用。然后将此信息提交给 Citrix，以帮助改进产品。
- Citrix 应用库 (NT SERVICE\CitrixAppLibrary)：支持 AppDisks 的管理和预配、AppDNA 集成以及 App-V 的管理。
- Citrix 代理服务 (NT SERVICE\CitrixBrokerService)：选择可供用户使用的虚拟桌面或应用程序。
- Citrix 配置日志服务 (NT SERVICE\CitrixConfigurationLogging)：记录管理员对站点所做的所有配置更改和其他状态更改。
- Citrix 配置服务 (NT SERVICE\CitrixConfigurationService)：用于共享配置的站点范围存储库。
- Citrix 委派管理服务 (NT SERVICE\CitrixDelegatedAdmin)：管理授予管理员的权限。
- Citrix 环境测试服务 (NT SERVICE\CitrixEnvTest)：管理其他交付控制器服务的自检。
- Citrix 主机服务 (NT SERVICE\CitrixHostService)：存储有关 Citrix Virtual Apps 或 Citrix Virtual Desktops 部署中使用的虚拟机管理程序基础结构的信息，并提供控制台用于枚举虚拟机管理程序池中资源的功能。
- Citrix 计算机创建服务 (NT SERVICE\CitrixMachineCreationService)：协调桌面虚拟机的创建。
- Citrix Monitor Service (NT SERVICE\CitrixMonitor)：收集 Citrix Virtual Apps 或 Citrix Virtual Desktops 的指标，存储历史信息，并为故障排除和报告工具提供查询接口。

- Citrix Storefront Service (NT SERVICE\ CitrixStorefront)：支持 StoreFront 的管理。（它不是 StoreFront 组件本身的一部分。）
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService)：支持 StoreFront 的特权管理操作。（它不是 StoreFront 组件本身的一部分。）
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService)：将配置数据从主站点数据库传播到本地主机缓存。
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService)：当主站点数据库不可用时，选择可供用户使用的虚拟桌面或应用程序。

Delivery Controller 安装还会创建以下 Windows 服务。这些服务在与其他 Citrix 组件一起安装时也会创建：

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc)：支持收集诊断信息供 Citrix 支持使用。
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService)：收集诊断信息供 Citrix 分析，以便管理员可以查看分析结果和建议，从而帮助诊断站点问题。

Delivery Controller 安装还会创建以下 Windows 服务。此服务目前未使用。如果已启用，请将其禁用。

- Citrix 远程代理提供程序 (NT SERVICE\XaXdCloudProxy)

Delivery Controller 安装还会创建以下 Windows 服务。这些服务目前未使用，但必须启用。请勿禁用它们。

- Citrix 编排服务 (NT SERVICE\CitrixOrchestration)
- Citrix 信任服务 (NT SERVICE\CitrixTrust)

除了 Citrix Storefront Privileged Administration Service 之外，这些服务都被授予“作为服务登录”的登录权限以及“调整进程的内存配额”、“生成安全审核”和“替换进程级别令牌”的特权。您无需更改这些用户权限。Delivery Controller 不使用这些特权，并且它们会自动禁用。

## 配置服务设置

除了 Citrix Storefront Privileged Administration 服务和 Citrix Telemetry Service 之外，配置用户权限部分中列出的 Delivery Controller Windows 服务都配置为以 NETWORK SERVICE 身份登录。请勿更改这些服务设置。

Citrix 配置同步服务需要 NETWORK SERVICE 帐户属于 Delivery Controller 上的本地管理员组。这允许本地主机缓存正常工作。

Citrix Storefront Privileged Administration 服务配置为以 Local System (NT AUTHORITY\SYSTEM) 身份登录。这是 Delivery Controller StoreFront 操作所必需的，这些操作通常对服务不可用（包括创建 Microsoft IIS 站点）。请勿更改其服务设置。

Citrix Telemetry 服务配置为以其自己的服务特定身份登录。

您可以禁用 Citrix Telemetry 服务。除了此服务以及已禁用的服务之外，请勿禁用任何其他 Delivery Controller Windows 服务。

## 配置注册表设置

不再需要在 VDA 文件系统上启用 8.3 文件名和文件夹的创建。可以将注册表项 **NtfsDisable8dot3NameCreation** 配置为禁用 8.3 文件名和文件夹的创建。您也可以使用 **fsutil.exe behavior set disable8dot3** 命令进行配置。

## 部署场景安全影响

您的用户环境可以包含由您的组织未管理且完全由用户控制的用户设备，也可以包含由您的组织管理和维护的用户设备。这两种环境的安全注意事项通常不同。

### 托管的用户设备

托管的用户设备处于管理控制之下；它们要么由您自己控制，要么由您信任的另一个组织控制。您可以直接配置和向用户提供用户设备；或者，您可以提供终端，在这些终端上单个桌面以全屏模式运行。请遵循上述所有托管用户设备的一般安全最佳实践。此版本的优势在于用户设备上所需的软件最少。

托管用户设备可以配置为仅在全屏模式或窗口模式下使用：

- 仅全屏模式：用户使用常规的“登录到 Windows”屏幕登录。然后，相同的用户凭据将用于自动登录到此版本。
- 用户在窗口中看到其桌面：用户首先登录到用户设备，然后通过此版本随附的网站登录到此版本。

### 非托管用户设备

不受信任组织管理和维护的用户设备不能被视为处于管理控制之下。例如，您可能允许用户获取和配置自己的设备，但用户可能不遵循上述一般安全最佳实践。此版本的优势在于，它可以安全地将桌面交付给非托管用户设备。这些设备仍应具有基本的防病毒保护，以抵御键盘记录器和类似的输入攻击。

### 数据存储注意事项

使用此版本时，您可以阻止用户将数据存储在其物理控制下的用户设备上。但是，您仍然必须考虑用户将数据存储在桌面上的影响。用户将数据存储在桌面上不是一个好习惯；数据应保存在文件服务器、数据库服务器或其他可以得到适当保护的存储库中。

您的桌面环境可能包含各种类型的桌面，例如池化桌面和专用桌面。用户绝不应将数据存储在用户之间共享的桌面（例如池化桌面）上。如果用户将数据存储在专用桌面上，则如果该桌面稍后可供其他用户使用，则应删除该数据。

### 混合版本环境

在某些升级过程中，混合版本环境是不可避免的。请遵循最佳实践，并尽量缩短不同版本 Citrix 组件共存的时间。在混合版本环境中，安全策略（例如）可能无法统一执行。

> **注意：**
>
> 这与其他软件产品类似；使用早期版本的 Active Directory 只能部分地与更高版本的 Windows 强制执行组策略。

> 以下场景描述了在特定混合版本 Citrix 环境中可能发生的安全问题。当使用 Citrix Receiver 1.7 连接到在 XenApp and XenDesktop 7.6 Feature Pack 2 中运行 VDA 的虚拟桌面时，站点中会启用策略设置 **允许桌面与客户端之间传输文件**，但运行 XenApp and XenDesktop 7.1 的 Delivery Controller 无法禁用此设置。它无法识别此策略设置，因为此设置是在产品的更高版本中发布的。此策略设置允许用户将文件上传和下载到其虚拟桌面，这就是安全问题。要解决此问题，请将 Delivery Controller（或 Studio 的独立实例）升级到 7.6 Feature Pack 2 版本，然后使用组策略禁用此策略设置。或者，在所有受影响的虚拟桌面上使用本地策略。

## 远程电脑访问安全注意事项

远程电脑访问实施以下安全功能：

- 支持智能卡使用。
- 当远程会话连接时，办公室电脑的显示器将显示为空白。
- 远程电脑访问将所有键盘和鼠标输入重定向到远程会话，但 CTRL+ALT+DEL 以及支持 USB 的智能卡和生物识别设备除外。
- SmoothRoaming 仅支持单个用户。
- 当用户将远程会话连接到办公室电脑时，只有该用户可以恢复对办公室电脑的本地访问。要恢复本地访问，用户需在本地电脑上按 Ctrl-Alt-Del，然后使用远程会话所用的相同凭据登录。如果您

的系统具有适当的第三方凭据提供程序集成，用户还可以通过插入智能卡或利用生物识别技术来恢复本地访问。可以通过组策略对象 (GPO) 启用快速用户切换或编辑注册表来覆盖此默认行为。

**注意：**

Citrix 建议您不要将 VDA 管理员权限分配给普通会话用户。

### 自动分配

默认情况下，远程电脑访问支持将多个用户自动分配给 VDA。在 XenDesktop 5.6 Feature Pack 1 中，管理员可以使用 RemotePCAccess.ps1 PowerShell 脚本覆盖此行为。此版本使用注册表项来允许或禁止多个自动远程电脑分配；此设置适用于整个站点。

**注意：**

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

要将自动分配限制为单个用户：

在站点中的每个 Controller 上，设置以下注册表项：

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple
user assignment.
```

如果存在任何现有用户分配，请使用 SDK 命令将其删除，以便 VDA 随后有资格进行单个自动分配。

- 从 VDA 中删除所有已分配的用户：`$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`

- 从交付组中移除 VDA：`$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

重新启动物理办公电脑。

### XML 信任

XML 信任设置适用于使用以下项的部署：

- 本地 StoreFront。
- 不需要密码的订阅者（用户）身份验证技术。此类技术的示例包括域直通、智能卡、SAML 和 Veridium 解决方案。

启用 XML 信任设置允许用户成功进行身份验证，然后启动应用程序。交付控制器信任从 StoreFront 发送的凭据。仅当您已确保交付控制器和 StoreFront 之间的通信安全（使用防火墙、IPsec 或其他安全建议）时，才启用此设置。

此设置默认禁用。

使用 Citrix Virtual Apps and Desktops PowerShell SDK 检查、启用或禁用 XML 信任设置。

- 要检查 XML 信任设置的当前值，请运行 `Get-BrokerSite` 并检查 `TrustRequestsSentToTheXMLServicePort` 的值。
- 要启用 XML 信任，请运行 `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true`。
- 要禁用 XML 信任，请运行 `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false`。

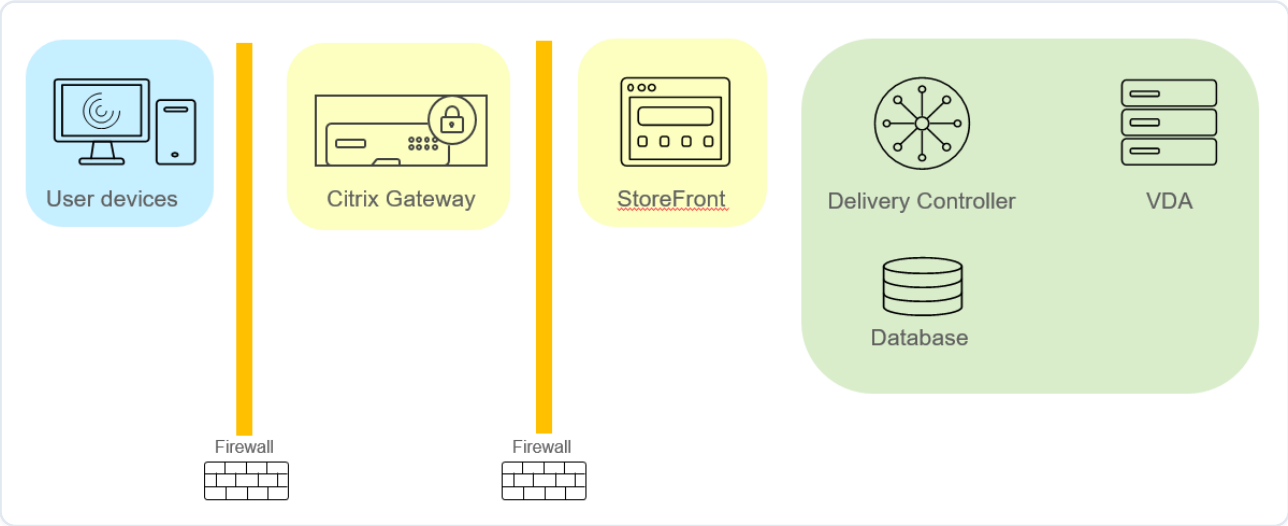
## 集成 思杰虚拟应用和桌面™ 与 思杰网关

StoreFront™ 服务器已部署并配置，以管理对已发布的资源和数据的访问。对于远程访问，建议在 StoreFront 前添加 Citrix Gateway。

> **注意：**

> 有关如何集成 Citrix Virtual Apps and Desktops 与 Citrix Gateway 的详细配置步骤，请参阅 StoreFront 文档。

以下图表说明了包含 Citrix Gateway 的简化 Citrix 部署示例。Citrix Gateway 与 StoreFront 通信，以保护 Citrix Virtual Apps and Desktops 交付的应用程序和数据。用户设备运行 Citrix Workspace™ 应用程序以创建安全连接并访问其应用程序、桌面和文件。




用户使用 Citrix Gateway 登录并进行身份验证。Citrix Gateway 部署在 DMZ 中并受到保护。已配置双因素身份验证。根据用户凭据，用户将获得相关的资源和应用程序。应用程序和数据位于适当的服务器上（图中未显示）。针对安全敏感的应用程序和数据使用单独的服务器。

## 委派管理

委派管理模型提供了灵活性，可根据您的组织希望如何委派管理活动（使用基于角色和基于对象的控制）进行匹配。委派管理适用于所有规模的部署，并允许您随着部署复杂性的增加配置更精细的权限。委派管理使用三个概念：管理员、角色和范围。

- **管理员：** 管理员代表由其 Active Directory 帐户标识的个人或人群。每个管理员都与一个或多个角色和范围对相关联。
- **角色：** 角色代表一项职能，并具有与之关联的已定义权限。例如，“交付组管理员”角色具有“创建交付组”和“从交付组中删除桌面”等权限。管理员可以为一个站点拥有多个角色，因此一个人可以是交付组管理员，也可以是计算机目录管理员。角色可以是内置的，也可以是自定义的。

  内置角色包括：

| 角色 | 权限 |
| --- | --- |
| 完全管理员 | 可以执行所有任务和操作。完全管理员始终与“所有”范围结合使用。 |
| 只读管理员 | 除了全局信息外，可以查看指定范围内的所有对象，但不能更改任何内容。例如，具有“范 |

| 角色 | 权限 |
| --- | --- |
| | 围=伦敦”的只读管理员可以查看所有全局对象（例如配置日志记录）和任何伦敦范围的对象（例如伦敦交付组）。但是，该管理员无法查看纽约范围内的对象（假设伦敦和纽约范围不重叠）。 |
| 帮助台管理员 | 可以查看交付组，并管理与这些组关联的会话和计算机。可以查看受监控交付组的计算机目录和主机信息。还可以对这些交付组中的计算机执行会话管理和计算机电源管理操作。 |
| 计算机目录管理员 | 可以创建和管理计算机目录，并将计算机预配到其中。可以从虚拟化基础架构、Provisioning Services 和物理机构建计算机目录。此角色可以管理基础映像和安装软件，但不能将应用程序或桌面分配给用户。 |
| 交付组管理员 | 可以交付应用程序、桌面和计算机；还可以管理关联的会话。还可以管理应用程序和桌面配置，例如策略和电源管理设置。 |
| 主机管理员 | 可以管理主机连接及其关联的资源设置。不能向用户交付计算机、应用程序或桌面。 |

在某些产品版本中，您可以创建自定义角色以满足您的组织要求，并更详细地委派权限。您可以使用自定义角色以控制台中操作或任务的粒度分配权限。

- **范围：** 范围代表对象的集合。范围用于以与您的组织相关的方式对对象进行分组（例如，销售团队使用的交付组集合）。对象可以存在于多个范围中；您可以将对象视为用一个或多个范围标记。有一个内置范围：“所有”，其中包含所有对象。完全管理员角色始终与“所有”范围配对。

## 示例

XYZ 公司决定根据其部门（财务、销售和仓库）及其桌面操作系统（Windows 7 或 Windows 8）来管理应用程序和桌面。管理员创建了五个范围，然后为每个交付组标记了两个范围：一个用于它们所使用的部门，一个用于它们所使用的操作系统。

创建了以下管理员：

| 管理员 | 角色 | 作用域 |
| --- | --- | --- |
| domain/fred | 完全管理员 | 所有（完全管理员角色始终具有“所有”作用域） |
| domain/rob | 只读管理员 | 所有 |
| domain/heidi | 只读管理员，技术支持管理员 | 所有销售 |
| domain/warehouseadmin | 帮助台管理员 | 仓库 |
| domain/peter | 交付组管理员、计算机目录管理员 | Win7 |

- Fred 是完全管理员，可以查看、编辑和删除系统中的所有对象。
- Rob 可以查看站点中的所有对象，但无法编辑或删除它们。
- Heidi 可以查看所有对象，并可以在销售范围内的交付组上执行技术支持任务。这使她能够管理与这些组关联的会话和计算机；她无法对交付组进行更改，例如添加或删除计算机。
- 任何属于 warehouseadmin Active Directory 安全组的成员都可以查看并对仓库范围内的计算机执行技术支持任务。
- Peter 是一名 Windows 7 专家，可以管理所有 Windows 7 计算机目录，并可以交付 Windows 7 应用程序、桌面和计算机，无论它们属于哪个部门范围。管理员曾考虑将 Peter 设置为 Win7 范围的完全管理员。但是，她决定不这样做，因为完全管理员还对所有未限定范围的对象（例如“站点”和“管理员”）拥有完全权限。

## 如何使用委派管理

通常，管理员的数量及其权限的粒度取决于部署的规模和复杂性。

- 在小型或概念验证部署中，一两个管理员负责所有事务。没有委派。在这种情况下，使用内置的完全管理员角色（具有“所有”范围）创建每个管理员。
- 在具有更多计算机、应用程序和桌面的大型部署中，需要更多的委派。多个管理员可能具有更具体的功能职责（角色）。例如，其中两名是完全管理员，其他是技术支持管理员。此外，管理员可能只管理特定对象组（范围），例如计算机目录。在这种情况下，创建新范围，并创建具有内置角色之一和相应范围的管理员。
- 更大的部署可能需要更多（或更具体）的范围，以及具有非常规角色的不同管理员。在这种情况下，编辑或创建更多范围，创建自定义角色，并使用内置或自定义角色以及现有和新范围创建每个管理员。

为了灵活性和易于配置，您可以在创建管理员时创建范围。您还可以在创建或编辑计算机目录或连接时指定范围。

## 创建和管理管理员

当您以本地管理员身份创建站点时，您的用户帐户会自动成为完全管理员，对所有对象拥有完全权限。站点创建后，本地管理员没有特殊权限。

完全管理员角色始终具有所有范围；您无法更改此设置。

默认情况下，管理员处于启用状态。如果您现在正在创建管理员，但该人员稍后才会开始管理职责，则可能需要禁用该管理员。对于现有已启用的管理员，您可能希望在重新组织对象/范围时禁用其中几个，然后在准备好使用更新的配置上线时重新启用它们。如果禁用完全管理员会导致没有已启用的完全管理员，则无法禁用该完全管理员。在创建、复制或编辑管理员时，可以使用启用/禁用复选框。

在复制、编辑或删除管理员时，如果您删除角色/范围对，它只会删除该管理员的角色与范围之间的关系。它不会删除角色或范围。它也不会影响配置了该角色/范围对的任何其他管理员。

要管理管理员，请在 Studio 导航窗格中单击**配置 > 管理员**，然后单击上方中间窗格中的**管理员**选项卡。

- **创建管理员：** 在“操作”窗格中单击**创建新管理员**。键入或浏览到用户帐户名，选择或创建范围，然后选择角色。新管理员默认启用；您可以更改此设置。
- **复制管理员：** 在中间窗格中选择管理员，然后在“操作”窗格中单击**复制管理员**。键入或浏览到用户帐户名。您可以选择然后编辑或删除任何角色/范围对，并添加新的。新管理员默认启用；您可以更改此设置。
- **编辑管理员：** 在中间窗格中选择管理员，然后在“操作”窗格中单击**编辑管理员**。您可以编辑或删除任何角色/范围对，并添加新的。
- **删除管理员：** 在中间窗格中选择管理员，然后在“操作”窗格中单击**删除管理员**。如果删除完全管理员会导致没有启用的完全管理员，则无法删除该完全管理员。

上方窗格显示您创建的管理员。选择一个管理员可在下方窗格中查看其详细信息。**警告**列指示与管理员关联的角色和范围对是否包含不可用的角色或范围。如果关联的角色和范围对包含不可用的角色或范围，则会出现以下警告消息：

- 关联的角色或范围不可用
    - 从管理员中删除角色和范围对。

**重要提示：**

仅当关联的角色和范围对包含不可用的角色、不可用的范围或两者都包含时，才会出现警告消息。

要从管理员中删除角色和范围对，请完成以下步骤之一：

- 删除角色和范围对。
  a. 在**操作**窗格中，单击**编辑管理员**。
  b. 在**编辑管理员**窗口中，选择角色和范围对，然后单击**删除**。
  c. 单击**确定**退出。
- 删除管理员。
  a. 在**操作**窗格中，单击**删除管理员**。
  b. 在 **Studio** 窗口中，单击**删除**。

## 创建和管理角色

管理员创建或编辑角色时，只能启用其自身拥有的权限。这可以防止管理员创建权限高于其当前权限的角色，然后将其分配给自己（或编辑已分配给他们的角色）。

角色名称最多可包含 64 个 Unicode 字符；不能包含：反斜杠、正斜杠、分号、冒号、井号、逗号、星号、问号、等号、左箭头或右箭头、管道符、左方括号或右方括号、左括号或右括号、引号或撇号。描述最多可包含 256 个 Unicode 字符。

您无法编辑或删除内置角色。如果任何管理员正在使用自定义角色，则无法删除该角色。

**注意：**

只有某些产品版本支持自定义角色。只有支持自定义角色的版本才在“操作”窗格中包含相关条目。

要管理角色，请在 Studio 导航窗格中单击“**配置 > 管理员**”，然后在上方中间窗格中单击“**角色**”选项卡。

- **查看角色详细信息：** 在中间窗格中选择角色。中间窗格的下半部分列出了该角色适用的对象类型和关联权限。单击下部窗格中的“管理员”选项卡可显示当前拥有此角色的管理员列表。
- **创建自定义角色：** 在“操作”窗格中单击“**创建新角色**”。输入名称和描述。选择对象类型和权限。
- **复制角色：** 在中间窗格中选择角色，然后在“操作”窗格中单击“**复制角色**”。根据需要更改名称、描述、对象类型和权限。
- **编辑自定义角色：** 在中间窗格中选择角色，然后在“操作”窗格中单击“**编辑角色**”。根据需要更改名称、描述、对象类型和权限。
- **删除自定义角色：** 在中间窗格中选择角色，然后在“操作”窗格中单击“**删除角色**”。出现提示时，确认删除。

## 创建和管理范围

创建站点时，唯一可用的作用域是“所有”作用域，该作用域无法删除。

您可以使用以下过程创建作用域。您还可以在创建管理员时创建作用域；每个管理员必须至少与一个角色和作用域对关联。创建或编辑桌面、计算机目录、应用程序或主机时，您可以将其添加到现有作用域。如果不将其添加到作用域，它们将保留在“所有”作用域中。

站点创建无法限定范围，委派管理对象（范围和角色）也无法限定范围。但是，无法限定范围的对象将包含在“所有”范围中。（完全管理员始终拥有“所有”范围。）计算机、电源操作、桌面和会话不直接限定范围。管理员可以通过关联的计算机目录或交付组获得这些对象的权限。

范围名称最多可包含 64 个 Unicode 字符。范围名称不能包含：反斜杠、正斜杠、分号、冒号、井号、逗号、星号、问号、等号、左箭头、右箭头、管道符、左方括号或右方括号、左括号或右括号、引号或撇号。描述最多可包含 256 个 Unicode 字符。

复制或编辑作用域时，请记住，从作用域中删除对象可能会导致管理员无法访问这些对象。如果编辑后的作用域与一个或多个角色配对，请确保作用域更新不会导致任何角色/作用域对无法使用。

要管理范围，请在 Studio 导航窗格中单击“**配置 > 管理员**”，然后在上方中间窗格中单击“**范围**”选项卡。

- **创建范围：** 在“操作”窗格中单击“**创建新范围**”。输入名称和描述。要包含特定类型的所有对象（例如，交付组），请选择对象类型。要包含特定对象，请展开该类型，然后选择单个对象（例如，销售团队使用的交付组）。
- **复制范围：** 在中间窗格中选择范围，然后在“操作”窗格中单击“**复制范围**”。输入名称和描述。根据需要更改对象类型和对象。
- **编辑范围：** 在中间窗格中选择范围，然后在“操作”窗格中单击“**编辑范围**”。根据需要更改名称、描述、对象类型和对象。

- **删除范围：** 在中间窗格中选择范围，然后在“操作”窗格中单击“**删除范围**”。出现提示时，确认删除。

## 创建报告

您可以创建两种类型的委派管理报告：

- 一份 HTML 报告，其中列出了与管理员关联的角色/范围对，以及每种对象类型（例如，交付组和计算机目录）的单独权限。您可以从 Studio 生成此报告。

  要创建此报告，请在 Studio 导航窗格中单击“**配置 > 管理员**”。在中间窗格中选择一个管理员，然后在“操作”窗格中单击“**创建报告**”。

  您也可以在创建、复制或编辑管理员时请求此报告。

- 一份 HTML 或 CSV 报告，将所有内置和自定义角色映射到权限。您可以通过运行名为 OutputPermissionMapping.ps1 的 PowerShell 脚本来生成此报告。

  要运行此脚本，您必须是完全管理员、只读管理员或具有读取角色权限的自定义管理员。该脚本位于：Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts。

  语法：

  `OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]`

| 参数 | 描述 |
| --- | --- |
| `-Help` | 显示脚本帮助。 |
| `-Csv` | 指定 CSV 输出。默认值 = HTML |
| `-Path string` | 输出写入位置。默认值 = stdout |
| `-AdminAddress string` | 要连接的 Delivery Controller™ 的 IP 地址或主机名。默认值 = localhost |
| `-Show` | （仅当也指定了 `-Path` 参数时有效）当您将输出写入文件时，`-Show` 会导致输出在适当的程序（例如 Web 浏览器）中打开。 |
| 通用参数 | `Verbose`、`Debug`、`ErrorAction`、`ErrorVariable`、`WarningAction`、`WarningVariable`、`OutBuffer` 和 |

| 参数 | 描述 |
| --- | --- |
| | `OutVariable`。有关详细信息，请参阅 Microsoft 文档。 |

以下示例将 HTML 表写入名为 Roles.html 的文件，并在 Web 浏览器中打开该表。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

-Path Roles.html –Show
```

以下示例将 CSV 表写入名为 Roles.csv 的文件。该表不显示。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

–CSV -Path Roles.csv
```

在 Windows 命令提示符下，前面的示例命令是：

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'

-CSV -Path Roles.csv"
```

# 管理安全密钥

**注意：**

- 您必须将此功能与 StoreFront™ 1912 LTSR CU2 或更高版本结合使用。
- Secure XML 功能仅在 Citrix ADC 和 Citrix Gateway 12.1 及更高版本上受支持。

> 此功能允许您仅授权经批准的 StoreFront 和 Citrix Gateway 计算机与 Citrix Delivery Controllers 通信。启用此功能后，任何不包含密钥的请求都将被阻止。使用此功能可增加一层安全性，以防范源自内部网络的攻击。

使用此功能的通用工作流程如下：

1. 启用 Studio 以显示功能设置。
2. 配置站点的设置。
3. 在 StoreFront 中配置设置。
4. 在 Citrix ADC 中配置设置。

## 启用 Studio 以显示功能设置

默认情况下，安全密钥的设置在 Studio 中是隐藏的。要启用 Studio 以显示这些设置，请按如下方式使用 PowerShell SDK：

1. 运行 Citrix Virtual Apps and Desktops™ PowerShell 开发工具包。
2. 在命令窗口中，运行以下命令：
   - `Add-PSSnapIn Citrix*`。此命令添加 Citrix 管理单元。
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManagementEnabled" -Value "True"`

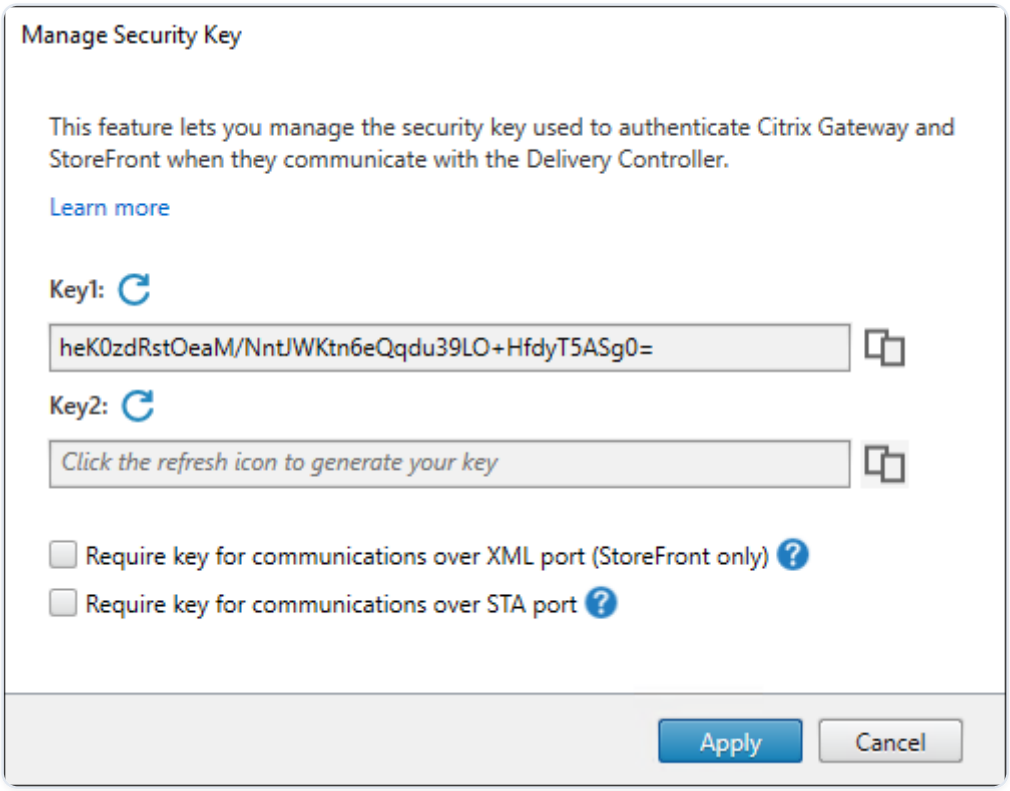
有关 PowerShell SDK 的详细信息，请参阅 SDK 和 API。

## 配置站点的设置

您可以使用 Studio 或 PowerShell 为您的站点配置安全密钥设置。

### 使用 Studio 控制台

1. 导航到 **Studio > 设置 > 管理安全密钥**，然后单击**编辑**。将显示**管理安全密钥**窗口。




**重要提示：**

- 有两个可用的密钥。您可以对通过 XML 和 STA 端口进行的通信使用相同密钥或不同密钥。我们建议您一次只使用一个密钥。未使用的密钥仅用于密钥轮换。
- 请勿单击刷新图标来更新已在使用的密钥。否则，服务将中断。

2. 单击刷新图标以生成新密钥。
3. 选择需要密钥的位置：
   - **要求通过 XML 端口进行通信时使用密钥（仅限 StoreFront）**。如果选中此选项，则要求使用密钥对通过 XML 端口进行的通信进行身份验证。StoreFront 通过此端口与 Citrix Cloud 通信。有关更改 XML 端口的信息，请参阅知识中心文章 CTX127945。
   - **要求通过 STA 端口进行通信时使用密钥**。如果选中此选项，则要求使用密钥对通过 STA 端口进行的通信进行身份验证。Citrix Gateway 和 StoreFront 通过此端口与 Citrix Cloud 通信。有关更改 STA 端口的信息，请参阅知识中心文章 CTX101988。
4. 单击“**保存**”以应用更改并退出窗口。

### 使用 PowerShell

以下是与 Studio 操作等效的 PowerShell 步骤。

1. 运行 Citrix Virtual Apps and Desktops 远程 PowerShell 开发工具包。
2. 在命令窗口中，运行以下命令：
   - `Add-PSSnapIn Citrix*`
3. 运行以下命令以生成密钥并设置 Key1：
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. 运行以下命令以生成密钥并设置 Key2：
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. 运行以下一个或两个命令以启用密钥用于身份验证通信：
   - 要通过 XML 端口验证通信：
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - 要通过 STA 端口验证通信：
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

有关指导和语法，请参阅 PowerShell 命令帮助。

## 在 StoreFront 中配置设置

完成站点的配置后，需要使用 PowerShell 在 StoreFront 中配置相关设置。

在 StoreFront 服务器上，运行以下 PowerShell 命令：

要配置用于通过 XML 端口进行通信的密钥，请使用命令 。例如：

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

为以下参数输入相应的值：

- `Path to store`
- `Resource feed name`
- `secret`

要配置通过 STA 端口进行通信的密钥，请使用 `New-STFSecureTicketAuthority` 和 `Set-STFRoamingGateway` 命令。例如：

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

为以下参数输入相应的值：

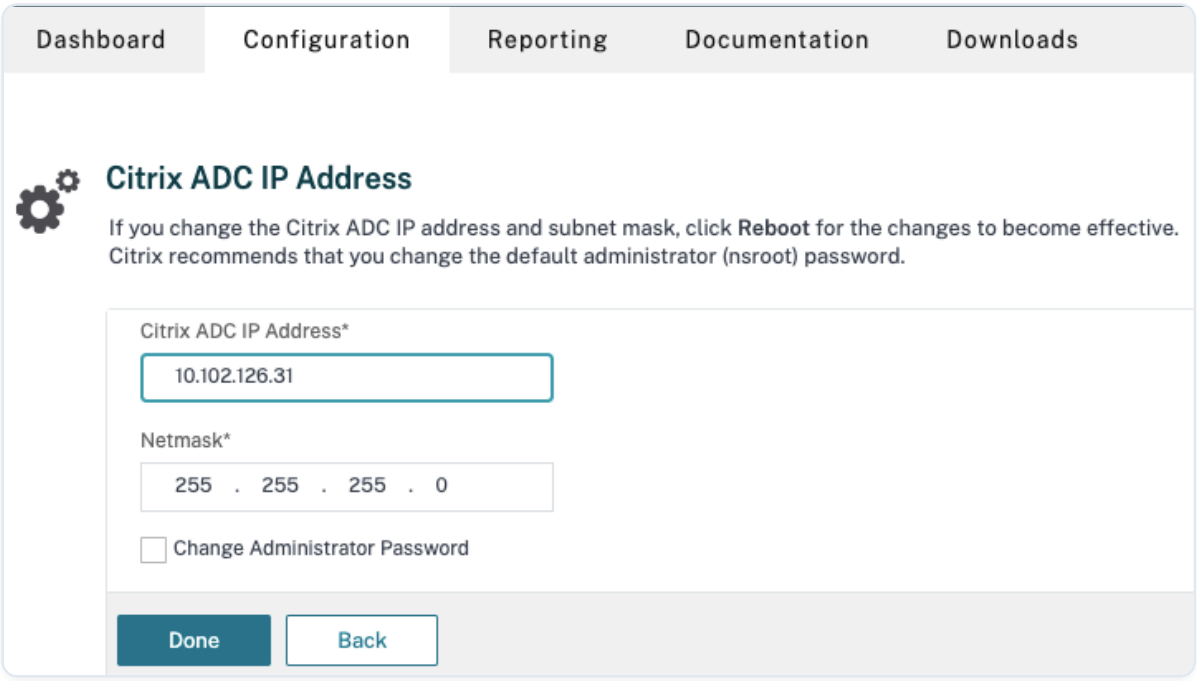
- `Gateway name`
- `STA URL`
- `Secret`

有关指导和语法，请参阅 PowerShell 命令帮助。

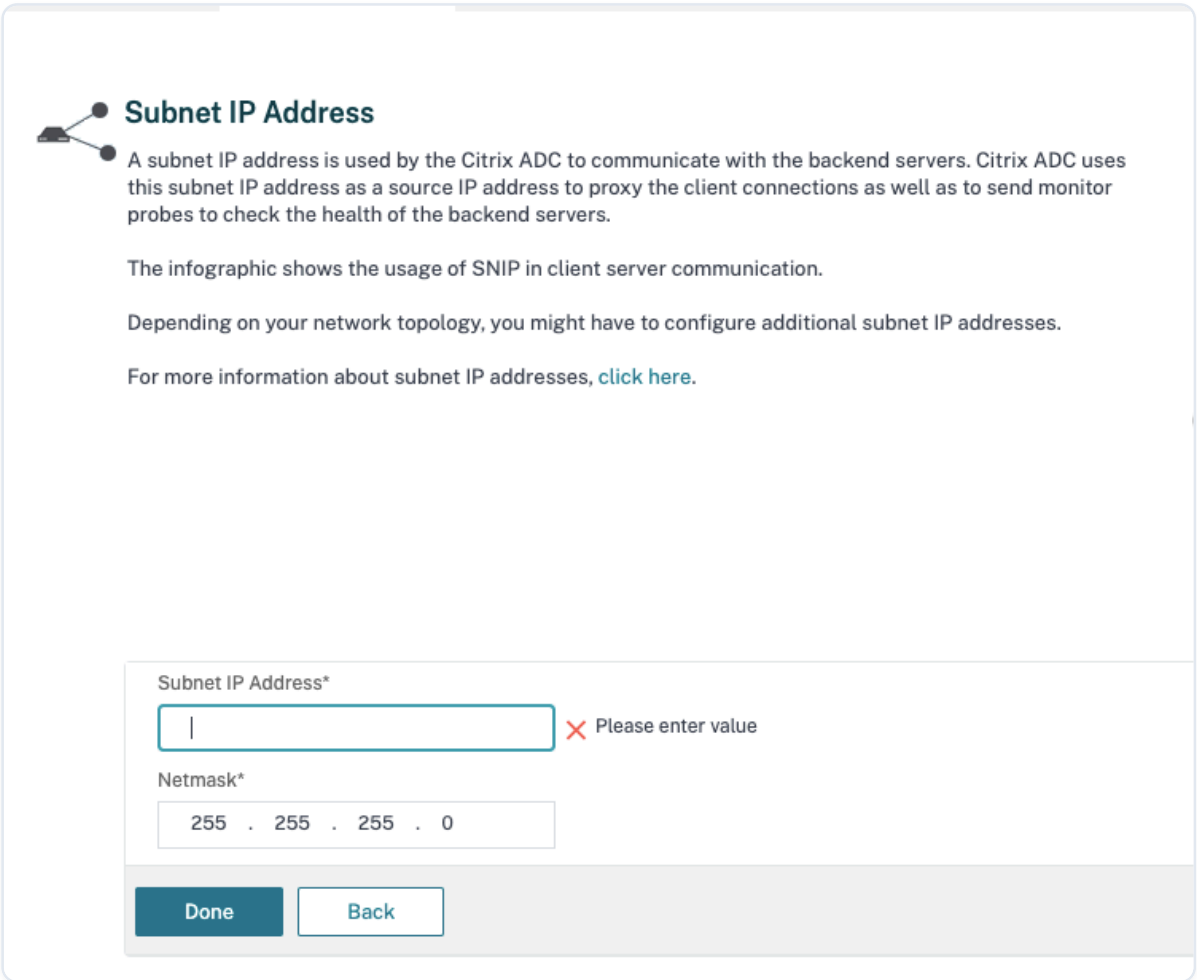
## 在 Citrix ADC 中配置设置

> **注意：**
>
> 除非您使用 Citrix ADC 作为网关，否则无需在 Citrix ADC 中配置此功能。如果您使用 Citrix ADC，请按照以下步骤操作。

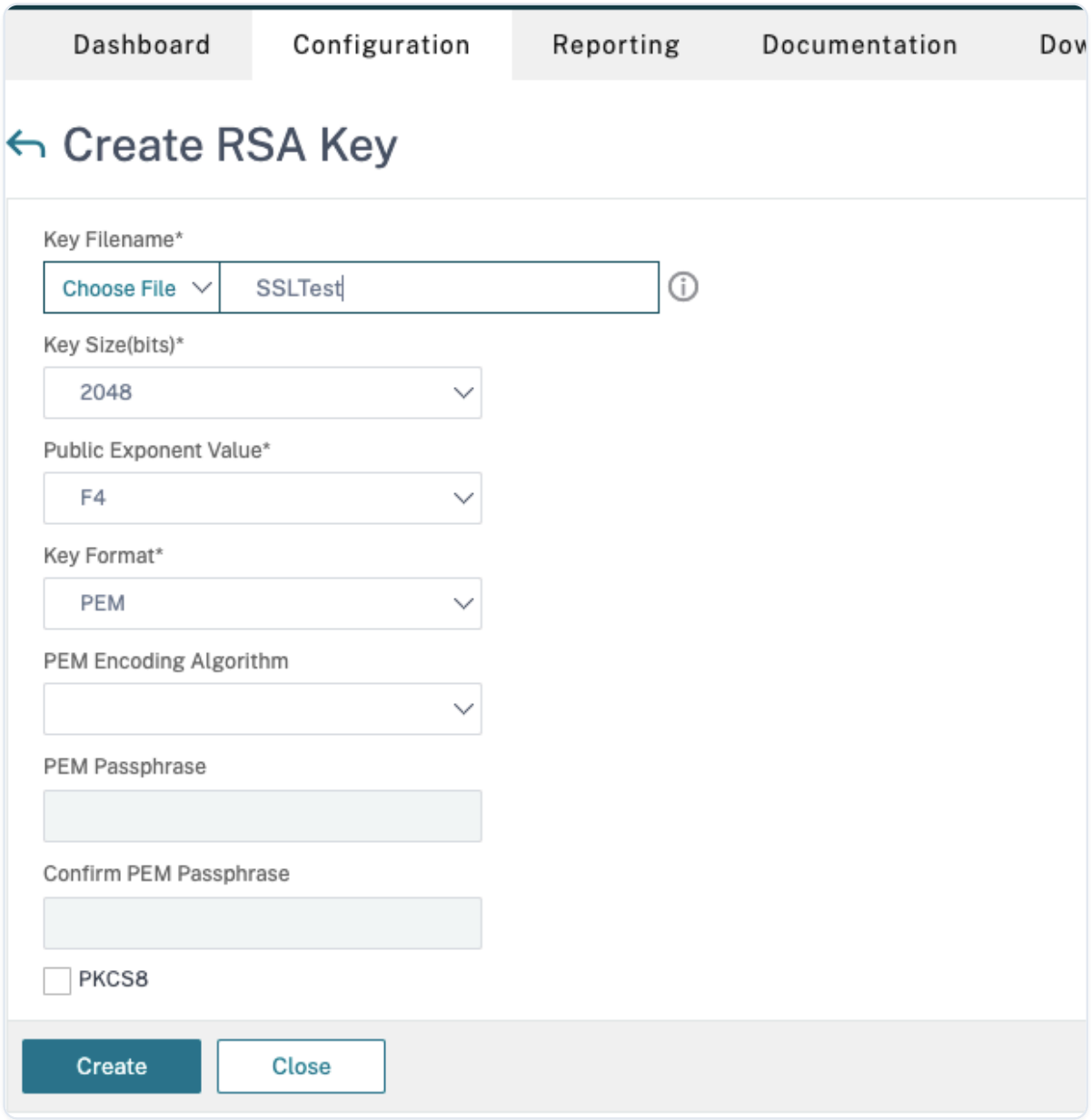
1. 确保已完成以下先决条件配置：
   - 已配置以下 Citrix ADC 相关 IP 地址。
     - 用于访问 Citrix ADC 控制台的 Citrix ADC 管理 IP (NSIP) 地址。有关详细信息，请参阅配置 NSIP 地址。



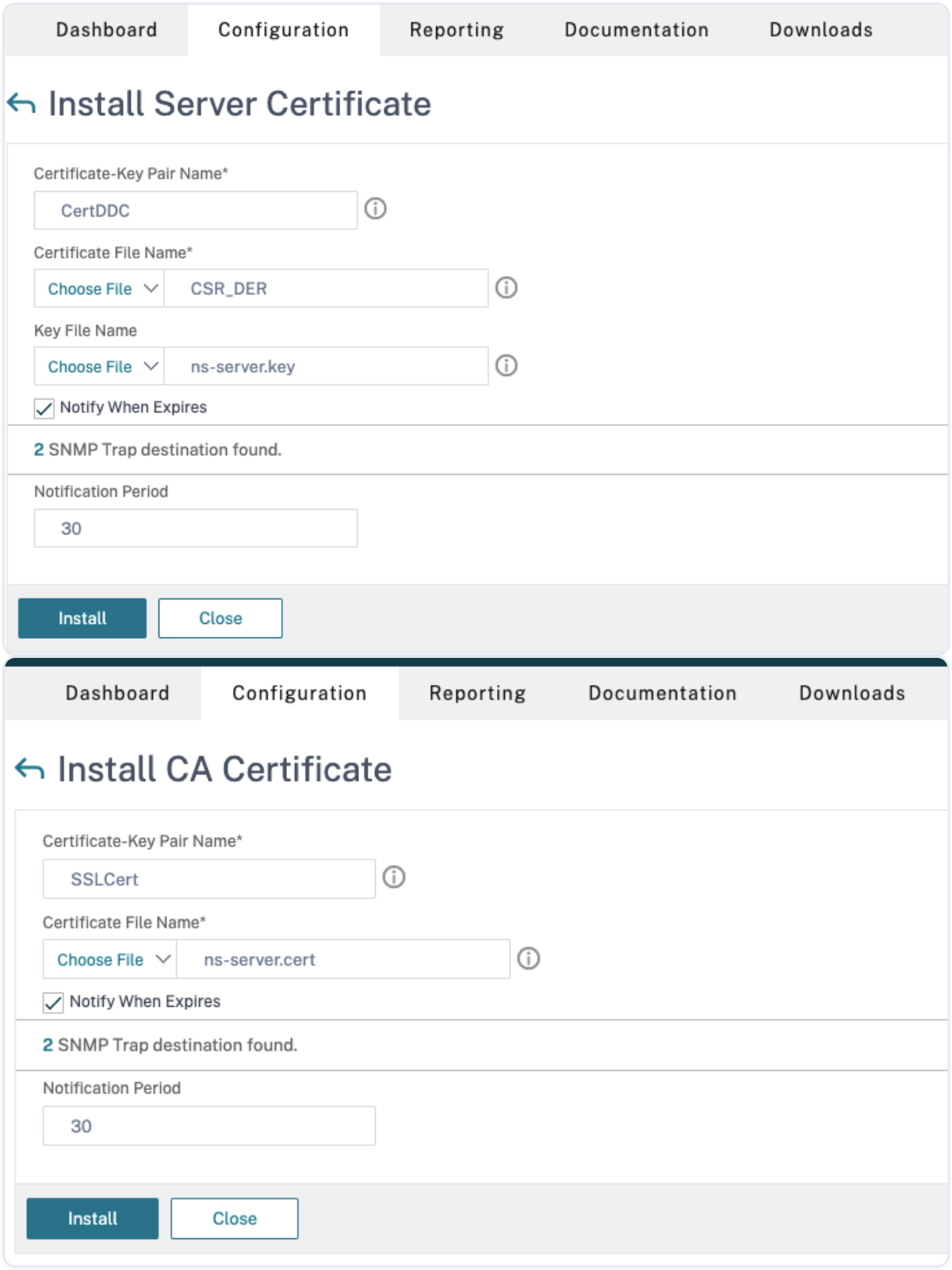

- 子网 IP (SNIP) 地址，用于启用 Citrix ADC 设备与后端服务器之间的通信。有关详细信息，请参阅 配置子网 IP 地址。
- Citrix Gateway 虚拟 IP 地址和负载均衡器虚拟 IP 地址，用于登录 ADC 设备以启动会话。有关详细信息，请参阅 创建虚拟服务器。



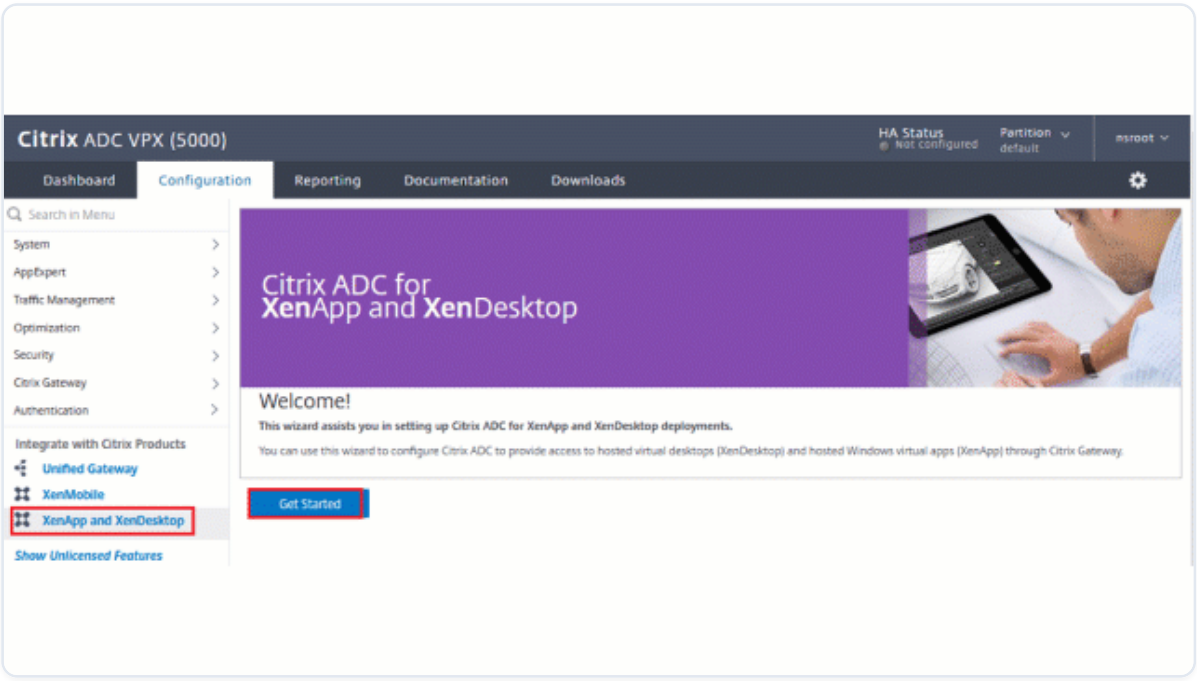
- Citrix ADC 设备中所需的模式和功能已启用。
  - 要启用这些模式，请在 Citrix ADC GUI 中导航到“**System > Settings > Configure Mode**”（系统 > 设置 > 配置模式）。
  - 要启用这些功能，请在 Citrix ADC GUI 中导航到“**System > Settings > Configure Basic Features**”（系统 > 设置 > 配置基本功能）。
- 证书相关配置已完成。
  - 证书签名请求 (CSR) 已创建。有关详细信息，请参阅 创建证书。




  - 服务器证书、CA 证书和根证书已安装。有关详细信息，请参阅 安装、链接和更新。



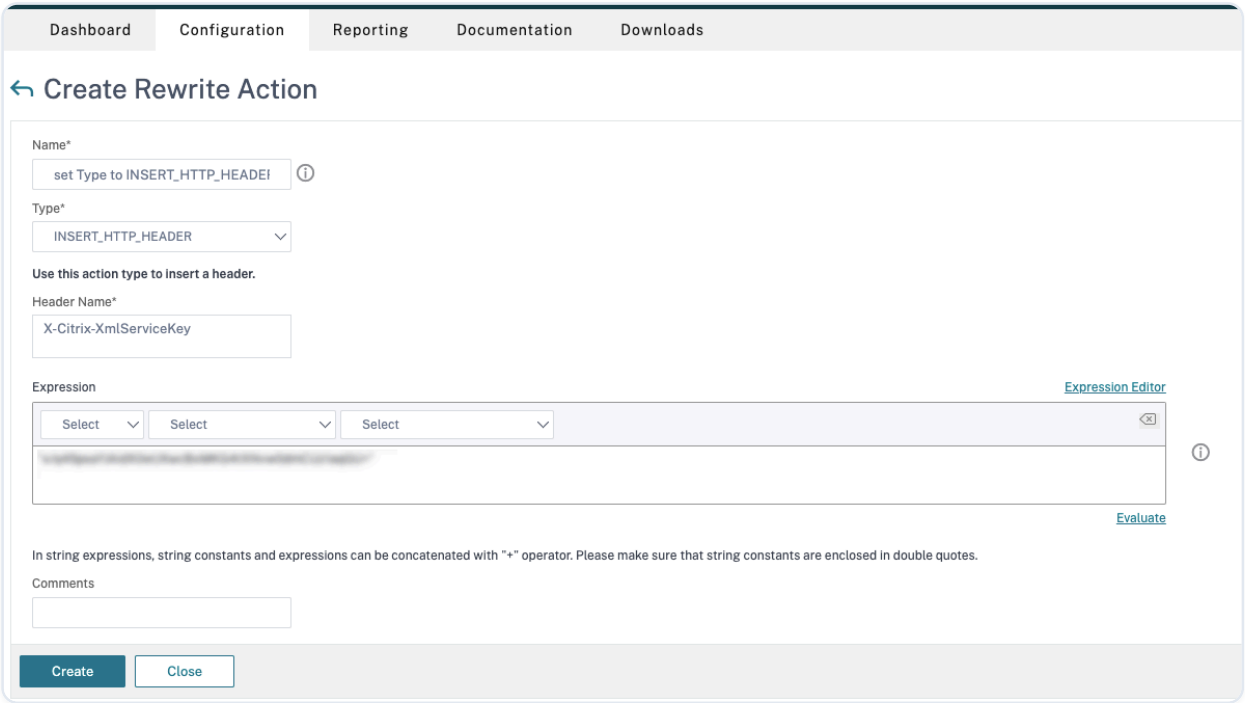

- 已为 Citrix Virtual Desktops 创建 Citrix Gateway。单击“**Test STA Connectivity**”（测试 STA 连接）按钮测试连接，以确认虚拟服务器在线。有关详细信息，请参阅为 Citrix Virtual Apps and Desktops 设置 Citrix ADC。




2. 添加重写操作。有关详细信息，请参阅 配置重写操作。

   a. 导航到“**AppExpert > Rewrite > Actions**”（AppExpert > 重写 > 操作）。

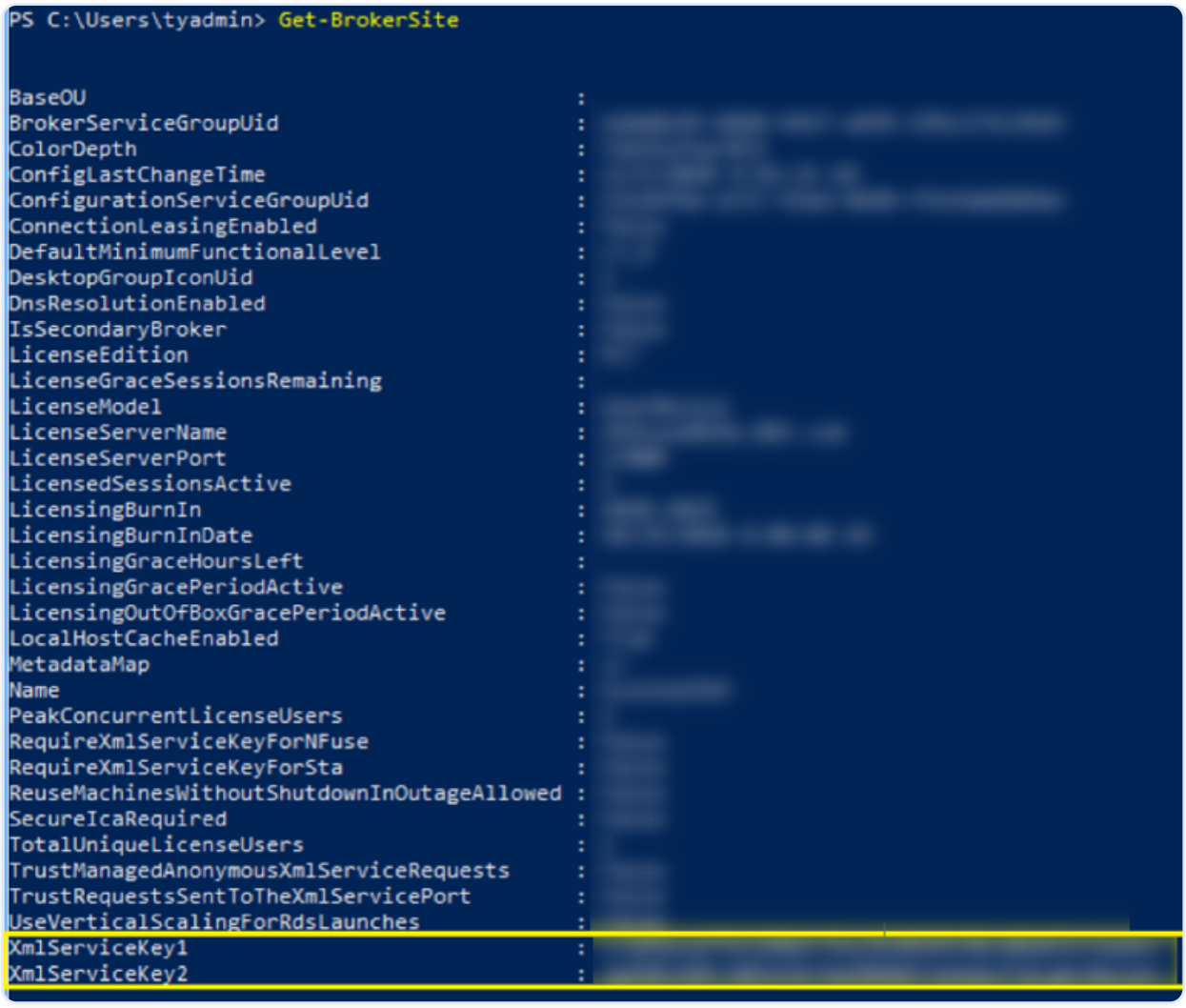
   b. 单击 **添加** 以添加新的重写操作。您可以将操作命名为“set Type to INSERT_HTTP_HEADER”。




   a. 在 **类型** 中，选择 **INSERT_HTTP_HEADER**。

   b. 在 **标头名称** 中，输入 X-Citrix-XmlServiceKey。

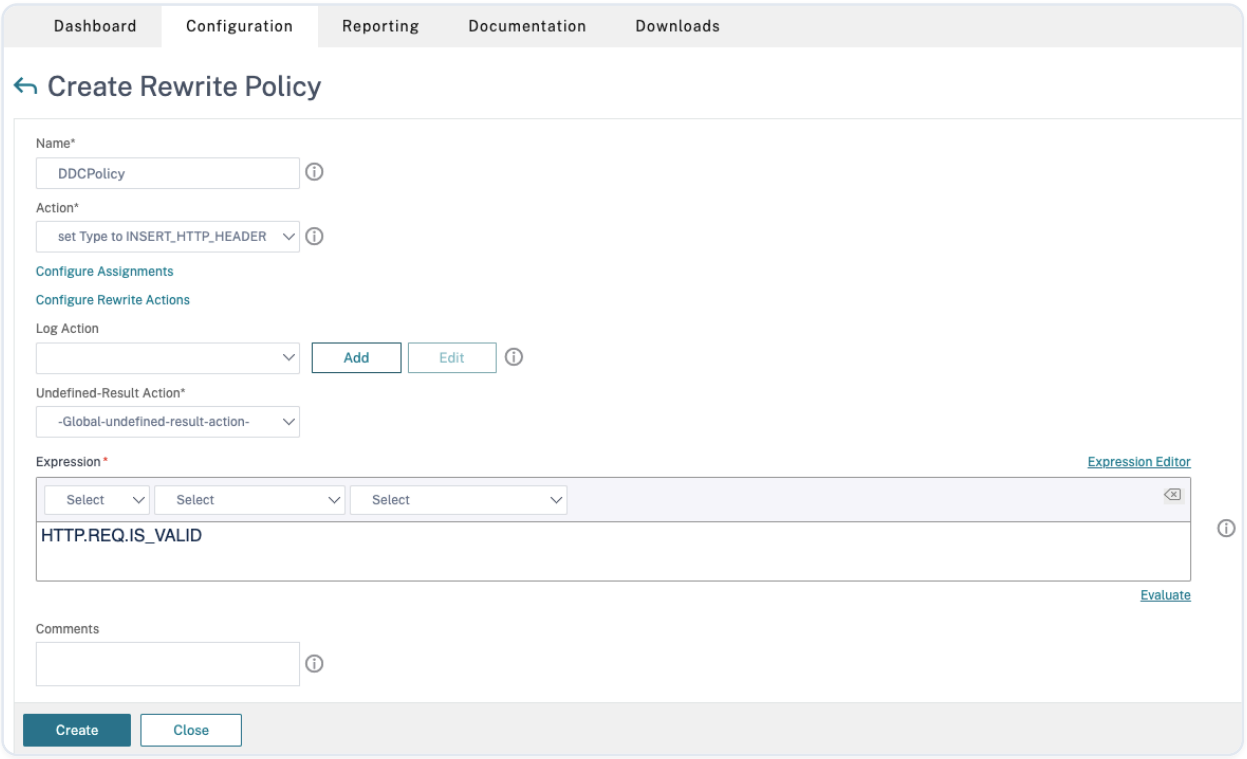
   c. 在 **表达式** 中，添加 `<XmlServiceKey1 value>` 并带引号。您可以从您的 Desktop Delivery Controller™ 配置中复制 XmlServiceKey1 值。




3. 添加重写策略。有关详细信息，请参阅配置重写策略。

   a. 导航到“**AppExpert > Rewrite > Policies**”（AppExpert > 重写 > 策略）。

   b. 单击 **添加** 以添加新策略。




a. 在 **操作** 中，选择上一步中创建的操作。

b. 在 **表达式** 中，添加 HTTP.REQ.IS_VALID。

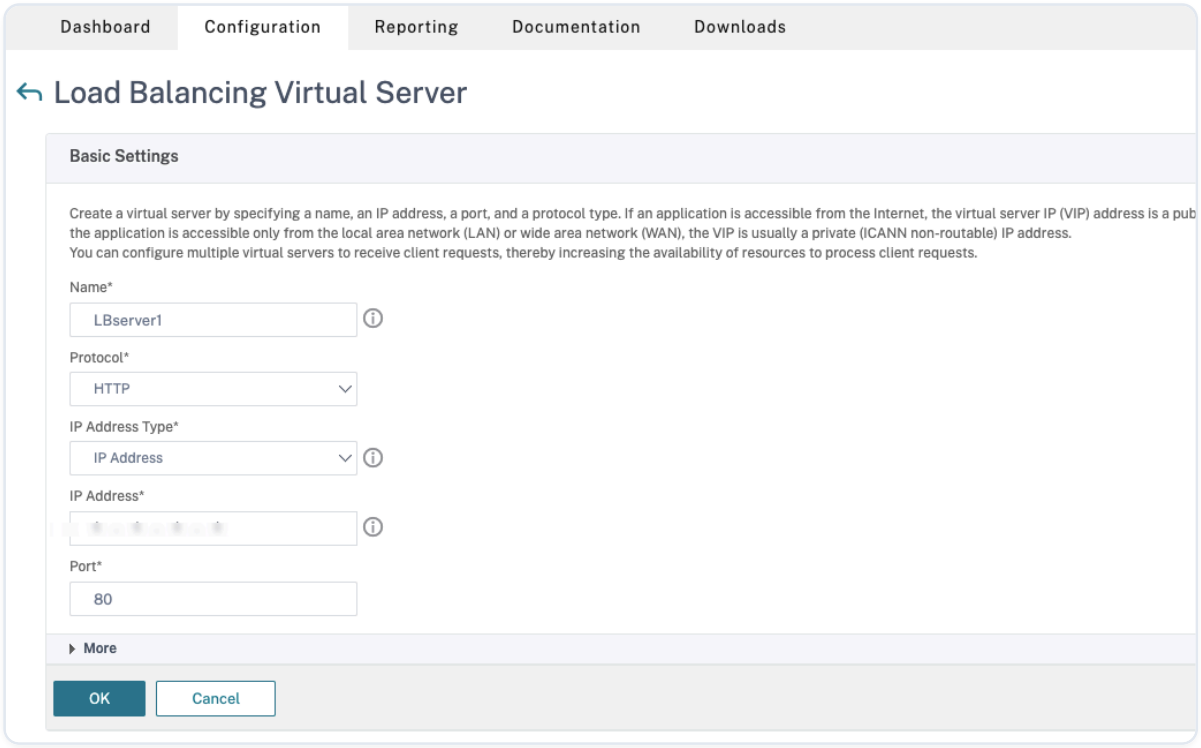
c. 单击 **确定**。

4. 设置负载平衡。您必须为每个 STA 服务器配置一个负载平衡虚拟服务器。否则会话将无法启动。

   有关详细信息，请参阅设置基本负载平衡。

   a. 创建负载平衡虚拟服务器。

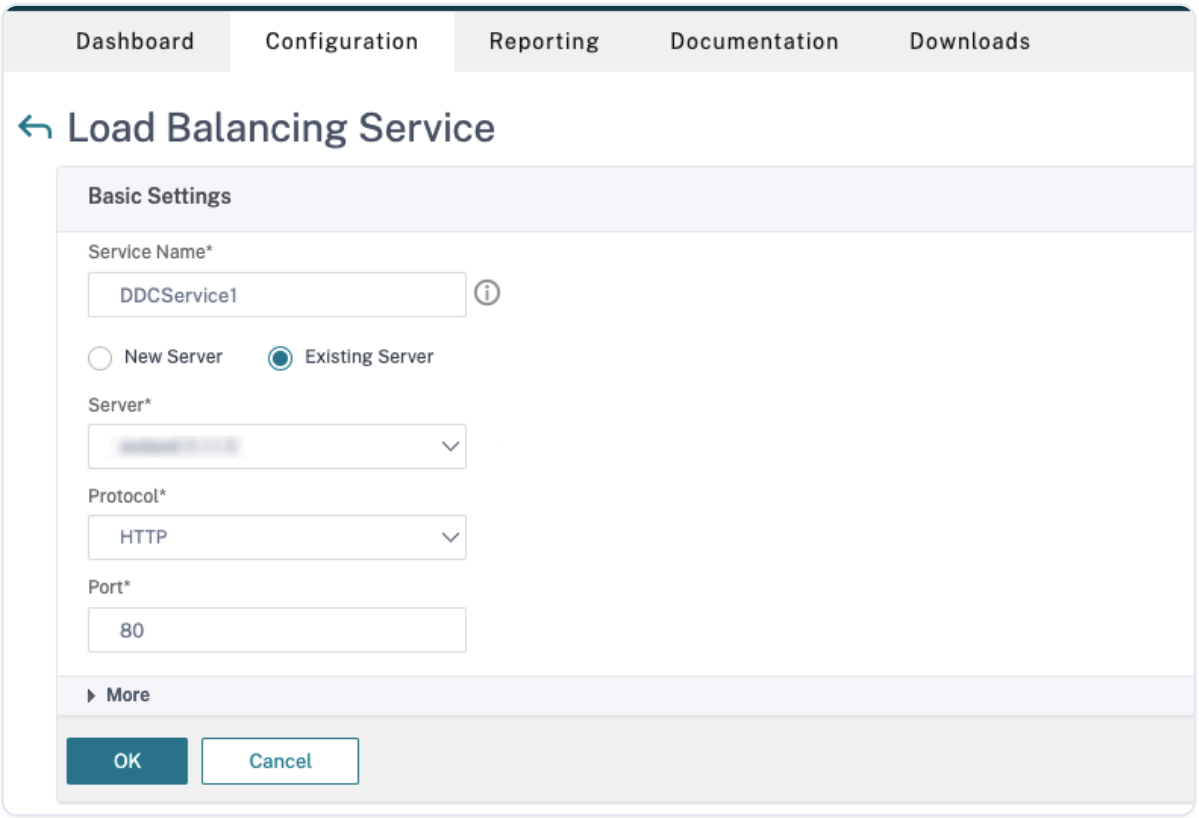
      - 导航到“**Traffic Management > Load Balancing > Servers**”（流量管理 > 负载平衡 > 服务器）。
      - 在“**Virtual Servers**”（虚拟服务器）页面上，单击“**Add**”（添加）。




- 在 **协议** 中，选择 **HTTP**。
- 添加负载平衡虚拟 IP 地址，并在 **端口** 中选择 **80**。
- 单击 **确定**。

b. 创建负载平衡服务。

- 导航到“**Traffic Management > Load Balancing > Services**”（流量管理 > 负载平衡 > 服务）。




- 在 **现有服务器** 中，选择上一步中创建的虚拟服务器。
- 在 **协议** 中，选择 **HTTP**，并在 **端口** 中选择 **80**。
- 单击 **确定**，然后单击 **完成**。

c. 将服务绑定到虚拟服务器。

- 选择之前创建的虚拟服务器，然后单击**编辑**。
- 在“**服务和服务组**”中，单击“**无负载平衡虚拟服务器服务绑定**”。

绑定服务到虚拟服务器(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-bind-service-to-lbvserver.png)

- 在“**Service Binding**”（服务绑定）中，选择之前创建的服务。
- 单击“**绑定**”。

d. 将之前创建的重写策略绑定到虚拟服务器。

- 选择之前创建的虚拟服务器，然后单击**编辑**。
- 在“**高级设置**”中，单击“**策略**”，然后在“**策略**”部分单击“**+**”。

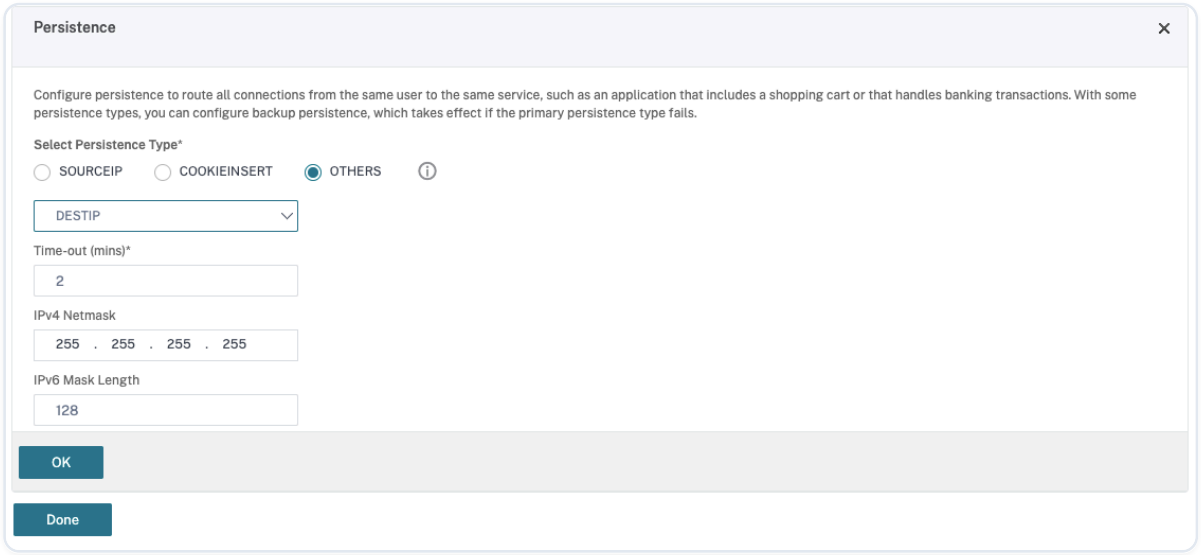
绑定重写策略(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-bind-rewrite-policy.png)

- 在“**选择策略**”中，选择“**重写**”，并在“**选择类型**”中，选择“**请求**”。

- 单击“**继续**”。
- 在“**选择策略**”中，选择之前创建的重写策略。
- 单击“**绑定**”。
- 点击 **完成**。

e. 如有必要，为虚拟服务器设置持久性。

- 选择之前创建的虚拟服务器，然后单击**编辑**。
- 在**高级设置**中，单击**持久性**。




- 选择持久性类型为**其他**。
- 选择 **DESTIP** 以根据虚拟服务器选择的服务 IP 地址（目标 IP 地址）创建持久性会话
- 在 **IPv4 Netmask** 中，添加与 DDC 相同的网络掩码。
- 单击 **确定**。

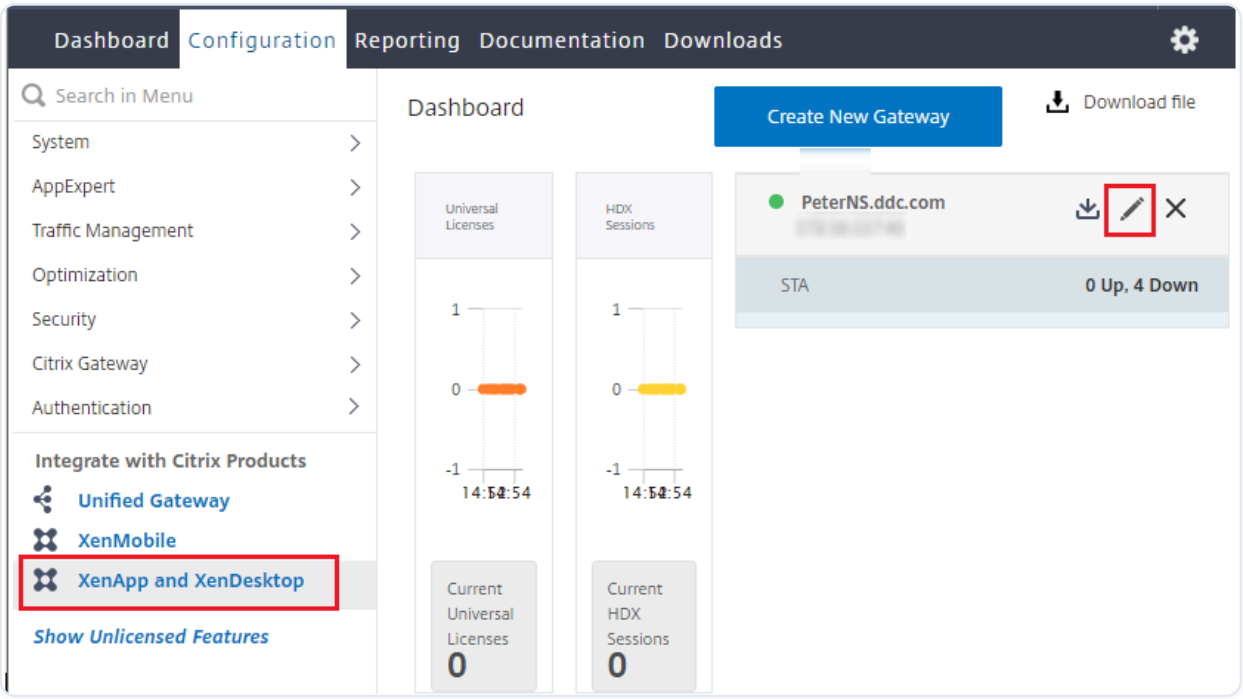
f. 对其他虚拟服务器也重复这些步骤。

### 如果 Citrix ADC 设备已配置 Citrix Virtual Desktops™，则需要进行的配置更改

如果您已将 Citrix ADC 设备配置为使用 Citrix Virtual Desktops，则要使用安全 XML 功能，必须进行以下配置更改。

- 在会话启动之前，更改网关的**安全票证颁发机构 URL**，以使用负载平衡虚拟服务器的 FQDN。
- 确保 `TrustRequestsSentToTheXmlServicePort` 参数设置为 False。默认情况下，`TrustRequestsSentToTheXmlServicePort` 参数设置为 False。但是，如果客户已为 Citrix Virtual Desktops 配置了 Citrix ADC，则 `TrustRequestsSentToTheXmlServicePort` 设置为 True。

1. 在 Citrix ADC GUI 中，导航到 **Configuration > Integrate with Citrix Products**，然后单击 **XenApp and XenDesktop®**。
2. 选择网关实例，然后单击编辑图标。




3. 在 StoreFront 窗格中，单击编辑图标。

   编辑 StoreFront 详细信息(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/edit-storefront-details.png)

4. 添加 **安全票证颁发机构 URL**。

   - 如果启用了安全 XML 功能，则 STA URL 必须是负载平衡服务的 URL。
   - 如果禁用了安全 XML 功能，则 STA URL 必须是 STA 的 URL（DDC 的地址），并且 DDC 上的 TrustRequestsSentToTheXmlServicePort 参数必须设置为 True。

   添加 STA URL(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/add-sta-urls.png)

# 智能卡

智能卡和等效技术在本文所述的指导原则范围内受支持。要在 Citrix Virtual Apps 或 Citrix Virtual Desktops™ 中使用智能卡，请执行以下操作:

- 了解贵组织有关智能卡使用的安全策略。例如，这些策略可能会说明智能卡如何颁发以及用户必须如何保护它们。这些策略的某些方面可能需要在 Citrix Virtual Apps™ 或 Citrix Virtual Desktops 环境中重新评估。
- 确定哪些用户设备类型、操作系统和已发布的应用程序将与智能卡一起使用。

- 熟悉智能卡技术以及您选择的智能卡供应商的硬件和软件。
- 了解如何在分布式环境中部署数字证书。

> **注意：**
>
> 智能卡注册不支持 快速智能卡。当快速智能卡禁用时，智能卡注册可能有效，但这取决于智能卡和中间件的类型。请联系您的智能卡和中间件供应商，了解其与 Citrix Virtual Apps and Desktops 的集成以及对通过虚拟会话进行智能卡注册的支持信息。

## 智能卡类型

企业和消费者智能卡具有相同的尺寸、电气连接器，并适用于相同的智能卡读卡器。

企业用途的智能卡包含数字证书。这些智能卡支持 Windows 登录，也可用于应用程序的数字签名以及文档和电子邮件的加密。Citrix Virtual Apps and Desktops™ 支持这些用途。

消费者用途的智能卡不包含数字证书；它们包含共享密钥。这些智能卡可以支持支付（例如芯片签名或芯片 PIN 信用卡）。它们不支持 Windows 登录或典型的 Windows 应用程序。需要专门的 Windows 应用程序和合适的软件基础设施（例如，连接到支付卡网络）才能使用这些智能卡。请联系您的 Citrix 代表，了解在 Citrix Virtual Apps 或 Citrix Virtual Desktops 上支持这些专用应用程序的信息。

对于企业智能卡，存在可以类似方式使用的兼容等效物。

- 智能卡等效 USB 令牌直接连接到 USB 端口。这些 USB 令牌通常与 USB 闪存驱动器大小相同，但也可以小到手机中使用的 SIM 卡。它们表现为智能卡加上 USB 智能卡读卡器的组合。
- 使用 Windows 可信平台模块 (TPM) 的虚拟智能卡表现为智能卡。这些虚拟智能卡支持 Windows 8 和 Windows 10，使用 Citrix Workspace 应用程序（最低版本 Citrix Receiver 4.3）。
    - 早于 XenApp and XenDesktop 7.6 FP3 的 Citrix Virtual Apps and Desktops 版本（以前称为 XenApp and XenDesktop）不支持虚拟智能卡。
    - 有关虚拟智能卡的更多信息，请参阅 虚拟智能卡概述。

    **注意：** 术语“虚拟智能卡”也用于描述存储在用户计算机上的数字证书。这些数字证书与智能卡并非严格等同。

Citrix Virtual Apps and Desktops 智能卡支持基于 Microsoft 个人计算机/智能卡 (PC/SC) 标准规范。最低要求是智能卡和智能卡设备必须受底层 Windows 操作系统支持，并且必须获得 Microsoft

Windows 硬件质量实验室 (WHQL) 的批准，才能在运行合格 Windows 操作系统的计算机上使用。有关硬件 PC/SC 合规性的更多信息，请参阅 Microsoft 文档。其他类型的用户设备可能符合 PS/SC 标准。有关详细信息，请参阅 Citrix Ready 计划。

通常，每个供应商的智能卡或等效设备都需要单独的设备驱动程序。但是，如果智能卡符合 NIST 个人身份验证 (PIV) 标准等标准，则可能可以使用单个设备驱动程序来支持一系列智能卡。设备驱动程序必须安装在用户设备和虚拟投递代理 (VDA) 上。设备驱动程序通常作为 Citrix 合作伙伴提供的智能卡中间件软件包的一部分提供；智能卡中间件软件包提供高级功能。设备驱动程序也可以描述为加密服务提供程序 (CSP)、密钥存储提供程序 (KSP) 或微型驱动程序。

Citrix 已测试以下适用于 Windows 系统的智能卡和中间件组合，作为其类型的代表性示例。但是，也可以使用其他智能卡和中间件。有关 Citrix 兼容智能卡和中间件的更多信息，请参阅 `<http://www.citrix.com/ready>`。

| 中间件 | 匹配的卡 |
| --- | --- |
| Gemalto .NET 卡微型驱动程序 | Gemalto .NET v2及以上 |

有关智能卡与其他类型设备一起使用的信息，请参阅该设备的 Citrix Workspace™ 应用程序文档。

## 远程电脑访问

智能卡仅支持远程访问运行 Windows 10、Windows 8 或 Windows 7 的物理办公电脑。

以下智能卡已通过远程电脑访问进行测试：

| 中间件 | 匹配的卡 |
| --- | --- |
| Gemalto .NET 微型驱动程序 | Gemalto .NET v2及以上 |

## 快速智能卡

快速智能卡是对现有基于 HDX PC/SC 的智能卡重定向的改进。它在智能卡用于高延迟 WAN 环境时提高了性能。当延迟较高时，性能改进可能非常显著（例如，Windows 快速智能卡登录需要 15 秒，而基于 PC/SC 的智能卡重定向则需要 1 分钟以上）。

快速智能卡在运行当前支持的 Windows VDA 的主机上默认启用。要在主机端禁用快速智能卡（例如，出于诊断目的），请将“Disable Cryptographic Redirection”注册表设置设置为任何非零值：

```
HKLM\SOFTWARE\Citrix\SmartCard

CryptographicRedirectionDisable (DWORD)
```

在客户端，要启用快速智能卡，请在关联的 StoreFront 站点的 *default.ica* 文件中包含 SmartCardCryptographicRedirection ICA 参数：

```
[WFClient]

SmartCardCryptographicRedirection=On
```

此外，在客户端，可以使用以下注册表设置强制启用或强制禁用快速智能卡（例如，出于诊断目的）：

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (作为非零 DWORD)

或者

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (作为非零 DWORD)

如果客户端计算机是 64 位，则必须指定 32 位注册表配置单元（使用 `WOW6432Node`）。

限制：

- 只有适用于 Windows 的 Citrix Workspace 应用程序支持快速智能卡。如果在 default.ica 文件中配置了快速智能卡，非 Windows 版本的 Citrix Workspace 应用程序仍将使用现有的 PC/SC 重定向。
- 快速智能卡唯一支持的双跳方案是在两个跳上都启用了快速智能卡的 ICA® > ICA。由于快速智能卡不支持 ICA > RDP 双跳方案，因此这些方案不起作用。
- 快速智能卡不支持下一代加密技术 (Cryptography Next Generation)。因此，快速智能卡不支持椭圆曲线加密 (ECC) 智能卡。
- 快速智能卡仅支持只读密钥容器操作。
- 快速智能卡不支持更改智能卡 PIN。

从 VDA 2203 版和适用于 Windows 的 Citrix Workspace 应用程序 2202 版（或更高版本）开始，快速智能卡与下一代加密技术 (CNG) 兼容。此外，椭圆曲线加密 (ECC) 智能卡支持以下曲线：P-256、P-384、P-521 位，适用于 ECDSA 和 ECDH。

从 VDA 2203 版开始，快速智能卡增加了在同一用户登录会话中的应用程序之间缓存智能卡 PIN 的功能。例如，如果启用了 **会话 PIN 缓存** 并且最终用户之前已将智能卡 PIN 提供给 Outlook，当 Word 用于签署文档时，Word 会使用已缓存的智能卡 PIN（已提交给 Outlook）。**会话 PIN 缓存** 通过减少用户输入智能卡 PIN 的次数来改善用户体验。此外，如果智能卡用于登录 VDA，Windows 智能卡登录 PIN 可以选择保存到 **会话 PIN 缓存** 中。这可以进一步改善用户体验。

**会话 PIN 缓存** 默认禁用。可以在 VDA 上使用以下注册表设置启用和控制它：

在 HKLM\SOFTWARE\Citrix\SmartCard 中:

- `EnablePinSessionCache` 作为 DWORD (非零表示启用)
- `EnableLogonPinSessionCache` 作为 DWORD (非零表示启用)
- `PinSessionCacheEntryStaleTimeout` 作为 DWORD (条目失效前的秒数，默认为 1 小时)

## 智能卡读卡器类型

智能卡读卡器可能内置于用户设备中，也可能单独连接到用户设备（通常通过 USB 或蓝牙）。支持符合 USB 芯片/智能卡接口设备 (CCID) 规范的接触式读卡器。它们包含一个插槽或刷卡口，用户可将智能卡插入其中。德国信贷经济 (DK) 标准定义了四类接触式读卡器。

- 1 类智能卡读卡器最常见，通常包含一个插槽。支持 1 类智能卡读卡器，通常随操作系统提供标准 CCID 设备驱动程序。
- 2 类智能卡读卡器还包含一个安全键盘，用户设备无法访问该键盘。2 类智能卡读卡器可能内置于带有集成安全键盘的键盘中。对于 2 类智能卡读卡器，请联系您的 Citrix 代表；可能需要读卡器特定的设备驱动程序才能启用安全键盘功能。
- 3 类智能卡读卡器还包含一个安全显示屏。不支持 3 类智能卡读卡器。
- 4 类智能卡读卡器还包含一个安全事务模块。不支持 4 类智能卡读卡器。

> **注意：**

> 智能卡读卡器类别与 USB 设备类别无关。

> 智能卡读卡器必须在用户设备上安装相应的设备驱动程序。

有关支持的智能卡读卡器的信息，请参阅您正在使用的 Citrix Workspace 应用程序的文档。在 Citrix Workspace 应用程序文档中，支持的版本列在智能卡文章或系统要求文章中。

## 用户体验

智能卡支持已集成到 Citrix Virtual Apps and Desktops 中，使用默认启用的特定 ICA/HDX 智能卡虚拟通道。

重要提示：请勿将通用 USB 重定向用于智能卡读卡器。智能卡读卡器默认禁用此功能，如果启用则不受支持。

可以在同一用户设备上使用多张智能卡和多个读卡器，但如果使用直通身份验证，则用户启动虚拟桌面或应用程序时只能插入一张智能卡。当智能卡在应用程序中使用时（例如，用于数字签名或加密功能），可能会出现其他提示，要求插入智能卡或输入 PIN 码。如果同时插入了多张智能卡，则可能会发生这种情况。

- 如果智能卡已在读卡器中，但系统仍提示用户插入智能卡，则用户必须选择“取消”。
- 如果系统提示用户输入 PIN 码，则用户必须再次输入 PIN 码。

您可以使用卡管理系统或供应商实用程序重置 PIN 码。

> **重要提示：**

> 在 Citrix Virtual Apps 或 Citrix Virtual Desktops 会话中，不支持将智能卡与 Microsoft 远程桌面连接应用程序配合使用。这有时被称为“双跳”使用。

## 部署智能卡之前

- 获取智能卡读卡器的设备驱动程序并将其安装在用户设备上。许多智能卡读卡器可以使用 Microsoft 提供的 CCID 设备驱动程序。
- 从智能卡供应商处获取设备驱动程序和加密服务提供程序 (CSP) 软件，并将其安装在用户设备和虚拟桌面上。驱动程序和 CSP 软件必须与 Citrix Virtual Apps and Desktops 兼容；请查阅供应商文档以了解兼容性。对于使用支持并使用微型驱动程序模型的智能卡的虚拟桌面，智能卡微型驱动程序会自动下载，但您也可以从 http://catalog.update.microsoft.com 或从您的供应商处获取它们。此外，如果需要 PKCS#11 中间件，请从卡供应商处获取。
- 重要提示：Citrix 建议您在安装 Citrix 软件之前，先在物理计算机上安装并测试驱动程序和 CSP 软件。
- 对于在 Windows 10 中使用 Internet Explorer 的智能卡用户，将 Citrix Receiver™ for Web URL 添加到“受信任站点”列表。在 Windows 10 中，Internet Explorer 默认情况下不会为受信任站点在保护模式下运行。

- 确保您的公钥基础结构 (PKI) 配置正确。这包括确保为 Active Directory 环境正确配置了证书到帐户的映射，并且可以成功执行用户证书验证。
- 确保您的部署符合与智能卡一起使用的其他 Citrix 组件（包括 Citrix Workspace 应用程序和 StoreFront）的系统要求。
- 确保可以访问站点中的以下服务器：
  - 与智能卡上的登录证书关联的用户帐户的 Active Directory 域控制器
  - 交付控制器™
  - 思杰 StoreFront
  - Citrix 网关/Citrix 访问网关 10.x
  - VDA
  - (远程电脑访问可选)：Microsoft Exchange Server

## 启用智能卡使用

**步骤 1.** 根据您的卡片颁发策略向用户颁发智能卡。

**步骤 2.** (可选) 设置智能卡以启用用户进行远程电脑访问。

**步骤 3.** 安装并配置 Delivery Controller 和 StoreFront（如果尚未安装），以用于智能卡远程处理。

**步骤 4.** 启用 StoreFront 以使用智能卡。有关详细信息，请参阅 StoreFront 文档中的“配置智能卡身份验证”。

**步骤 5.** 启用 Citrix Gateway/Access Gateway 以使用智能卡。有关详细信息，请参阅 NetScaler 文档中的“配置身份验证和授权”以及“通过 Web 界面配置智能卡访问”。

**步骤 6.** 启用 VDA 以使用智能卡。

- 确保 VDA 具有所需的应用程序和更新。
- 安装中间件。
- 设置智能卡远程处理，以实现在用户设备上的 Citrix Workspace 应用程序与虚拟桌面会话之间智能卡数据的通信。

**步骤 7.** 启用用户设备（包括已加入域或未加入域的计算机）以使用智能卡。有关详细信息，请参阅 StoreFront 文档中的“配置智能卡身份验证”。

- 将证书颁发机构根证书和颁发证书颁发机构证书导入设备的密钥库。
- 安装供应商的智能卡中间件。

- 安装并配置适用于 Windows 的 Citrix Workspace 应用程序，务必使用组策略管理控制台导入 icaclient.adm 并启用智能卡身份验证。

**步骤 8.** 测试部署。通过使用测试用户的智能卡启动虚拟桌面，确保部署已正确配置。测试所有可能的访问机制（例如，通过 Internet Explorer 和 Citrix Workspace 应用程序访问桌面）。

## 跟踪智能卡读卡器插入计数

通过智能卡远程处理，您可以使用 SCardGetStatusChange 函数跟踪智能卡插入或从读卡器中移除的次数。该函数会更新一个 SCARD_READERSTATE 数据结构数组，每个您监控的读卡器对应一个。每个 SCARD_READERSTATE 的 dwEventState 字段的高字（16 位）包含读卡器计数。有关详细信息，请参阅 Microsoft 文章 SCardGetStatusChangeA function 和 SCARD_READERSTATEA structure。

“**读卡器插入计数报告**”设置默认处于禁用状态。要启用跟踪，请添加以下注册表项：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

名称: EnableReaderInsertCountReporting

类型: DWORD

值: 任何非零值

会话断开连接时，计数将重置为零。

“**读卡器插入计数报告**”与第三方智能卡中间件兼容。

## 智能卡部署

此产品版本以及包含此版本的混合环境支持以下类型的智能卡部署。其他配置可能有效，但不受支持。

| 类型 | STOREFRONT™ 连接 |
| --- | --- |
| 本地已加入域的计算机 | 直接连接 |
| 从已加入域的计算机进行远程访问 | 通过 Citrix Gateway 连接 |
| 未加入域的计算机 | 直接连接 |
| 从未加入域的计算机进行远程访问 | 通过 Citrix Gateway 连接 |

| 类型 | STOREFRONT™ 连接 |
| --- | --- |
| 访问 Desktop Appliance 站点的未加入域的计算机和瘦客户端 | 通过 Desktop Appliance 站点连接 |
| 通过 XenApp® Services URL 访问 StoreFront 的已加入域的计算机和瘦客户端 | 通过 XenApp Services URL 连接 |

部署类型由智能卡读卡器所连接的用户设备的特性决定：

- 设备是已加入域还是未加入域。
- 设备如何连接到 StoreFront。
- 用于查看虚拟桌面和应用程序的软件是什么。

此外，这些部署中可以使用支持智能卡的应用程序，例如 Microsoft Word 和 Microsoft Excel。这些应用程序允许用户对文档进行数字签名或加密。

### 双模式身份验证

在这些部署中，Receiver 尽可能通过向用户提供使用智能卡或输入其用户名和密码的选择来支持双模式身份验证。如果智能卡无法使用（例如，用户将其遗忘在家中或登录证书已过期），此功能会很有用。

由于未加入域的设备用户直接登录到 Receiver for Windows，因此您可以让用户回退到显式身份验证。如果配置双模式身份验证，用户最初会收到使用智能卡和 PIN 登录的提示，但如果他们的智能卡出现任何问题，他们可以选择显式身份验证。

如果部署 Citrix Gateway，用户将登录其设备，并且 Receiver for Windows 会提示他们向 Citrix Gateway 进行身份验证。这适用于已加入域和未加入域的设备。用户可以使用其智能卡和 PIN 或显式凭据登录到 Citrix Gateway。这使您能够为 Citrix Gateway 登录提供双模式身份验证。配置从 Citrix Gateway 到 StoreFront 的直通身份验证，并将凭据验证委托给 Citrix Gateway 以供智能卡用户使用，以便用户可以静默地向 StoreFront 进行身份验证。

### 多个 Active Directory 林注意事项

在 Citrix 环境中，智能卡在单个林中受支持。跨林的智能卡登录需要与所有用户帐户建立直接的双向林信任。不支持涉及智能卡的更复杂的多林部署（即，信任仅为单向或不同类型的部署）。

您可以在包含远程桌面的 Citrix 环境中使用智能卡。此功能可以本地安装（在智能卡连接到的用户设备上）或远程安装（在用户设备连接到的远程桌面上）。

### 智能卡移除策略

产品上设置的智能卡移除策略决定了在会话期间从读卡器中移除智能卡时会发生什么。智能卡移除策略通过 Windows 操作系统进行配置和处理。

| 策略设置 | 桌面行为 |
| --- | --- |
| 无操作 | 无操作。 |
| 锁定工作站 | 桌面会话已断开连接，虚拟桌面已锁定。 |
| 强制注销 | 用户被强制注销。如果网络连接丢失且此设置已启用，会话可能会被注销，用户可能会丢失数据。 |
| 如果是远程终端服务会话，则断开连接 | 会话已断开连接，虚拟桌面已锁定。 |

### 证书吊销检查

如果启用了证书吊销检查，并且用户将带有无效证书的智能卡插入读卡器，则用户无法进行身份验证或访问与该证书相关的桌面或应用程序。例如，如果无效证书用于电子邮件解密，则电子邮件仍将保持加密状态。如果卡上的其他证书（例如用于身份验证的证书）仍然有效，则这些功能将保持活动状态。

### 部署示例：已加入域的计算机

此部署涉及运行 Desktop Viewer 并直接连接到 StoreFront 的已加入域的用户设备。

部署示例：已加入域的计算机(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/smartcard1_1.png)

用户使用智能卡和 PIN 登录设备。Receiver 使用集成 Windows 身份验证 (IWA) 对用户向 StoreFront 服务器进行身份验证。StoreFront 将用户安全标识符 (SID) 传递给 Citrix Virtual Apps 或 Citrix Virtual Desktops。当用户启动虚拟桌面或应用程序时，由于 Receiver 上配置了单点登录功能，因此不会再次提示用户输入 PIN。

通过添加第二个 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展为双跳。虚拟桌面中的 Receiver 向第二个 StoreFront 服务器进行身份验证。此第二个连接可以使用任何身份验证方法。第一个跳中显示的配置可以在第二个跳中重复使用，或者仅在第二个跳中使用。

### 部署示例：从已加入域的计算机进行远程访问

此部署涉及运行 Desktop Viewer 并通过 Citrix Gateway/Access Gateway 连接到 StoreFront 的已加入域的用户设备。

部署示例：从已加入域的计算机进行远程访问(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/smartcard2_1.png)

用户使用智能卡和 PIN 登录到设备，然后再次登录到 Citrix Gateway/Access Gateway。第二次登录可以使用智能卡和 PIN，也可以使用用户名和密码，因为在此部署中 Receiver 允许双模式身份验证。

用户自动登录到 StoreFront，StoreFront 将用户安全标识符 (SID) 传递给 Citrix Virtual Apps™ 或 Citrix Virtual Desktops。当用户启动虚拟桌面或应用程序时，不会再次提示用户输入 PIN，因为 Receiver 上已配置单点登录功能。

此部署可以通过添加第二个 StoreFront 服务器和托管应用程序的服务器来扩展为双跳。虚拟桌面中的 Receiver 向第二个 StoreFront 服务器进行身份验证。此第二个连接可以使用任何身份验证方法。为第一跳显示的配置可以在第二跳中重复使用，或者仅在第二跳中使用。

### 部署示例：未加入域的计算机

此部署涉及运行 Desktop Viewer 并直接连接到 StoreFront 的未加入域的用户设备。

部署示例：未加入域的计算机(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/smartcard3_1.png)

用户登录到设备。通常，用户输入用户名和密码，但由于设备未加入域，因此此登录的凭据是可选的。由于在此部署中可以进行双模式身份验证，因此 Receiver 会提示用户输入智能卡和 PIN 或用户名和密码。然后 Receiver 向 StoreFront 进行身份验证。

StoreFront 将用户安全标识符 (SID) 传递给 Citrix Virtual Apps 或 Citrix Virtual Desktops。当用户启动虚拟桌面或应用程序时，会再次提示用户输入 PIN，因为此部署中不提供单点登录功能。

此部署可以通过添加第二个 StoreFront 服务器和托管应用程序的服务器来扩展为双跳。虚拟桌面中的 Receiver 向第二个 StoreFront 服务器进行身份验证。此第二个连接可以使用任何身份验证方法。为第一跳显示的配置可以在第二跳中重复使用，或者仅在第二跳中使用。

### 部署示例：从未加入域的计算机进行远程访问

此部署涉及运行 Desktop Viewer 并直接连接到 StoreFront 的未加入域的用户设备。

部署示例：从未加入域的计算机进行远程访问(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/smartcard4_1.png)

用户登录到设备。通常，用户输入用户名和密码，但由于设备未加入域，因此此登录的凭据是可选的。由于在此部署中可以进行双模式身份验证，因此 Receiver 会提示用户输入智能卡和 PIN 或用户名和密码。然后 Receiver 向 StoreFront 进行身份验证。

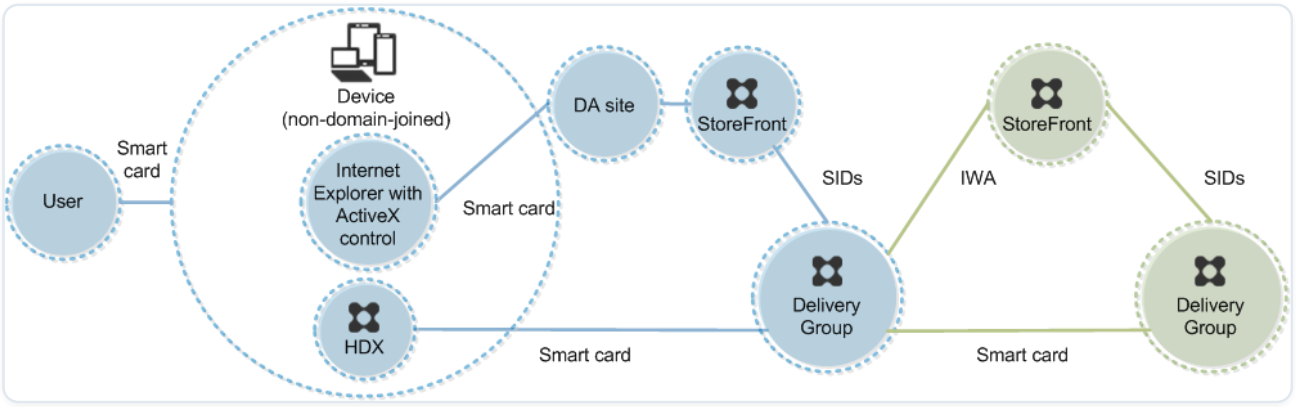
StoreFront 将用户安全标识符 (SID) 传递给 Citrix Virtual Apps 或 Citrix Virtual Desktops。当用户启动虚拟桌面或应用程序时，由于此部署中不提供单点登录功能，用户将再次被要求输入 PIN。

通过添加第二个 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展为双跳。虚拟桌面中的 Receiver 向第二个 StoreFront 服务器进行身份验证。此第二个连接可以使用任何身份验证方法。第一个跳中显示的配置可以在第二个跳中重复使用，或者仅在第二个跳中使用。

### 部署示例：非域加入计算机和瘦客户端访问桌面设备站点

此部署涉及非域加入的用户设备，这些设备可能运行 Desktop Lock 并通过桌面设备站点连接到 StoreFront。

Desktop Lock 是一个单独的组件，随 Citrix Virtual Apps、Citrix Virtual Desktops 和 VDI-in-a-Box 一起发布。它是 Desktop Viewer 的替代方案，主要为重新利用的 Windows 计算机和 Windows 瘦客户端设计。Desktop Lock 会替换这些用户设备中的 Windows shell 和任务管理器，从而阻止用户访问底层设备。使用 Desktop Lock，用户可以访问 Windows Server Machine 桌面和 Windows Desktop Machine 桌面。Desktop Lock 的安装是可选的。



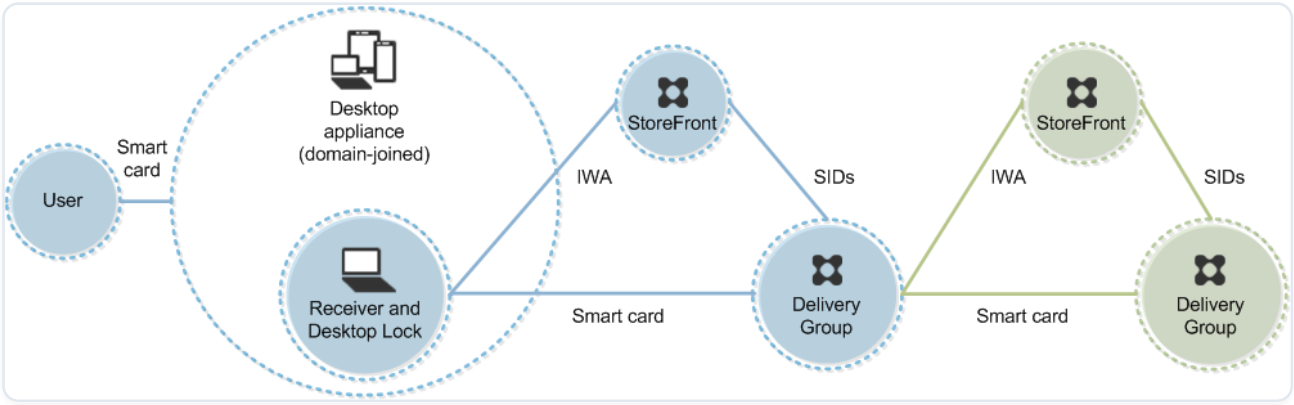

用户使用智能卡登录设备。如果设备上运行 Desktop Lock，则设备配置为通过在 Kiosk 模式下运行的 Internet Explorer 启动桌面设备站点。站点上的 ActiveX 控件会提示用户输入 PIN，并将其发送到 StoreFront。StoreFront 将用户安全标识符 (SID) 传递给 Citrix Virtual Apps 或 Citrix Virtual Desktops。分配的桌面组中按字母顺序排列的第一个可用桌面将启动。

通过添加第二个 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展为双跳。虚拟桌面中的 Receiver 向第二个 StoreFront 服务器进行身份验证。此第二个连接可以使用任何身份验证方法。第一个跳中显示的配置可以在第二个跳中重复使用，或者仅在第二个跳中使用。

### 部署示例：域加入计算机和瘦客户端通过 XenApp Services URL 访问 StoreFront

此部署涉及运行 Desktop Lock 并通过 XenApp Services URL 连接到 StoreFront 的域加入用户设备。

Desktop Lock 是一个单独的组件，随 Citrix Virtual Apps、Citrix Virtual Desktops 和 VDI-in-a-Box 一起发布。它是 Desktop Viewer 的替代方案，主要为重新利用的 Windows 计算机和 Windows 瘦客户端设计。Desktop Lock 会替换这些用户设备中的 Windows shell 和任务管理器，从而阻止用户访问底层设备。使用 Desktop Lock，用户可以访问 Windows Server Machine 桌面和 Windows Desktop Machine 桌面。Desktop Lock 的安装是可选的。




用户使用智能卡和 PIN 登录设备。如果设备上运行 Desktop Lock，它会使用集成 Windows 身份验证 (IWA) 对用户向 StoreFront 服务器进行身份验证。StoreFront 将用户安全标识符 (SID) 传递给 Citrix Virtual Apps 或 Citrix Virtual Desktops。当用户启动虚拟桌面时，由于 Receiver 上配置了单点登录功能，用户不会再次被要求输入 PIN。

通过添加第二个 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展为双跳。虚拟桌面中的 Receiver 向第二个 StoreFront 服务器进行身份验证。此第二个连接可以使用任何身份验证方法。第一个跳中显示的配置可以在第二个跳中重复使用，或者仅在第二个跳中使用。

## 智能卡直通身份验证和单点登录

### 直通身份验证

智能卡直通身份验证到虚拟桌面在运行 Windows 10、Windows 8 和 Windows 7 SP1 企业版和专业版的用户设备上受支持。

使用智能卡对托管应用程序进行直通身份验证，在运行 Windows Server 2016、Windows Server 2012 R2、Windows Server 2012 和 Windows Server 2008 R2 SP1 的服务器上受支持。

要将智能卡直通身份验证用于托管应用程序，请确保在将智能卡直通配置为站点的身份验证方法时启用 Kerberos。

注意：智能卡直通身份验证的可用性取决于许多因素，包括但不限于：

- 您的组织关于直通身份验证的安全策略。
- 中间件类型和配置。
- 智能卡读卡器类型。

- 中间件 PIN 缓存策略。

智能卡直通身份验证在 Citrix StoreFront 上配置。有关详细信息，请参阅 StoreFront 文档。

### 单点登录

单点登录是 Citrix 的一项功能，它通过虚拟桌面和应用程序启动实现直通身份验证。您可以在已加入域、直接连接到 StoreFront 以及已加入域、NetScaler 连接到 StoreFront 的智能卡部署中使用此功能，以减少用户输入 PIN 的次数。要在这些部署类型中使用单点登录，请编辑 StoreFront 服务器上 default.ica 文件中的以下参数：

- 已加入域、直接连接到 StoreFront 的智能卡部署 — 将 DisableCtrlAltDel 设置为 Off
- 已加入域、NetScaler 连接到 StoreFront 的智能卡部署 — 将 UseLocalUserAndPassword 设置为 On

有关设置这些参数的更多说明，请参阅 StoreFront 或 Citrix Gateway 文档。

单点登录功能的可用性取决于多种因素，包括但不限于：

- 您组织关于单点登录的安全策略。
- 中间件类型和配置。
- 智能卡读卡器类型。
- 中间件 PIN 缓存策略。

> **注意：**
>
> 当用户在连接了智能卡读卡器的计算机上登录到 Virtual Delivery Agent (VDA) 时，可能会出现一个 Windows 磁贴，表示之前成功的身份验证模式，例如智能卡或密码。因此，当启用单点登录时，可能会出现单点登录磁贴。要登录，用户必须选择 **切换用户** 以选择另一个磁贴，因为单点登录磁贴将不起作用。

# FIDO2 和 WebAuthn 身份验证

## 使用 FIDO2 和 WebAuthn 进行本地授权和虚拟身份验证

用户可以使用 FIDO2 安全密钥以及集成 TPM 2.0 和 Windows Hello 的生物识别设备，在其虚拟会话中对利用 FIDO2 或 WebAuthn 的应用程序进行身份验证。

有关 FIDO2 的更多信息，请参阅 FIDO2: WebAuthn & CTAP。

有关使用此功能的信息，请参阅 FIDO2 重定向。

**注意**

请注意，此功能不支持使用 WebAuthn 或 FIDO2 登录虚拟会话。此功能仅允许在虚拟会话中的应用程序中使用这些身份验证方法。

双跳场景不支持此功能。

## 支持矩阵

| 会话主机操作系统 | WEB 应用程序身份验证 | UWP 应用程序身份验证 |
| --- | --- | --- |
| Windows 服务器 2016 | 通过 USB 重定向支持 | 不支持 |
| Windows 服务器 2019 | 受支持 | 不支持 |
| Windows 服务器 2022 | 受支持 | 受支持 |
| Windows 10 系统 | 受支持 | 受支持 |
| Windows 十一 | 受支持 | 受支持 |

有关其他信息，请查看以下要求。

## Web 应用程序身份验证

### 要求

以下是使用 FIDO2 和 WebAuthn 对 Web 应用程序进行身份验证的要求：

#### Citrix® 控制平面

- Citrix Virtual Apps and Desktops™ 2009 或更高版本

#### 会话主机

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows Server 2019 或更高版本

- VDA
  - Windows: 2009 版或更高版本

**客户端设备**

- 操作系统
  - Windows 10 1809 或更高版本
  - Linux: 请参阅适用于 Linux 的 Workspace 应用程序的系统要求
- Workspace 应用程序
  - Windows: 2009.1 版或更高版本
  - Linux: 2303 或更高版本

**Web 浏览器要求**

- 仅限 64 位浏览器

**支持的身份验证方法**

- FIDO2 安全密钥
- Windows 你好
  - TPM 2.0
  - 集成生物识别
    - 面部识别
    - 指纹扫描仪
  - WebAuthn

## UWP 应用程序身份验证

随着 Citrix Virtual Apps and Desktops 2112 的发布，Citrix 支持 UWP 应用程序中的 WebAuthn 和 FIDO2 身份验证。

Microsoft Teams、Microsoft Outlook for Office 365 和 OneDrive 等应用程序使用 UWP 应用程序进行身份验证，作为与 Azure Active Directory 的链接。Citrix 现在支持使用 FIDO2 对这些应用程序进行身份验证。

## 要求

以下是使用 FIDO2 和 WebAuthn 身份验证与 UWP 应用程序的要求：

### Citrix 控制平面

- Citrix Virtual Apps and Desktops 2112 或更高版本

### 会话主机

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows Server 2022 或更高版本
- VDA
  - Windows：版本 2112 或更高版本

### 客户端设备

- 操作系统
  - Windows 10 1809 或更高版本
  - Linux：请参阅适用于 Linux 的 Workspace 应用程序的系统要求
- Workspace 应用程序
  - Windows：版本 2009.1 或更高版本
  - Linux：2303 或更高版本

### 支持的身份验证方法

- FIDO2 安全密钥
- Windows 你好
  - TPM 2.0
  - 集成生物识别
    - 面部识别
    - 指纹扫描仪
  - WebAuthn

# 传输层安全性 (TLS)

Citrix Virtual Apps and Desktops 支持传输层安全性 (TLS) 协议，用于组件之间基于 TCP 的连接。Citrix Virtual Apps and Desktops 还支持数据报传输层安全性 (DTLS) 协议，用于基于 UDP 的 ICA/HDX 连接，使用 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/technical-overview/hdx/adaptive-transport.html)。

TLS 和 DTLS 相似，并且支持相同的数字证书。将 Citrix Virtual Apps 或 Citrix Virtual Desktops™ 站点配置为使用 TLS 也会将其配置为使用 DTLS。请使用以下过程；除非另有说明，否则这些步骤对 TLS 和 DTLS 均适用：

- 在所有 Delivery Controller 上获取、安装和注册服务器证书，并使用 TLS 证书配置端口。有关详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/secure/tls.html#install-tls-server-certificates-on-controllers)。

  您可以选择更改 Controller 用于侦听 HTTP 和 HTTPS 流量的端口。

- 通过完成以下任务，在 Citrix Workspace™ 应用程序和 Virtual Delivery Agent (VDA) 之间启用 TLS 连接：

  - 在安装 VDA 的计算机上配置 TLS。（为方便起见，以后将安装 VDA 的计算机简称为“VDA”。）有关常规信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/secure/tls.html#tls-settings-on-vdas)。强烈建议您使用 Citrix 提供的 PowerShell 脚本来配置 TLS/DTLS。有关详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/secure/tls.html#configure-tls-on-a-vda-using-the-powershell-script)。但是，如果您想手动配置 TLS/DTLS，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/secure/tls.html#manually-configure-tls-on-a-vda)。
  - 通过在 Studio 中运行一组 PowerShell cmdlet，在包含 VDA 的交付组中配置 TLS。有关详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/secure/tls.html#configure-tls-on-delivery-groups)。

    要求和注意事项：

    - 在用户和 VDA 之间启用 TLS 连接仅适用于 XenApp 7.6 和 XenDesktop 7.6 站点以及更高版本支持的发行版。
    - 在安装组件、创建站点、创建计算机目录和创建交付组之后，在交付组和 VDA 上配置 TLS。
    - 要在交付组中配置 TLS，您必须具有更改 Controller 访问规则的权限。完全管理员拥有此权限。
    - 要在 VDA 上配置 TLS，您必须是安装 VDA 的计算机上的 Windows 管理员。

- 在由 Machine Creation Services™ 或 Provisioning Services 预配的池化 VDA 上，VDA 计算机映像会在重新启动时重置，导致以前的 TLS 设置丢失。每次 VDA 重新启动时运行 PowerShell 脚本以重新配置 TLS 设置。

**警告：**

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

有关为站点数据库启用 TLS 的信息，请参阅 CTX137556。

## 在控制器上安装 TLS 服务器证书

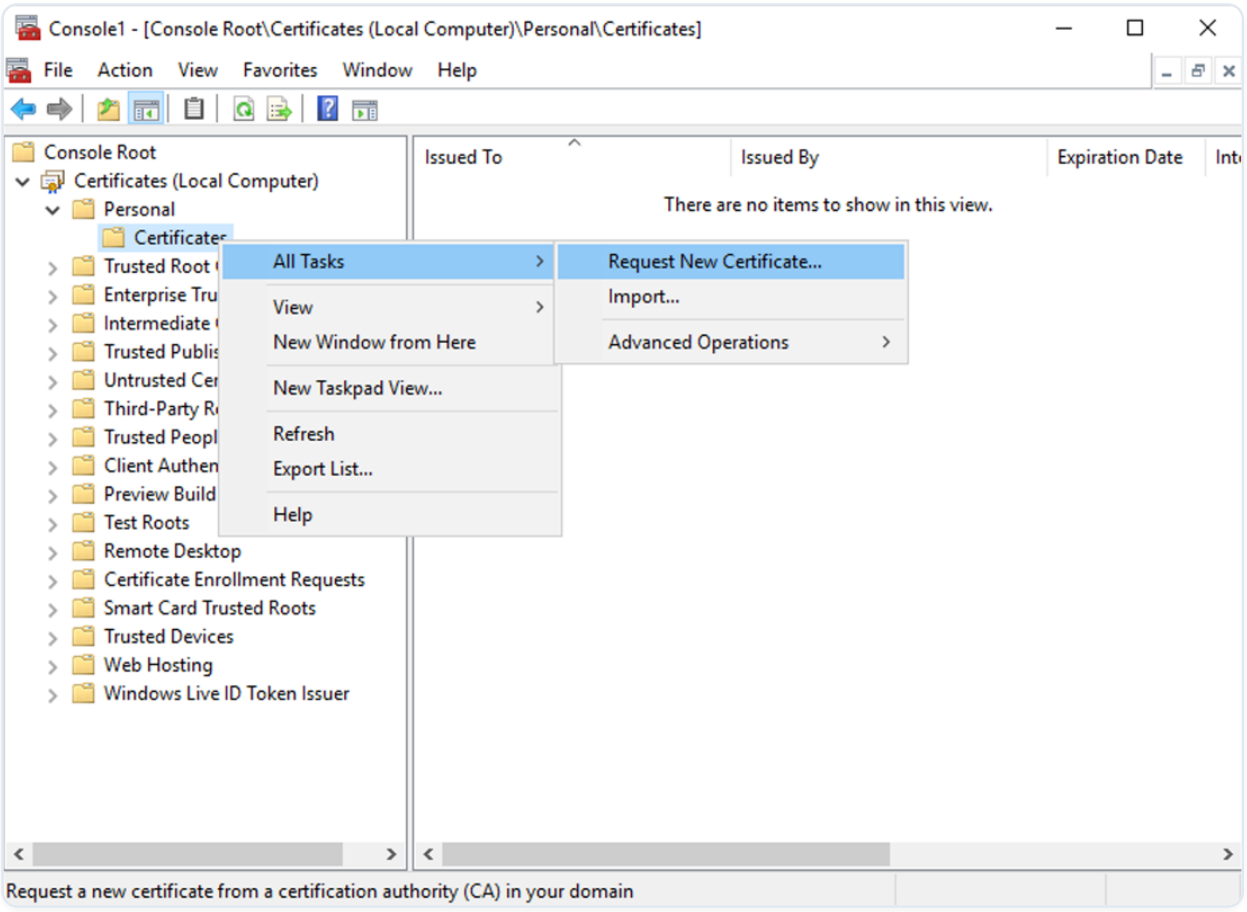
对于 HTTPS，XML Service 通过使用服务器证书（而非客户端证书）支持 TLS 功能。本部分介绍如何在 Delivery Controller 中获取和安装 TLS 证书。相同的步骤可应用于 Cloud Connector 以加密 STA 和 XML 流量。

尽管有各种不同类型的证书颁发机构以及从它们请求证书的方法，但本文介绍的是 Microsoft 证书颁发机构。Microsoft 证书颁发机构需要发布一个证书模板，其用途为服务器身份验证。

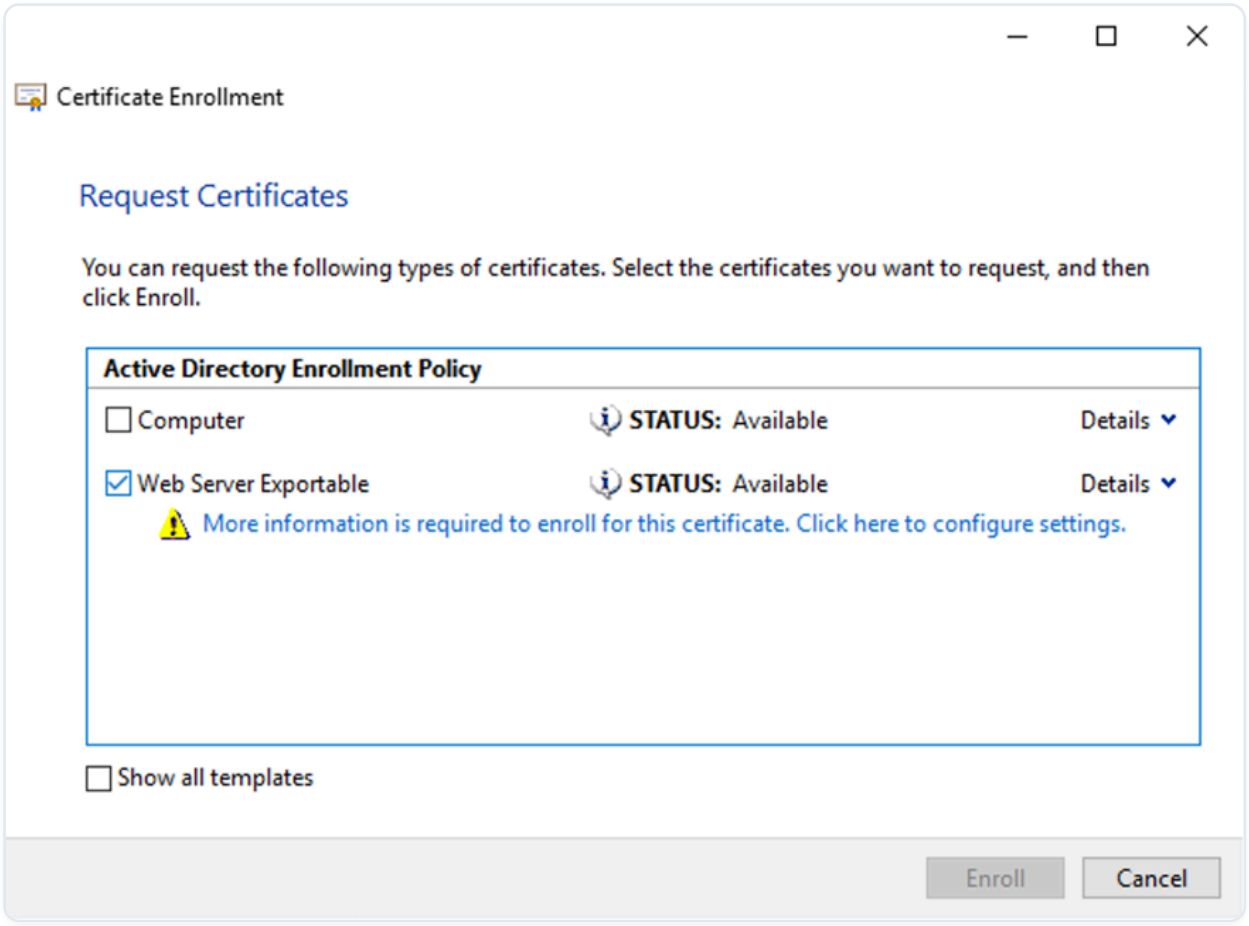
如果 Microsoft 证书颁发机构集成到 Active Directory 域或 Delivery Controller 所加入的受信任林中，则可以从“证书”MMC 管理单元的“证书注册向导”获取证书。

### 请求和安装证书

1. 在 Delivery Controller™ 上，打开 MMC 控制台并添加“证书”管理单元。出现提示时，选择“计算机帐户”。
2. 展开“**个人 > 证书**”，然后使用“**所有任务 > 请求新证书**”上下文菜单命令。



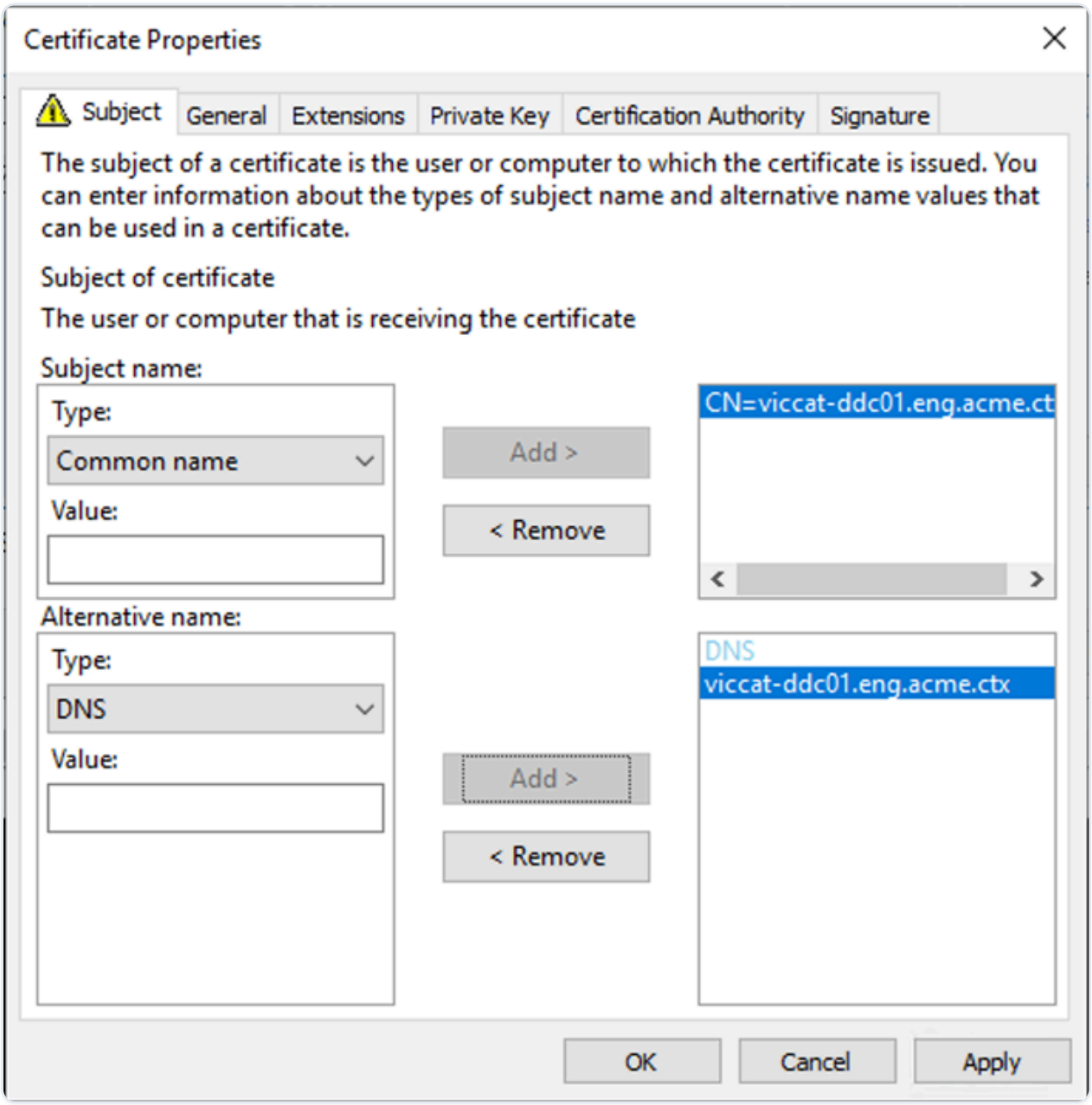

3. 单击“**下一步**”开始，然后单击“**下一步**”确认您正在从 Active Directory 注册获取证书。
4. 选择服务器身份验证证书的模板。如果模板已设置为自动提供主题的值，则无需提供更多详细信息即可单击“**注册**”。




5. 要为证书模板提供更多详细信息，请单击“**详细信息**”箭头按钮并配置以下内容：

   **主题名称**：选择“公用名”并添加 Delivery Controller 的 FQDN。

   **备用名称**：选择“DNS”并添加 Delivery Controller 的 FQDN。




### 配置 SSL/TLS 侦听器端口

如果 IIS Windows 组件安装在同一服务器上（作为 Web Studio 和 Director 的一部分安装），则可以使用 IIS 配置 TLS。有关详细信息，请参阅在 Web Studio 和 Director 上启用 TLS。否则，要使用 PowerShell 配置证书，请执行以下操作：

1. 要检查是否存在已绑定的证书，请打开命令提示符并运行 `netsh http show sslcert`：

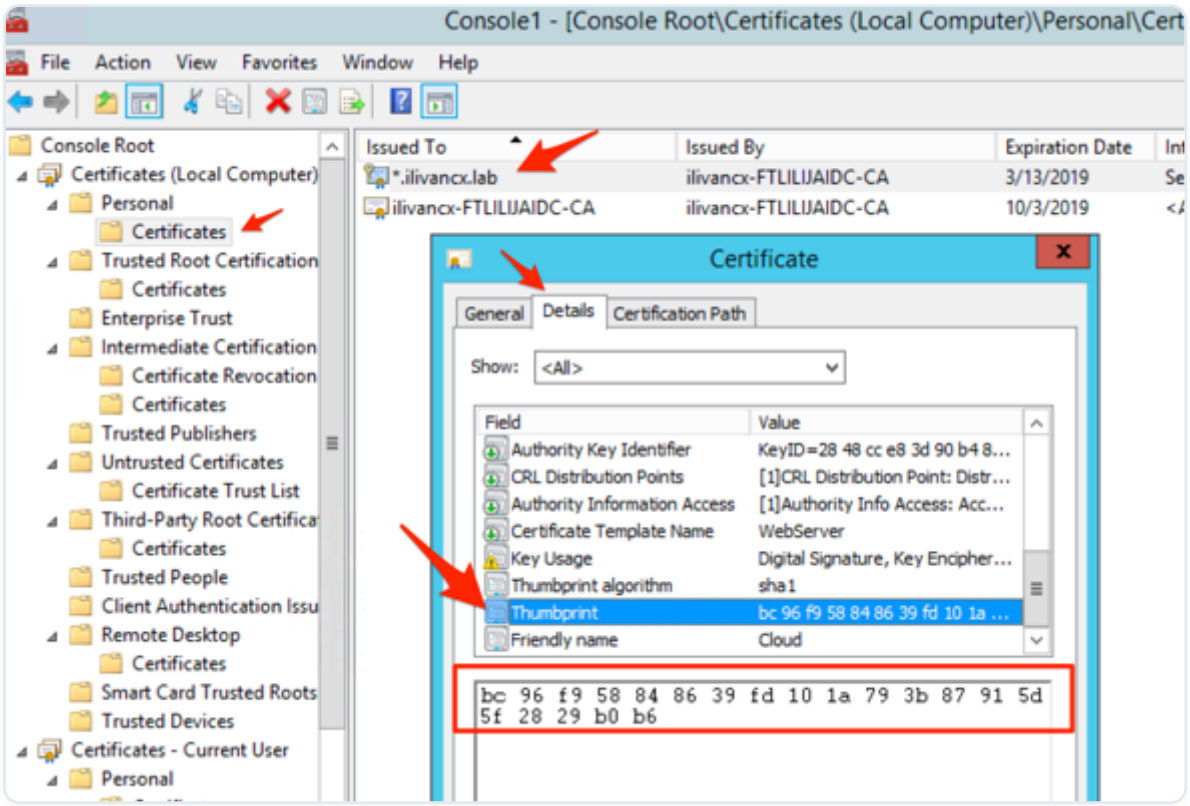
```
netsh http show sslcert
```

2. 如果存在现有绑定，请将其删除。

```
netsh http delete sslcert ipport=0.0.0.0:443
```

如果现有绑定中指定了 IP 地址和端口，请将 `0.0.0.0:443` 替换为特定的 IP 地址和端口。

3. 查找您之前安装的证书的指纹。要查看指纹，请打开**管理计算机证书**，浏览到该证书并将其打开，然后转到**详细信息**选项卡。




或者，您可以使用 PowerShell。例如，以下脚本查找其公用名与服务器主机名匹配的证书并打印缩略图：

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

如果证书公用名与主机名不匹配，则此操作将失败。如果主机名存在多个证书，则此操作将返回多个连接在一起的指纹，您必须选择相应的指纹。

以下示例按友好名称查找证书：

```
$friendlyName = "My certificate name"

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $friendlyName: $
($Thumbprint)" -Foreground Yellow
```

如果存在多个具有指定友好名称的证书，则此操作将返回多个连接在一起的指纹，您必须选择相应的指纹。

4. 要将证书绑定到端口，请使用 `netsh http add sslcert` 命令：

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`：IP 地址和端口。使用 0.0.0.0:443 将其应用于所有 IP 地址。您也可以指定特定的 IP 地址。
- `certhash`：您在上一步中确定的证书指纹。
- `appid`: Citrix Broker 服务的 GUID。

> **注意：**
>
> 续订证书或重新绑定时，请使用与 Broker Service 关联的特定 `appid`，而不是任意 GUID。
>
> 要查找 Citrix Broker Service 的正确 `appid`：

a. 以管理员身份打开 PowerShell 命令窗口并运行以下命令：

```
Get-WmiObject -Class Win32_Product | Select-String -Pattern
"broker"
```

b. 在输出中找到 Citrix Broker Service 的 IdentifyingNumber (GUID)（例如，`{D333C884-187F-447C-8C67-463F33989C8F}`）。将此 GUID 用于 `appid` 参数。

- `disablelegacytls=enable`：禁用旧版 TLS。此参数在 Windows 2022 及更高版本上可用。在 Windows 2022 上，它会禁用 TLS 1.0 和 1.1。在 Windows 2025 上，这没有必要，因为 TLS 1.0 和 1.1 默认处于禁用状态。

例如，运行以下命令将指纹为 `bc96f958848639fd101a793b87915d5f2829b0b6` 的证书绑定到所有 IP 地址上的端口 `443`：

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

启用 HTTPS 后，您应配置任何 StoreFront 部署 和 Netscaler Gateway 以使用 HTTPS 而不是 HTTP 连接到交付控制器。

**注意：**

如果控制器安装在 Windows Server 2016 上，并且 StoreFront 安装在 Windows Server 2012 R2 上，则需要在控制器上进行配置更改，以更改 TLS 密码套件的顺序。对于控制器和 StoreFront 与其他 Windows Server 版本组合的情况，则不需要此配置更改。

密码套件顺序列表必须包含 `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` 或 `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` 密码套件（或两者）；并且这些密码套件必须位于任何 `TLS_DHE_` 密码套件之前。

1. 使用 Microsoft 组策略编辑器，浏览到 **计算机配置 > 管理模板 > 网络 > SSL 配置设置**。
2. 编辑策略“SSL 密码套件顺序”。默认情况下，此策略设置为“未配置”。将此策略设置为“已启用”。
3. 按正确顺序排列套件；删除任何您不想使用的密码套件。

确保 `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` 或 `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` 位于任何 `TLS_DHE_` 密码套件之前。

在 Microsoft MSDN 上，另请参阅 优先处理 Schannel 密码套件。

## 更改 HTTP 或 HTTPS 端口

默认情况下，Controller 上的 XML Service 侦听端口 80 用于 HTTP 流量，侦听端口 443 用于 HTTPS 流量。尽管您可以使用非默认端口，但请注意将 Controller 暴露给不受信任网络的安全风险。部署独立的 StoreFront 服务器优于更改默认设置。

要更改 Controller 使用的默认 HTTP 或 HTTPS 端口，请从 Studio 运行以下命令：

```
BrokerService.exe -WIPORT \<http-port> -WISSLPORT \<https-port>
```

其中 `<http-port>` 是 HTTP 流量的端口号，`<https-port>` 是 HTTPS 流量的端口号。

> **注意：**
>
> 更改端口后，Studio 可能会显示有关许可证兼容性和升级的消息。要解决此问题，请使用以下 PowerShell cmdlet 序列重新注册服务实例：

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS
|

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

### 仅强制执行 HTTPS 流量

如果您希望 XML Service 忽略 HTTP 流量，请在 Controller 上的 HKLM\Software\Citrix\DesktopServer\ 中创建以下注册表设置，然后重新启动 Broker Service。

要忽略 HTTP 流量，请创建 DWORD XmlServicesEnableNonSsl 并将其设置为 0。

您可以创建一个相应的注册表 DWORD 值来忽略 HTTPS 流量：DWORD XmlServicesEnableSsl。确保其未设置为 0。

## VDA 上的 TLS 设置

交付组不能混合配置了 TLS 的 VDA 和未配置 TLS 的 VDA。在为交付组配置 TLS 之前，请确保已为该交付组中的所有 VDA 配置了 TLS。

在 VDA 上配置 TLS 时，已安装的 TLS 证书的权限会发生更改，从而授予 ICA® Service 对证书私钥的读取访问权限，并通知 ICA Service 以下信息：

- **证书存储中用于 TLS 的证书**。
- **用于 TLS 连接的 TCP 端口号**。

必须配置 Windows 防火墙（如果已启用）以允许在此 TCP 端口上进行入站连接。当您使用 PowerShell 脚本时，此配置会自动完成。

- **允许的 TLS 协议版本**。

> **重要提示：**
>
> Citrix 建议您审查 SSLv3 的使用情况，并在适当的情况下重新配置这些部署以删除对 SSLv3 的支持。请参阅 CTX200238。
>
> 支持的 TLS 协议版本遵循以下层次结构（从低到高）：SSL 3.0、TLS 1.0、TLS 1.1 和 TLS 1.2。指定允许的最低版本；使用该版本或更高版本的所有协议连接都将被允许。

例如，如果将 TLS 1.1 指定为最低版本，则允许 TLS 1.1 和 TLS 1.2 协议连接。如果将 SSL 3.0 指定为最低版本，则允许所有受支持版本的连接。如果将 TLS 1.2 指定为最低版本，则只允许 TLS 1.2 连接。

DTLS 1.0 对应于 TLS 1.1，DTLS 1.2 对应于 TLS 1.2。

- **允许哪些 TLS 密码套件。**

密码套件选择用于连接的加密方式。客户端和 VDA 可以支持不同的密码套件集。当客户端（Citrix Workspace 应用程序或 StoreFront）连接并发送支持的 TLS 密码套件列表时，VDA 会将客户端的密码套件之一与其自身配置的密码套件列表中的一个密码套件进行匹配，并接受连接。如果没有匹配的密码套件，VDA 将拒绝连接。

VDA 支持三组密码套件（也称为合规模式）：GOV（政府）、COM（商业）和 ALL。可接受的密码套件还取决于 Windows FIPS 模式；有关 Windows FIPS 模式的信息，请参阅 `<http://support.microsoft.com/kb/811833>`。下表列出了每组中的密码套件：

| TLS/DTLS 密码套件 | ALL | COM | GOV | ALL | COM | GOV |
|---|---|---|---|---|---|---|
| **FIPS 模式** | 关闭 | 关闭 | 关闭 | 开 | 开 | 开 |
| TLS_ECDHE_RSA_WITH_AES_256_ | X | | X | X | | X |

| TLS/ DTLS 密码套件 | ALL | COM | GOV | ALL | COM | GOV |
|---|---|---|---|---|---|---|
| GCM_SHA384* | | | | | | |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | X | | X | X | | X |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | X | X | | X | X | |

* 不支持 Windows Server 2012 R2。

**注意：**

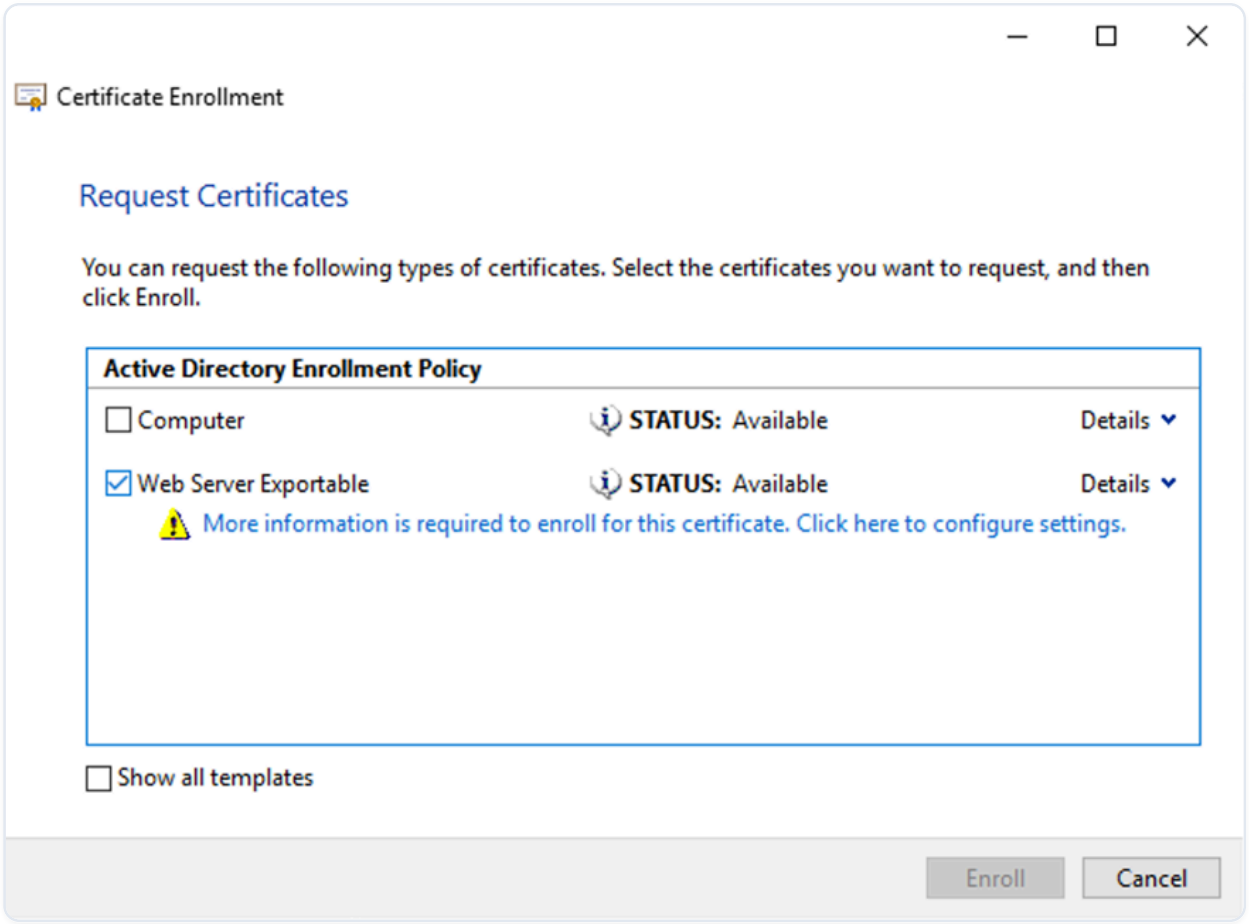
VDA 不支持 DHE 密码套件（例如，TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CBC_SHA、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 和 TLS_DHE_RSA_WITH_AES_128_CBC_SHA）。如果由 Windows 选择，Receiver 可能无法使用它们。

如果您正在使用 Citrix Gateway，请参阅 Citrix ADC 文档，了解有关后端通信的密码套件支持信息。有关 TLS 密码套件支持的信息，请参阅 Citrix ADC 设备上可用的密码。有关 DTLS 密码套件支持的信息，请参阅 DTLS 密码支持。

### 请求和安装证书

1. 在 VDA 上，打开 MMC 控制台并添加“证书”管理单元。出现提示时，选择“计算机帐户”。
2. 展开 **个人 > 证书**，然后使用上下文菜单命令 **所有任务 > 请求新证书**。

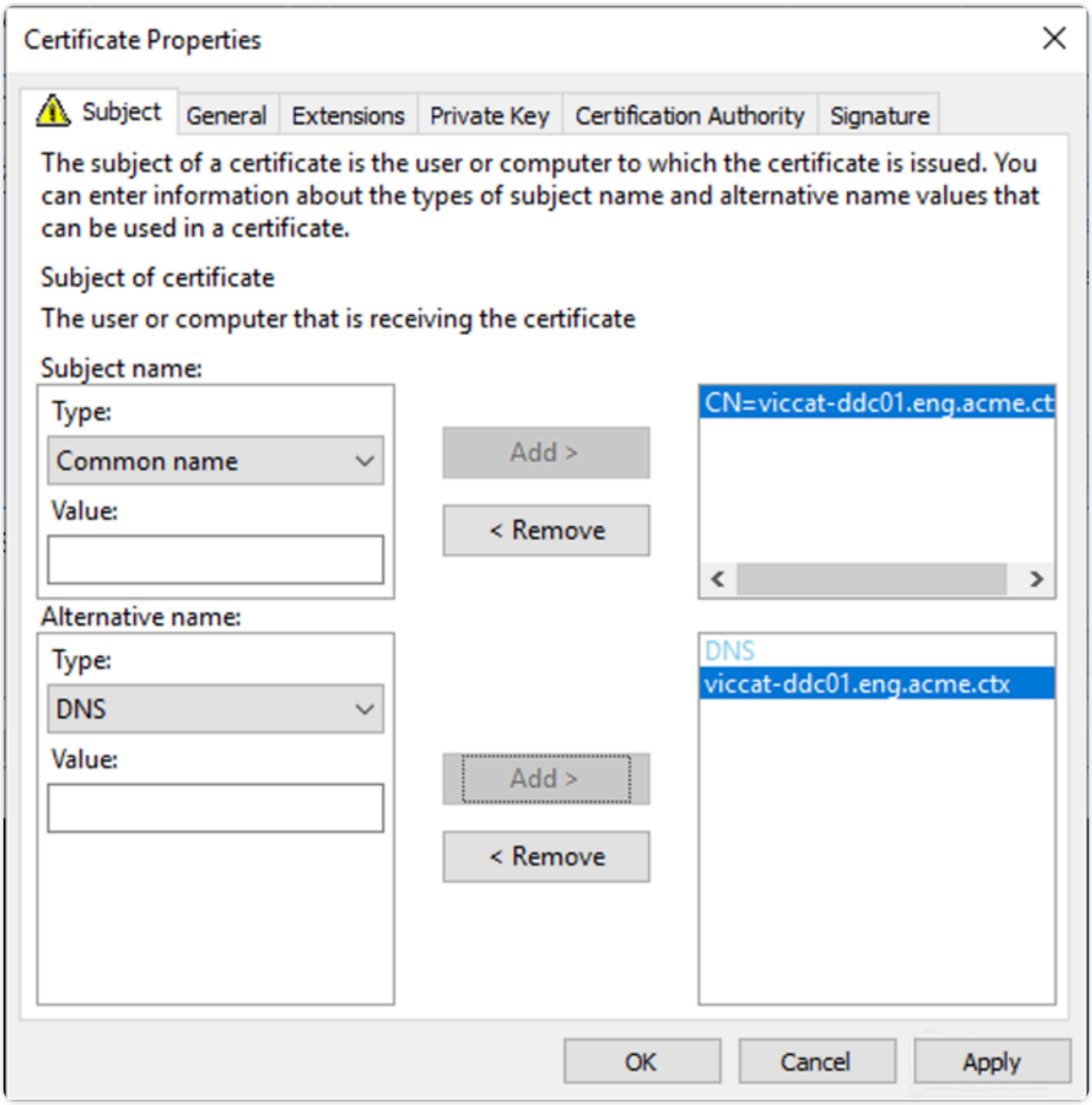
3. 单击 **下一步** 开始，并单击 **下一步** 确认您正在从 Active Directory 注册获取证书。
4. 选择服务器身份验证证书的模板。默认的 Windows **计算机** 或 **Web 服务器可导出** 均可接受。如果模板已设置为自动提供主题的值，则无需提供更多详细信息即可单击 **注册**。




5. 要为证书模板提供更多详细信息，请单击 **详细信息** 并配置以下内容：

   **主题名称** — 选择类型 **公用名** 并添加 VDA 的 FQDN

   **备用名称** — 选择类型 **DNS** 并添加 VDA 的 FQDN



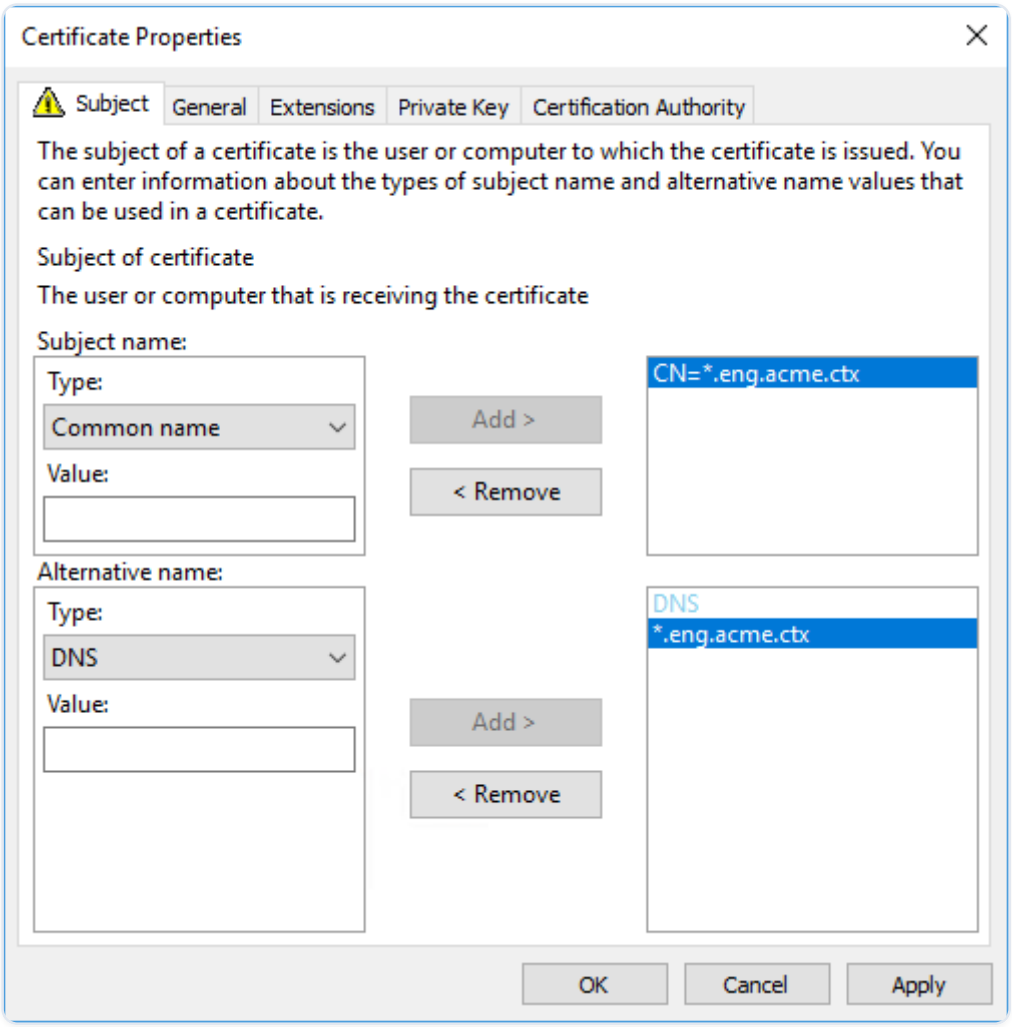

**注意：**

使用 Active Directory 证书服务证书自动注册来自动颁发和部署证书到 VDA。这在 `<https://support.citrix.com/article/CTX205473>` 中进行了描述。

您可以使用通配符证书来允许单个证书保护多个 VDA：

**主题名称** — 选择类型 **通用名称** 并输入 VDA 的 *.primary.domain

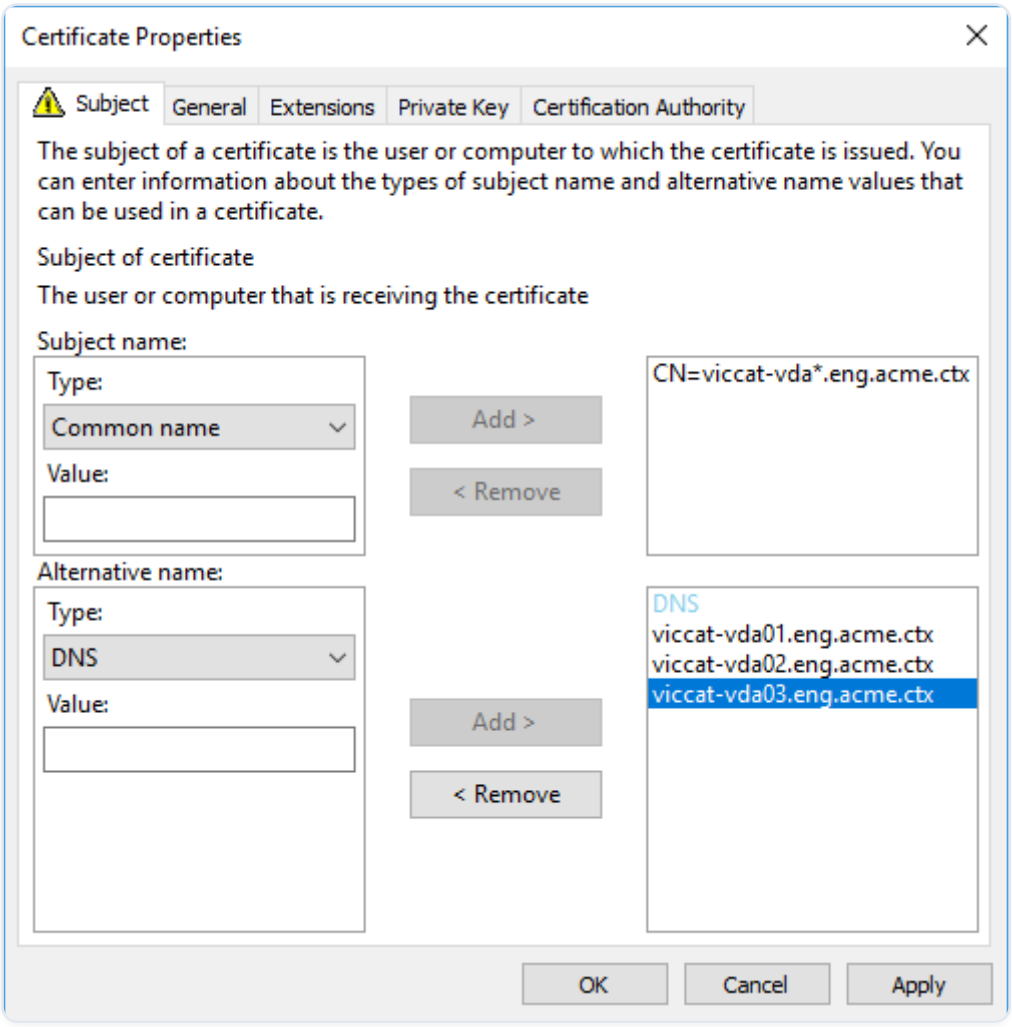
**备用名称** — 选择类型 **DNS** 并添加 VDA 的 *.primary.domain




您可以使用 SAN 证书来允许单个证书保护多个特定的 VDA：

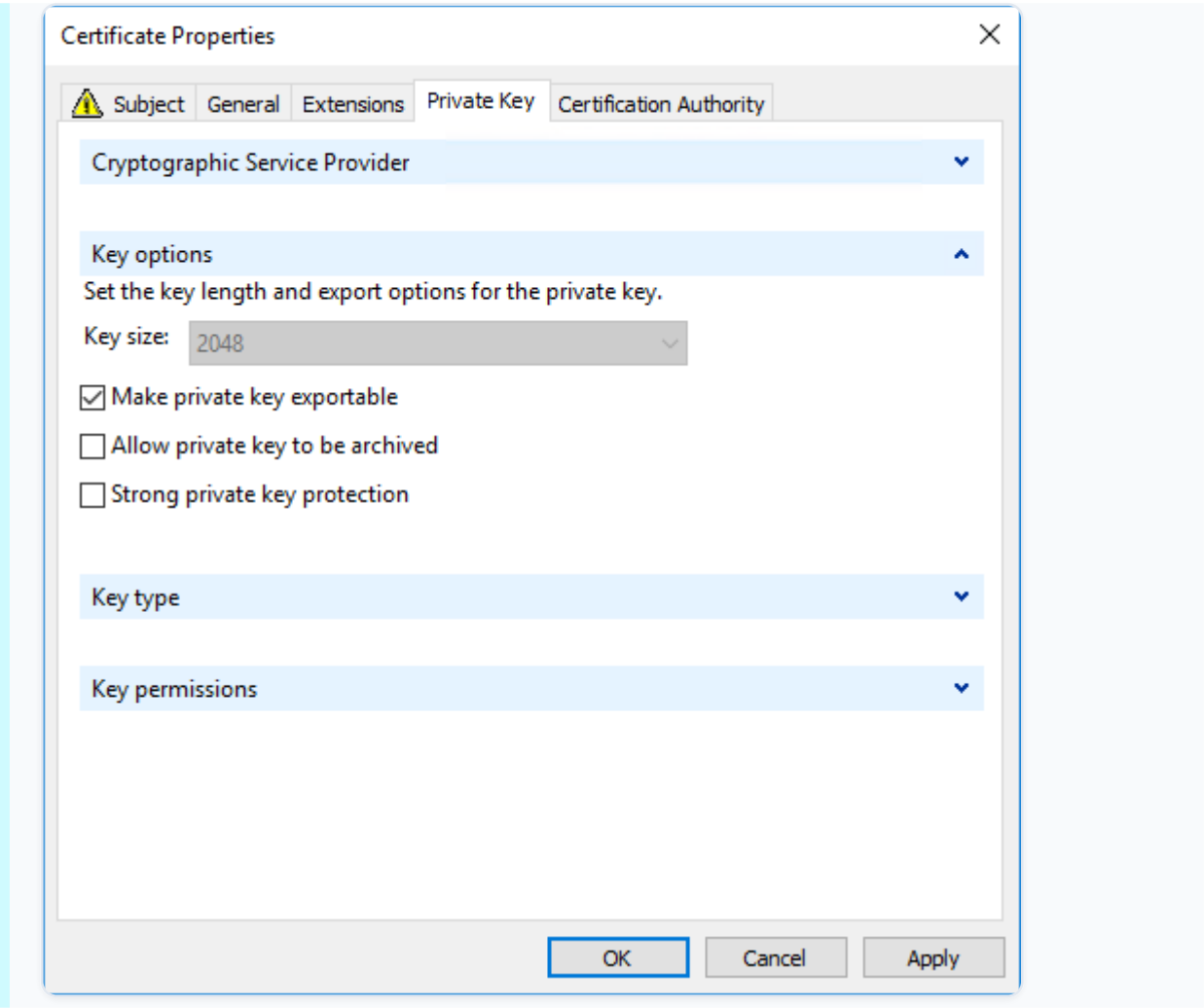
**主题名称** — 选择类型 **通用名称** 并输入一个字符串以帮助识别证书用途

**备用名称** — 选择类型 **DNS** 并为每个 VDA 的 FQDN 添加一个条目。将备用名称的数量保持在最低限度，以确保最佳的 TLS 协商。




**注意：**

通配符证书和 SAN 证书都要求在“私钥”选项卡上选择 **允许导出私钥**：




### 使用 PowerShell 脚本在 VDA 上配置 TLS

将 TLS 证书安装在证书存储的“本地计算机”>“个人”>“证书”区域中。如果该位置存在多个证书，请向 PowerShell 脚本提供证书的指纹。

> **注意：**
>
> 从 XenApp and XenDesktop 7.16 LTSR 开始，PowerShell 脚本会根据 VDA 的 FQDN 查找正确的证书。当 VDA FQDN 只有一个证书时，您无需提供指纹。

> Enable-VdaSSL.ps1 脚本用于在 VDA 上启用或禁用 TLS 侦听器。此脚本位于安装介质的 *Support* > *Tools* > *SslSupport* 文件夹中。

启用 TLS 时，DHE 密码套件将被禁用。ECDHE 密码套件不受影响。

启用 TLS 时，脚本会禁用指定 TCP 端口的所有现有 Windows 防火墙规则。然后，它会添加一条新规则，允许 ICA 服务仅在 TLS TCP 和 UDP 端口上接受传入连接。它还会禁用以下 Windows 防火墙规则：

- Citrix ICA（默认值：1494）
- Citrix CGP（默认值：2598）
- Citrix WebSocket（默认值：8008）

结果是用户只能使用 TLS 或 DTLS 进行连接。如果没有 TLS 或 DTLS，他们将无法使用 ICA/HDX、带有会话可靠性的 ICA/HDX 或通过 WebSocket 的 HDX。

> **注意：**
>
> DTLS 不支持通过 UDP 实时传输的 ICA/HDX 音频，也不支持 ICA/HDX Framehawk。
>
> 请参阅网络端口。

该脚本包含以下语法说明以及其他示例；您可以使用 Notepad++ 等工具查看此信息。

> **重要提示：**
>
> 指定 Enable 或 Disable 参数以及 CertificateThumbPrint 参数。其他参数是可选的。

### 语法

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]
```

| 参数 | 描述 |
| --- | --- |
| 启用 | 在 VDA 上安装并启用 TLS 侦听器。此参数或 Disable 参数是必需的。 |
| 禁用 | 禁用 VDA 上的 TLS 侦听器。此参数或 Enable 参数是必需的。如果指定此参数，则其他参数无效。 |

| 参数 | 描述 |
| --- | --- |
| 证书指纹 "<thumbprint>" | 证书存储中 TLS 证书的指纹，用引号引起来。脚本使用指定的指纹选择要使用的证书。如果省略此参数，则会选择不正确的证书。 |
| SSL端口 <port> | TLS 端口。默认值：443 |
| SSL最低版本 "<version>" | 最低 TLS 协议版本，用引号引起来。有效值：“TLS_1.0”（默认）、“TLS_1.1”和“TLS_1.2”。 |
| SSL密码套件 "<suite>" | TLS 密码套件，用引号引起来。有效值：“GOV”、“COM”和“ALL”（默认）。 |

### 示例

以下脚本安装并启用 TLS 协议版本值。指纹（在此示例中表示为“12345678987654321”）用于选择要使用的证书。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

以下脚本安装并启用 TLS 侦听器，并指定 TLS 端口 400、GOV 密码套件和最低 TLS 1.2 协议值。指纹（在此示例中表示为“12345678987654321”）用于选择要使用的证书。

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.2"

-SSLCipherSuite "All"
```

以下脚本禁用 VDA 上的 TLS 侦听器。

```
Enable-VdaSSL -Disable
```

### 在 VDA 上手动配置 TLS

在 VDA 上手动配置 TLS 时，您需要为每个 VDA 上的相应服务授予 TLS 证书私钥的通用读取权限：对于适用于 Windows 单会话操作系统的 VDA，为 NT SERVICE\PorticaService；对于适用于 Windows 多会话操作系统的 VDA，为 NT SERVICE\TermService。在安装 VDA 的计算机上：

**步骤 1**。启动 Microsoft 管理控制台 (MMC)：开始 > 运行 > mmc.exe。

**步骤 2**。将“证书”管理单元添加到 MMC：

1. 选择“文件”>“添加/删除管理单元”。
2. 选择“证书”，然后单击“添加”。
3. 当系统提示“此管理单元将始终管理以下对象的证书:”时，选择“计算机帐户”，然后单击“下一步”。
4. 当系统提示“选择此管理单元要管理的计算机”时，选择“本地计算机”，然后单击“完成”。

**步骤 3**。在“证书 (本地计算机)”>“个人”>“证书”下，右键单击证书，然后选择“所有任务”>“管理私钥”。

**步骤 4**。访问控制列表编辑器显示“（友好名称）私钥的权限”，其中（友好名称）是您的 TLS 证书的名称。添加以下服务之一并为其授予“读取”访问权限：

- 对于 Windows 单会话操作系统 VDA，“PORTICASERVICE”
- 对于 Windows 多会话操作系统 VDA，“TERMSERVICE”

**步骤 5**。双击已安装的 TLS 证书。在证书对话框中，选择“详细信息”选项卡，然后滚动到底部。单击“指纹”。

**步骤 6**。运行 regedit 并转到 HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd。

1. 编辑 SSL Thumbprint 密钥，并将 TLS 证书指纹的值复制到此二进制值中。您可以安全地忽略“编辑二进制值”对话框中的未知项（例如“0000”和特殊字符）。
2. 编辑 SSLEnabled 密钥并将 DWORD 值更改为 1。（要稍后禁用 SSL，请将 DWORD 值更改为 0。）
3. 如果要更改默认设置（可选），请在同一注册表路径中使用以下内容：

   SSLPort DWORD – SSL 端口号。默认值：443。

   SSLMinVersion DWORD – 1 = SSL 3.0，2 = TLS 1.0，3 = TLS 1.1，4 = TLS 1.2。默认值：2 (TLS 1.0)。

SSLCipherSuite DWORD – 1 = GOV，2 = COM，3 = ALL。默认值：3 (ALL)。

**步骤 7.** 如果 TLS TCP 和 UDP 端口不是默认的 443，请确保它们在 Windows 防火墙中处于打开状态。（在 Windows 防火墙中创建入站规则时，请确保其属性中选中了“允许连接”和“已启用”条目。）

**步骤 8.** 确保没有其他应用程序或服务（例如 IIS）正在使用 TLS TCP 端口。

**步骤 9.** 对于适用于 Windows 多会话操作系统的 VDA，请重新启动计算机以使更改生效。（您无需重新启动包含适用于 Windows 单会话操作系统的 VDA 的计算机。）

**重要提示：**

当 VDA 位于 Windows Server 2012 R2、Windows Server 2016 或 Windows 10 周年更新版或更高版本支持的版本上时，需要执行额外的步骤。这会影响来自适用于 Windows 的 Citrix Receiver（版本 4.6 到 4.9）、适用于 HTML5 的 Citrix Workspace 应用程序和适用于 Chrome 的 Citrix Workspace 应用程序的连接。这还包括使用 Citrix Gateway 的连接。

如果配置了 Citrix Gateway 和 VDA 之间的 TLS，则所有使用 Citrix Gateway 的连接（适用于所有 VDA 版本）也需要此步骤。这会影响所有 Citrix Receiver™ 版本。

在 VDA（Windows Server 2012 R2、Windows Server 2016 或 Windows 10 周年更新版或更高版本）上，使用组策略编辑器，转到“计算机配置”>“策略”>“管理模板”>“网络”>“SSL 配置设置”>“SSL 密码套件顺序”。选择以下顺序：

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

**注意：**

> 前六项还指定了椭圆曲线 P384 或 P256。确保未选择“curve25519”。FIPS 模式不会阻止使用“curve25519”。

> 配置此组策略设置后，VDA 仅在密码套件同时出现在两个列表中时才选择它：组策略列表和所选合规模式（COM、GOV 或 ALL）的列表。密码套件还必须出现在客户端（Citrix Workspace 应用程序或 StoreFront）发送的列表中。

此组策略配置还会影响 VDA 上的其他 TLS 应用程序和服务。如果您的应用程序需要特定的密码套件，您可能需要将它们添加到此组策略列表中。

> **重要提示：**
>
> 尽管组策略更改在应用时会显示，但 TLS 配置的组策略更改仅在操作系统重新启动后才会生效。因此，对于池化桌面，请将 TLS 配置的组策略更改应用到基础映像。

### 在交付组上配置 TLS

对于包含已配置为 TLS 连接的 VDA 的每个交付组，请完成此过程。

1. 从 Studio 打开 PowerShell 控制台。
2. 运行 **asnp Citrix.*** 以加载 Citrix 产品 cmdlet。
3. 运行 **Get-BrokerAccessPolicyRule -DesktopGroupName '\<*delivery-group-name*>' \| Set-BrokerAccessPolicyRule -HdxSslEnabled $true**。
4. 运行 **Set-BrokerSite -DnsResolutionEnabled $true**。

### 故障排除

如果发生连接错误，请检查 VDA 上的系统事件日志。

使用适用于 Windows 的 Citrix Workspace 应用程序时，如果收到指示 TLS 错误的连接错误，请禁用 Desktop Viewer，然后尝试重新连接。尽管连接仍然失败，但可能会提供有关底层 TLS 问题的解释。（例如，在向证书颁发机构请求证书时指定了不正确的模板。）

大多数使用 HDX™ 自适应传输的配置都可以成功使用 DTLS，包括使用最新版本的 Citrix Workspace 应用程序、Citrix Gateway 和 VDA 的配置。某些在 Citrix Workspace 应用程序和 Citrix Gateway 之间使用 DTLS 以及在 Citrix Gateway 和 VDA 之间使用 DTLS 的配置需要额外操作。

在以下情况下需要额外操作：

- Citrix Receiver 版本支持 HDX 自适应传输和 DTLS：适用于 Windows 的 Receiver (4.7, 4.8, 4.9)、适用于 Mac 的 Receiver (12.5, 12.6, 12.7)、适用于 iOS 的 Receiver (7.2, 7.3.x) 或适用于 Linux 的 Receiver (13.7)

并且以下任一情况也适用：

- Citrix Gateway 版本支持到 VDA 的 DTLS，但 VDA 版本不支持 DTLS（版本 7.15 或更早版本），
- VDA 版本支持 DTLS（版本 7.16 或更高版本），但 Citrix Gateway 版本不支持到 VDA 的 DTLS。

为避免 Citrix Receiver 连接失败，请执行以下操作之一：

- 将 Citrix Receiver 更新到适用于 Windows 的 Receiver 4.10 或更高版本、适用于 Mac 的 Receiver 12.8 或更高版本，或适用于 iOS 的 Receiver 7.5 或更高版本；或者，
- 将 Citrix Gateway 更新到支持到 VDA 的 DTLS 的版本；或者，
- 将 VDA 更新到 7.16 或更高版本；或者，
- 在 VDA 上禁用 DTLS；或者，
- 禁用 HDX 自适应传输。

> **注意：**
>
> 适用于 Linux 版 Receiver 的相应更新尚未推出。Android 版 Receiver（版本 3.12.3）不支持通过 Citrix Gateway 使用 HDX 自适应传输和 DTLS，因此不受影响。

> 要在 VDA 上禁用 DTLS，请修改 VDA 防火墙配置以禁用 UDP 端口 443。请参阅网络端口。

## Controller 与 VDA 之间的通信

Windows Communication Framework (WCF) 消息级保护可保护 Controller 与 VDA 之间的通信。不需要使用 TLS 的额外传输级保护。WCF 配置使用 Kerberos 在 Controller 和 VDA 之间进行相互身份验证。加密使用具有 256 位密钥的 CBC 模式 AES。消息完整性使用 SHA-1。

根据 Microsoft 的说法，WCF 使用的安全协议符合 OASIS（结构化信息标准促进组织）的标准，包括 WS-SecurityPolicy 1.2。此外，Microsoft 表示 WCF 支持安全策略 1.2中列出的所有算法套件。

Controller 与 VDA 之间的通信使用 basic256 算法套件，其算法如上所述。

### TLS 与 HTML5 视频重定向以及浏览器内容重定向

您可以使用 HTML5 视频重定向和浏览器内容重定向来重定向 HTTPS 网站。注入到这些网站中的 JavaScript 必须与在 VDA 上运行的 Citrix HDX HTML5 视频重定向服务建立 TLS 连接。为此，HTML5 视频重定向服务会在 VDA 上的证书存储中生成两个自定义证书。停止服务会删除这些证书。

HTML5 视频重定向策略默认处于禁用状态。

浏览器内容重定向默认处于启用状态。

有关 HTML5 视频重定向的详细信息，请参阅多媒体策略设置。

## 通用打印服务器上的传输层安全 (TLS)

虚拟投递代理 (VDA) 和通用打印服务器之间的基于 TCP 的连接支持传输层安全 (TLS) 协议。

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

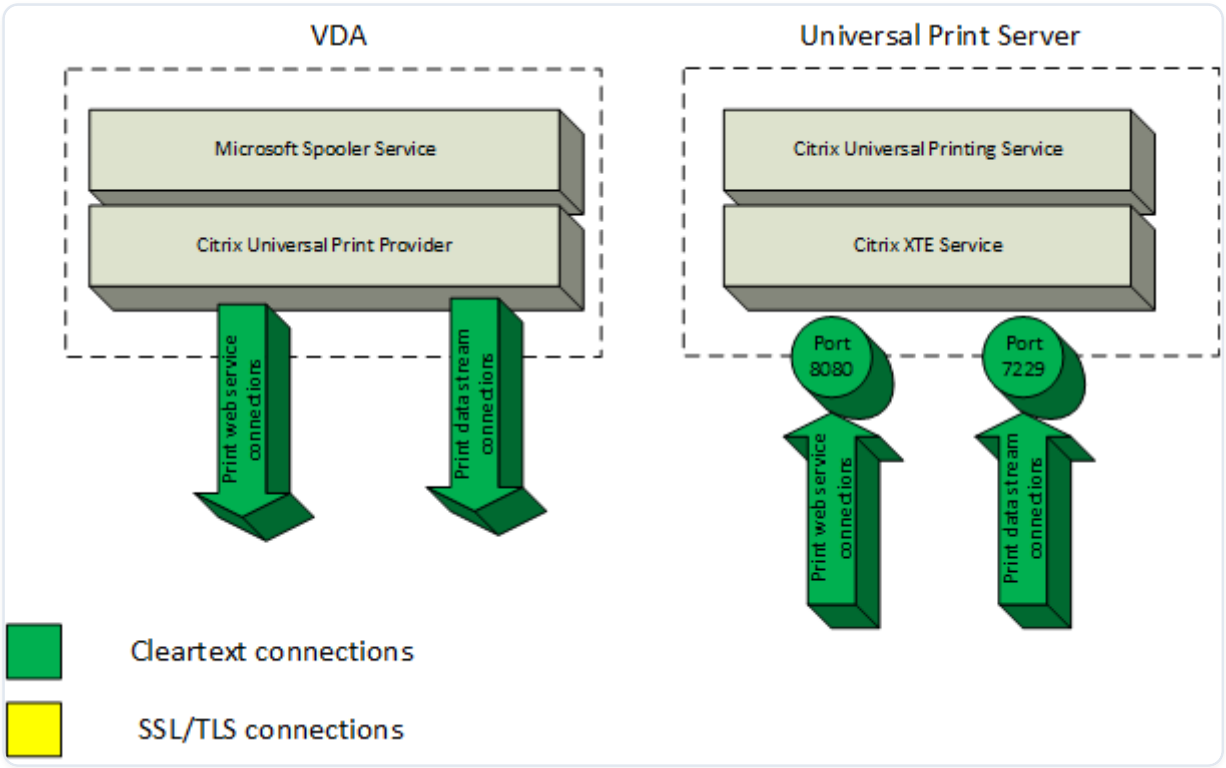
### VDA 与通用打印服务器之间的打印连接类型

#### 明文连接

以下与打印相关的连接源自 VDA 并连接到通用打印服务器上的端口。仅当 **SSL enabled** 策略设置为 **Disabled**（默认值）时，才会建立这些连接。

- 明文打印 Web 服务连接（TCP 端口 8080）
- 明文打印数据流 (CGP) 连接（TCP 端口 7229）

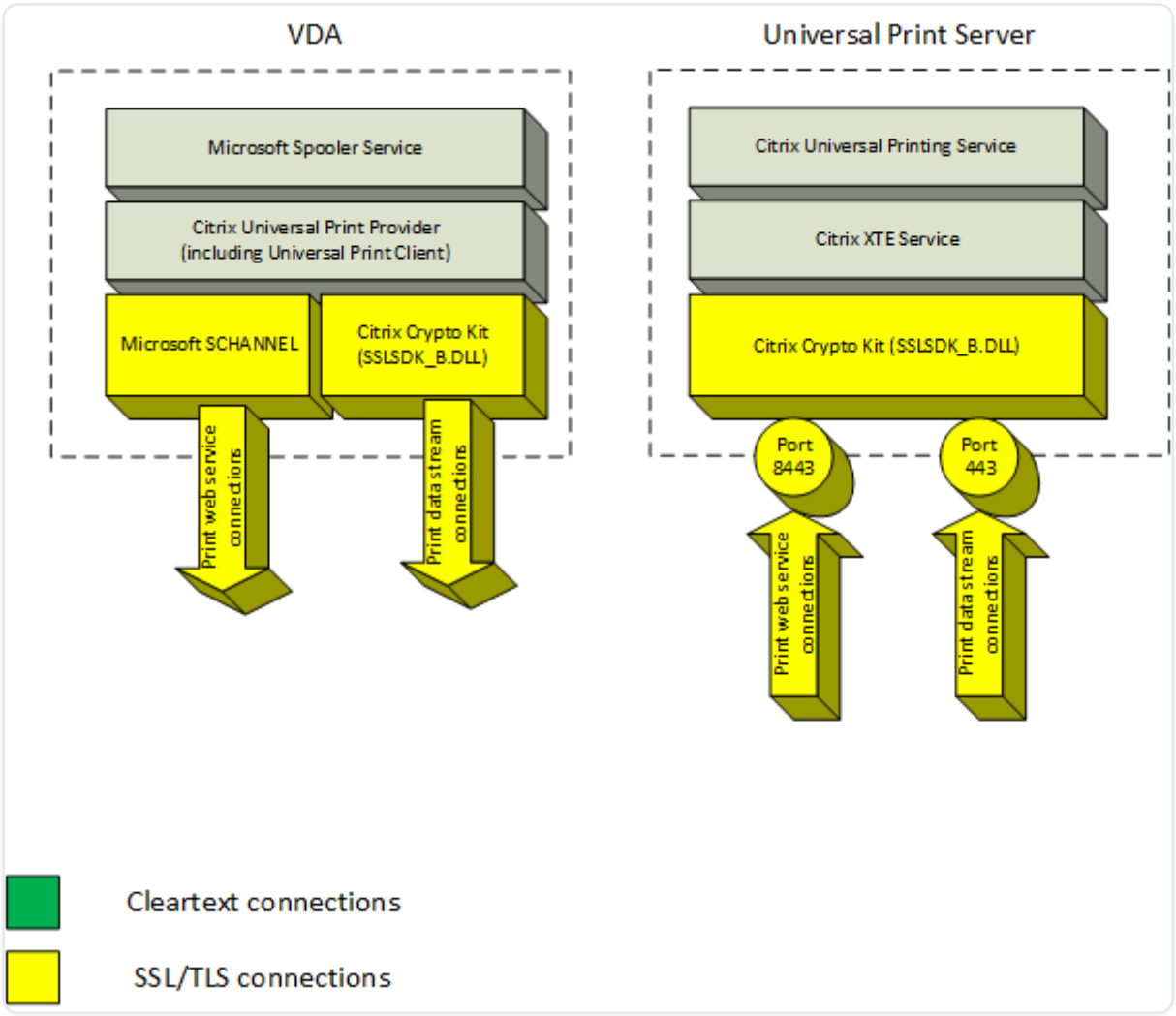
Microsoft 支持文章 Windows 服务概述和网络端口要求 介绍了 Microsoft Windows 打印后台处理程序服务使用的端口。本文档中的 SSL/TLS 设置不适用于 Windows 打印后台处理程序服务进行的 NETBIOS 和 RPC 连接。如果 **Universal Print Server enable** 策略设置设置为 **Enabled with fallback to Windows' native remote printing**，VDA 将使用 Windows 网络打印提供程序 (win32spl.dll) 作为备用。




**加密连接**

这些与打印相关的 SSL/TLS 连接源自 VDA 并连接到通用打印服务器上的端口。仅当 **SSL enabled** 策略设置为 **Enabled** 时，才会建立这些连接。

- 加密打印 Web 服务连接（TCP 端口 8443）
- 加密打印数据流 (CGP) 连接（TCP 端口 443）




**SSL/TLS 客户端配置**

VDA 充当 SSL/TLS 客户端。

使用 Microsoft 组策略和注册表配置 Microsoft SCHANNEL SSP，以用于加密的打印 Web 服务连接（TCP 端口 8443）。Microsoft 支持文章 TLS 注册表设置 介绍了 Microsoft SCHANNEL SSP 的注册表设置。

在 VDA（Windows Server 2016 或 Windows 10）上，使用组策略编辑器，转到 **计算机配置 > 管理模板 > 网络 > SSL 配置设置 > SSL 密码套件顺序**。选择以下顺序：

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **注意：**

> 配置此组策略设置后，VDA 仅当连接同时出现在两个 SSL 密码套件列表中时，才会为加密的打印 Web 服务连接（默认端口：8443）选择密码套件：

> - 组策略 SSL 密码套件顺序列表
> - 与所选 SSL 密码套件策略设置（COM、GOV 或 ALL）对应的列表

> 此组策略配置还会影响 VDA 上的其他 TLS 应用程序和服务。如果您的应用程序需要特定的密码套件，您可能需要将它们添加到此组策略密码套件顺序列表中。

> **重要提示：**

> TLS 配置的组策略更改仅在操作系统重新启动后生效。

> 使用 Citrix 策略配置加密打印数据流 (CGP) 连接（TCP 端口 443）的 SSL/TLS 设置。

**SSL/TLS 服务器配置**

Universal Print Server 充当 SSL/TLS 服务器。

使用 `Enable-UpsSsl.ps1` PowerShell 脚本配置 SSL/TLS 设置。

**在通用打印服务器上安装 TLS 服务器证书**

对于 HTTPS，Universal Print Server 通过使用服务器证书支持 TLS 功能。不使用客户端证书。使用 Microsoft Active Directory 证书服务或其他证书颁发机构为 Universal Print Server 请求证书。

使用微软活动目录证书服务注册/请求证书时，请记住以下注意事项：

1. 将证书放置在本地计算机的 **个人** 证书存储中。
2. 将证书主题可分辨名称 (Subject DN) 的 **公用名** 属性设置为通用打印服务器的完全限定域名 (FQDN)。在证书模板中指定此项。
3. 将用于生成证书请求和私钥的加密服务提供程序 (CSP) 设置为 **Microsoft 增强型 RSA 和 AES 加密提供程序 (加密)**。在证书模板中指定此项。
4. 将密钥大小设置为至少 2048 位。在证书模板中指定此项。

### 在通用打印服务器上配置 SSL

通用打印服务器上的 XTE 服务侦听传入连接。启用 SSL 后，它将充当 SSL 服务器。传入连接有两种类型：包含打印命令的打印 Web 服务连接，以及包含打印作业的打印数据流连接。可以在这些连接上启用 SSL。SSL 可保护这些连接的机密性和完整性。默认情况下，SSL 处于禁用状态。

用于配置 SSL 的 PowerShell 脚本位于安装介质上，文件名为：`\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

### 在通用打印服务器上配置侦听端口号

以下是 XTE 服务的默认端口：

- 明文打印 Web 服务 (HTTP) TCP 端口：8080
- 明文打印数据流 (CGP) TCP 端口: 7229
- 加密打印 Web 服务 (HTTPS) TCP 端口: 8443
- 加密打印数据流 (CGP) TCP 端口: 443

要更改通用打印服务器上 XTE 服务使用的端口，请以管理员身份在 PowerShell 中运行以下命令（有关 Enable-UpsSsl.ps1 PowerShell 脚本用法的说明，请参阅后面的部分）：

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` 或 `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

### 通用打印服务器上的 TLS 设置

如果您在负载平衡配置中拥有多个 Universal Print Server，请确保所有 Universal Print Server 上的 TLS 设置配置一致。

在 Universal Print Server 上配置 TLS 时，已安装的 TLS 证书的权限会更改，从而授予 Universal Printing Service 对证书私钥的读取访问权限，并通知 Universal Printing Service 以下信息：

- 证书存储中用于 TLS 的证书。
- 用于 TLS 连接的 TCP 端口号。

必须配置 Windows 防火墙（如果已启用）以允许这些 TCP 端口上的入站连接。当您使用 Enable-UpsSsl.ps1 PowerShell 脚本时，将为您完成此配置。

- 允许的 TLS 协议版本。

Universal Print Server 支持 TLS 协议版本 1.2、1.1 和 1.0。指定允许的最低版本。

默认 TLS 协议版本为 1.2。

- 允许的 TLS 密码套件。

密码套件选择用于连接的加密算法。VDA 和 Universal Print Server 可以支持不同的密码套件集。当 VDA 连接并发送支持的 TLS 密码套件列表时，Universal Print Server 会将其自身配置的密码套件列表中的一个密码套件与客户端的一个密码套件进行匹配，并接受连接。如果没有匹配的密码套件，Universal Print Server 将拒绝连接。

Universal Print Server 支持名为 GOV(ernment)、COM(mercial) 和 ALL 的密码套件集，用于 OPEN、FIPS 和 SP800-52 本机 Crypto Kit 模式。可接受的密码套件还取决于 **SSL FIPS Mode** 策略设置和 Windows FIPS 模式。有关 Windows FIPS 模式的信息，请参阅此 Microsoft 支持文章。

| 密码套件（按优先级降序排列） | OPEN ALL | OPEN COM | OPEN GOV | FIPS ALL | FIPS COM | FIPS GOV | SP800-52 ALL | SP800-52 COM | SP800-52 GOV |
|---|---|---|---|---|---|---|---|---|---|
| TLS_ECDHE_RSA_AES256_GCM_SHA384 | X | | X | X | | X | X | | X |
| TLS_ECDHE_RSA_AES256_CBC_ | X | | X | X | | X | X | | X |

| 密码套件（按优先级降序排列） | OPEN ALL | OPEN COM | OPEN GOV | FIPS ALL | FIPS COM | FIPS GOV | SP800-52 ALL | SP800-52 COM | SP800-52 GOV |
|---|---|---|---|---|---|---|---|---|---|
| SHA384 | | | | | | | | | |
| TLS_ECDHE_RSA_AES256_CBC_SHA | X | X | | X | X | | X | X | |

### 使用 PowerShell 脚本在 Universal Print Server 上配置 TLS

将 TLS 证书安装到证书存储的 **本地计算机 > 个人 > 证书** 区域。如果该位置存在多个证书，请向 `Enable-UpsSsl.ps1` PowerShell 脚本提供证书的指纹。

> **注意：**
>
> PowerShell 脚本根据 Universal Print Server 的 FQDN 查找正确的证书。如果 Universal Print Server FQDN 只有一个证书，则无需提供证书指纹。

> `Enable-UpsSsl.ps1` 脚本启用或禁用从 VDA 到 Universal Print Server 的 TLS 连接。此脚本位于安装介质的 **Support > Tools > SslSupport** 文件夹中。

启用 TLS 后，脚本会禁用 Universal Print Server 的 TCP 端口的所有现有 Windows 防火墙规则。然后，它会添加新规则，允许 XTE 服务仅在 TLS TCP 和 UDP 端口上接受传入连接。它还会禁用以下 Windows 防火墙规则：

- 明文打印 Web 服务连接（默认值：8080）
- 明文打印数据流 (CGP) 连接（默认值：7229）

其效果是 VDA 只能在使用 TLS 时建立这些连接。

**注意：**

启用 TLS 不会影响从 VDA 发起到 Universal Print Server 的 Windows 打印后台处理程序 RPC/SMB 连接。

**重要提示：**

将 **Enable** 或 **Disable** 指定为第一个参数。如果本地计算机个人证书存储中只有一个证书具有 Universal Print Server 的 FQDN，则 CertificateThumbprint 参数是可选的。其他参数是可选的。

### 语法

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort &lt;port&gt;] [-CGPPort &lt;port&gt;] [-HTTPSPort &lt;port&gt;] [-CGPSSLPort &lt;port&gt;] [-SSLMinVersion &lt;version&gt;] [-SSLCipherSuite &lt;name&gt;] [-CertificateThumbprint &lt;thumbprint&gt;] [-FIPSMode &lt;Boolean&gt;] [-ComplianceMode &lt;mode&gt;]

Enable-UpsSSL.ps1 -Disable [-HTTPPort &lt;portnum&gt;] [-CGPPort &lt;portnum&gt;]
```

| 参数 | 描述 |
| --- | --- |
| 启用 | 在 XTE Server 上启用 SSL/TLS。此参数或 Disable 参数是必需的。 |
| 禁用 | 在 XTE Server 上禁用 SSL/TLS。此参数或 Enable 参数是必需的。 |
| 证书指纹 `"<thumbprint>"` | 本地计算机个人证书存储中 TLS 证书的指纹，用引号引起来。脚本使用指定的指纹来选择要使用的证书。 |
| HTTP 端口 `<port>` | 明文打印 Web 服务 (HTTP/SOAP) 端口。默认值：8080 |
| CGP 端口 `<port>` | 明文打印数据流 (CGP) 端口。默认值：7229 |

| 参数 | 描述 |
| --- | --- |
| HTTPS 端口 `<port>` | 加密打印 Web 服务 (HTTPS/SOAP) 端口。默认值：8443 |
| CGPSSL 端口 `<port>` | 加密打印数据流 (CGP) 端口。默认值：443 |
| SSL 最低版本 `"<version>"` | 最低 TLS 协议版本，用引号括起来。有效值：“TLS_1.0”、“TLS_1.1”和“TLS_1.2”。默认值：TLS_1.2。 |
| SSL 密码套件 `“<name>”` | TLS 密码套件包的名称，用引号括起来。有效值：“GOV”、“COM”和“ALL”（默认）。 |
| FIPS 模式 `<Boolean>` | 在 XTE 服务器中启用或禁用 FIPS 140 模式。有效值：$true 启用 FIPS 140 模式，$false 禁用 FIPS 140 模式。 |

#### 示例

以下脚本启用 TLS。指纹（在此示例中表示为“12345678987654321”）用于选择要使用的证书。

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

以下脚本禁用 TLS。

```
Enable-UpsSsl.ps1 –Disable
```

### 配置 FIPS 模式

启用美国联邦信息处理标准 (FIPS) 模式可确保通用打印服务器加密连接仅使用符合 FIPS 140 的加密技术。

在客户端上配置 FIPS 模式之前，请先在服务器上配置 FIPS 模式。

查阅 Microsoft 的文档网站以启用/禁用 Windows FIPS 模式。

#### 在客户端上启用 FIPS 模式

在 Delivery Controller™ 上，运行 Citrix Studio 并将 **SSL FIPS 模式** Citrix 策略设置设为“**已启用**”。启用 Citrix 策略。

在每个 VDA 上执行以下操作：

1. 启用 Windows FIPS 模式。

2. 重新启动 VDA。

### 在服务器上启用 FIPS 模式

在每个通用打印服务器上执行以下操作：

1. 启用 Windows FIPS 模式。
2. 以管理员身份运行此 PowerShell 命令: `stop-service CitrixXTEServer, UpSvc`
3. 使用 `-Enable -FIPSMode $true` 参数运行 `Enable-UpsSsl.ps1` 脚本。
4. 重新启动 Universal Print Server。

### 在客户端禁用 FIPS 模式

在 Delivery Controller 上，运行 Citrix Studio 并将 **SSL FIPS 模式** Citrix 策略设置设为“**已禁用**”。启用 Citrix 策略。您还可以删除 **SSL FIPS 模式** Citrix 策略设置。

在每个 VDA 上执行此操作：

1. 禁用 Windows FIPS 模式。
2. 重新启动 VDA。

### 在服务器上禁用 FIPS 模式

在每个 Universal Print Server 上执行此操作：

1. 禁用 Windows FIPS 模式。
2. 以管理员身份运行此 PowerShell 命令: `stop-service CitrixXTEServer, UpSvc`
3. 使用 `-Enable -FIPSMode $false` 参数运行 `Enable-UpsSsl.ps1` 脚本。
4. 重新启动 Universal Print Server。

## 配置 SSL/TLS 协议版本

默认的 SSL/TLS 协议版本是 TLS 1.2。TLS 1.2 是唯一推荐用于生产环境的 SSL/TLS 协议版本。为了进行故障排除，可能需要在非生产环境中临时更改 SSL/TLS 协议版本。

通用打印服务器不支持 SSL 2.0 和 SSL 3.0。

### 在服务器上设置 SSL/TLS 协议版本

在每个通用打印服务器上执行以下操作：

1. 以管理员身份运行此 PowerShell 命令: `stop-service CitrixXTEServer, UpSvc`
2. 运行 `Enable-UpsSsl.ps1` 脚本并使用 `-Enable -SSLMinVersion` 版本参数。请记住，测试完成后将其设置回 TLS 1.2。

3. 重新启动 Universal Print Server。

**在客户端上设置 SSL/TLS 协议版本**

在每个 VDA 上执行以下操作：

1. 在 Delivery Controller 上，将**SSL 协议版本**策略设置设为所需的协议版本并启用该策略。
2. Microsoft 支持文章 TLS 注册表设置 介绍了 Microsoft SCHANNEL SSP 的注册表设置。使用注册表设置启用客户端 **TLS 1.0、TLS 1.1 或 TLS 1.2**。

> **重要提示：**
>
> 请记住，测试完成后，将注册表设置恢复为原始值。

3. 重新启动 VDA。

**故障排除**

如果发生连接错误，请检查 Universal Print Server 上的 C:\Program Files (x86)\Citrix\XTE\logs\error.log 日志文件。

如果 SSL/TLS 握手失败，此日志文件中将显示错误消息 **SSL handshake from client failed**。如果 VDA 和通用打印服务器上的 SSL/TLS 协议版本不匹配，则可能会发生此类故障。

在包含通用打印服务器主机名的以下策略设置中使用通用打印服务器 FQDN：

- 会话打印机
- 打印机分配
- 用于负载平衡的通用打印服务器

确保通用打印服务器和 VDA 上的系统时钟（日期、时间、时区）正确。

# 虚拟通道安全性

默认情况下，虚拟通道允许列表功能已启用。因此，只有 Citrix® 虚拟通道允许在虚拟应用和桌面会话中打开。如果需要使用自定义虚拟通道，无论是内部开发的还是来自第三方的，都需要明确将其添加到允许列表中。

## 将虚拟通道添加到允许列表

要将虚拟通道添加到允许列表，您需要：

1. 代码中定义的虚拟通道名称，最多可包含七个字符。例如，`CTXCVC1`。
2. 在 VDA 计算机上打开虚拟通道的进程路径。例如，`C:\Program Files\Application\run.exe`。

获得所需信息后，您必须使用 虚拟通道允许列表策略设置 将虚拟通道添加到允许列表。要将虚拟通道添加到列表中，请输入虚拟通道名称，后跟逗号，然后是访问该虚拟通道的进程路径。如果有多个进程，可以用逗号分隔添加。

> **注意：**
>
> 更改策略后，重新启动 VDA 以确保更改生效。

> 根据前面的示例，您会将以下内容添加到列表中：

```
CTXCVC1,C:\Program Files\Application\run.exe
```

如果有多个进程，您会将以下内容添加到列表中：

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

## Citrix 虚拟通道注意事项

所有内置的 Citrix 虚拟通道都受信任并允许打开，无需进一步配置。但是，有两个功能由于外部依赖性，需要在允许列表中明确列出：

- 多媒体重定向
- HDX™ 适用于 Skype for Business 的实时优化包

### 多媒体重定向

允许列表条目需要以下信息：

- 虚拟通道名称：CTXMM
- 进程：VDA 计算机中使用的媒体播放器路径。例如，C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- 允许列表条目：`CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

### 适用于 Skype for Business 的 HDX RealTime 优化包

允许列表条目需要以下信息：

- 虚拟通道名称：CTXRMEP
- 进程：VDA 计算机中 Skype for Business 可执行文件的路径，该路径可能因 Skype for Business 版本或您是否使用了自定义安装路径而异。例如，C:\Program Files\Microsoft Office\root\Office16\lync.exe。
- 允许列表条目：`CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

## 获取虚拟通道名称和进程

获取虚拟通道名称以及在 VDA 计算机上打开该通道的进程的最简单方法是，从提供该虚拟通道的开发人员或第三方供应商处获取信息。

此外，还可以通过应用功能的日志并执行以下步骤来获取此信息：

1. 自定义虚拟通道的客户端和服务器组件就位后，启动虚拟应用程序或虚拟桌面。
2. 在 VDA 计算机的系统事件日志中，在以下事件中查找自定义虚拟通道的名称：
   - 在单会话 VDA 中，查找源 Picadd 的事件 ID 2004。
   - 在多会话 VDA 中，查找源 Rpm 的事件 ID 16。
3. 从会话注销。
4. 在已识别的虚拟通道的“虚拟通道允许列表”策略设置中添加一个条目，其中只包含虚拟通道名称。
5. 重新启动 VDA。
6. 再次启动虚拟应用程序或虚拟桌面。
7. 在 VDA 计算机的系统事件日志中，在以下事件中查找尝试打开虚拟通道的进程：
   - 在单会话 VDA 中，查找源 Picadd 的事件 ID 2002。
   - 在多会话 VDA 中，查找源 Rpm 的事件 ID 14。
8. 从会话注销。
9. 编辑虚拟通道允许列表策略设置中的条目，以包含已识别的进程。
10. 重新启动 VDA。
11. 启动虚拟应用程序或虚拟桌面，以验证自定义虚拟通道是否成功打开。

## 虚拟通道允许列表日志记录

以下事件记录在单会话 VDA 计算机的事件日志中：

| | |
|---|---|
| 日志名称 | 系统 |
| ID | 2001 |
| 源 | 添加图片 |
| 级别 | 信息 |
| 描述 | 自定义虚拟通道 `<vcName>` 已由进程 `<processName>` 打开 |

| | |
|---|---|
| 日志名称 | 系统 |
| ID | 2002 |
| 源 | 添加图片 |
| 级别 | 警告 |
| 描述 | 自定义虚拟通道 `<vcName>` 无法由进程 `<processName>` 打开 |

| | |
|---|---|
| 日志名称 | 系统 |
| ID | 2003 |
| 源 | 添加图片 |
| 级别 | 信息 |
| 描述 | `<username>` 打开了自定义虚拟通道 `<vcName>` |

| | |
|---|---|
| 日志名称 | 系统 |
| ID | 2004 |
| 源 | 添加图片 |

| | |
|---|---|
| 级别 | 警告 |
| 描述 | `<username>` 尝试打开自定义虚拟通道 `<vcName>` |

以下事件记录在多会话 VDA 计算机的事件日志中：

| | |
|---|---|
| 日志名称 | 系统 |
| ID | 13 |
| 源 | Rpm |
| 级别 | 信息 |
| 描述 | 自定义虚拟通道 `<vcName>` 已由进程 `<processName>` 打开 |

| | |
|---|---|
| 日志名称 | 系统 |
| ID | 14 |
| 源 | Rpm |
| 级别 | 警告 |
| 描述 | 自定义虚拟通道 `<vcName>` 无法由进程 `<processName>` 打开 |

| | |
|---|---|
| 日志名称 | 系统 |
| ID | 15 |
| 源 | Rpm |
| 级别 | 信息 |
| 描述 | `<username>` 打开了自定义虚拟通道 `<vcName>` |

| | |
|---|---|
| 日志名称 | 系统 |
| ID | 16 |
| 源 | Rpm |
| 级别 | 警告 |
| 描述 | `<username>` 尝试打开自定义虚拟通道 `<vcName>` |

### 已知第三方虚拟通道

以下是使用自定义 Citrix 虚拟通道的已知第三方解决方案。此列表不包括所有使用自定义 Citrix 虚拟通道的解决方案。

- 赛纳
- 思科 Webex Teams
- 思科 WebEx Meetings 虚拟桌面软件
- 艾派克曲速引擎
- Midmark IQPath 客户端扩展
- Nuance PowerMic 客户端扩展
- 纽昂斯 龙 医疗网络版 360 vSync
- 适用于 VDI 的 Zoom Meetings

要获取将相关虚拟通道添加到允许列表的详细信息，请联系解决方案供应商。或者，按照 获取虚拟通道名称和进程 部分中概述的步骤操作。

## 联邦身份验证服务

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

有关使用联邦身份验证服务保护部署的更多信息，请参阅其自己的文档中的联邦身份验证服务文档。

# 设备

HDX™ 可在任何设备、任何位置提供高清用户体验。“设备”部分中的文章介绍了以下设备：

- 通用 USB 设备
- 移动和触摸屏设备
- 串行设备
- 专用键盘
- TWAIN 设备
- 网络摄像头
- WIA 设备

## 优化型 USB 设备与通用型 USB 设备

优化型 USB 设备是指 Citrix Workspace™ 应用程序提供特定支持的设备。例如，能够使用 HDX 多媒体虚拟通道重定向网络摄像头。通用设备是指 Citrix Workspace 应用程序中没有特定支持的 USB 设备。

默认情况下，通用 USB 重定向无法重定向具有优化虚拟通道支持的 USB 设备，除非将其置于通用模式。

通常，USB 设备在优化模式下的性能优于通用模式。但是，在某些情况下，USB 设备在优化模式下无法提供完整功能。此时可能需要切换到通用模式才能完全访问其功能。

对于 USB 大容量存储设备，您可以使用客户端驱动器映射或通用 USB 重定向，或两者结合，具体由 Citrix® 策略控制。主要区别在于：

如果通用 USB 重定向和客户端驱动器映射策略都已启用，并且在大容量存储设备在会话开始之前或之后插入，则会使用客户端驱动器映射对其进行重定向。

当这些条件成立时，大容量存储设备将使用通用 USB 重定向：

- 通用 USB 重定向和客户端驱动器映射策略都已启用。
- 设备已配置为自动重定向。
- 大容量存储设备在会话开始之前或之后插入。

有关详细信息，请参阅 `<http://support.citrix.com/article/CTX123015>`。

| 功能 | 客户端驱动器映射 | 通用 USB 重定向 |
| --- | --- | --- |
| 默认启用 | 是 | 否 |
| 可配置只读访问 | 是 | 否 |
| 加密设备访问 | 是，如果加密在设备于虚拟会话中访问之前已解锁。 | 仅适用于 Citrix Virtual Desktops™ |

# 多显示器混合 DPI

Citrix Virtual Apps and Desktops 环境不支持在不同显示器之间使用不同的 DPI。您可以使用 Windows 控制面板 > 显示选项来验证 DPI（% 缩放）。如果使用 Windows 8.1 或 Windows 10 客户端设备，在 Windows 控制面板 > 显示选项中启用**让我为所有显示器选择一个缩放级别选项**可正确配置显示器。有关详细信息，请参阅知识中心文章 CTX201696。

# 映射的客户端驱动器

作为一项安全预防措施，当用户登录到 Citrix Virtual Apps and Desktops 时，默认情况下，服务器会映射客户端驱动器，但没有用户运行权限。要使用户能够运行驻留在映射客户端驱动器上的可执行文件，请通过编辑服务器上的注册表来覆盖此默认设置。有关注册表设置的信息，请参阅注册表管理的功能列表中的映射的客户端驱动器。

Citrix Virtual Apps and Desktops™ 7 2006 是第一个包含此注册表位置的版本。早期版本的 Citrix Virtual Apps and Desktops 使用了不同的注册表位置。

# 通用 USB 设备

HDX™ 技术为大多数常用 USB 设备提供**优化支持**。这些设备包括：

- 显示器
- 鼠标
- 键盘
- IP 电话
- 耳机
- 网络摄像头

- 扫描仪
- 摄像头
- 打印机
- 驱动器
- 智能卡读卡器
- 绘图板
- 签名板

优化支持通过广域网提供更好的性能和带宽效率，从而改善用户体验。优化支持通常是最佳选择，尤其是在高延迟或安全敏感的环境中。

HDX 技术为没有优化支持或不适合的专用设备提供**通用 USB 重定向**。有关通用 USB 重定向的更多信息，请参阅通用 USB 重定向。

有关 USB 设备和适用于 Windows 的 Citrix Workspace 应用程序的更多信息，请参阅 配置复合 USB 设备重定向 和 配置 USB 支持。

# 对移动和触摸屏客户端设备的支持

Citrix Virtual Apps and Desktops™ 允许用户从移动和触摸屏客户端设备访问其发布的应用程序和桌面。

## 要求

### Citrix® 控制平面

- Citrix Virtual Apps and Desktops 7.15 或更高版本
- 思杰 DaaS™

### 会话主机

- 操作系统
  - Windows 10 1903 或更高版本
  - Windows Server 2016 或更高版本
- VDA
  - Windows：版本 7.15 或更高版本

### 客户端设备

- 操作系统
  - Windows 10 1809 或更高版本
- 适用于 Windows 的 Citrix Workspace™ 应用程序 1808 版或更高版本

## 使用 Windows Continuum 的触摸屏设备的平板电脑模式

Continuum 是 Windows 10 的一项功能，可根据客户端设备的使用方式进行调整。当 VDA 检测到触摸屏客户端上存在键盘或鼠标时，它会将客户端置于桌面模式。如果不存在键盘或鼠标，VDA 会将客户端置于平板电脑/移动模式。此检测在会话连接和重新连接时发生，并在会话中当键盘或鼠标连接或分离时也会发生。

此功能默认启用。要禁用此功能，请配置策略设置 平板电脑模式切换策略设置。

除了上述触屏设备的要求外，Windows Continuum 还需要满足以下条件：

### 思杰虚拟机监控程序™

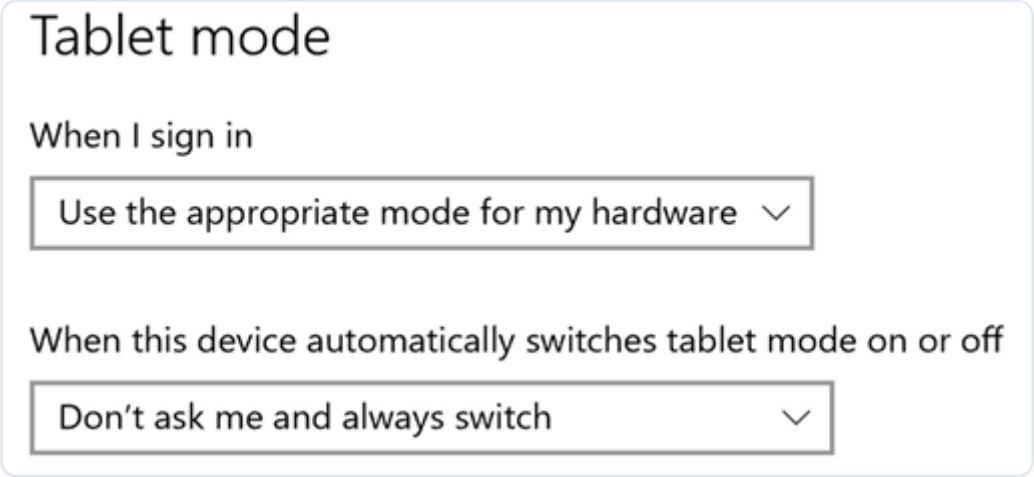
- Citrix Hypervisor 8.2 或更高版本
- 请运行以下 XenServer CLI 命令以允许笔记本电脑/平板电脑切换： **xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1**

> **重要提示：**
>
> 更改元数据设置后更新现有计算机目录的基础映像不会影响任何以前预配的 VM。更改 XenServer VM 基础映像后，请创建目录，选择基础映像，然后预配新的 Machine Creation Services™ (MCS) 计算机。

### 会话主机

- 操作系统
  - Windows 10 1903 或更高版本
  - Windows 十一
- VDA
  - Windows: 7.16 版或更高版本

- **由于操作系统配置的当前限制，用户在启动第一个 ICA® 会话并重新启动 VDA 后，必须从下拉菜单中设置以下选项：**
  - **设置 > 系统 > 平板电脑模式**
    - 为我的硬件使用适当的模式
    - 不询问我并始终切换




**平板电脑模式**提供更适合触摸屏的用户界面：

- 按钮略大。
- “开始”屏幕和您启动的任何应用程序都以全屏模式打开。
- 任务栏包含一个返回按钮。
- 任务栏中的图标已删除。

您可以访问文件资源管理器。



Windows 10 根据此更新的 BIOS 在目标虚拟机上加载 GPIO 驱动程序。它用于在虚拟机内切换平板电脑模式和桌面模式。

适用于 HTML5 的 Citrix Workspace 应用程序不支持 Windows Continuum 功能。

**桌面模式** 提供传统的用户界面，您可以通过与使用 PC、键盘和鼠标相同的方式进行交互。

## 微软 Surface Pro 和 Surface Book 触控笔

我们支持基于 Windows Ink 的应用程序的标准触控笔功能。支持包括指向、擦除、笔压、蓝牙信号以及其他功能，具体取决于操作系统固件和触控笔型号。例如，笔压可达 4096 级。此功能默认启用。

触控笔功能支持的要求如下：

### Citrix 控制平面

- Citrix Virtual Apps and Desktops 1903 或更高版本
- 思杰 DaaS

### 会话主机

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows Server 2016 或更高版本
  - Windows 十一
- VDA
  - Windows：版本 1903 或更高版本

### 客户端设备

- 操作系统
  - Windows 10 1809 或更高版本
- 适用于 Windows 的 Citrix Workspace 应用程序最低版本 1902

要查看 Windows Ink 和笔功能的演示，请单击此图：



要禁用或启用此功能，请参阅通过注册表管理的特性列表中的 Microsoft Surface Pro 和 Surface Book 触控笔。

### 已知问题

以下是笔支持的已知问题：

- 由于 Windows Server 2k22 中的操作系统限制，用户在连接到 2k22 服务器应用程序或桌面时，将无法在“控制面板”中设置笔快捷方式或调整笔/墨迹设置。
- 由于操作系统限制，从启用了笔功能的 Windows 11 客户端发出的笔快捷方式未被识别。

## 串行端口

大多数新电脑没有内置串行 (COM) 端口。通过使用 USB 转换器可以轻松添加这些端口。适用于串行端口的应用程序通常涉及传感器、控制器、旧式支票读取器、手写板等。某些 USB 虚拟 COM 端口设备使用供应商专用驱动程序，而不是 Windows 提供的驱动程序 (usbser.sys)。这些驱动程序允许您强制指定 USB 设备的虚拟 COM 端口，使其即使连接到不同的 USB 插槽也不会更改。这可以通过**设备管理器 > 端口 (COM 和 LPT) > 属性**或控制设备的应用程序来完成。

客户端 COM 端口映射允许在虚拟会话期间使用连接到用户端点上 COM 端口的设备。您可以像使用任何其他网络映射一样使用这些映射。

对于每个 COM 端口，操作系统中的驱动程序会分配一个符号链接名称，例如 COM1 和 COM2。然后应用程序使用该链接访问端口。

> **重要提示：**

> 设备可以通过 USB 直接连接到端点，但这并不意味着它可以使用通用 USB 重定向进行重定向。某些 USB 设备充当虚拟 COM 端口，应用程序可以像访问物理串行端口一样访问它们。操作系统可以抽象化 COM 端口并将其视为文件共享。虚拟 COM 的两种常见协议是 CDC ACM 或 MCT。通过 RS-485 端口连接时，应用程序可能根本无法工作。获取 RS-485 到 RS232 转换器以将 RS-485 用作 COM 端口。 **重要提示：**

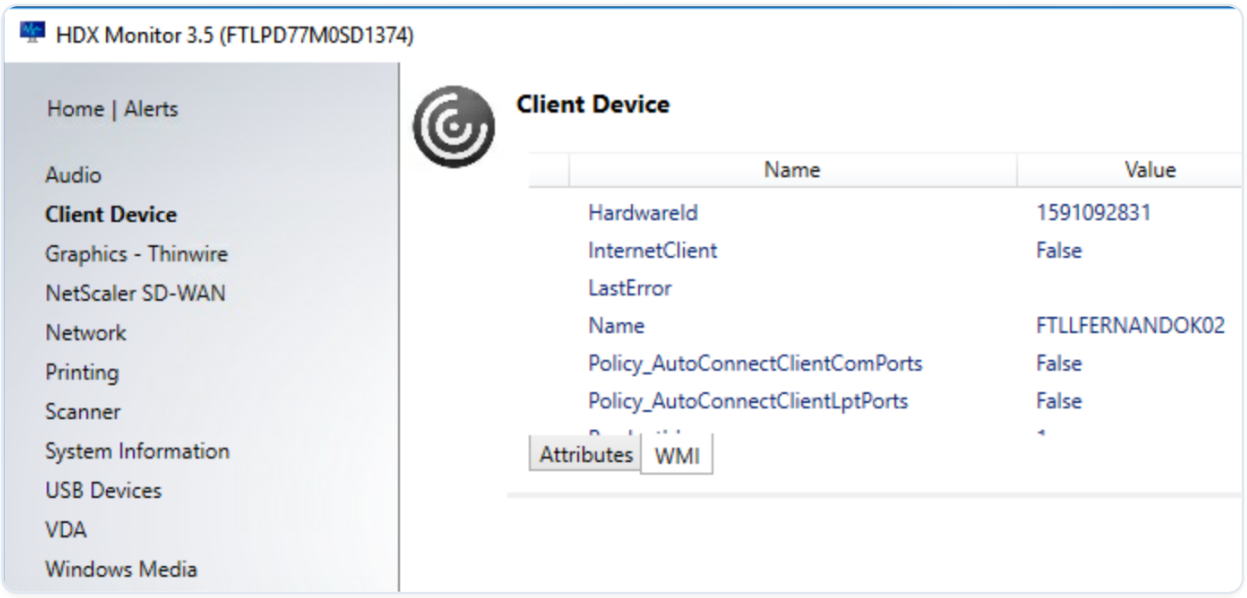
> 某些应用程序仅在设备（例如签名板）连接到客户端工作站上的 COM1 或 COM2 时才能始终如一地识别该设备。

### 将客户端 COM 端口映射到服务器 COM 端口

您可以通过以下三种方式将客户端 COM 端口映射到 Citrix® 会话：

- Studio 策略。有关策略的详细信息，请参阅端口重定向策略设置。
- VDA 命令行。
- 远程桌面（终端服务）配置工具。

1. 启用**客户端 COM 端口重定向**和**自动连接客户端 COM 端口** Studio策略。应用后，HDX™ Monitor 中会提供一些信息。




2. 如果**自动连接客户端 COM 端口**未能映射端口，您可以手动映射端口或使用登录脚本。登录到 VDA，并在命令行窗口中键入：

   NET USE COMX: `\\CLIENT\COMZ`:

   或者

   NET USE COMX: `\\CLIENT\CLIENTPORT:COMZ`:

   **X** 是 VDA 上的 COM 端口号（端口 1 到 9 可用于映射）。**Z** 是您要映射的客户端 COM 端口号。

   要确认操作成功，请在 VDA 命令提示符下键入 **NET USE**。出现的列表包含映射的驱动器、LPT 端口和映射的 COM 端口。

```
C:\Windows\system32>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
             COM3      \\Client\COM3:            Citrix Client Network
```

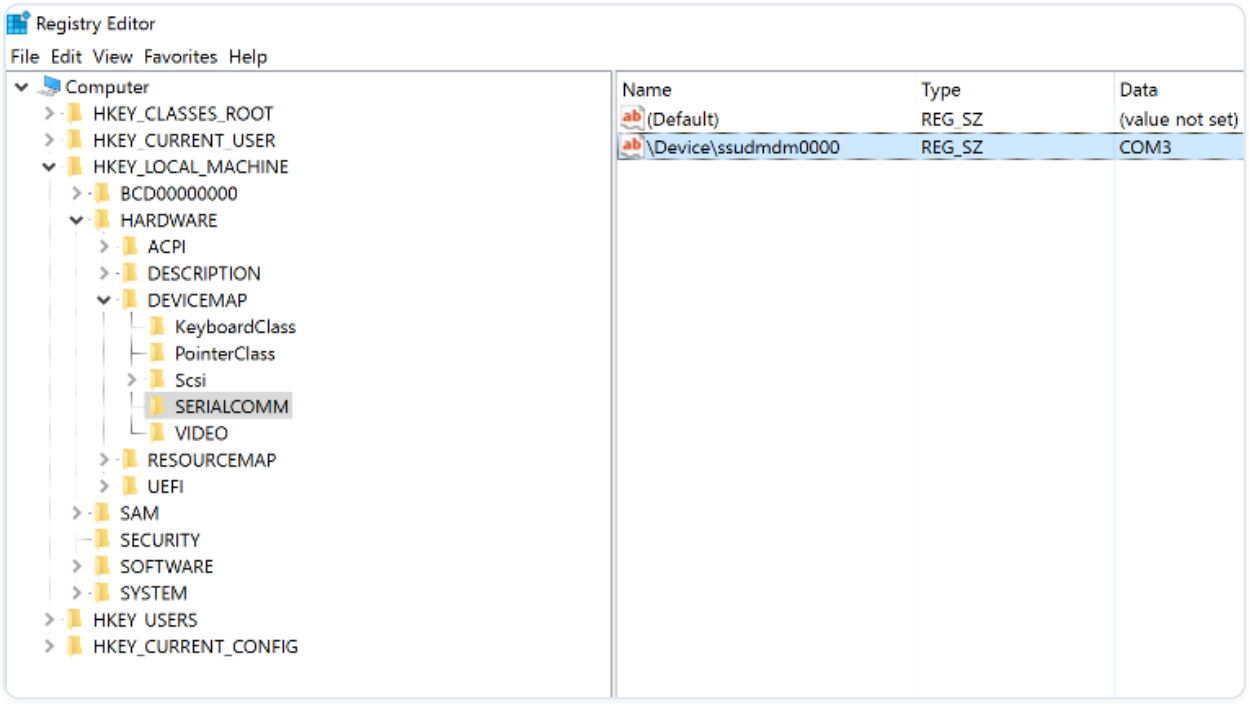
3. 要在虚拟桌面或应用程序中使用此 COM 端口，请安装您的用户设备应用程序并将其指向映射的 COM 端口名称。例如，如果您将客户端上的 COM1 映射到服务器上的 COM3，请在 VDA 中安装您的 COM 端口设备应用程序，并在会话期间将其指向 COM3。像使用用户设备上的 COM 端口一样使用此映射的 COM 端口。

**重要提示：**

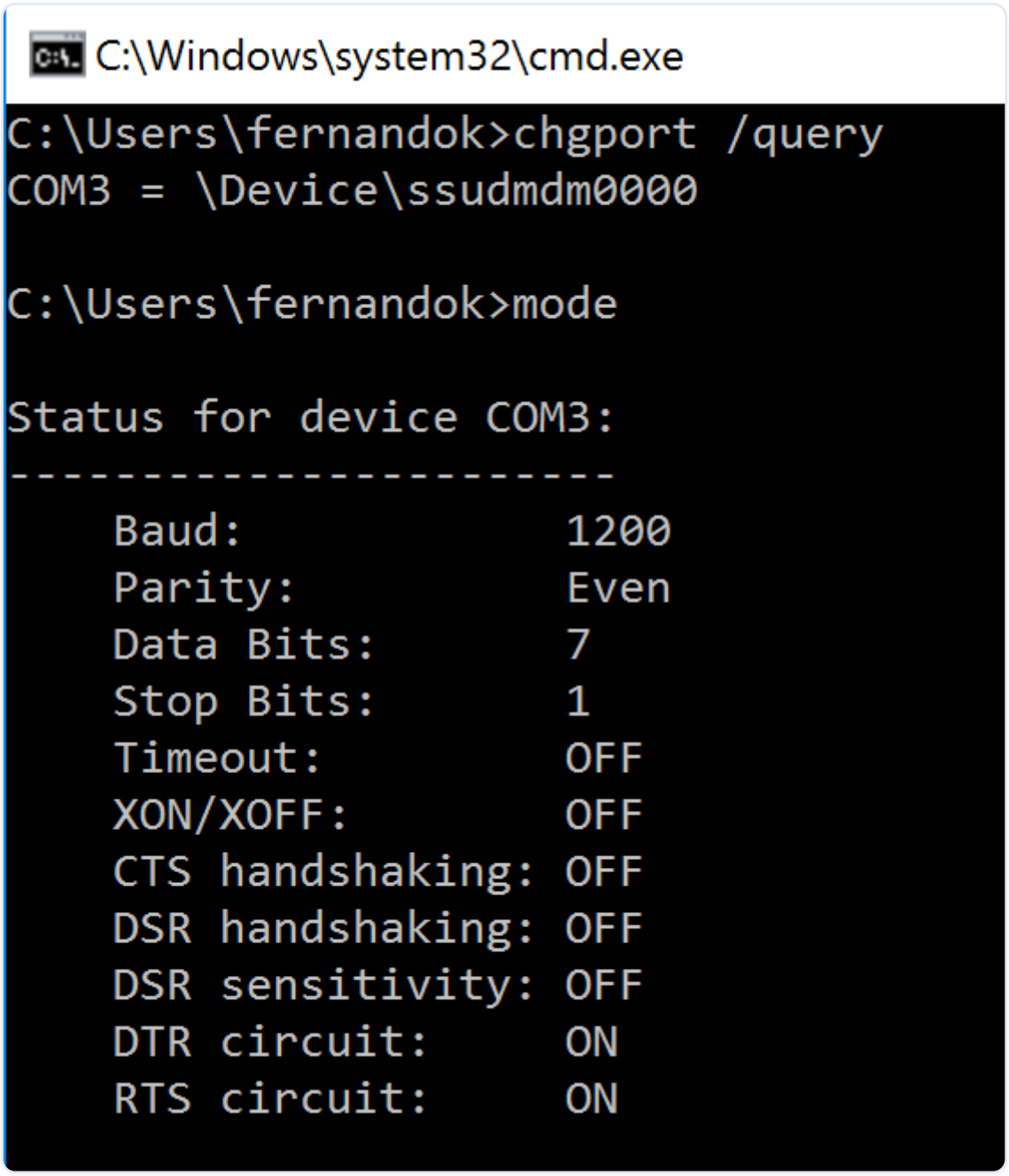
COM 端口映射与 TAPI 不兼容。您无法将 Windows 电话应用程序编程接口 (TAPI) 设备映射到客户端 COM 端口。TAPI 定义了一种标准方式，供应用程序控制数据、传真和语音呼叫的电话功能。TAPI 管理信令，包括拨号、接听和结束呼叫。此外，还包括保持、转接和电话会议等补充服务。

## 故障排除

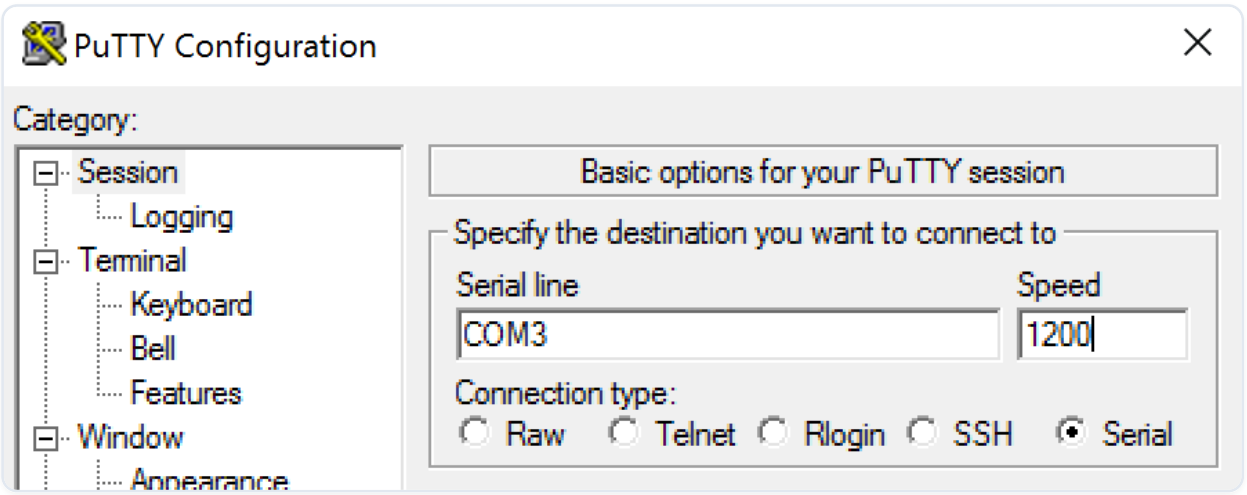
1. 确保您可以直接从端点访问设备，绕过 Citrix。当端口未映射到 VDA 时，您未连接到 Citrix 会话。请遵循设备随附的任何故障排除说明，并首先验证其在本地是否正常工作。 当设备连接到串行 COM 端口时，会在此处所示的配置单元上创建一个注册表项：




您还可以通过在命令提示符下运行 **chgport /query** 来查找此信息。




如果设备没有故障排除说明，请尝试打开 PuTTY 会话。选择**会话**，并在**串行线路**中指定您的 COM 端口。



您可以在本地命令窗口中运行 **MODE**。输出可能会显示正在使用的 COM 端口以及波特率/奇偶校验/数据位/停止位，这些信息是您在 PuTTY 会话中需要的。如果 PuTTY 连接成功，请按 **Enter** 键查看设备的反馈。您键入的任何字符都可能会在屏幕上重复显示或得到响应。如果此步骤不成功，则无法从虚拟会话访问设备。

2. 将本地 COM 端口映射到 VDA（使用策略或 **NET USE COMX: `\\CLIENT\COMZ`:**），然后重复上一步中的 PuTTY 过程，但这次是从 VDA PuTTY 执行。如果 PuTTY 未能显示错误 **Unable to open connection to COM1. Unable to open serial port**，则可能是另一个设备正在使用 COM1。
3. 运行 **chgport /query**。如果 VDA 上的内置 Windows 串行驱动程序将 \Device\Serial0 自动分配给 VDA 的 COM1 端口，请执行以下操作： A. 在 VDA 上打开 CMD 并键入 **NET USE.**

   B. 删除 VDA 上任何现有映射（例如 COM1）。

   **NET USE COM1 /DELETE**

   C. 将设备映射到 VDA。

   **NET USE COM1: `\\CLIENT\COM3`:**

   D. 将 VDA 上的应用程序指向 COM3。

   最后，尝试将本地 COM 端口（例如 COM3）映射到 VDA 上的另一个 COM 端口（COM1 除外，例如 COM3）。确保您的应用程序指向该端口： **NET USE COM3: `\\CLIENT\COM3`**
4. 如果现在您确实看到端口已映射，PuTTY 正在工作但没有数据传输，则可能是竞态条件。应用程序可能在端口映射之前连接并打开端口，从而阻止其被映射。请尝试以下方法之一：

   - 打开在同一服务器上发布的第二个应用程序。等待几秒钟，直到端口被映射，然后打开尝试使用该端口的实际应用程序。
   - 从 Active Directory 中的组策略编辑器而不是 Studio 启用 COM 端口重定向策略。这些策略是 **Client COM port redirection** 和 **Auto connect client COM ports**。以这种方式应用的策略可能会在 Studio 策略之前处理，从而确保 COM 端口已映射。Citrix 策略被推送到 VDA 并存储在： `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
   - 为用户使用此登录脚本，或者不发布应用程序，而是发布一个 .bat 脚本，该脚本首先删除 VDA 上的任何映射，重新映射虚拟 COM 端口，然后启动应用程序：

   @echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: `\\CLIENT\COM1`: NET USE COM2: `\\CLIENT\COM2`: MODE COM1: BAUD=1200 （或所需的任何值） MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 （或所需的任何值） START C:\Program Files\\\<Your Software Path>\\\<your_software.exe>

5. Sysinternals 的 Process Monitor 是最后的手段。在 VDA 上运行该工具时，查找并筛选 COM3、picaser.sys、CdmRedirector 等对象，尤其是 \<your_app\>.exe。任何错误都可能显示为 Access Denied 或类似内容。

# 专业键盘

## 彭博键盘

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

Citrix Virtual Apps and Desktops™ 支持 Bloomberg 型号 5、型号 4 Starboard 键盘（以及更早的型号 3）。此键盘使金融行业的客户能够利用键盘的特殊功能，快速访问金融市场数据并执行交易。

> **重要提示：**
>
> 建议您仅将 Bloomberg 键盘与一个会话配合使用。不建议将键盘与多个并发会话（一个客户端对应多个会话）配合使用。

Bloomberg 键盘是一种 USB 复合设备，在一个物理外壳中包含多个 USB 设备：

- 键盘。
- 指纹识别器。
- 带有用于增大和减小音量以及静音扬声器和麦克风的按键的音频设备。此设备包括板载扬声器、麦克风以及用于麦克风和耳机的插孔。
- 用于将所有这些设备连接到系统的 USB 集线器。

**要求：**

- Citrix Workspace™ app for Windows 连接到的会话必须支持 USB 设备。
- 最低需要 Citrix Workspace app 2207 for Linux 才能支持 Bloomberg 键盘型号 5。

- 最低需要 Citrix Workspace app 2109 for Windows 才能支持 Bloomberg 键盘型号 5。
- 最低需要 Citrix Workspace app 1808 for Windows 或 Citrix Receiver for Windows 4.8 才能支持 Bloomberg 键盘型号 3 和 4。
- 最低需要 Citrix Workspace app 1808 for Windows 或 Citrix Receiver for Windows 4.12 才能将型号 4 用于 KVM 模式（两根 USB 电缆，其中一根通过 KVM 路由）。

有关在 Citrix Workspace app for Windows 上配置 Bloomberg 键盘的信息，请参阅配置 Bloomberg 键盘。

要启用 Bloomberg 键盘支持，请参阅通过注册表管理的功能列表中的Bloomberg 键盘。

**验证支持：**

要确定 Citrix Workspace 应用程序中是否启用了 Bloomberg 键盘支持，请检查 Desktop Viewer 是否正确报告了 Bloomberg 键盘的设备。

桌面场景：

打开 Desktop Viewer。如果启用了 Bloomberg 键盘支持，Desktop Viewer 会在 USB 图标下显示三个设备：

对于 Bloomberg 5 键盘：

- Bloomberg LP Bloomberg 生物识别模块
- Bloomberg LP 键盘（具有两个接口的复合设备）
- Bloomberg LP 键盘音频（具有三个接口的复合设备）

对于 Bloomberg 3 和 4 键盘：

- Bloomberg 指纹扫描仪
- Bloomberg 键盘功能
- Bloomberg LP 键盘 2013

仅限无缝应用程序场景：

从 Citrix Workspace 应用程序通知区域图标打开“**连接中心**”菜单。如果启用了 Bloomberg 键盘支持，这三个设备将显示在“**设备**”菜单中。

这些设备旁边的复选标记表示它们已远程连接到会话。

# TWAIN 设备

## 要求

- 扫描仪必须兼容 TWAIN。
- 在本地设备上安装 TWAIN 驱动程序。服务器上不需要这些驱动程序。
- 在本地连接扫描仪（例如，通过 USB）。
- 确保扫描仪正在使用本地 TWAIN 驱动程序，而不是 Windows 图像采集服务。
- 确保用于测试的用户帐户未应用任何策略，并且该策略未限制 ICA® 会话中的带宽。例如，客户端 USB 重定向带宽限制。

有关策略设置的信息，请参阅 TWAIN devices policy settings。

# 网络摄像头

## 高清网络摄像头流式传输

网络摄像头可供在虚拟会话中运行的视频会议应用程序使用。服务器上的应用程序根据支持的格式类型选择网络摄像头格式和分辨率。会话启动时，客户端会将网络摄像头信息发送到服务器。从视频会议应用程序中选择一个网络摄像头。当网络摄像头和应用程序都支持高清渲染时，应用程序将使用高清分辨率。我们支持高达 1920x1080 的网络摄像头分辨率。

此功能需要 Citrix Receiver for Windows 4.10 或更高版本。有关支持 HDX 网络摄像头重定向的 Citrix Workspace 应用程序平台列表，请参阅 (/zh-cn/citrix-workspace-app/citrix-workspace-app-feature-matrix.html)。

有关高清网络摄像头流式传输的详细信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/multimedia/webcam-compression.html)。

您可以使用注册表项禁用和启用该功能，然后配置特定的分辨率。有关信息，请参阅注册表管理的功能列表中的 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/policies/reference/hdx-registry-settings.html)。

# WIA 设备

## 要求

- 扫描仪必须符合 WIA 标准。
- 在本地设备上安装 WIA 驱动程序。服务器上不需要这些驱动程序。

- 在本地连接扫描仪（例如，通过 USB）。
- 确保扫描仪使用的是本地 Windows 图像采集服务，而不是 TWAIN 驱动程序。
- 确保用于测试的用户帐户未应用任何策略，并且该策略未限制 ICA® 会话中的带宽。例如，客户端 USB 重定向带宽限制。

### Windows 图像采集应用程序允许列表

允许列表可让您控制 VDA 上的哪些应用程序可以访问 Windows 图像采集扫描仪重定向。注册表编辑器使用每个包含 Windows 图像采集的 VDA 上的允许列表设置的输入。默认情况下，没有应用程序可以访问 Windows 图像采集。

要调整 VDA 上应用程序的 Windows 图像采集，请参阅通过注册表管理的特性列表中的 Windows 图像采集应用程序允许列表 设置。

有关策略设置的信息，请参阅 WIA 设备策略设置。

# 图形

Citrix HDX 图形包含一套广泛的图形加速和编码技术，可优化 Citrix Virtual Apps and Desktops 中丰富图形应用程序的交付。这些图形技术在远程使用图形密集型虚拟应用程序时，提供与使用物理桌面相同的体验。

您可以使用软件或硬件进行图形渲染。软件渲染需要一个名为软件光栅化器的第三方库。例如，Windows 包含用于基于 DirectX 图形的 WARP 光栅化器。有时，您可能希望使用替代的软件渲染器。硬件渲染（硬件加速）需要图形处理器 (GPU)。

HDX™ Graphics 提供默认编码配置，该配置针对最常见的用例进行了优化。通过使用 Citrix 策略，IT 管理员还可以配置各种图形相关设置，以满足不同要求并提供所需的用户体验。

### 思睿

Thinwire 是 Citrix Virtual Apps and Desktops 中使用的 Citrix 默认显示远程处理技术。

显示远程处理技术允许将一台计算机上生成的图形（通常通过网络）传输到另一台计算机进行显示。图形是用户输入（例如，击键或鼠标操作）的结果。

### HDX 3D 专业版

Citrix Virtual Apps and Desktops 中的 HDX 3D Pro 功能使您能够交付使用图形处理单元 (GPU) 进行硬件加速时性能最佳的桌面和应用程序。这些应用程序包括基于 OpenGL 和 DirectX 的 3D 专业图形应用程序。标准 VDA 仅支持 DirectX 的 GPU 加速。

### 适用于 Windows 单会话操作系统的 GPU 加速

通过使用 HDX 3D Pro，您可以将图形密集型应用程序作为托管桌面或应用程序的一部分交付到单会话操作系统计算机上。HDX 3D Pro 支持物理主机计算机（包括桌面、刀片和机架工作站）以及 XenServer®、vSphere 和 Hyper-V（仅直通）管理程序提供的 GPU 直通和 GPU 虚拟化技术。

使用 GPU 直通，您可以创建对专用图形处理硬件具有独占访问权限的 VM。您可以在管理程序上安装多个 GPU，并以一对一的方式将 VM 分配给每个 GPU。

使用 GPU 虚拟化，多个虚拟机可以直接访问单个物理 GPU 的图形处理能力。

### 适用于 Windows 多会话操作系统的 GPU 加速

HDX 3D Pro 允许在 Windows 多会话操作系统会话中运行的图形密集型应用程序在服务器图形处理单元 (GPU) 上进行渲染。通过将 OpenGL、DirectX、Direct3D 和 Windows Presentation Foundation (WPF) 渲染转移到服务器 GPU，图形渲染不会减慢服务器 CPU 的速度。此外，由于工作负载在 CPU 和 GPU 之间分配，服务器能够处理更多的图形。

### 弗雷姆霍克

> **重要提示：**
>
> 自 Citrix Virtual Apps and Desktops 7 1903 起，Framehawk 不再受支持。请改用启用(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/technical-overview/hdx/adaptive-transport.html)的 Thinwire。
>
> Framehawk 是一种显示远程处理技术，适用于通过宽带无线连接（Wi-Fi 和 4G/LTE 蜂窝网络）工作的移动员工。Framehawk 克服了频谱干扰和多径传播的挑战，为虚拟应用程序和桌面的用户提供了流畅且交互式的用户体验。

### 基于文本的会话水印

基于文本的会话水印有助于阻止和跟踪数据盗窃。此可追溯信息显示在会话桌面上，以阻止那些使用照片和屏幕截图窃取数据的人。您可以指定一个文本层水印。水印可以显示在整个会话屏幕上，而不会更改原始文档的内容。基于文本的会话水印需要 VDA 支持。

## 相关信息

- HDX 三维专业版
- 适用于 Windows 单会话操作系统的 GPU 加速
- 适用于 Windows 多会话操作系统的 GPU 加速
- 弗雷姆霍克
- 瘦线
- 基于文本的会话水印

## HDX™ 3D 专业版

Citrix Virtual Apps and Desktops™ 的 HDX 3D Pro 功能使您能够交付使用图形处理单元 (GPU) 进行硬件加速时性能最佳的桌面和应用程序。这些应用程序包括基于 OpenGL 和 DirectX 的 3D 专业图形应用程序。标准 VDA 仅支持 DirectX 的 GPU 加速。

有关 HDX 3D Pro 策略设置，请参阅 优化 3D 图形工作负载。

所有受支持的 Citrix Workspace 应用程序都可以与 3D 图形配合使用。为了在复杂的 3D 工作负载、高分辨率显示器、多显示器配置和高帧率应用程序中获得最佳性能，我们建议使用最新版本的适用于 Windows 的 Citrix Workspace 应用程序和适用于 Linux 的 Citrix Workspace 应用程序。有关 Citrix Workspace 应用程序支持的版本的更多信息，请参阅 Citrix Workspace 应用程序的生命周期里程碑。

3D 专业应用程序的示例包括：

- 计算机辅助设计、制造和工程 (CAD/CAM/CAE) 应用程序
- 地理信息系统 (GIS) 软件
- 用于医学成像的图片归档和通信系统 (PACS)
- 使用最新 OpenGL、DirectX、NVIDIA CUDA、OpenCL 和 WebGL 版本的应用程序
- 使用 NVIDIA 计算统一设备架构 (CUDA) GPU 进行并行计算的计算密集型非图形应用程序

HDX 3D Pro 在任何带宽下都能提供最佳用户体验：

- 在 WAN 连接上：通过带宽低至 1.5 Mbps 的 WAN 连接提供交互式用户体验。
- 在 LAN 连接上：在 LAN 连接上提供与本地桌面相当的用户体验。

  您可以通过将图形处理移至数据中心进行集中管理，从而用更简单的用户设备取代复杂且昂贵的工作站。

HDX 3D Pro 为 Windows 单会话操作系统计算机和 Windows 多会话操作系统计算机提供 GPU 加速。有关详细信息，请参阅 适用于 Windows 单会话操作系统的 GPU 加速 和 适用于 Windows 多会话操作系统的 GPU 加速。

除了裸机之外，HDX 3D Pro 还与以下管理程序提供的 GPU 直通和 GPU 虚拟化技术兼容：

- 思杰虚拟机管理程序™
  - NVIDIA GRID、AMD 和 Intel GVT-d 的 GPU 直通
  - NVIDIA GRID、AMD 和 Intel GVT-g 的 GPU 虚拟化
  - 有关硬件兼容性，请参阅管理程序硬件兼容性列表。

使用 HDX Monitor 工具验证 HDX 可视化技术的运行和配置，并诊断和解决 HDX 问题。要下载该工具并了解更多信息，请参阅 `<https://taas.citrix.com/hdx/download/>`。

# Windows 多会话操作系统的 GPU 加速

HDX™ 3D Pro 允许在 Windows 多会话操作系统会话中运行的图形密集型应用程序在服务器的图形处理单元 (GPU) 上进行渲染。通过将 OpenGL、DirectX、Direct3D 和 Windows Presentation Foundation (WPF) 渲染转移到服务器的 GPU，图形渲染不会降低服务器 CPU 的速度。此外，由于工作负载在 CPU 和 GPU 之间分配，服务器能够处理更多的图形。

由于 Windows Server 是一个多用户操作系统，多个用户可以共享 Citrix Virtual Apps™ 访问的 GPU，而无需 GPU 虚拟化 (vGPU)。

对于涉及编辑注册表的过程，请务必小心：不正确地编辑注册表可能会导致严重问题，甚至可能需要重新安装操作系统。Citrix® 无法保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。在编辑注册表之前，请务必备份注册表。

## GPU 共享

GPU 共享可在远程桌面会话中实现 OpenGL 和 DirectX 应用程序的 GPU 硬件渲染。它具有以下特点：

- 可用于裸机或虚拟机，以提高应用程序的可伸缩性和性能。
- 允许多个并发会话共享 GPU 资源（大多数用户不需要专用 GPU 的渲染性能）。
- 无需特殊设置。

根据管理程序和 GPU 供应商的要求，可以将 GPU 以完全直通或虚拟 GPU (vGPU) 模式分配给 Windows Server 虚拟机。还支持在物理 Windows Server 机器上进行裸机部署。

GPU 共享不依赖于任何特定的显卡。

- 对于虚拟机，请选择与所用管理程序兼容的显卡。有关 Citrix Hypervisor 硬件兼容性列表，请参阅管理程序硬件兼容性列表。
- 在裸机上运行时，建议操作系统只启用一个显示适配器。如果硬件上安装了多个 GPU，请使用设备管理器禁用除一个之外的所有 GPU。

使用 GPU 共享的可伸缩性取决于几个因素：

- 正在运行的应用程序
- 它们消耗的显存量
- 显卡的图形处理能力

有些应用程序比其他应用程序更能很好地处理显存不足的情况。如果硬件过载，可能会导致显卡驱动程序不稳定或崩溃。限制并发用户数以避免此类问题。

要确认正在进行 GPU 加速，请使用第三方工具（例如 GPU-Z）。GPU-Z 可在 `<http://www.techpowerup.com/gpuz/>` 获取。

- 访问适用于 NVIDIA GPU 和 Intel Iris Pro 图形处理器的高性能视频编码器。策略设置（默认启用）控制此功能，并允许对 H.264 编码使用硬件编码（如果可用）。如果此类硬件不可用，VDA 将回退到使用软件视频编解码器进行基于 CPU 的编码。有关详细信息，请参阅图形策略设置。

### DirectX、Direct3D 和 WPF 渲染

DirectX、Direct3D 和 WPF 渲染仅适用于支持显示驱动程序接口 (DDI) 版本 9ex、10 或 11 的 GPU 的服务器。

- 在 Windows Server 2008 R2 上，DirectX 和 Direct3D 无需特殊设置即可使用单个 GPU。
- 在 Windows Server 2012 及更高版本上，RD 会话主机服务器上的远程桌面服务 (RDS) 会话使用 Microsoft 基本渲染驱动程序作为默认适配器。要在 Windows Server 2012 及更高版本上的 RDS 会话中使用 GPU，请在组策略 **本地计算机策略** \> **计算机配置** \> **管理模板** \> **Windows 组件** \> **远程桌面服务** \> **远程桌面会话主机** \> **远程会话环境** 中启用**将硬件默认图形适配器用于所有远程桌面服务会话**设置。
- 要使 WPF 应用程序能够使用服务器的 GPU 进行渲染，请在运行 Windows 多会话操作系统会话的服务器注册表中创建设置。有关注册表设置的信息，请参阅注册表管理的功能列表中的 Windows Presentation Foundation (WPF) 渲染。

### 适用于 CUDA 或 OpenCL 应用程序的 GPU 加速

在用户会话中运行的 CUDA 和 OpenCL 应用程序的 GPU 加速默认情况下处于禁用状态。

要使用 CUDA 加速 POC 功能，请启用注册表设置。有关信息，请参阅注册表管理的功能列表中的适用于 CUDA 或 OpenCL 应用程序的 GPU 加速。

## 适用于 Windows 单会话操作系统的 GPU 加速

借助 HDX 3D Pro，您可以将图形密集型应用程序作为托管桌面或应用程序的一部分交付到单会话操作系统计算机。HDX 3D Pro 支持物理主机计算机（包括桌面、刀片和机架工作站）以及 Citrix Hypervisor™、vSphere、Nutanix 和 Hyper-V（仅直通）管理程序提供的 GPU 直通和 GPU 虚拟化技术。

HDX™ 3D Pro 提供以下功能：

- 基于 H.264 或 H.265 的自适应深度压缩，可实现最佳 WAN 和无线性能。HDX 3D Pro 使用基于 CPU 的全屏 H.264 压缩作为默认编码压缩技术。支持 NVENC 的 NVIDIA、Intel 和 AMD 显卡使用 H.264 硬件编码。支持 NVENC 的 NVIDIA 显卡使用 H.265 硬件编码。

- 适用于特殊用例的无损压缩选项。HDX 3D Pro 还提供基于 CPU 的无损编解码器，以支持需要像素级完美图形的应用程序，例如医学成像。仅建议在特殊用例中使用真正的无损压缩，因为它会消耗更多网络和处理资源。

  使用无损压缩时：

  - 无损指示器（一个通知区域图标）会通知用户显示的屏幕是有损帧还是无损帧。当**视觉质量**策略设置指定**构建为无损**时，此图标会提供帮助。当发送的帧为无损时，无损指示器会变为绿色。
  - 无损开关使用户能够在会话内随时切换到“始终无损”模式。要在会话内随时选择或取消选择**无损**，请右键单击图标，然后单击**切换到像素完美**，或使用快捷方式 ALT+SHIFT+1。

    对于无损压缩：无论通过策略选择何种编解码器，HDX 3D Pro 都使用无损编解码器进行压缩。

    对于有损压缩：HDX 3D Pro 使用原始编解码器，无论是默认编解码器还是通过策略选择的编解码器。

    无损开关设置不会保留到后续会话。要为每个连接使用无损编解码器，请在**视觉质量**策略设置中选择**始终无损**。

- 您可以覆盖默认快捷方式 ALT+SHIFT+1，以在会话内选择或取消选择无损。在 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator` 配置新的注册表设置。
  - 名称: HKEY_LOCAL_MACHINE_HotKey, 类型: String
  - 配置快捷方式组合的格式为 C=0 | 1, A=0 | 1, S=0 | 1, W=0 | 1, K=val。键必须用逗号“,”分隔。键的顺序无关紧要。
  - A、C、S、W 和 K 是键，其中 C=Control，A=ALT，S=SHIFT，W=Win，K=有效键。K 的允许值为 0–9、a–z 和任何虚拟键代码。
  - 例如：
    - 对于 F10，设置 K=0x79
    - 对于 Ctrl + F10，设置 C=1, K=0x79
    - 对于 Alt + A，设置 A=1, K=a 或 A=1, K=A 或 K=A, A=1
    - 对于 Ctrl + Alt + 5，设置 C=1, A=1, K=5 或 A=1, K=5, C=1
    - 对于 Ctrl + Shift + F5，设置 A=1, S=1, K=0x74

**注意：**

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

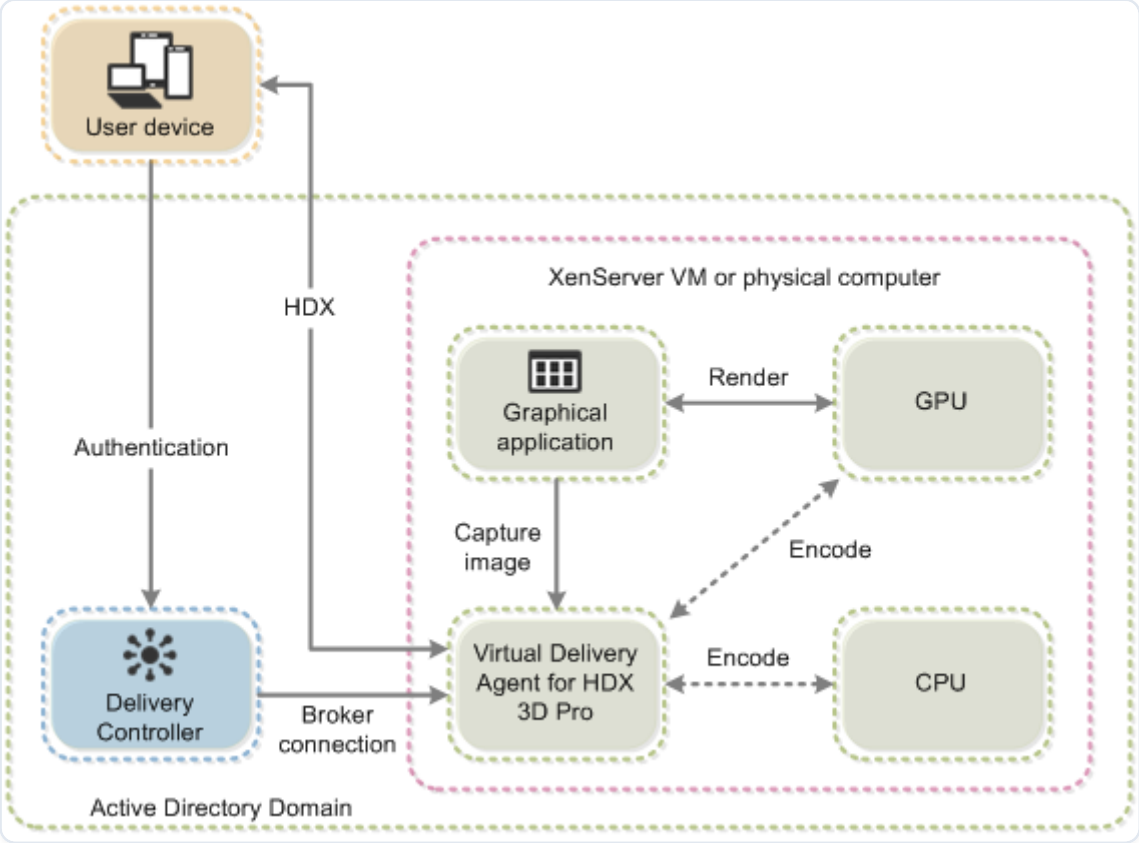
- 多显示器和高分辨率显示器支持。对于单会话操作系统计算机，HDX 3D Pro 支持最多连接四个显示器的用户设备。用户可以按任意配置排列显示器，并且可以混合使用不同分辨率和方向的显示器。显示器数量受限于主机 GPU、用户设备的功能以及可用带宽。HDX 3D Pro 支持所有显示器分辨率，并且仅受限于主机 GPU 的功能。
- 动态分辨率。您可以将虚拟桌面或应用程序窗口调整为任意分辨率。**注意**：更改分辨率的唯一受支持方法是调整 VDA 会话窗口的大小。不支持在 VDA 会话中更改分辨率（使用**控制面板 > 外观**和**个性化 > 显示 > 屏幕分辨率**）。
- 支持 NVIDIA vGPU 架构。HDX 3D Pro 支持 NVIDIA vGPU 卡。有关信息，请参阅 NVIDIA vGPU，了解 GPU 直通和 GPU 共享。NVIDIA vGPU 允许多个 VM 同时直接访问单个物理 GPU，使用与部署在非虚拟化操作系统上的 NVIDIA 图形驱动程序相同的驱动程序。
- 支持使用虚拟直接图形加速 (vDGA) 的 VMware vSphere 和 VMware ESX - 您可以将 HDX 3D Pro 与 vDGA 结合使用，以处理 RDS 和 VDI 工作负载。
- 支持使用 NVIDIA vGPU 和 AMD MxGPU 的 VMware vSphere/ESX。
- 支持在 Windows Server 2016 中使用离散设备分配的 Microsoft HyperV。
- 支持采用 Intel Xeon Processor E3 系列的数据中心图形。HDX 3D Pro 支持多显示器（最多 3 个）、控制台消隐、自定义分辨率以及支持的 Intel 处理器系列的高帧率。有关详细信息，请参阅 `<http://www.citrix.com/intel>` 和 `<http://www.intel.com/content/www/us/en/servers/data-center-graphics.html>`。
- 支持 AMD FirePro S 系列服务器卡上的 AMD RapidFire。HDX 3D Pro 支持多显示器（最多 6 个）、控制台消隐、自定义分辨率和高帧率。注意：HDX 3D Pro 对 AMD MxGPU（GPU 虚拟化）的支持仅适用于 VMware vSphere vGPU。Citrix Hypervisor 和 Hyper-V 支持 GPU 直通。有关详细信息，请参阅 AMD 虚拟化解决方案。
- 访问适用于 NVIDIA GPU、AMD GPU 和 Intel Iris Pro 图形处理器的高性能视频编码器。策略设置（默认启用）控制此功能。此功能允许对 H.264 编码使用硬件编码（如果可用）。如果此类硬件不可用，VDA 将回退到使用软件视频编解码器进行基于 CPU 的编码。有关详细信息，请参阅 图形策略设置。

如下图所示：

- 当用户登录到 Citrix Workspace™ 应用程序并访问虚拟应用程序或桌面时，Controller 会对用户进行身份验证。然后，Controller 会联系适用于 HDX 3D Pro 的 VDA，以代理连接到托管图形应用程序的计算机。

适用于 HDX 3D Pro 的 VDA 使用主机上相应的硬件来压缩整个桌面或仅图形应用程序的视图。

- 桌面或应用程序视图以及用户与它们的交互在主机和用户设备之间传输。此传输通过 Citrix Workspace 应用程序与适用于 HDX 3D Pro 的 VDA 之间的直接 HDX 连接完成。




### 优化 HDX 3D Pro 用户体验

当多个用户共享带宽有限的连接（例如，在分支机构）时，建议使用“**会话总带宽限制**”策略设置来限制每个用户可用的带宽。使用此设置可确保可用带宽不会随着用户的登录和注销而大幅波动。由于 HDX 3D Pro 会自动调整以使用所有可用带宽，因此用户会话期间可用带宽的巨大变化可能会对性能产生负面影响。

例如，如果 20 个用户共享 60 Mbps 连接，则每个用户可用的带宽可能在 3 Mbps 到 60 Mbps 之间变化，具体取决于并发用户数。为了在此场景中优化用户体验，请确定高峰期每个用户所需的带宽，并始终将用户限制在此数量。

对于 3D 鼠标用户，建议将通用 USB 重定向虚拟通道的优先级提高到 0。有关更改虚拟通道优先级的详细信息，请参阅知识中心文章 CTX128190。

## 弗雷姆霍克

> **重要提示：**

> 自 Citrix Virtual Apps and Desktops 7 1903 起，Framehawk 不再受支持。请改用启用自适应传输的 Thinwire。

> Framehawk 是一种专门的显示远程处理技术，适用于在易受高数据包丢失影响的宽带无线连接（Wi-Fi 和 4G/LTE 蜂窝网络）上工作的移动办公人员。Framehawk 克服了频谱干扰和多径传播的挑战。Framehawk 为在 Windows 和 iOS 移动设备（如笔记本电脑和平板电脑）上使用虚拟应用和桌面的用户提供流畅且交互式的用户体验。为了最大限度地提高服务器可伸缩性并最大限度地减少网络带宽消耗，我们建议仅在上述特定用例中使用 Framehawk。对于所有其他用例，我们建议使用自适应传输，它融合了许多 Framehawk 概念以最大限度地提高数据吞吐量。

您可以使用 Citrix® 策略模板，以适合您组织的方式为一组用户和访问场景实施 Framehawk。Framehawk 针对单屏移动用例，例如笔记本电脑和平板电脑。在实时交互性能的业务价值能够证明服务器资源额外成本和宽带连接要求合理的情况下，请使用 Framehawk。

## Framehawk 如何保持流畅的用户体验

可以将 Framehawk 视为人眼的软件实现，它查看帧缓冲区中的内容并识别屏幕上不同类型的内容。对用户而言，什么最重要？当屏幕区域快速变化时，例如视频或移动图形，即使丢失一些像素，人眼也无所谓。这些区域会很快被新数据覆盖。

但是，当涉及到屏幕的静态区域时，人眼会很挑剔。例如，通知区域或工具栏中的图标，或者滚动到用户想要开始阅读的位置后的文本。用户希望这些区域像素完美。与旨在从**二进制**角度实现技术准确性的协议不同，Framehawk 旨在与使用该技术的人相关。

Framehawk 包含下一代服务质量信号放大器以及基于时间的热图，用于更精细、更高效地识别工作负载。除了数据压缩之外，它还使用自主、自修复转换，并避免数据重传，以保持点击响应、线性度和一致的节奏。在有损网络连接上，Framehawk 可以通过插值隐藏丢失，用户仍然可以感知到良好的图像质量，同时享受更流畅的体验。此外，Framehawk 算法能够智能地区分不同类型的数据包丢失。例如，随机丢失（发送更多数据以补偿）与拥塞丢失（不发送更多数据，因为通道已堵塞）。

Citrix Workspace™ 应用程序中的 Framehawk 意图引擎可区分向上或向下滚动、缩放、向左或向右移动、阅读、打字以及其他常见操作。该引擎还使用共享字典管理与虚拟投递代理 (VDA) 的通信。如果用户正在尝试阅读，则文本的视觉质量必须非常出色。如果用户正在滚动，则必须快速流畅。并且它必须是可中断的，以便用户始终能够控制与应用程序或桌面的交互。

通过测量网络连接上的节奏（**传动**，类似于自行车链条上的张力），Framehawk 逻辑反应更快，在高延迟连接上提供卓越的体验。这种独特且获得专利的传动系统提供持续更新的网络状况反馈，使 Framehawk 能够立即对带宽、延迟和丢失的变化做出反应。

## 使用 Thinwire 和 Framehawk 的设计注意事项

Framehawk 使用建立在用户数据报协议 (UDP) 之上的数据传输层。UDP 只是 Framehawk 如何克服有损性的一小部分，您可以通过将 Framehawk 的性能与其他基于 UDP 的协议进行比较来看到这一点。UDP 为使 Framehawk 脱颖而出的人性化技术提供了重要基础。

Framehawk 需要多少带宽？

宽带无线的含义取决于几个因素，包括有多少用户共享连接、连接质量以及正在使用的应用程序。为了获得最佳性能，Citrix 建议基础带宽为 4 Mbps 或 5 Mbps，外加每并发用户约 150 Kbps。

我们对 Thinwire 的带宽建议通常是基础带宽 1.5 Mbps，外加每用户 150 Kbps。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 带宽博客）。在 3% 的数据包丢失率下，您会发现基于 TCP 的 Thinwire 需要比 Framehawk 更多的带宽才能保持良好的用户体验。

Thinwire 仍然是 ICA® 协议中的主要显示远程处理通道。Framehawk 默认处于禁用状态。Citrix 建议有选择地启用它，以解决您组织中的宽带无线访问场景。请记住，Framehawk 比 Thinwire 需要更多的服务器资源（CPU 和内存）。

## 要求和注意事项

Framehawk 需要最低 VDA 7.6.300 和组策略管理 7.6.300。

端点必须至少具有适用于 Windows 1808 的 Workspace 应用程序、适用于 Windows 4.3.100 的 Citrix Receiver、适用于 iOS 1808 的 Workspace 应用程序或适用于 iOS 6.0.1 的 Citrix Receiver。

默认情况下，Framehawk 使用双向用户数据报协议 (UDP) 端口范围（3224 到 3324）与 Citrix Workspace 应用程序交换 Framehawk 显示通道数据。可以在名为“**Framehawk 显示通道端口范围**”的策略设置中自定义该范围。客户端与虚拟桌面之间的每个并发连接都需要一个唯一的端口。对于多用户操作系统环境（例如 Citrix Virtual Apps™ 服务器），请定义足够的端口以支持最大数量的并发用户会话。对于单用户操作系统（例如 VDI 桌面），定义单个 UDP 端口就足够了。Framehawk 尝试使用第一个定义的端口，直到范围中指定的最后一个端口。这适用于通过 Citrix Gateway 的情况，以及直接连接到 StoreFront 服务器的内部连接。

对于远程访问，必须部署 Citrix Gateway。默认情况下，Citrix Gateway 使用 UDP 端口 443 在客户端 Citrix Workspace 应用程序和网关之间进行加密通信。必须在任何外部防火墙上打开此端口，以允许双向安全通信。此功能称为数据报传输层安全性 (DTLS)。

> **注意：**

> FIPS 设备不支持 Framehawk/DTLS 连接。

> 从 NetScaler Gateway 11.0.62 版和 NetScaler Unified Gateway 11.0.64.34 版或更高版本开始，支持加密的 Framehawk 连接。

从 XenApp 和 XenDesktop 7.12 开始支持 NetScaler 高可用性。

在实施 Framehawk 之前，请考虑以下建议：

- 请联系您的安全管理员，确认为 Framehawk 定义的 UDP 端口已在防火墙上打开。安装过程不会自动配置防火墙。
- 通常，Citrix Gateway 可能安装在 DMZ 中，外部和内部两侧都有防火墙。确保外部防火墙上打开了 UDP 端口 443。如果环境使用默认端口范围，请确保内部防火墙上打开了 UDP 端口 3224 到 3324。

## 配置

> **注意：**

> Citrix 建议您仅为可能遇到高数据包丢失的用户启用 Framehawk。我们还建议您不要将 Framehawk 作为站点中所有对象的通用策略启用。

> Framehawk 默认处于禁用状态。启用后，服务器会尝试将 Framehawk 用于用户图形和输入。如果由于任何原因未满足先决条件，则使用默认模式 (Thinwire) 建立连接。

以下策略设置会影响 Framehawk：

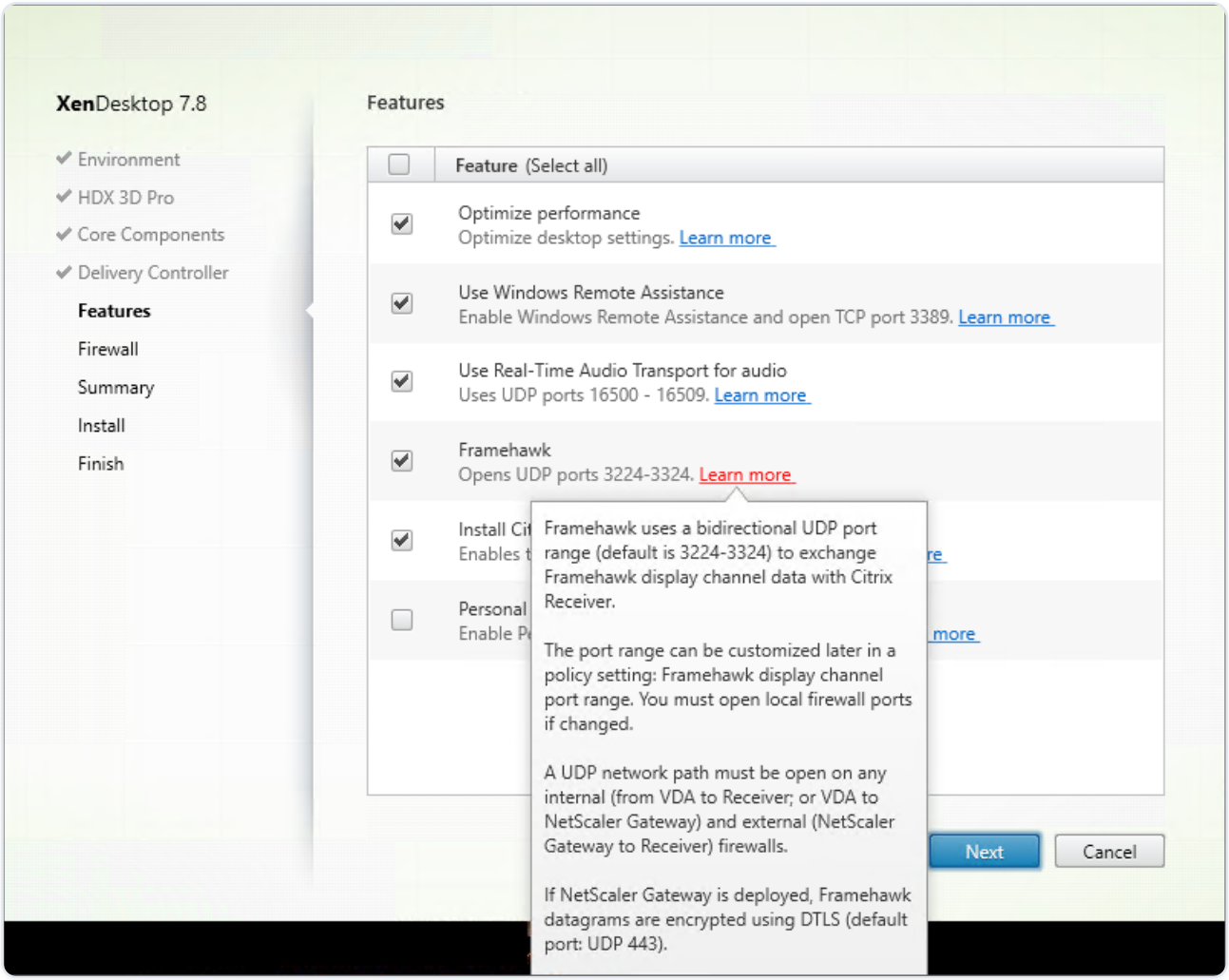
- Framehawk 显示通道: 启用或禁用此功能。
- Framehawk 显示通道端口范围: 指定 VDA 用于与用户设备交换 Framehawk 显示通道数据的 UDP 端口号范围（从最低端口号到最高端口号）。VDA 会尝试使用每个端口，从最低端口号开始，每次尝试递增。该端口处理入站和出站流量。

## 为 Framehawk 显示通道打开端口

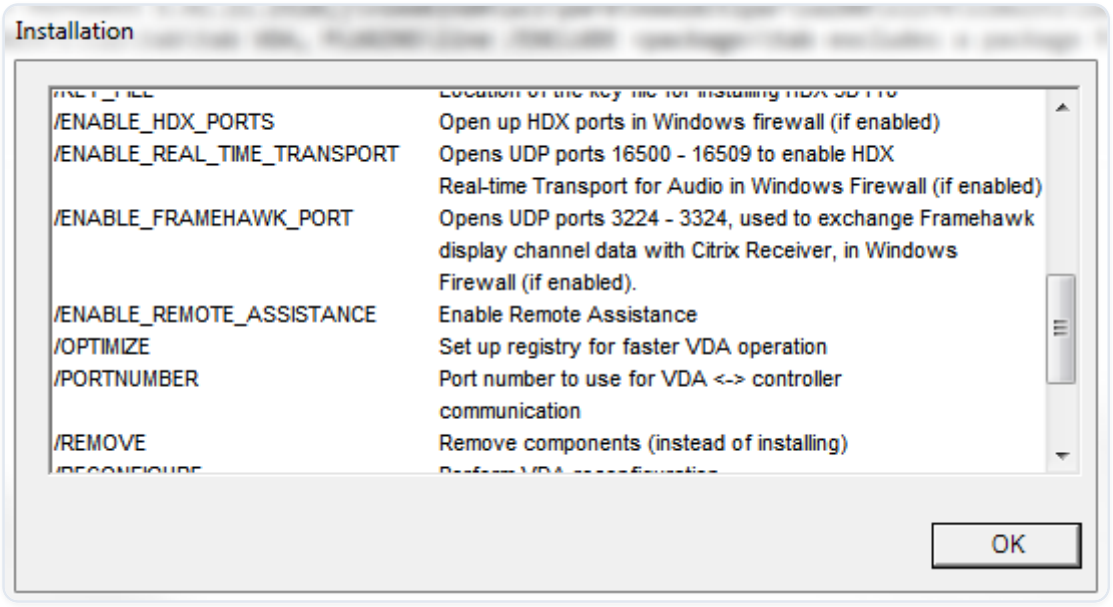
从 XenApp and XenDesktop 7.8 开始，VDA 安装程序的**功能**步骤中提供了一个选项，用于重新配置防火墙。如果选中此复选框，则会在 Windows 防火墙上打开 UDP 端口 3224 到 3324。在某些情况下需要手动配置防火墙：

- 对于任何网络防火墙。 或者
- 默认端口范围已自定义。

要打开这些 UDP 端口，请选中 **Framehawk** 复选框：

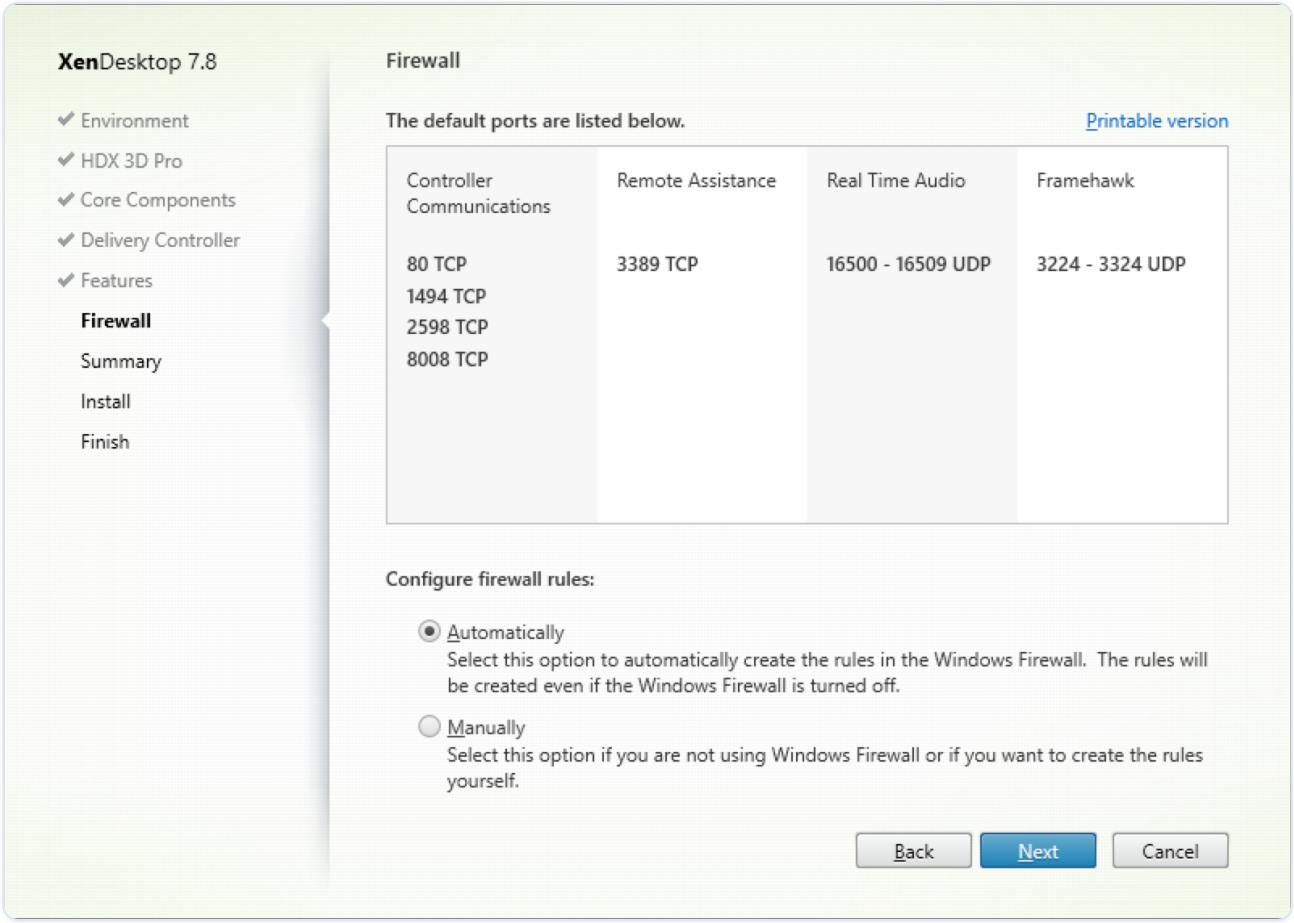



您还可以使用命令行通过 **/ENABLE_FRAMEHAWK_PORT** 为 Framehawk 打开 UDP 端口：

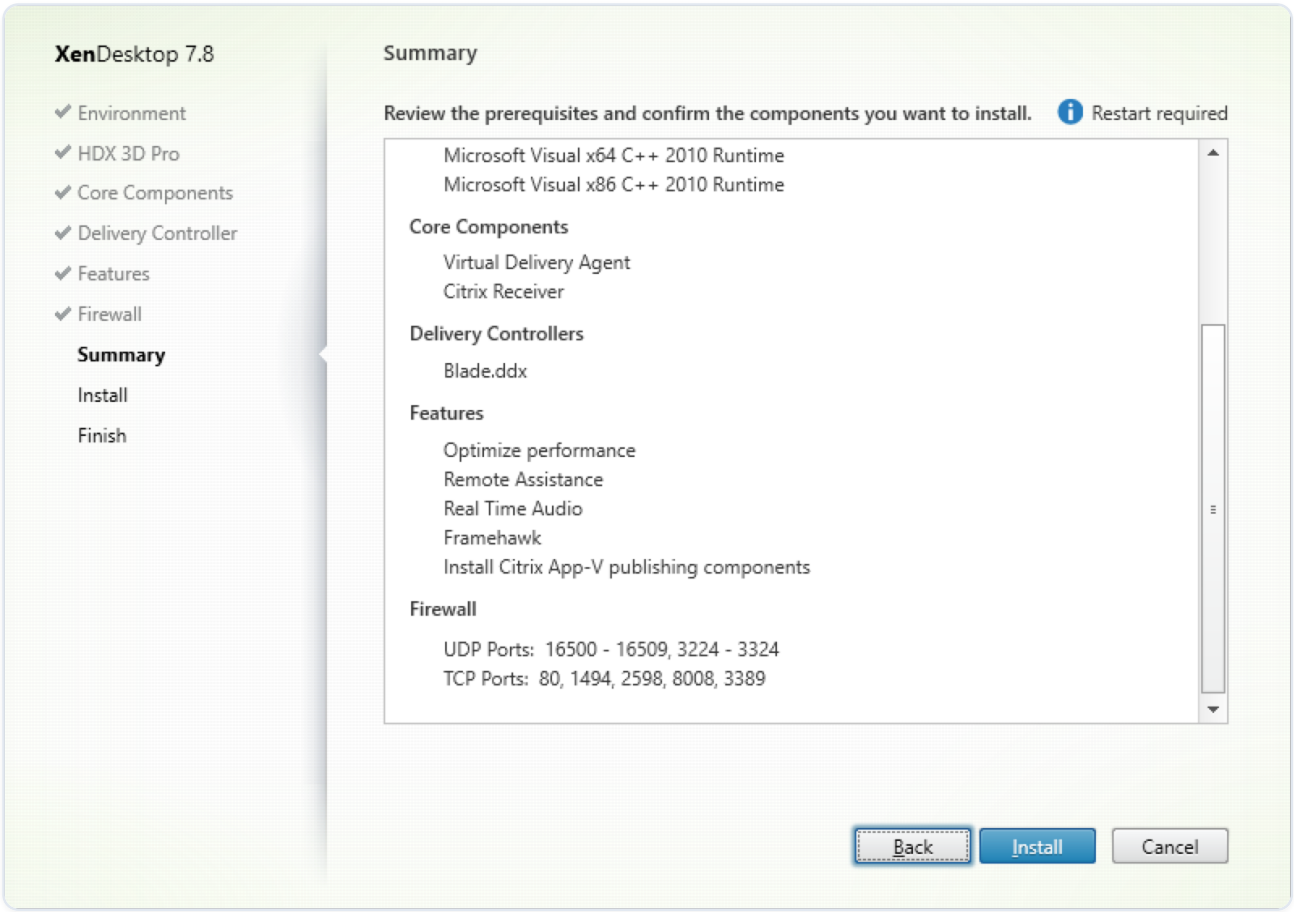



## 验证 Framehawk UDP 端口分配

在安装过程中，您可以在**防火墙**屏幕中验证分配给 Framehawk 的 UDP 端口：




**摘要**屏幕指示 Framehawk 功能是否已启用：




## Citrix Gateway 对 Framehawk 的支持

Citrix Gateway 1808 或更高版本、NetScaler Gateway 11.0.62.10 或更高版本以及 Citrix Unified Gateway 1808 和 NetScaler Unified Gateway 11.0.64.34 或更高版本支持加密的 Framehawk 流量。

- Citrix Gateway 指的是部署架构，其中 Gateway VPN 虚拟服务器可从最终用户设备直接访问。也就是说，VPN 虚拟服务器分配有公共 IP 地址，用户直接连接到此 IP 地址。
- 带 Unified Gateway 的 Citrix Gateway 指的是部署架构，其中 Gateway VPN 虚拟服务器作为目标绑定到内容交换虚拟服务器 (CS)。在此部署中，CS 虚拟服务器具有公共 Internet 协议地址，而 Gateway VPN 虚拟服务器具有虚拟 Internet 协议地址。

要在 Citrix Gateway 上启用 Framehawk 支持，必须在 Gateway VPN 虚拟服务器级别启用 DTLS 参数。启用该参数并正确更新 Citrix Virtual Apps 或 Citrix Virtual Desktops™ 上的组件后，Framehawk 音频、视频和交互式流量将在 Gateway VPN 虚拟服务器和用户设备之间加密。

Framehawk 支持 Citrix Gateway、Unified Gateway 和 Citrix Gateway + 全局服务器负载平衡。

Framehawk 不支持以下方案：

- HDX™ 洞察

- Citrix Gateway 的 IPv6 模式
- Citrix 网关双跳
- 采用群集设置的 Citrix Gateway

| 方案 | FRAMEHAWK 支持 |
| --- | --- |
| 思杰网关 | 是 |
| Citrix Gateway + 全局服务器负载平衡 | 是 |
| 带统一网关的思杰网关 | 是。**注意：**支持 Unified Gateway 11.0.64.34 及更高版本。 |
| HDX 洞察 | 否 |
| Citrix Gateway 的 IPv6 模式 | 否 |
| Citrix 网关双跳 | 否 |
| Citrix Gateway 上的多个安全票证颁发机构 | 是 |
| Citrix Gateway 和高可用性 | 是 |
| Citrix Gateway 和群集设置 | 否 |

## 配置 Citrix Gateway 以支持 Framehawk

要在 Citrix Gateway 上启用 Framehawk 支持，请在 Gateway VPN *虚拟服务器*级别启用 DTLS 参数。参数启用后，并且 Citrix Virtual Apps and Desktops™ 上的组件已正确更新，Framehawk 音频、视频和交互式流量将在 Gateway VPN 虚拟服务器和用户设备之间加密。

如果您正在 Citrix Gateway 上为远程访问启用 UDP 加密，则需要此配置。

配置 Citrix Gateway 以支持 Framehawk 时：

- 确保任何外部防火墙上都打开了 UDP 端口 443
- 确保任何外部防火墙上都打开了 CGP 端口（默认 2598）
- 在 VPN 虚拟服务器的设置中启用 DTLS
- 解绑并重新绑定 SSL 证书-密钥对。如果您使用的是 Citrix Gateway 1808 或更高版本，或者 NetScaler 11.0.64.34 或更高版本，则不需要此步骤。

要配置 Citrix Gateway 以支持 Framehawk：

1. 部署和配置 Citrix Gateway 以与 StoreFront™ 通信并对 Citrix Virtual Apps and Desktops 的用户进行身份验证。
2. 在 Citrix Gateway 配置选项卡中，展开 Citrix Gateway，然后选择 **Virtual Servers**。
3. 选择 **Edit** 以显示 VPN 虚拟服务器的基本设置；验证 DTLS 设置的状态。
4. 选择 **More** 以显示更多配置选项：
5. 选择 **DTLS** 以提供数据报协议（例如 Framehawk）的通信安全。单击 **OK**。VPN 虚拟服务器的基本设置区域显示 DTLS 标志设置为 **True**。
6. 重新打开“服务器证书绑定”屏幕，然后单击 **+** 以绑定证书密钥对。
7. 选择之前使用的证书密钥对，然后单击 **Select**。
8. 保存对服务器证书绑定的更改。
9. 保存后，将显示证书密钥对。单击 **Bind**。
10. 如果出现 **No usable ciphers configured on the SSL vserver/service** 警告消息，请忽略它。

### 适用于旧版 NetScaler® Gateway 的步骤

如果您使用的是早于 11.0.64.34 版本的 NetScaler Gateway：

1. 重新打开“服务器证书绑定”屏幕，然后单击 + 以绑定证书密钥对。
2. 选择之前使用的证书密钥对，然后单击 **Select**。
3. 保存对服务器证书绑定的更改。
4. 保存后，证书密钥对出现。点击**绑定**。
5. 如果出现“**SSL vserver/service 上未配置可用密码**”警告消息，请忽略。

要为 Framehawk 支持配置 Unified Gateway：

1. 确保 Unified Gateway 已安装并正确配置。有关其他信息，请参阅 Citrix 产品文档站点上的 Unified Gateway 信息。
2. 在 VPN *虚拟服务器*上启用 DTLS 参数，该参数作为目标*虚拟服务器*绑定到 CS *虚拟服务器*。

## 限制

如果客户端设备上存在 Citrix Gateway 虚拟服务器的陈旧 DNS 条目，自适应传输和 Framehawk 可能会回退到 TCP 传输而不是 UDP 传输。如果发生回退到 TCP 传输的情况，请刷新客户端上的 DNS 缓存并重新连接以使用 UDP 传输建立会话。

Framehawk 不支持 32 位鼠标光标，例如 PTC Creo 等应用程序中使用的光标。

Framehawk 专为使用单个显示器（例如笔记本电脑和平板电脑）的移动设备而设计，在双显示器或多显示器配置中，它将回退到 Thinwire。

### 对其他 VPN 产品的支持

Citrix Gateway 是唯一支持 Framehawk 所需 UDP 加密的 SSL VPN 产品。如果使用其他 SSL VPN 或不正确版本的 Citrix Gateway，Framehawk 策略可能无法应用。传统的 IPsec VPN 产品无需任何修改即可支持 Framehawk。

### 监视 Framehawk

您可以从 Citrix Director 监视 Framehawk 的使用和性能。HDX 虚拟通道详细信息视图包含用于在任何会话中排查和监视 Framehawk 的有用信息。要查看 Framehawk 相关指标，请选择 **Graphics-Framehawk**。

如果 Framehawk 连接已建立，您将在详细信息页面中看到 **Provider = VD3D** 和 **Connected = True**。虚拟通道状态为空闲是正常的，因为它监视信令通道，该通道仅在初始握手期间使用。此页面还提供有关连接的其他有用统计信息。

如果遇到问题，请参阅 Framehawk 故障排除博客。

## 思睿线

### 简介

Thinwire 是 Citrix HDX 技术的一部分，是 Citrix Virtual Apps and Desktops 中使用的 Citrix 默认显示远程处理技术。

显示远程处理技术允许将一台计算机上生成的图形传输到另一台计算机上显示，通常通过网络传输。

成功的显示远程处理解决方案可提供高度交互的用户体验，类似于本地 PC。Thinwire 通过使用一系列复杂而高效的图像分析和压缩技术来实现这种体验。Thinwire 可最大限度地提高服务器可伸缩性，并且比其他显示远程处理技术消耗更少的带宽。

由于这种平衡，Thinwire 满足了大多数通用业务用例，并被用作 Citrix Virtual Apps and Desktops 中的默认显示远程处理技术。

### HDX™ 3D 专业版

在其默认配置中，Thinwire 可以提供 3D 或高度交互的图形，并在存在图形处理单元 (GPU) 的情况下使用它。但是，对于存在 GPU 的场景，我们建议使用**针对 3D 图形工作负载进行优化**或**视觉质量**

**> 构建为无损**策略来启用 HDX 3D Pro 模式。这些策略将 Thinwire 配置为在存在 GPU 的情况下使用视频编解码器（H.264 或 H.265）通过硬件加速对整个屏幕进行编码。这样做可以为 3D 专业图形提供更流畅的体验。有关详细信息，请参阅 H.264 构建为无损、HDX 3D Pro 和 Windows 单会话操作系统 GPU 加速。

## 要求

Thinwire 针对现代操作系统进行了优化，包括 Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows Server 2012 R2、Windows 10 和 Windows 7。对于 Windows Server 2008 R2，建议使用旧版图形模式。使用内置的 Citrix 策略模板、高服务器可伸缩性-旧版操作系统和针对 WAN-旧版操作系统优化来提供 Citrix 推荐的这些用例的策略设置组合。

> **注意：**
>
> 此版本不支持旧版图形模式。它用于在使用 XenApp 7.15 LTSR、XenDesktop 7.15 LTSR 以及以前的 VDA 版本与 Windows 7 和 Windows 2008 R2 时的向后兼容性。

- 驱动 Thinwire 行为的策略设置**使用视频编解码器进行压缩**在 Citrix Virtual Apps and Desktops 7 1808 或更高版本以及 XenApp and XenDesktop 7.6 FP3 或更高版本中的 VDA 版本上可用。**首选时使用视频编解码器**选项是 Citrix Virtual Apps and Desktops 7 1808 或更高版本以及 XenApp and XenDesktop 7.9 或更高版本中的 VDA 版本的默认设置。
- 所有 Citrix Workspace™ 应用程序都支持 Thinwire。某些 Citrix Workspace 应用程序可能支持 Thinwire 的某些功能，而其他应用程序不支持，例如，用于减少带宽使用的 8 位或 16 位图形。Citrix Workspace 应用程序会自动协商对此类功能的支持。
- 在多显示器和高分辨率场景中，Thinwire 会使用更多的服务器资源（CPU、内存）。可以调整 Thinwire 使用的资源量，但是，带宽使用量可能会因此增加。
- 在低带宽或高延迟场景中，请考虑启用 8 位或 16 位图形以提高交互性。视觉质量可能会受到影响，尤其是在 8 位颜色深度下。

## 编码方法

Thinwire 可以根据策略和客户端功能在两种不同的编码模式下运行：

- Thinwire 全屏 H.264 或 H.265
- Thinwire 选择性 H.264 或 H.265

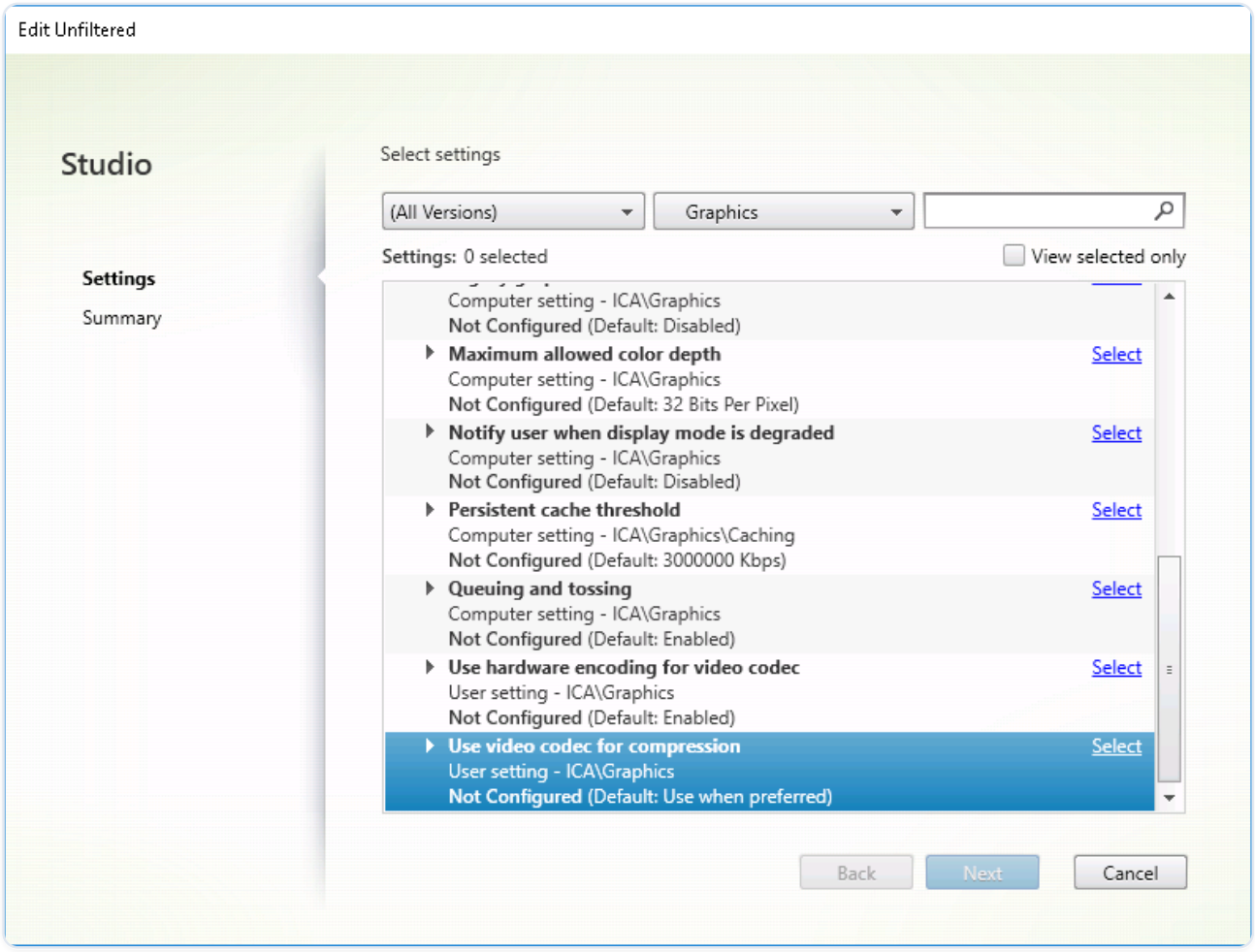
传统的 GDI 远程处理使用 XPDM 远程处理驱动程序，而不是 Thinwire 位图编码器。

## 配置

Thinwire 是默认的显示远程处理技术。

以下图形策略设置可设置默认值并为不同的用例提供替代方案：

- 使用视频编解码器进行压缩
  - **首选时使用视频编解码器**。这是默认设置。无需额外配置。将此设置保留为默认值可确保为所有 Citrix 连接选择 Thinwire，并针对可伸缩性、带宽和典型桌面工作负载的卓越图像质量进行优化。这在功能上等同于**对于活动变化区域**。
- 此策略设置中的其他选项继续将 Thinwire 与其他技术结合使用，以适应不同的用例。例如：
  - **对于活动变化区域**。Thinwire 中的自适应显示技术可识别移动图像（视频、运动中的 3D），并且仅在图像移动的屏幕部分使用 H.264 或 H.265。
  - **对于整个屏幕**。提供带有全屏 H.264 或 H.265 的 Thinwire，以优化在大量使用 3D 图形情况下的用户体验和带宽。在 H.264 4:2:0 的情况下（**视觉无损**策略已禁用），最终图像并非像素完美（无损），可能不适用于某些场景。在这种情况下，请考虑改用 H.264 构建为无损。



其他各种策略设置，包括以下视觉显示策略设置，可用于微调显示远程处理技术的性能。Thinwire 支持所有这些设置。

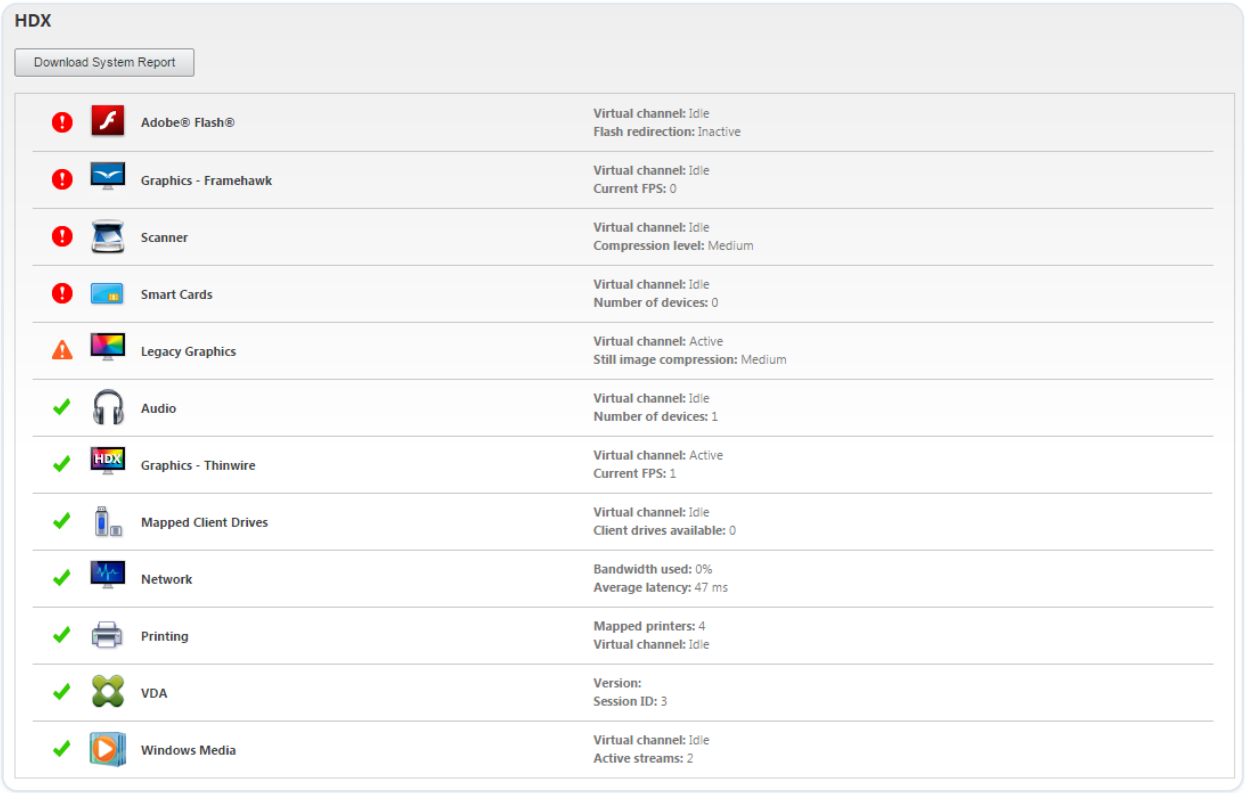
- 简单图形的首选颜色深度
- 目标帧速率
- 视觉质量

要获取适用于不同业务用例的 Citrix 推荐策略设置组合，请使用内置的 Citrix 策略模板。**高服务器可伸缩性**和**超高清用户体验**模板都使用 Thinwire，并结合了最适合您组织优先级和用户期望的策略设置。

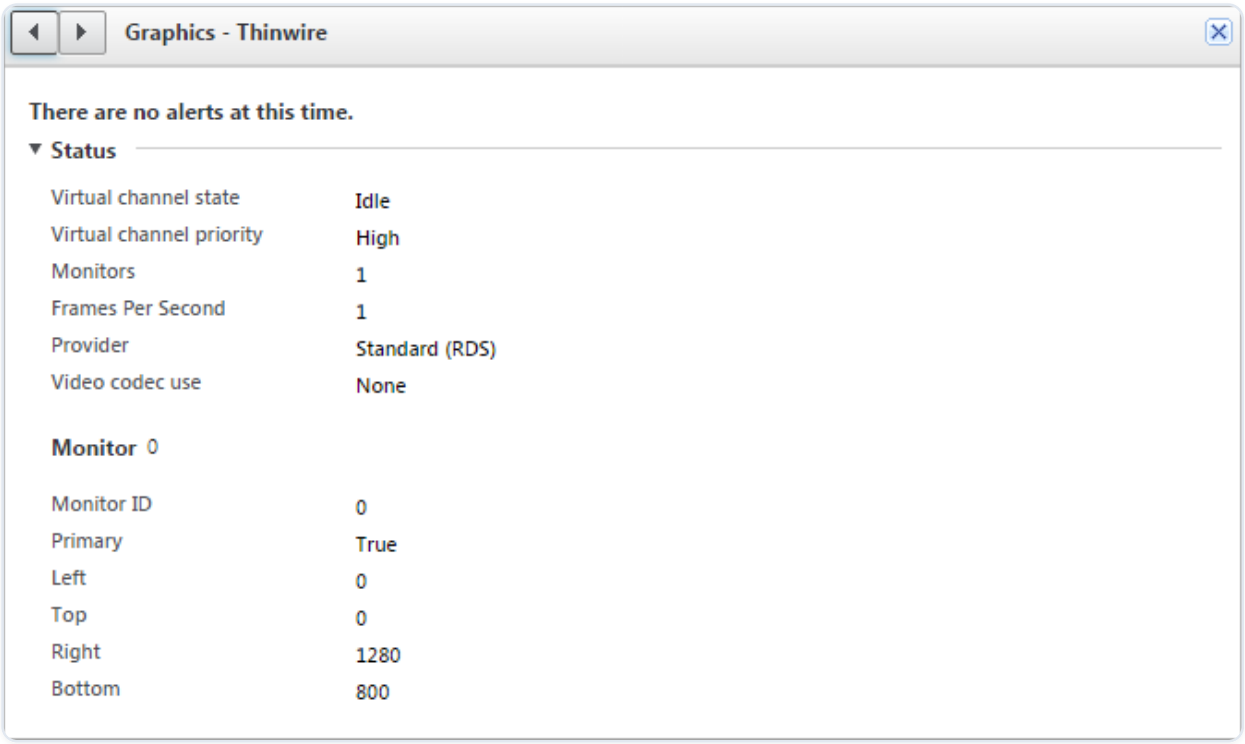
## 监视 Thinwire

您可以从 Citrix Director 监视 Thinwire 的使用情况和性能。HDX 虚拟通道详细信息视图包含用于故障排除和监视任何会话中 Thinwire 的有用信息。要查看与 Thinwire 相关的指标：

1. 在 Director 中，搜索用户、计算机或端点，打开活动会话，然后单击“**详细信息**”。或者，您可以选择“**筛选器**”>“**会话**”>“**所有会话**”，打开活动会话，然后单击“**详细信息**”。
2. 向下滚动到“**HDX**”面板。




3. 选择“**图形 - Thinwire**”。




## 无损压缩编解码器 (MDRLE)

在典型的桌面会话中，大多数图像是简单的图形或文本区域。Thinwire 确定这些区域的位置，并使用 2DRLE 编解码器选择这些区域进行无损编码。在 Citrix Workspace 应用程序客户端，这些元素使用 Citrix Workspace 应用程序端的 2DRLE 解码器进行解码以显示会话。

在 XenApp 和 XenDesktop 7.17 中，我们添加了更高压缩比的 MDRLE 编解码器，与 2DRLE 编解码器相比，它在典型桌面会话中消耗的带宽更少。此新编解码器不影响服务器可伸缩性。

较低的带宽通常意味着改进的会话交互性（尤其是在共享或受限链路上）和降低的成本。例如，对于典型的 Office 类工作负载，使用 MDRLE 编解码器时的预期带宽消耗比 XenApp 和 XenDesktop 7.15 LTSR 大约减少 10–15%。

MDRLE 编解码器不需要配置。如果 Citrix Workspace 应用程序支持 MDRLE 解码，则 VDA 使用 VDA MDRLE 编码和 Citrix Workspace 应用程序 MDRLE 解码。如果 Citrix Workspace 应用程序不支持 MDRLE 解码，则 VDA 会自动回退到 2DRLE 编码。

**MDRLE 要求：**

- Citrix 虚拟应用和桌面 最低版本 7 1808 VDA
- XenApp and XenDesktop 最低版本 7.17 VDA
- 适用于 Windows 的 Citrix Workspace 应用程序最低版本 1808
- 适用于 Windows 的 Citrix Receiver 最低版本 4.11

## 渐进模式

Citrix Virtual Apps and Desktops 1808 引入了渐进模式并默认启用。在网络条件受限的情况下（默认：带宽 < 2 Mbps 或延迟 > 200 ms），Thinwire 会增加文本和静态图像的压缩，以在屏幕活动期间提高交互性。然后，当屏幕活动停止时，这些高度压缩的文本和图像会以随机块的方式逐步锐化。虽然这种压缩和锐化方式可以提高整体交互性，但它会降低缓存效率并增加带宽使用量。

从 Citrix Virtual Apps and Desktops 1906 开始，渐进模式默认禁用。我们现在采用不同的方法。静止图像的质量现在基于网络条件，并在每个**视觉质量**设置的预定义最小值和最大值之间浮动。由于没有明确的锐化步骤，Thinwire 优化了图像传输并保持了缓存效率，同时提供了渐进模式几乎所有的优势。

### 更改渐进模式行为

您可以使用注册表项更改渐进模式状态。有关信息，请参阅注册表管理的特性列表中的渐进模式。

## H.264 构建为无损

**构建为无损**是一种特殊的 Thinwire 配置，可优化图形传输以实现交互性和最终图像质量。您可以通过将**视觉质量**策略设置为**构建为无损**来启用此设置。

构建为无损在屏幕活动期间使用 H.264（或 H.265）压缩屏幕，并在活动停止时锐化至像素完美（无损）。H.264（或 H.265）图像质量会根据可用资源进行调整，以保持最佳帧率。锐化步骤是逐步执行的，如果用户在锐化开始后不久开始屏幕活动，则会立即响应。例如，选择模型并旋转它。

H.264 **构建为无损**提供了全屏 H.264 或 H.265 的所有优势，包括硬件加速，但额外的好处是最终的、有保证的无损屏幕。这对于需要最终像素完美图像的 3D 类型工作负载至关重要。例如，操作医疗图像。此外，H.264 **构建为无损**比全屏 H.264 4:4:4 使用更少的资源。因此，使用**构建为无损**通常会比视觉无损 H.264 4:4:4 产生更高的帧率。

> **注意：**
>
> 除了**视觉质量**策略之外，请将**使用视频编解码器**策略设置为**首选时使用**（默认）或**用于活动变化区域**。您可以通过将**使用视频编解码器**策略设置为**不使用视频编解码器**来恢复为非 H.264 构建为无损。这将导致移动图像使用 JPEG 而不是 H.264（或 H.265）进行编码。

# 基于文本的会话水印

基于文本的会话水印有助于阻止和实现数据盗窃追踪。此可追踪信息显示在会话桌面上，以威慑那些使用照片和屏幕截图窃取数据的人。您可以指定一个水印，它是一个文本层，显示在整个会话屏幕上，而不会更改原始文档的内容。基于文本的会话水印需要 VDA 支持。

> **重要提示：**
>
> 基于文本的会话水印不是安全功能。此解决方案不能完全阻止数据盗窃，但它提供了一定程度的威慑和可追溯性。尽管我们不保证在使用此功能时信息完全可追溯，但我们建议您酌情将此功能与其他安全解决方案结合使用。
>
> 会话水印是文本，应用于交付给用户的会话。会话水印携带用于追踪数据盗窃的信息。最重要的数据是截取屏幕图像的当前会话的登录用户的身份。为了更有效地追踪数据泄露，请包含其他信息，例如服务器或客户端的 Internet 协议地址以及连接时间。

要调整用户体验，请使用会话水印策略设置来配置水印在屏幕上的位置和外观。

**要求：**

虚拟投递代理：

多会话操作系统 7.17 单会话操作系统 7.17

**限制：**

- 在使用本地应用程序访问、Windows 媒体重定向、MediaStream、浏览器内容重定向和 HTML5 视频重定向的会话中不支持会话水印。要使用会话水印，请确保禁用这些功能。
- 如果会话在全屏硬件加速模式（全屏 H.264 或 H.265 编码）下运行，则不支持会话水印，并且不显示水印。
- 如果设置了这些 HDX™ 策略，水印设置将不生效，并且会话显示中不显示水印。

**对视频编解码器使用硬件编码**设置为**已启用 使用视频编解码器进行压缩**设置为**针对整个屏幕**

- 如果设置了这些 HDX 策略，则行为不确定，并且水印可能不显示。

  **对视频编解码器使用硬件编码**设置为**已启用 使用视频编解码器进行压缩**设置为**在首选时使用视频编解码器**

  要确保显示水印，请将**对视频编解码器使用硬件编码**设置为**已禁用**，或将**使用视频编解码器进行压缩**设置为**针对活动变化的区域**或**不使用视频编解码器**。

- 会话水印仅支持 Thinwire 图形模式。
- 如果您使用会话录制，录制的会话不包含水印。
- 如果您使用 Windows 远程协助，则不显示水印。
- 如果用户按 **Print Screen** 键捕获屏幕，则在 VDA 端捕获的屏幕不包含水印。我们建议您采取措施，避免捕获的图像被复制。

# 屏幕共享

屏幕共享允许用户与他人共享 Citrix Virtual Desktop 会话，包括屏幕内容、键盘和鼠标控制。

## 系统要求

- Windows：单会话或多会话操作系统 VDA
- Linux：有关共享 Linux 会话的更多信息，请参阅Linux VDA 文档。
- 只能共享桌面会话。
- 托管会话的 VDA 与连接到共享会话的计算机之间必须存在网络连接。网络端口要求基于正在使用的 ICA 端口（TCP/UDP 1494 或 2598）和屏幕共享策略配置（默认为 TCP 52525 到 52625）。

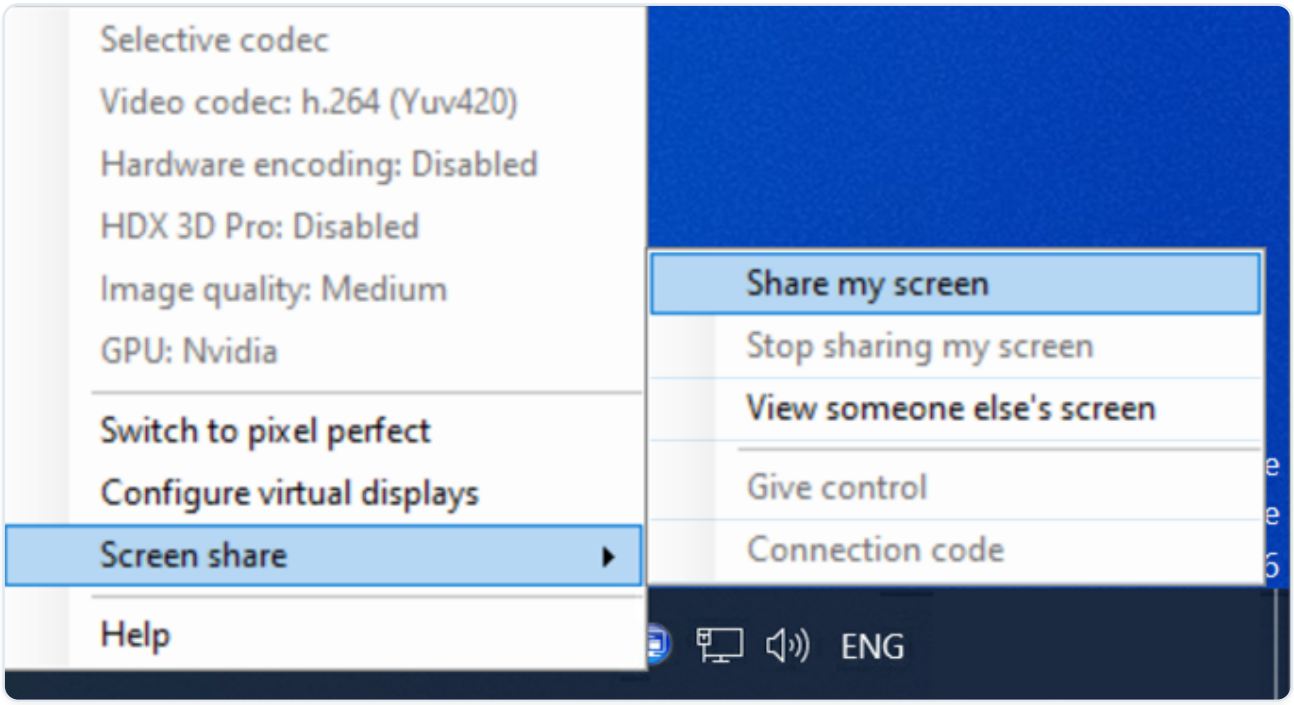
## 配置

必须使用 Citrix 策略启用屏幕共享。屏幕共享默认处于禁用状态。配置屏幕共享策略以启用或禁用该功能并分配可用的网络端口范围。

启用图形状态指示器策略以显示包含用于共享和连接会话的控件的用户界面。

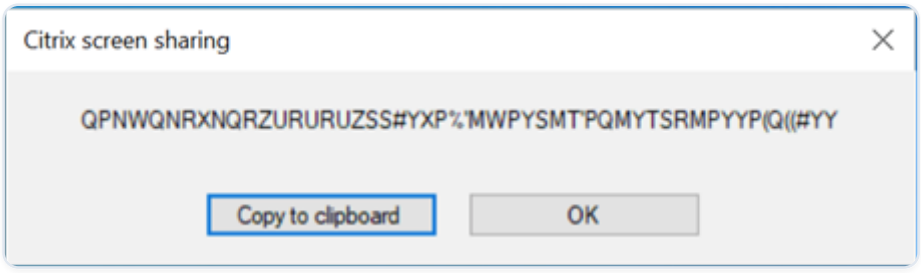
## 共享会话

要共享会话，请在 Windows 通知区域中查找 HDX™ 图形状态指示器图标。右键单击它以显示菜单并选择 **Screen share > Share my screen**（屏幕共享 > 共享我的屏幕）。




单击 **Copy to clipboard**（复制到剪贴板）或手动选择并复制对话框中显示的整个字符串。然后可以将该字符串粘贴到所选应用程序（例如电子邮件或即时消息客户端）中，以分发给其他用户。

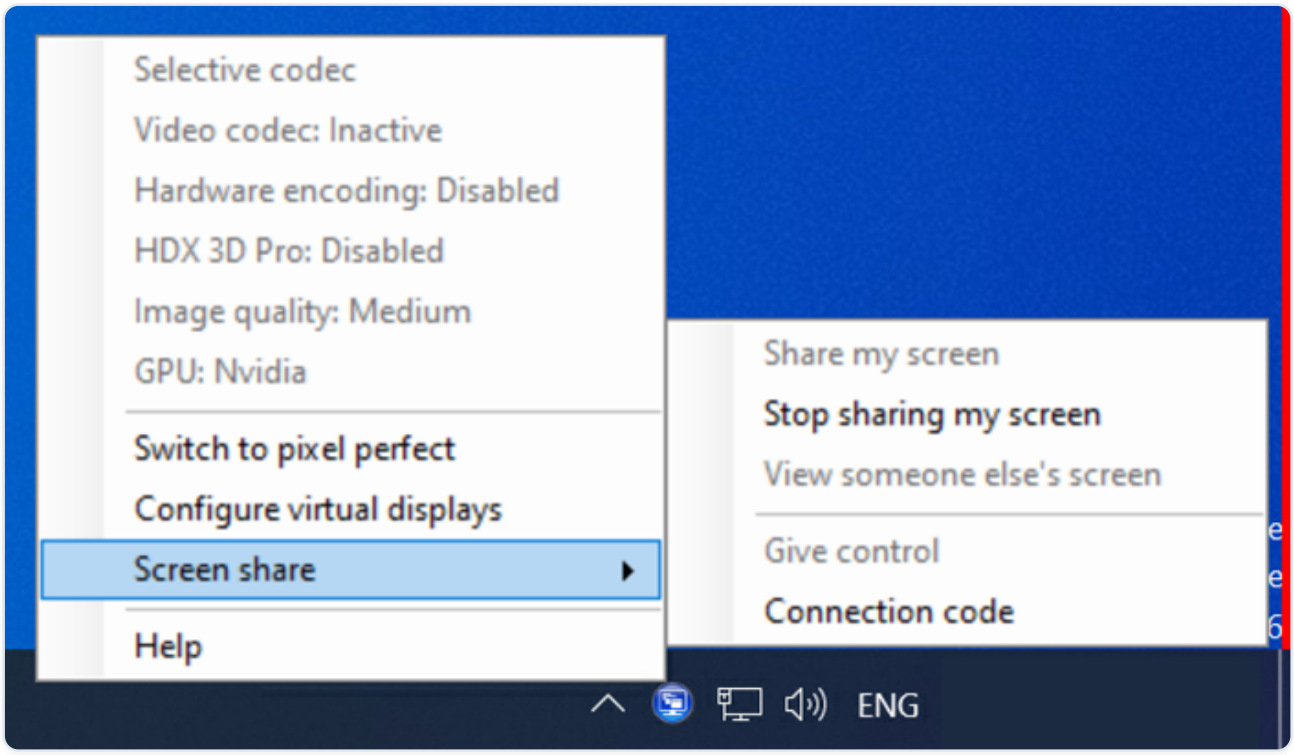
单击 **OK**（确定）或 **x** 关闭对话框。在会话共享期间，可以随时从 **Screen share > Connection code**（屏幕共享 > 连接代码）菜单选项中检索连接代码。




屏幕周围会出现红色轮廓，表示会话正在共享并可供其他人查看。

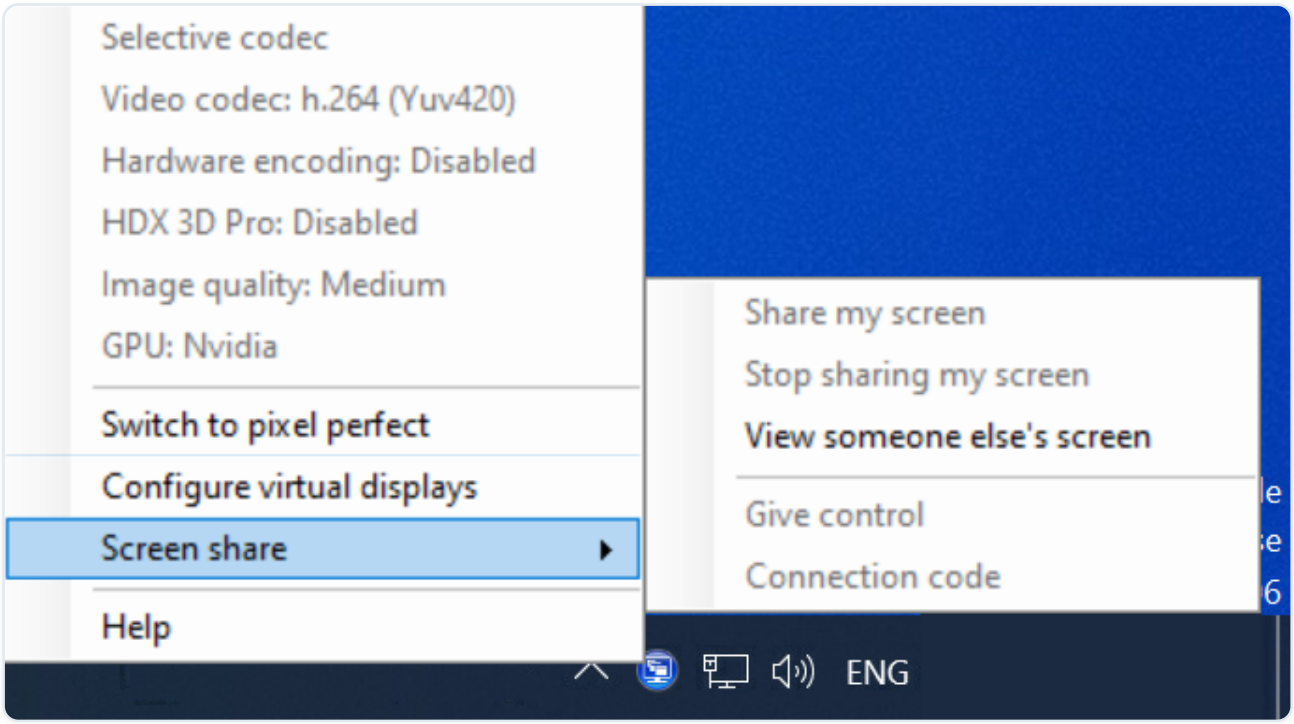
还可以使用 **Screen share > Give control**（屏幕共享 > 授予控制权）菜单选项与其他用户共享键盘和鼠标控制。

使用 **Screen share > Stop sharing my screen**（屏幕共享 > 停止共享我的屏幕）菜单选项停止共享会话并断开所有用户的连接。

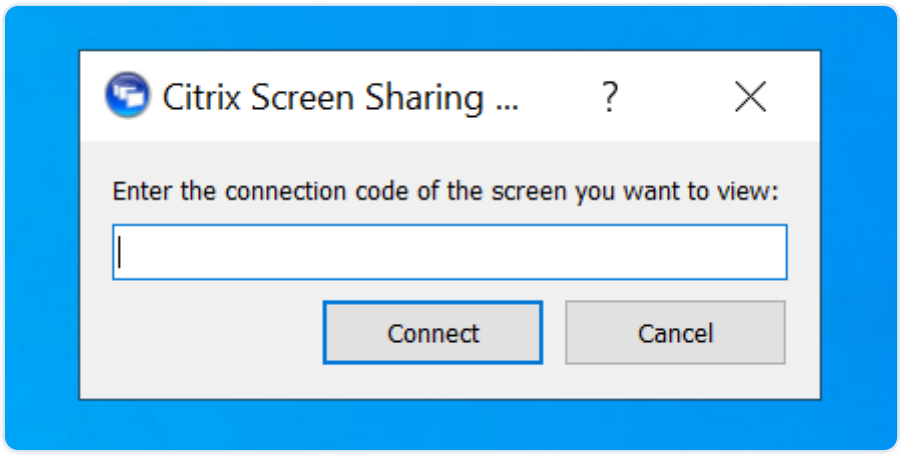



## 连接到共享会话

要连接到其他人的会话，请在 Windows 通知区域中查找 HDX 图形状态指示器图标。右键单击它以显示菜单，然后选择 **屏幕共享 > 查看其他人的屏幕**。

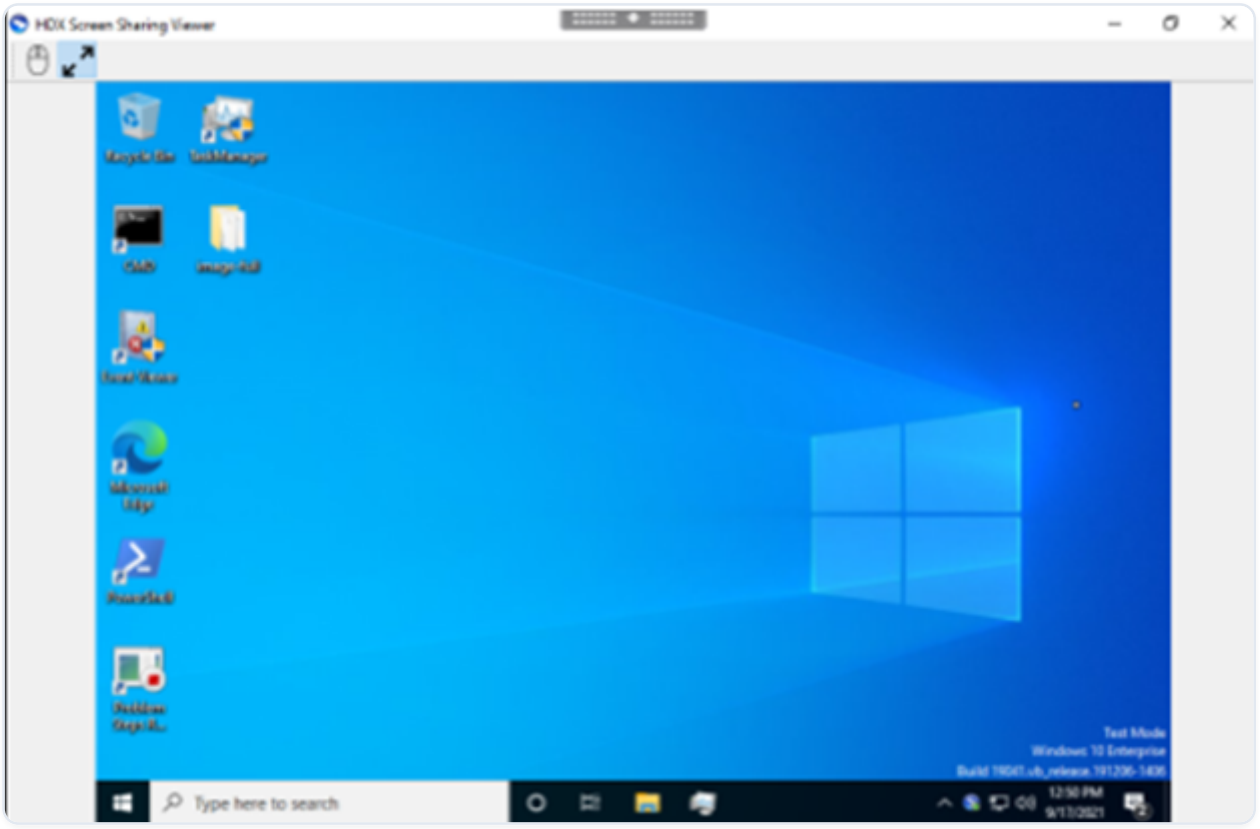



在文本框中输入或粘贴共享会话的用户提供的连接字符串。单击**连接**以建立连接。




通过单击 **HDX 屏幕共享查看器**窗口左上角的鼠标图标，您可以请求键盘和鼠标控制。

随时关闭 **HDX 屏幕共享查看器**窗口以断开与共享会话的连接。



## 其他注意事项

- 屏幕共享查看器应用程序随 VDA 一起安装在 *C:\Program Files\Citrix\HDX\bin\TwPlayer.exe* 中，并且可以使用 Virtual Apps Server 部署为已发布的应用程序。此替代部署模型允许与无法访问虚拟桌面的用户进行协作。
- 可以使用屏幕共享策略中的网络端口范围来限制允许连接到共享会话的用户数量。每个用户需要一个端口。默认范围最多允许 100 个用户。
- 连接到会话的所有显示器都将共享。您无法选择单个显示器。

- 不支持 H.265 视频编解码器。

# 多媒体

HDX™ 技术栈通过两种互补的方法支持多媒体应用程序的交付：

- 服务器端渲染多媒体交付
- 客户端渲染多媒体重定向

此策略可确保您能够交付全范围的多媒体格式，提供出色的用户体验，同时最大限度地提高服务器可伸缩性以降低每用户成本。

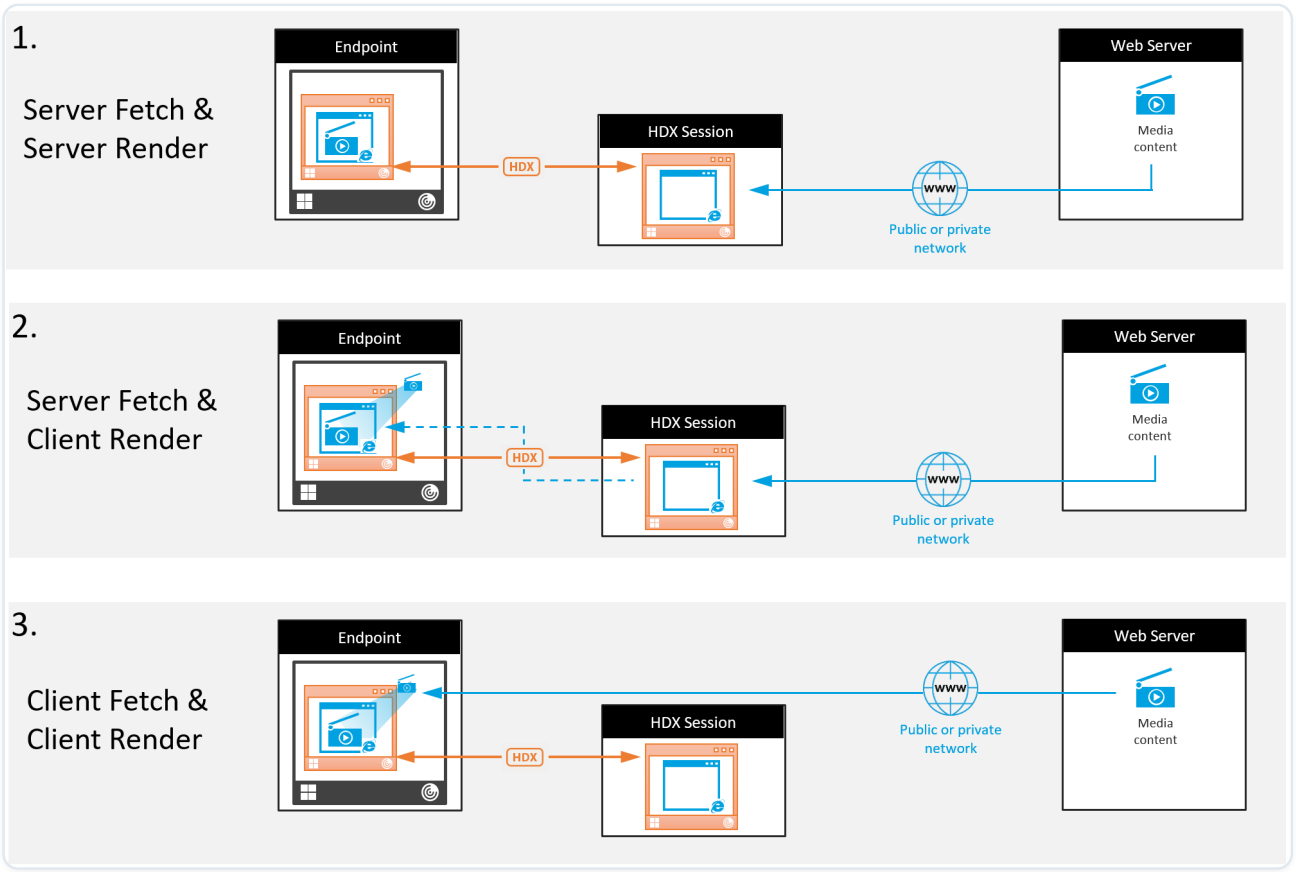
通过服务器渲染的多媒体交付，音频和视频内容由应用程序在 Citrix Virtual Apps and Desktops 服务器上解码和渲染。然后，内容使用 ICA 协议压缩并交付到用户设备上的 Citrix Workspace 应用程序。此方法提供了与各种应用程序和媒体格式的最高兼容性。由于视频处理是计算密集型的，因此服务器渲染的多媒体交付极大地受益于板载硬件加速。例如，对 DirectX 视频加速 (DXVA) 的支持通过在单独的硬件中执行 H.264 解码来分担 CPU 负载。Intel Quick Sync、AMD RapidFire 和 NVIDIA NVENC 技术提供硬件加速的 H.264 编码。

由于大多数服务器不提供任何用于视频压缩的硬件加速，如果所有视频处理都在服务器 CPU 上完成，服务器可伸缩性会受到负面影响。通过将许多多媒体格式重定向到用户设备进行本地渲染，可以保持较高的服务器可伸缩性。

- Windows Media 重定向可为通常与 Windows Media Player 关联的各种媒体格式分担服务器负载。
- HTML5 视频已变得流行，Citrix® 引入了一种针对此类内容的重定向技术。我们建议对使用 HTML5、HLS、DASH 或 WebRTC 的网站使用浏览器内容重定向。
- 您可以将通用联系重定向技术（主机到客户端重定向和本地应用程序访问）应用于多媒体内容。

综合这些技术，如果您不配置重定向，HDX 将执行服务器端渲染。 如果您配置重定向，HDX 将使用服务器获取和客户端渲染或客户端获取和客户端渲染。如果这些方法失败，HDX 将根据需要回退到服务器端渲染，并受回退预防策略的约束。

# 示例场景




**场景 1.（服务器获取和服务器渲染）：**

1. 服务器从其源获取媒体文件，解码，然后将内容呈现给音频设备或显示设备。
2. 服务器分别从显示设备或音频设备中提取呈现的图像或声音。
3. 服务器可以选择性地压缩它，然后将其传输到客户端。

这种方法会带来高 CPU 成本、高带宽成本（如果提取的图像/声音未有效压缩），并且服务器可伸缩性较低。

Thinwire 和音频虚拟通道处理此方法。这种方法的优点是它降低了客户端的硬件和软件要求。使用这种方法，解码在服务器上进行，并且适用于更广泛的设备和格式。

**场景 2.（服务器获取和客户端渲染）：**

这种方法依赖于能够在媒体内容解码并呈现给音频或显示设备之前对其进行拦截。压缩的音频/视频内容会发送到客户端，并在客户端进行解码和本地呈现。这种方法的优点是，这些被卸载到客户端设备，从而节省了服务器上的 CPU 周期。

但是，它也为客户端引入了一些额外的硬件和软件要求。客户端必须能够解码它可能接收的每种格式。

**场景 3.（客户端获取和客户端渲染）：**

这种方法依赖于能够在媒体内容 URL 从源获取之前对其进行拦截。URL 会发送到客户端，并在客户端获取、解码和本地呈现媒体内容。这种方法在概念上很简单。它的优点是既节省了服务器上的 CPU 周期，又节省了带宽，因为服务器只发送控制命令。但是，媒体内容并非总是可供客户端访问。

**框架和平台：**

单会话操作系统（Windows、Mac OS X 和 Linux）提供多媒体框架，可加快多媒体应用程序的开发。此表列出了一些更流行的多媒体框架。每个框架将媒体处理分为多个阶段，并使用基于管道的架构。

| 框架 | 平台 |
| --- | --- |
| DirectShow | Windows (98 及更高版本) |
| 媒体基础 | Windows (Vista 及更高版本) |
| 吉斯特里默 | 林纳克斯 |
| 快克时间 | Mac 操作系统 X |

# 支持媒体重定向技术的双跳

| | |
| --- | --- |
| 音频重定向 | 否 |
| 浏览器内容重定向 | 否 |
| HDX 网络摄像头重定向 | 是 |
| HTML5 视频重定向 | 是 |
| Windows Media 重定向 | 是 |

# 音频功能

您可以配置以下 Citrix 策略设置并将其添加到优化 HDX 音频功能的策略中。有关用法详细信息以及与其他策略设置的关系和依赖项，请参阅音频策略设置、带宽策略设置和多流连接策略设置。

## 自适应音频

借助自适应音频，您无需手动配置 VDA 上的音频质量策略。自适应音频可优化您的环境设置，并替换过时的音频压缩格式，以提供卓越的用户体验。

自适应音频默认启用。要禁用自适应音频，请参阅音频策略设置。

> **重要提示：**
>
> 当需要实时音频应用程序时，我们建议使用用户数据报协议 (UDP) 而不是 TCP 来传输音频。只有 Windows 虚拟投递代理 (VDA) 支持通过 UDP 传输音频。
>
> 使用 DTLS 的 UDP 音频加密仅在 Citrix Gateway 和 Citrix Workspace™ app 之间可用。因此，有时可能更倾向于使用 TCP 传输。TCP 支持从 VDA 到 Citrix Workspace app 的端到端 TLS 加密。
>
> 有关自适应音频和 UDP 音频的更多信息，请参阅通过 UDP 实时传输音频和音频 UDP 端口范围。

## 音频质量

通常，通过向用户设备发送更多音频数据，更高的音质会消耗更多的带宽和服务器 CPU 利用率。声音压缩允许您平衡音质与整体会话性能；使用 Citrix 策略设置来配置应用于声音文件的压缩级别。

默认情况下，当使用 TCP 传输时，**音频质量策略**设置为“高 - 高清音频”。当使用 UDP 传输（推荐）时，该策略设置为“中 - 语音优化”。**高清音频**设置提供高保真立体声，但比其他质量设置消耗更多带宽。请勿将此音频质量用于未经优化的语音聊天或视频聊天应用程序（例如软电话）。原因是它可能会在音频路径中引入不适合实时通信的延迟。无论选择何种传输协议，我们都建议将语音优化策略设置用于实时音频。

当带宽受限时（例如卫星或拨号连接），将音频质量降低到**低**会消耗最少的带宽。在这种情况下，请为低带宽连接上的用户创建单独的策略，以免对高带宽连接上的用户产生不利影响。

有关设置详细信息，请参阅音频策略设置。请记住在用户设备上启用客户端音频设置。

音频播放和录制带宽指南：

- 自适应音频（默认）
    - 比特率：可变自适应

- 通道数：播放为 2（立体声），麦克风捕获为 1（单声道）
- 频率：48000 Hz
- 位深度: 16 位

- 高质量
  - 比特率：播放时约 100 kbps（最小 75，最大 175 kbps）/ 麦克风捕获时约 70 kbps
  - 通道数：播放时 2（立体声），麦克风捕获时 1（单声道）
  - 频率：44100 Hz
  - 位深度: 16 位
- 中等质量 (建议用于 VoIP)
  - 比特率: 播放时约为 16 kbps (最小 20 kbps，最大 40 kbps)，麦克风捕获时约为 16 kbps
  - 通道数: 播放和捕获均为 1 (单声道)
  - 频率: 16000 Hz (宽带)
  - 位深度: 16 位
- 低质量
  - 比特率: 播放时约为 11 kbps (最小 10 kbps；最大 25 kbps)，麦克风捕获时约为 11 kbps
  - 通道数: 播放和捕获均为 1 (单声道)
  - 频率: 8000 Hz (窄带)
  - 位深度: 16 位

## 客户端音频重定向

要允许用户通过用户设备上的扬声器或其他声音设备接收来自服务器上应用程序的音频，请将**客户端音频重定向**设置保留为**允许**。这是默认设置。

客户端音频映射会增加服务器和网络的额外负载。但是，禁止客户端音频重定向会禁用所有 HDX™ 音频功能。

有关设置详细信息，请参阅音频策略设置。请记住在用户设备上启用客户端音频设置。

## 客户端麦克风重定向

要允许用户使用用户设备上的麦克风等输入设备录制音频，请将“**客户端麦克风重定向**”设置保留为默认值（允许）。

为安全起见，当用户不信任的服务器尝试访问麦克风时，用户设备会提醒其用户。用户可以在使用麦克风之前选择接受或拒绝访问。用户可以在 Citrix Workspace 应用程序上禁用此警报。

有关设置详细信息，请参阅音频策略设置。请记住在用户设备上启用客户端音频设置。

## 音频即插即用

“音频即插即用”策略设置允许或阻止使用多个音频设备录制和播放声音。此设置默认情况下处于“**已启用**”状态。音频即插即用功能使音频设备能够被识别。即使设备在用户会话启动后才插入，也能被识别。

此设置仅适用于 Windows 多会话操作系统计算机。

有关设置详细信息，请参阅音频策略设置。

## 音频重定向带宽限制和音频重定向带宽限制百分比

“音频重定向带宽限制”策略设置指定了会话中播放和录制音频的最大带宽（以千比特每秒为单位）。

“音频重定向带宽限制百分比”设置指定了音频重定向的最大带宽，该带宽是总可用带宽的百分比。

默认情况下，这两个设置都指定为零（无最大值）。如果同时配置了这两个设置，则使用带宽限制较低的那个。

有关设置详细信息，请参阅带宽策略设置。请记住在用户设备上启用客户端音频设置。

## 通过 UDP 实时传输的音频和音频 UDP 端口范围

默认情况下，允许通过用户数据报协议 (UDP) 实时传输音频（在安装时选择）。它在服务器上打开一个 UDP 端口，用于使用通过 UDP 实时传输的音频的连接。如果存在网络拥塞或数据包丢失，我们建议为音频配置 UDP/RTP，以确保最佳的用户体验。对于任何实时音频（例如软电话应用程序），UDP 音频优于 EDT。UDP 允许数据包丢失而无需重新传输，从而确保在高数据包丢失的连接上不会增加延迟。

> **重要提示：**
>
> 当 Citrix Gateway 不在路径中时，通过 UDP 传输的音频数据不会加密。如果 Citrix Gateway 配置为访问 Citrix Virtual Apps and Desktops™ 资源，则端点设备与 Citrix Gateway 之间的音频流量将使用 DTLS 协议进行保护。

> 音频 UDP 端口范围指定了 Windows VDA 用于与用户设备交换音频数据包的端口号范围。

默认情况下，范围是 16500 到 16509。

> **注意：**
>
> 如果自适应音频不需要通过 UDP 实时传输音频，Citrix 建议将策略设置配置为“已禁用”。这有助于避免 Citrix Workspace 应用程序客户端请求打开 UDP 连接或触发不必要的 Citrix Workspace 应用程序客户端防火墙配置对话框窗口出现。

> 有关通过 UDP 实时传输音频的设置详细信息，请参阅音频策略设置。有关音频 UDP 端口范围的详细信息，请参阅多流连接策略设置。请记住在用户设备上启用客户端音频设置。

通过 UDP 传输音频需要 Windows VDA。有关 Linux VDA 上支持的策略，请参阅策略支持列表。

## 用户设备的音频设置策略

1. 按照配置组策略对象管理模板中的说明加载组策略模板。
2. 在组策略编辑器中，展开**管理模板 > Citrix 组件 > Citrix Workspace > 用户体验**。
3. 对于**客户端音频设置**，选择**未配置**、**已启用**或**已禁用**。
   - **未配置**。默认情况下，音频重定向使用高质量音频或以前配置的自定义音频设置启用。
   - **已启用**。使用选定的选项启用音频重定向。
   - **已禁用**。禁用音频重定向。
4. 如果选择**已启用**，请选择一种音质。对于 UDP 音频，请使用**中等**（默认）。
5. 仅对于 UDP 音频，选择**启用实时传输**，然后设置要在本地 Windows 防火墙中打开的传入端口范围。
6. 要将 UDP 音频与 Citrix Gateway 结合使用，请选择 **允许通过网关进行实时传输**。使用 DTLS 配置 Citrix Gateway。有关详细信息，请参阅这篇文章。

作为管理员，如果您无法控制端点设备进行这些更改，请使用 StoreFront 中的 default.ica 属性来启用 UDP 音频。例如，对于自带设备或家用计算机。

1. 在 StoreFront 计算机上，使用记事本等编辑器打开 C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica。
2. 在 部分下进行以下条目。

```
; 此文本启用实时传输
```

EnableRtpAudio=真

; 此文本允许通过网关进行实时传输

EnableUDPThroughGateway=真

; 此文本将音频质量设置为中等

AudioBandwidthLimit=1

; UDP 端口范围

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509

如果您通过编辑 default.ica 启用用户数据报协议 (UDP) 音频，则该存储的所有用户都将启用 UDP 音频。

## 避免多媒体会议期间的回声

音频或视频会议中的用户可能会听到回声。回声通常发生在扬声器和麦克风距离过近时。因此，我们建议在音频和视频会议中使用耳机。

HDX 提供回声消除选项（默认启用），可最大程度地减少任何回声。回声消除的有效性对扬声器和麦克风之间的距离很敏感。请确保设备不要靠得太近或太远。

您可以更改注册表设置以禁用回声消除。有关信息，请参阅注册表管理的功能列表中的避免多媒体会议期间的回声。

## 软电话

软电话是充当电话界面的软件。您可以使用软电话通过互联网从计算机或其他智能设备拨打电话。通过使用软电话，您可以使用屏幕拨打电话号码并执行其他与电话相关的功能。

Citrix Virtual Apps and Desktops 支持多种交付软电话的替代方案。

- **控制模式**。托管软电话控制物理电话机。在此模式下，没有音频流量通过 Citrix Virtual Apps and Desktops 服务器。
- **HDX RealTime 优化软电话支持（推荐）**。媒体引擎在用户设备上运行，并且互联网协议语音流量以对等方式流动。例如，请参阅：
  - 适用于 Microsoft Teams 的 HDX 优化(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/multimedia/opt-ms-teams.html)

    - HDX RealTime Optimization Pack，它能够优化 Microsoft Skype for Business 的交付
    - Cisco Jabber Softphone for VDI（以前被称作 VXME）
    - 思科 Webex 会议 for VDI
    - Avaya VDI 爱酷诺克斯（以前称为 VDI 通信器）
    - Zoom VDI 插件
    - 捷信纯粹互动云
    - Nuance Dragon PowerMic 听写设备

- **本地应用程序访问**。Citrix Virtual Apps and Desktops 功能，允许软电话等应用程序在 Windows 用户设备上本地运行，但仍能与虚拟/已发布的桌面无缝集成。此功能将所有音频处理卸载到用户设备。有关详细信息，请参阅本地应用程序访问和 URL 重定向。
- **HDX RealTime 通用软电话支持**。基于 ICA 的互联网协议语音。

***通用软电话支持***

通用软电话支持使您能够在数据中心的 XenApp 或 XenDesktop 上托管未经修改的软电话。音频流量通过 Citrix ICA 协议（最好使用 UDP/RTP）传输到运行 Citrix Workspace 应用程序的用户设备。

通用软电话支持是 HDX RealTime 的一项功能。这种软电话交付方法在以下情况下特别有用：

- 没有可用的优化软电话交付解决方案，并且用户不在可以使用本地应用访问的 Windows 设备上。
- 优化交付软电话所需的媒体引擎未安装在用户设备上，或者不适用于用户设备上运行的操作系统版本。在这种情况下，通用 HDX RealTime 提供了一个有价值的备用解决方案。

使用 Citrix Virtual Apps and Desktops 交付软电话时，需要考虑以下两点：

- 软电话应用程序如何交付到虚拟/已发布的桌面。
- 音频如何传输到用户耳机、麦克风和扬声器，或 USB 电话机，以及如何从这些设备传输音频。

Citrix Virtual Apps and Desktops 包含多种技术来支持通用软电话交付：

- 针对语音优化的编解码器，用于实时音频的快速编码和带宽效率。
- 低延迟音频堆栈。
- 服务器端抖动缓冲区，用于在网络延迟波动时平滑音频。
- 服务质量 (Quality of Service) 的数据包标记 (DSCP 和 WMM)。
    - 用于 RTP 数据包 (第 3 层) 的 DSCP 标记

- 用于 Wi-Fi 的 WMM 标记

适用于 Windows、Linux、Chrome 和 Mac 的 Citrix Workspace 应用程序版本也支持语音通过 Internet 协议 (Voice over Internet Protocol)。适用于 Windows 的 Citrix Workspace 应用程序提供以下功能：

- 客户端抖动缓冲区 - 即使网络延迟波动，也能确保音频流畅。
- 回声消除 - 对于不使用耳机的员工，允许麦克风和扬声器之间的距离有更大的变化。
- 音频即插即用 - 音频设备无需在会话开始前插入。它们可以随时插入。
- 音频设备路由 - 用户可以将铃声定向到扬声器，但将语音路径定向到其耳机。
- 多流 ICA - 支持基于服务质量 (Quality of Service) 的灵活网络路由。
- ICA 支持四个 TCP 流和两个 UDP 流。其中一个 UDP 流支持通过 RTP 进行实时音频传输。

有关 Citrix Workspace 应用程序功能的摘要，请参阅 Citrix Receiver 功能矩阵。

***系统配置建议***

*客户端硬件和软件*：为了获得最佳音频质量，我们建议使用最新版本的 Citrix Workspace 应用程序和具有声学回声消除 (AEC) 功能的优质耳机。适用于 Windows、Linux 和 Mac 的 Citrix Workspace 应用程序版本支持语音通过 Internet 协议 (Voice over Internet Protocol)。此外，Dell Wyse 还为 ThinOS (WTOS) 提供语音通过 Internet 协议 (Voice over Internet Protocol) 支持。

*CPU 考量*：监视 VDA 上的 CPU 使用率，以确定是否需要为每个虚拟机分配两个虚拟 CPU。实时语音和视频是数据密集型的。配置两个虚拟 CPU 可减少线程切换延迟。因此，我们建议您在 Citrix Virtual Desktops™ VDI 环境中配置两个 vCPU。

拥有两个虚拟 CPU 并不一定意味着物理 CPU 数量翻倍，因为物理 CPU 可以在会话之间共享。

Citrix Gateway Protocol (CGP) 用于会话可靠性功能，也会增加 CPU 消耗。在高质量网络连接上，您可以禁用此功能以降低 VDA 上的 CPU 消耗。在功能强大的服务器上，上述任何步骤可能都不必要。

*UDP 音频*: 通过 UDP 传输的音频对网络拥塞和数据包丢失具有出色的容忍度。如果可用，我们建议使用它而不是 TCP。

*LAN/WAN 配置*: 正确的网络配置对于良好的实时音频质量至关重要。通常，您必须配置虚拟 LAN (VLAN)，因为过多的广播数据包可能会引入抖动。启用 IPv6 的设备可能会生成许多广播数据包。如果不需要 IPv6 支持，您可以在这些设备上禁用 IPv6。配置以支持服务质量。

*WAN 连接使用设置*: 您可以通过 LAN 和 WAN 连接使用语音聊天。在 WAN 连接上，音频质量取决于连接的延迟、数据包丢失和抖动。如果通过 WAN 连接向用户交付软电话，我们建议在数据中心和远程办公室之间使用 NetScaler® SD-WAN。这样做可以保持高服务质量。NetScaler SD-WAN 支持多流 ICA，包括 UDP。此外，对于单个 TCP 流，可以区分各种 ICA 虚拟通道的优先级，以确保高优先级实时音频数据获得优先处理。

使用 Director 或 HDX Monitor 验证您的 HDX 配置。

*远程用户连接*: Citrix Gateway 支持 DTLS 以本机方式（不封装在 TCP 中）交付 UDP/RTP 流量。为通过端口 443 的 UDP 流量双向打开防火墙。

*编解码器选择和带宽消耗*: 在用户设备和数据中心 VDA 之间，我们建议使用 **Optimized-for-Speech** 编解码器设置，也称为中等质量音频。在 VDA 平台和 IP-PBX 之间，软电话使用配置或协商的任何编解码器。例如：

- G711 提供良好的语音质量，但每个呼叫的带宽要求为 80 到 100 千比特每秒（取决于网络第 2 层开销）。
- G729 提供良好的语音质量，并且每个呼叫的带宽要求较低，为 30 到 40 千比特每秒（取决于网络第 2 层开销）。

### *将软电话应用程序交付到虚拟桌面*

您可以通过两种方法将软电话交付到 XenDesktop® 虚拟桌面：

- 应用程序可以安装在虚拟桌面映像中。
- 应用程序可以使用 Microsoft App-V 流式传输到虚拟桌面。这种方法具有可管理性优势，因为虚拟桌面映像保持整洁。流式传输到虚拟桌面后，应用程序在该环境中运行，就像以常规方式安装一样。并非所有应用程序都与 App-V 兼容。

### *向用户设备交付音频以及从用户设备接收音频*

通用 HDX RealTime 支持两种向用户设备交付音频以及从用户设备接收音频的方法：

- **Citrix 音频虚拟通道**。我们通常推荐使用 Citrix 音频虚拟通道，因为它专为音频传输而设计。
- **通用 USB 重定向**。如果用户设备通过 LAN 或类似 LAN 的连接回连到 Citrix Virtual Apps and Desktops 服务器，则支持带有按钮或显示屏（或两者兼有）的音频设备、人机接口设备 (HID)。

### *Citrix 音频虚拟通道*

双向 Citrix 音频虚拟通道 (CTXCAM) 能够高效地通过网络传输音频。通用 HDX RealTime 从用户耳机或麦克风获取音频并进行压缩。然后，通过 ICA 将其发送到虚拟桌面上的软电话应用程序。同样，软电话的音频输出也会被压缩并沿另一个方向发送到用户耳机或扬声器。此压缩独立于软电话

本身使用的压缩（例如 G.729 或 G.711）。它使用 Optimized-for-Speech 编解码器（中等质量）完成。其特性非常适合 IP 语音。它具有快速编码时间，并且仅消耗大约每秒 56 千比特的网络带宽（每个方向 28 Kbps），峰值。此编解码器必须在 Studio 控制台中明确选择，因为它不是默认音频编解码器。默认是 HD 音频编解码器（高质量）。此编解码器非常适合高保真立体声配乐，但与 Optimized-for-Speech 编解码器相比，编码速度较慢。

***通用 USB 重定向***

Citrix 通用 USB 重定向技术（CTXGUSB 虚拟通道）提供了一种通用的远程连接 USB 设备的方法，包括复合设备（音频加 HID）和同步 USB 设备。此方法仅限于 LAN 连接的用户。原因是 USB 协议往往对网络延迟敏感，并且需要大量的网络带宽。同步 USB 重定向在使用某些软电话时效果很好。这种重定向提供了出色的语音质量和低延迟。但是，Citrix 音频虚拟通道是首选，因为它针对音频流量进行了优化。主要例外情况是当您使用带有按钮的音频设备时。例如，连接到用户设备并与数据中心进行 LAN 连接的 USB 电话。在这种情况下，通用 USB 重定向支持电话机或耳机上的按钮，这些按钮通过向软电话发送信号来控制功能。对于在设备本地工作的按钮没有问题。

## 限制

您在客户端上安装音频设备，启用音频重定向，然后启动 RDS 会话。音频文件可能无法播放，并显示错误消息。

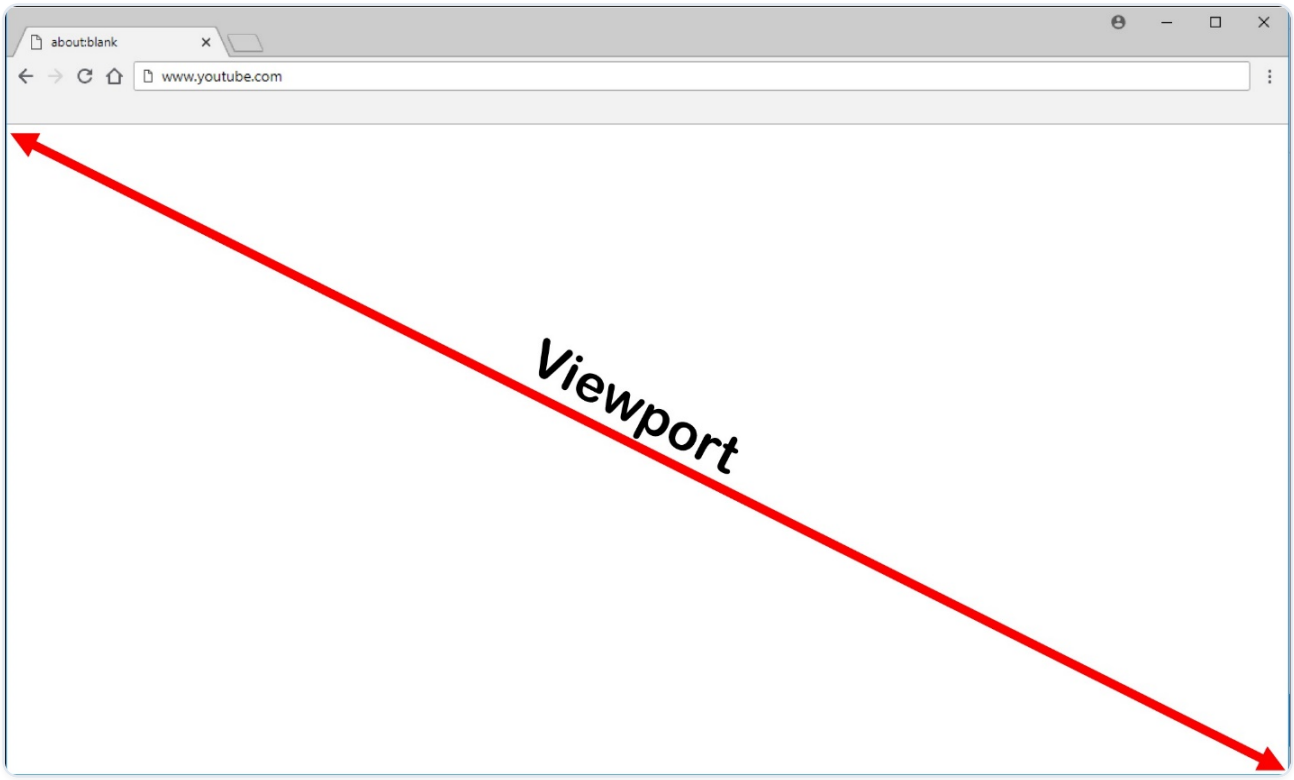
作为一种解决方法，请在 RDS 计算机上添加注册表项，然后重新启动计算机。有关信息，请参阅注册表管理的功能列表中的音频限制。

# 浏览器内容重定向

浏览器内容重定向阻止在 VDA 端呈现允许列表中的网页。此功能使用适用于 Windows 的 Citrix Workspace™ 应用程序或适用于 Linux 的 Citrix Workspace 应用程序在客户端实例化相应的呈现引擎，该引擎从 URL 获取 HTTP 和 HTTPS 内容。

> **注意：**
>
> 您可以使用阻止列表指定将网页重定向到 VDA 端（而不是在客户端重定向）。
>
> 此覆盖 Web 布局引擎在端点设备而不是 VDA 上运行，并使用端点的 CPU、GPU、RAM 和网络。

仅重定向浏览器视口。视口是浏览器中显示内容的矩形区域。视口不包括地址栏、**收藏夹**工具栏、状态栏等内容。这些项目位于用户界面中，它们仍在 VDA 中的浏览器上运行。




1. 配置一个 Studio 策略，该策略指定一个访问控制列表，其中包含用于重定向的允许列表中的 URL 或禁用特定 URL 路径重定向的阻止列表。为了让 VDA 上的浏览器检测到用户正在导航的 URL 是否与允许列表匹配或不与阻止列表匹配，浏览器扩展程序会执行比较。Internet Explorer 11 的浏览器扩展程序包含在安装介质中并自动安装。对于 Chrome，浏览器扩展程序可在 Chrome 网上应用店中获取，您可以使用组策略和 ADMX 文件进行部署。Chrome 扩展程序是按用户安装的。无需更新黄金映像来添加或删除扩展程序。
2. 如果在允许列表中找到匹配项（例如 `https://www.mycompany.com/`），并且阻止列表中的 URL 没有匹配项（例如 `https://www.mycompany.com/engineering`），虚拟通道 (CTXCSB) 会指示 Citrix Workspace 应用程序需要重定向并中继 URL。Citrix Workspace 应用程序随后会实例化本地呈现引擎并显示网站。
3. Citrix Workspace 应用程序随后将网站无缝地融合回虚拟桌面浏览器内容区域。

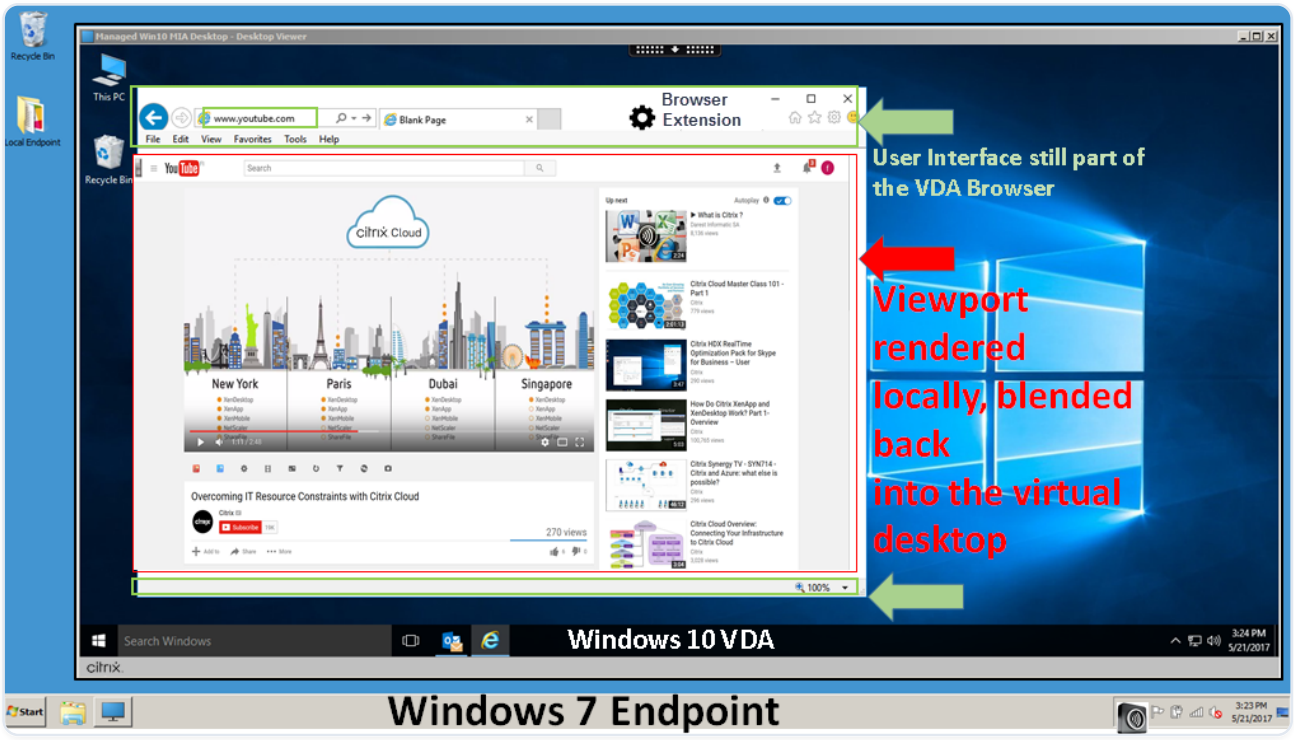
> **注意：**
>
> 有关浏览器内容重定向扩展程序的新增功能和修复的更多信息，请访问 Chrome 网上应用店并搜索“citrix® bcr”以查找该扩展程序。

> 徽标的颜色指定 Chrome 扩展程序的状态。它有以下三种颜色：

- 绿色：活动且已连接。
- 灰色：在当前选项卡上不活动/空闲。

- 红色：损坏/不工作。

您可以通过使用扩展程序菜单中的**选项**来调试日志记录。



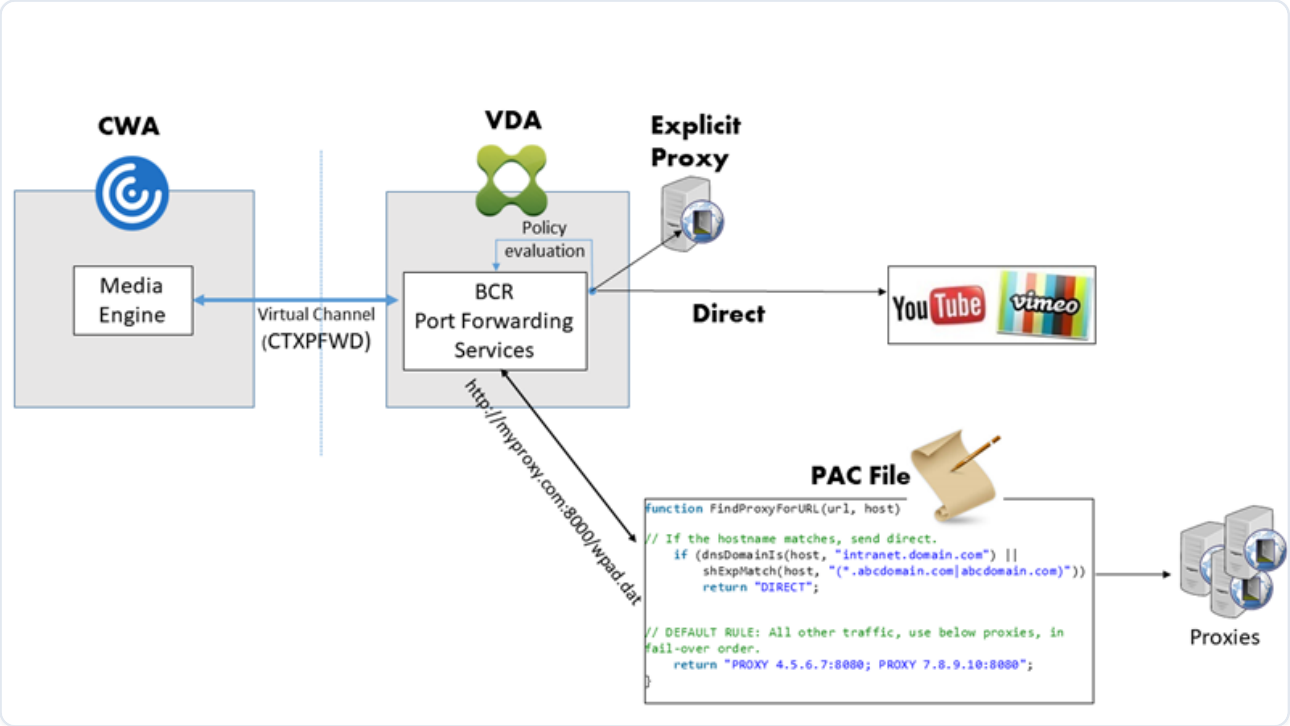

以下是 Citrix Workspace 应用程序获取内容的场景：

- **服务器提取和服务器呈现**：没有重定向，因为您没有将站点添加到允许列表或重定向失败。我们会回退到在 VDA 上呈现网页并使用 Thinwire 远程传输图形。使用策略控制回退行为。VDA 上的 CPU、RAM 和带宽消耗高。
- **服务器获取和客户端渲染**：Citrix Workspace 应用程序通过 VDA 使用虚拟通道 (CTXPFWD) 联系 Web 服务器并从中获取内容。当客户端没有 Internet 访问权限时（例如瘦客户端），此选项非常有用。VDA 上的 CPU 和 RAM 消耗低，但 ICA® 虚拟通道会消耗带宽。

  此场景有三种操作模式。术语“代理”是指 VDA 访问以获取 Internet 访问权限的代理设备。

  要选择的策略选项：

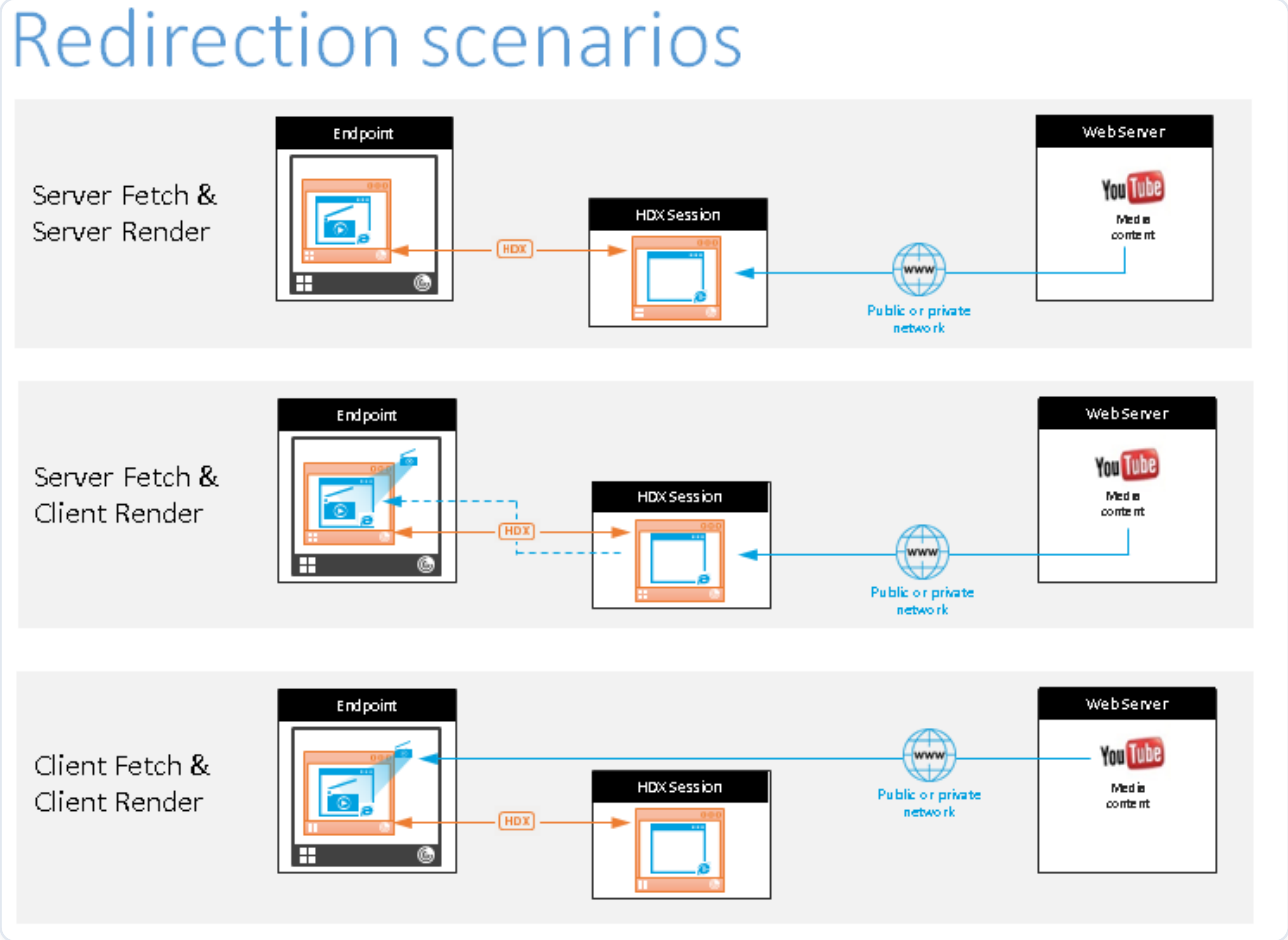
  - 显式代理 - 如果您的数据中心中有一个显式代理。
  - 直接或透明 - 如果您没有代理，或者您使用透明代理。
  - PAC 文件 - 如果您依赖 PAC 文件，以便 VDA 中的浏览器可以自动选择适当的代理服务器来获取指定的 URL。




- **客户端获取和客户端渲染**：由于 Citrix Workspace 应用程序直接联系 Web 服务器，因此它需要 Internet 访问。此场景将所有网络、CPU 和 RAM 使用量从您的 XenApp and XenDesktop® 站点卸载。

  优势：

  - 更好的最终用户体验（自适应比特率 (ABR)）
  - 降低 VDA 资源使用率 (CPU/RAM/IO)
  - 降低带宽消耗




**回退机制：**

有时客户端重定向可能会失败。例如，如果客户端计算机没有直接 Internet 访问权限，则错误响应可能会返回到 VDA。在这种情况下，VDA 上的浏览器可以重新加载并在服务器上渲染页面。

您可以使用现有的 **Windows Media 回退预防**策略来抑制视频元素的服务器渲染。将此策略设置为**仅在客户端播放所有内容**或**仅在客户端播放客户端可访问的内容**。如果客户端重定向失败，这些设置会阻止视频元素在服务器上播放。此策略仅在您启用浏览器内容重定向且**访问控制列表**策略包含回退的 URL 时生效。该 URL 不能在阻止列表策略中。

**系统要求：**

Windows 端点：

- Windows 10 系统
- 适用于 Windows 的 Citrix Workspace app 1809 或更高版本

> **注意：**

> 浏览器内容重定向仅在适用于 Windows 的 Citrix Workspace 应用程序的当前版本上受支持，但在 Citrix Workspace 应用程序 LTSR 版本 1912 和 2203.1 上不受支持。

> Linux 端点：

- 适用于 Linux 的 Citrix Workspace 应用程序 1808 或更高版本
- 瘦客户端终端必须包含 WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808 或更高版本以及 XenApp and XenDesktop 7.15 CU5 或更高版本：

- VDA 操作系统：Windows 10（最低版本 1607）、Windows Server 2012 R2 服务器、Windows Server 2016 服务器、Windows Server 2019 服务器
- VDA 上的浏览器：
  - Google Chrome v66 或更高版本（Chrome 要求用户端点上安装 Citrix Workspace 应用程序 1809 for Windows 或更高版本，Citrix Virtual Apps and Desktops™ 7 1808 VDA 或更高版本，以及浏览器内容重定向扩展程序）
  - Internet Explorer 11 并配置以下选项：
    - 在 **Internet 选项** > **高级 > 安全** 下清除 **增强保护模式**
    - 在 **Internet 选项 > 高级 > 浏览** 下选中 **启用第三方浏览器扩展**

## 故障排除

有关故障排除信息，请参阅知识中心文章 https://support.citrix.com/article/CTX230052

## 浏览器内容重定向 Chrome 扩展程序

要在 Chrome 中使用浏览器内容重定向，请从 Chrome 网上应用店添加浏览器内容重定向扩展程序。在 Citrix Virtual Apps and Desktops 环境中单击 **添加到 Chrome**。

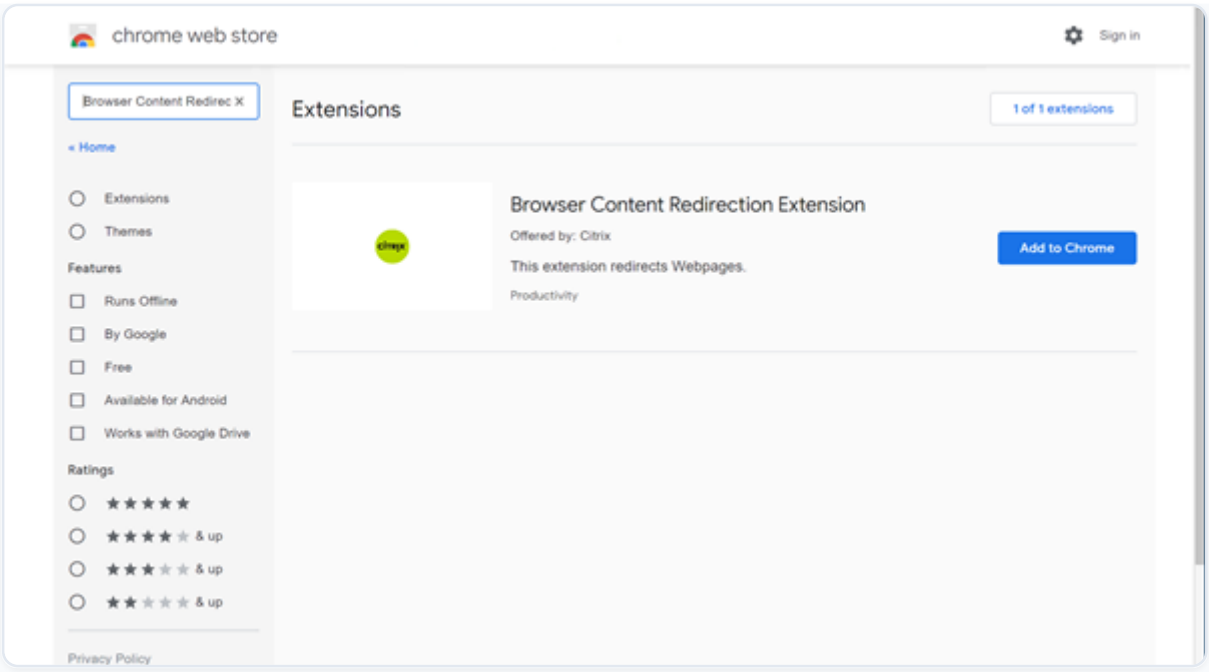
用户客户端计算机上**不需要**此扩展程序 – 仅在 VDA 中需要。

### 系统要求

- Chrome v66 或更高版本
- 浏览器内容重定向扩展程序
- Citrix Virtual Apps and Desktops 7 1808 或更高版本
- Citrix Workspace 应用程序 1809 for Windows 或更高版本

**注意：**

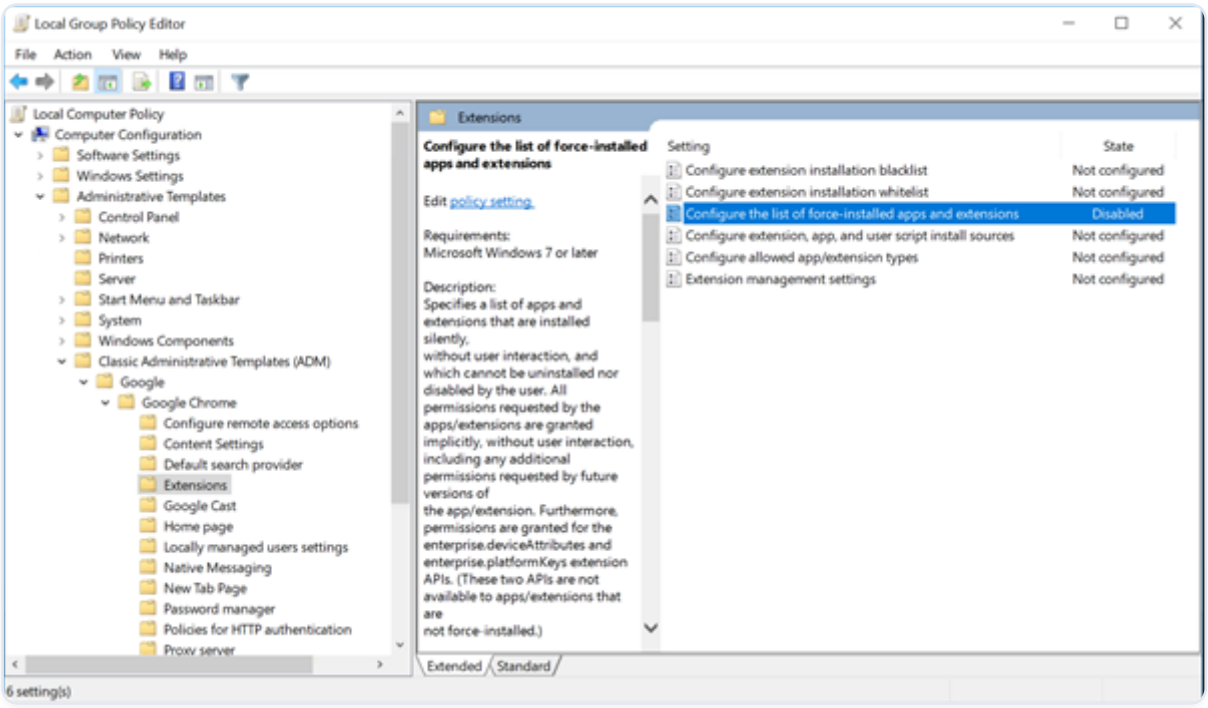
浏览器内容重定向仅在 Citrix Workspace 应用程序 for Windows 的当前版本上受支持，但在 Citrix Workspace 应用程序 LTSR 版本 1912 和 2203.1 上不受支持。




这种方法适用于单个用户。要将扩展部署到组织中的大量用户，请使用组策略部署扩展。

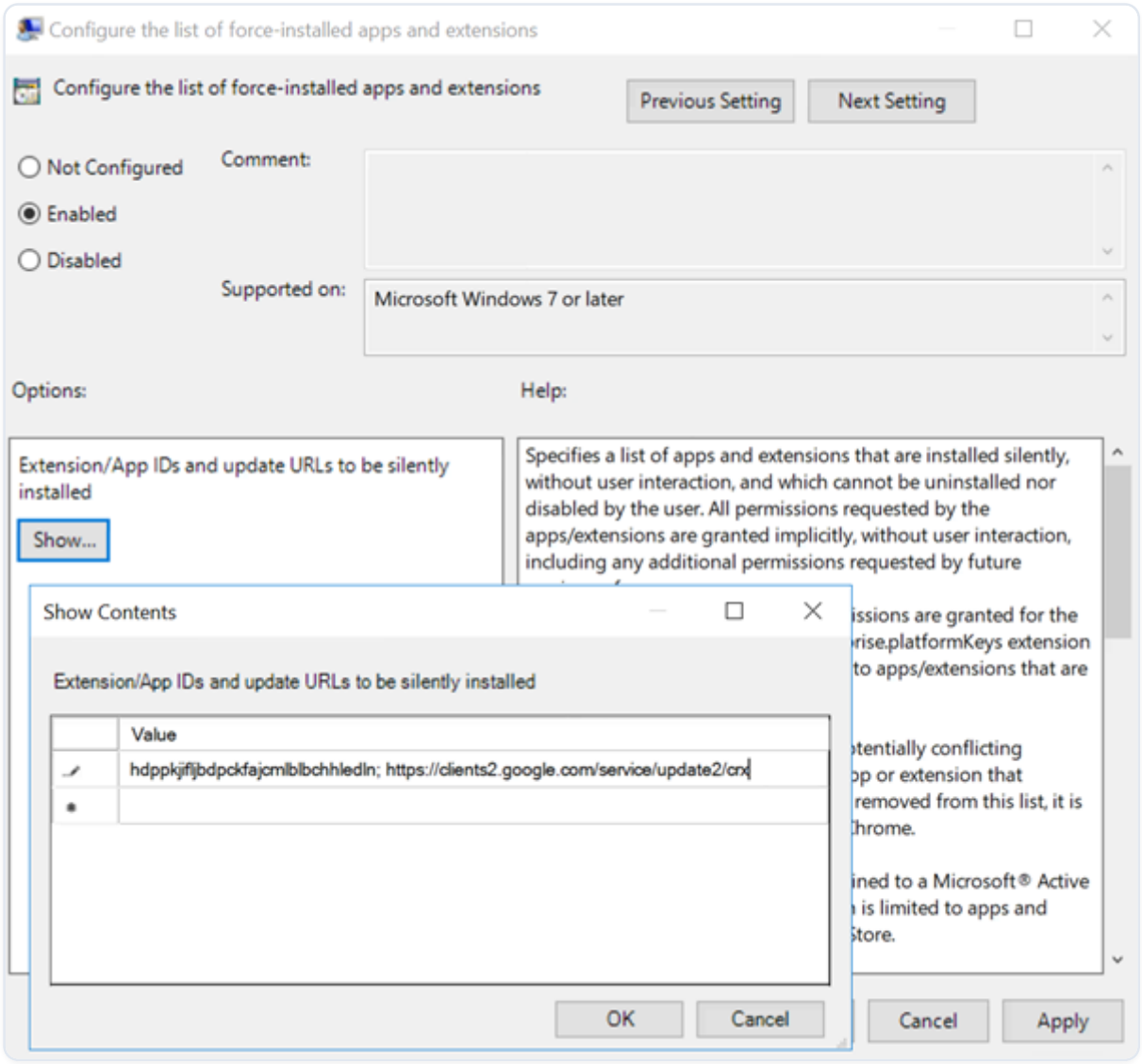
### 使用组策略部署扩展

1. 将 Google Chrome ADMX 文件导入您的环境。有关下载策略模板以及在组策略编辑器中安装和配置模板的信息，请参阅 在托管 PC 上设置 Chrome 浏览器策略。
2. 打开组策略管理控制台，然后转到 **用户配置 \ 管理模板\经典管理模板 (ADM) \ Google\ Google Chrome \ 扩展程序**。启用 **配置强制安装的应用程序和扩展程序列表** 设置。




3. 单击 **显示** 并键入以下字符串，该字符串对应于扩展程序 ID。更新浏览器内容重定向扩展程序的 URL。

   `hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx`




4. 应用此设置，并在 **gpupdate** 刷新后，用户将自动收到此扩展程序。如果您在用户会话中启动 Chrome 浏览器，则该扩展程序已应用，并且用户无法将其删除。

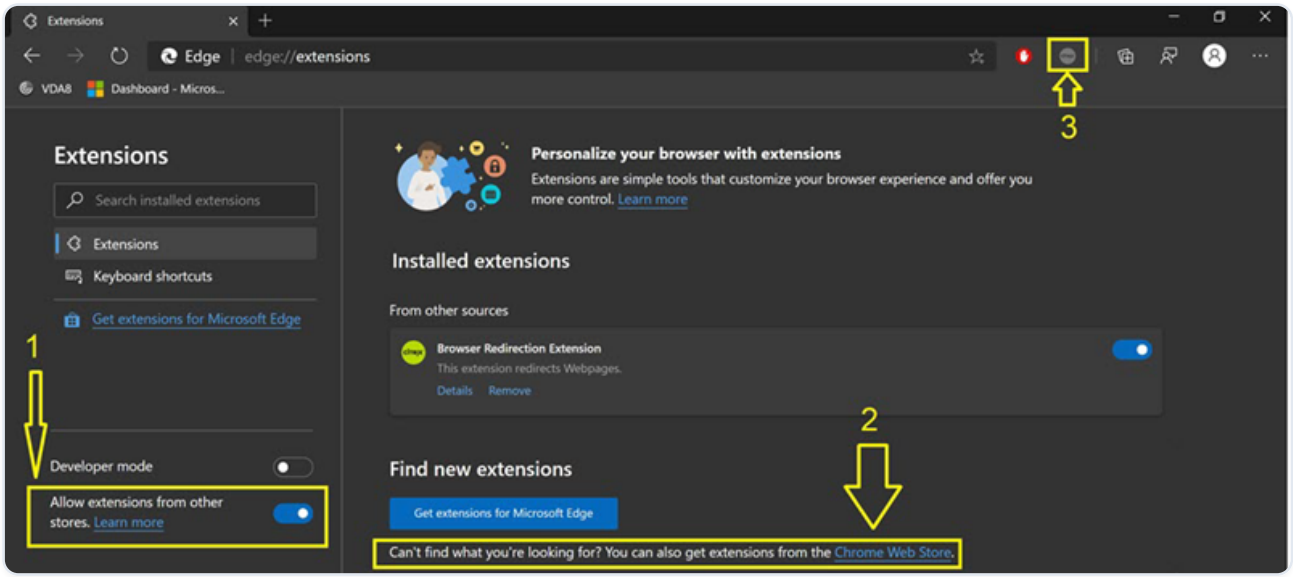
   扩展程序的任何更新都将通过您在设置中指定的更新 URL 自动安装到用户的计算机上。

   如果 **配置强制安装的应用程序和扩展程序列表** 设置为 **禁用**，则该扩展程序将自动从所有用户的 Chrome 中删除。

## 浏览器内容重定向 Edge Chromium 扩展程序

要在 Edge 中安装浏览器内容重定向扩展程序，请确保已安装版本为 **83.0.478.37** 或更高版本的 Edge 浏览器。

1. 单击 **扩展程序** 选项。选择 **管理扩展程序**。开启 **允许来自其他商店的扩展程序**。
2. 单击 **Chrome 网上应用店** 链接，扩展程序将显示在右上角的栏中。 有关 Microsoft Edge 扩展程序的更多信息，请参阅 扩展程序。




## 浏览器内容重定向和 DPI

当在用户计算机上使用浏览器内容重定向且 DPI（缩放）设置为 100% 以上时，重定向的浏览器内容屏幕显示不正确。为避免此问题，在使用浏览器内容重定向时不要设置 DPI。避免此问题的另一种方法是，通过在用户计算机上创建注册表项来禁用 Chrome 浏览器内容重定向 GPU 加速。有关信息，请参阅注册表管理的功能列表中的 浏览器内容重定向和 DPI。

## 使用集成 Windows 身份验证的单点登录

浏览器内容重定向增强了覆盖层，以便对与 VDA 位于同一域中且配置了集成 Windows 身份验证 (IWA) 的 Web 服务器进行身份验证时使用协商方案。

默认情况下，浏览器内容重定向使用基本身份验证方案，该方案要求用户每次访问 Web 服务器时都使用其 VDA 凭据进行身份验证。对于单点登录，您可以启用**浏览器内容重定向集成 Windows 身份验证支持**策略设置，或在 VDA 上创建注册表项。

在启用单点登录之前，请完成以下操作：

- 配置 Kerberos 基础结构以颁发从主机名构建的服务主体名称 (SPN) 的票证。例如，`HTTP/serverhostname.com`。
- 对于服务器提取：当您在服务器提取模式下使用浏览器内容重定向时，请确保在 VDA 上正确配置了 DNS。
- 对于客户端提取：当您在客户端提取模式下使用浏览器内容重定向时，请确保在客户端设备上正确配置了 DNS，并且允许从覆盖层到 Web 服务器 IP 地址的 TCP 连接。

要使用浏览器内容重定向策略配置单点登录，请参阅 浏览器内容重定向集成 Windows 身份验证支持 设置。

此外，您可以通过在 VDA 上添加注册表项来启用对 Web 服务器的单点登录。有关信息，请参阅注册表管理的功能列表中的 使用集成 Windows 身份验证实现浏览器内容重定向的单点登录。

### User-agent 请求标头

user-agent 标头有助于识别从浏览器内容重定向发送的 HTTP 请求。此设置在配置代理和防火墙规则时非常有用。例如，如果服务器阻止了从浏览器内容重定向发送的请求，则可以创建包含 user-agent 标头的规则以绕过某些要求。

只有 Windows 设备支持 user-agent 请求标头。

默认情况下，user-agent 请求标头字符串处于禁用状态。要为客户端呈现的内容启用 user-agent 标头，请使用注册表编辑器。有关信息，请参阅注册表管理的功能列表中的 User-agent 请求标头。

### 浏览器内容重定向客户端兼容性

您可以使用 WMI 检查您的客户端是否与浏览器内容重定向兼容。任何访问 WMI 的方法都适用。以下是使用 PowerShell 的示例。

1. 打开 PowerShell。
2. 运行 `Get-WmiObject -Class CTXBCRStatus`。
3. 检查 `BCR_Capable` 参数。
    - 如果 `True`，则客户端与浏览器内容重定向兼容。
    - 如果 `False`，则客户端与浏览器内容重定向不兼容。

#### 附加信息

- 如果 `CtxBrowserSvc` 不可用，则运行命令时不会显示任何结果。
- 如果 `CtxBrowserSvc` 从未运行过，则结果将返回无效类错误。

## HDX™ 视频会议和网络摄像头视频压缩

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

> 虚拟会话中运行的应用程序可以通过使用 HDX 网络摄像头视频压缩或 HDX 即插即用通用 USB 重定向来使用网络摄像头。使用 **Citrix Workspace™ app > 首选项 > 设备** 在模式之间切换。如果可能，Citrix 建议您始终使用 HDX 网络摄像头视频压缩。仅当 HDX 视频压缩存在应用程序兼容性问题或需要网络摄像头的高级本机功能时，才建议使用 HDX 通用 USB 重定向。为了获得更好的性能，Citrix 建议虚拟投递代理 (VDA) 至少具有两个虚拟 CPU。

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

## HDX 网络摄像头视频压缩

HDX 网络摄像头视频压缩也称为**优化**网络摄像头模式。这种类型的网络摄像头视频压缩将 H.264 视频直接发送到虚拟会话中运行的视频会议应用程序。为了优化 VDA 资源，HDX 网络摄像头压缩不会对网络摄像头视频进行编码、转码和解码。此功能默认启用。

要禁用从服务器到视频会议应用程序的直接视频流，请将 VDA 上的注册表项设置为 0。有关信息，请参阅注册表管理的特性列表中的 网络摄像头视频压缩。

如果禁用视频资源流的默认功能，HDX 网络摄像头视频压缩将使用客户端操作系统中的多媒体框架技术来拦截来自捕获设备的视频，并对其进行转码和压缩。捕获设备制造商提供插入操作系统内核流式处理架构的驱动程序。

客户端处理与网络摄像头的通信。然后，客户端仅将视频发送到可以正确显示它的服务器。服务器不直接处理网络摄像头，但其集成可在您的桌面上提供相同的体验。Workspace 应用程序会压缩视频以节省带宽，并在 WAN 场景中提供更好的弹性。

网络摄像头压缩(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/webcam-compression.png)

HDX 网络摄像头视频压缩要求启用以下策略设置（所有设置默认均已启用）。

- 多媒体会议
- Windows Media 重定向

如果网络摄像头支持硬件编码，HDX 视频压缩默认使用硬件编码。硬件编码可能比软件编码消耗更多带宽。要强制进行软件压缩，请编辑客户端上的注册表项。有关信息，请参阅注册表管理的特性列表中的 网络摄像头软件压缩。

### HDX 网络摄像头视频压缩要求

HDX 网络摄像头视频压缩支持以下版本的 Citrix Workspace 应用程序：

| 平台 | 处理器 |
| --- | --- |
| 适用于 Windows 的 Citrix Workspace 应用程序 | 适用于 Windows 的 Citrix Workspace 应用程序支持 XenApp 和 XenDesktop 7.17 及更高版本上的 32 位和 64 位应用程序的网络摄像头视频压缩。在早期版本中，适用于 Windows 的 Citrix Workspace 应用程序仅支持 32 位应用程序。 |
| 适用于 Mac 的 Citrix Workspace 应用程序 | 适用于 Mac 的 Citrix Workspace 应用程序 2006 或更高版本支持 XenApp 和 XenDesktop 7.17 及更高版本上的 64 位应用程序的网络摄像头视频压缩。在早期版本中，适用于 Mac 的 Citrix Workspace 应用程序仅支持 32 位应用程序。 |
| 适用于 Linux 的 Citrix Workspace 应用程序 | 适用于 Linux 的 Citrix Workspace 应用程序在虚拟桌面上仅支持 32 位应用程序。 |
| 适用于 Chrome 的 Citrix Workspace 应用程序 | 由于某些 ARM Chromebook 不支持 H.264 编码，因此只有 32 位应用程序才能使用优化的 HDX 网络摄像头视频压缩。 |

基于 Media Foundation 的视频应用程序在 Windows 8.x 或更高版本以及 Windows Server 2012 R2 或更高版本上支持 HDX 网络摄像头视频压缩。有关详细信息，请参阅知识中心文章 CTX132764。

其他用户设备要求：

- 产生声音的适当硬件。
- DirectShow 兼容网络摄像头（使用网络摄像头默认设置）。支持硬件编码的网络摄像头可降低客户端 CPU 使用率。
- 对于 HDX 网络摄像头视频压缩，如果可能，请在客户端上安装从摄像头制造商处获取的网络摄像头驱动程序。服务器上不需要安装设备驱动程序。

不同的网络摄像头提供不同的帧速率，并具有不同的亮度和对比度级别。调整网络摄像头的对比度可以显著减少上行流量。Citrix 使用以下网络摄像头进行初始功能验证：

- Microsoft LifeCam VX 型号（2000、3000、5000、7000）
- 创新 Live! 摄像头 Optia Pro
- 罗技 QuickCam Messenger
- 罗技 C600, C920

- HP Deluxe 网络摄像头

要调整首选视频帧速率，请编辑客户端上的注册表项。有关信息，请参阅注册表管理的功能列表中的 网络摄像头视频压缩帧速率。

### 高清网络摄像头流式传输

服务器上的视频会议应用程序根据支持的格式类型选择网络摄像头格式和分辨率。会话启动时，客户端会将网络摄像头信息发送到服务器。从应用程序中选择一个网络摄像头。当网络摄像头和视频会议应用程序支持高清渲染时，应用程序将使用高清分辨率。我们支持高达 1920x1080 的网络摄像头分辨率。

此功能需要适用于 Windows 的 Citrix Workspace 应用程序（最低版本 1808）或适用于 Windows 的 Citrix Receiver（最低版本 4.10）。

您可以使用注册表项禁用和启用此功能。有关信息，请参阅注册表管理的功能列表中的 高清网络摄像头流式传输。

如果媒体类型协商失败，HDX 将回退到 352x288 CIF 的默认分辨率。您可以使用客户端上的注册表项来配置默认分辨率。确保摄像头支持指定的分辨率。有关信息，请参阅注册表管理的功能列表中的高清网络摄像头分辨率。

HDX 网络摄像头视频压缩与即插即用通用 USB 重定向相比，使用的带宽显著减少，并且在 WAN 连接上运行良好。要调整带宽，请在客户端上设置注册表项。有关信息，请参阅注册表管理的特性列表中的 高清网络摄像头带宽。

输入每秒位数的值。如果未指定带宽，视频会议应用程序默认使用 350000 bps。

### HDX 即插即用通用 USB 重定向

HDX 即插即用通用 USB 重定向（同步）也称为**通用**网络摄像头模式。HDX 即插即用通用 USB 重定向的优点是您无需在瘦客户端/端点上安装驱动程序。USB 堆栈是虚拟化的，因此您插入本地客户端的任何设备都会发送到远程 VM。远程桌面表现得就像您本地插入了设备一样。Windows 桌面处理与硬件的所有交互，并通过即插即用逻辑查找正确的驱动程序。如果服务器上存在驱动程序，大多数网络摄像头都可以工作，并且可以通过 ICA 工作。通用网络摄像头模式使用显著更多的带宽（每秒数兆比特），因为您通过网络使用 USB 协议发送未压缩的视频。

## HTML5 多媒体重定向

HTML5 多媒体重定向扩展了 HDX™ MediaStream 的多媒体重定向功能，以包括 HTML5 音频和视频。由于多媒体内容在线分发的增长，尤其是针对移动设备，浏览器行业开发了更高效的音频和视频呈现方式。

Flash 曾是标准，但它需要插件，并非在所有设备上都可用，并且在移动设备上电池使用量更高。像 YouTube、Netflix 以及 Mozilla、Google 和 Microsoft 的新版浏览器等公司正在转向 HTML5，使其成为新标准。

基于 HTML5 的多媒体相对于专有插件具有许多优势，包括：

- 独立于公司的标准 (W3C)
- 简化的数字版权管理 (DRM) 工作流程
- 更好的性能，没有插件带来的安全问题

## HTTP 渐进式下载

HTTP 渐进式下载是一种基于 HTTP 的伪流式传输方法，支持 HTML5。在渐进式下载中，浏览器在从 HTTP Web 服务器下载单个文件（以单一质量编码）时播放该文件。视频在接收时存储到驱动器中，并从驱动器播放。如果您重新观看视频，浏览器可以从缓存加载视频。

有关渐进式下载的示例，请参阅 HTML5 视频重定向测试页面。要检查网页中的视频元素并在 HTML5 视频标签中查找源（mp4 容器格式），请使用浏览器中的开发人员工具：

## 比较 HTML5 和 Flash

| 功能 | HTML5 | 闪存 |
| --- | --- | --- |
| 需要专有播放器 | 否 | 是 |
| 在移动设备上运行 | 是 | 部分 |
| 在不同平台上的运行速度 | 高 | 慢 |
| iOS 支持 | 是 | 否 |
| 资源使用情况 | 较少 | 较多 |
| 加载更快 | 是 | 否 |

## 要求

我们仅支持 mp4 格式的渐进式下载重定向。我们不支持 WebM 和 DASH/HLS 等自适应比特率流技术。

我们支持以下功能，并使用策略来控制它们。有关详细信息，请参阅多媒体策略设置。

- 服务器端渲染

- 服务器获取客户端渲染
- 客户端获取和渲染

Citrix Workspace™ 应用程序和 Citrix Receiver™ 的最低版本：

- 适用于 Windows 的 Citrix Workspace 应用程序 1808
- 适用于 Windows 的 Citrix Receiver 4.5
- 适用于 Linux 的 Citrix Workspace 应用程序 1808
- 适用于 Linux 的 Citrix Receiver 13.5

| 最低 VDA 浏览器版本 | WINDOWS 操作系统版本、内部版本、服务包 |
| --- | --- |
| Internet Explorer 浏览器 11.0 | Windows 10 32位 (1607 RS1) 和 64位 (1607 RS1)；Windows 7 32位 和 64位；Windows 服务器 2016 RTM 14393 (1607)；Windows 服务器 2012 R2 |
| Firefox 47 手动将证书添加到 Firefox 证书存储，或将 Firefox 配置为从 Windows 信任的证书存储中搜索证书。有关详细信息，请参阅 `https://wiki.mozilla.org/CA:AddRootToFirefox` | Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1)；Windows 7 x86 和 x64；Windows 服务器 2016 正式发布版本 14393 (1607)；Windows 服务器 2012 R2 |
| 谷歌浏览器 51 | Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1)；Windows 7 x86 和 x64；Windows 服务器 2016 正式发布版本 14393 (1607)；Windows 服务器 2012 R2 |

## HTML5 视频重定向解决方案的组件

- **HdxVideo.js** - 拦截网站上视频命令的 JavaScript 挂钩。HdxVideo.js 使用安全 WebSocket (SSL/TLS) 与 WebSocketService 通信。
- **WebSocket SSL 证书**
  - 对于 CA（根）：**Citrix XenApp/XenDesktop HDX 产品内 CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA) 位置：**证书 (本地计算机) > 受信任的根证书颁发机构 > 证书**。

  - 对于最终实体（叶）：**Citrix XenApp/XenDesktop HDX 服务** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service) 位置：**证书 (本地计算机) > 个人 > 证书**。

- **WebSocketService.exe** - 在本地系统上运行，执行 SSL 终止和用户会话映射。TLS 安全 WebSocket 侦听 127.0.0.1 端口 9001。
- **WebSocketAgent.exe** - 在用户会话上运行，并根据 WebSocketService 命令的指示呈现视频。

### 如何启用 HTML5 视频重定向?

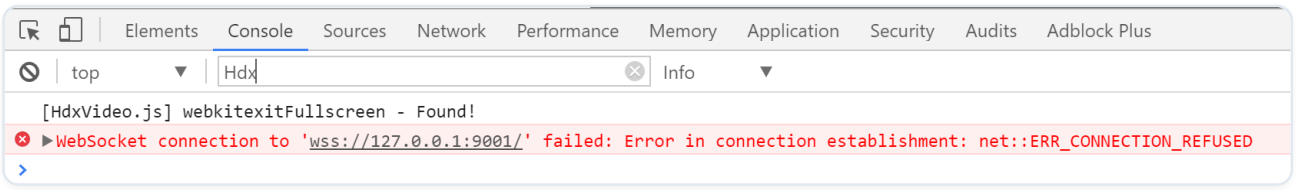
在此版本中，此功能仅适用于受控网页。它要求将 HdxVideo.js JavaScript（包含在 Citrix Virtual Apps and Desktops 安装介质中）添加到提供 HTML5 多媒体内容的网页中。例如，内部培训站点上的视频。

不支持基于自适应比特率技术（例如，HTTP Live Streaming (HLS) 和 Dynamic Adaptive Streaming over HTTP (DASH)）的网站，例如 youtube.com。

有关详细信息，请参阅 *多媒体策略设置*。

### 故障排除提示

当网页尝试运行 HdxVideo.js 时，可能会发生错误。如果 JavaScript 加载失败，HTML5 重定向机制也会失败。通过检查浏览器开发人员工具窗口中的控制台，确保没有与 HdxVideo.js 相关的错误。例如：




## Microsoft Teams（经典版）优化

Citrix 使用 Citrix Virtual Apps and Desktops™ 和 Citrix Workspace™ 应用程序为基于桌面的 Microsoft Teams 提供优化。默认情况下，我们将所有必需的组件捆绑到 Citrix Workspace 应用程序和虚拟投递代理 (VDA) 中。

我们对 Microsoft Teams 的优化包括 VDA 端的 HDX™ 服务以及一个用于与 Microsoft Teams 托管应用程序接口以接收命令的 API。这些组件会打开一个控制虚拟通道 (CTXMTOP) 到 Citrix Workspace 应用程序端的媒体引擎。端点在本地解码并提供多媒体，将 Citrix Workspace 应用程序窗口移回托管的 Microsoft Teams 应用程序中。

身份验证和信令在 Microsoft Teams 托管应用程序上本地发生，就像其他 Microsoft Teams 服务（例如聊天或协作）一样。音频/视频重定向不会影响它们。

`CTXMTOP` 是一个命令和控制虚拟通道。这意味着媒体不会在 Citrix Workspace 应用程序和 VDA 之间交换。

仅支持客户端获取/客户端渲染。

此视频演示让您了解 Microsoft Teams 在 Citrix 虚拟环境中的工作方式。

## 微软团队安装

Citrix 和 Microsoft 建议使用最新版本的 Microsoft Teams 并保持其更新。 发布日期比当前版本发布日期早 90 天以上的 Microsoft Teams 桌面应用程序版本不受支持。 不受支持的 Microsoft Teams 桌面应用程序版本会向用户显示阻止页面，并要求更新应用程序。

有关最新可用版本的信息，请参阅 Teams 应用（桌面和 Mac）的更新历史记录。

> **注意：**
>
> 建议在黄金映像中安装 Microsoft Teams 之前安装 VDA。此安装顺序是为了使 **ALLUSER=1** 标志生效。如果您在安装 VDA 之前已在虚拟机中安装 Microsoft Teams，请卸载并重新安装 Microsoft Teams。如果您正在使用 App Layering，请参阅 有关 App Layering 以了解更多详细信息。

> 建议您遵循 Microsoft Teams 计算机范围安装指南。此外，请避免使用将 Microsoft Teams 安装到 `AppData` 的 .exe 安装程序。相反，请通过命令行使用 **ALLUSER=1** 标志将其安装到 `C:\Program Files (x86)\Microsoft\Teams`。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

此示例还使用了 **ALLUSERS=1** 参数。设置此参数后，Microsoft Teams 计算机范围安装程序将显示在“**控制面板**”中的“**程序和功能**”下。此外，它还会显示在计算机所有用户的 Windows 设置中的“**应用和功能**”下。如果所有用户都具有管理员凭据，则可以卸载 Microsoft Teams。

了解 **ALLUSERS=1** 和 **ALLUSER=1** 之间的区别非常重要。您可以在非 VDI 和 VDI 环境中使用 **ALLUSERS=1** 参数。仅在 VDI 环境中使用 **ALLUSER=1** 参数来指定每计算机安装。

在 **ALLUSER=1** 模式下，Microsoft Teams 应用程序在新版本发布时不会自动更新。我们建议将此模式用于非持久性环境，例如 Windows Server 或 Windows 10 随机/池化目录中的托管共享应用程序或桌面。有关详细信息，请参阅 使用 MSI 安装 Microsoft Teams（VDI 安装部分）。

假设您有 Windows 10 专用持久性 VDI 环境。您希望 Microsoft Teams 应用程序自动更新，并希望 Microsoft Teams 以每用户方式安装在 `Appdata/Local` 下。在这种情况下，请使用 `.exe` 安装程序或不带 **ALLUSER=1** 的 MSI。

## 适用于远程电脑访问

我们建议您在安装 VDA 后安装 Microsoft Teams 版本 1.4.00.22472 或更高版本。否则，您需要注销并重新登录，Microsoft Teams 才能按预期检测到 VDA。版本 1.4.00.22472 及更高版本包含在 Microsoft Teams 启动时和登录时运行的增强逻辑，用于 VDA 检测。这些版本还包括活动会话类型识别（HDX、RDP 或本地连接到客户端计算机）。如果您是本地连接，以前版本的 Microsoft Teams 可能无法检测并禁用某些功能或 UI 元素。例如，分组讨论室、会议和聊天弹出窗口或会议反应。

在某些远程电脑访问场景中，当您从支持 HDX 优化的新端点重新连接到以前未优化的会话时，您可能需要重新启动 Microsoft Teams 以支持 HDX 优化。

## 对于应用程序分层

如果使用 Citrix App Layering 在不同层中管理 VDA 和 Microsoft Teams 安装，请在安装带有 **ALLUSER=1** 的 Microsoft Teams 之前，在 Windows VDA 上部署此注册表项。有关信息，请参阅注册表管理的功能列表中的 使用 Citrix App Layering 优化 Microsoft Teams。

## 配置文件管理建议

我们建议将计算机范围安装程序用于 Windows Server 和池化 VDI Windows 10 环境。

当从命令行将 **ALLUSER=1** 标志传递给 MSI（计算机范围安装程序）时，Microsoft Teams 应用程序将安装在 `C:\Program Files (x86)` (~300 MB) 下。该应用程序使用 `AppData\Local\Microsoft\TeamsMeetingAddin` 存储日志，并使用 `AppData\Roaming\Microsoft\Teams` (~600–700 MB) 存储用户特定配置、用户界面元素缓存等。

> **重要提示：**

> 如果您不传递 **ALLUSER=1** 标志，MSI 会将 Teams.exe 安装程序和 `setup.json` 放置在 `C:\Program Files (x86)\Teams Installer` 下。注册表项 (TeamsMachineInstaller) 将添

> 加到：`HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`

> 随后的用户登录将改为触发 **AppData** 中的最终安装。

### 计算机范围安装程序

以下是在 Windows Server 2016 64 位 VM 上安装 Microsoft Teams 计算机范围安装程序所创建的文件夹、桌面快捷方式和注册表示例：

*文件夹：*

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*桌面快捷方式:*

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

*注册表:*

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- 名称: `Teams`
- 类型: `REG_SZ`
- 值: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **注意：**

> 注册表位置因底层操作系统和位数而异。

### 建议

- 我们建议通过删除 Microsoft Teams 注册表项来禁用自动启动。这样做可以防止许多同时发生的登录（例如，在工作日开始时）导致 VM 的 CPU 飙升。

- 如果虚拟桌面没有 GPU/vGPU，我们建议在 Microsoft Teams 的**设置**中设置**禁用 GPU 硬件加速**以提高性能。此设置 ( `"disableGpu":true` ) 存储在 `desktop-config.json` 中的 `%Appdata%\Microsoft\Teams` 。您可以使用登录脚本编辑该文件并将值设置为 **true**。
- 如果使用 Citrix Workspace Environment Management™ (WEM)，请启用**CPU 峰值保护**以管理 Microsoft Teams 的处理器消耗。

### 每用户安装程序

使用 `.exe` 安装程序时，安装过程有所不同。所有文件都放置在 AppData 中。

*文件夹:*

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*桌面快捷方式:*

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

*注册表:*

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

### 最佳实践

最佳实践建议基于用例场景。 在非持久性设置中使用 Microsoft Teams 需要配置文件缓存管理器，以实现高效的 Microsoft Teams 运行时数据同步。通过配置文件缓存管理器，在用户会话期间会缓存适当的用户特定信息。例如，用户特定信息包括用户数据、配置文件和设置。同步以下两个文件夹中的数据：

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

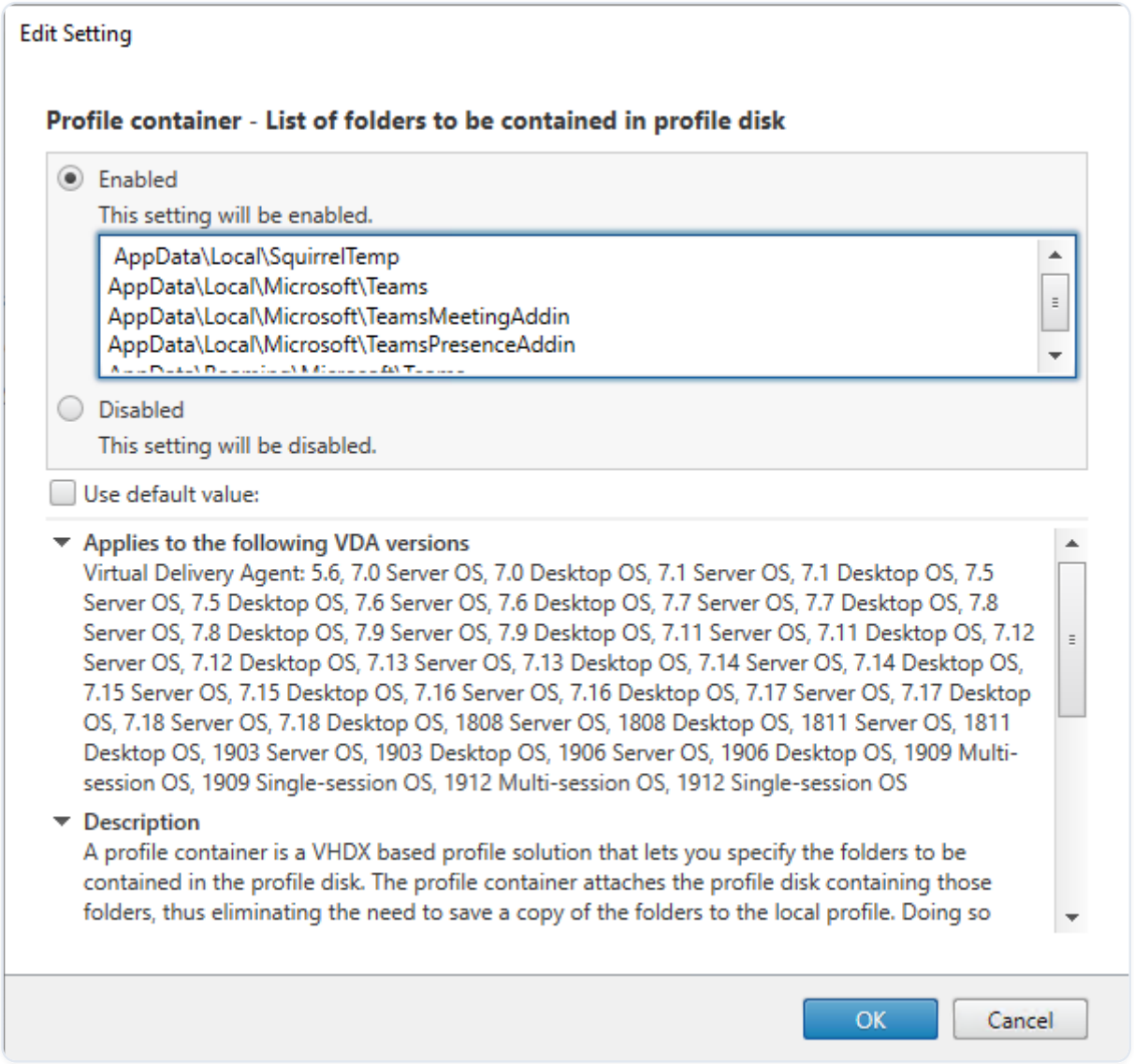
#### Microsoft Teams 缓存内容排除列表，适用于非持久性设置

按照 Microsoft 文档中的说明，从 Microsoft Teams 缓存文件夹中排除文件和目录。此操作有助于减小用户缓存大小，从而进一步优化您的非持久性设置。

**用例：单会话场景**

在此场景中，最终用户一次在一个位置使用 Microsoft Teams。他们不需要同时在两个 Windows 会话中运行 Microsoft Teams。在常见的虚拟桌面部署中，每个用户分配到一个桌面，Microsoft Teams 作为单个应用程序部署在虚拟桌面中。 我们建议启用 Citrix Profile 容器，并将 Per-user installer 中列出的每个用户目录重定向到该容器中。

1. 在黄金映像中部署 Microsoft Teams 机器范围安装程序 (**ALLUSER=1**)。
2. 启用 Citrix Profile Management 并设置具有适当权限的用户配置文件存储。
3. 启用以下 Profile Management 策略设置：**文件系统 > 同步 > 配置文件容器 – 配置文件磁盘中包含的文件夹列表**。




将所有每个用户目录列入此配置。您还可以使用 Citrix Workspace Environment Management (WEM) 服务配置这些设置。

4. 将设置应用于正确的交付组。
5. 登录以验证部署。

# 系统要求

### 最低推荐版本 - Delivery Controller (DDCs) 1906.2

如果您使用的是早期版本，请参阅 启用 Microsoft Teams 优化：

支持的操作系统：

- Windows Server 2022、2019、2016、2012R2 Standard 和数据中心版，以及带 Server Core 选项的版本

### 最低版本 - 虚拟交付代理 (VDA) 1906.2

支持的操作系统：

- 视窗 11。
- Windows 10 64 位，版本 1607 及更高版本。Citrix Workspace 应用程序 2109.1 及更高版本（适用于 Windows）支持 VM 托管应用程序。
- Windows Server 2022、2019、2016 和 2012 R2（Standard 和数据中心版）。

要求：

- BCR_x64.msi - 包含 Microsoft Teams 优化代码并从 GUI 自动启动的 MSI。如果您使用命令行界面进行 VDA 安装，请勿将其排除在外。

### 推荐版本 – 适用于 Windows 的 Citrix Workspace 应用程序最新 CR 和最低版本 - 适用于 Windows 的 Citrix Workspace 应用程序 1907

- 视窗 11。
- Windows 10（32 位和 64 位版本，包括嵌入式版本）（对 Windows 7 的支持已在版本 2006 停止）（对 Windows 8.1 的支持已在版本 2204.1 停止）。
- Windows 10 物联网企业版 2016 LTSB (v1607) 和 2019 LTSC (v1809)。
- 支持的处理器 (CPU) 架构：x86 和 x64（不支持 ARM）。
- 端点要求：大约 2.2–2.4 GHz 双核 CPU，能够在点对点视频会议通话期间支持 720p 高清分辨率。
- 双核或四核CPU，基础速度较低（约1.5 GHz），配备Intel Turbo Boost或AMD Turbo Core，可提升至至少2.4 GHz。
- 经验证的HP瘦客户端：t630/t640、t730/t740、mt44/mt45。
- 经验证的Dell瘦客户端：5070、5470移动TC和一体机。
- 经验证的10ZiG瘦客户端：4510和5810q。

- 有关经验证的端点的完整列表，请参阅瘦客户端。
- Citrix Workspace 应用程序至少需要600 MB可用磁盘空间和1 GB RAM。
- Microsoft .NET Framework 的最低要求是版本4.8。如果系统中不存在 .NET Framework，Citrix Workspace 应用程序将自动下载并安装。

管理员可以通过更改Teams 优化策略来启用/禁用以优化模式启动的Microsoft Teams。在Citrix Workspace 应用程序中以优化模式启动的用户无法禁用Microsoft Teams。

### 最低版本 - 适用于 Linux 的 Citrix Workspace 应用程序 2006

有关详细信息，请参阅适用于 Linux 的 Citrix Workspace app 文档中的Microsoft Teams 优化。

软件：

- `GStreamer` 1.0 或更高版本，或 Cairo 2
- libc++-9.0 或更高版本
- `libgdk` 3.22 或更高版本
- OpenSSL 1.1.1d
- x64 Linux 发行版

硬件：

- 最低 1.8 GHz 双核 CPU，能够在点对点视频会议通话期间支持 720p 高清分辨率
- 双核或四核 CPU，基本速度为 1.8 GHz，Intel Turbo Boost 高速至少为 2.9 GHz

有关已验证端点的完整列表，请参阅瘦客户端。

有关详细信息，请参阅安装 Citrix Workspace 应用程序的必备条件。

您可以通过将 `/opt/Citrix/ICAClient/config/module.ini` 文件中 **VDWEBRTC** 字段的值更新为 Off 来禁用 Microsoft Teams 优化。默认值为 VDWEBRTC=On。更新完成后，重新启动会话。（需要 Root 权限）。

### 最低版本 - 适用于 Mac 的 Citrix Workspace 应用程序 2012

支持的操作系统：

- macOS Catalina (10.15) 版本。
- macOS Big Sur 11.0.1 及更高版本。
- macOS Monterey 版本。

支持的功能：

- 音频
- 视频
- 屏幕共享优化（传入和传出）

> **注意：**
>
> Citrix Viewer 应用程序需要访问 macOS 安全与隐私偏好设置，才能使屏幕共享正常工作。用户可在以下位置配置此偏好设置：**Apple 菜单 > 系统偏好设置 > 安全与隐私 > 隐私选项卡 > 屏幕录制**，并选择 **Citrix Viewer**。

> Microsoft Teams 优化默认情况下适用于 Citrix Workspace 应用程序 2012 及更高版本以及 macOS 10.15。

如果要禁用 Microsoft Teams 优化，请在终端中运行此命令并重新启动 Citrix Workspace 应用程序：

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

### 最低版本 - 在最新版 Chrome OS 上运行的适用于 Chrome OS 的最新版 Citrix Workspace 应用程序

硬件：

- 性能与或优于 Intel i3 四核 2.4 GHz 的处理器。

支持的功能：

- 音频
- 视频
- 屏幕共享优化（传入和传出）- 默认禁用。有关如何启用此功能的说明，请参阅这些设置。

## 单服务器可扩展性

本节提供建议和指导，以估算单个物理主机可支持的用户或虚拟机 (VM) 数量。这通常被称为 Citrix Virtual Apps and Desktops 单服务器可扩展性 (SSS)。在 Citrix Virtual Apps (CVA) 或会话虚拟化中，它也通常被称为用户密度。其目的是找出在运行主要虚拟机管理程序的单个硬件上可以运行多少用户或虚拟机。

**注意：**

本节包含估算 SSS 的指南。请注意，此指南是概括性的，可能不一定适用于您的具体情况或环境。真正了解 Citrix Virtual Apps and Desktops SSS 的唯一方法是使用可伸缩性或负载测试工具，例如 Login VSI。Citrix 建议仅使用此指南和这些简单规则来快速估算 SSS。但是，Citrix 建议使用 Login VSI 或您选择的负载测试工具来验证结果，尤其是在购买硬件或做出任何财务决策之前。

### 硬件（被测系统）

- 戴尔 PowerEdge R740
- Intel Xeon (Gold) 6126 @ 2.60 GHz (最大睿频 3.70 GHz)，每个插槽 12 个核心，双插槽，启用超线程
- 382 GB 内存
- 本地 SSD RAID 0 存储（11 块磁盘）6 TB

### 软件

单个虚拟机（40 个逻辑处理器），运行 Windows 2019 (TSVDA) 和 Citrix Virtual Apps and Desktops 2106 VMware ESXi 6.7

### 术语

- 知识工作者工作负载：包括 Acrobat Reader、Freemind/Java、照片查看器、Edge 以及 MS Office 应用程序，例如 Excel、Outlook、PowerPoint 和 Word。
- 基准：运行知识工作者工作负载（不含 Microsoft Teams）的服务器可伸缩性测试。
- Microsoft Teams 工作负载：知识工作者典型工作负载 + Microsoft Teams。

### Microsoft Teams 如何进行压力测试

- Microsoft Teams 已通过 HDX 优化。因此，所有多媒体处理都卸载到端点或客户端，不属于测量范围。
- 在工作负载启动之前，所有 Microsoft Teams 进程已停止或终止。
- 打开 Microsoft Teams（冷启动）。
- 测量 Microsoft Teams 加载并获取 Microsoft Teams 主窗口焦点所需的时间。
- 使用键盘快捷方式切换到聊天窗口。
- 使用键盘快捷方式切换到日历窗口。

- 使用键盘快捷方式向特定用户发送聊天消息。
- 使用键盘快捷方式切换到 Microsoft Teams 窗口。

### 结果

- 与基线（137 个用户）相比，Microsoft Teams 工作负载（81 个用户）的可伸缩性影响为 40%。
- 将服务器容量增加约 40%（在 CPU 方面）可恢复与基线工作负载相同的用户数量。
- 与基线相比，Microsoft Teams 工作负载需要额外 20% 的内存。
- 将每个用户的存储大小增加 512-1024 MB。
- IOPS 写入增加约 50%，IOPS 读取增加约 100%。Microsoft Teams 对存储速度较慢的环境可能会产生显著影响。

## 功能矩阵和版本支持

| 功能 | MICROSOFT TEAMS（最低版本） | VDA（最低版本） | 适用于 WINDOWS CR 的 CITRIX WORKSPACE 应用程序 | 适用于 WINDOWS 1912 LTSR 的 CITRIX WORKSPACE 应用程序（以及 CU1-CU4） | 适用于 WINDOWS 1912 CU5 的 CITRIX WORKSPACE 应用程序 | 适用于 WINDOWS 1912 CU6（或更高版本）的 CITRIX WORKSPACE 应用程序 | 适用于 MAC 的 CITRIX WORKSPACE 应用程序 | 适用于 LINUX 的 CITRIX WORKSPACE 应用程序 | 适用于 CHROMEOS 的 CITRIX WORKSPACE 应用程序 |
|---|---|---|---|---|---|---|---|---|---|
| 屏幕共享 | 当前版本减去 90 天 | 1906 | 1907 | 是 | 是 | 是 | 2012 | 2006 | 2105.5 (1) |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| i. 屏幕指示器红色边框 | 当前版本减去 90 天 | 1906 | 2002 | 是 | 是 | 是 | 2012 | 2006 | 否 |
| ii. 将捕获限制为 Desktop Viewer | 当前版本减去 90 天 | 1906 | 2009.5 | 否 | 是 | 是 | 2012 | 2006 | 否 |
| 三、多显示器 | 当前版本减去 90 天 | 1906 | 2106 (2) | 否 | 否 | 是 (2) | 2106 | 2106 | 否 |
| DTMF | 当前版本减去 90 天 | N/A | 2102 | 否 | 是 (5) | 是 (5) | 2101 | 2101 | 2111.1 |
| 代理服务器支持 | 当前版本减去 90 天 | N/A | 2012 (3) | 否 | 是 (3) (5) | 是 (3) (5) | 2104 (4) | 2101 (4) | 否 |
| 应用程序共享 | 当前版本减去 90 天 | 2109 | 2109.1 | 否 | 否 | 否 | 2203.1 | 否 | 否 |
| 多窗口 | 1.5.00.11865 | 2112 | 2112.1 | 否 | 否 | 否 | 2203.1 | 2203 | 否 |
| 授予控制权 | 当前版本减去 90 天 | N/A | 2112.1 | 否 | 否 | 否 | 2203.1 | 否 | 否 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 请求控制权 | 当前版本减去 90 天 | N/A | 2112.1 | 否 | 否 | 否 | 2203.1 | 否 | 否 |
| 实时字幕 | 当前版本减去 90 天 | N/A | 2109.1 | 否 | 否 | 否 | 2109 | 2109 | 否 |
| 动态 e911 | 当前版本减去 90 天 | N/A | 2112.1 | 否 | 否 | 否 | 2112 | 2112 | 2112 |

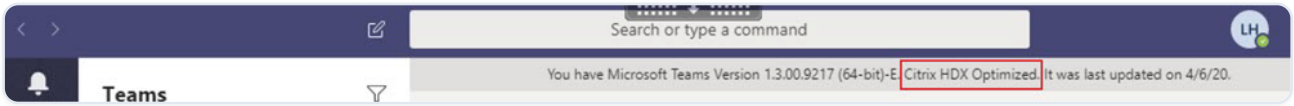
1. 默认禁用，需要管理员启用。
2. CD Viewer 仅在全屏模式下。不支持 SHIFT+F2。
3. Negotiate/Kerberos、NTLM、Basic 和 Digest。也支持 `Pac` 文件。
4. 仅匿名。
5. 仅适用于 Windows 10、Windows IoT 客户端操作系统。
6. Microsoft Teams 中目前不可用的功能。有关预计到达时间 (ETA) 的信息，请参阅 Microsoft 页面。

## 启用 Microsoft Teams 优化

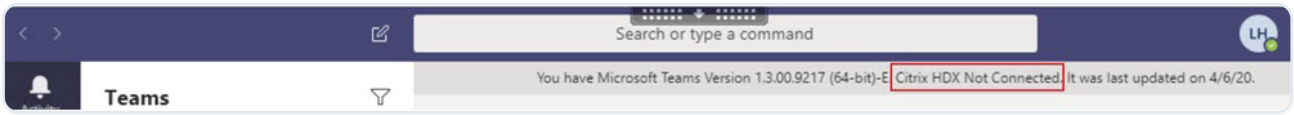
要为 Microsoft Teams 启用优化，请使用 Microsoft Teams 重定向 策略中描述的管理控制台策略。此策略默认情况下处于 **ON** 状态。除了启用此策略之外，HDX 还会检查以验证 Citrix Workspace 应用程序的版本是否至少达到最低要求版本。如果启用了该策略并且 Citrix Workspace 应用程序版本受支持，则 VDA 上的 **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** 将自动设置为 **1**。Microsoft Teams 读取该密钥以在 VDI 模式下加载。

> **注意：**
>
> 如果您使用的是 1906.2 或更高版本的 VDA，或者使用的是在“管理”控制台 (Studio) 中没有可用策略的旧控制器版本（例如，版本 7.15），您的 VDA 仍然可以进行优化。VDA 中默认启用 Microsoft Teams 的 HDX 优化。

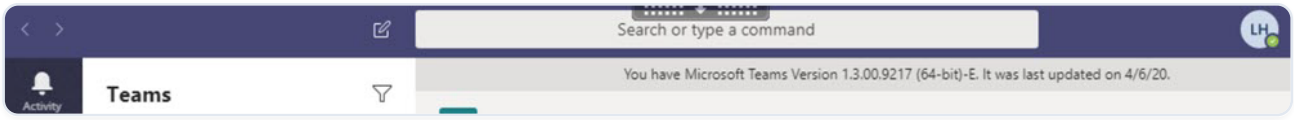
如果单击“**关于 > 版本**”，则会显示“**Citrix HDX 已优化**”图例：




如果看到“**Citrix HDX 未连接**”，则表示 Citrix API 已加载到 Microsoft Teams 中。加载 API 是重定向的第一步。但堆栈的后续部分存在错误。该错误很可能出现在 VDA 服务或 Citrix Workspace 应用程序中。




如果未看到任何图例，则表示 Microsoft Teams 未能加载 Citrix API。右键单击通知区域图标并重新启动以退出 Microsoft Teams。确保管理控制台策略未设置为 **Prohibited** 且 Citrix Workspace 应用程序版本受支持。




**重要：会话重新连接**

- 当连接性发生变化时，您可能需要重新启动 Microsoft Teams 才能获得 HDX 优化会话。例如，如果您从不受支持的端点（适用于 iOS、Android 或旧版 Windows/Linux/Mac 的 Workspace 应用程序）漫游到受支持的端点（适用于 Windows/Linux/Mac/ChromeOS/HTML5 的 Workspace 应用程序），反之亦然。
- 如果您已在 VDA 中使用 Microsoft Teams .exe 安装程序安装了该应用程序，则还需要重新启动 Microsoft Teams。.exe 安装程序推荐用于持久性 VDI 部署。在这种情况下，当 HDX 会话处于断开连接状态时，Microsoft Teams 可以自动更新。因此，重新连接到 HDX 会话的用户会发现 Microsoft Teams 未优化运行。
- 当您从本地会话漫游到 HDX 会话时，必须重新启动 Microsoft Teams 以使用 HDX 进行优化。在远程电脑访问方案中需要此操作。

## 网络要求

Microsoft Teams 依赖 Microsoft 365 中的媒体处理器服务器进行会议或多方通话。此外，Microsoft Teams 依赖 Microsoft 365 传输中继来处理以下场景：

- 点对点呼叫中的两个对等方没有直接连接
- 参与者与媒体处理器没有直接连接。

因此，对等方与 Microsoft 365 云之间的网络状况决定了呼叫的性能。有关网络规划的详细指南，请参阅 Microsoft 365 网络连接原则。

我们建议评估您的环境，以识别可能影响您的整体云语音和视频部署的任何风险和要求。 使用 Skype for Business 网络评估工具 测试您的网络是否已为 Microsoft Teams 做好准备。有关支持信息，请参阅 支持。

### 实时传输协议 (RTP) 流量的关键网络建议摘要

- 从分支机构尽可能直接连接到 Microsoft 365 网络。
- 规划并提供分支机构的充足带宽。
- 检查每个分支机构的网络连接和质量。
- 如果必须在分支机构使用以下任何一项，请确保 RTP/UDP 流量（由 Citrix Workspace 应用程序中的 HdxRtcEngine.exe 处理）畅通无阻。
    - 绕过代理服务器
    - 网络 SSL 拦截
    - 深度包检测设备
    - VPN 回环（如果可能，请使用拆分隧道）

> **重要提示：VPN 拆分隧道配置**

> HdxRtcEngine.exe 流量必须从 VPN 隧道中分流，并允许使用用户的本地 Internet 连接直接连接到服务。实现此目的的方式将因所使用的 VPN 产品和机器平台而异，但大多数 VPN 解决方案都允许通过一些简单的策略配置来应用此逻辑。有关 VPN 平台特定拆分隧道指南的更多信息，请参阅 这篇 Microsoft 文章。

> Workspace 应用程序中的 WebRTC 媒体引擎 (HdxRtcEngine.exe) 使用安全实时传输协议 (SRTP) 处理卸载到客户端的多媒体流。SRTP 为 RTP 提供机密性和身份验证。对于此功能，对称密钥（通过 DTLS 协商）用于使用 AES 加密算法加密媒体和控制消息。

建议使用以下指标以获得积极的用户体验：

| 指标 | 端点到 MICROSOFT 365 |
| --- | --- |
| 延迟（单向） | < 50 毫秒 |

| 指标 | 端点到 MICROSOFT 365 |
| --- | --- |
| 延迟 (RTT) | < 100 毫秒 |
| 丢包率 | 在任意 15 秒间隔内 <1% |
| 数据包到达间隔抖动 | 在任意 15 秒间隔内 <30 毫秒 |

有关更多信息，请参阅 为 Microsoft Teams 准备组织网络。

对于带宽要求，Microsoft Teams 优化可以使用各种音频编解码器 (OPUS/G.722/PCM G711) 和视频编解码器 (H264)。

对等方在呼叫建立过程中使用会话描述协议 (SDP) Offer/Answer 协商这些编解码器。 Citrix 对每个用户的最低建议是：

| 类型 | 带宽 | 编解码器 |
| --- | --- | --- |
| 音频（每个方向） | 约 90 kbps | G.722 |
| 音频（每个方向） | 约 60 kbps | 奥普斯* |
| 视频（每个方向） | 约 700 kbps | H264 360p @ 30 帧/秒 16:9 |
| 屏幕共享 | 约 300 kbps | H264 1080p @ 15 帧/秒 |

* Opus 支持从 6 kbps 到 510 kbps 的恒定和可变比特率编码。

Opus 和 H264 是点对点和电话会议的首选编解码器。

**重要提示：**

关于性能，在客户端计算机上，编码比解码更消耗 CPU 资源。您可以在适用于 Linux 和 Windows 的 Citrix Workspace 应用程序中硬编码最大编码分辨率。请参阅 编码器性能估算器 和 Microsoft Teams 优化。

### 思杰网关

本地 Citrix Gateway 或 Citrix Gateway 服务作为 HDX 代理的存在不会影响 Microsoft Teams 优化。这是因为 Workspace 应用程序和 VDA 之间只建立了一个命令和控制虚拟通道。

所有音频或视频流都卸载到客户端进行本地处理。因此，没有服务器端渲染。

根据您环境中的配置，命令和控制虚拟通道通过 Citrix Gateway 流动，使用以下任一方式：

- 用于 TCP 的 TLS
- 用于 EDT 的 DTLS

如果您也使用 Citrix Gateway 进行 VPN，请确保允许客户端计算机直接访问 O365 Microsoft Teams 服务器。您可以通过拆分隧道或其他方法实现此目的。

## 代理服务器

根据代理的位置，请考虑以下事项：

- VDA 上的代理配置：

  如果您在 VDA 中配置了显式代理服务器并通过代理将连接路由到 localhost，则重定向会失败。要正确配置代理，您必须在 **Internet 选项 > 连接 > 局域网设置 > 代理服务器** 中选择 **对于本地地址不使用代理服务器** 设置，并确保 `127.0.0.1:9002` 被绕过。

  如果您使用 PAC 文件，则 PAC 文件中的 VDA 代理配置脚本必须为 `wss://127.0.0.1:9002` 返回 **DIRECT**。否则，优化将失败。为确保脚本返回 **DIRECT**，请使用 `shExpMatch(url, "wss://127.0.0.1:9002/*")`。

- Citrix Workspace 应用程序上的代理配置：

  如果分支机构配置为通过代理访问 Internet，则以下版本支持代理服务器：

  - 适用于 Windows 的 Citrix Workspace 应用程序版本 2012（支持协商/Kerberos、NTLM、Basic 和 Digest。还支持 `Pac` 文件）
  - 适用于 Windows 的 Citrix Workspace 应用程序版本 1912 CU5（支持协商/Kerberos、NTLM、Basic 和 Digest。还支持 `Pac` 文件）
  - 适用于 Linux 的 Citrix Workspace 应用程序版本 2101（匿名身份验证）
  - 适用于 Mac 的 Citrix Workspace 应用程序版本 2104（匿名身份验证）

运行早期版本 Citrix Workspace 应用程序的客户端设备无法读取代理配置。这些设备会将流量直接发送到 Microsoft 365 TURN 服务器。

> **重要提示：**

- 验证客户端设备是否可以连接到 DNS 服务器以执行 DNS 解析。客户端设备必须能够解析以下 Microsoft Teams 中继服务器的 FQDN：
  - `worldaz.relay.teams.microsoft.com`
  - `inaz.relay.teams.microsoft.com`
  - `uaeaz.relay.teams.microsoft.com`
  - `euaz.relay.teams.microsoft.com`
  - `usaz.relay.teams.microsoft.com`
  - `turn.dod.teams.microsoft.us`
  - `turn.gov.teams.microsoft.us`

如果 DNS 请求不成功，与外部用户的 P2P 呼叫和会议呼叫媒体建立将失败。

- 会议服务器的位置是根据第一个参与者的虚拟桌面位置（而不是客户端）选择的。

## 呼叫建立和媒体流路径

在可能的情况下，Citrix Workspace 应用程序中的 HDX WebRTC 媒体引擎 (HdxRtcEngine.exe) 尝试通过用户数据报协议 (UDP) 在点对点呼叫中建立直接网络安全实时传输协议 (SRTP) 连接。如果 UDP 高端口被阻止，媒体引擎将回退到 TCP/TLS 443。

HDX 媒体引擎支持 ICE、NAT 会话遍历实用程序 (STUN) 和使用 NAT 中继遍历 (TURN)，用于候选发现和建立连接。此支持意味着端点必须能够执行 DNS 解析。

设想这样一种情况：两个对等点之间或对等点与会议服务器之间没有直接路径，并且您正在加入多方呼叫或会议。HdxRtcEngine.exe 使用 Microsoft 365 中的 Microsoft Teams 传输中继服务器来连接其他对等点或媒体处理器（会议在此处托管）。您的客户端计算机必须能够访问三个 Microsoft 365 子网 IP 地址范围和四个 UDP 端口（如果 UDP 被阻止，则回退到 TCP/TLS 443）。有关详细信息，请参阅 呼叫设置 和 Office 365 URL 和 IP 地址范围 ID 11 中的体系结构图。

| ID | 类别 | 地址 | 目标端口 |
| --- | --- | --- | --- |
| 11 | 需要优化 | 13.107.64.0/18、52.112.0.0/14、52.120.0.0/14 | **UDP：** 3478、3479、3480、3481，**TCP：** 443（回退） |

这些范围包括传输中继和媒体处理器，由 Azure 负载均衡器前端。 Microsoft Teams 传输中继提供 STUN 和 TURN 功能，但它们不是 ICE 端点。此外，Microsoft Teams 传输中继不终止媒体、TLS 或执行任何转码。当它们将流量转发到其他对等方或媒体处理器时，它们可以将 TCP（如果 HdxRtcEngine.exe 使用 TCP）桥接到 UDP。

Workspace 应用程序 WebRTC 媒体引擎联系 Microsoft 365 云中最近的 Microsoft Teams 传输中继。媒体引擎使用任播 IP 和端口 3478–3481 UDP（每个工作负载使用不同的 UDP 端口，尽管可能发生多路复用）或 443 TCP/TLS 进行回退。呼叫质量取决于底层网络协议。由于 UDP 始终优于 TCP，因此我们建议您设计网络以适应分支机构中的 UDP 流量。

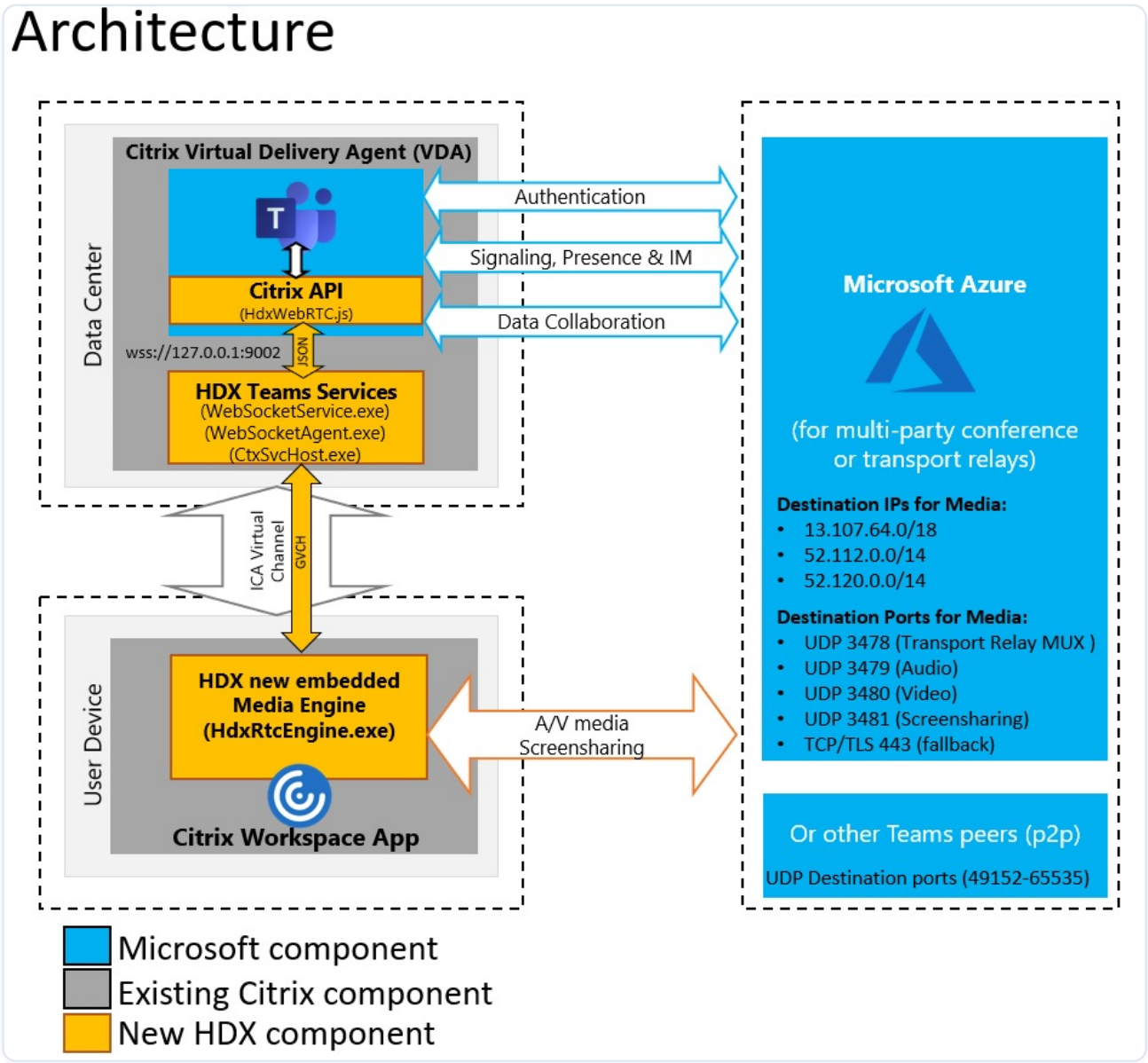
如果 Microsoft Teams 以优化模式加载且 HdxRtcEngine.exe 在端点上运行，则 ICE 故障可能会导致呼叫设置失败或仅单向音频/视频。如果呼叫无法完成或媒体流不是全双工，请首先检查端点上的 **Wireshark 跟踪**。有关 ICE 候选收集过程的更多信息，请参阅 支持 部分中的“收集日志”。

> **注意：**
>
> 如果端点没有互联网访问权限，则如果用户都在同一 LAN 上，他们仍然可以进行点对点呼叫。会议将失败。在这种情况下，呼叫设置开始前会有 30 秒的超时。

### 呼叫设置

使用此架构图作为呼叫流序列的视觉参考。图中指示了相应的步骤。

### 架构




1. 启动 微软团队。
2. Microsoft Teams 向 O365 进行身份验证。租户策略被下发到 Microsoft Teams 客户端，相关的 TURN 和信令通道信息被中继到应用程序。
3. Microsoft Teams 检测到它正在 VDA 中运行，并向 Citrix JavaScript API 发出 API 调用。
4. Microsoft Teams 中的 Citrix JavaScript 打开一个安全的 WebSocket 连接到在 VDA 上运行的 WebSocketService.exe，它在用户会话中生成 WebSocketAgent.exe。
5. WebSocketAgent.exe 通过调用 Citrix HDX Microsoft Teams 重定向服务 (CtxSvcHost.exe) 实例化一个通用虚拟通道。
6. Citrix Workspace 应用程序的 wfica32.exe (HDX 引擎) 生成一个名为 HdxRtcEngine.exe 的新进程，这是用于 Microsoft Teams 优化的新 WebRTC 引擎。
7. Citrix 媒体引擎和 Teams.exe 具有双向虚拟通道路径，可以开始处理多媒体请求。

-----用户呼叫------

8. **对等方 A** 单击“**呼叫**”按钮。Teams.exe 与 Microsoft 365 中的 Microsoft Teams 服务通信，与**对等方 B** 建立端到端信令路径。Microsoft Teams 向 HdxRtcEngine 请求一系列支持的呼叫参数（编解码器、分辨率等，这被称为会话描述协议 (SDP) 提议）。然后，这些呼叫参数通过信令路径中继到 Microsoft 365 中的 Microsoft Teams 服务，并从那里中继到另一个对等方。
9. SDP 要约/应答（单次协商）通过信令通道进行，并且 ICE 连接检查（使用 STUN 绑定请求进行 NAT 和防火墙遍历）完成。然后，安全实时传输协议 (SRTP) 媒体直接在 HdxRtcEngine.exe 和其他对等方之间（如果是会议，则在 HdxRtcEngine.exe 和 Microsoft 365 会议服务器之间）流动。

## Microsoft 电话系统

电话系统是 Microsoft 的技术，它通过 Microsoft Teams 在 Microsoft 365 云中实现呼叫控制和 PBX。Microsoft Teams 优化支持电话系统，使用 Microsoft 365 呼叫计划或直接路由。通过直接路由，您可以将自己支持的会话边界控制器直接连接到 Microsoft 电话系统，而无需任何额外的本地软件。 支持呼叫队列、转接、呼叫转移、保持、静音和恢复呼叫。

### DTMF

双音多频 (DTMF) 功能支持以下版本的 Citrix Workspace 应用程序（及更高版本）：

- 适用于 Windows 版本 2102 的 Citrix Workspace 应用程序
- 适用于 Windows LTSR 1912 CU5 的 Citrix Workspace 应用程序（仅限 Windows 10 操作系统）
- 适用于 Linux 的 Citrix Workspace 应用程序版本 2101
- 适用于 Mac 的 Citrix Workspace 应用程序版本 2101
- 适用于 Chrome OS 的 Citrix Workspace 应用程序版本 2111.1

### 支持动态 e911

从版本 2112 开始，Citrix Workspace 应用程序支持动态紧急呼叫。在 Microsoft Calling Plans、Operator Connect 和 Direct Routing 中使用时，它允许您执行以下操作：

- 配置和路由紧急呼叫。
- 通知安全人员。

通知是根据在端点上运行的 Citrix Workspace 应用程序的当前位置提供的，而不是根据在 VDA 上运行的 Microsoft Teams 客户端的位置提供的。

Ray Baum 法案要求将 911 呼叫者的可调度位置传输到相应的公共安全应答点 (PSAP)。当与以下版本的 Citrix Workspace 应用程序一起使用时，通过 HDX 进行的 Microsoft Teams 优化符合 Ray Baum 法案：

- 适用于 Windows 的 Citrix Workspace 应用程序版本 2112.1 及更高版本
- 适用于 Linux 的 Citrix Workspace 应用程序版本 2112 及更高版本
- 适用于 Mac 的 Citrix Workspace 应用程序版本 2112 及更高版本
- 适用于 Chrome OS 的 Citrix Workspace 应用程序版本 2112 及更高版本

要启用动态紧急呼叫，管理员必须使用 Microsoft Teams 管理中心并配置以下内容以创建网络或紧急位置映射：

- 网络设置
- 位置信息服务 (LIS)

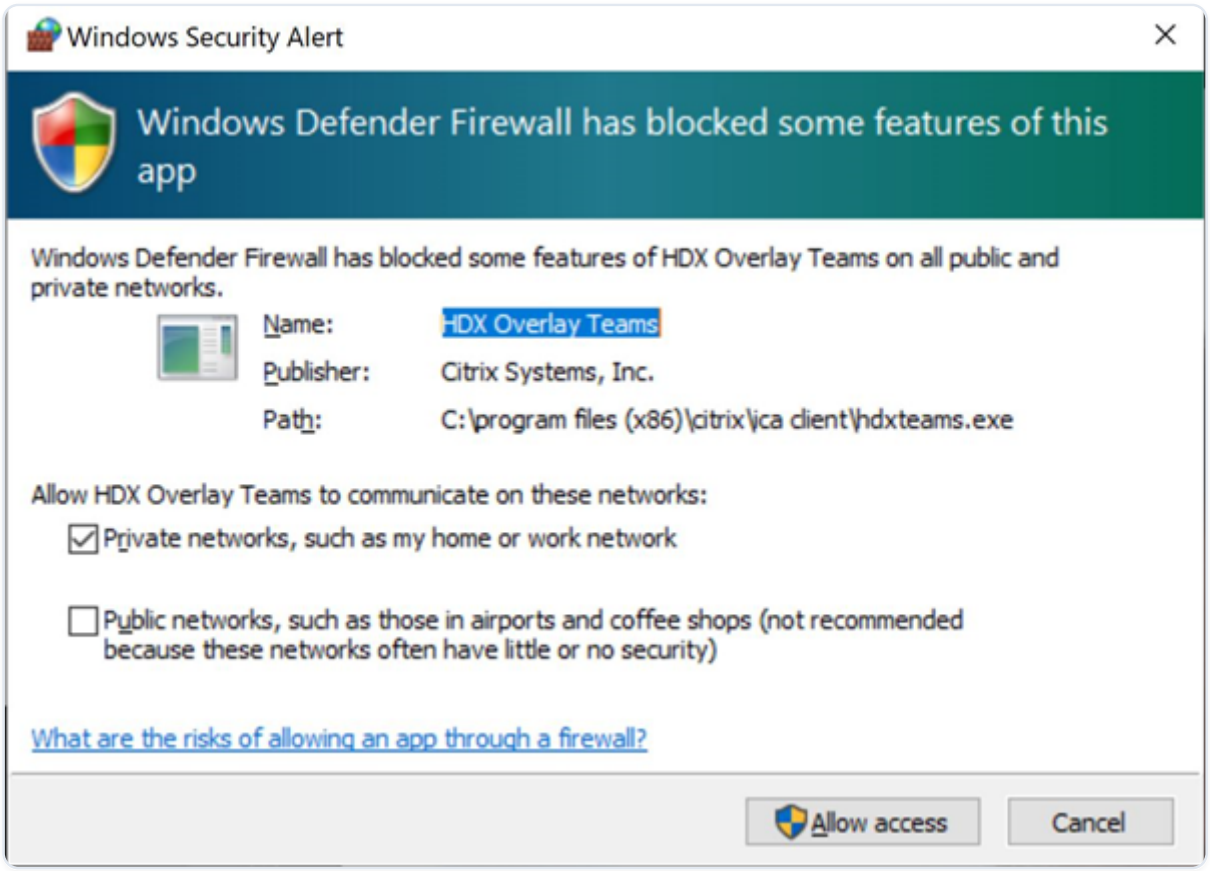
有关动态紧急呼叫的更多信息，请参阅 Microsoft 文档。

Citrix Workspace 应用程序中继到 Microsoft Teams 的可调度位置信息包括：

- 使用链路层发现协议 (LLDP) 的以太网/交换机连接的机箱 ID/端口 ID。以太网/交换机 (LLDP) 支持以下平台：
  - Windows 8.1 和 10 版本
  - macOS，需要 LLDP 启用软件
  - Linux，需要将 LLDP 库包含在瘦客户端的操作系统 (OS) 分发中。
- 安装了 Citrix Workspace 应用程序的端点的 WLAN BBSID 和 {IPv4-IPv6；子网；MAC 地址}。
  - Workspace 应用程序（适用于 Windows、Linux 和 Mac）支持基于子网和 WiFi 的位置。
- 纬度和经度，如果用户在安装 Citrix Workspace 应用程序的操作系统级别授予了权限（权限设置为 HDX RTC Engine）
  - 所有 Workspace 应用程序平台均支持。但是，对于适用于 Linux 的 Citrix Workspace，您必须在瘦客户端的操作系统分发中包含 `libgps` 库（>sudo apt-get install libgps-dev gpsd lldpd）。

## 防火墙注意事项

当用户首次使用 Microsoft Teams 客户端启动优化呼叫时，他们可能会注意到 **Windows 防火墙**设置的警告。该警告要求用户允许 HdxTeams.exe 或 HdxRtcEngine.exe（HDX Overlay Microsoft Teams）进行通信。




以下四个条目已添加到 **Windows Defender 防火墙 > 高级安全** 控制台的 **入站规则** 下。如果需要，您可以应用更严格的规则。

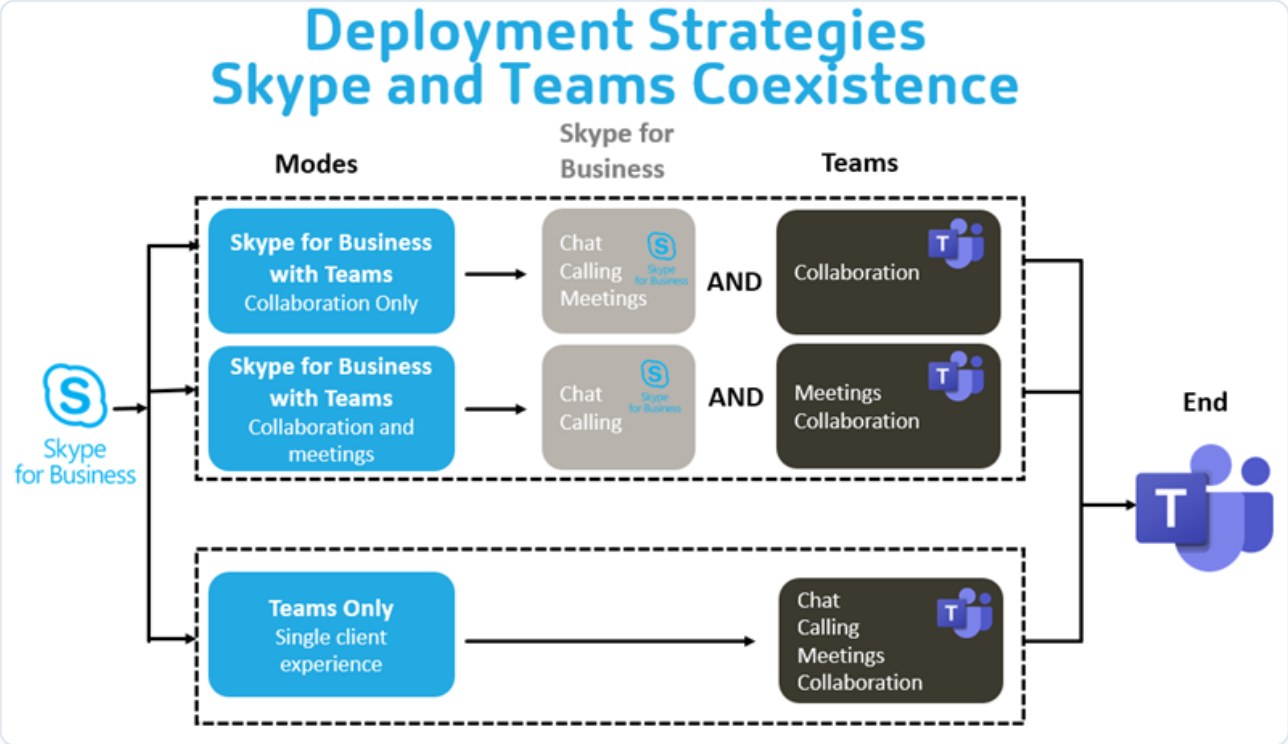
防火墙入站规则 ](/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/firewall2.png)

## 微软团队 和 商务版 Skype 共存

您可以将 Microsoft Teams 和 Skype for Business 作为两个具有重叠功能的独立解决方案并排部署。 有关详细信息，请参阅了解 Microsoft Teams 和 Skype for Business 共存和互操作性。

Citrix RealTime Optimization Pack 和适用于 Microsoft Teams 多媒体引擎的 HDX 优化将遵循您环境中设置的配置。示例包括孤岛模式以及 Skype for Business 与 Microsoft Teams 协作。此外，还包括 Skype for Business 与 Microsoft Teams 协作和会议。

外设访问一次只能授予单个应用程序。例如，RealTime Media Engine 在通话期间访问网络摄像头会锁定成像设备。当设备释放后，它将可用于 Microsoft Teams。




## Citrix SD-WAN™：针对 Microsoft Teams 优化的网络连接

最佳的音频和视频质量需要连接到 Microsoft 365 云的网络，该网络应具有低延迟、低抖动和低数据包丢失。将来自分支机构的 Citrix Workspace 应用程序用户的 Microsoft Teams 音视频 RTP 流量回传到数据中心，然后再传输到互联网，可能会增加过多的延迟。这还可能导致 WAN 链路拥塞。Citrix SD-WAN 遵循 Microsoft 365 网络连接原则，优化了 Microsoft Teams 的连接。Citrix SD-WAN 使用基于 Microsoft REST 的 Microsoft 365 IP 地址和 Web 服务以及近端 DNS。此用途旨在识别、分类和引导 Microsoft Teams 流量。

许多地区的商业宽带互联网连接都存在间歇性数据包丢失、过度抖动和中断的问题。

当网络状况不稳定或降级时，Citrix SD-WAN 提供两种解决方案来保持 Microsoft Teams 音视频质量。

- 如果您使用 Microsoft Azure，部署在 Azure VNET 中的 Citrix SD-WAN 虚拟设备 (VPX) 可提供高级连接优化。这些优化包括无缝链路故障转移和音频数据包竞速。
- Citrix SD-WAN 客户可以通过 Citrix Cloud™ Direct 服务连接到 Microsoft 365。此服务为所有互联网流量提供可靠且安全的传输。

如果分支机构互联网连接质量不是问题，那么最小化延迟可能就足够了。将 Microsoft Teams 流量直接从 Citrix SD-WAN 分支设备引导到最近的 Microsoft 365 前端，以最大程度地减少延迟。有关详细信息，请参阅Citrix SD-WAN Office 365 优化。

思杰 SD-WAN ](/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/sd-wan.png)

## 多窗口会议和聊天

您可以在 Windows 中为 Microsoft Teams 使用多个会议或聊天窗口。有关弹出功能的详细信息，请参阅 Microsoft 365 网站上的Microsoft Teams 聊天和会议弹出窗口。

> **注意：**
>
> 此功能支持适用于 Windows 2112.1、Mac 2203、Linux 2203 的 Citrix Workspace 应用程序以及 VDA 2112。

## Microsoft Teams 中的图库视图和活动发言人

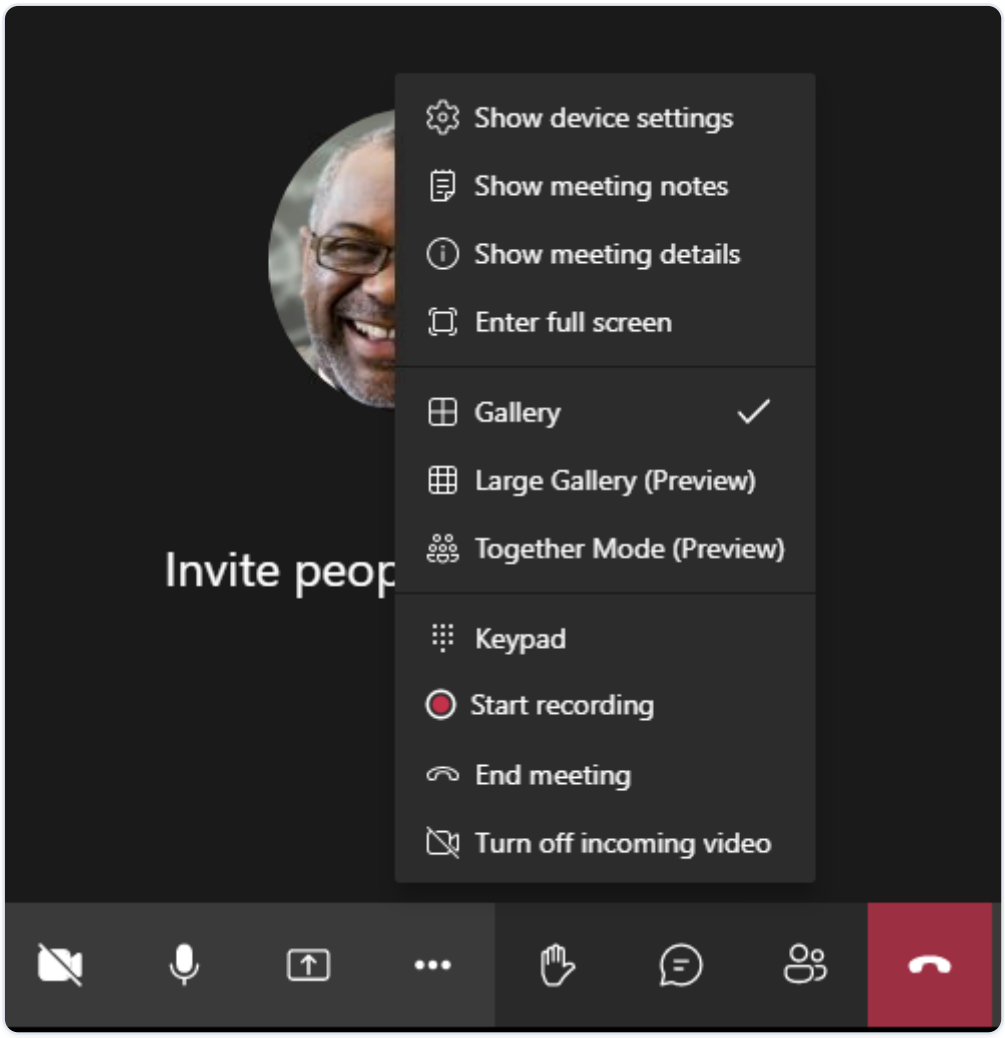
Microsoft Teams 支持 **Gallery**（图库）、**Large gallery**（大型图库）和 **Together mode**（同框模式）布局。

Microsoft Teams 显示一个 2x2 的网格，其中包含四名参与者的视频流（称为 **Gallery**）。在这种情况下，Microsoft Teams 会向客户端设备发送四个视频流进行解码。当超过四名参与者共享视频时，屏幕上只会显示最后四名最活跃的发言人。

Microsoft Teams 还提供最大 7x7 网格的大型图库视图。因此，Microsoft Teams 会议服务器会合成单个视频源并将其发送到客户端设备进行解码，从而降低 CPU 消耗。这种单一的矩阵式视频源也可能包含用户的自预览视频。

最后，Microsoft Teams 支持 **Together mode**（同框模式），这是新会议体验的一部分。Microsoft Teams 使用 AI 分割技术将参与者数字地放置在共享背景中，从而将所有参与者置于同一礼堂中。

用户可以在电话会议期间通过在省略号菜单中选择 **Gallery**（图库）、**Large gallery**（大型图库）或 **Together mode**（同框模式）布局来控制这些模式。




支持视频宽高比限制（适用于 Windows 2102 的 CWA、适用于 Linux 2106 的 CWA、适用于 MAC 2106 及更高版本的 CWA）：

- 在图库/大型图库视图中，可以使用 **Fill to frame**（填充到帧）选项。此选项会裁剪视频大小以使其适合子窗口。另一方面，**Fit to frame**（适应帧）会在视频两侧显示黑边（信箱模式），因此不会进行裁剪。

下表提供了图库和大型图库布局的比较：

| | 图库视图 2X2（默认） | 大型图库视图 |
|---|---|---|
| 布局/网格 | 显示一个 2x2 网格，其中包含四名参与者的视频流。屏幕上仅显示最后四位最活跃的发言者，其他参与者不会显示在网格中。 | 显示一个 7x7 网格，其中包含 49 名参与者的视频流。 |
| 混合技术 | 媒体路由器将每个参与者的单个流转发给每个用户。 | 中央会议服务器混合并转码所有音频或视频，为每个参与者 |

| | 图库视图 2X2（默认） | 大型图库视图 |
|---|---|---|
| | | 创建定制的复合布局。此操作会引入一些额外的延迟。 |
| 活跃发言者 | 新的活跃发言者会替换网格中最不活跃的发言者。 | 显示所有参与者，无论他们是活跃还是不活跃。 |
| 端点编码 | 单个高质量视频流。您可以在客户端上设置编码分辨率值。有关详细信息，请参阅 编码器性能估算器 和 Microsoft Teams 优化。质量定义为分辨率和每秒帧数。目前不支持同步视频。 | 单个高质量视频流。您可以在客户端上设置编码分辨率值。有关详细信息，请参阅 编码器性能估算器 和 Microsoft Teams 优化。 |
| 端点解码 | 每个参与者最多可获得四个独立的媒体流。这会增加端点上 HdxRtcEngine.exe 的 CPU 消耗（用于解码/渲染）。 | 每个参与者只获得一个音频和视频流。此设置可降低端点的 CPU 消耗。 |
| 最大分辨率 | 720p。当四名参与者共享视频时，每个视频源的最大分辨率为 360p。如果共享视频的参与者少于四名，每个视频源的分辨率可能会更高。 | 复合布局或混音为 720p。在复合布局中，每个参与者不需要高质量视频流。由于此条件，每个发送方都会降低分辨率或上传比特率。 |
| “慢速用户”问题 | 发送方将每种模式（音频/视频/屏幕共享）的质量调整为参与者中最低的通用网络质量。然后，此多媒体流会转发给所有其他参与者。因此，网络状况不佳的参与者会影响通话中其他所有人的质量。 | 不易受最低通用网络质量场景的影响。会议服务器根据单个参与者的网络状况提供不同的质量。 |
| 自预览 | 实时以小缩略图显示自己。 | 以缩略图显示自己，并与其余视频源混合。因此，您可能会看到自己被包含在主视频布局中，并带有一些额外的延迟。 |

# Microsoft Teams 中的屏幕共享

Microsoft Teams 依赖于基于视频的屏幕共享 (VBSS)，它使用 H264 等视频编解码器有效地编码共享桌面并创建高清流。通过 HDX 优化，传入的屏幕共享被视为视频流。

从适用于 Windows、Linux 或 Mac 的 Citrix Workspace 应用程序 2109 或更高版本开始，用户可以同时共享其屏幕和视频摄像头。

在早期版本中，如果您正在进行视频通话，而另一位对等方开始共享桌面，则原始摄像头视频源会暂停。取而代之的是显示屏幕共享视频源。然后，对等方必须手动恢复摄像头共享。

> **PowerPoint Live 注意事项**

> 如果您正在从 PowerPoint Live 共享内容，则不存在此限制。在这种情况下，其他对等方仍然可以看到您的网络摄像头和内容，并可以来回导航以查看其他幻灯片。在此场景中，幻灯片在 VDA 上呈现。要访问 PowerPoint Live 幻灯片组，请单击“共享托盘”按钮并选择建议的 PowerPoint 幻灯片之一，或者单击“浏览”并在您的计算机或 OneDrive 中查找 PowerPoint 文件。

> 出站屏幕共享也经过优化并卸载到 Citrix Workspace 应用程序。在这种情况下，媒体引擎仅捕获并传输 Citrix Desktop Viewer (CDViewer.exe) 窗口，该窗口周围会绘制红色边框。任何与 Desktop Viewer 重叠的本地应用程序都不会被捕获。

> **注意**

> 在适用于 Mac 的 Citrix Workspace 应用程序中设置特定权限以启用屏幕共享。有关详细信息，请参阅系统要求。

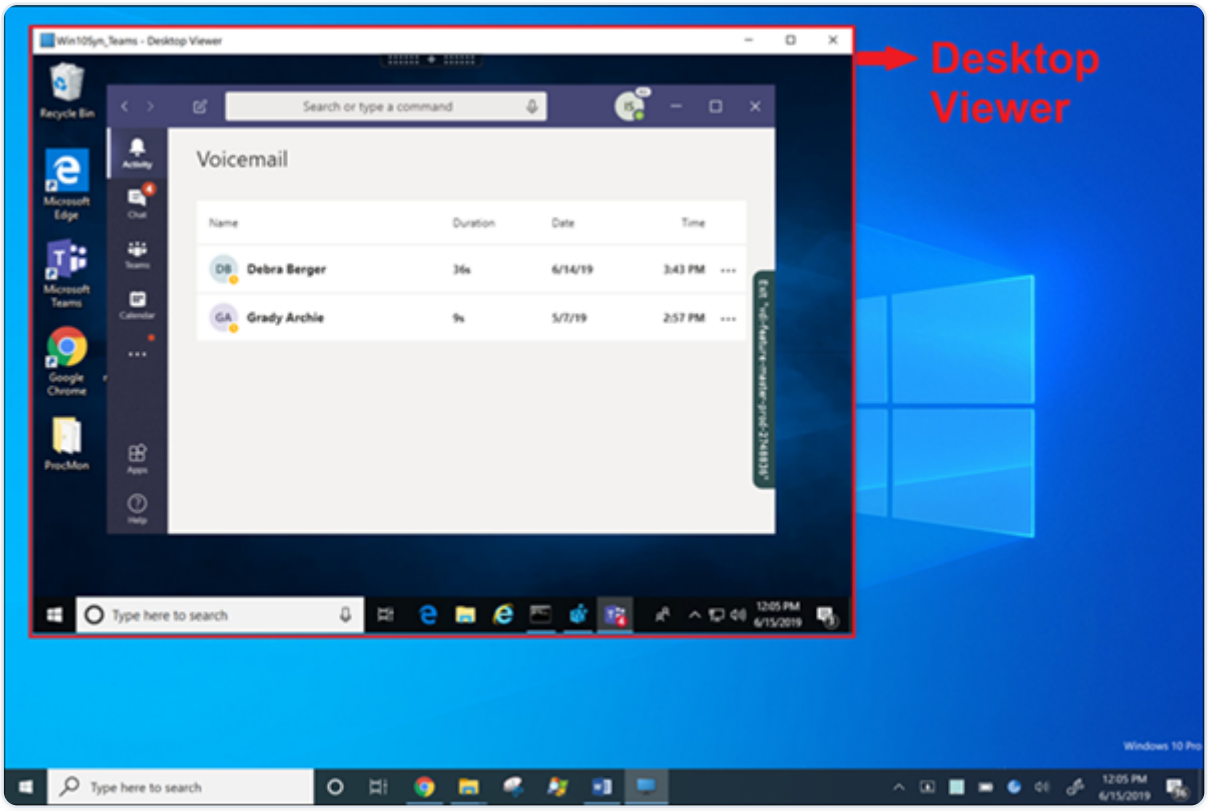
## 多显示器

如果 Desktop Viewer (CDViewer.exe) 处于全屏模式并跨多显示器设置，Citrix Workspace 应用程序 2106 或更高版本（Windows/Linux/Mac）允许屏幕选择器选择要共享的显示器。

**已知限制：**

- 如果 Desktop Viewer 被禁用或正在使用 Desktop Lock，则 Microsoft Teams 屏幕选择器中无法进行多显示器选择。可以通过编辑 `.ICA` 文件模板或 `StoreFront web.config` 来禁用 Desktop Viewer。SHIFT+F2 热键与多显示器屏幕共享不兼容。

- 在 2106 之前的 Workspace 应用程序版本中，仅共享主显示器。将虚拟桌面中的应用程序拖动到主显示器，以便通话中的其他对等方可以看到它。
- 如果您使用虚拟显示器布局功能（单个物理显示器的逻辑分区）配置 Citrix Workspace 应用程序，则多显示器屏幕共享可能无法工作。在这种情况下，所有虚拟显示器都将作为复合图像共享。
- 较旧版本的适用于 Windows 的 Citrix Workspace 应用程序（1907 至 2008）还会共享在客户端计算机中运行的本地应用程序。仅当本地应用程序覆盖在 Desktop Viewer 之上时，才可能进行此共享。此行为已在 2009.6 或更高版本以及 1912 CU5 或更高版本中移除。




**从无缝应用程序进行屏幕共享：**

如果您将 Microsoft Teams 发布为独立的无缝应用程序，屏幕共享将捕获物理端点的本地桌面。需要 Citrix Workspace 应用程序最低版本 1909。

### 应用共享

从适用于 Windows 2112.1 的 Citrix Workspace 应用程序和 VDA 2112 开始，Microsoft Teams 支持使用 HDX 3D Pro 进行应用程序共享。

从适用于 Windows 2109 的 Citrix Workspace 应用程序、适用于 Mac 2203 的 Citrix Workspace 应用程序和 VDA 2109 开始，Microsoft Teams 支持共享在虚拟会话中运行的特定应用程序的屏幕。要共享特定应用程序：

1. 在远程会话中导航到 Microsoft Teams 应用程序。

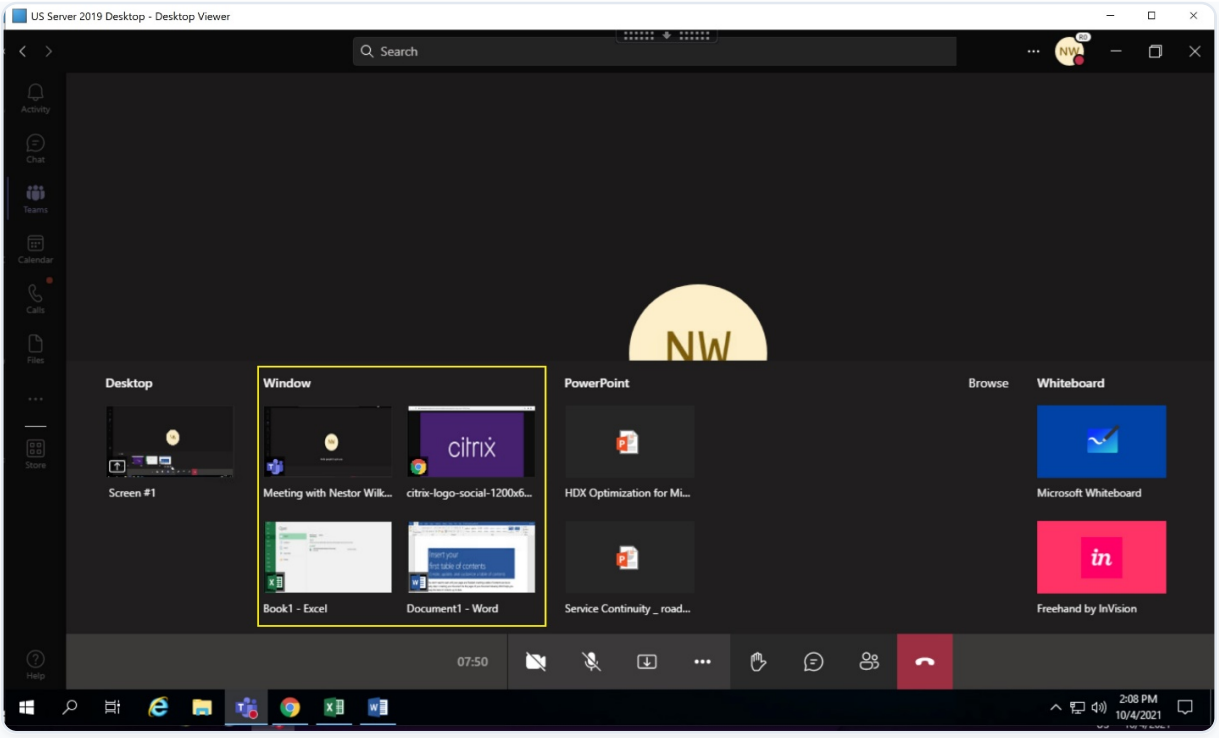
2. 在 Microsoft Teams UI 中单击**共享内容**。
3. 选择要在会议中共享的应用程序。您选择的应用程序周围会出现红色边框，通话中的参与者可以看到共享的应用程序。

要共享其他应用程序，请再次单击**共享内容**并选择一个新应用程序。

如果要禁用应用程序共享，请在 VDA 上的 `HKLM\SOFTWARE\Citrix\Graphics` 处创建以下注册表项：名称：`UseWsProvider` 类型：`DWORD` 值：0

**注意：**

- 如果最小化应用程序，Microsoft Teams 将显示共享应用程序的最后一张图像。您可以最大化窗口以恢复屏幕共享。
- 屏幕共享取决于 VDA 侧的窗口捕获。然后内容以最大速率中继到 Citrix Workspace 应用程序。最大速率为每秒 30 帧。Citrix Workspace 应用程序将内容转发给参与者或会议服务器。




**特定应用程序屏幕共享的已知限制：**

- 屏幕共享应用程序时，鼠标指针不可见。
- 如果您在共享应用程序时将其最小化，则屏幕选择器中只会显示应用程序图标。屏幕选择器中不会预览应用程序的缩略图。您无法共享内容，并且直到您最大化应用程序后才会出现红色边框。

**与应用程序保护的兼容性** 特定应用程序的屏幕共享与 HDX 优化版 Microsoft Teams 中的应用程序保护功能兼容。如果您从启用了应用程序保护的交付组启动应用程序或桌面，则可以屏幕共享特定应用程序。

当您在 Microsoft Teams UI 中单击“**共享内容**”时，屏幕选择器会移除“**桌面**”选项。您只能选择“**窗口**”选项来共享任何打开的应用程序。

> **注意：**
>
> 如果您使用的是适用于 Windows 2202 或更早版本的 Workspace 应用程序，则在从启用了应用程序保护的交付组启动应用程序或桌面时，您将无法看到传入的视频或屏幕共享。此限制在适用于 Windows 2203 LTSR 及更高版本的 Workspace 应用程序中不存在。

### 在 Microsoft Teams 中授予和请求控制权

此功能在以下版本的 Citrix Workspace 应用程序中受支持（不依赖于 VDA 版本或操作系统、单会话或多会话）：

- 适用于 Windows 的 Citrix Workspace 应用程序版本 2112.1 及更高版本
- 适用于 Mac 的 Citrix Workspace 应用程序版本 2203.1 及更高版本

在 Microsoft Teams 通话期间，当参与者共享屏幕时，您可以请求控制权。获得控制权后，您可以对共享屏幕进行选择、编辑或其他键盘和鼠标操作。

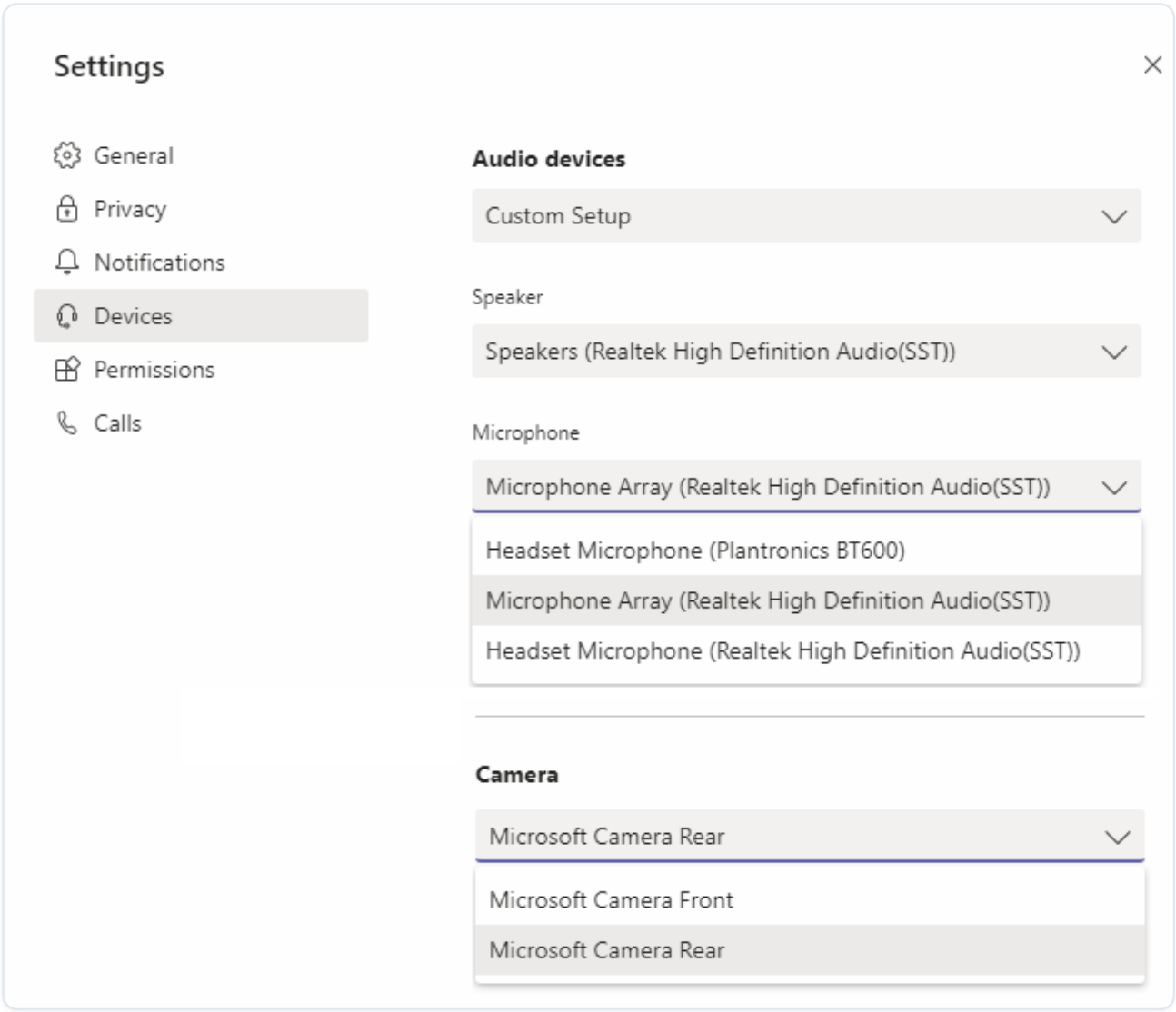
要在共享屏幕时获得控制权，请单击 Microsoft Teams UI 中的“**请求控制**”按钮。共享屏幕的会议参与者可以允许或拒绝您的请求。

在您拥有控制权时，您可以对共享屏幕进行选择、编辑和其他修改。对于这些操作，您可以使用键盘和鼠标。完成后，单击“**请求控制**”。

> **限制：**
>
> - 如果用户共享单个应用程序（也称为应用程序共享），则授予和请求控制权不可用。必须共享整个桌面或显示器。
> - 将控制栏固定到特定位置的功能不可用。

## Microsoft Teams 中的外设

当 Microsoft Teams 优化处于活动状态时，Citrix Workspace 应用程序会访问外设（耳机、麦克风、摄像头、扬声器等）。然后，外设会在 Microsoft Teams UI (**设置 > 设备**) 中正确列出。




Microsoft Teams 不直接访问设备。相反，它依赖于 Workspace 应用程序 WebRTC 媒体引擎来获取、捕获和处理媒体。Microsoft Teams 列出设备供用户选择。

在 Microsoft Teams 处于活动状态时插入的外设默认情况下不会被选中。您必须从 Microsoft Teams UI 的 **设置** > **设备** 屏幕手动选择外设。选择外设后，Microsoft Teams 会缓存外设信息。因此，当您从同一端点重新连接到会话时，外设会自动选中。

**建议：**

- Microsoft Teams 认证耳机 具有内置回声消除功能。在具有额外外设的设置中，如果麦克风和扬声器位于不同的设备上，可能会出现回声。例如，带有内置麦克风的网络摄像头和带有扬声器的显示器。使用外部扬声器时，请将其尽可能远离麦克风。此外，请将它们放置在远离任何可能将声音折射到麦克风中的表面。

- Microsoft Teams 认证摄像头，尽管 Skype for Business 认证外设 与 Microsoft Teams 兼容。
- Citrix Workspace 应用程序媒体引擎无法利用执行板载 H.264 编码的网络摄像头（UVC 1.1 和 1.5）进行 CPU 卸载。

**注意：**

适用于 Windows 的 Workspace 应用程序 2009.6 现在可以获取支持 24 位音频格式或高于 96 kHz 频率的外设。

HdxTeams.exe（在适用于 Windows 的 Citrix Workspace 应用程序 2009 或更早版本中）仅支持以下特定的音频设备格式（通道、位深度和采样率）：

- 播放设备：最多2通道，16位，频率高达96,000 Hz
- 录音设备：最多4通道，16位，频率高达96,000 Hz

即使一个扬声器或麦克风与预期设置不匹配，Microsoft Teams 中的设备枚举也会失败，并且在 **设置 > 设备** 下显示 **无**。

**HdxTeams.exe** 中的 **Webrpc** 日志显示此类信息：

`Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.

`Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!`!

作为一种变通方法，请禁用特定设备或：

1. 打开 **声音控制面板** (mmsys.cpl)。
2. 选择播放或录音设备。
3. 转到 **属性 > 高级** 并将设置更改为受支持的模式。

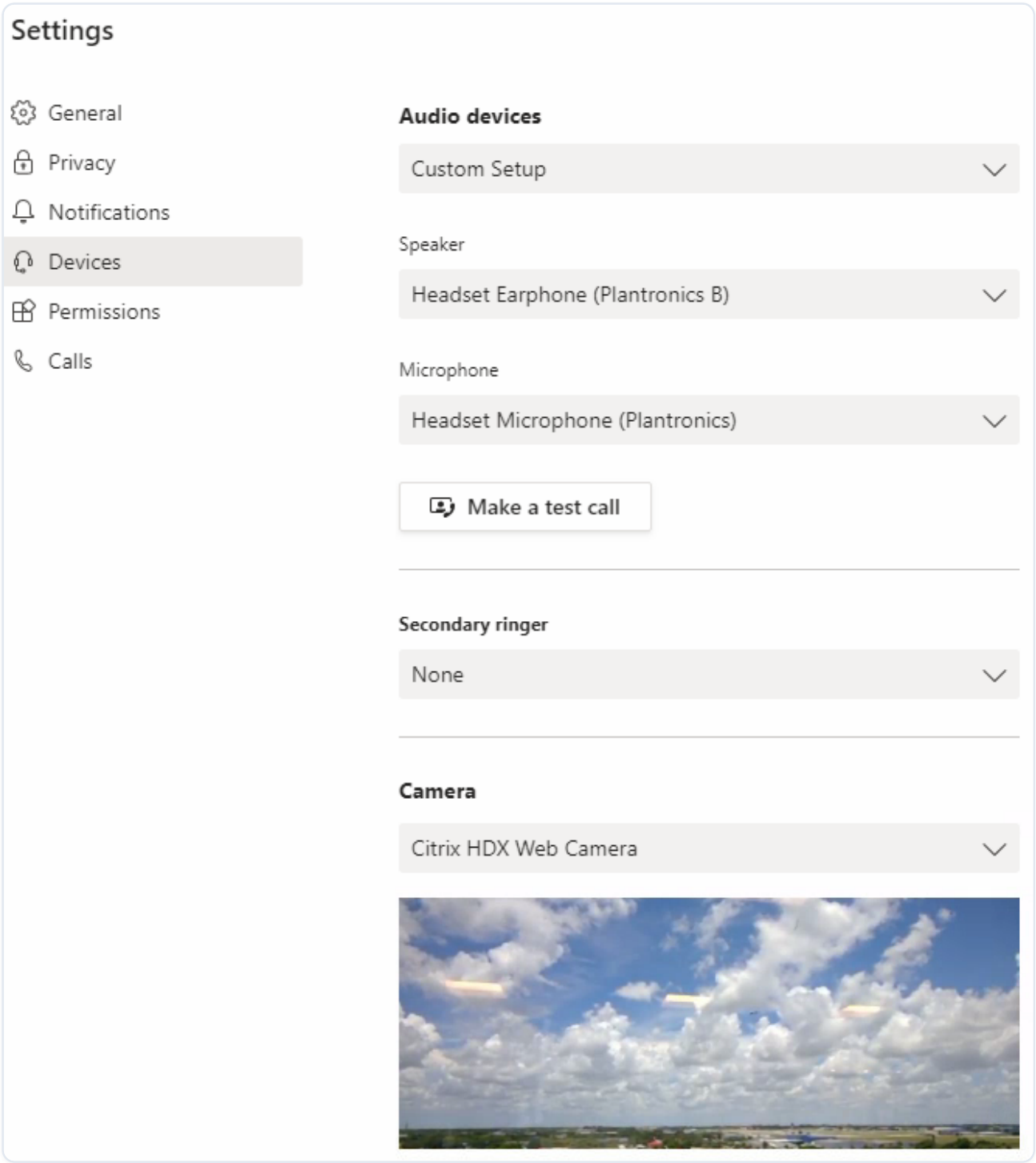
### 回退模式

如果 Microsoft Teams 未能以优化的 VDI 模式加载（在 Teams/关于/版本中显示“Citrix HDX 未连接”），VDA 将回退到旧版 HDX 技术。旧版 HDX 技术可能是网络摄像头重定向以及客户端音频和麦克风重定向。如果您使用的 Workspace 应用程序版本/平台操作系统不支持 Microsoft Teams 优化，则回退注册表项不适用。 在回退模式下，外设会映射到 VDA。外设在 Microsoft Teams 应用程序中显示，就像它们本地连接到虚拟桌面一样。

您现在可以通过在 VDA 中设置注册表项来精细控制回退机制。有关信息，请参阅注册表管理的功能列表中的 Microsoft Teams 回退模式。

此功能需要 Microsoft Teams 1.3.0.13565 或更高版本。

在 Microsoft Teams 应用程序中查看 **设置 > 设备** 选项卡时，要确定您处于优化模式还是未优化模式，主要区别在于摄像头名称。如果 Microsoft Teams 以未优化模式加载，则会启动旧版 HDX 技术。网络摄像头名称带有 **Citrix HDX** 后缀，如以下图所示。与优化模式相比，扬声器和麦克风设备名称可能略有不同（或被截断）。




当使用旧版 HDX 技术时，Microsoft Teams 不会将音频、视频和屏幕共享处理卸载到端点的 Citrix Workspace 应用程序 WebRTC 媒体引擎。相反，HDX 技术使用服务器端渲染。开启视频时，预计 VDA 上的 CPU 消耗会很高。实时音频性能可能不理想。

## 已知限制

### Citrix 限制

Citrix Workspace 应用程序的限制：

- HID 按钮 - 不支持接听和结束通话。支持音量增大和减小。

- Microsoft Teams 管理中心中的 QoS 设置不适用于 VDI 用户。
- 如果用户在 VDA 上使用截图工具，则无法截取 Teams 内容的屏幕截图。只有在客户端使用时才能捕获内容。

VDA 上的限制：

- 当您将 Citrix Workspace 应用程序的高 DPI 设置配置为 **是** 时，重定向的视频窗口会显示错位。当显示器的 DPI 缩放因子设置为 100% 以上时，会出现此限制。

Citrix Workspace 应用程序和 VDA 上的限制：

- 您只能使用客户端计算机上的音量条控制优化通话的音量，而不能在 VDA 上控制。

### Microsoft 限制

- 不支持 3x3 画廊视图。Microsoft Teams 依赖项 – 请联系 Microsoft 了解何时可以预期 3x3 网格。
- 与 Skype for Business 的互操作性仅限于音频通话，不支持视频模式。
- 传入和传出视频流的最大分辨率为 720p。
- 不支持 PSTN 呼叫回铃音。
- 不支持直接路由的媒体旁路。
- 不支持广播和直播活动的制作人及演示者角色。支持与会者角色，但未优化（而是在 VDA 上呈现）。
- 不支持 Microsoft Teams 中的放大和缩小功能。
- 不支持基于位置的路由和媒体旁路。
- 呼叫运行状况不可用。
- VDI 参与者支持分组讨论室。如果组织者是 VDI 用户，Microsoft Teams 不支持分组讨论室。
- 不支持呼叫合并（用户界面中不显示此选项）。

### Citrix 和 Microsoft 限制

- 进行屏幕共享时，**包括系统音频** 选项不可用。
- 不支持同步广播。
- 不支持**辅助铃声**（**Teams** > **设置** > **设备**）。
- 不支持模糊或自定义背景的选项。

## 即将终止支持的 Microsoft Teams 单窗口模式

在 January 31, 2024，Microsoft 将停止对使用 VDI Microsoft Teams 优化时的单窗口 UI 的 Microsoft Teams 支持，并且仅支持多窗口体验。Microsoft 已于 9/8/2023 在 M365 管理中心（帖子 ID：MC674419）发布了此弃用通知。 有关多窗口功能的公开详细信息，请参阅技术社区文章：Microsoft Teams 中的新会议和呼叫体验。

您必须将 VDA 和 Citrix Workspace 应用程序升级到受支持的版本，才能继续在优化模式下使用 Microsoft Teams 进行视频和屏幕共享。如果您不升级您的基础架构和端点以支持多窗口，您将只能建立音频呼叫。您将无法使用优化的视频和屏幕共享功能。

下表说明了在 Citrix VDI 上继续使用 Microsoft Teams 优化呼叫所需的 VDA 和 Citrix Workspace 应用程序的最低版本、LTSR 版本和推荐版本：

| 组件 | 最低版本 | LTSR 支持的版本 | 推荐版本 |
| --- | --- | --- | --- |
| 微软 Teams | 1.5.00.11865 | 不适用 | 最新 |
| VDA | 1912 CU6 LTSR, 2112 CR | 1912 CU7+, 2203 CU2+ | 2308 CR+ |
| 适用于 Windows 的 Citrix Workspace 应用程序 | 2205 CR | 2203 CU2+ | 2309 CR+ |
| 适用于 Mac 的 Citrix Workspace 应用程序 | 2209 CR | 不适用 | 2308 CR+ |
| 适用于 Linux 的 Citrix Workspace 应用程序 | 2209 CR | 不适用 | 2308 CR+ |
| 适用于 ChromeOS 或 HTML5 的 Citrix Workspace 应用程序 | 2303 CR | 不适用 | 2309 CR+ |

## WebRTC 中 SDP 格式（方案 B）的弃用公告

Citrix 计划在未来的版本中弃用 WebRTC 对当前 SDP 格式（方案 B）的支持。您必须在 WebRTC 中使用统一计划 (Unified Plan) 来支持优化的 Microsoft Teams 功能。

### 受影响的产品

在 Citrix Workspace 应用程序的未来版本中，即将发布的 Citrix Workspace 应用程序的端点与 Citrix Workspace 应用程序 2108 或更早版本的端点之间的呼叫将不受支持。此呼叫不兼容性包括 1912 LTSR Citrix Workspace 应用程序客户端 (CWA)。以下 CWA 客户端受到影响：

- 适用于 Windows 的 Citrix Workspace 应用程序
- 适用于 Linux 的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序
- 适用于 Chrome 的 Citrix Workspace 应用程序

### 方案 B 的替代方案

如果您运行的 Citrix Workspace 应用程序版本低于 2109，则必须升级到受支持的版本（最好是最新的 CR 版本）。否则，与未来版本或更新端点的任何呼叫都将无法连接。如果联合通信合作伙伴尚未升级其 Citrix Workspace，则未来版本与您的联合通信合作伙伴之间的呼叫也可能无法完成。

Citrix Workspace 应用程序 2108 版本已于 2023 年 3 月结束支持，必须升级到更新版本。有关 Citrix Workspace 应用程序版本支持的详细信息，请参阅 Workspace 应用程序。

有关方案 B 弃用的更多信息，请参阅 WebRTC 文档。

## 更多信息

- 监视、故障排除和支持 Microsoft Teams
- 将 Microsoft Teams 桌面应用程序部署到 VM
- 使用 MSI 安装 Microsoft Teams（VDI 安装部分）
- 瘦客户端
- Skype for Business 网络评估工具
- 了解 Microsoft Teams 和 Skype for Business 的共存和互操作性

## 监视、故障排除和支持 Microsoft Teams

### 监视 Teams

本节提供了使用 HDX 监视 Microsoft Teams 优化的指导。 如果您在优化模式下运行，并且 `HdxRtcEngine.exe` 正在客户端计算机上运行，则 VDA 上名为 `WebSocketAgent.exe` 的进程将在会话中运行。使用 Director 中的“**活动管理器**”查看应用程序。

](/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/teams-activity-manager.png)

使用 VDA 最低版本 1912，您可以使用 Citrix HDX Monitor（最低版本 3.11）监控活动的 Teams 呼叫。Citrix Virtual Apps and Desktops 产品 ISO 包含文件夹 `layout\image-full\Support\HDX Monitor` 中的最新 `hdxmonitor.msi`。

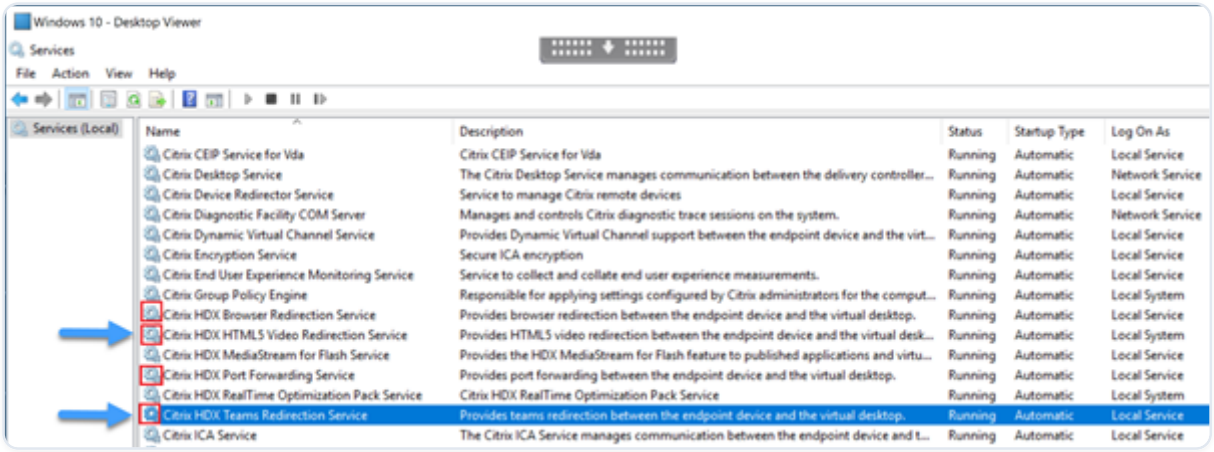
有关详细信息，请参阅知识中心文章 CTX253754 中的“*监视*”。

### 故障排除

本节提供了在使用 Microsoft Teams 优化时可能遇到的问题的故障排除技巧。有关详细信息，请参阅 CTX253754。

#### 在 虚拟交付代理 上

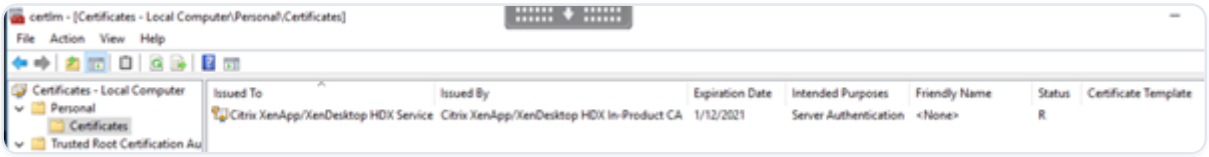
BCR_x64.msi 安装了四个服务。其中只有两个负责 VDA 中的 Microsoft Teams 重定向。



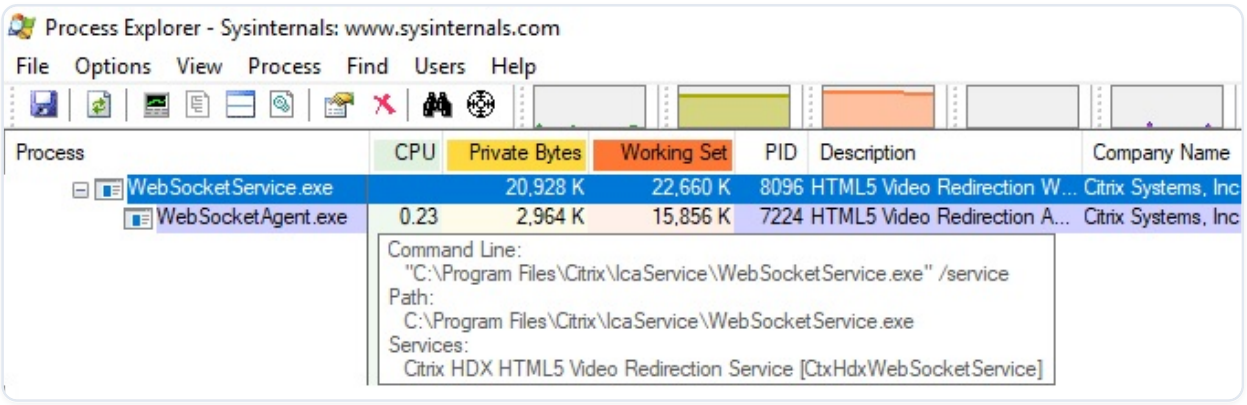

- **Citrix HDX Teams 重定向服务**建立 Microsoft Teams 中使用的虚拟通道。该服务依赖于 CtxSvcHost.exe。
- **Citrix HDX HTML5 视频重定向服务**作为 WebSocketService.exe 运行，侦听 127.0.0.1:9002 TCP。WebSocketService.exe 执行两个主要功能：

  i. **安全 WebSocket 的 TLS 终止**从 vdiCitrixPeerConnection.js 接收安全 WebSocket 连接，vdiCitrixPeerConnection.js 是 Microsoft Teams 应用程序中的一个组件。您可以使用进程监视器对其进行跟踪。有关证书的详细信息，请参阅 Controller 和 VDA 之间的通信 下的“TLS 和 HTML5 视频重定向以及浏览器内容重定向”部分。

  某些防病毒和桌面安全软件会干扰 `WebSocketService.exe` 及其证书的正常运行。尽管 Citrix HDX HTML5 视频重定向服务可能在 `services.msc` 控制台中运行，但 localhost `127.0.0.1:9002` TCP 套接字从未处于侦听模式，如 netstat 中所示。尝试重新启动服务会导致其挂起（“正在停止...”）。确保为 `WebSocketService.exe` 进程应用适当的排除项。




ii. **用户会话映射。**当 Microsoft Teams 应用程序启动时，WebSocketService.exe 会在 VDA 中用户的会话中启动 WebSocketAgent.exe 进程。WebSocketService.exe 在会话 0 中以 LocalSystem 帐户运行。




您可以使用 `netstat` 检查 WebSocketService.exe 服务在 VDA 中是否处于活动侦听状态。

从提升的命令提示符窗口运行 `netstat -anob -p tcp`：

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

成功连接后，状态将变为 ESTABLISHED：

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

**重要提示：**

WebSocketService.exe 侦听两个 TCP 套接字：127.0.0.1:9001 和 127.0.0.1:9002。端口 9001 用于浏览器内容重定向和 HTML5 视频重定向。端口 9002 用于 Microsoft Teams 重定向。确保 VDA 的 Windows 操作系统中没有任何代理配置会阻止 Teams.exe 和 WebSocketService.exe 之间的直接通信。有时，当您在 Internet Explorer 11 中配置显式代理（**Internet 选项 > 连接 > 局域网设置 > 代理服务器**）时，连接可能会通过分配的代理服务器。使用手动和显式代理设置时，请验证是否选中了**对于本地地址不使用代理服务器**。

### 服务位置和说明

| 服务 | WINDOWS SERVER 操作系统中可执行文件的路径 | 登录为 | 描述 |
|---|---|---|---|
| Citrix HTML5 视频重定向服务 | "C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service | 本地系统帐户 | 为多个 HDX 多媒体服务提供在虚拟桌面和端点设备之间执行媒体重定向所需的初始框架。 |
| Citrix HDX 浏览器内容重定向服务 | "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g 浏览器重定向服务 | 此帐户（本地服务） | 提供端点设备和虚拟桌面之间的浏览器内容重定向。 |
| Citrix 端口转发服务 | "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs | 此帐户（本地服务） | 为浏览器内容重定向提供端点设备和虚拟桌面之间的端口转发。 |
| Citrix HDX Teams 重定向服务 | "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs | 本地系统帐户 | 提供端点设备和虚拟桌面之间的 Microsoft Teams 重定向。 |

### Citrix Workspace™ 应用程序

在用户的端点上，适用于 Windows 的 Citrix Workspace 应用程序会实例化一个名为 HdxTeams.exe 或 HdxRtcEngine.exe 的新服务。当 Microsoft Teams 在 VDA 中启动且用户尝试在自预览中呼叫或访问外设时，会发生这种情况。如果您没有看到此服务，请检查以下各项：

1. 确保您至少安装了适用于 Windows 的 Workspace App 1905 版。您是否在 Workspace 应用程序安装路径中看到 HdxTeams.exe 或 HdxRtcEngine.exe 以及 webrpc.dll 二进制文件？
2. 如果您已验证步骤 1，请执行以下操作以检查 HdxTeams.exe 或 HdxRtcEngine.exe 是否正在启动。
    a. 退出 VDA 上的 Microsoft Teams。
    b. 在 VDA 上启动 services.msc。
    c. 停止 Citrix HDX Teams 重定向服务。
    d. 断开 ICA® 会话。

e. 连接 ICA 会话。

f. 启动 Citrix HDX Teams 重定向服务。

g. 重新启动 Citrix HDX HTML5 视频重定向服务。

h. 在 VDA 上启动 Microsoft Teams。

3. 如果客户端端点上仍未启动 HdxTeams.exe 或 HdxRtcEngine.exe，请执行以下操作：

a. 重新启动 VDA。

b. 重新启动客户端端点。

## 支持

Citrix 和 Microsoft 共同支持使用 Microsoft Teams 优化功能从 Citrix Virtual Apps and Desktops™ 交付 Microsoft Teams。这种联合支持是两家公司密切合作的结果。如果您拥有有效的支持合同，并且在使用此解决方案时遇到问题，请向您怀疑其代码导致问题的供应商提交支持工单。也就是说，Microsoft 负责 Teams，Citrix 负责优化组件。 Citrix 或 Microsoft 会收到工单，对问题进行分类，并酌情上报。您无需联系两家公司的支持团队。

当您遇到问题时，我们建议您在 Teams UI 中单击“**帮助 > 报告问题**”。VDA 端日志会在 Citrix 和 Microsoft 之间自动共享，以更快地解决技术问题。

### 收集日志

HDX 媒体引擎日志可在用户计算机上找到（而非 VDA 上）。如果出现任何问题，请务必将日志附加到您的支持案例中。

**Windows 日志：**

您可以在 %TEMP% 中 **HDXTeams** 文件夹内找到 Windows 日志 (AppData/Local/Temp/HDXTeams 或 AppData/Local/Temp/HdxRtcEngine)。查找名为 webrpc_Day_Month_timestamp_Year.txt 的 .txt 文件。如果您使用的是较新版本的 Citrix Workspace 应用程序（例如 Citrix Workspace 应用程序 2009.5 或更高版本），请将日志存储在 AppData\Local\Temp\HdxRtcEngine 中。

每个会话都会为日志创建一个单独的文件夹。

**Mac 日志：**

1. VDWEBRTC 日志 - 记录虚拟通道的执行情况。

   位置：`/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. HdxRtcEngine 日志 - 记录 HdxRtcEngine 上进程的执行情况。

位置：`$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

HdxRtcEngine 日志默认情况下处于启用状态。

3. Webrpc 日志 - 是最重要的日志，记录 webrtc 库的封装执行情况。

位置：`/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

**Linux 日志：**

您可以在 `/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/` 文件夹中找到 Linux 日志。 Webrtc 日志：`/tmp/webrpc/<current date>/webrtc.log` 内核日志：`/var/log/syslog`

**ICE/STUN/TURN/ 日志：**

建立呼叫时，需要以下四个 ICE 阶段：

- 候选收集
- 候选交换
- 连接性检查 (STUN 绑定请求)
- 候选提升

在 HdxRtcEngine.exe 日志中，以下条目是相关的交互式连接建立 (ICE) 条目。这些条目必须存在，呼叫设置才能成功。请参阅以下收集阶段的示例代码片段：

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]
```

```
webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.
```

```
>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

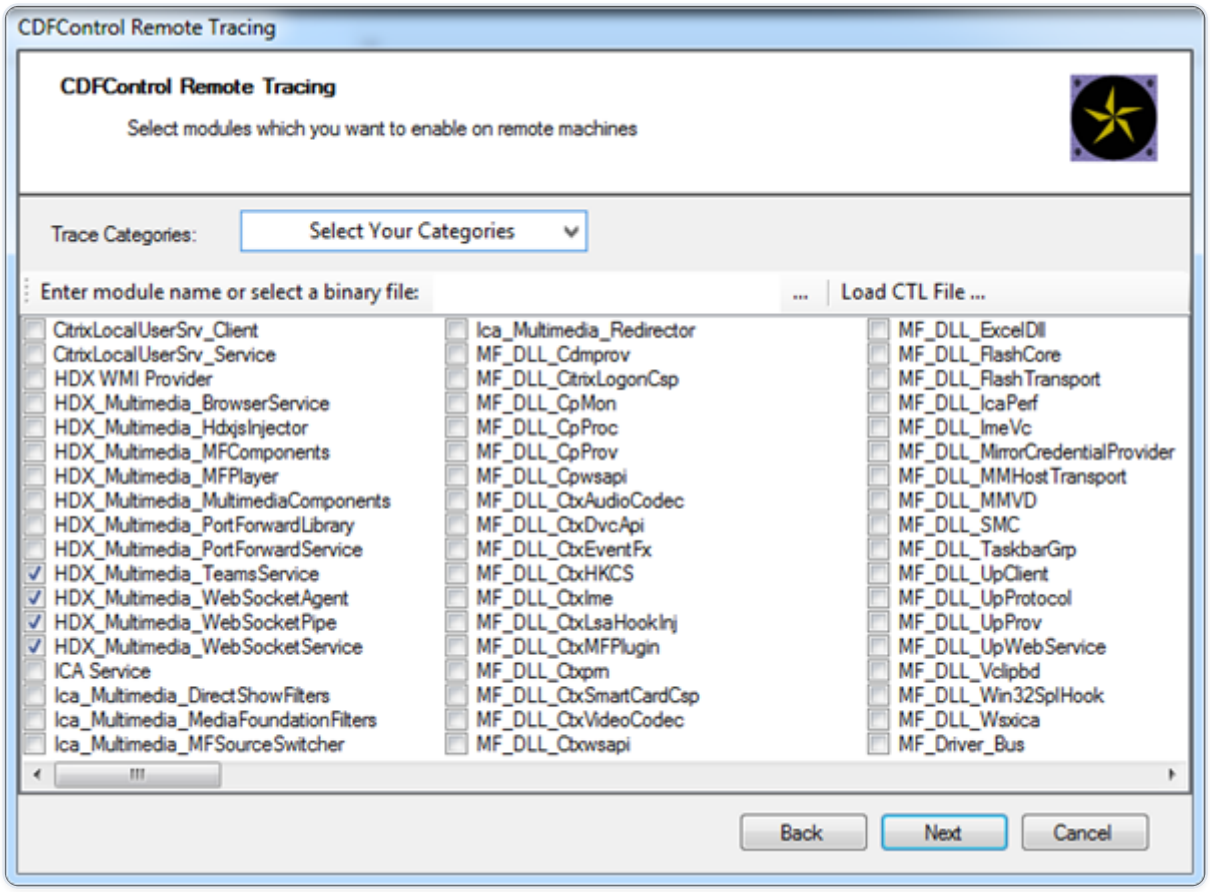
如果存在多个 ICE 候选，则首选顺序为：

1. 主机
2. 对等反射
3. 服务器反射
4. 传输中继

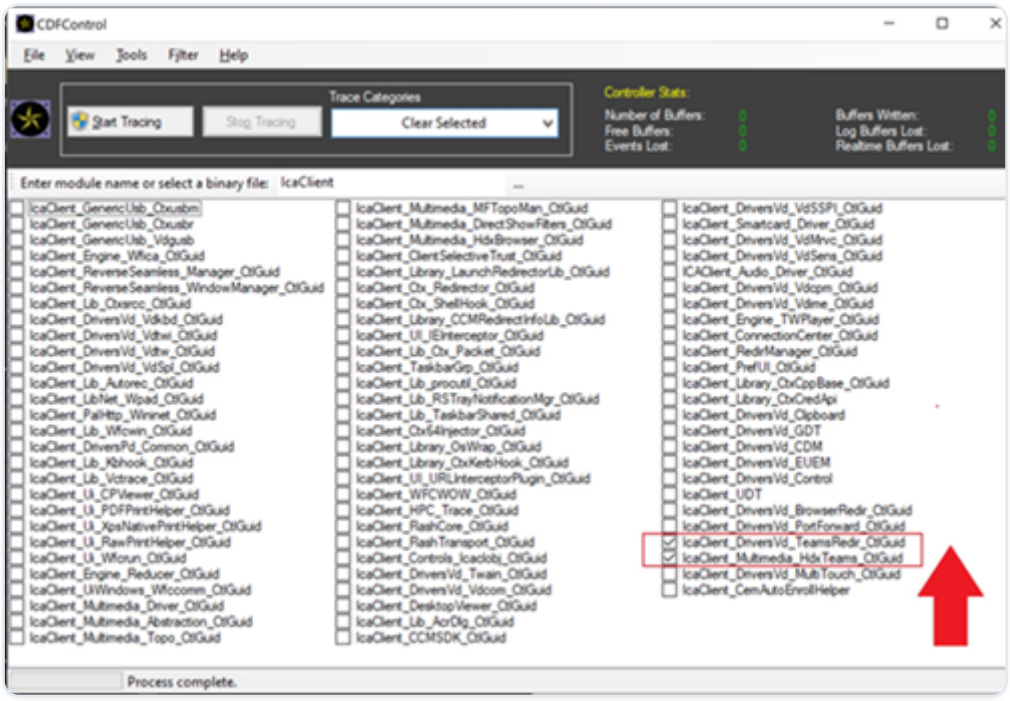
如果您遇到问题并且可以持续重现，我们建议您在 Teams 中单击**帮助 > 报告问题**。如果您已向 Microsoft 提交案例，Citrix 和 Microsoft 之间会共享日志以解决技术问题。 在联系 Citrix 支持之前捕获 CDF 跟踪也很有益。有关详细信息，请参阅知识中心文章 CDFcontrol。

有关收集 CDF 跟踪的建议，请参阅知识中心文章 收集 CDF 跟踪的建议。

**VDA 端 CDF 跟踪 - 启用以下 CDF 跟踪提供程序：**




**Workspace 应用程序端 CDF 跟踪 - 启用以下 CDF 跟踪提供程序：**




- IcaClient_DriversVd_TeamsRedir（可选）
- IcaClient_Multimedia_HdxTeams（需要 Citrix Workspace 应用程序 2012 或更高版本）

# Windows Media 重定向

Windows Media 重定向控制并优化服务器向用户交付流式音频和视频的方式。通过在客户端设备而非服务器上播放媒体运行时文件，Windows Media 重定向减少了播放多媒体文件所需的带宽。Windows Media 重定向提高了在虚拟 Windows 桌面上运行的 Windows Media Player 和兼容播放器的性能。

如果未满足 Windows Media 客户端内容获取的要求，媒体交付会自动使用服务器端获取。此方法对用户是透明的。您可以使用 Citrix Scout 从 HostMMTransport.dll 执行 Citrix 诊断工具 (CDF) 跟踪，以确定所使用的方法。有关详细信息，请参阅 Citrix Scout。

Windows Media 重定向在主机服务器上拦截媒体管道，捕获其本机压缩格式的媒体数据，并将内容重定向到客户端设备。然后，客户端设备会重新创建媒体管道，以解压缩并呈现从主机服务器接收的媒体数据。Windows Media 重定向在运行 Windows 操作系统的客户端设备上运行良好。这些设备具有重建主机服务器上存在的媒体管道所需的多媒体框架。Linux 客户端使用类似的开源媒体框架来重建媒体管道。

策略设置 **Windows Media 重定向** 控制此功能，并且默认情况下为 **允许**。通常，此设置会将从服务器呈现的音频和视频质量提高到与在客户端设备上本地播放的内容相当的水平。在极少数情况下，使用 Windows Media 重定向播放的媒体效果可能比使用基本 ICA® 压缩和常规音频呈现的媒体效果差。您可以通过将 **Windows Media 重定向** 设置添加到策略并将其值设置为 **禁用** 来禁用此功能。

有关策略设置的详细信息，请参阅 多媒体策略设置。

**限制：**

当您在会话中使用 Windows Media Player 并启用远程音频和视频扩展 (RAVE) 时，可能会出现黑屏。如果您右键单击视频内容并选择 **始终在顶部显示“正在播放”**，则可能会出现此黑屏。

# 通用内容重定向

内容重定向允许您控制用户是通过服务器上发布的应用程序访问信息，还是通过在用户设备本地运行的应用程序访问信息。

### 客户端文件夹重定向

客户端文件夹重定向改变了客户端文件在主机端会话中的访问方式。

- 当您仅在服务器上启用客户端驱动器映射时，客户端完整卷会自动作为通用命名约定 (UNC) 链接映射到会话。
- 当您在服务器上启用客户端文件夹重定向并且用户在 Windows 桌面设备上对其进行配置时，用户指定的本地卷部分将被重定向。

### 主机到客户端重定向

对于某些不常见的用例，请考虑使用主机到客户端重定向。通常，其他形式的内容重定向可能更好。我们仅在多会话操作系统 VDA 上支持此类型的重定向，而不支持在单会话操作系统 VDA 上。

### 本地应用访问和 URL 重定向

本地应用访问将本地安装的 Windows 应用程序无缝集成到托管桌面环境中。它无需在不同计算机之间切换即可实现此目的。

HDX™ 技术为没有优化支持或不适用的专用设备提供**通用 USB 重定向**。

## 客户端文件夹重定向

客户端文件夹重定向改变了客户端文件在主机端会话中可访问的方式。如果仅在服务器上启用客户端驱动器映射，则客户端的完整卷将自动映射为通用命名约定 (UNC) 链接到会话。当您在服务器上启用客户端文件夹重定向并且用户在用户设备上对其进行配置时，用户指定的本地卷部分将被重定向。

只有用户指定的文件夹会作为 UNC 链接出现在会话中。也就是说，它不是用户设备上的完整文件系统。如果通过注册表禁用 UNC 链接，则客户端文件夹会作为映射驱动器出现在会话中。

客户端文件夹重定向仅在 Windows 单会话操作系统计算机上受支持。

外部 USB 驱动器的客户端文件夹重定向在设备分离和重新连接时不会保存。

在服务器上启用客户端文件夹重定向。然后，在客户端设备上指定要重定向的文件夹。用于指定客户端文件夹选项的应用程序随此版本提供的 Citrix Workspace™ 应用程序一起提供。

**要求：**

对于服务器：

- Windows 服务器 2022
- Windows Server 2019，标准版和数据中心版
- Windows Server 2016，标准版和数据中心版
- Windows Server 2012 R2，标准版和数据中心版

对于客户端：

- Windows 10，32 位和 64 位版本（最低版本 1607）
- Windows 8.1，32 位和 64 位版本（包括 Embedded 版本）
- Windows 7，32 位和 64 位版本（包括 Embedded 版本）

要在服务器上启用客户端文件夹重定向，请参阅注册表管理的功能列表中的客户端文件夹重定向。

在用户设备上，指定要重定向的文件夹：

1. 确保已安装最新版本的 Citrix Workspace 应用程序。
2. 从 Citrix Workspace 应用程序安装目录中，启动 CtxCFRUI.exe。
3. 选择“**自定义**”单选按钮，然后添加、编辑或删除文件夹。
4. 断开并重新连接会话以使设置生效。

# 主机到客户端重定向

主机到客户端重定向允许在 Citrix® 会话中运行的应用程序中作为超链接嵌入的 URL 使用用户端点设备上的相应应用程序打开。主机到客户端重定向的一些常见用例包括：

- 在 Citrix 服务器无法访问 Internet 或网络源的情况下重定向网站。
- 出于安全、性能、兼容性或可伸缩性原因，不希望在 Citrix 会话中运行 Web 浏览器时重定向网站。
- 在 Citrix 服务器上未安装打开 URL 所需的应用程序的情况下重定向特定 URL 类型。

主机到客户端重定向不适用于您在网页上访问或在 Citrix 会话中运行的 Web 浏览器的地址栏中键入的 URL。有关 Web 浏览器中 URL 的重定向，请参阅双向 URL 重定向或浏览器内容重定向。

## 系统要求

- 多会话操作系统 VDA
- 支持的客户端：
  - 适用于 Windows 的 Citrix Workspace™ 应用程序
  - 适用于 Mac 的 Citrix Workspace 应用程序
  - 适用于 Linux 的 Citrix Workspace 应用程序
  - 适用于 HTML5 的 Citrix Workspace 应用程序
  - 适用于 Chrome 的 Citrix Workspace 应用程序

客户端设备必须安装并配置一个应用程序，用于处理 URL 类型的重定向。

## 配置

使用主机到客户端重定向 Citrix 策略启用此功能。**主机到客户端重定向**默认处于禁用状态。启用主机到客户端重定向策略后，Citrix Launcher 应用程序会向 Windows 服务器注册，以确保它可以拦截 URL 并将其发送到客户端设备。

然后，您必须配置 Windows 组策略，以使用 Citrix Launcher 作为所需 URL 类型的默认应用程序。在 Citrix 服务器 VDA 上，创建 ServerFTAdefaultPolicy.xml 文件并插入以下 XML 代码。

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
</DefaultAssociations>
```

在组策略管理控制台中，转到 **计算机配置 > 管理模板 > Windows 组件 > 文件资源管理器 > 设置默认关联配置文件**， 并保存您的 ServerFTAdefaultPolicy.xml 文件。

> **注意：**
>
> 如果 Citrix 服务器没有组策略设置，Windows 会提示用户选择一个应用程序来打开 URL。
>
> 默认情况下，我们支持以下 URL 类型的重定向：

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

要将其他标准或自定义 URL 类型添加到重定向列表，请在前面引用的 ServerFTAdefaultPolicy.xml 文件中创建新的 **Association Identifier** 行。例如：

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

将 URL 类型添加到列表还需要客户端配置。在 Windows 客户端上创建以下注册表项和值。

> **注意：**

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

- 项：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 值名称：ExtraURLProtocols
- 值类型：REG_SZ
- 值数据：指定所需的 URL 类型，用分号分隔。包括 URL 权限部分之前的所有内容。例如：`ftp://;mailto:;customtype1://;custometype2://`

您只能为 Windows 客户端添加 URL 类型。缺少上述注册表设置的客户端将拒绝重定向回 Citrix 会话。客户端必须安装并配置一个应用程序来处理指定的 URL 类型。

要从默认重定向列表中删除 URL 类型，请在服务器 VDA 上创建以下注册表项和值。

- 项: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 值名称: DisableServerFTA
- 值类型: DWORD
- 值数据: 1
- 值名称: NoRedirectClasses
- 值类型: REG_MULTI_SZ
- 值数据: 指定以下值的任意组合：`http`、`https`、`rtsp`、`rtspu`、`pnm` 或 `mms`。在单独的行上键入多个值。例如：

`http`

`https`

`rtsp`

要为特定网站集启用主机到客户端重定向，请在服务器 VDA 上创建注册表项和值。

- 项: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 值名称: ValidSites
- 值类型: REG_MULTI_SZ

- 值数据: 指定完全限定域名 (FQDN) 的任意组合。在单独的行上键入多个 FQDN。仅包含 FQDN，不带协议 (`http://` 或 `https://`)。FQDN 只能在最左侧位置包含星号 (`*`) 作为通配符。此通配符匹配单个域级别，这与 RFC 6125 中的规则一致。例如：

`www.exmaple.com`

`*.example.com`

> **注意：**
>
> 不能将 **ValidSites** 密钥与 **DisableServerFTA** 和 **NoRedirectClasses** 密钥结合使用。

### 服务器 VDA 默认浏览器配置

本节中提及的启用主机到客户端重定向将覆盖服务器 VDA 上的任何先前默认浏览器配置。如果 Web URL 未重定向，Citrix Launcher 会将 URL 传递给 `command_backup` 注册表项中配置的浏览器。该项默认指向 Internet Explorer，但您可以修改它以包含不同浏览器的路径。有关详细信息，请参阅注册表管理的功能列表中的服务器 VDA 默认浏览器配置。

## 双向内容重定向

双向内容重定向允许 Web 浏览器中的 HTTP 或 HTTPS URL，或嵌入到应用程序中的 URL，在 Citrix VDA 会话和客户端端点之间双向转发。在 Citrix 会话中运行的浏览器中输入的 URL 可以使用客户端的默认浏览器打开。相反，在客户端上运行的浏览器中输入的 URL 可以在 Citrix 会话中打开，无论是通过发布的应用程序还是桌面。双向内容重定向的一些常见用例包括：

- 在启动浏览器无法访问源的网络的情况下重定向 Web URL。
- 出于浏览器兼容性和安全原因重定向 Web URL。
- 当不希望在 Citrix 会话或客户端上运行 Web 浏览器时，重定向嵌入在应用程序中的 Web URL。

### 系统要求

- 单会话或多会话操作系统 VDA
- 适用于 Windows 的 Citrix Workspace™ 应用程序

浏览器：

- IE 浏览器 11
- 附带 Citrix 浏览器重定向扩展程序的 Google Chrome（可在 Google Chrome 网上应用店获取）

- 附带 Citrix 浏览器重定向扩展程序的 Microsoft Edge (Chromium)（可在 Google Chrome 网上应用店获取）

## 配置

必须在 VDA 和客户端上使用 Citrix 策略启用双向内容重定向，才能使重定向生效。双向内容重定向默认处于禁用状态。

对于 VDA 配置，请参阅 ICA 策略设置中的双向内容重定向。

对于客户端配置，请参阅适用于 Windows 的 Citrix Workspace 应用程序文档中的双向内容重定向。

必须使用所示命令注册浏览器扩展。根据所使用的浏览器，在 VDA 和客户端上按需运行这些命令。

要在 VDA 上注册浏览器扩展，请打开命令提示符。然后，运行 `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` 并使用所需的浏览器选项，如所示示例中所示：

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

要在所有可用浏览器上注册扩展，请运行：

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

要注销浏览器扩展，请使用 `/unreg<browser>` 选项，如所示示例中所示：

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

要在客户端上注册浏览器扩展，请打开命令提示符并运行 `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe`，使用与所示示例相同的选项。

> **注意：**
>
> 注册命令会使 Chrome 和 Edge 浏览器在首次启动时提示用户启用 Citrix 浏览器重定向扩展。浏览器扩展也可以从 Google Chrome 网上应用店手动安装。

## 从 Citrix VDA 到客户端的通配符重定向

双向内容重定向支持在定义要重定向的 URL 时使用通配符。要配置双向内容重定向，请参阅配置说明。

在 Citrix Studio 中，在 **Allowed URLs to be redirected to Client** 中设置通配符 URL。星号 (*) 是通配符。

> **注意：**
>
> - 不要在客户端策略中设置 **Allowed URLs to be redirected to VDA**。确保站点设置了 **Allowed URLs to be redirected to VDA** 以避免无限重定向循环。
> - 不支持顶级域。例如，`https://www.citrix.*` 或 `http://www.citrix.co*` 不会被重定向。

## 其他注意事项

- 浏览器要求和配置仅适用于启动重定向的浏览器。目标浏览器（重定向成功后 URL 打开的浏览器）不被视为支持对象。将 URL 从 VDA 重定向到客户端时，仅 VDA 上需要支持的浏览器配置。相反，将 URL 从客户端重定向到 VDA 时，仅客户端上需要支持的浏览器配置。重定向的 URL 将根据方向（客户端或 VDA）交给目标计算机上配置的默认浏览器。VDA 和客户端上不需要使用相同类型的浏览器。
- 检查重定向规则是否会导致循环配置。例如，VDA 策略设置为重定向 `https://www.citrix.com`，而客户端策略设置为重定向相同的 URL，从而导致无限循环。
- 仅支持 HTTP/HTTPS 协议的 URL。不支持 URL 缩短器。
- 客户端到 VDA 的重定向需要以管理员权限安装 Windows 客户端。
- 如果目标浏览器已打开，重定向的 URL 会在新选项卡中打开。否则，URL 会在新浏览器窗口中打开。
- 启用本地应用访问 (LAA) 时，双向内容重定向不起作用。

# 本地应用程序访问和 URL 重定向

## 简介

本地应用访问将本地安装的 Windows 应用程序无缝集成到托管桌面环境中，无需在不同桌面之间切换。通过本地应用访问，您可以：

- 直接从虚拟桌面访问安装在物理笔记本电脑、PC 或其他设备上的本地应用程序。
- 提供灵活的应用程序交付解决方案。如果用户拥有无法虚拟化或 IT 部门不维护的本地应用程序，这些应用程序仍会像安装在虚拟桌面上一样运行。

- 消除应用程序与虚拟桌面分开托管时产生的双跳延迟。为此，请在用户的 Windows 设备上放置已发布的应用程序的快捷方式。
- 使用以下应用程序：
  - 视频会议软件，例如 GoToMeeting。
  - 尚未虚拟化的专业或小众应用程序。
  - 否则会将大量数据从用户设备传输到服务器再传回用户设备的应用程序和外围设备。例如，DVD 刻录机和电视调谐器。

在 Citrix Virtual Apps and Desktops™ 中，托管桌面会话使用 URL 重定向来启动本地应用访问应用程序。URL 重定向使应用程序可以通过多个 URL 地址访问。它通过在桌面会话的浏览器中选择嵌入式链接来启动本地浏览器（基于浏览器的 URL 阻止列表）。如果您导航到阻止列表中不存在的 URL，该 URL 将在桌面会话中再次打开。

URL 重定向仅适用于桌面会话，不适用于应用程序会话。可用于应用程序会话的唯一重定向功能是主机到客户端的内容重定向，这是一种服务器 FTA（文件类型关联）重定向。此 FTA 将某些协议（例如 HTTP、HTTPS、RTSP 或 MMS）重定向到客户端。例如，如果您仅使用 HTTP 打开嵌入式链接，则这些链接将直接通过客户端应用程序打开。不支持 URL 阻止列表或允许列表。

启用本地应用访问后，以本地运行的应用程序、用户托管的应用程序中的链接或桌面快捷方式形式显示给用户的 URL 将通过以下方式之一进行重定向：

- 从用户计算机到托管桌面
- 从 Citrix Virtual Apps and Desktops 服务器到用户计算机
- 在它们启动的环境中呈现（未重定向）

要指定来自特定网站内容的重定向路径，请在虚拟投递代理上配置 URL 允许列表和 URL 阻止列表。这些列表包含指定 URL 重定向策略设置的多字符串注册表项。有关详细信息，请参阅本地应用程序访问策略设置。

URL 可以在 VDA 上呈现，但有以下例外情况：

- 地理/区域信息 — 需要区域信息的网站，例如 msn.com 或 news.google.com（根据地理位置打开特定国家/地区的页面）。例如，如果 VDA 是从英国的数据中心预配的，并且客户端从印度连接，则用户期望看到 in.msn.com。但用户看到的却是 uk.msn.com。
- 多媒体内容 — 包含富媒体内容的网站在客户端设备上呈现时，可为最终用户提供原生体验，即使在高延迟网络中也能节省带宽。此功能可重定向包含其他媒体类型（例如 Silverlight）的站点。此过程在安全环境中进行。也就是说，管理员批准的 URL 在客户端上运行，而其余 URL 则重定向到 VDA。

除了 URL 重定向之外，您还可以使用 FTA 重定向。当会话中遇到文件时，FTA 会启动本地应用程序。如果启动了本地应用程序，则该本地应用程序必须有权访问该文件才能将其打开。因此，您只能使用本地应用程序打开位于网络共享或客户端驱动器（使用客户端驱动器映射）上的文件。例如，当打开 PDF 文件时，如果 PDF 阅读器是本地应用程序，则文件将使用该 PDF 阅读器打开。由于本地应用程序可以直接访问文件，因此无需通过 ICA® 进行文件网络传输即可打开文件。

## 要求、注意事项和限制

我们支持在适用于 Windows 多会话操作系统 VDA 和适用于 Windows 单会话操作系统 VDA 的有效操作系统上使用本地应用程序访问。本地应用程序访问需要 Citrix Workspace app for Windows 4.1 版（最低版本）。支持以下浏览器：

- Edge，最新版本
- Firefox，最新版本和扩展支持版本
- Chrome，最新版本

使用本地应用程序访问和 URL 重定向时，请查看以下注意事项和限制。

- 本地应用程序访问专为跨所有显示器的全屏虚拟桌面而设计：
  - 如果您将本地应用程序访问与在窗口模式下运行或未覆盖所有显示器的虚拟桌面一起使用，用户体验可能会令人困惑。
  - 多显示器 — 当一个显示器最大化时，它将成为在该会话中启动的所有应用程序的默认桌面。即使后续应用程序通常在另一个显示器上启动，也会出现此默认设置。
  - 该功能支持一个 VDA。不支持与多个并发 VDA 集成。
- 某些应用程序可能会出现意外行为，从而影响用户：
  - 驱动器盘符可能会让用户感到困惑，例如本地 C: 盘而不是虚拟桌面 C: 盘。
  - 虚拟桌面中可用的打印机不适用于本地应用程序。
  - 需要提升权限的应用程序不能作为客户端托管应用程序启动。
  - 对于单实例应用程序（例如 Windows Media Player），没有特殊处理。
  - 本地应用程序显示本地计算机的 Windows 主题。
  - 不支持全屏应用程序。这些应用程序包括以全屏模式打开的应用程序，例如 PowerPoint 幻灯片演示或覆盖整个桌面的照片查看器。
  - 本地应用程序访问在 VDA 上复制本地应用程序的属性（例如客户端桌面和“开始”菜单上的快捷方式）。但是，它不复制其他属性，例如快捷键和只读属性。

  - 自定义重叠窗口顺序处理方式的应用程序可能会产生不可预测的结果。例如，某些窗口可能会被隐藏。
  - 不支持快捷方式，包括“我的电脑”、“回收站”、“控制面板”、“网络驱动器”快捷方式和文件夹快捷方式。
  - 不支持以下文件类型和文件：自定义文件类型、没有关联程序的文件、zip 文件和隐藏文件。
  - 对于混合的 32 位和 64 位客户端托管或 VDA 应用程序，不支持任务栏分组。也就是说，不支持将 32 位本地应用程序与 64 位 VDA 应用程序分组。
  - 无法使用 COM 启动应用程序。例如，如果您在 Office 应用程序中单击嵌入的 Office 文档，则无法检测到进程启动，并且本地应用程序集成会失败。
- 不支持双跳场景，即用户在另一个虚拟桌面会话中启动虚拟桌面。
- URL 重定向仅支持显式 URL（即，根据浏览器不同，显示在浏览器地址栏中或通过浏览器内导航找到的 URL）。
- URL 重定向仅适用于桌面会话，不适用于应用程序会话。
- VDA 会话中的本地桌面文件夹不允许用户创建文件。
- 本地运行的应用程序的多个实例的行为方式与为虚拟桌面建立的任务栏设置一致。但是，本地运行的应用程序的快捷方式不会与这些应用程序的运行实例分组。它们也不会与托管应用程序的运行实例或托管应用程序的固定快捷方式分组。用户只能从任务栏关闭本地运行的应用程序窗口。尽管用户可以将本地应用程序窗口固定到桌面任务栏和“开始”菜单，但使用这些快捷方式时，应用程序可能无法一致地启动。
- 如果将“**允许本地应用程序访问**”策略设置设为“**已启用**”，则不支持浏览器内容重定向。默认情况下，本地应用程序访问被禁止。

## 与 Windows 的交互

本地应用程序访问与 Windows 的交互包括以下行为。

- Windows 8 和 Windows Server 2012 快捷方式行为
  - 客户端上安装的 Windows 应用商店应用程序不会作为本地应用程序访问快捷方式的一部分进行枚举。
  - 图像和视频文件默认使用 Windows 应用商店应用程序打开。但是，本地应用程序访问会枚举 Windows 应用商店应用程序并使用桌面应用程序打开快捷方式。
- 本地程序
  - 对于 Windows 7，该文件夹在“开始”菜单中可用。

  - 对于 Windows 8，“本地程序”仅在用户从“开始”屏幕中选择“**所有应用**”作为类别时才可用。“本地程序”中不会显示所有子文件夹。

- 适用于应用程序的 Windows 8 图形功能
  - 桌面应用程序仅限于桌面区域，并由“开始”屏幕和 Windows 8 样式应用程序覆盖。
  - 本地应用访问应用程序在多显示器模式下行为不像桌面应用程序。在多显示器模式下，开始屏幕和桌面显示在不同的显示器上。
- Windows 8 和本地应用访问 URL 重定向
  - 由于 Windows 8 Internet Explorer 未启用任何加载项，请使用桌面版 Internet Explorer 启用 URL 重定向。
  - 在 Windows Server 2012 中，Internet Explorer 默认禁用加载项。要实施 URL 重定向，请禁用 Internet Explorer 增强配置。然后重置 Internet Explorer 选项并重新启动，以确保为标准用户启用加载项。

## 配置本地应用访问和 URL 重定向

要将本地应用访问和 URL 重定向与 Citrix Workspace™ 应用程序结合使用：

- 在本地客户端计算机上安装 Citrix Workspace 应用程序。您可以在 Citrix Workspace 应用程序安装期间启用这两个功能，也可以使用组策略编辑器启用本地应用程序访问模板。
- 将“**允许本地应用程序访问**”策略设置设为“**已启用**”。您还可以配置用于 URL 重定向的 URL 允许列表和阻止列表策略设置。有关详细信息，请参阅本地应用程序访问策略设置。

### 启用本地应用访问和 URL 重定向

要针对所有本地应用程序启用本地应用访问，请执行以下步骤：

1. 启动 思杰工作室。
   - 对于本地部署，从“**开始”菜单**打开 **Citrix Studio**。
   - 对于云服务部署，转到“**Citrix Cloud™ > Virtual Apps and Desktops service > 管理**”选项卡。
2. 在 Studio 导航窗格中，单击“**策略**”。
3. 在“操作”窗格中，单击“**创建策略**”。
4. 在“创建策略”窗口中，在搜索框中键入“允许本地应用访问”，然后单击“**选择**”。
5. 在“编辑设置”窗口中，选择“**允许**”。默认情况下，“**允许本地应用访问**”策略是禁止的。当此设置被允许时，VDA 允许最终用户决定是否在会话中启用已发布的应用程序和本地应用访问快捷方

式。（当此设置被禁止时，已发布的应用程序和本地应用访问快捷方式均不适用于 VDA。）此策略设置适用于整个计算机和 URL 重定向策略。

6. 在“创建策略”窗口中，在搜索框中键入“URL 重定向允许列表”，然后单击“**选择**”。URL 重定向允许列表指定要在远程会话的默认浏览器中打开的 URL。
7. 在“编辑设置”窗口中，单击“**添加**”以添加 URL，然后单击“**确定**”。
8. 在“创建策略”窗口中，在搜索框中键入“URL 重定向阻止列表”，然后单击“**选择**”。URL 重定向阻止列表指定了重定向到在端点上运行的默认浏览器的 URL。
9. 在“编辑设置”窗口中，单击“**添加**”以添加 URL，然后单击“**确定**”。
10. 在“设置”页面上，单击“**下一步**”。
11. 在“用户和计算机”页面上，将策略分配给适用的交付组，然后单击“**下一步**”。
12. 在“摘要”页面上，查看设置，然后单击“**完成**”。

要在 Citrix Workspace 应用程序安装期间为所有本地应用程序启用 URL 重定向，请按照以下步骤操作：

1. 在计算机上为所有用户安装 Citrix Workspace 应用程序时启用 URL 重定向。这样做还会注册 URL 重定向所需的浏览器加载项。
2. 从命令提示符处，运行相应的命令以使用以下选项之一安装 Citrix Workspace 应用程序：
   - 对于 CitrixReceiver.exe，请使用 `/ALLOW_CLIENTHOSTEDAPPSURL=1`。
   - 对于 CitrixReceiverWeb.exe，请使用 `/ALLOW_CLIENTHOSTEDAPPSURL=1`。

### 使用组策略编辑器启用本地应用程序访问模板

**注意：**

- 在使用组策略编辑器启用本地应用程序访问模板之前，将 receiver.admx/adml 模板文件添加到本地 GPO。有关详细信息，请参阅配置组策略对象管理模板。
- 适用于 Windows 的 Citrix Workspace 应用程序模板文件仅当您将 CitrixBase.admx/CitrixBase.adml 添加到 %systemroot%\policyDefinitions 文件夹时，才可在本地 GPO 的“**管理模板 > Citrix 组件 > Citrix Workspace**”文件夹中找到。

要使用组策略编辑器启用本地应用程序访问模板，请按照以下步骤操作：

1. 运行 **gpedit.msc**。

2. 转到 **计算机配置 > 管理模板 > 经典管理模板 (ADM) > Citrix 组件 > Citrix Workspace > 用户体验**。
3. 单击 **本地应用程序访问设置**。
4. 选择 **已启用**，然后选择 **允许 URL 重定向**。对于 URL 重定向，请使用本文档后面 *注册浏览器加载项* 部分中描述的命令行注册浏览器加载项。

### 仅提供对已发布应用程序的访问

您可以使用注册表编辑器或 PowerShell SDK 提供对已发布应用程序的访问。

对于注册表编辑器，请参阅注册表管理的功能列表中的 已发布应用程序的本地应用程序访问。

要使用 PowerShell SDK：

1. 在运行 Delivery Controller™ 的计算机上打开 PowerShell。
2. 输入以下命令：`set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

要在云服务部署中访问“**添加本地应用程序访问应用程序**”，请使用 Citrix DaaS 远程 PowerShell SDK。有关详细信息，请参阅 Citrix DaaS 远程 PowerShell SDK。

1. 下载安装程序：

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`
2. 运行以下命令：

   a. `asnp citrix.*`.

   b. `Get-XdAuthentication`
3. 输入以下命令：`set-configsitemetadata -name “studio_clientHostedAppsEnabled” -value “true”`。

完成适用的上述步骤后，请按照以下步骤继续操作。

1. 从“**开始**”菜单中打开 **Citrix Studio**。
2. 在 Studio 导航窗格中，单击“**应用程序**”。
3. 在中间靠上的窗格中，右键单击空白区域，然后从上下文菜单中选择“**添加本地应用程序访问应用程序**”。您也可以在“操作”窗格中单击“**添加本地应用程序访问应用程序**”。要在“操作”窗格中显示“添加本地应用程序访问应用程序”选项，请单击“**刷新**”。
4. 发布本地应用程序访问应用程序。

- 本地应用程序访问向导将启动并显示“简介”页面，您可以选择在以后启动向导时不再显示此页面。
- 该向导将引导您完成下面介绍的“组”、“位置”、“标识”、“交付”和“摘要”页面。完成每个页面后，单击“**下一步**”，直到到达“摘要”页面。
- 在“组”页面上，选择一个或多个要添加新应用程序的交付组，然后单击“**下一步**”。
- 在“位置”页面上，键入用户本地计算机上应用程序的完整可执行路径，然后键入应用程序所在文件夹的路径。Citrix 建议您使用系统环境变量路径；例如，%ProgramFiles(x86)%\Internet Explorer\iexplore.exe。
- 在“标识”页面上，接受默认值或键入所需信息，然后单击“**下一步**”。
- 在“交付”页面上，配置此应用程序如何交付给用户，然后单击**下一步**。您可以为所选应用程序指定图标。您还可以指定虚拟桌面上的本地应用程序快捷方式是在“开始”菜单、桌面还是两者上可见。
- 在“摘要”页面上，查看设置，然后单击“**完成**”以退出本地应用程序访问向导。

### 注册浏览器加载项

> **注意：**
>
> 当您使用 /ALLOW_CLIENTHOSTEDAPPSURL=1 选项从命令行安装 Citrix Workspace 应用程序时，URL 重定向所需的浏览器加载项会自动注册。
>
> 您可以使用以下命令注册和注销一个或所有加载项：

- 要在客户端设备上注册加载项：\<*client-installation-folder*>\redirector.exe /reg\<*browser*>
- 要在客户端设备上注销加载项：\<*client-installation-folder*>\redirector.exe /unreg\<*browser*>
- 要在 VDA 上注册加载项：\<*VDAinstallation-folder*>\VDARedirector.exe /reg\<*browser*>
- 要在 VDA 上注销加载项：\<*VDAinstallation-folder*>\VDARedirector.exe /unreg\<*browser*>

其中 \<*browser*> 是 Internet Explorer、Firefox、Chrome 或所有。

例如，以下命令在运行 Citrix Workspace 应用程序的设备上注册 Internet Explorer 加载项。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

以下命令在 Windows 多会话操作系统 VDA 上注册所有加载项。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

### 跨浏览器 URL 拦截

- 默认情况下，Internet Explorer 会重定向指定的 URL。如果 URL 不在阻止列表中，但浏览器或网站将其重定向到另一个 URL，则最终 URL 不会被重定向。即使它在阻止列表中，也不会被重定向。

要使 URL 重定向正常工作，请在浏览器提示时启用加载项。如果使用 Internet 选项的加载项或提示中的加载项被禁用，则 URL 重定向将无法正常工作。

- Firefox 附加组件始终重定向 URL。

安装附加组件时，Firefox 会提示在新标签页上允许或阻止安装该附加组件。允许该附加组件才能使功能正常工作。

- Chrome 附加组件始终重定向导航到的最终 URL，而不是输入的 URL。

扩展程序已外部安装。禁用扩展程序后，URL 重定向功能在 Chrome 中不起作用。如果在无痕模式下需要 URL 重定向，请在浏览器设置中允许该扩展程序在该模式下运行。

### 配置注销和断开连接时的本地应用程序行为

> **注意：**
>
> 如果您不按照这些步骤配置设置，则默认情况下，当用户注销或断开与虚拟桌面的连接时，本地应用程序会继续运行。重新连接后，如果本地应用程序在虚拟桌面上可用，则会重新集成。

> 要配置注销和断开连接时的本地应用程序行为，请参阅注册表管理的功能列表中的注销和断开连接时的本地应用程序行为。

# 通用 USB 重定向和客户端驱动器注意事项

HDX™ 技术为大多数常用 USB 设备提供**优化支持**。优化支持通过 WAN 提供更好的性能和带宽效率，从而改善用户体验。优化支持通常是最佳选择，尤其是在高延迟或安全敏感环境中。

HDX 技术为没有优化支持或不适用的专用设备提供**通用 USB 重定向**，例如：

- USB 设备具有不属于优化支持的更高级功能，例如具有更多按钮的鼠标或网络摄像头。
- 用户需要不属于优化支持的功能。
- USB 设备是专用设备，例如测试和测量设备或工业控制器。
- 应用程序需要作为 USB 设备直接访问该设备。

- USB 设备只有 Windows 驱动程序可用。例如，智能卡读卡器可能没有适用于 Android 版 Citrix Workspace™ 应用程序的驱动程序。
- Citrix Workspace 应用程序的版本不提供对此类 USB 设备的任何优化支持。

使用通用 USB 重定向：

- 用户无需在用户设备上安装设备驱动程序。
- USB 客户端驱动程序安装在 VDA 计算机上。

> **重要提示：**
>
> - 通用 USB 重定向可以与优化支持一起使用。如果启用通用 USB 重定向，请为通用 USB 重定向和优化支持配置 Citrix USB 设备策略设置。
> - Citrix 客户端 USB 设备优化规则 中的策略设置是通用 USB 重定向的特定设置，适用于特定 USB 设备。它不适用于此处所述的优化支持。

## USB 设备的性能注意事项

网络延迟和带宽在使用通用 USB 重定向某些类型的 USB 设备时，可能会影响用户体验和 USB 设备操作。例如，对时间敏感的设备可能无法在高延迟、低带宽链路上正常运行。在可能的情况下，请改用优化支持。

某些 USB 设备需要高带宽才能使用，例如 3D 鼠标（与通常也需要高带宽的 3D 应用程序一起使用）。如果无法增加带宽，您可以通过使用带宽策略设置调整其他组件的带宽使用情况来缓解此问题。有关详细信息，请参阅客户端 USB 设备重定向的 带宽策略设置和 多流连接策略设置。

## USB 设备的安全性注意事项

某些 USB 设备本质上对安全性敏感，例如智能卡读卡器、指纹识别器和签名板。其他 USB 设备（例如 USB 存储设备）可用于传输可能敏感的数据。

> **重要提示：**
>
> 不要将通用 USB 重定向用于智能卡读卡器。此功能默认情况下对智能卡读卡器禁用，如果启用则不受支持。

USB 设备通常用于分发恶意软件。Citrix Workspace 应用程序和 Citrix Virtual Apps and Desktops™ 的配置可以降低但不能消除这些 USB 设备带来的风险。无论使用通用 USB 重定向还是优化支持，此情况都适用。

**重要提示：**

对于安全敏感的设备和数据，请始终使用 TLS 或 IPsec 保护 HDX 连接。

仅启用您需要的 USB 设备支持。配置通用 USB 重定向和优化支持以满足此需求。

为用户提供安全使用 USB 设备的指导：

- 仅使用从可信来源获取的 USB 设备。
- 请勿将 USB 设备无人看管地留在开放环境中，例如，网吧中的闪存驱动器。
- 解释在多台计算机上使用 USB 设备的风险。

## 与通用 USB 重定向的兼容性

通用 USB 重定向支持 USB 2.0 及更早版本的设备。通用 USB 重定向也支持连接到 USB 2.0 或 USB 3.0 端口的 USB 3.0 设备。通用 USB 重定向不支持 USB 3.0 中引入的 USB 功能，例如超高速。

以下 Citrix Workspace 应用程序支持通用 USB 重定向：

- 适用于 Windows 的 Citrix Workspace 应用程序，请参阅 配置应用程序交付。
- 适用于 Mac 的 Citrix Workspace 应用程序，请参阅 适用于 Mac 的 Citrix Workspace 应用程序。
- 适用于 Linux 的 Citrix Workspace 应用程序，请参阅 优化。
- 适用于 Chrome OS 的 Citrix Workspace 应用程序，请参阅 适用于 Chrome 的 Citrix Workspace 应用程序。

有关 Citrix Workspace 应用程序版本，请参阅 Citrix Workspace 应用程序功能矩阵。

如果您使用的是早期版本的 Citrix Workspace 应用程序，请参阅 Citrix Workspace 应用程序文档以确认是否支持通用 USB 重定向。有关支持的 USB 设备类型的任何限制，请参阅 Citrix Workspace 应用程序文档。

通用 USB 重定向支持从 VDA for Single-session OS 7.6 版到当前版本的桌面会话。

通用 USB 重定向支持从 VDA for Multi-session OS 7.6 版到当前版本的桌面会话，但有以下限制：

- VDA 必须运行 Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 或 Windows Server 2022。
- USB 设备驱动程序必须与 VDA 操作系统 (Windows 2012 R2) 的远程桌面会话主机 (RDSH) 完全兼容，包括完整的虚拟化支持。

某些类型的 USB 设备不支持通用 USB 重定向，因为重定向它们没有用处：

- USB 调制解调器。
- USB 网卡。
- USB 集线器。连接到 USB 集线器的 USB 设备将单独处理。
- USB 虚拟 COM 端口。请使用 COM 端口重定向而不是通用 USB 重定向。

有关已通过通用 USB 重定向测试的 USB 设备的信息，请参阅 Citrix Ready Marketplace。某些 USB 设备无法通过通用 USB 重定向正常运行。

## 配置通用 USB 重定向

您可以控制并单独配置哪些类型的 USB 设备使用通用 USB 重定向：

- 在 VDA 上，使用 Citrix 策略设置。有关详细信息，请参阅策略设置参考中的 客户端驱动器和用户设备的重定向 和 USB 设备策略设置。
- 在 Citrix Workspace 应用程序中，使用 Citrix Workspace 应用程序相关的机制。例如，管理模板控制配置适用于 Windows 的 Citrix Workspace 应用程序的注册表设置。默认情况下，某些类别的 USB 设备允许 USB 重定向，而其他类别则被拒绝。有关详细信息，请参阅适用于 Windows 的 Citrix Workspace 应用程序文档中的 配置。

这种单独的配置提供了灵活性。例如：

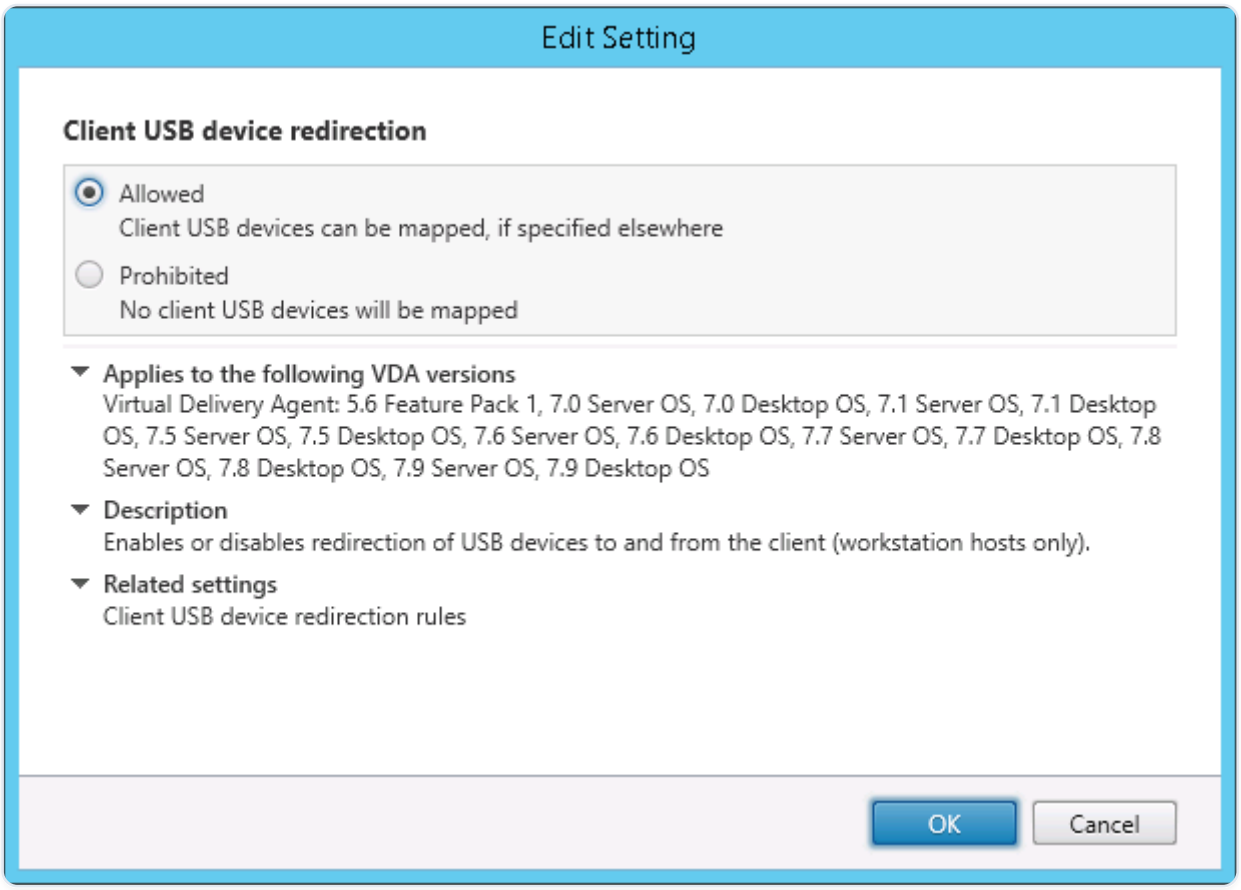
- 如果两个不同的组织或部门负责 Citrix Workspace 应用程序和 VDA，他们可以单独实施控制。当一个组织中的用户访问另一个组织中的应用程序时，此配置适用。
- Citrix 策略设置可以控制仅允许特定用户或仅通过 LAN（而不是通过 Citrix Gateway）连接的用户使用的 USB 设备。

# 启用通用 USB 重定向

要启用通用 USB 重定向且无需用户手动重定向，请同时配置 Citrix 策略设置和 Citrix Workspace 应用程序连接首选项。

在 Citrix 策略设置中：

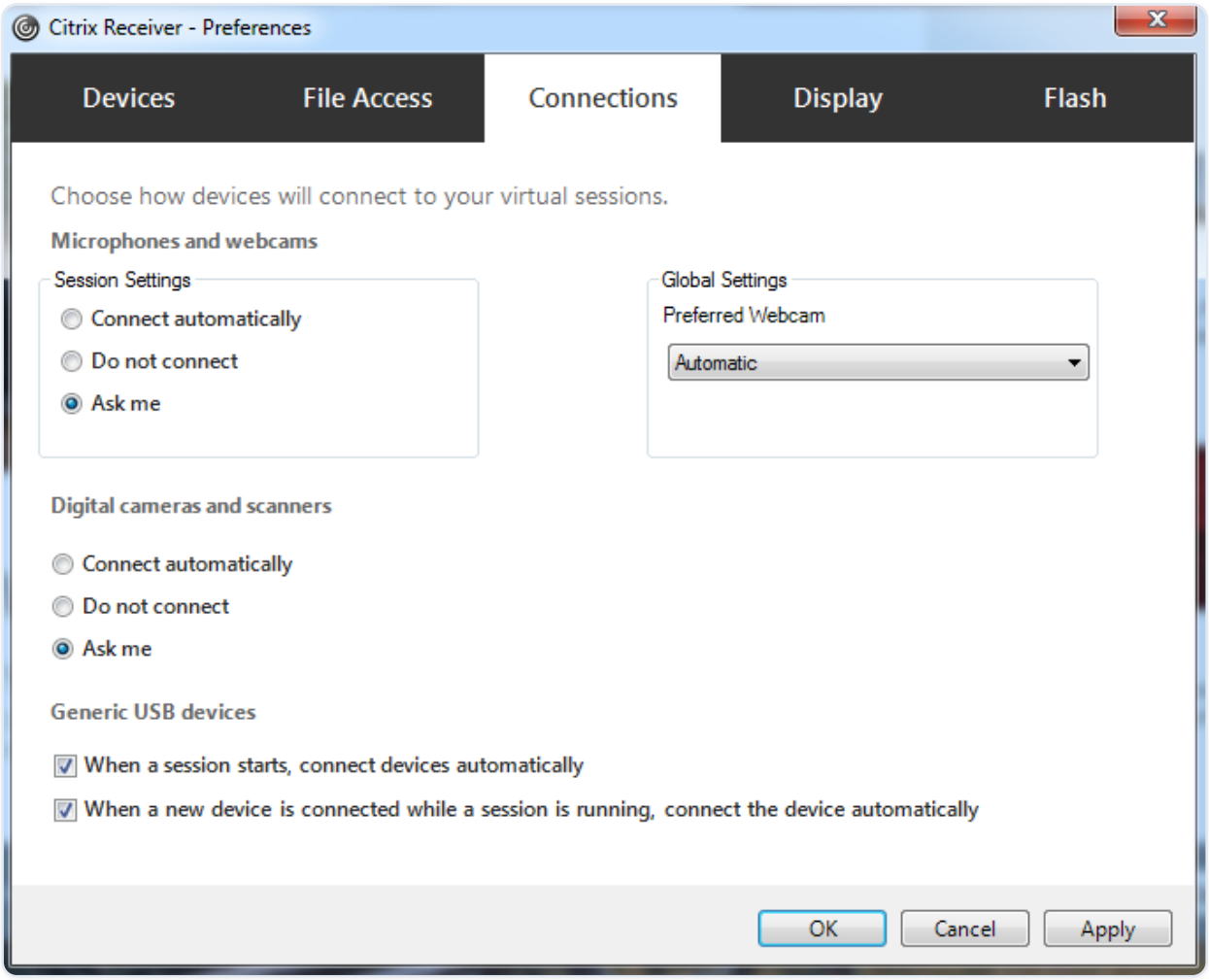
1. 将 客户端 USB 设备重定向 添加到策略，并将其值设置为**允许**。




2. （可选）要更新可用于重定向的 USB 设备列表，请将 客户端 USB 设备重定向规则 设置添加到策略并指定 USB 策略规则。

策略设置完成后，在 Citrix Workspace 应用程序中：

3. 指定设备自动连接，无需手动重定向。您可以使用管理模板或在适用于 **Windows > 首选项 > 连接**的 Citrix Workspace 应用程序中执行此操作。



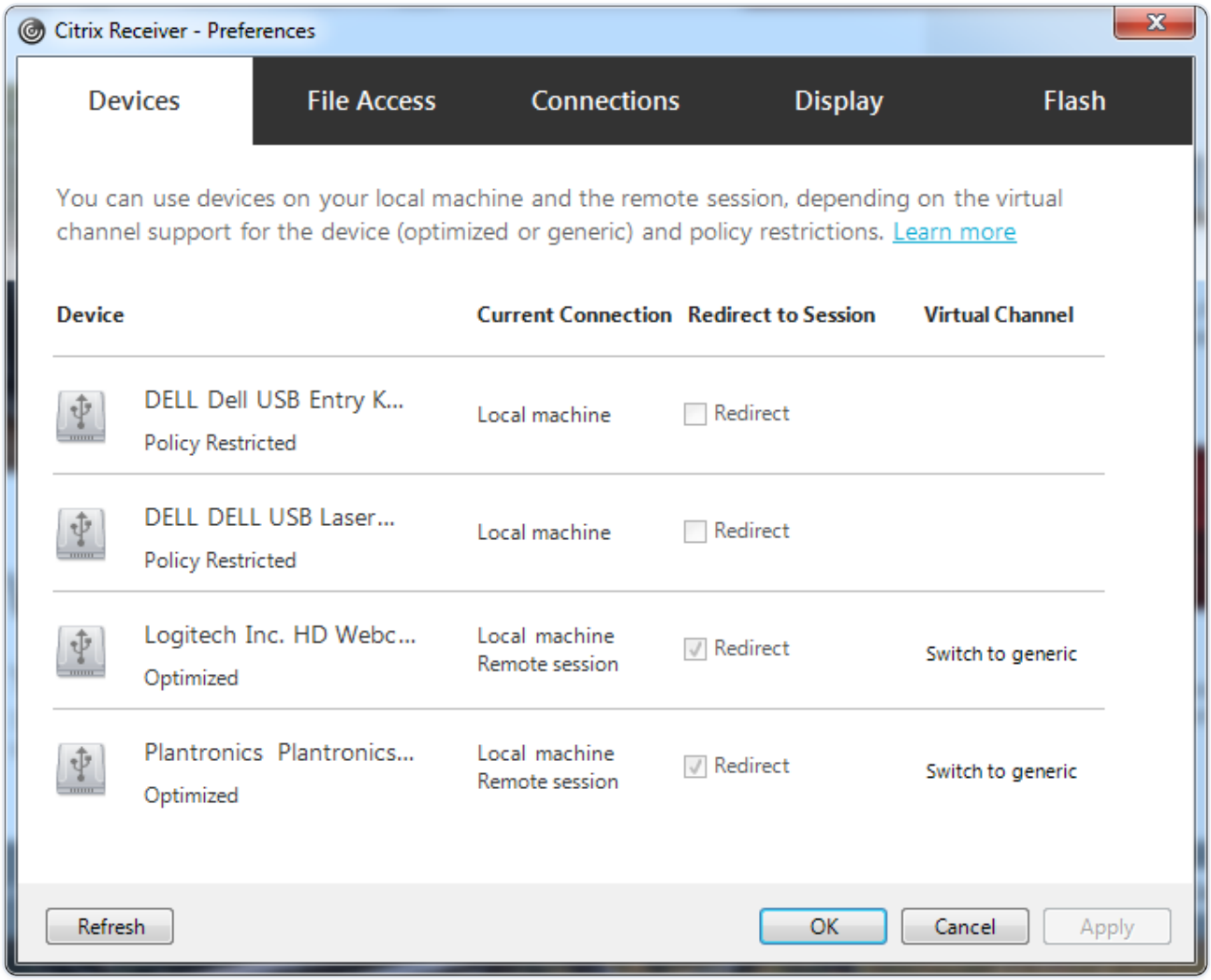

如果您在上一步中为 VDA 指定了 USB 策略规则，请为 Citrix Workspace 应用程序指定相同的策略规则。

对于瘦客户端，请咨询制造商以了解 USB 支持的详细信息和任何所需的配置。

## 配置可用于通用 USB 重定向的 USB 设备类型

当启用 USB 支持并将 USB 用户首选项设置为自动连接 USB 设备时，USB 设备会自动重定向。当连接栏不存在时，USB 设备也会自动重定向。

用户可以通过从 USB 设备列表中选择设备来显式重定向未自动重定向的设备。有关详细信息，请参阅适用于 Windows 的 Citrix Workspace 应用程序用户帮助文章：在 Desktop Viewer 中显示您的设备。




要使用通用 USB 重定向而不是优化支持，您可以选择以下任一方式：

- 在 Citrix Workspace 应用程序中，手动选择要使用通用 USB 重定向的 USB 设备，从“首选项”对话框的“设备”选项卡中选择**切换到通用**。
- 通过配置 USB 设备类型的自动重定向（例如，AutoRedirectStorage=1）并设置 USB 用户首选项以自动连接 USB 设备，自动选择要使用通用 USB 重定向的 USB 设备。有关详细信息，请参阅配置 USB 设备的自动重定向。

**注意：**

仅当发现网络摄像头与 HDX 多媒体重定向不兼容时，才配置通用 USB 重定向以与网络摄像头配合使用。

为防止 USB 设备被列出或重定向，您可以为 Citrix Workspace 应用程序和 VDA 指定设备规则。

对于通用 USB 重定向，您至少需要知道 USB 设备类和子类。并非所有 USB 设备都使用其明显的 USB 设备类和子类。例如：

- 笔使用鼠标设备类。
- 智能卡读卡器可以使用供应商定义或 HID 设备类。

为了更精确的控制，您需要知道供应商 ID、产品 ID 和发布 ID。您可以从设备供应商处获取此信息。

> **重要提示：**

> 恶意 USB 设备可能会呈现与其预期用途不符的 USB 设备特性。设备规则并非旨在阻止此行为。

> 您可以通过指定 USB 设备重定向规则来控制可用于通用 USB 重定向的 USB 设备，以覆盖默认的 USB 策略规则。

Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）：

- 在大多数情况下，下载 Citrix 组策略管理控制台 MSI（`CitrixGroupPolicyManagement_x64.msi`）并将其安装到您的 Active Directory 系统中，然后管理 AD 组策略。（请勿在 VDA 上安装 MSI。）
- 对于适用于 Windows 的 Citrix Workspace 应用程序，请编辑用户设备注册表。安装介质中包含一个管理模板 (ADM 文件)，因此您可以通过 Active Directory 组策略更改用户设备：dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

本地 Citrix Virtual Apps and Desktops：

- 对于 VDA，通过组策略规则编辑多会话操作系统计算机的管理员覆盖规则。组策略管理控制台包含在安装介质中：
  - x64: dvd 根 `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86: DVD 根目录 `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`
- 对于适用于 Windows 的 Citrix Workspace 应用程序，请编辑用户设备注册表。安装介质中包含一个管理模板 (ADM 文件)，以便您可以通过 Active Directory 组策略更改用户设备：DVD 根目录 `\os\lang\Support\Configuration\icaclient_usb.adm`

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

> 产品默认规则存储在 HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\GenericUSB 中。请勿编辑这些产品默认规则。相反，请将它们用作创建管理员覆盖规则的指南，本文稍后将对此进行说明。GPO 覆盖在产品默认规则之前进行评估。

管理员覆盖规则存储在 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules 中。GPO 策略规则采用 **{Allow: | Deny:}** 格式，后跟一组以空格分隔的 *tag=value* 表达式。

支持以下标记：

| 标记 | 描述 |
| --- | --- |
| VID | 来自设备描述符的供应商 ID |
| PID | 来自设备描述符的产品 ID |
| REL | 来自设备描述符的发布 ID |
| 类 | 来自设备描述符或接口描述符的类；有关可用的 USB 类代码，请参阅 `<http://www.usb.org/>` 处的 USB 网站 |
| 子类 | 来自设备描述符或接口描述符的子类 |
| 协议 | 来自设备描述符或接口描述符的协议 |

创建策略规则时，请注意以下事项：

- 规则不区分大小写。
- 规则末尾可以包含可选注释，由 `#` 引入。不需要分隔符，并且注释在匹配时会被忽略。
- 空行和纯注释行将被忽略。
- 空格用作分隔符，但不能出现在数字或标识符的中间。例如，Deny: Class = 08 SubClass=05 是有效规则，但 Deny: Class=0 Sub Class=05 不是。

- 标记必须使用匹配运算符 =。例如，VID=1230。
- 每条规则必须另起一行，或构成以分号分隔的列表的一部分。

> **注意：**
>
> 如果您使用的是 ADM 模板文件，则必须在单行上创建规则，作为以分号分隔的列表。

> 示例：

- 以下示例显示了用于供应商和产品标识符的管理员定义的 USB 策略规则：

  ```
  Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products
  ```

- 以下示例显示了用于定义的类、子类和协议的管理员定义的 USB 策略规则：

  ```
  Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices
  ```

## 使用和移除 USB 设备

用户可以在启动虚拟会话之前或之后连接 USB 设备。

使用适用于 Windows 的 Citrix Workspace 应用程序时，适用以下情况：

- 会话开始后连接的设备会立即显示在 Desktop Viewer 的 USB 菜单中。
- 如果 USB 设备未正确重定向，您可以尝试等到虚拟会话启动后再连接设备，以解决此问题。
- 为避免数据丢失，请在移除 USB 设备之前使用 Windows“安全删除硬件”图标。

## USB 大容量存储设备的安全性控制

USB 大容量存储设备提供优化支持。此支持是 Citrix Virtual Apps and Desktops 客户端驱动器映射的一部分。用户登录时，用户设备上的驱动器会自动映射到虚拟桌面上的驱动器盘符。这些驱动器显示为具有映射驱动器盘符的共享文件夹。要配置客户端驱动器映射，请使用“**客户端可移动驱动器**”设置。此设置位于 ICA 策略设置的 文件重定向策略设置部分。

对于 USB 大容量存储设备，您可以使用客户端驱动器映射或通用 USB 重定向，或两者都使用。使用 Citrix 策略控制它们。主要区别在于：

| 功能 | 客户端驱动器映射 | 通用 USB 重定向 |
| --- | --- | --- |
| 默认启用 | 是 | 否 |
| 可配置只读访问 | 是 | 否 |
| 加密设备访问 | 是，如果设备在访问前已解锁加密 | 是 |
| BitLocker To Go 设备 | 否 | 否 |
| 在会话期间删除设备是安全的 | 否 | 是，前提是用户遵循操作系统的安全移除建议 |

如果同时启用了通用 USB 重定向和客户端驱动器映射策略，并且在大容量存储设备在会话开始之前或之后插入，则使用客户端驱动器映射进行重定向。当同时启用通用 USB 重定向和客户端驱动器映射策略，并且设备配置为自动重定向，并且大容量存储设备在会话开始之前或之后插入时，则使用通用 USB 重定向进行重定向。有关详细信息，请参阅知识中心文章 CTX123015。

> **注意：**
>
> USB 重定向支持较低带宽连接，例如 50 Kbps。但是，复制大文件不起作用。

## 使用客户端驱动器映射控制文件访问

您可以控制用户是否可以将文件从其虚拟环境复制到其用户设备。默认情况下，映射的客户端驱动器上的文件和文件夹在会话中以读/写模式可用。

为防止用户在映射的客户端设备上添加或更改文件和文件夹，请启用**只读客户端驱动器访问**策略设置。将此设置添加到策略时，请确保客户端驱动器重定向设置设置为**允许**，并且也已添加到策略中。

# 打印

在您的环境中管理打印机是一个多阶段过程：

1. 如果您还不熟悉打印概念，请先熟悉它们。
2. 规划您的打印体系结构。这包括分析您的业务需求、现有打印基础结构、用户和应用程序当前如何与打印交互，以及哪种打印管理模型最适合您的环境。
3. 通过选择打印机预配方法，然后创建策略来部署您的打印设计，从而配置您的打印环境。添加新员工或服务器时，请更新策略。
4. 在向用户部署之前，测试试用打印配置。
5. 通过管理打印机驱动程序和优化打印性能来维护您的 Citrix® 打印环境。
6. 解决可能出现的问题。

## 打印概念

在开始规划部署之前，请确保您了解以下核心打印概念：

- 可用的打印机预配类型
- 打印作业的路由方式
- 打印机驱动程序管理基础知识

打印概念建立在 Windows 打印概念之上。要在您的环境中配置和成功管理打印，您必须了解 Windows 网络和客户端打印的工作原理，以及这如何转化为此环境中的打印行为。

## 打印过程

在此环境中，所有打印都由用户在托管应用程序的计算机上启动。打印作业通过网络打印服务器或用户设备重定向到打印设备。

虚拟桌面和应用程序的用户没有持久性工作区。会话结束时，用户的工作区将被删除，因此所有设置都需要在每个会话开始时重建。结果是，每次用户启动新会话时，系统都必须重建用户的工作区。

当用户打印时：

- 确定要为用户提供哪些打印机。这称为打印机预配。
- 恢复用户的打印首选项。
- 确定哪个打印机是会话的默认打印机。

您可以通过配置打印机预配、打印作业路由、打印机属性保留和驱动程序管理选项来自定义如何执行这些任务。务必评估各种选项设置可能如何改变您的环境中的打印性能和用户体验。

# 打印机预配

使打印机在会话中可用的过程称为预配。打印机预配通常是动态处理的。也就是说，会话中出现的打印机不是预先确定和存储的。相反，打印机是根据策略在登录和重新连接期间构建会话时组装的。因此，只要策略中反映了更改，打印机就可以根据策略、用户位置和网络更改而变化。因此，漫游到不同位置的用户可能会看到其工作区发生变化。

系统还会监视客户端打印机，并根据客户端打印机的添加、删除和更改动态调整会话中自动创建的打印机。这种动态打印机发现有利于移动用户，因为他们可以从各种设备连接。

最常见的打印机预配方法是：

- **Universal Print Server** - Citrix Universal Print Server 为网络打印机提供通用打印支持。Universal Print Server 使用通用打印驱动程序。此解决方案使您能够在多会话操作系统计算机上使用单个驱动程序，以允许从任何设备进行网络打印。

Citrix 推荐将 Citrix Universal™ Print Server 用于远程打印服务器方案。Universal Print Server 以优化和压缩的格式通过网络传输打印作业，从而最大限度地减少网络使用并改善用户体验。

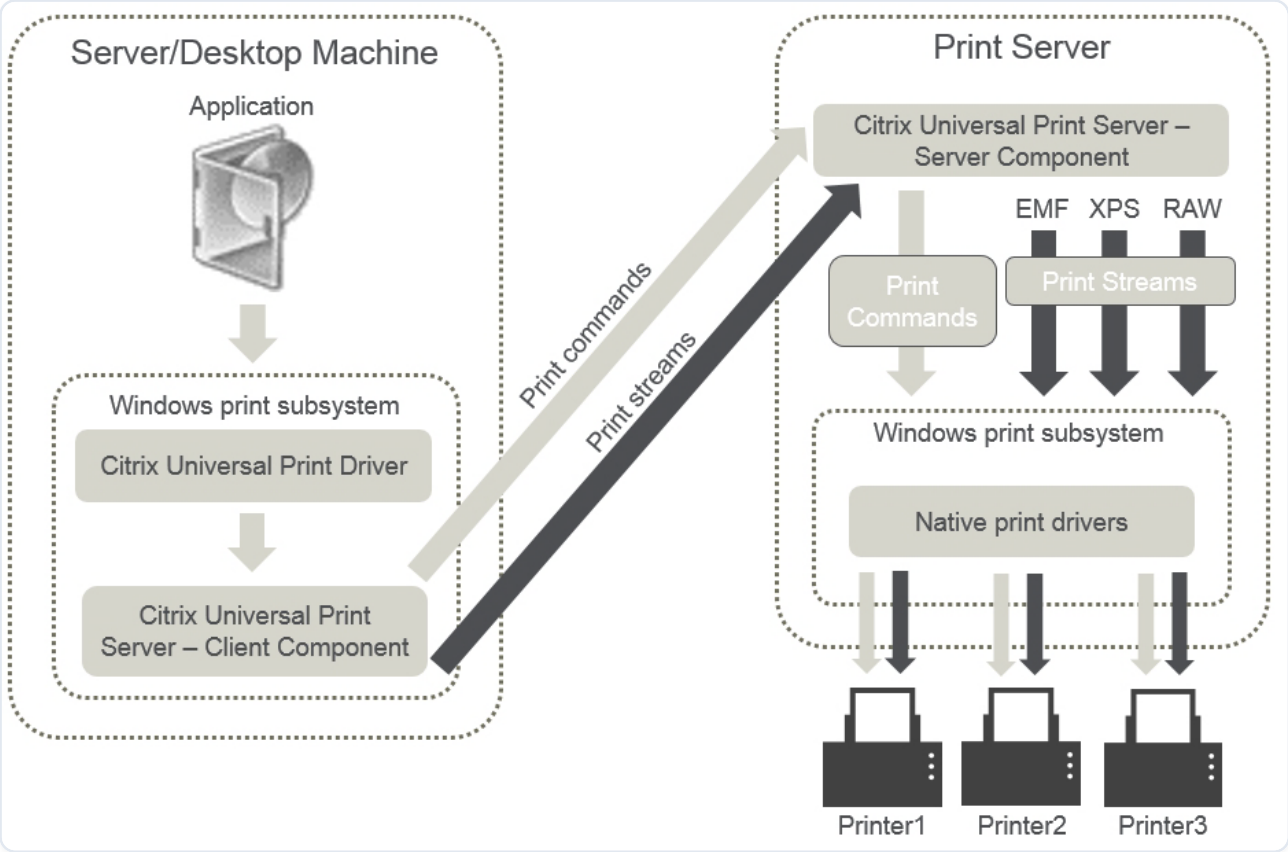
Universal Print Server 功能包括：

客户端组件 **UPClient** - 在每台预配会话网络打印机并使用通用打印驱动程序的多会话操作系统计算机上启用 UPClient。

服务器组件 **UPServer** - 在每台预配会话网络打印机并为会话打印机使用通用打印驱动程序的打印服务器上安装 UPServer（无论会话打印机是否集中预配）。

有关 Universal Print Server 的要求和设置详细信息，请参阅 系统要求 和 安装 文章。

下图显示了在使用 Universal Print Server 的环境中基于网络打印机的典型工作流。




启用 Citrix Universal Print Server 后，所有连接的网络打印机都将通过自动发现功能自动利用它。

- **自动创建** - *自动创建*是指在每个会话开始时自动创建的打印机。远程网络打印机和本地连接的客户端打印机都可以自动创建。对于每个用户拥有大量打印机的环境，请考虑仅自动创建默认客户端打印机。自动创建较少数量的打印机可减少多会话操作系统计算机上的开销（内存和 CPU）。最大限度地减少自动创建的打印机还可以缩短用户登录时间。

  自动创建的打印机基于：

  - 用户设备上安装的打印机。
  - 适用于会话的任何策略。

    自动创建策略设置使您能够限制自动创建的打印机的数量或类型。默认情况下，当自动配置用户设备上的所有打印机（包括本地连接的打印机和网络打印机）时，这些打印机在会话中可用。

  用户结束会话后，该会话的打印机将被删除。

  客户端和网络打印机自动创建具有相关的维护工作。例如，添加打印机需要您执行以下操作：

  - 更新会话打印机策略设置。
  - 使用打印机驱动程序映射和兼容性策略设置将驱动程序添加到所有多会话操作系统计算机。

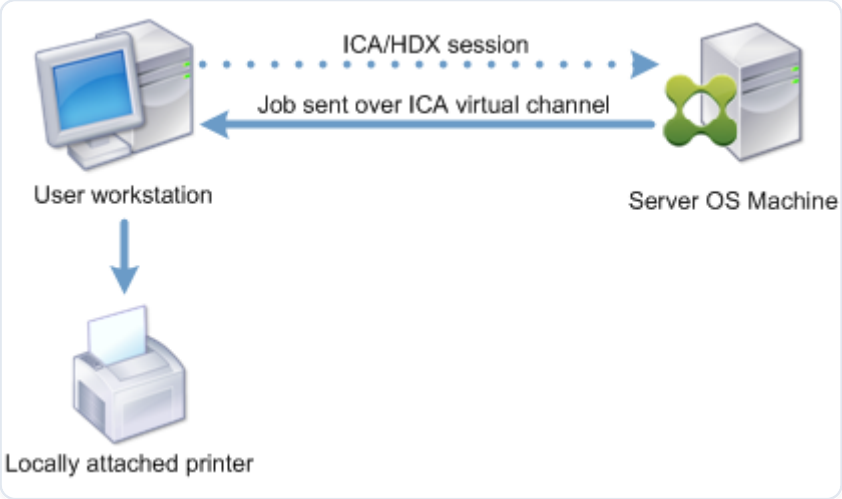
# 打印作业路由

术语“打印路径”既包括打印作业的路由路径，也包括打印作业的后台处理位置。此概念的这两个方面都很重要。路由会影响网络流量。后台处理会影响处理作业的设备上的本地资源利用率。

在此环境中，打印作业可以通过两条路径到达打印设备：通过客户端或通过网络打印服务器。这些路径分别称为客户端打印路径和网络打印路径。默认选择哪条路径取决于所使用的打印机类型。

## 本地连接的打印机

系统将作业从多会话操作系统计算机通过客户端路由到本地连接的打印机，然后再路由到打印设备。ICA® 协议优化并压缩打印作业流量。当打印设备本地连接到用户设备时，打印作业通过 ICA 虚拟通道路由。



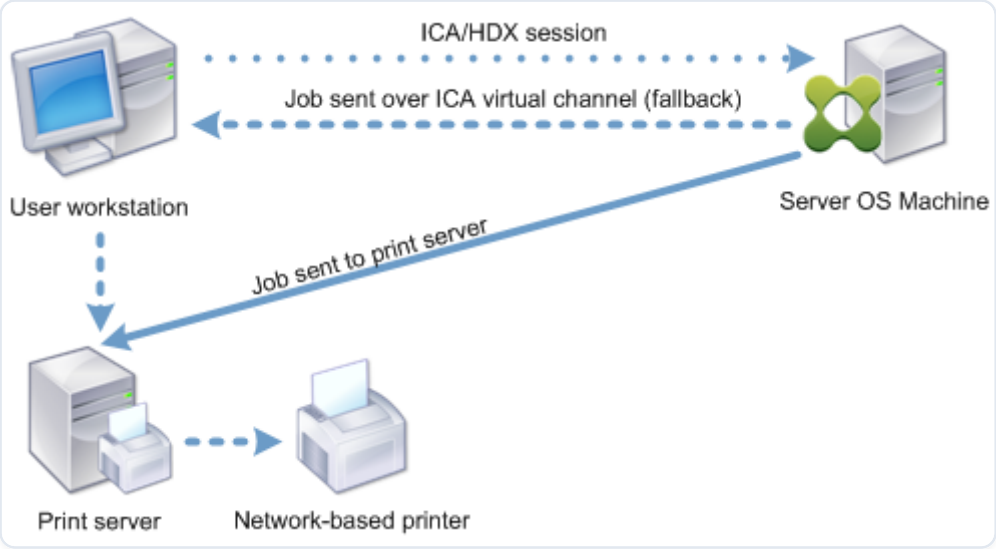

## 基于网络的打印机

默认情况下，所有发往网络打印机的打印作业都从多会话操作系统计算机通过网络直接路由到打印服务器。但是，在以下情况下，打印作业会自动通过 ICA 连接路由：

- 如果虚拟桌面或应用程序无法联系打印服务器。
- 如果多会话操作系统计算机上没有本机打印机驱动程序。

如果未启用通用打印服务器，则为网络打印配置客户端打印路径对于低带宽连接（例如广域网）非常有用，因为通过 ICA 连接发送作业可以受益于优化和流量压缩。

客户端打印路径还允许您限制流量或限制为打印作业分配的带宽。如果无法通过用户设备路由作业（例如对于没有打印功能的瘦客户端），则应配置服务质量以优先处理 ICA/HDX 流量并确保良好的会话内用户体验。




# 打印驱动程序管理

Citrix 通用打印驱动程序 (UPD) 是一种与设备无关的打印驱动程序，与大多数打印机兼容。Citrix UPD 由两个组件组成：

**服务器组件**。Citrix UPD 作为 Citrix Virtual Apps and Desktops™ VDA 安装的一部分进行安装。VDA 会随 Citrix UPD 安装以下驱动程序：“Citrix Universal Printer”（EMF 驱动程序）和“Citrix XPS Universal Printer”（XPS 驱动程序）。

| Name | Processor | Type |
| --- | --- | --- |
| Citrix Universal Printer | x64 | Type 3 - User Mode |
| Citrix XPS Universal Printer | x64 | Type 3 - User Mode |

VDA 安装程序不再提供用于控制通用打印服务器 PDF 打印机驱动程序安装的选项。PDF 打印机驱动程序现在始终自动安装。当您升级到 7.17 VDA（或更高支持版本）时，任何以前安装的 Citrix PDF 打印机驱动程序都将自动删除并替换为最新版本。

启动打印作业时，驱动程序会记录应用程序的输出，并将其发送到端点设备，不进行任何修改。

**客户端组件**。Citrix UPD 作为 Citrix Workspace™ 应用程序安装的一部分进行安装。它为 Citrix Virtual Apps and Desktops 会话获取传入的打印流。然后，它将打印流转发到本地打印子系统，在该子系统中，使用设备特定的打印机驱动程序呈现打印作业。

Citrix UPD 支持以下打印格式：

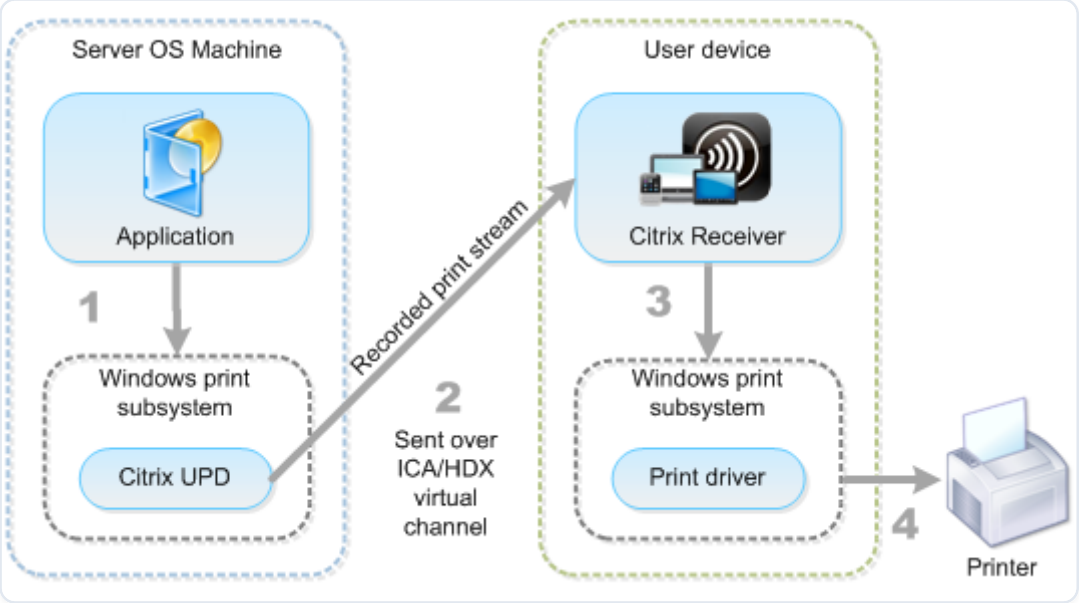
- 增强型图元文件格式 (**EMF**)，默认。EMF 是 Windows 图元文件 (WMF) 格式的 32 位版本。EMF 驱动程序只能由基于 Windows 的客户端使用。
- XML 纸张规范 (**XPS**)。XPS 驱动程序使用 XML 创建与 Adobe PDF 格式类似的平台无关的“电子纸”。

- 打印机命令语言 (**PCL5c** 和 **PCL4**)。PCL 是惠普公司最初为喷墨打印机开发的打印协议。它用于打印基本文本和图形，并广泛支持惠普 LaserJet 和多功能外围设备。
- PostScript (**PS**)。PostScript 是一种可用于打印文本和矢量图形的计算机语言。该驱动程序广泛用于低成本打印机和多功能外围设备。

PCL 和 PS 驱动程序最适合用于非 Windows 设备，例如 Mac 或 UNIX 客户端。可以使用 通用驱动程序首选项 策略设置更改 Citrix UPD 尝试使用驱动程序的顺序。

Citrix UPD（EMF 和 XPS 驱动程序）支持高级打印功能，例如装订和纸张来源选择。如果本机驱动程序使用 Microsoft 打印功能技术提供这些功能，则这些功能可用。本机驱动程序应在打印功能 XML 中使用标准化的打印架构关键字。如果使用非标准关键字，则无法使用 Citrix 通用打印驱动程序提供高级打印功能。

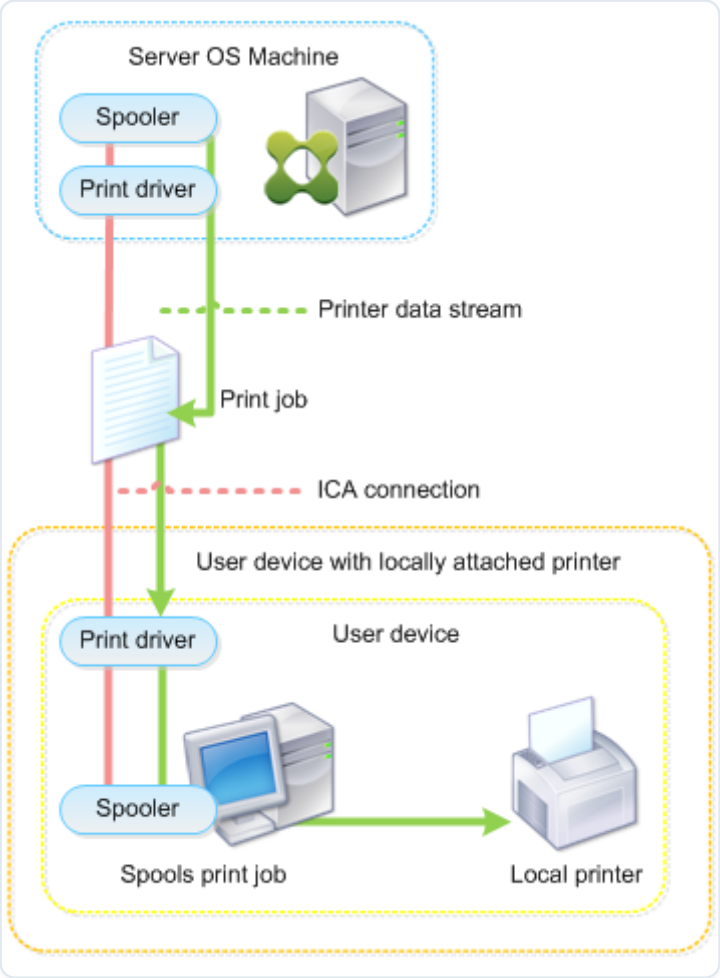
下图显示了通用打印驱动程序组件以及本地连接到设备的打印机的典型工作流。




规划驱动程序管理策略时，确定是支持通用打印驱动程序、设备专用驱动程序还是两者都支持。如果支持标准驱动程序，则必须确定：

在打印机自动创建期间，如果系统检测到连接到用户设备的新本地打印机，它会检查多会话操作系统计算机以查找所需的打印机驱动程序。默认情况下，如果 Windows 本机驱动程序不可用，系统将使用通用打印驱动程序。

多会话操作系统计算机上的打印机驱动程序和用户设备上的驱动程序必须匹配才能成功打印。下图显示了打印机驱动程序在客户端打印的两个位置中的使用方式。




- 要支持的驱动程序类型。
- 当多会话操作系统计算机中缺少打印机驱动程序时，是否自动安装它们。
- 是否创建驱动程序兼容性列表。

## 相关内容

- 打印配置示例
- 最佳实践、安全注意事项和默认操作
- 打印策略和首选项
- 预配打印机
- 维护打印环境

## 打印配置示例

选择最适合您需求和环境的打印配置选项可以简化管理。尽管默认打印配置允许用户在大多数环境中进行打印，但默认设置可能无法提供预期的用户体验，也无法为您的环境提供最佳的网络使用率和管理开销。

您的打印配置取决于：

- 您的业务需求和您现有的打印基础架构。

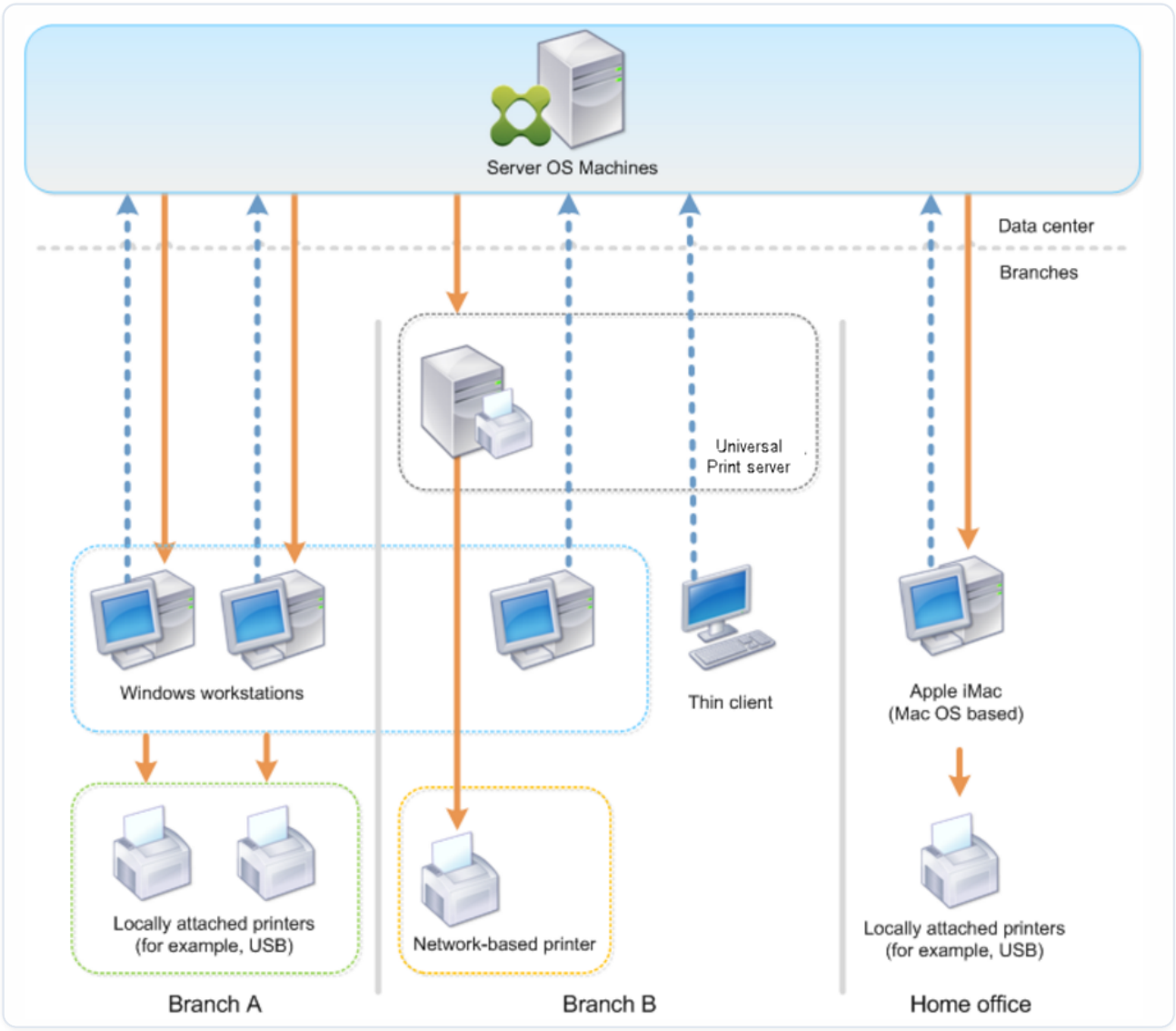
  根据您组织的需求设计您的打印配置。您现有的打印实施（例如，用户是否可以添加打印机、哪些用户可以访问哪些打印机等）在定义打印配置时可能是一个有用的指导。
- 您的组织是否有安全策略为特定用户保留打印机（例如，供人力资源或薪资部门使用的打印机）。
- 用户是否需要在离开其主要工作地点时进行打印，例如在工作站之间移动或出差的员工。

在设计打印配置时，尽量让用户在会话中获得与从本地用户设备打印时相同的体验。

## 打印部署示例

下图显示了这些用例的打印部署：

- **分支机构 A** - 一个拥有少量 Windows 工作站的小型海外分支机构。每个用户工作站都连接着一台本地专用打印机。
- **分支机构 B** - 一个拥有瘦客户端和基于 Windows 的工作站的大型分支机构。为了提高效率，该分支机构的用户共享基于网络的打印机（每层一台）。位于分支机构内的基于 Windows 的打印服务器管理打印队列。
- **家庭办公室** - 一个拥有基于 Mac OS 的用户设备的家庭办公室，该设备访问公司的 Citrix® 基础架构。该用户设备连接着一台本地打印机。




以下部分描述了能够最大限度地降低环境复杂性并简化其管理的配置。

## 自动创建的客户端打印机和 Citrix Universal™ 打印机驱动程序

在分支 A，所有用户都在基于 Windows 的工作站上工作，因此，使用自动创建的客户端打印机和通用打印机驱动程序。这些技术提供了以下优势：

- 性能 - 打印作业通过 ICA® 打印通道传输，因此，打印数据可以被压缩以节省带宽。

  为确保单个用户打印大型文档不会降低其他用户的会话性能，配置了 Citrix 策略以指定最大打印带宽。

  另一种解决方案是利用多流 ICA 连接，其中打印流量在单独的低优先级 TCP 连接中传输。当 WAN 连接上未实施服务质量 (QoS) 时，多流 ICA 是一种选择。

- 灵活性 - 使用 Citrix Universal 打印机驱动程序可确保连接到客户端的所有打印机也可以从虚拟桌面或应用程序会话中使用，而无需在数据中心集成新的打印机驱动程序。

## Citrix 通用打印服务器

在分支 B，所有打印机都是基于网络的，并且其队列在 Windows 打印服务器上进行管理，因此，Citrix 通用打印服务器是最有效的配置。

所有必需的打印机驱动程序都由本地管理员安装并在打印服务器上进行管理。将打印机映射到虚拟桌面或应用程序会话的工作方式如下：

- 对于基于 Windows 的工作站 - 本地 IT 团队帮助用户将其 Windows 工作站连接到相应的网络打印机。这使用户能够从本地安装的应用程序进行打印。

  在虚拟桌面或应用程序会话期间，本地配置的打印机通过自动创建进行枚举。如果可能，虚拟桌面或应用程序随后会作为直接网络连接连接到打印服务器。

  Citrix 通用打印服务器组件已安装并启用，因此不需要本机打印机驱动程序。如果驱动程序更新或打印机队列修改，数据中心无需额外配置。
- 对于瘦客户端 - 对于瘦客户端用户，打印机必须在虚拟桌面或应用程序会话中连接。为向用户提供最简单的打印体验，管理员为每个楼层配置一个 Citrix 会话打印机策略，以将该楼层的打印机连接为默认打印机。

  为确保即使在用户在楼层之间漫游时也能连接正确的打印机，策略会根据子网或瘦客户端的名称进行筛选。该配置，称为邻近打印，允许进行本地打印机驱动程序维护（根据委派管理模型）。

  如果需要修改或添加打印机队列，Citrix 管理员必须修改环境中的相应会话打印机策略。

由于网络打印流量将发送到 ICA 虚拟通道之外，因此实施了 QoS。ICA/HDX 流量使用的端口上的入站和出站网络流量优先于所有其他网络流量。此配置可确保用户会话不受大型打印作业的影响。

## 自动创建的客户端打印机和 Citrix 通用打印机驱动程序

对于用户在非标准工作站上工作并使用非托管打印设备的家庭办公室，最简单的方法是使用自动创建的客户端打印机和通用打印机驱动程序。

## 部署摘要

总而言之，示例部署配置如下：

- 多会话操作系统计算机上未安装打印机驱动程序。仅使用 Citrix 通用打印机驱动程序。已禁用回退到本机打印和打印机驱动程序的自动安装。
- 已配置策略以自动为所有用户创建所有客户端打印机。多会话操作系统计算机默认将直接连接到打印服务器。唯一需要的配置是启用通用打印服务器组件。
- 已为分支机构 B 的每个楼层配置会话打印机策略，并将其应用于相应楼层的所有瘦客户端。

- 为分支机构 B 实施了 QoS，以确保卓越的用户体验。

# 最佳实践、安全注意事项和默认操作

## 最佳实践

许多因素决定了特定环境的最佳打印解决方案。其中一些最佳实践可能不适用于您的站点。

- 使用 Citrix Universal™ 打印服务器。
- 使用通用打印机驱动程序或 Windows 本机驱动程序。
- 尽量减少在多会话操作系统计算机上安装的打印机驱动程序数量。
- 使用驱动程序映射到本机驱动程序。
- 切勿在生产站点上安装未经测试的打印机驱动程序。
- 避免更新驱动程序。始终尝试卸载驱动程序，重新启动打印服务器，然后安装替换驱动程序。
- 卸载未使用的驱动程序，或使用打印机驱动程序映射和兼容性策略来防止使用该驱动程序创建打印机。
- 尽量避免使用版本 2 内核模式驱动程序。
- 要确定是否支持某个打印机型号，请联系制造商或参阅 Citrix Ready 产品指南：www.citrix.com/ready。

  通常，所有 Microsoft 提供的打印机驱动程序都经过了终端服务测试，并保证与 Citrix 兼容。但是，在使用第三方打印机驱动程序之前，请咨询您的打印机驱动程序供应商，以确保该驱动程序已通过 Windows 硬件质量实验室 (WHQL) 计划的终端服务认证。Citrix 不对打印机驱动程序进行认证。

## 安全注意事项

Citrix 打印解决方案在设计上是安全的。

- Citrix Print Manager 服务持续监控并响应会话事件，例如登录和注销、断开连接、重新连接以及会话终止。它通过模拟实际会话用户来处理服务请求。
- Citrix 打印在会话中为每个打印机分配唯一的命名空间。
- Citrix 打印为自动创建的打印机设置默认安全描述符，以确保在一个会话中自动创建的客户端打印机对在其他会话中运行的用户不可访问。默认情况下，即使管理员用户可以看到并手动调整任何客户端打印机的权限，他们也无法意外地打印到其他会话的客户端打印机。

## 默认打印操作

默认情况下，如果您未配置任何策略规则，打印行为如下：

- 通用打印服务器已禁用。
- 用户设备上配置的所有打印机都会在每个会话开始时自动创建。

  此行为等同于将 Citrix 策略设置“自动创建客户端打印机”配置为“自动创建所有客户端打印机”选项。
- 系统将所有排队到本地连接到用户设备的打印机的打印作业作为客户端打印作业（即，通过 ICA® 通道和用户设备）进行路由。
- 系统直接从多会话操作系统计算机路由所有排队到网络打印机的打印作业。如果系统无法通过网络路由作业，它将通过用户设备将其作为重定向的客户端打印作业进行路由。

  此行为等同于禁用 Citrix 策略设置“直接连接到打印服务器”。
- 系统尝试将打印属性（用户打印首选项和打印设备特定设置的组合）存储在用户设备上。如果客户端不支持此操作，系统会将打印属性存储在多会话操作系统计算机上的用户配置文件中。

  此行为等同于将 Citrix 策略设置“打印机属性保留”配置为“仅当未保存在客户端时才保留在配置文件中”选项。
- 在 VDA 7.16 及更高版本中，Citrix 策略设置“自动安装收件箱打印机驱动程序”对 Windows 8 及更高版本的 Windows 操作系统没有影响，因为 V3 收件箱打印机驱动程序不包含在操作系统中。
- 在早于 7.16 的 VDA 中，如果多会话操作系统计算机上提供了打印机驱动程序的 Windows 版本，系统将使用该版本。如果打印机驱动程序不可用，系统会尝试从 Windows 操作系统安装驱动程序。如果 Windows 中没有该驱动程序，则使用 Citrix 通用打印驱动程序。

  此行为等同于启用 Citrix 策略设置“自动安装收件箱打印机驱动程序”，并将通用打印设置配置为“仅当请求的驱动程序不可用时才使用通用打印”。

  启用“自动安装内置打印机驱动程序”可能会导致安装大量本机打印机驱动程序。

**注意：**

如果您不确定打印的默认设置是什么，可以通过创建新策略并将所有打印策略规则设置为“已启用”来显示它们。出现的选项即为默认设置。

### 始终开启的日志记录

VDA 上的打印服务器和打印子系统提供了始终开启的日志记录功能。

要将日志整理为 ZIP 文件以供通过电子邮件发送，或自动将日志上传到 Citrix Insight Services，请使用 **Start-TelemetryUpload** PowerShell cmdlet。

## 打印策略和首选项

当用户从已发布的应用程序访问打印机时，您可以配置 Citrix® 策略以指定：

- 如何预配打印机（或将其添加到会话）
- 如何路由打印作业
- 如何管理打印机驱动程序

您可以为不同的用户设备、用户或任何其他应用策略筛选的对象设置不同的打印配置。

大多数打印功能通过 Citrix 打印策略设置 进行配置。打印设置遵循标准 Citrix 策略行为。

如果用户的网络帐户具有足够的权限，系统可以将打印机设置写入会话结束时的打印机对象或客户端打印设备。默认情况下，Citrix Workspace™ app 在查找其他位置的设置和首选项之前，会使用会话中打印机对象中存储的设置。

默认情况下，系统将打印机属性存储或保留在用户设备上（如果设备支持）或 Multi-session OS 计算机上的用户配置文件中。当用户在会话期间更改打印机属性时，这些更改会在计算机上的用户配置文件中更新。用户下次登录或重新连接时，用户设备会继承这些保留的设置。也就是说，用户设备上的打印机属性更改在用户注销并重新登录之前不会影响当前会话。

### 打印首选项位置

在 Windows 打印环境中，对打印首选项所做的更改可以存储在本地计算机或文档中。在此环境中，当用户修改打印设置时，这些设置会存储在以下位置：

- **在用户设备本身上** - Windows 用户可以通过右键单击“控制面板”中的打印机并选择“打印首选项”来更改用户设备上的设备设置。例如，如果选择“横向”作为页面方向，则“横向”将保存为该打印机的默认页面方向首选项。
- **在文档内部** - 在文字处理和桌面出版程序中，页面方向等文档设置通常存储在文档内部。例如，当您将文档排队打印时，Microsoft Word 通常会将您指定的打印首选项（例如页面方向和打印机名称）存储在文档内部。下次打印该文档时，这些设置会默认显示。
- **用户在会话期间所做的更改** - 如果更改是在会话中的“控制面板”中进行的，即在 Multi-session OS 计算机上进行的，则系统仅保留对自动创建的打印机的打印设置所做的更改。

- **在 Multi-session OS 计算机上** - 这些是与计算机上特定打印机驱动程序关联的默认设置。

在任何基于 Windows 的环境中保留的设置会因用户进行更改的位置而异。这也意味着在一个地方（例如在电子表格程序中）出现的打印设置可能与在其他地方（例如文档中）出现的打印设置不同。因此，应用于特定打印机的打印设置在整个会话期间可能会发生变化。

### 用户打印首选项的层次结构

由于打印首选项可以存储在多个位置，因此系统会根据特定的优先级对其进行处理。此外，需要注意的是，设备设置与文档设置是分开处理的，并且通常优先于文档设置。

默认情况下，系统始终在考虑任何其他设置之前应用用户在会话期间修改的任何打印设置（即保留的设置）。当用户打印时，系统会将存储在多会话操作系统计算机上的默认打印机设置与任何保留的或客户端打印机设置合并并应用。

### 保存用户打印首选项

Citrix 建议您不要更改打印机属性的存储位置。默认设置是将打印机属性保存在用户设备上，这是确保打印属性一致性的最简单方法。如果系统无法将属性保存在用户设备上，它会自动回退到多会话操作系统计算机上的用户配置文件。

如果以下情况适用，请查看“打印机属性保留策略”设置：

- 如果您使用不允许用户将打印机属性存储在用户设备上的旧版插件。
- 如果您在 Windows 网络上使用强制配置文件并希望保留用户的打印机属性。

## 预配打印机

### Citrix Universal™ 打印服务器

在确定适合您环境的最佳打印解决方案时，请考虑以下因素：

- Universal Print Server 提供了 Windows Print Provider 不具备的功能：图像和字体缓存、高级压缩、优化和 QoS 支持。
- 通用打印驱动程序支持 Microsoft 定义的公共设备独立设置。如果用户需要访问特定于打印机驱动程序制造商的设备设置，则 Universal Print Server 与 Windows 本机驱动程序结合使用可能是最佳解决方案。通过此配置，您可以保留 Universal Print Server 的优势，同时为用户提供对专用打印机功能的访问。需要考虑的一个权衡是，Windows 本机驱动程序需要维护。
- Citrix Universal Print Server 为网络打印机提供通用打印支持。Universal Print Server 使用通用打印驱动程序，这是多会话操作系统计算机上的单个驱动程序，允许从任何设备（包括瘦客户端和平板电脑）进行本地或网络打印。

要将 Universal Print Server 与 Windows 本机驱动程序结合使用，请启用 Universal Print Server。默认情况下，如果 Windows 本机驱动程序可用，则使用它。否则，将使用通用打印驱动程序。要指定对该行为的更改，例如仅使用 Windows 本机驱动程序或仅使用通用打印驱动程序，请更新通用打印驱动程序使用策略设置。

### 安装通用打印服务器

要使用 Universal Print Server，请按照安装文档中的说明在打印服务器上安装 UpsServer 组件并进行配置。有关详细信息，请参阅安装核心组件 和使用命令行安装。

对于要单独部署 UPClient 组件的环境，例如使用 **XenApp 6.5** 的环境：

1. 下载适用于 Windows 单会话操作系统或 Windows 多会话操作系统的 Citrix Virtual Apps and Desktops™ Virtual Delivery Agent (VDA) 独立软件包。
2. 使用使用命令行安装 中描述的命令行说明提取 VDA。
3. 从 `\Image-Full\Support\VcRedist_2013_RTM` 安装必备组件
    - Vcredist_x64 / vcredist_x86
        - 对于 32 位部署，运行 x86；对于 64 位部署，两者都运行。
4. 从 `\Image-Full\x64\Virtual Desktop Components` 或 `\Image-Full\x86\Virtual Desktop Components` 安装 cdf 先决条件。
    - Cdf_x64 / Cdf_x86
        - x86 用于 32 位，x64 用于 64 位
5. 在 `\Image-Full\x64\Virtual Desktop Components` 或 `\Image-Full\x86\Virtual Desktop Components` 中找到 UPClient 组件。
6. 通过提取然后启动组件的 MSI 来安装 UPClient 组件。
7. 安装 UPClient 组件后需要重新启动。

### 退出通用打印服务器的 CEIP

安装 Universal Print Server 时，您将自动加入 Citrix 客户体验改善计划 (CEIP)。首次数据上传将在安装日期和时间起七天后进行。

要退出 CEIP，请编辑注册表项 **`HKLM\Software\Citrix\Universal Print Server\CEIPEnabled`** 并将 **DWORD** 值设置为 **0**。

要重新加入，请将 DWORD 值设置为 1。

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

有关详细信息，请参阅 Citrix Insight Services。

### 配置通用打印服务器

使用以下 Citrix 策略设置来配置 Universal Print Server。有关详细信息，请参阅屏幕上的策略设置帮助。

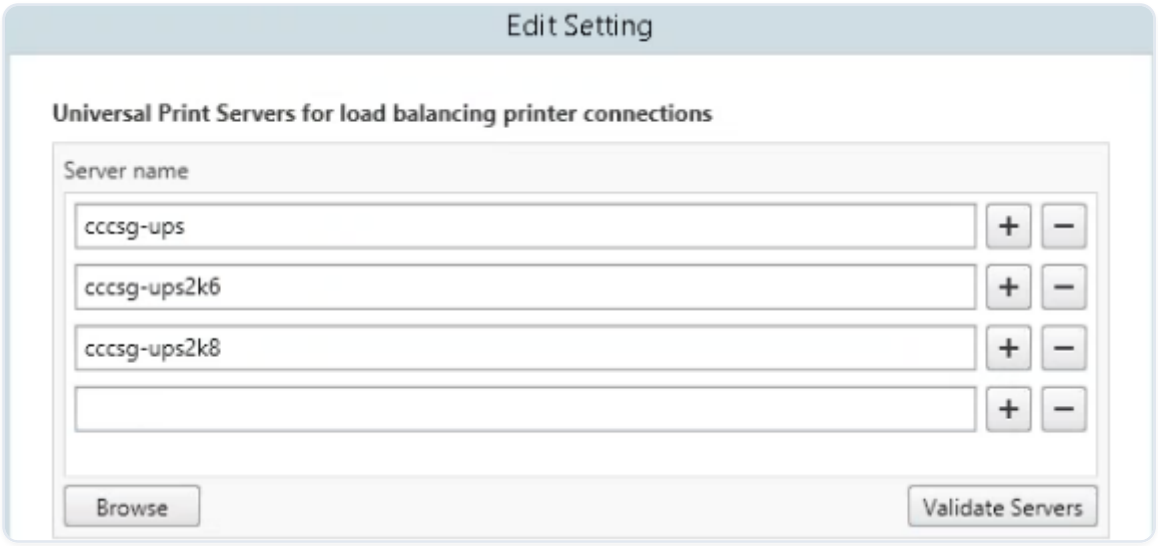
- **启用 Universal Print Server**。Universal Print Server 默认处于禁用状态。启用 Universal Print Server 时，您可以选择在 Universal Print Server 不可用时是否使用 Windows 打印提供程序。启用 Universal Print Server 后，用户可以通过 Windows 打印提供程序和 Citrix 提供程序接口添加和枚举网络打印机。
- **Universal Print Server 打印数据流 (CGP) 端口**。指定 Universal Print Server 打印数据流 CGP（通用网关协议）侦听器使用的 TCP 端口号。默认为 **7229**。
- **Universal Print Server Web 服务 (HTTP/SOAP) 端口**。指定 Universal Print Server 侦听器用于传入 HTTP/SOAP 请求的 TCP 端口号。默认为 **8080**。

要更改 Universal Print Server 与 Citrix Virtual Apps and Desktops VDA 通信的默认 HTTP 端口 8080，还必须在 Universal Print Server 计算机上创建以下注册表并修改端口号值：

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies`
"UpsHttpPort"=DWORD:\<portnumber\>

此端口号必须与 Studio 中的 HDX 策略、Universal Print Server Web 服务 (HTTP/SOAP) 端口匹配。

- **Universal Print Server 打印流输入带宽限制 (kbps)**。指定使用 CGP 从每个打印作业传输到 Universal Print Server 的打印数据传输速率的上限（以千比特每秒为单位）。默认为 0（无限制）。
- **用于负载平衡的 Universal Print Server**。此设置列出了在评估其他 Citrix 打印策略设置后，用于在会话启动时建立的打印机连接进行负载平衡的 Universal Print Server。为优化打印机创建时间，Citrix 建议所有打印服务器都具有相同的共享打印机集。




- **Universal Print Server 脱机阈值**。指定负载平衡器应等待不可用打印服务器恢复的时间，然后才确定该服务器永久脱机并将其负载重新分配给其他可用打印服务器。默认值为 180（秒）。

在 Delivery Controller™ 上修改打印策略后，策略更改可能需要几分钟才能应用于 VDA。

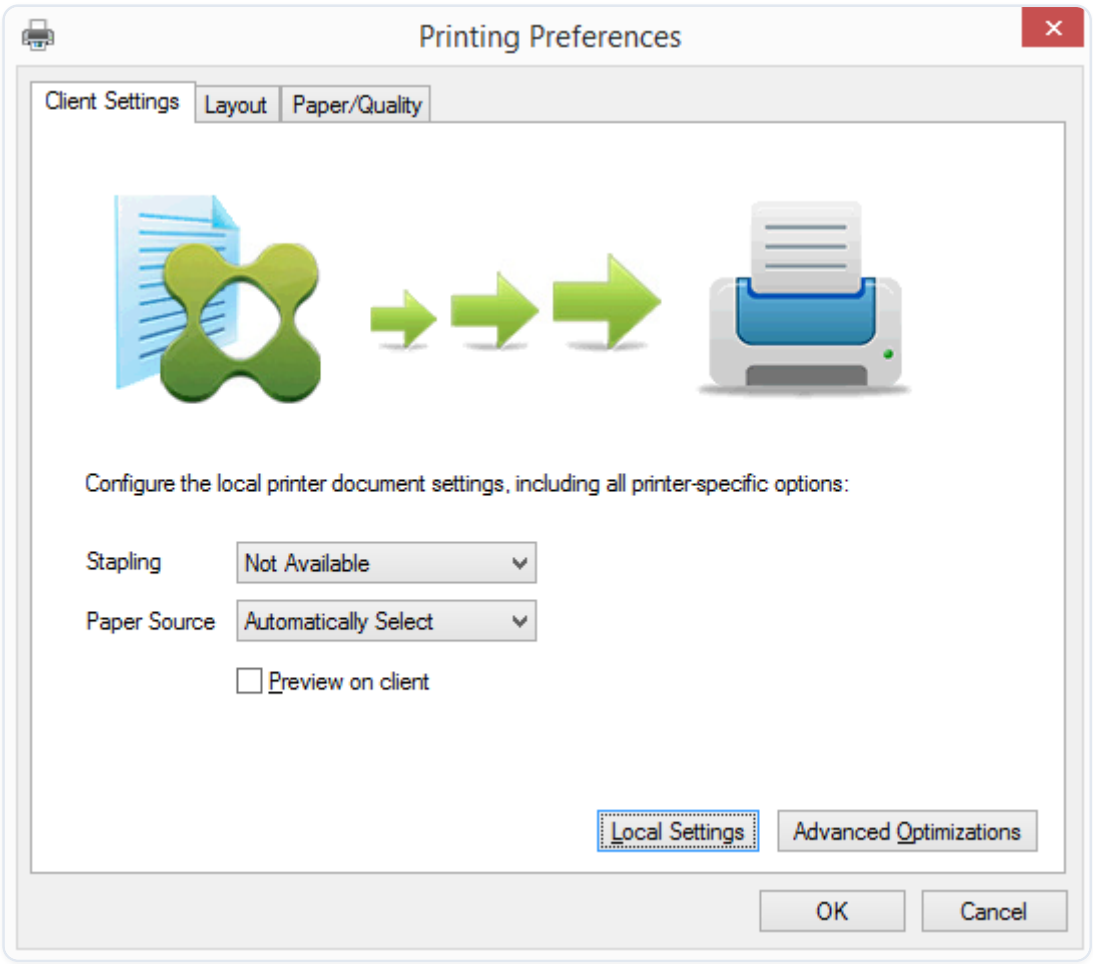
**与其他策略设置的交互** - Universal Print Server 遵循其他 Citrix 打印策略设置，并按照下表所示与它们进行交互。提供的信息假定 Universal Print Server 策略设置已启用，Universal Print Server 组件已安装，并且策略设置已应用。

| 策略设置 | 交互 |
| --- | --- |
| 客户端打印机重定向，自动创建客户端打印机 | 启用 Universal Print Server 后，客户端网络打印机将使用通用打印驱动程序而不是本机驱动程序创建。用户看到的打印机名称与以前相同。 |
| 会话打印机 | 使用 Citrix Universal Print Server 解决方案时，将遵循通用打印驱动程序策略设置。 |
| 直接连接到打印服务器 | 启用 Universal Print Server 且通用打印驱动程序使用策略设置配置为仅使用通用打印时，可以使用通用打印驱动程序创建到打印服务器的直接网络打印机连接。 |
| UPD 首选项 | 支持 EMF 和 XPS 驱动程序。 |

**对用户界面的影响** - Universal Print Server 使用的 Citrix 通用打印驱动程序会禁用以下用户界面控件：

- 在“打印机属性”对话框中，“本地打印机设置”按钮
- 在“文档属性”对话框中，“本地打印机设置”和“在客户端上预览”按钮

Citrix 通用打印驱动程序（EMF 和 XPS 驱动程序）支持高级打印功能，例如装订和纸张来源。如果会话中映射到 UPD 的客户端或网络打印机支持这些功能，用户可以从自定义 UPD 打印对话框中选择“装订”或“纸张来源”选项。




要设置非标准打印机设置（例如装订和安全 PIN），请在客户 UPD 打印对话框中为使用 Citrix UPD EMF 或 XPS 驱动程序的任何客户端映射打印机选择**本地设置**。映射打印机的**打印首选项**对话框将在会话外部的客户端上显示，允许用户更改任何打印机选项，并且修改后的打印机设置将在打印该文档时用于活动会话。

如果本机驱动程序使用 Microsoft 打印功能技术提供这些功能，则这些功能可用。本机驱动程序应在打印功能 XML 中使用标准化的打印架构关键字。如果使用非标准关键字，则无法使用 Citrix 通用打印驱动程序提供高级打印功能。

使用 Universal Print Server 时，Citrix Print Provider 的“添加打印机向导”与 Windows Print Provider 的“添加打印机向导”相同，但有以下例外：

- 按名称或地址添加打印机时，可以为打印服务器提供 HTTP/SOAP 端口号。该端口号将成为打印机名称的一部分并显示在显示屏中。

- 如果 Citrix 通用打印驱动程序使用策略设置指定必须使用通用打印，则在选择打印机时会显示通用打印驱动程序名称。Windows 打印提供程序无法使用通用打印驱动程序。

Citrix 打印提供程序不支持客户端呈现。

有关通用打印服务器的更多信息，请参阅 CTX200328。

## 自动创建的客户端打印机

为客户端打印机提供了以下通用打印解决方案：

- **Citrix Universal Printer** - 在会话开始时创建的通用打印机，不与特定打印设备绑定。Citrix Universal Printer 无需在登录期间枚举可用的客户端打印机，这可以大大减少资源使用并缩短用户登录时间。Universal Printer 可以打印到任何客户端打印设备。

  Citrix Universal Printer 可能不适用于您的环境中所有用户设备或 Citrix Workspace™ 应用程序。Citrix Universal Printer 需要 Windows 环境，并且不支持 Citrix Offline Plug-in 或流式传输到客户端的应用程序。对于此类环境，请考虑使用自动创建的客户端打印机和通用打印驱动程序。

  要为非 Windows Citrix Workspace 应用程序使用通用打印解决方案，请使用其他基于 PostScript/PCL 并自动安装的通用打印驱动程序之一。

- **Citrix 通用打印驱动程序** - 一种与设备无关的打印机驱动程序。如果您配置了 Citrix 通用打印驱动程序，系统将默认使用基于 EMF 的通用打印驱动程序。

  Citrix 通用打印驱动程序创建的打印作业可能比旧版或不那么先进的打印机驱动程序小。但是，可能需要设备专用驱动程序来优化专业打印机的打印作业。

**配置通用打印** - 使用以下 Citrix 策略设置来配置通用打印。有关更多信息，请参阅屏幕上的策略设置帮助。

- 通用打印驱动程序使用。指定何时使用通用打印。
- 自动创建通用打印机。当使用与通用打印兼容的用户设备时，启用或禁用为会话自动创建通用 Citrix Universal Printer 对象。默认情况下，不自动创建通用 Universal Printer 对象。
- 通用驱动程序首选项。指定系统尝试使用通用打印驱动程序的顺序，从列表中的第一个条目开始。您可以添加、编辑或删除驱动程序，并更改列表中驱动程序的顺序。
- 通用打印预览首选项。指定是否对自动创建的或通用打印机使用打印预览功能。
- 通用打印 EMF 处理模式。控制在 Windows 用户设备上处理 EMF 后台打印文件的方法。默认情况下，EMF 记录直接后台打印到打印机。直接后台打印到打印机可让后台打印程序更快地处理记录，并使用更少的 CPU 资源。

有关更多策略，请参阅优化打印性能。要更改纸张大小、打印质量、颜色、双面打印和份数等设置的默认值，请参阅CTX113148。

**从用户设备自动创建打印机** - 默认情况下，在会话开始时，系统会自动创建用户设备上的所有打印机。您可以控制向用户预配哪些（如果有）类型的打印机，并阻止自动创建。

使用 Citrix 策略设置 自动创建客户端打印机来控制自动创建。您可以指定：

- 用户设备可见的所有打印机（包括网络打印机和本地连接的打印机）在每个会话开始时自动创建（默认）
- 物理连接到用户设备的所有本地打印机均自动创建
- 仅自动创建用户设备的默认打印机
- 禁用所有客户端打印机的自动创建

“自动创建客户端打印机”设置要求“客户端打印机重定向”设置处于“允许”状态（默认值）。

## 将网络打印机分配给用户

默认情况下，用户设备上的网络打印机在会话开始时自动创建。系统允许您通过指定要在每个会话中创建的网络打印机来减少枚举和映射的网络打印机数量。此类打印机称为会话打印机。

您可以按 IP 地址筛选会话打印机策略以提供邻近打印。邻近打印使用户能够在指定 IP 地址范围内自动访问该范围内存在的网络打印设备。邻近打印由 Citrix Universal Print Server 提供，不需要本节中介绍的配置。

邻近打印可能涉及以下场景：

- 公司内部网络使用 DHCP 服务器运行，该服务器自动为用户分配 IP 地址。
- 公司内所有部门都有唯一的指定 IP 地址范围。
- 网络打印机存在于每个部门的 IP 地址范围内。

配置了邻近打印后，当员工从一个部门到另一个部门时，无需进行额外的打印设备配置。一旦用户设备在新部门的 IP 地址范围内被识别，它将可以访问该范围内的所有网络打印机。

**配置要在会话中重定向的特定打印机** - 要创建管理员分配的打印机，请配置 Citrix 策略设置“会话打印机”。使用以下方法之一将网络打印机添加到该策略：

- 使用 `\\servername\printername` 格式输入打印机 UNC 路径。
- 浏览到网络上的打印机位置。
- 浏览特定服务器上的打印机。使用 `\\servername` 格式输入服务器名称，然后单击“浏览”。

重要提示：服务器会合并所有已应用策略的所有已启用会话打印机设置，从最高优先级到最低优先级。当打印机在多个策略对象中配置时，自定义默认设置仅从配置了该打印机的最高优先级策略对象中获取。

使用“会话打印机”设置创建的网络打印机可以根据会话发起位置而有所不同，例如通过筛选子网等对象。

**为会话指定默认网络打印机** - 默认情况下，用户的主要打印机用作会话的默认打印机。使用 Citrix 策略设置“默认打印机”来更改会话中用户设备上默认打印机的建立方式。

1. 在“默认打印机设置”页面上，为“选择客户端的默认打印机”选择一个设置：
    - 网络打印机名称。使用“会话打印机”策略设置添加的打印机将显示在此菜单中。选择要用作此策略默认值的网络打印机。
    - 不调整用户的默认打印机。使用当前的终端服务或 Windows 用户配置文件设置作为默认打印机。有关详细信息，请参阅屏幕上的策略设置帮助。
2. 将策略应用于您要影响的用户组（或其他筛选对象）。

**配置邻近打印** - 邻近打印也由 Citrix Universal Print Server 提供，它不需要此处描述的配置。

1. 为每个子网（或与打印机位置对应）创建单独的策略。
2. 在每个策略中，将该子网地理位置中的打印机添加到“会话打印机”设置。
3. 将“默认打印机”设置设为“不调整用户的默认打印机”。
4. 按客户端 IP 地址筛选策略。请务必更新这些策略以反映 DHCP IP 地址范围的更改。

# 维护打印环境

维护打印环境包括：

- 管理打印机驱动程序
- 优化打印性能
- 显示打印机和管理打印队列

## 管理打印机驱动程序

为最大程度地减少管理开销和打印驱动程序问题的可能性，Citrix 建议使用 Citrix Universal™ 打印驱动程序。

如果自动创建失败，系统默认安装 Windows 提供的 Windows 本机打印机驱动程序。如果驱动程序不可用，系统将回退到通用打印驱动程序。有关打印机驱动程序默认值的详细信息，请参阅 最佳做法、安全注意事项和默认操作。

如果 Citrix Universal 打印驱动程序并非适用于所有情况，请映射打印机驱动程序以最大程度地减少在多会话操作系统计算机上安装的驱动程序数量。此外，映射打印机驱动程序使您能够：

- 允许指定的打印机仅使用 Citrix Universal 打印驱动程序
- 允许或阻止使用指定驱动程序创建打印机
- 用好的打印机驱动程序替换过时或损坏的驱动程序
- 用 Windows 服务器上可用的驱动程序替换客户端驱动程序名称

**阻止自动安装打印机驱动程序** - 应禁用打印驱动程序的自动安装，以确保多会话操作系统计算机之间的一致性。这可以通过 Citrix® 策略、Microsoft 策略或两者来实现。要阻止自动安装 Windows 本机打印机驱动程序，请禁用 Citrix 策略设置“自动安装内置打印机驱动程序”。

**映射客户端打印机驱动程序** - 每个客户端在登录期间提供有关客户端打印机的信息，包括打印机驱动程序名称。在客户端打印机自动创建期间，将选择与客户端提供的打印机型号名称对应的 Windows 服务器打印机驱动程序名称。然后，自动创建过程使用已识别的可用打印机驱动程序来构建重定向的客户端打印队列。

以下是定义驱动程序替换规则和编辑映射客户端打印机驱动程序打印设置的一般过程：

1. 要为自动创建的客户端打印机指定驱动程序替换规则，请通过添加客户端打印机驱动程序名称并从“查找打印机驱动程序”菜单中选择要替换客户端打印机驱动程序的服务器驱动程序来配置 Citrix 策略设置“打印机驱动程序映射和兼容性”。您可以在此设置中使用通配符。例如，要强制所有 HP 打印机使用特定驱动程序，请在策略设置中指定 HP*。
2. 要禁用打印机驱动程序，请选择驱动程序名称并选择“不创建”设置。
3. 根据需要，编辑现有映射、删除映射或更改列表中驱动程序条目的顺序。
4. 要编辑映射客户端打印机驱动程序的打印设置，请选择打印机驱动程序，单击“设置”，然后指定打印质量、方向和颜色等设置。如果指定的打印选项不受打印机驱动程序支持，则该选项无效。此设置将覆盖用户在上一会话中设置的保留打印机设置。
5. Citrix 建议在映射驱动程序后详细测试打印机的行为，因为某些打印机功能可能仅在特定驱动程序下可用。

用户登录时，系统会在设置客户端打印机之前检查客户端打印机驱动程序兼容性列表。

# 优化打印性能

要优化打印性能，请使用通用打印服务器和通用打印驱动程序。以下策略控制打印优化和压缩：

- 通用打印优化默认值。指定为会话创建通用打印机时的默认设置：
  - “所需图像质量”指定应用于通用打印的默认图像压缩限制。默认情况下，启用“标准质量”，这意味着用户只能使用标准或降低质量的压缩来打印图像。
  - “启用重量级压缩”启用或禁用在不损失图像质量的情况下，将带宽降低到超出“所需图像质量”设置的压缩级别。默认情况下，重量级压缩处于禁用状态。
  - 图像和字体缓存设置指定是否缓存打印流中多次出现的图像和字体，确保每个唯一的图像或字体仅发送到打印机一次。默认情况下，嵌入式图像和字体会被缓存。
  - 允许非管理员修改这些设置指定用户是否可以在会话中更改默认打印优化设置。默认情况下，不允许用户更改默认打印优化设置。
- 通用打印图像压缩限制。定义使用通用打印驱动程序打印的图像可用的最大质量和最小压缩级别。默认情况下，图像压缩限制设置为“最佳质量”（无损压缩）。
- 通用打印质量限制。指定会话中生成打印输出可用的最大每英寸点数 (dpi)。默认情况下，未指定限制。

默认情况下，所有发往网络打印机的打印作业都从多会话操作系统计算机通过网络直接路由到打印服务器。如果网络延迟较大或带宽有限，请考虑通过 ICA® 连接路由打印作业。为此，请禁用 Citrix 策略设置“直接连接到打印服务器”。通过 ICA 连接发送的数据会进行压缩，因此数据在 WAN 上传输时消耗的带宽会更少。

**通过限制打印带宽来提高会话性能** - 当从多会话操作系统计算机向用户打印机打印文件时，其他虚拟通道（例如视频）可能会由于带宽竞争而导致性能下降，尤其是在用户通过较慢的网络访问服务器时。为防止此类性能下降，您可以限制用户打印所使用的带宽。通过限制打印的数据传输速率，您可以在 HDX™ 数据流中为视频、击键和鼠标数据的传输提供更多可用带宽。

> **重要提示：**
>
> 即使没有其他通道在使用，打印机带宽限制也始终会强制执行。
>
> 使用以下 Citrix 策略带宽打印机设置来配置打印带宽会话限制。要为站点设置限制，请使用 Studio 执行此任务。要为单个服务器设置限制，请在每台多会话操作系统计算机上本地使用 Windows 中的组策略管理控制台执行此任务。

- 打印机重定向带宽限制设置指定了以千比特每秒 (kbps) 为单位的可用打印带宽。

- 打印机重定向带宽限制百分比设置将可用打印带宽限制为总可用带宽的某个百分比。

  注意：要使用打印机重定向带宽限制百分比设置将带宽指定为百分比，还需要启用总体会话带宽限制。

  如果您为这两个设置都输入了值，则应用限制最严格的设置（较低的值）。

要获取有关打印带宽的实时信息，请使用 Citrix Director。

## 负载均衡通用打印服务器

通用打印服务器解决方案可以通过向负载均衡解决方案中添加更多打印服务器来扩展。由于每个 VDA 都有自己的负载均衡器来将打印负载分配给所有打印服务器，因此不存在单点故障。

使用策略设置 Universal Print Servers for load balancing 和 Universal Print Servers out-of-service threshold，将打印负载分配到负载均衡解决方案中的所有打印服务器。

如果打印服务器发生意外故障，每个 VDA 中的负载均衡器的故障转移机制会自动将分配给故障打印服务器的打印机连接重新分配给其他可用打印服务器，从而使所有现有和传入会话正常运行，而不会影响用户体验，也无需管理员立即干预。

管理员可以使用一组性能计数器来监控 VDA 上负载均衡打印服务器的活动，以跟踪以下内容：

- VDA 上负载均衡打印服务器的列表及其状态（可用、不可用）
- 每个打印服务器接受的打印机连接数
- 每个打印服务器上失败的打印机连接数
- 每个打印服务器上活动的打印机连接数
- 每个打印服务器上待处理的打印机连接数

## 显示和管理打印队列

下表总结了您可以在何处显示打印机以及管理环境中的打印队列。

| | 打印路径 | 位置 |
|---|---|---|
| 客户端打印机（连接到用户设备的打印机） | 客户端打印路径 | UAC 启用：位于 Microsoft 管理控制台中的打印管理管理单元；UAC 禁用：Windows 8 之前：控制面板，Windows 8：打印管理管理单元 |

| | 打印路径 | 位置 |
|---|---|---|
| 网络打印机（网络打印服务器上的打印机） | 网络打印路径 | UAC 启用：打印服务器 \> 位于 Microsoft 管理控制台中的打印管理管理单元；UAC 禁用：打印服务器 \> 控制面板 |
| 网络打印机（网络打印服务器上的打印机） | 客户端打印路径 | UAC 启用：打印服务器 \> 位于 Microsoft 管理控制台中的打印管理管理单元；UAC 禁用：Windows 8 之前：控制面板，Windows 8：打印管理管理单元 |
| 本地网络服务器打印机（从网络打印服务器添加到多会话操作系统计算机的打印机） | 网络打印路径 | UAC 启用时：打印服务器 \> 控制面板；UAC 禁用时：打印服务器 \> 控制面板 |

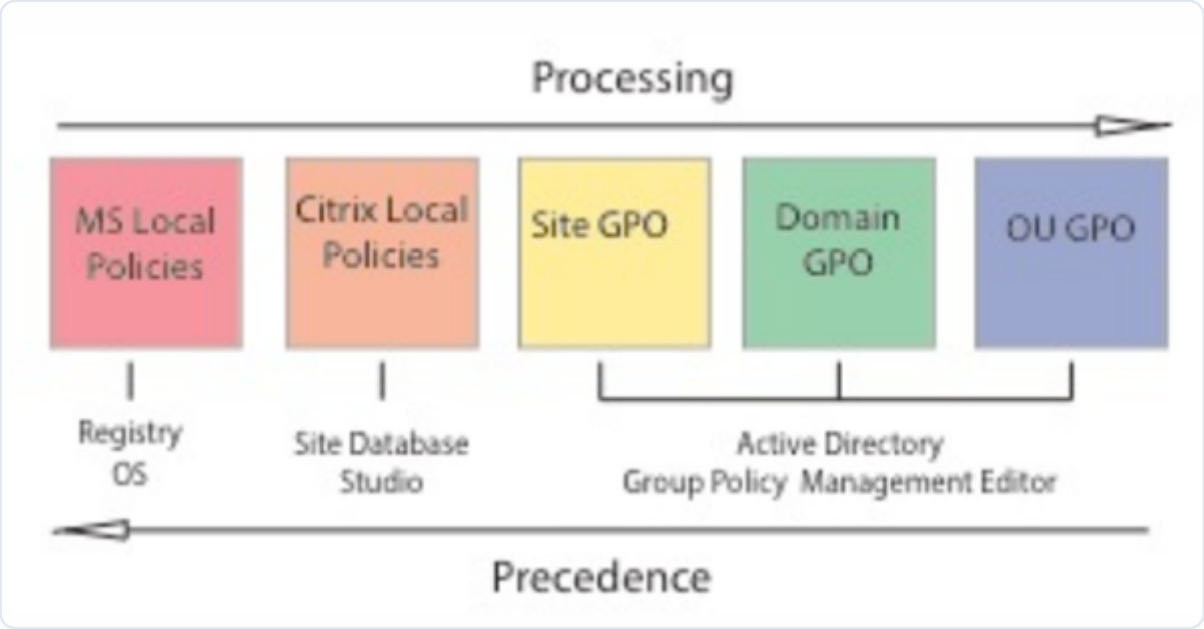
**注意：**

使用网络打印路径的网络打印机的打印队列是私有的，无法通过系统进行管理。

# 策略

策略是设置的集合，用于定义如何管理一组用户、设备或连接类型的会话、带宽和安全性。

您可以将策略设置应用于物理机和虚拟机或用户。您可以在本地级别或 Active Directory 中的安全组中将设置应用于单个用户。这些配置定义了特定的条件和规则。如果您未明确分配策略，则这些设置将应用于所有连接。




您可以在网络的不同级别应用策略。放置在组织单位 GPO 级别的策略设置在网络上具有最高优先级。域 GPO 级别的策略会覆盖站点组策略对象级别的策略。站点组策略对象级别会覆盖 Microsoft 和 Citrix 本地策略级别上的任何冲突策略。

所有 Citrix 本地策略都在 Citrix Studio 控制台中创建和管理，并存储在站点数据库中。组策略使用 Microsoft 组策略管理控制台 (GPMC) 创建和管理，并存储在 Active Directory 中。Microsoft 本地策略在 Windows 操作系统中创建，并存储在注册表中。

Studio 使用建模向导帮助管理员比较模板和策略中的配置设置，以帮助消除冲突和冗余设置。管理员可以使用 GPMC 设置 GPO 来配置设置。此外，还可以将它们应用于网络不同级别的目标用户集。

这些 GPO 存储在 Active Directory 中。出于安全考虑，大多数 IT 人员对这些设置的管理访问权限受到限制。

设置根据优先级及其条件进行合并。任何禁用的设置都会覆盖排名较低的已启用设置。未配置的策略设置将被忽略，并且不会覆盖排名较低的设置。

本地策略也可能与 Active Directory 中的组策略发生冲突，这些策略可能会根据情况相互覆盖。

所有策略按以下顺序处理：

1. 最终用户使用域凭据登录到计算机。
2. 凭据发送到域控制器。
3. Active Directory 应用所有策略（最终用户、端点、组织单位和域）。
4. 最终用户登录到 Citrix Workspace™ 应用程序并访问应用程序或桌面。
5. Citrix 和 Microsoft 策略针对最终用户和托管资源的计算机进行处理。
6. Active Directory 确定策略设置的优先级。然后，它将这些设置应用于端点设备的注册表和托管资源的计算机。
7. 最终用户从资源注销。最终用户和端点设备的 Citrix 策略不再处于活动状态。
8. 最终用户从用户设备注销，这将释放 GPO 用户策略。
9. 最终用户关闭设备，这将释放 GPO 计算机策略。

为用户、设备和计算机组创建策略时，某些成员可能具有不同的要求，并且需要对某些策略设置进行例外处理。例外情况通过 Studio 和 GPMC 中的筛选器进行设置，这些筛选器确定策略影响的对象。

> **注意：** 我们不支持在同一个 GPO 中混合使用 Windows 和 Citrix 策略。

# 使用策略

配置 Citrix® 策略以控制用户访问和会话环境。Citrix 策略是控制连接、安全和带宽设置的最有效方法。您可以为特定用户组、设备或连接类型创建策略。每个策略可以包含多个设置。

## 使用 Citrix 策略的工具

您可以将以下工具与 Citrix 策略结合使用。

- **Studio** - 如果您是没有管理组策略权限的 Citrix 管理员，请使用 Studio 为您的站点创建策略。使用 Studio 创建的策略存储在站点数据库中。更新会在虚拟桌面向代理注册时或用户连接到该虚拟桌面时推送到虚拟桌面。

- **本地组策略编辑器**（Microsoft 管理控制台管理单元）- 如果您的网络环境使用 Active Directory 并且您有权管理组策略，则可以使用本地组策略编辑器为您的站点创建策略。您配置的设置会影响您在组策略管理控制台中指定的组策略对象 (GPO)。

> **重要提示：**
>
> 使用本地组策略编辑器配置某些策略设置。这些策略设置包括与向控制器注册 VDA 相关的设置。此外，还包括与 Microsoft App-V 服务器相关的设置。

## 策略处理顺序和优先级

组策略设置按以下顺序处理：

1. 本地 GPO
2. XenApp 或 XenDesktop® 站点 GPO（存储在站点数据库中）
3. 站点级 GPO
4. 域级 GPO
5. 组织单位

但是，如果发生冲突，最后处理的策略设置将覆盖之前处理的设置。此配置意味着策略设置按以下顺序优先：

1. 组织单位
2. 域级 GPO
3. 站点级 GPO
4. XenApp® 或 XenDesktop 站点 GPO（存储在站点数据库中）
5. 本地 GPO

例如，Citrix 管理员使用 Studio 创建一个策略（策略 A），该策略为公司的销售员工启用客户端文件重定向。同时，另一位管理员使用组策略编辑器创建一个策略（策略 B），该策略为销售员工禁用客户端文件重定向。当销售员工登录到虚拟桌面时，将应用策略 B，而忽略策略 A。原因是策略 B 在域级别处理，而策略 A 在 XenApp 或 XenDesktop 站点 GPO 级别处理。

但是，当用户启动 ICA® 或远程桌面协议 (RDP) 会话时，Citrix 会话设置会覆盖在 Active Directory 策略中配置的相同设置或使用远程桌面会话主机配置的设置。此设置包括与典型 RDP 客户端连接设置相关的设置。RDP 客户端连接设置的示例包括桌面壁纸、菜单动画和拖动时查看窗口内容。

使用多个策略时，您可以优先处理包含冲突设置的策略。有关详细信息，请参阅 比较、确定优先级、建模和故障排除策略。

## Citrix 策略的工作流程

配置策略的过程如下：

1. 创建策略。
2. 配置策略设置。
3. 将策略分配给计算机和用户对象。
4. 确定策略的优先级。
5. 通过运行 Citrix 组策略建模向导验证有效策略。

> **注意：**
>
> 您可以通过导航到 **Policies > Modeling**（策略 > 建模）选项卡，然后单击 **Actions**（操作）窗格中的 **Launch Modeling Wizard**（启动建模向导）来打开 Citrix 组策略建模向导。**Modeling**（建模）选项卡在 Citrix Cloud 中托管的 Studio 中不可用。

## 导航 Citrix 策略和设置

在本地组策略编辑器中，策略和设置分为两类：计算机配置和用户配置。每个类别都有一个 Citrix 策略节点。有关导航和使用此管理单元的详细信息，请参阅 Microsoft 文档。

在 Studio 中，策略设置根据其影响的功能或特性进行分类。例如，**Profile Management**（配置文件管理）部分包含配置文件管理的策略设置。

- 计算机设置（应用于计算机的策略设置）定义虚拟桌面的行为，并在虚拟桌面启动时应用。即使虚拟桌面上没有活动用户会话，这些设置也适用。用户设置定义了使用 ICA 连接时的用户体验。用户策略在用户使用 ICA 连接或重新连接时应用。如果用户使用 RDP 连接或直接登录到控制台，则不应用用户策略。

  要访问策略、设置或模板，请在 Studio 导航窗格中选择 **策略**。

  - **策略** 选项卡列出了所有策略。当您选择一个策略时，右侧会显示以下选项卡：
    - 概述（名称、优先级、启用/禁用状态和描述）
    - 设置（已配置设置的列表）
    - 分配给（分配了策略的用户和计算机对象）。 有关详细信息，请参阅 创建策略。

- **模板** 选项卡列出了 Citrix 提供的模板以及您创建的自定义模板。当您选择一个模板时，右侧会显示以下选项卡：
  - 描述（您可能希望使用此模板的原因）
  - 设置（已配置设置的列表）。 有关详细信息，请参阅 策略模板。
- **比较** 选项卡使您能够将策略或模板中的设置与其他策略或模板中的设置进行比较。例如，您可能需要验证设置值以确保符合最佳实践。有关详细信息，请参阅 比较、确定优先级、建模和故障排除策略。
- 在 **建模** 选项卡中，您可以模拟使用 Citrix 策略的连接方案。有关详细信息，请参阅 比较、确定优先级、建模和故障排除策略。

> **注意：**
>
> **建模** 选项卡在 Citrix Cloud 中托管的 Studio 中不可用。

要在策略或模板中搜索设置：

a. 选择策略或模板。
b. 在 **操作** 窗格中选择 **编辑策略** 或 **编辑模板**。
c. 在“设置”页面上，开始键入设置的名称。

您可以通过选择以下项来优化搜索：

- 特定产品版本
- 某个类别（例如，“带宽”）
- “仅查看选定项”复选框
- 仅搜索已添加到所选策略的设置。

对于未筛选的搜索，请选择 **所有设置**。

- 要在策略中搜索设置：

a. 选择策略。
b. 选择 **设置** 选项卡并键入设置的名称。

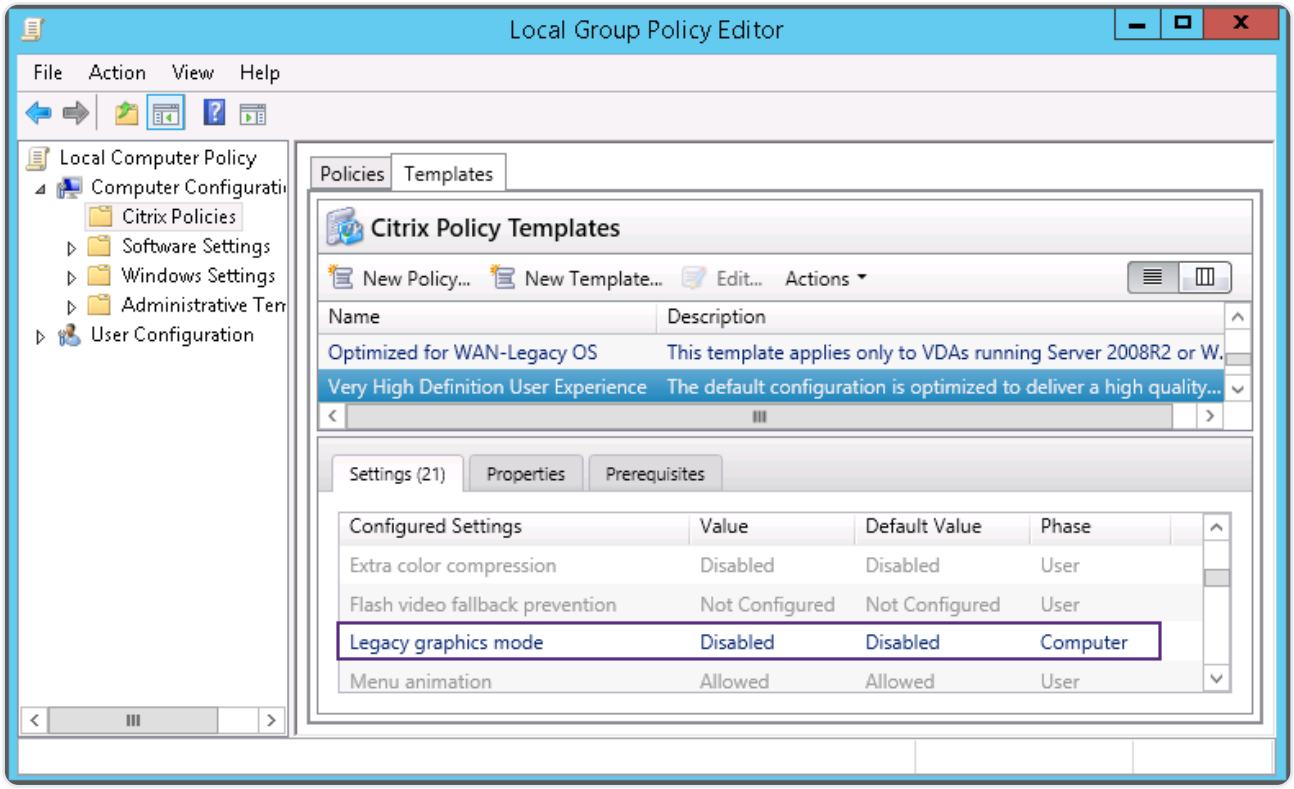
您可以通过选择特定产品版本或选择类别来优化搜索。对于未筛选的搜索，请选择 **所有设置**。

策略一旦创建，便独立于所使用的模板。您可以在新策略上使用 **描述** 字段来跟踪所使用的源模板。

在 Studio 中，策略和模板显示在单个列表中，无论它们包含用户、计算机还是两种类型的设置。此外，策略和模板都可以使用用户和计算机筛选器进行应用。

在组策略编辑器中，计算机和用户设置必须单独应用，即使它们是根据包含这两种类型设置的模板创建的。在此示例中，选择在计算机配置中使用“超高清用户体验”：

- 旧版图形模式是计算机设置，用于从此模板创建的策略中。
- 灰显的“用户设置”不会在此模板创建的策略中使用。




# 策略模板

模板是根据预定义起点创建策略的来源。内置的 Citrix® 模板针对特定环境或网络条件进行了优化，可用作：

- 创建您自己的策略和模板并在站点之间共享的来源。
- 在部署之间更轻松地比较结果的参考，因为您可以引用结果，例如“...使用 Citrix 模板 x 或 y 时...”.
- 通过导入或导出模板与 Citrix 支持或受信任的第三方通信策略的方法。

策略模板可以导入和导出。

有关使用模板创建策略时的注意事项，请参阅知识中心文章 CTX202330。要下载 PDF，请使用您的凭据登录。

# 内置 Citrix 模板

提供以下策略模板：

- **超高清用户体验**。此模板强制实施可最大程度提高用户体验的默认设置。在按优先级顺序处理多个策略的场景中使用此模板。
- **高服务器可扩展性**。应用此模板可节省服务器资源。此模板平衡了用户体验和服务器可扩展性。它在增加单个服务器可承载的用户数量的同时，提供了良好的用户体验。此模板不使用视频编解码器进行图形压缩，并阻止服务器端多媒体渲染。
- **高服务器可扩展性 - 旧版操作系统**。此高服务器可扩展性模板仅适用于运行 Windows Server 2008 R2 或 Windows 7 及更早版本的 VDA。此模板依赖于旧版图形模式，该模式对于这些操作系统更高效。
- **针对 NetScaler SD-WAN 优化**。为使用 NetScaler SD-WAN 优化 Citrix Virtual Desktops 交付的分支机构用户应用此模板。（NetScaler SD-WAN 是 CloudBridge 的新名称）。
- **针对 WAN 优化**。此模板适用于使用共享 WAN 连接的分支机构中的任务工作者，或通过低带宽连接访问图形用户界面简单且多媒体内容较少的应用程序的远程位置。此模板以牺牲视频播放体验和部分服务器可扩展性为代价，以优化带宽效率。
- **针对 WAN 优化 - 旧版操作系统**。此 *针对 WAN 优化* 模板仅适用于运行 Windows Server 2008 R2 或 Windows 7 及更早版本的 VDA。此模板依赖于旧版图形模式，该模式对于这些操作系统更高效。
- **安全和控制**。在风险容忍度低的环境中使用此模板，以最大程度地减少 Citrix Virtual Apps and Desktops 中默认启用的功能。此模板包含禁用用户设备上的打印、剪贴板、外围设备、驱动器映射、端口重定向和 Flash 加速访问的设置。应用此模板可能会占用更多带宽并降低每个服务器的用户密度。

虽然我们建议使用内置 Citrix 模板的默认设置，但有些设置没有特定的推荐值。例如，**会话总带宽限制**，包含在“针对 WAN 优化”模板中。在这种情况下，模板会公开该设置，以便管理员了解此设置可能适用于该场景。

模板默认设置图像(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/template-default-settings.png)

如果您正在使用早于 XenApp 和 XenDesktop 7.6 FP3 的部署（策略管理和 VDA），并且需要“高服务器可伸缩性”和“针对 WAN 优化”模板，请在适用时使用这些模板的旧版操作系统版本。

> **注意：**
>
> Citrix 创建并更新内置模板。您无法修改或删除这些模板。

## 使用 Studio 创建和管理模板

要基于模板创建模板：

1. 在 Studio 导航窗格中选择“**策略**”。
2. 选择“**模板**”选项卡，然后选择要从中创建模板的模板。
3. 在“操作”窗格中选择“**创建模板**”。
4. 选择并配置要包含在模板中的策略设置。删除任何不相关的现有设置。输入模板的名称。

单击“**完成**”后，新模板将显示在“**模板**”选项卡上。

要基于策略创建模板：

1. 在 Studio 导航窗格中选择“**策略**”。
2. 选择“**策略**”选项卡，然后选择要从中创建模板的策略。
3. 在“操作”窗格中选择“**另存为模板**”。
4. 选择并配置要包含在模板中的任何新策略设置。删除任何不相关的现有设置。输入模板的名称和描述，然后单击“**完成**”。

要导入模板：

1. 在 Studio 导航窗格中选择“**策略**”。
2. 选择**模板**选项卡，然后选择**导入模板**。
3. 选择要导入的模板文件，然后单击**打开**。如果导入的模板与现有模板同名，可以选择覆盖现有模板，或以自动生成的不同名称保存模板。

要导出模板：

1. 在 Studio 导航窗格中选择**策略**。
2. 选择**模板**选项卡，然后选择**导出模板**。
3. 选择要保存模板的位置，然后单击**保存**。

在指定位置创建了一个 `.gpt` 文件。

## 使用组策略编辑器创建和管理模板

在组策略编辑器中，展开“计算机配置”或“用户配置”。展开**策略**节点，然后选择**Citrix 策略**。选择相应的操作。

| 任务 | 说明 |
| --- | --- |
| 从现有策略创建模板 | 在**策略**选项卡上，选择策略，然后选择**操作 > 另存为模板**。 |
| 从现有模板创建策略 | 在“**模板**”选项卡上，选择模板，然后单击“**新建策略**”。 |
| 从现有模板创建模板 | 在**模板**选项卡上，选择模板，然后单击**新建模板**。 |
| 导入模板 | 在**模板**选项卡上，选择**操作 > 导入**。 |
| 导出模板 | 在“**模板**”选项卡上，选择“**操作 > 导出**”。 |
| 查看模板设置 | 在“**模板**”选项卡上，选择模板，然后单击“**设置**”选项卡。 |
| 查看模板属性摘要 | 在“**模板**”选项卡上，选择模板，然后单击“**属性**”选项卡。 |
| 查看模板必备条件 | 在“**模板**”选项卡上，选择模板，然后单击“**必备条件**”选项卡。 |

### 模板和委派管理

策略模板存储在安装了策略管理包的计算机上。此计算机可以是 Delivery Controller 计算机或组策略对象管理计算机，而不是 Citrix Virtual Apps and Desktops 站点的数据库。这意味着 Windows 管理权限控制策略模板文件，而不是站点的委派管理角色和范围。

因此，具有站点只读权限的管理员可以创建模板。但是，由于模板是本地文件，因此不会对您的环境进行任何更改。

自定义模板仅对创建它们的用户帐户可见，并存储在用户的 Windows 配置文件中。要进一步公开自定义模板，请从中创建策略或将其导出到共享位置。

## 创建策略

在创建策略之前，请确定它可能影响的用户或设备组。您可能希望创建基于用户工作职能、连接类型、用户设备或地理位置的策略。您还可以使用与 Windows Active Directory 组策略相同的条件。

如果您已创建适用于某个组的策略，请考虑编辑该策略而不是创建另一个策略。编辑策略后，配置相应的设置。避免仅仅为了启用特定设置或将策略排除在某些用户之外而创建策略。

创建策略时，您可以基于策略模板中的设置，并根据需要自定义设置。您也可以不使用模板创建策略，并添加所需的所有设置。

在 Citrix Studio 中，新创建的策略被设置为“禁用”，除非明确选中“**启用策略**”复选框。

## 策略设置

策略设置可以启用、禁用或不配置。默认情况下，策略设置未配置，这意味着它们未添加到策略中。设置仅在添加到策略时才应用。

某些策略设置可以处于以下状态之一：

- “允许”或“禁止”允许或阻止由设置控制的操作。有时，用户被允许或阻止在会话中管理设置的操作。例如，如果菜单动画设置设置为“允许”，则用户可以在其客户端环境中控制菜单动画。
- “启用”或“禁用”可打开或关闭设置。如果禁用某个设置，则在较低级别的策略中不会启用该设置。

此外，某些设置控制依赖设置的有效性。例如，“客户端驱动器重定向”控制用户是否被允许访问其设备上的驱动器。此设置和“**客户端网络驱动器**”设置都必须添加到策略中，才能允许用户访问其网络驱动器。如果“**客户端驱动器重定向**”设置被禁用，即使“**客户端网络驱动器**”设置已启用，用户也无法访问其网络驱动器。

通常，影响计算机的策略设置更改在虚拟桌面重新启动或用户登录时生效。影响用户的策略设置更改在用户下次登录时生效。如果您使用的是 Active Directory，则策略设置会在 Active Directory 每隔 90 分钟重新评估策略时更新。策略设置在虚拟桌面重新启动或用户登录时应用。

对于某些策略设置，在将设置添加到策略时，可以输入或选择一个值。可以通过选择“使用默认值”来限制设置的配置。此选择会禁用设置的配置，并且仅允许在应用策略时使用设置的默认值。此选择与在选择“使用默认值”之前输入的值无关。

最佳实践：

- 将策略分配给组而不是单个用户。如果您将策略分配给组，则在您从组中添加或删除用户时，分配会自动更新。
- 不要在远程桌面会话主机配置中启用冲突或重叠的设置。有时，远程桌面会话主机配置提供的功能与 Citrix 策略设置类似。如果可能，请保持所有设置一致（启用或禁用），以便于故障排除。
- 禁用未使用的策略。未添加任何设置的策略会产生不必要的处理。

## 策略分配

创建策略时，您可以将其分配给特定的用户和计算机对象。该策略根据特定的条件或规则应用于连接。通常，您可以根据条件的组合，向策略添加任意数量的分配。如果未指定任何分配，则该策略将应用于所有连接。

下表列出了可用的分配:

| 分配名称 | 基于以下条件应用策略 |
| --- | --- |
| 访问控制 | 客户端连接所通过的访问控制条件。*连接类型* - 是否将策略应用于通过或不通过 NetScaler® Gateway 建立的连接。*NetScaler Gateway 场名称* - NetScaler Gateway 虚拟服务器的名称。*访问条件* - 要使用的端点分析策略或会话策略的名称。 |
| NetScaler SD-WAN | 用户会话是否通过 NetScaler SD-WAN 启动。**注意：** 您只能向策略添加一个 NetScaler SD-WAN 分配。 |
| 客户端 IP 地址 | 用于连接会话的用户设备的 IP 地址：IPv4 示例：12.0.0.0、12.0.0.*、12.0.0.1-12.0.0.70、12.0.0.1/24；IPv6 示例：2001:0db8:3c4d:0015:0:0:abcd:ef12、2001:0db8:3c4d:0015::/54 |
| 客户端名称 | 用户设备的名称。精确匹配：ClientABCName。使用通配符：Client*Name。 |
| 交付组 | 交付组隶属关系。 |
| 交付组类型 | 桌面或应用程序类型：专用桌面、共享桌面、专用应用程序或共享应用程序。**注意：** 专用桌面和共享桌面筛选选项仅适用于 Citrix Virtual Apps and Desktops 7.x。有关详细信息，请参阅 CTX219153。 |
| 组织单位 (OU) | 组织单位。 |
| 标记 | 标记。**注意：** 将此策略应用于所有带标记的计算机。不包括应用程序标记。 |
| 用户或组 | 用户或组名称。 |

当用户登录时，将识别所有与连接分配匹配的策略。这些策略按优先级顺序排序，并比较任何设置的多个实例。每个设置都根据策略的优先级排名应用。任何已禁用的策略设置都优先于较低级别的已启用设置。未配置的策略设置将被忽略。

> **重要提示：**
>
> 使用组策略管理控制台配置 Active Directory 和 Citrix 策略时，分配和设置可能无法按预期应用。有关详细信息，请参阅 CTX127461
>
> 默认情况下提供名为“未筛选”的策略。

- 如果您使用 Studio 管理 Citrix 策略，您添加到“未筛选”策略的设置将应用于站点中的所有服务器、桌面和连接。
- 如果您使用本地组策略编辑器管理 Citrix 策略，则添加到“未筛选”策略的设置将应用于所有站点和连接。站点和连接必须在包含该策略的组策略对象 (GPO) 的范围内。例如，销售 OU 包含一个名为 Sales-US 的 GPO，其中包含美国销售团队的所有成员。Sales-US GPO 配置了“未筛选”策略，其中包含多个用户策略设置。当美国销售经理登录到站点时，“未筛选”策略中的设置会自动应用于会话。此配置是因为该用户是 Sales-US GPO 的成员。

分配模式决定了策略是否仅应用于与所有分配条件匹配的连接。如果模式设置为“允许”（默认值），则策略仅应用于与分配条件匹配的连接。如果模式设置为“拒绝”，则如果连接不匹配分配条件，则应用策略。以下示例说明了当存在多个分配时，分配模式如何影响 Citrix 策略。

- **示例：具有不同模式的同类型分配** - 在具有两个相同类型分配的策略中，一个设置为“允许”，一个设置为“拒绝”，如果连接满足两个分配，则设置为“拒绝”的分配优先。例如：

  策略 1 包含以下分配：

  - 分配 A 指定销售组。模式设置为“允许”。
  - 分配 B 指定销售经理的帐户。模式设置为“拒绝”。

  由于分配 B 的模式设置为“拒绝”，因此即使销售经理是销售组的成员，当其登录到站点时，也不会应用该策略。

- **示例：具有相同模式的不同类型分配** - 在具有两个或更多不同类型分配（设置为“允许”）的策略中，连接必须满足每种类型至少一个分配，才能应用策略。例如：

  策略 2 包含以下分配：

  - 分配 C 是一个用户分配，指定销售组。模式设置为“允许”。

- 分配 D 是一个客户端 IP 地址分配，指定 10.8.169.*（公司网络）。模式设置为“允许”。

当销售经理从办公室登录到站点时，策略会应用，因为连接满足两个分配。

策略 3 包含以下分配：

- 分配 E 是一个用户分配，指定了销售组。模式设置为“允许”。
- 分配 F 是一个访问控制分配，指定了 NetScaler Gateway 连接条件。模式设置为“允许”。

当销售经理从办公室登录到站点时，策略不会应用，因为连接不满足分配 F。

## 使用 Studio 基于模板创建策略

1. 在 Studio 导航窗格中选择“**策略**”。
2. 选择 **模板** 选项卡并选择一个模板。
3. 在“**操作**”窗格中，从“**模板**”中选择“**创建策略**”。
4. 默认情况下，新策略使用模板中的所有默认设置。在这种情况下，“**使用模板默认设置**”处于选中状态。如果要更改设置，请选择“**修改默认值并添加更多设置**”，然后添加或删除设置。
5. 通过选择以下选项之一来指定如何应用策略：
   - 分配给选定的用户和计算机对象，然后选择必须应用策略的用户和计算机对象。
   - 分配给站点中的所有对象，以将策略应用于站点中的所有用户和计算机对象。
6. 输入策略名称或接受默认名称。考虑根据策略影响的对象（例如“会计部门”或“远程用户”）来命名策略。（可选）添加说明。

   策略默认启用；您可以禁用它。启用策略后，它会立即应用于登录用户。禁用策略会阻止其应用。如果您必须优先处理策略或稍后添加设置，请考虑禁用策略，直到您准备好应用它。

## 使用 Studio 创建策略

1. 在 Studio 导航窗格中选择“**策略**”。
2. 选择**策略**选项卡。
3. 在“**操作**”窗格中选择“**创建策略**”。
4. 添加和配置策略设置。
5. 通过选择以下选项之一来指定如何应用策略：
   - 分配给选定的用户和计算机对象，然后选择必须应用策略的用户和计算机对象。
   - 分配给站点中的所有对象，以将策略应用于站点中的所有用户和计算机对象。

6. 输入策略名称或接受默认名称。请考虑根据策略影响的对象或内容来命名策略，例如“会计部门”或“远程用户”。（可选）添加说明。

   策略默认启用；您可以禁用它。启用策略后，它会立即应用于登录用户。禁用策略会阻止其应用。如果您必须优先处理策略或稍后添加设置，请考虑禁用策略，直到您准备好应用它。

## 使用组策略编辑器创建和管理策略

在组策略编辑器中，展开**计算机配置或用户配置**。展开**策略**节点，然后选择**Citrix 策略**。选择相应的操作：

| 任务 | 说明 |
| --- | --- |
| 创建策略 | 在**策略**选项卡上，单击**新建**。 |
| 编辑现有策略 | 在**策略**选项卡上，选择策略，然后单击**编辑**。 |
| 更改现有策略的优先级 | 在“**策略**”选项卡上，选择策略，然后单击“**提高**”或“**降低**”。 |
| 查看策略的摘要信息 | 在“**策略**”选项卡上，选择策略，然后单击“**摘要**”选项卡。 |
| 查看和修改策略设置 | 在“**策略**”选项卡上，选择策略，然后单击“**设置**”选项卡。 |
| 查看和修改策略筛选器 | 在“**策略**”选项卡上，选择策略，然后单击“**筛选器**”选项卡。当您向策略添加多个筛选器时，必须满足所有筛选器条件才能应用该策略。 |
| 启用或禁用策略 | 在“**策略**”选项卡上，选择策略，然后选择“**操作 > 启用**”或“**操作 > 禁用**”。 |
| 从现有模板创建策略 | 在“**模板**”选项卡上，选择模板，然后单击“**新建策略**”。 |

# 比较、确定优先级、建模和故障排除策略

您可以使用多个策略来自定义环境，以根据用户的职务、地理位置或连接类型满足其需求。例如，为了增强安全性，可以对经常与敏感数据交互的用户组施加限制。

您还可以创建策略，以防止用户将敏感文件保存到其本地客户端驱动器上。但是，如果用户组中的某些用户确实需要访问其本地驱动器，则可以仅为这些用户创建另一个策略。然后，对这两个策略进行排名或确定优先级，以控制哪个策略优先。使用多个策略时，必须确定：

- 如何确定策略的优先级
- 如何创建例外
- 当策略冲突时如何查看有效策略。

通常，策略会覆盖为整个站点、特定交付控制器或用户设备配置的类似设置。此原则的例外是安全性。环境中最高的加密设置始终会覆盖其他设置和策略。最高的加密设置包括操作系统和限制最严格的影子设置。

Citrix® 策略与您在操作系统中设置的策略交互。在 Citrix 环境中，Citrix 设置会覆盖在 Active Directory 策略中或使用远程桌面会话主机配置配置的相同设置。此设置包括与典型远程桌面协议 (RDP) 客户端连接设置相关的设置。典型的 RDP 设置包括桌面墙纸、菜单动画和拖动时查看窗口内容等设置。

某些策略设置（例如 Secure ICA®）必须与操作系统中的设置匹配。如果在其他位置设置了更高优先级的加密级别，则您在策略中或交付应用程序和桌面时指定的 **Secure ICA 策略**设置可能会被覆盖。

例如，您在创建交付组时指定的加密设置必须与您在整个环境中指定的加密设置处于同一级别。

> **注意：**
>
> 在双跳场景的第二跳中，请考虑单会话操作系统 VDA 连接到多会话操作系统 VDA。在这种情况下，Citrix 策略作用于单会话操作系统 VDA，就好像它是用户设备一样。例如，假设策略设置为在用户设备上缓存图像。在此示例中，双跳场景中为第二跳缓存的图像将缓存在单会话操作系统 VDA 计算机上。

## 比较策略和模板

您可以将策略或模板中的设置与其他策略或模板的设置进行比较。例如，您可能需要验证设置值以保持符合最佳实践。您可能还希望将策略或模板中的设置与 Citrix 提供的默认设置进行比较。

1. 在 Studio 导航窗格中选择“策略”。
2. 单击“比较”选项卡，然后单击“选择”。
3. 选择要比较的策略或模板。要在比较中包含默认值，请选中“与默认设置比较”复选框。

4. 点击比较后，配置的设置将以列的形式显示。
5. 要查看所有设置，请选择“显示所有设置”。要返回默认视图，请选择“显示常用设置”。

## 优先处理策略

对策略进行优先级排序，可让您在策略包含冲突设置时定义策略的优先顺序。当用户登录时，将识别所有与连接分配匹配的策略。这些策略将按优先级顺序排序，并比较任何设置的多个实例。每个设置都将根据策略的优先级排名应用。

您可以通过在 Studio 中为策略指定不同的优先级编号来确定其优先级。默认情况下，新策略的优先级最低。如果策略设置冲突，则优先级较高的策略（优先级编号为 1 的策略最高）将覆盖优先级较低的策略。设置将根据优先级和设置的条件进行合并。例如，设置是禁用还是启用。任何禁用的设置都将覆盖已启用的较低优先级设置。未配置的策略设置将被忽略，并且不会覆盖较低优先级设置的设置。

1. 在 Studio 导航窗格中选择“**策略**”。确保已选择“**策略**”选项卡。
2. 选择一个策略。
3. 在“**操作**”窗格中选择“**降低优先级**”或“**提高优先级**”。

## 例外情况

当您为用户组、用户设备或计算机创建策略时，可能会发现组中的某些成员需要对某些策略设置进行例外处理。您可以通过以下方式创建例外：

- 仅为需要例外的组员创建策略，然后将该策略的优先级排在整个组的策略之上
- 对添加到策略的分配使用“拒绝”模式

将模式设置为“拒绝”的分配仅将策略应用于不符合分配条件的连接。例如，一个策略包含以下分配：

- 分配 A 是一个客户端 IP 地址分配，指定范围为 208.77.88.*。模式设置为“允许”
- 分配 B 是一个用户分配，指定一个特定的用户帐户。模式设置为“拒绝”。

该策略应用于所有使用分配 A 中指定的 IP 地址范围登录到站点的用户。但是，该策略不应用于使用分配 B 中指定的用户帐户登录到站点的用户。

## 确定哪些策略适用于连接

有时，由于应用了多个策略，连接未按预期响应。如果优先级更高的策略应用于连接，它可能会覆盖您在原始策略中配置的设置。您可以计算策略的结果集，并确定最终策略设置如何为连接合并。

您可以通过以下方式计算策略的结果集：

- 使用 Citrix 组策略建模向导模拟连接场景，并识别 Citrix 策略可能如何应用。您可以为连接场景指定条件，例如：
  - 域控制器
  - 用户
  - Citrix 策略分配证据值
  - 模拟环境设置，例如网络连接缓慢 向导生成的报告列出了在该场景中可能生效的 Citrix 策略。假设您以域用户身份登录到控制器。在这种情况下，向导会使用站点策略设置和 Active Directory 组策略对象 (GPO) 来计算策略的结果集。
- 使用组策略结果生成报告，描述对给定用户和控制器生效的 Citrix 策略。组策略结果工具可帮助您评估环境中 GPO 的当前状态并生成报告。生成的报告描述了这些对象（包括 Citrix 策略）当前如何应用于特定用户和控制器。

您可以从 **Citrix Studio** 的**操作**窗格启动 Citrix 组策略建模向导。您可以在 Windows 的组策略管理控制台中启动任一工具。

在以下情况下，使用 Studio 创建的站点策略设置不包含在策略的结果集中：

- 如果您从组策略管理控制台运行 Citrix 组策略建模向导 或者，
- 如果您从组策略管理控制台运行组策略结果工具

为确保获得最全面的策略结果集，Citrix 建议从 Studio 启动 Citrix 组策略建模向导，除非您仅使用组策略管理控制台创建策略。

## 使用 Citrix 组策略建模向导

使用以下方法之一打开 Citrix 组策略建模向导：

- 在 Studio 导航窗格中选择“策略”，选择“建模”选项卡，然后在“操作”窗格中选择“启动建模向导”。
- 启动组策略管理控制台 (gpmc.msc)，在树窗格中右键单击 Citrix 组策略建模，然后选择 Citrix 组策略建模向导。

按照向导说明选择以下各项：

- 域控制器
- 用户
- 计算机
- 环境设置
- 在模拟中使用的 Citrix 分配条件。

单击“**完成**”后，向导会生成建模结果报告。在 Studio 中，该报告显示在中间窗格的“**建模**”选项卡下。

要查看报告，请选择“**查看建模报告**”。

> **注意：**
>
> 在 Citrix Cloud 中托管的 Studio 中，“**建模**”选项卡不可用。

### 策略故障排除

用户、IP 地址和其他分配的对象可以同时应用多个策略。这种情况可能导致冲突，从而使策略无法按预期运行。当您运行 Citrix 组策略建模向导或组策略结果工具时，可能会发现没有策略应用于用户连接。在这种情况下，策略设置不会应用于在符合策略评估条件的条件下连接到其应用程序和桌面的用户。出现这种情况的原因是：

- 没有策略具有与策略评估条件匹配的分配。
- 与分配匹配的策略未配置任何设置。
- 与分配匹配的策略已禁用。

如果要将策略设置应用于符合指定条件的连接，请确保：

- 要应用于这些连接的策略已启用。
- 要应用的策略已配置适当的设置。

## 默认策略设置

下表列出了策略设置、其默认值以及适用的 Virtual Delivery Agent (VDA) 版本。

### ICA®

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 自适应传输 | 关闭；在首选时使用 | VDA 7.13–7.15；VDA 7.16 到当前版本 |
| 客户端剪贴板重定向 | 允许 | 所有 VDA 版本 |
| 客户端剪贴板写入允许的格式 | 未指定任何格式 | VDA 7.6 到当前版本 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 桌面启动 | 禁止 | 适用于多会话操作系统 VDA 7 到当前版本 |
| ICA 侦听器端口号 | 1494 | 所有 VDA 版本 |
| 客户端连接期间启动未发布的程序 | 禁止 | 适用于多会话操作系统 VDA 7 到当前版本 |
| 限制剪贴板客户端到会话的传输大小 | 已禁用 | VDA 2009 |
| 限制剪贴板会话到客户端的传输大小 | 已禁用 | VDA 2009 |
| 容忍丢包模式 | 允许 | VDA 2003。注意：容错模式尚不可用。此版本的 VDA 在其可用时将支持此模式。 |
| 容忍丢包阈值 | 当容错模式可用时：数据包丢失：5%，延迟：300 毫秒 (RTT) | VDA 2003 到当前版本 |
| Rendezvous 协议 | 已禁用 | 仅适用于通过 Citrix Cloud 建立的 HDX 会话。 |
| 限制客户端剪贴板写入 | 禁止 | VDA 7.6 到当前版本 |
| 限制会话剪贴板写入 | 禁止 | VDA 7.6 到当前版本 |
| 允许会话剪贴板写入的格式 | 未指定任何格式 | VDA 7.6 到当前版本 |
| 平板电脑模式切换 | 启用 | VDA 7.16 到当前版本；对于 VDA 7.14 和 7.15 LTSR，请使用注册表配置此设置。 |
| 虚拟通道允许列表 | 启用 | VDA 2109 |

## ICA/Adobe Flash 交付/Flash 重定向

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| Flash 视频回退预防 | 未配置 | VDA 7.6 FP3 到当前版本 |
| Flash 视频回退预防错误 *.swf | VDA 7.6 FP3 到当前版本 | |

## ICA/音频

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 自适应音频 | 启用 | 适用于使用 Citrix Virtual Apps and Desktops™ 2109 或更高版本的 VDA 的单会话操作系统和多会话操作系统会话。 |
| 通过 UDP 实时传输的音频 | 允许 | 所有 VDA 版本 |
| 音频即插即用 | 允许 | 适用于多会话操作系统 7 到当前版本的 VDA |
| 音频质量 | 高 - 高清音频 | 所有 VDA 版本 |
| 客户端音频重定向 | 允许 | 所有 VDA 版本 |
| 客户端麦克风重定向 | 允许 | 所有 VDA 版本 |

## ICA/客户端自动重新连接

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 客户端自动重新连接 | 允许 | 所有 VDA 版本 |
| 自动客户端重新连接身份验证 | 不要求身份验证 | 所有 VDA 版本 |
| 自动客户端重新连接日志记录 | 不记录自动重新连接事件 | 所有 VDA 版本 |
| 自动客户端重新连接超时 | 120 秒 | VDA 7.13 到当前版本 |
| 重新连接 UI 透明度级别 | 80% | VDA 7.13 到当前版本 |

# ICA/带宽

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 音频重定向带宽限制 | 0 千比特/秒 | 所有 VDA 版本 |
| 音频重定向带宽限制百分比 | 0 | 所有 VDA 版本 |
| 客户端 USB 设备重定向带宽限制 | 0 千比特/秒 | VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 到当前版本、适用于单会话操作系统的 VDA 7 到当前版本 |
| 客户端 USB 设备重定向带宽限制百分比 | 0 | VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 到当前版本、适用于单会话操作系统的 VDA 7 到当前版本 |
| 剪贴板重定向带宽限制 | 0 千比特/秒 | 所有 VDA 版本 |
| 剪贴板重定向带宽限制百分比 | 0 | 所有 VDA 版本 |
| COM 端口重定向带宽限制 | 0 千比特/秒 | 所有 VDA 版本；对于 VDA 7.0 到 7.8，请使用注册表配置此设置 |
| COM 端口重定向带宽限制百分比 | 0 | 所有 VDA 版本；对于 VDA 7.0 到 7.8，请使用注册表配置此设置 |
| 文件重定向带宽限制 | 0 千比特/秒 | 所有 VDA 版本 |
| 文件重定向带宽限制百分比 | 0 | 所有 VDA 版本 |
| HDX MediaStream 多媒体加速带宽限制 | 0 千比特/秒 | VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 和适用于单会话操作系统的 VDA 7 到当前适用于多会话操作系统的 VDA 和适用于单会话操作系统的 VDA |
| HDX MediaStream 多媒体加速带宽限制百分比 | 0 | VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 到当 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| | | 前版本、适用于单会话操作系统的 VDA 7 到当前版本 |
| LPT 端口重定向带宽限制 | 0 千比特/秒 | 所有 VDA 版本；对于 VDA 7.0 到 7.8，请使用注册表配置此设置 |
| LPT 端口重定向带宽限制百分比 | 0 | 所有 VDA 版本；对于 VDA 7.0 到 7.8，请使用注册表配置此设置 |
| 总体会话带宽限制 | 0 千比特/秒 | 所有 VDA 版本 |
| 打印机重定向带宽限制 | 0 千比特/秒 | 所有 VDA 版本 |
| 打印机重定向带宽限制百分比 | 0 | 所有 VDA 版本 |
| TWAIN 设备重定向带宽限制 | 0 千比特/秒 | VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 到当前版本、适用于单会话操作系统的 VDA 7 到当前版本 |
| TWAIN 设备重定向带宽限制百分比 | 0 | VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 到当前版本、适用于单会话操作系统的 VDA 7 到当前版本 |

## ICA/双向内容重定向

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 允许双向内容重定向 | 禁止 | VDA 7.13 到当前版本 |
| 允许重定向到客户端的 URL | 空 | VDA 7.13 到当前版本 |
| 允许重定向到 VDA 的 URL | 空 | VDA 7.13 到当前版本 |
| 客户端到主机 (VDA) 和客户端到客户端双向内容重定向 | 使用 Citrix Workspace™ 应用程序组策略对象管理模板 | |

## ICA/浏览器内容重定向

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 浏览器内容重定向 | 允许 | VDA 7.16 到当前版本 |
| 浏览器内容重定向 ACL 配置 | `https://www.youtube.com/*` | VDA 7.16 到当前版本 |
| 浏览器内容重定向集成 Windows 身份验证支持 | 禁止 | VDA 2106 到当前版本 |
| 浏览器内容重定向代理配置 | 空 | VDA 7.16 到当前版本 |
| 浏览器内容重定向服务器获取 Web 代理身份验证 | 禁止 | VDA 2012 到当前版本 |

## ICA/客户端传感器

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 允许应用程序使用客户端设备的物理位置 | 禁止 | VDA 5.6 FP1，适用于多会话操作系统的 VDA 7 到当前版本，适用于单会话操作系统的 VDA 7 到当前版本 |

## ICA/桌面 UI

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 桌面组合重定向 | 已禁用（7.6 FP3 到当前版本）；已启用（5.6 到 7.6 FP2） | VDA 5.6，适用于单会话操作系统的 VDA 7 到 7.15 |
| 桌面组合重定向图形质量 | 中等 | VDA 5.6，适用于单会话操作系统的 VDA 7 到 7.15 |
| 桌面壁纸 | 允许 | 所有 VDA 版本 |
| 菜单动画 | 允许 | 所有 VDA 版本 |
| 拖动时查看窗口内容 | 允许 | 所有 VDA 版本 |

## ICA/最终用户监控

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| ICA 往返计算 | 启用 | 所有 VDA 版本 |
| ICA 往返计算间隔 | 15 秒 | 所有 VDA 版本 |
| 空闲连接的 ICA 往返计算 | 已禁用 | 所有 VDA 版本 |

## ICA/增强桌面体验

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 增强桌面体验 | 允许 | 适用于多会话操作系统 7 及更高版本的 VDA |

## ICA/文件重定向

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 自动连接客户端驱动器 | 允许 | 所有 VDA 版本 |
| 客户端驱动器重定向 | 允许 | 所有 VDA 版本 |
| 客户端固定驱动器 | 允许 | 所有 VDA 版本 |
| 客户端软盘驱动器 | 允许 | 所有 VDA 版本 |
| 客户端网络驱动器 | 允许 | 所有 VDA 版本 |
| 客户端光驱 | 允许 | 所有 VDA 版本 |
| 客户端可移动驱动器 | 允许 | 所有 VDA 版本 |
| 主机到客户端重定向 | 已禁用 | 适用于多会话操作系统的 VDA 7 到当前版本 |
| 保留客户端驱动器盘符 | 已禁用 | VDA 5、5.5、5.6 FP1，适用于单会话操作系统的 VDA 7 到当前版本 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 只读客户端驱动器访问 | 已禁用 | VDA 5.5、5.6 FP1，适用于多会话操作系统的 VDA 7 到当前版本，适用于单会话操作系统的 VDA 7 到当前版本 |
| 特殊文件夹重定向 | 允许 | 仅限 Web Interface 部署；适用于多会话操作系统的 VDA 7 到当前版本 |
| 使用异步写入 | 已禁用 | 所有 VDA 版本 |

## ICA/图形

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 允许视觉无损压缩 | 已禁用 | VDA 7.6 到当前版本 |
| 显示内存限制 | 65,536 Kb | VDA 5、5.5、5.6 FP1、适用于单会话操作系统的 VDA 7 到当前版本 |
| 显示模式降级首选项 | 优先降低颜色深度 | 所有 VDA 版本 |
| 动态窗口预览 | 启用 | VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 到当前版本、适用于单会话操作系统的 VDA 7 到当前版本 |
| 图形状态指示器 | 已禁用 | VDA 7.16 到当前版本 |
| 图像缓存 | 启用 | VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 到当前版本、适用于单会话操作系统的 VDA 7 到当前版本 |
| 旧版图形模式 | 已禁用 | 适用于多会话操作系统的 VDA 7 到当前版本、适用于单会话操作系统的 VDA 7 到当前版本 |
| 最大允许颜色深度 | 每像素 32 位 | 所有 VDA 版本 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 显示模式降级时通知用户 | 已禁用 | 适用于多会话操作系统 7 及更高版本的 VDA |
| 优化 3D 图形工作负载 | 已禁用 | VDA 7.17 及更高版本 |
| 排队和丢弃 | 启用 | 所有 VDA 版本 |
| 屏幕共享 | 已禁用 | VDA 2112 |
| 使用视频编解码器进行压缩 | 首选时使用视频编解码器 | VDA 7.6 FP3 及更高版本 |
| 对视频编解码器使用硬件编码 | 启用 | VDA 7.11 及更高版本 |

## ICA/图形/缓存

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 持久缓存阈值 | 3,000,000 比特/秒 | 适用于多会话操作系统 7 及更高版本的 VDA |

## ICA/图形/Framehawk

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| Framehawk 显示通道 | 已禁用 | VDA 7.6 FP2 至当前版本 |
| Framehawk 显示通道端口范围 | 3224,3324 | VDA 7.6 FP2 至当前版本 |

## ICA/保持活动

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| ICA 保持活动超时 | 60 秒 | 所有 VDA 版本 |
| ICA 保持活动 | 不发送 ICA 保持活动消息 | 所有 VDA 版本 |

## ICA/本地应用访问

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 允许本地应用访问 | 禁止 | 多会话操作系统 VDA 7 到当前版本，单会话操作系统 VDA 7 到当前版本 |
| URL 重定向阻止列表 | 未指定任何站点 | 多会话操作系统 VDA 7 到当前版本，单会话操作系统 VDA 7 到当前版本 |
| URL 重定向允许列表 | 未指定任何站点 | 多会话操作系统 VDA 7 到当前版本，单会话操作系统 VDA 7 到当前版本 |

## ICA/移动体验

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 自动键盘显示 | 禁止 | VDA 5.6 FP1，多会话操作系统 VDA 7 到当前版本，单会话操作系统 VDA 7 到当前版本 |
| 启动触摸优化桌面 | 允许 | VDA 5.6 FP1，多会话操作系统 VDA 7 到当前版本，单会话操作系统 VDA 7 到当前版本。此设置已禁用，不适用于 Windows 10 和 Windows Server 2016 计算机。 |
| 远程组合框 | 禁止 | VDA 5.6 FP1，多会话操作系统 VDA 7 到当前版本，单会话操作系统 VDA 7 到当前版本 |

## ICA/多媒体

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| HTML5 视频重定向 | 禁止 | VDA 7.12 到当前版本 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 限制视频质量 | 未配置 | 适用于多会话操作系统 7 到当前版本的 VDA，适用于单会话操作系统 7 到当前版本的 VDA |
| Microsoft Teams 重定向 | 允许 | 适用于多会话操作系统 VDA 1906 到当前版本，适用于单会话操作系统 VDA 1906 到当前版本。 |
| 多媒体会议 | 允许 | 所有 VDA 版本 |
| 通过 WAN 优化 Windows Media 多媒体重定向 | 允许 | 适用于多会话操作系统 7 到当前版本的 VDA，适用于单会话操作系统 7 到当前版本的 VDA |
| 使用 GPU 优化通过 WAN 的 Windows Media 多媒体重定向 | 禁止 | 适用于多会话操作系统 7 到当前版本的 VDA，适用于单会话操作系统 7 到当前版本的 VDA |
| Windows Media 回退阻止 | 未配置 | VDA 7.6 FP3 到当前版本 |
| Windows Media 客户端内容获取 | 允许 | 适用于多会话操作系统 7 到当前版本的 VDA，适用于单会话操作系统 7 到当前版本的 VDA |
| Windows Media 重定向 | 允许 | 所有 VDA 版本 |
| Windows Media 重定向缓冲区大小 | 5 秒 | VDA 5、5.5、5.6 FP1 到当前版本 |
| Windows Media 重定向缓冲区大小使用 | 已禁用 | VDA 5、5.5、5.6 FP1 到当前版本 |

## ICA/多流连接

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 通过 UDP 传输音频 | 允许 | 适用于多会话操作系统 7 到当前版本的 VDA |
| 音频 UDP 端口范围 | 16500、16509 | VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 到当前版本、适用于单会话操作系统的 VDA 7 到当前版本 |
| 多端口策略 | 主端口 (2598) 具有高优先级 | VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 到当前版本、适用于单会话操作系统的 VDA 7 到当前版本 |
| 多流计算机设置 | 已禁用 | VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 到当前版本、适用于单会话操作系统的 VDA 7 到当前版本 |
| 多流用户设置 | 已禁用 | VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 到当前版本、适用于单会话操作系统的 VDA 7 到当前版本 |
| Multi-Stream 虚拟通道流分配设置 | 有关默认流分配，请参阅 Multi-Stream 虚拟通道分配设置 | VDA 2003 |

## ICA/端口重定向

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 自动连接客户端 COM 端口 | 已禁用 | 所有 VDA 版本；对于 VDA 7.0 到 7.8，请使用注册表配置此设置 |
| 自动连接客户端 LPT 端口 | 已禁用 | 所有 VDA 版本；对于 VDA 7.0 到 7.8，请使用注册表配置此设置 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 客户端 COM 端口重定向 | 禁止 | 所有 VDA 版本；对于 VDA 7.0 到 7.8，请使用注册表配置此设置 |
| 客户端 LPT 端口重定向 | 禁止 | 所有 VDA 版本；对于 VDA 7.0 到 7.8，请使用注册表配置此设置 |

## ICA/打印

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 客户端打印机重定向 | 允许 | 所有 VDA 版本 |
| 默认打印机 | 将默认打印机设置为客户端的主打印机 | 所有 VDA 版本 |
| 打印机分配 | 用户的当前打印机用作会话的默认打印机 | 所有 VDA 版本 |
| 打印机自动创建事件日志首选项 | 记录错误和警告 | 所有 VDA 版本 |
| 会话打印机 | 未指定打印机 | 所有 VDA 版本 |
| 等待创建打印机（桌面） | 已禁用 | 所有 VDA 版本 |

## ICA/打印/客户端打印机

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 自动创建客户端打印机 | 自动创建所有客户端打印机 | 所有 VDA 版本 |
| 自动创建通用通用打印机 | 已禁用 | 所有 VDA 版本 |
| 客户端打印机名称 | 标准打印机名称 | VDA 5.6 |
| 直接连接到打印服务器 | 启用 | 所有 VDA 版本 |
| 打印机驱动程序映射和兼容性 | 未指定任何规则 | 所有 VDA 版本 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 打印机属性保留 | 仅当未保存在客户端时才保留在配置文件中 | 所有 VDA 版本 |
| 保留并还原客户端打印机 | 允许 | VDA 5、5.5、5.6 FP1 |

## ICA/打印/驱动程序

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 自动安装内置打印机驱动程序 | 启用 | 所有 VDA 版本 |
| 通用驱动程序首选项 | EMF; XPS; PCL5c; PCL4; PS | 所有 VDA 版本 |
| 通用打印驱动程序使用情况 | 仅当请求的驱动程序不可用时才使用通用打印 | 所有 VDA 版本 |

## ICA/打印/通用打印服务器

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 启用通用打印服务器 | 已禁用 | 所有 VDA 版本 |
| 通用打印服务器打印数据流 (CGP) 端口 | 7229 | 所有 VDA 版本 |
| 通用打印服务器打印流输入带宽限制 (kbps) | 0 | 所有 VDA 版本 |
| 通用打印服务器 Web 服务 (HTTP/SOAP) 端口 | 8080 | 所有 VDA 版本 |
| 用于负载平衡的通用打印服务器 | VDA 版本 7.9 到当前版本 | |
| 通用打印服务器停止服务阈值 | 180（秒） | VDA 版本 7.9 到当前版本 |

## ICA/打印/通用打印

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 通用打印 EMF 处理模式 | 直接后台处理到打印机 | 所有 VDA 版本 |
| 通用打印图像压缩限制 | 最佳质量（无损压缩） | 所有 VDA 版本 |
| 通用打印优化默认值 | 图像压缩: 期望图像质量 = 标准质量, 启用重量级压缩 = 否; 图像和字体缓存: 允许缓存嵌入图像 = 是; 允许非管理员修改这些设置 = 否; | 所有 VDA 版本 |
| 通用打印预览首选项 | 不要对自动创建或通用打印机使用打印预览 | 所有 VDA 版本 |
| 通用打印质量限制 | 无限制 | 所有 VDA 版本 |

## ICA/安全

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| SecureICA 最低加密级别 | 基本 | 适用于多会话操作系统 7 到当前版本的 VDA |

## ICA/服务器限制

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 服务器空闲计时器间隔 | 0 毫秒 | 适用于多会话操作系统 7 到当前版本的 VDA |

## ICA/会话限制

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 断开连接的会话计时器 | 已禁用 | VDA 5、5.5、5.6 FP1、适用于单会话操作系统 7 到当前版本的 VDA |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 远程电脑访问断开连接会话计时器 | 已禁用 | 适用于单会话操作系统 7 到当前版本的 VDA |
| 断开连接的会话计时器间隔 | 1,440 分钟 | VDA 5、5.5、5.6 FP1、适用于单会话操作系统 7 到当前版本的 VDA |
| 会话连接计时器 | 已禁用 | VDA 5、5.5、5.6 FP1、适用于单会话操作系统 7 到当前版本的 VDA |
| 会话连接计时器间隔 | 1,440 分钟 | VDA 5、5.5、5.6 FP1、适用于单会话操作系统 7 到当前版本的 VDA |
| 会话空闲计时器 | 启用 | VDA 5、5.5、5.6 FP1、适用于单会话操作系统 7 到当前版本的 VDA |
| 会话空闲计时器间隔 | 1,440 分钟 | VDA 5、5.5、5.6 FP1、适用于单会话操作系统 7 到当前版本的 VDA |

## ICA/会话可靠性

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 会话可靠性连接 | 允许 | 所有 VDA 版本 |
| 会话可靠性端口号 | 2598 | 所有 VDA 版本 |
| 会话可靠性超时 | 180 秒 | 所有 VDA 版本 |

## ICA/时区控制

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 为旧版客户端估算本地时间 | 启用 | 适用于多会话操作系统 7 及更高版本的 VDA |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 在会话断开连接或注销时恢复单会话操作系统时区 | 启用 | 当前 VDA 版本 |
| 使用客户端本地时间 | 使用服务器时区 | 所有 VDA 版本 |

## ICA/TWAIN 设备

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 客户端 TWAIN 设备重定向 | 允许 | VDA 5.5、5.6 FP1、适用于多会话操作系统 7 及更高版本的 VDA、适用于单会话操作系统 7 及更高版本的 VDA |
| TWAIN 压缩级别 | 中等 | VDA 5.5、5.6 FP1、适用于多会话操作系统 7 及更高版本的 VDA、适用于单会话操作系统 7 及更高版本的 VDA |

## ICA/USB 设备

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 客户端 USB 设备优化规则 | 已启用 (VDA 7.6 FP3 到当前版本)；已禁用 (VDA 7.11 到当前版本)；默认情况下，未指定任何规则 | VDA 7.6 FP3 到当前版本 |
| 客户端 USB 设备重定向 | 禁止 | 所有 VDA 版本 |
| 客户端 USB 设备重定向规则 | 未指定任何规则 | 所有 VDA 版本 |
| 客户端 USB 即插即用设备重定向 | 允许 | 适用于多会话 OS 的 VDA 7 到当前版本，适用于单会话 OS 的 VDA 7 到当前版本 |

## ICA/视觉显示

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 简单图形的首选颜色深度 | 每像素 24 位 | VDA 7.6 FP3 到当前版本 |
| 目标帧率 | 30 帧/秒 | 所有 VDA 版本 |
| 视觉质量 | 中等 | 适用于多会话 OS 的 VDA 7 到当前版本，适用于单会话 OS 的 VDA 7 到当前版本 |

## ICA/视觉显示/移动图像

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 最低图像质量 | 正常 | VDA 5.5、5.6 FP1、多会话操作系统 VDA 7 到当前版本、单会话操作系统 VDA 7 到当前版本 |
| 动态图像压缩 | 启用 | VDA 5.5、5.6 FP1、多会话操作系统 VDA 7 到当前版本、单会话操作系统 VDA 7 到当前版本 |
| 渐进式压缩级别 | 无 | VDA 5.5、5.6 FP1、多会话操作系统 VDA 7 到当前版本、单会话操作系统 VDA 7 到当前版本 |
| 渐进式压缩阈值 | 2,147,483,647 千比特/秒 | VDA 5.5、5.6 FP1、多会话操作系统 VDA 7 到当前版本、单会话操作系统 VDA 7 到当前版本 |
| 目标最小帧率 | 10 帧每秒 | VDA 5.5、5.6 FP1、多会话操作系统 VDA 7 到当前版本、单会话操作系统 VDA 7 到当前版本 |

## ICA/视觉显示/静态图像

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 额外颜色压缩 | 已禁用 | 所有 VDA 版本 |
| 额外颜色压缩阈值 | 8,192 千比特每秒 | 所有 VDA 版本 |
| 重量级压缩 | 已禁用 | 所有 VDA 版本 |
| 有损压缩级别 | 中等 | 所有 VDA 版本 |
| 有损压缩阈值 | 2,147,483,647 千比特每秒 | 所有 VDA 版本 |

## ICA/WebSockets

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| WebSockets 连接 | 禁止 | 适用于多会话操作系统 7 到当前版本的 VDA，适用于单会话操作系统 7 到当前版本的 VDA |
| WebSockets 端口号 | 8008 | 适用于多会话操作系统 7 到当前版本的 VDA，适用于单会话操作系统 7 到当前版本的 VDA |
| WebSockets 受信任的源服务器列表 | 通配符 * 用于信任所有 Receiver for Web URL | 适用于多会话操作系统 7 到当前版本的 VDA，适用于单会话操作系统 7 到当前版本的 VDA |

## 负载管理

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 并发登录容忍度 | 2 | 适用于多会话操作系统 7 到当前版本的 VDA |
| CPU 使用率 | 已禁用 | 适用于多会话操作系统 7 到当前版本的 VDA |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| CPU 使用率排除进程优先级 | 低于正常或低 | 适用于多会话操作系统 7 到当前版本的 VDA |
| 磁盘使用情况 | 已禁用 | 适用于多会话操作系统 7 到当前版本的 VDA |
| 最大会话数 | 250 | 适用于多会话操作系统 7 到当前版本的 VDA |
| 内存使用情况 | 已禁用 | 适用于多会话操作系统 7 到当前版本的 VDA |
| 内存使用量基本负载 | 零负载：768 MB | 适用于多会话操作系统 7 到当前版本的 VDA |

## 配置文件管理/高级设置

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 禁用自动配置 | 已禁用 | 所有 VDA 版本 |
| 如果遇到问题，注销用户 | 已禁用 | 所有 VDA 版本 |
| 访问锁定文件时的重试次数 | 5 | 所有 VDA 版本 |
| 注销时处理 Internet Cookie 文件 | 已禁用 | 所有 VDA 版本 |

## 配置文件管理/基本设置

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 活动回写 | 已禁用 | 所有 VDA 版本 |
| 启用配置文件管理 | 已禁用 | 所有 VDA 版本 |
| 排除的组 | 已禁用。处理所有用户组的成员。 | 所有 VDA 版本 |
| 脱机配置文件支持 | 已禁用 | 所有 VDA 版本 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 用户存储路径 | 视窗 | 所有 VDA 版本 |
| 处理本地管理员的登录 | 已禁用 | 所有 VDA 版本 |
| 已处理的组 | 已禁用。处理所有用户组的成员。 | 所有 VDA 版本 |

## 配置文件管理/跨平台设置

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 跨平台设置用户组 | 已禁用。处理“已处理组”中指定的所有用户组 | 所有 VDA 版本 |
| 启用跨平台设置 | 已禁用 | 所有 VDA 版本 |
| 跨平台定义路径 | 已禁用。未指定路径。 | 所有 VDA 版本 |
| 跨平台设置存储路径 | 已禁用。使用 Windows\PM_CM。 | 所有 VDA 版本 |
| 创建跨平台设置的源 | 已禁用 | 所有 VDA 版本 |

## 配置文件管理/文件系统/排除项

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 排除列表 - 目录 | 已禁用。用户配置文件中的所有文件夹都已同步。 | 所有 VDA 版本 |
| 排除列表 - 文件 | 已禁用。用户配置文件中的所有文件都已同步。 | 所有 VDA 版本 |

## 配置文件管理/文件系统/同步

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 要同步的目录 | 已禁用。仅同步未排除的文件夹。 | 所有 VDA 版本 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 要同步的文件 | 已禁用。仅同步未排除的文件。 | 所有 VDA 版本 |
| 要镜像的文件夹 | 已禁用。未镜像任何文件夹。 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 授予管理员访问权限 | 已禁用 | 所有 VDA 版本 |
| 包含域名 | 已禁用 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/AppData(漫游)

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| AppData(漫游) 路径 | 已禁用。未指定任何位置。 | 所有 VDA 版本 |
| AppData(漫游) 的重定向设置 | 内容将重定向到 AppData(漫游) 路径策略设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/联系人

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 联系人路径 | 已禁用。未指定位置。 | 所有 VDA 版本 |
| 联系人的重定向设置 | 内容将重定向到**联系人路径策略**设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/桌面

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 桌面路径 | 已禁用。未指定位置。 | 所有 VDA 版本 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 桌面重定向设置 | 内容将重定向到**桌面路径策略**设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/文档

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 文档路径 | 已禁用。未指定位置。 | 所有 VDA 版本 |
| 文档重定向设置 | 内容将重定向到**文档路径策略**设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/下载

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 下载路径 | 已禁用。未指定位置。 | 所有 VDA 版本 |
| 下载重定向设置 | 内容被重定向到**下载路径策略**设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/收藏夹

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 收藏夹路径 | 已禁用。未指定位置。 | 所有 VDA 版本 |
| 收藏夹的重定向设置 | 内容被重定向到**收藏夹路径策略**设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/链接

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 链接路径 | 已禁用。未指定位置。 | 所有 VDA 版本 |
| 链接的重定向设置 | 内容被重定向到**链接路径策略**设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/音乐

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 音乐路径 | 已禁用。未指定位置。 | 所有 VDA 版本 |
| 音乐的重定向设置 | 内容将重定向到 **音乐路径策略** 设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/图片

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 图片路径 | 已禁用。未指定位置。 | 所有 VDA 版本 |
| 图片的重定向设置 | 内容将重定向到 **图片路径策略** 设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/保存的游戏

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 保存的游戏路径 | 已禁用。未指定位置。 | 所有 VDA 版本 |
| 保存的游戏的重定向设置 | 内容将重定向到**保存的游戏路径策略**设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/搜索

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 搜索路径 | 已禁用。未指定位置。 | 所有 VDA 版本 |
| 搜索的重定向设置 | 内容将重定向到**搜索路径策略**设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/开始菜单

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 开始菜单路径 | 已禁用。未指定位置。 | 所有 VDA 版本 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 开始菜单的重定向设置 | 内容重定向到在“开始菜单路径”策略设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/文件夹重定向/视频

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 视频路径 | 已禁用。未指定位置。 | 所有 VDA 版本 |
| 视频的重定向设置 | 内容重定向到在**视频路径策略**设置中指定的 UNC 路径 | 所有 VDA 版本 |

## 配置文件管理/日志设置

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 活动目录操作 | 已禁用 | 所有 VDA 版本 |
| 常见信息 | 已禁用 | 所有 VDA 版本 |
| 常见警告 | 已禁用 | 所有 VDA 版本 |
| 启用日志记录 | 已禁用 | 所有 VDA 版本 |
| 文件系统操作 | 已禁用 | 所有 VDA 版本 |
| 文件系统通知 | 已禁用 | 所有 VDA 版本 |
| 注销 | 已禁用 | 所有 VDA 版本 |
| 登录 | 已禁用 | 所有 VDA 版本 |
| 日志文件的最大大小 | 1048576 | 所有 VDA 版本 |
| 日志文件路径 | 已禁用。日志文件保存在默认位置；%SystemRoot%\System32\Logfiles\UserProfileManager。 | 所有 VDA 版本 |
| 个性化用户信息 | 已禁用 | 所有 VDA 版本 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 登录和注销时的策略值 | 已禁用 | 所有 VDA 版本 |
| 注册表操作 | 已禁用 | 所有 VDA 版本 |
| 注销时的注册表差异 | 已禁用 | 所有 VDA 版本 |

## 配置文件管理/配置文件处理

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 删除缓存配置文件前的延迟 | 0 | 所有 VDA 版本 |
| 在注销时删除本地缓存的配置文件 | 已禁用 | 所有 VDA 版本 |
| 本地配置文件冲突处理 | 使用本地配置文件 | 所有 VDA 版本 |
| 现有配置文件的迁移 | 本地和漫游 | 所有 VDA 版本 |
| 模板配置文件路径 | 已禁用。新用户配置文件是在用户首次登录的设备上从默认用户配置文件创建的。 | 所有 VDA 版本 |
| 模板配置文件覆盖本地配置文件 | 已禁用 | 所有 VDA 版本 |
| 模板配置文件覆盖漫游配置文件 | 已禁用 | 所有 VDA 版本 |
| 用作所有登录的 Citrix® 强制配置文件的模板配置文件 | 已禁用 | 所有 VDA 版本 |

## 配置文件管理/注册表

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 排除列表 | 已禁用。用户注销时，HKCU 配置单元中的所有注册表项都会被处理。 | 所有 VDA 版本 |

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 包含列表 | 已禁用。用户注销时，HKCU 配置单元中的所有注册表项都会被处理。 | 所有 VDA 版本 |

## 配置文件管理/流式用户配置文件

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 始终缓存 | 已禁用 | 所有 VDA 版本 |
| 始终缓存大小 | 0 MB | 所有 VDA 版本 |
| 配置文件流技术 | 已禁用 | 所有 VDA 版本 |
| 流式用户配置文件组 | 已禁用。OU 中的所有用户配置文件都会正常处理。 | 所有 VDA 版本 |
| 挂起区域锁定文件的超时（天） | 1 天 | 所有 VDA 版本 |

## 接收器

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| StoreFront™ 帐户列表 | 未指定任何应用商店 | 多会话操作系统 VDA 7 到当前版本，单会话操作系统 VDA 7 到当前版本 |

## 用户个性化层

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 用户层存储库路径 | 已禁用。未指定路径。 | VDA 19.12 及更高版本 |
| 用户层大小（GB） | 10 GB。用户层是精简预配的磁盘，可扩展到设定的大小。用户层的大小永不减小。 | VDA 19.12 或更高版本 |

## 虚拟投递代理

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 控制器注册 IPv6 子网掩码 | 未指定子网掩码 | 适用于多会话操作系统 7 到当前版本的 VDA，适用于单会话操作系统 7 到当前版本的 VDA |
| 控制器注册端口 | 80 | 所有 VDA 版本 |
| 控制器 SID | 未指定 SID | 所有 VDA 版本 |
| 控制器 | 未指定控制器 | 所有 VDA 版本 |
| 启用控制器自动更新 | 启用 | 适用于多会话操作系统 7 到当前版本的 VDA，适用于单会话操作系统 7 到当前版本的 VDA |
| 仅使用 IPv6 控制器注册 | 已禁用 | 适用于多会话操作系统 7 到当前版本的 VDA，适用于单会话操作系统 7 到当前版本的 VDA |
| 站点 GUID | 未指定 GUID | 所有 VDA 版本 |

## 虚拟交付代理/HDX 3D Pro

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 启用无损 | 启用 | VDA 5.5, 5.6 FP1 |
| HDX 3D Pro 质量设置 | VDA 5.5, 5.6 FP1 | |

## 虚拟投递代理/监控

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 启用进程监控 | 已禁用 | VDA 7.11 到当前版本 |
| 启用资源监控 | 启用 | VDA 7.11 到当前版本 |

### 虚拟 IP

| 名称 | 默认设置 | VDA |
| --- | --- | --- |
| 虚拟 IP 环回支持 | 已禁用 | VDA 7.6 到当前版本 |
| 虚拟 IP 虚拟环回程序列表 | 无 | VDA 7.6 到当前版本 |

## 策略设置参考

策略包含在策略强制执行时应用的设置。本节中的描述还指明了是否需要更多设置才能启用某个功能，或者这些设置是否与某个设置类似。

### 快速参考

下表列出了可在策略中配置的设置。在左列中找到要完成的任务，然后在右列中找到其对应的设置。

所有策略设置的完整列表均以 .CHM（编译的 HTML）格式和 .CSV 格式提供。这些文件位于安装了代理（交付控制器）的服务器上的 `\program files\citrix\grouppolicy` 文件夹中。您也可以单击此处下载最新版本的策略设置。

### 音频

| 对于此任务 | 使用此策略设置 |
| --- | --- |
| 控制是否允许多个音频设备的使用 | 音频即插即用 |
| 控制是否允许从用户设备上的麦克风输入音频 | 客户端麦克风重定向 |
| 控制用户设备上的音频质量 | 音频质量 |
| 控制用户设备上扬声器的音频映射 | 客户端音频重定向 |

### 用户设备的带宽

| 要限制用于以下目的的带宽 | 使用此策略设置 |
| --- | --- |
| 客户端音频映射 | 音频重定向带宽限制或音频重定向带宽限制百分比 |

| 要限制用于以下目的的带宽 | 使用此策略设置 |
| --- | --- |
| 使用本地剪贴板进行剪切和粘贴 | 剪贴板重定向带宽限制或剪贴板重定向带宽限制百分比 |
| 在会话中访问本地客户端驱动器 | 文件重定向带宽限制或文件重定向带宽限制百分比 |
| HDX™ MediaStream 多媒体加速 | HDX MediaStream 多媒体加速带宽限制或 HDX MediaStream 多媒体加速带宽限制百分比 |
| 客户端会话 | 总体会话带宽限制 |
| 打印 | 打印机重定向带宽限制或打印机重定向带宽限制百分比 |
| TWAIN 设备（例如照相机或扫描仪） | TWAIN 设备重定向带宽限制或 TWAIN 设备重定向带宽限制百分比 |
| USB 设备 | 客户端 USB 设备重定向带宽限制或客户端 USB 设备重定向带宽限制百分比 |

## 客户端驱动器和用户设备的重定向

| 对于此任务 | 使用此策略设置 |
| --- | --- |
| 控制用户登录服务器时是否连接用户设备上的驱动器 | 自动连接客户端驱动器 |
| 控制服务器与本地剪贴板之间的剪切和粘贴数据传输 | 客户端剪贴板重定向 |
| 控制驱动器如何从用户设备映射 | 客户端驱动器重定向 |
| 控制用户的本地硬盘驱动器在会话中是否可用 | 客户端固定驱动器和客户端驱动器重定向 |
| 控制用户的本地软盘驱动器在会话中是否可用 | 客户端软盘驱动器和客户端驱动器重定向 |
| 控制用户的网络驱动器在会话中是否可用 | 客户端网络驱动器和客户端驱动器重定向 |
| 控制用户的本地 CD、DVD 或蓝光驱动器在会话中是否可用 | 客户端光盘驱动器和客户端驱动器重定向 |

| 对于此任务 | 使用此策略设置 |
| --- | --- |
| 控制用户的本地可移动驱动器在会话中是否可用 | 客户端可移动驱动器和客户端驱动器重定向 |
| 控制用户的 TWAIN 设备（例如扫描仪和照相机）在会话中是否可用，并控制图像数据传输的压缩 | 客户端 TWAIN 设备重定向；TWAIN 压缩重定向 |
| 控制 USB 设备在会话中是否可用 | 客户端 USB 设备重定向和客户端 USB 设备重定向规则 |
| 提高通过 WAN 向客户端磁盘写入和复制文件的速度 | 使用异步写入 |

## 内容重定向

| 对于此任务 | 使用此策略设置 |
| --- | --- |
| 控制是否使用从服务器到用户设备的内容重定向 | 主机到客户端重定向 |

## 桌面 UI

| 对于此任务 | 使用此策略设置 |
| --- | --- |
| 控制是否在用户会话中使用桌面壁纸 | 桌面壁纸 |
| 在拖动窗口时查看窗口内容 | 拖动时查看窗口内容 |

## 图形和多媒体

**重要提示：**

Flash 策略保留仅是为了允许使用旧版 VDA 的客户使用较新的控制器（例如，版本 1912 控制器）并仍可使用 Flash。此 VDA 版本不支持 Flash。

| 对于此任务 | 使用此策略设置 |
| --- | --- |
| 控制从虚拟桌面发送到用户设备的最大每秒帧数 | 目标帧率 |
| 控制在用户设备上显示的图像的视觉质量 | 视觉质量 |
| 控制网站在会话中访问时是否可以显示 Flash 内容 | Flash 服务器端内容获取 URL 列表；Flash URL 兼容性列表；Flash 视频回退阻止策略设置；Flash 视频回退阻止错误 *.swf |
| 控制服务器渲染视频的压缩 | 使用视频编解码器进行压缩；对视频编解码器使用硬件编码 |
| 控制向用户交付 HTML5 多媒体 Web 内容 | HTML5 视频重定向 |

## 优先处理多流网络流量

| 对于此任务 | 使用此策略设置 |
| --- | --- |
| 指定跨多个连接的 ICA® 流量端口并建立网络优先级 | 多端口策略 |
| 启用服务器和用户设备之间的多流连接支持 | 多流（计算机和用户设置） |

## 打印

| 对于此任务 | 使用此策略设置 |
| --- | --- |
| 控制在用户设备上创建客户端打印机 | 自动创建客户端打印机和客户端打印机重定向 |
| 控制打印机属性的存储位置 | 打印机属性保留 |
| 控制客户端或服务器是否处理打印请求 | 直接连接到打印服务器 |
| 控制用户是否可以访问连接到其用户设备的打印机 | 客户端打印机重定向 |
| 控制在自动创建客户端和网络打印机时安装本机 Windows 驱动程序 | 自动安装内置打印机驱动程序 |

| 对于此任务 | 使用此策略设置 |
| --- | --- |
| 控制何时使用通用打印机驱动程序 | 通用打印机驱动程序使用情况 |
| 根据漫游用户会话信息选择打印机 | 默认打印机 |
| 为通用打印服务器配置负载平衡和故障转移阈值 | 用于负载平衡的通用打印服务器；通用打印服务器停用阈值 |

**注意：**

策略不能用于在桌面或应用程序会话中启用屏幕保护程序。对于需要屏幕保护程序的用户，屏幕保护程序可以在用户设备上实现。

## ICA® 策略设置

**注意：**

此页面提供 ICA 策略设置的说明和支持的配置值。有关使用策略的更多信息，请参阅 使用策略 部分。

### 自适应传输

此设置允许或阻止通过 EDT 进行数据传输，EDT 为主要方式，并回退到 TCP。

默认情况下，自适应传输处于启用状态（**首选**），并且在可能的情况下使用 EDT，并回退到 TCP。如果已禁用并要启用它，请按照此过程操作。

1. 在 Studio 中，启用策略设置 HDX™ 自适应传输。我们还建议您不要将此功能作为站点中所有对象的通用策略启用。
2. 要启用策略设置，请将值设置为 **首选**，然后单击 **确定**。

**首选**。在可能的情况下使用通过 EDT 的自适应传输，并回退到 TCP。

**诊断模式**。EDT 被强制启用，并且回退到 TCP 被禁用。我们建议仅将此设置用于故障排除。

**关闭**。TCP 被强制启用，并且 EDT 被禁用。

有关更多信息，请参阅 自适应传输。

### 拖放设置

此设置允许或阻止在客户端与虚拟应用程序或桌面之间拖放文件。默认情况下，拖放策略处于禁用状态。要启用此策略，请执行以下操作：

1. 在 Citrix Studio 中，启用策略设置 **拖放**。
2. 将值设置为 **已启用**，然后单击 **确定**。

### 应用程序启动等待超时

此设置指定会话等待第一个应用程序启动的等待超时值（以毫秒为单位）。如果应用程序的启动超出此时间段，则会话将结束。

您可以选择默认时间（10,000 毫秒）或指定一个以毫秒为单位的数字。

### 客户端剪贴板重定向

此设置允许或阻止将用户设备上的剪贴板映射到服务器上的剪贴板。

默认情况下，允许剪贴板重定向。

要阻止会话与本地剪贴板之间的数据剪切和粘贴传输，请选择 **禁止**。用户仍然可以在会话中运行的应用程序之间剪切和粘贴数据。

允许此设置后，请配置剪贴板在客户端连接中可占用的最大允许带宽。使用**剪贴板重定向带宽限制**或**剪贴板重定向带宽限制百分比**设置。

#### 客户端剪贴板写入允许的格式

当**限制客户端剪贴板写入**设置为**已启用**时，主机剪贴板数据无法与客户端端点共享。您可以使用此设置允许特定的数据格式与客户端端点剪贴板共享。要使用此设置，请启用它并添加要允许的特定格式。

以下剪贴板格式是系统定义的：

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT

- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

以下自定义格式在 XenApp 和 XenDesktop 以及 Citrix Virtual Apps and Desktops™ 中预定义：

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML 格式默认处于禁用状态。要启用此功能：

- 验证 **客户端剪贴板重定向** 是否设置为 **允许**。
- 验证 **限制客户端剪贴板写入** 是否设置为 **已启用**。
- 在 **客户端剪贴板写入允许的格式** 中添加 **CF_HTML**（以及您希望支持的任何其他格式）的条目。

您可以添加更多自定义格式。自定义格式名称必须与要注册到系统的格式匹配。格式名称区分大小写。

如果 **客户端剪贴板重定向** 策略设置为 **已禁止** 或 **限制客户端剪贴板写入** 策略设置为 **已禁用**，则此设置不适用。

> **注意：**
>
> 启用 HTML 格式剪贴板复制支持 (CF_HTML) 会将复制内容源中的任何脚本复制到目标。在继续复制之前，请检查您是否信任该源。如果您复制了包含脚本的内容，则只有将目标文件保存为 HTML 文件并运行它时，这些脚本才会生效。

**限制剪贴板客户端到会话的传输大小**

此设置指定用户在单个剪切和粘贴操作期间可以从客户端端点传输到虚拟会话的剪贴板数据的最大大小。

要限制剪贴板传输大小，请启用 **限制剪贴板客户端到会话的传输大小** 设置。然后，在 **大小限制** 字段中，输入一个以千字节为单位的值，以定义本地剪贴板与会话之间的数据传输大小。

默认情况下，此设置处于禁用状态，并且客户端到会话的传输没有限制。

**限制剪贴板会话到客户端的传输大小**

此设置指定用户在单个剪切和粘贴操作期间可以从虚拟会话传输到客户端端点的剪贴板数据的最大大小。

要限制剪贴板传输大小，请启用**限制剪贴板会话到客户端的传输大小**设置。然后，在**大小限制**字段中，输入一个以千字节为单位的值，以定义会话与本地剪贴板之间的数据传输大小。

默认情况下，此设置处于禁用状态，并且会话到客户端的传输没有限制。

**限制客户端剪贴板写入**

如果此设置为“**已启用**”，则主机剪贴板数据无法与客户端端点共享。您可以通过启用“**允许客户端剪贴板写入的格式**”设置来允许特定格式。

默认情况下，此设置为“**已禁用**”。

**限制会话剪贴板写入**

如果此设置为“**已启用**”，则客户端剪贴板数据无法与会话应用程序共享。您可以通过启用“**允许会话剪贴板写入的格式**”设置来允许特定格式。

默认情况下，此设置为“**已禁用**”。

### 允许会话剪贴板写入的格式

当“**限制会话剪贴板写入**”设置为“**已启用**”时，客户端剪贴板数据无法与会话应用程序共享。您可以使用此设置来允许特定数据格式与会话剪贴板共享。

以下剪贴板格式是系统定义的：

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

以下自定义格式已在 XenApp and XenDesktop 以及 Citrix Virtual Apps and Desktops 中预定义：

- CFX_RICHTEXT

- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML 格式默认处于禁用状态。要启用此功能，请执行以下操作：

- 验证**客户端剪贴板重定向**是否设置为**允许**。
- 验证**限制会话剪贴板写入**是否设置为**已启用**。
- 在**允许会话剪贴板写入的格式**中添加 **CF_HTML**（以及您希望支持的任何其他格式）的条目。

您可以添加更多自定义格式。自定义格式名称必须与要向系统注册的格式匹配。格式名称区分大小写。

如果**客户端剪贴板重定向**策略设置为**已禁止**或**限制会话剪贴板写入**策略设置为**已禁用**，则此设置不适用。

> **注意：**
>
> 启用 HTML 格式剪贴板复制支持 (CF_HTML) 会将复制内容源中的所有脚本复制到目标。在继续复制之前，请检查您是否信任源。如果您复制了包含脚本的内容，则只有将目标文件另存为 HTML 文件并运行它时，这些脚本才会生效。

### 桌面启动

此设置允许或阻止 VDA Direct Access Users 组中的非管理用户使用 ICA 连接连接到该 VDA 上的会话。

默认情况下，非管理用户无法连接到这些会话。

此设置不影响 VDA 直接访问用户组中正在使用 RDP 连接的非管理用户。无论此设置是启用还是禁用，这些用户都可以连接到 VDA。此设置不影响不在 VDA 直接访问用户组中的非管理用户。无论此设置是启用还是禁用，这些用户都无法连接到 VDA。

### FIDO2 重定向

此设置启用或禁用 FIDO2 重定向。FIDO2 重定向允许用户利用虚拟机中的本地端点 FIDO2 组件。用户可以通过 FIDO2 安全密钥或在具有 TPM 2.0 和 Windows Hello 的设备上使用集成生物识别技术对虚拟会话进行身份验证。

当此设置为 **允许** 时，用户可以通过使用本地端点功能执行 FIDO2 身份验证。默认情况下，此设置为 **允许**。

还可以通过配置以下注册表项在客户端端点上启用或禁用 FIDO2 重定向：

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\

名称: FIDO2

类型：REG_DWORD

值：1

将值设置为 0 可禁用该功能，设置为 1 可启用该功能。默认情况下，该功能处于启用状态。

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

### ICA 侦听器连接超时

此设置指定完成使用 ICA 协议的连接的最大等待时间。

默认情况下，最大等待时间为 120,000 毫秒，即两分钟。

### ICA 侦听器端口号

此设置指定服务器上 ICA 协议使用的 TCP/IP 端口号。

默认情况下，端口号设置为 1494。

有效的端口号必须在 0-65535 的范围内，并且不得与其他知名端口号冲突。如果更改端口号，请重新启动服务器以使新值生效。如果更改服务器上的端口号，还必须在连接到服务器的每个 Citrix Workspace™ 应用程序或插件上更改它。

### 键盘和输入法编辑器 (IME)

此设置启用或禁用以下功能：

- 动态键盘布局同步
- 输入法编辑器 (IME)
- Unicode 键盘布局映射
- 隐藏或显示键盘布局切换通知对话框消息

1. 在 Studio 中，选择 **键盘和 IME**。
2. 选择 **客户端键盘布局同步和 IME 改进** 以控制 VDA 中的动态键盘布局同步和通用客户端输入法编辑器 (IME) 功能。您可以配置：

   **已禁用** - 动态键盘布局同步和通用客户端输入法编辑器 (IME)。

   **支持动态客户端键盘布局同步** - 启用动态键盘布局同步。

   **支持动态客户端键盘布局同步和 IME 改进** - 同时启用动态键盘布局同步和通用客户端输入法编辑器 (IME)。
3. 选择 **启用 Unicode 键盘布局映射** 以启用或禁用 Unicode 键盘映射。
4. 选择 **隐藏键盘布局切换弹出消息框** 以控制是否显示一条消息，指示用户更改客户端键盘布局时键盘布局正在同步。如果您阻止消息出现，用户必须等待片刻才能开始输入，以避免字符输入不正确。

默认设置：

- **客户端键盘布局同步和 IME 改进**
  - 在 Windows Server 2016 和 Windows Server 2019 中已禁用。
  - 在 Windows Server 2012 和 Windows 2010 中支持动态客户端键盘布局同步和 IME 改进。
- **禁用 Unicode 键盘布局映射**
- **显示键盘布局切换弹出消息框**

此策略替换了策略设置的**描述**部分中列出的注册表设置。

### 注销检查器启动延迟

此设置指定延迟注销检查器启动的持续时间。使用此策略可设置客户端会话在断开连接之前等待的时间（以秒为单位）。

此设置还会增加用户从服务器注销所需的时间。

### 容忍丢包模式

> **重要提示：**
>
> - 此功能至少需要适用于 Windows 的 Citrix Workspace 应用程序 2002。此版本的 VDA 在可用时将支持此功能。

- 容错模式在 Citrix Gateway 或 Citrix Gateway Service 上不受支持。此模式仅在直接连接时可用。

此设置启用或禁用容错模式。

默认情况下，容错模式为**允许**。

允许时，当数据包丢失和延迟超过阈值时进入此模式。您可以使用容错阈值策略设置阈值。

有关详细信息，请参阅容错模式。

### 容错阈值

当容错模式可用时，此设置指定网络指标阈值，在该阈值下会话切换到容错模式。

默认阈值为：

- 数据包丢失：5%
- 延迟：300 毫秒 (RTT)

有关详细信息，请参阅容错模式。

### Rendezvous 协议

此设置更改了使用 Citrix Gateway Service 时 HDX 会话的代理方式。启用后，HDX 流量不再流经 Citrix Cloud Connector。相反，VDA 直接与 Citrix Gateway Service 建立出站连接（从而增强了 Cloud Connector 的可扩展性）。

**重要提示：**

Citrix Cloud™ 中的功能切换和 HDX 策略设置控制此功能。Citrix Cloud 功能切换默认启用，而 HDX 设置默认禁用。HDX 设置仅影响通过 Citrix Gateway Service 建立的 HDX 会话。此设置不影响客户端与 VDA 之间直接建立的会话或通过本地 Citrix Gateway 建立的会话。

有关信息，请参阅 Rendezvous 协议。

### Rendezvous 代理配置

此设置允许您配置用于 Rendezvous 协议的显式代理。如果使用透明代理，则无需启用此设置。

默认情况下，此设置为禁用。

禁用后，VDA 在尝试与 Gateway Service 建立 Rendezvous 连接时，不会通过任何非透明代理路由出站流量。

启用后，VDA 会尝试通过此设置中定义的代理与 Gateway Service 建立 Rendezvous 连接。

VDA 支持将 HTTP 和 SOCKS5 代理用于 Rendezvous 连接。要将 VDA 配置为对 Rendezvous 连接使用代理，必须启用此设置。此外，请指定代理地址或 PAC 文件路径。例如：

- 代理地址：`http://<URL or IP>:<port>` 或 `socks5://<URL or IP>:<port>`
- PAC 文件：`http://<URL or IP>/<path>/<filename>.pac`

  VDA 2103 版是使用 PAC 文件进行代理配置的最低支持版本。有关 SOCKS5 代理的 PAC 文件架构的详细信息，请参阅代理配置。

> **注意：**
>
> 只有 SOCKS5 代理支持通过 EDT 进行数据传输。对于 HTTP 代理，请使用 TCP 作为 ICA 的传输协议。
>
> 有关详细信息，请参阅Rendezvous 协议。

### 在客户端连接期间启动未发布的程序

此设置指定是否允许通过 RDP 在服务器上启动初始应用程序。

默认情况下，不允许通过 RDP 在服务器上启动初始应用程序。

### 平板电脑模式切换策略设置

平板电脑模式切换可优化 VDA 上 Store 应用程序、Win32 应用程序和 Windows shell 的外观和行为。它通过在从手机和平板电脑等小型设备或任何支持触摸的设备连接时自动将虚拟桌面切换到平板电脑模式来实现此目的。

如果禁用此策略，VDA 将处于用户设置的模式，并且无论客户端类型如何，都将始终保持相同的模式。

### 自动客户端重新连接策略设置

“**自动客户端重新连接**”部分包含用于控制会话自动重新连接的策略设置。

#### 自动客户端重新连接

此设置允许或阻止在连接中断后由同一客户端自动重新连接。

对于 Citrix Receiver for Windows 4.7 及更高版本以及 Citrix Workspace app 1808 及更高版本，自动客户端重新连接仅使用 Citrix Studio 中的策略设置。在 Studio 中更新这些策略会将自动客户端重新连接从服务器同步到客户端。对于旧版 Citrix Receiver for Windows，要配置自动客户端重新连接，请使用 Studio 策略并更改注册表或 default.ica 文件。

允许自动客户端重新连接使用户能够在连接中断后从中断处继续工作。自动重新连接会检测到中断的连接，然后将用户重新连接到其会话。

如果不使用包含会话 ID 和凭据密钥的 Citrix Workspace™ app cookie，自动重新连接可能会导致启动新会话。也就是说，不是重新连接到现有会话。如果 cookie 已过期，则不会使用该 cookie。例如，cookie 可能会因重新连接延迟或需要重新输入凭据而过期。如果用户有意断开连接，则不会触发自动客户端重新连接。

重新连接正在进行时，会话窗口会灰显。倒计时计时器显示会话重新连接前的剩余时间。会话超时后，它将断开连接。

对于应用程序会话，当允许自动重新连接时，通知区域中会显示一个倒计时计时器。此计时器指定会话重新连接前的剩余时间。Citrix Workspace app 会尝试重新连接到会话，直到成功重新连接或用户取消重新连接尝试。

对于用户会话，当允许自动重新连接时，Citrix Workspace app 会在指定时间内尝试重新连接到会话，除非成功重新连接或用户取消重新连接尝试。默认情况下，此期限为两分钟。要更改此期限，请编辑策略。

默认情况下，允许自动客户端重新连接。

要禁用自动客户端重新连接：

1. 启动 Citrix Studio 应用程序。
2. 打开**自动客户端重新连接**策略。
3. 将策略设置为**禁止**。

自动客户端重新连接图像

**自动客户端重新连接身份验证**

此设置要求对自动客户端重新连接进行身份验证。

用户首次登录时，凭据会被加密并存储在内存中，同时会创建一个包含加密密钥的 cookie。该 cookie 会发送到 Citrix Workspace app。配置此设置后，将不使用 cookie。相反，当 Citrix Workspace app 尝试自动重新连接时，会向用户显示一个对话框，要求输入凭据。

默认情况下，不需要身份验证。

要更改自动客户端重新连接身份验证：

1. 启动 Citrix Studio 应用程序。
2. 打开**自动客户端重新连接身份验证**策略。
3. 启用或禁用身份验证。
4. 选择**确定**。

**自动客户端重新连接日志记录**

此设置启用或禁用在事件日志中记录自动客户端重新连接。

启用日志记录后，服务器系统日志会捕获有关成功和失败的自动重新连接事件的信息。站点不提供所有服务器的重新连接事件的组合日志。

默认情况下，日志记录处于禁用状态。

要更改自动客户端重新连接日志记录：

1. 请启动 Citrix Studio。
2. 打开**自动客户端重新连接日志记录**策略。
3. 启用或禁用日志记录。
4. 选择 **确定**。

**自动客户端重新连接超时**

默认情况下，客户端自动重新连接超时设置为 120 秒，客户端自动重新连接超时的最大可配置值为 300 秒。

要更改客户端自动重新连接超时：

1. 请启动 Citrix Studio。
2. 打开 **客户端自动重新连接超时** 策略。
3. 编辑超时值。
4. 选择 **确定**。

**重新连接 UI 透明度级别**

您可以使用 Studio 策略配置在会话可靠性重新连接期间应用于 XenApp 或 XenDesktop® 会话窗口的透明度级别。

默认情况下，重新连接 UI 透明度设置为 80%。

要更改重新连接用户界面透明度级别：

1. 启动 Citrix Studio 应用程序。
2. 打开 **重新连接 UI 透明度级别** 策略。
3. 编辑该值。
4. 选择 **确定**。

## 音频策略设置

**音频**部分包含策略设置，这些设置允许用户设备在会话中发送和接收音频，而不会降低性能。

### 自适应音频

此设置启用或禁用自适应音频。启用此策略后，音频质量设置将动态调整，以提供最佳用户体验。此设置适用于使用 Citrix Virtual Apps and Desktops™ 2109 或更高版本的 VDA 的单会话操作系统和多会话操作系统会话。

禁止此设置时，将应用音频质量策略。有关详细信息，请参阅音频质量。

默认情况下，自适应音频策略处于启用状态。

要禁用自适应音频：

1. 启动 Citrix Studio 应用程序。
2. 打开**自适应音频**策略。
3. 将策略设置为**禁止**。

自适应音频策略 1(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/policy-adaptive-audio1.png)

自适应音频策略 2(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/policy-adaptive-audio2.png)

### 通过 UDP 实时传输音频

此设置允许或阻止 VDA 和用户设备之间通过 RTP 使用用户数据报协议 (UDP) 传输和接收音频。禁用此设置时，音频将通过 TCP 发送和接收。

默认情况下，允许通过 UDP 传输音频。

### 音频即插即用

此设置允许或阻止使用多个音频设备录制和播放声音。

默认情况下，允许使用多个音频设备。

此设置仅适用于 Windows 多会话操作系统计算机。

### 音频质量

此设置指定用户会话中接收到的声音质量级别。

默认情况下，声音质量设置为“高 - 高清音频”。

要控制声音质量，请选择以下选项之一：

- 选择“低” - 适用于低带宽连接的低速连接。发送到用户设备的声音被压缩到 16 Kbps。这种压缩会导致声音质量显著下降。但也能为低带宽连接提供合理的性能。
- 选择中等 - 针对语音进行优化，以提供 IP 语音应用程序。此设置可在网络连接不佳（线路低于 512 Kbps，或存在严重拥塞和数据包丢失）的情况下提供媒体应用程序。此编解码器提供快速编码时间，使其非常适合在需要服务器端媒体处理时与软电话和统一通信应用程序配合使用。

  发送到用户设备的音频被压缩到 64 Kbps。这种压缩会导致用户设备上播放的音频质量适度降低，同时提供低延迟并消耗低带宽。如果 IP 语音质量不理想，请确保“通过 UDP 的音频实时传输”策略设置已设置为“允许”。

  现在，仅当选择此音频质量时，才支持通过 UDP 的实时传输 (RTP)。即使对于通过低速（低于 512 Kbps）线路等具有挑战性的网络连接传输媒体应用程序，也请使用此音频质量。此外，当网络中存在拥塞和数据包丢失时也适用。
- 选择高 - 适用于带宽充足且音质重要的连接的高清音频。客户端可以以其原始速率播放声音。声音以高质量级别压缩，可保持高达 CD 质量，并使用高达 112 Kbps 的带宽。传输此量的数据可能会导致 CPU 使用率增加和网络拥塞。

带宽仅在录制或播放音频时消耗。如果两者同时发生，带宽消耗将翻倍。

要指定最大带宽量，请配置“**音频重定向带宽限制**”或“**音频重定向带宽限制百分比**”设置。

### 客户端音频重定向

此设置指定服务器上托管的应用程序是否可以通过用户设备上安装的声音设备播放声音。此设置还指定用户是否可以录制音频输入。

默认情况下，允许音频重定向。

允许此设置后，您可以限制播放或录制音频所消耗的带宽。限制音频消耗的带宽量可以提高应用程序性能，但也可能会降低音频质量。带宽仅在录制或播放音频时消耗。如果两者同时发生，带宽消耗将翻倍。要指定最大带宽量，请配置“**音频重定向带宽限制**”或“**音频重定向带宽限制百分比**”设置。

在 Windows 多会话操作系统计算机上，请确保启用“**音频即插即用**”设置以支持多个音频设备。

重要提示：禁止客户端音频重定向会禁用所有 HDX™ 音频功能。

#### 客户端麦克风重定向

此设置启用或禁用客户端麦克风重定向。启用后，用户可以使用麦克风在会话中录制音频输入。

默认情况下，允许麦克风重定向。

为了安全起见，当设备上的不受信任服务器尝试访问麦克风时，会向用户发出警报。用户可以选择接受或不接受访问。用户可以在 Citrix Workspace™ 应用程序上禁用此警报。

在 Windows 多会话操作系统计算机上，请确保启用“音频即插即用”设置以支持多个音频设备。

如果用户设备上禁用了**客户端音频重定向**设置，则此规则无效。

### 带宽策略设置

**带宽**部分包含用于避免与客户端会话带宽使用相关的性能问题的策略设置。

重要提示：将这些策略设置与**多流策略**设置一起使用可能会产生意外结果。如果您在策略中使用多流设置，请确保不包含这些带宽限制策略设置。

#### 音频重定向带宽限制

此设置指定用户会话中播放或录制音频允许的最大带宽。允许的最大带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为**音频重定向带宽限制百分比**设置输入一个值，则应用限制性最强的设置（较低的值）。

#### 音频重定向带宽限制百分比

此设置指定播放或录制音频允许的最大带宽限制，占总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为**音频重定向带宽限制**设置输入一个值，则应用限制性最强的设置（较低的值）。

如果您配置此设置，则还必须配置**会话总带宽限制**设置，该设置指定可用于客户端会话的带宽总量。

#### 客户端 USB 设备重定向带宽限制

此设置指定将 USB 设备重定向到客户端和从客户端重定向允许的最大带宽。允许的最大带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为**客户端 USB 设备重定向带宽限制百分比**设置输入一个值，则应用限制性最强的设置（较低的值）。

**客户端 USB 设备重定向带宽限制百分比**

此设置指定将 USB 设备重定向到客户端和从客户端重定向允许的最大带宽，占总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为 **客户端 USB 设备重定向带宽限制** 设置输入一个值，则应用限制最严格的设置（较低的值）。

如果您配置此设置，则还必须配置 **会话总带宽限制** 设置，该设置指定了客户端会话可用的总带宽量。

**剪贴板重定向带宽限制**

此设置指定了会话与本地剪贴板之间数据传输的最大允许带宽。最大允许带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为 **剪贴板重定向带宽限制百分比** 设置输入一个值，则应用限制最严格的设置（较低的值）。

**剪贴板重定向带宽限制百分比**

此设置指定了会话与本地剪贴板之间数据传输的最大允许带宽，该带宽是会话总带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为 **剪贴板重定向带宽限制** 设置输入一个值，则应用限制最严格的设置（较低的值）。

如果您配置此设置，则还必须配置 **会话总带宽限制** 设置，该设置指定了客户端会话可用的总带宽量。

**COM 端口重定向带宽限制**

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置；请参阅 使用注册表配置 COM 端口和 LPT 端口重定向设置。

此设置指定了客户端连接中访问 COM 端口的最大允许带宽（以千比特每秒为单位）。如果您为此设置输入一个值，并为 **COM 端口重定向带宽限制百分比** 设置输入一个值，则应用限制最严格的设置（较低的值）。

### COM 端口重定向带宽限制百分比

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置；请参阅 使用注册表配置 COM 端口和 LPT 端口重定向设置。

此设置指定了客户端连接中访问 COM 端口的最大允许带宽，该带宽是会话总带宽的百分比。

默认情况下，未指定最大值（零）

如果您为此设置输入一个值，并为 **COM 端口重定向带宽限制** 设置输入一个值，则应用限制最严格的设置（较低的值）。

如果您配置此设置，则还必须配置“**会话总带宽限制**”设置，该设置指定客户端会话可用的总带宽量。

### 文件重定向带宽限制

此设置指定用户会话中访问客户端驱动器的最大允许带宽。最大允许带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**文件重定向带宽限制百分比**”设置输入一个值，则最严格的设置（较低的值）将生效。

### 文件重定向带宽限制百分比

此设置指定访问客户端驱动器的最大允许带宽限制，该限制是总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**文件重定向带宽限制**”设置输入一个值，则最严格的设置（较低的值）将应用。

如果您配置此设置，则还必须配置“**会话总带宽限制**”设置，该设置指定客户端会话可用的总带宽量。

### HDX™ MediaStream 多媒体加速带宽限制

此设置指定使用 HDX MediaStream 多媒体加速传输流式音频和视频的最大允许带宽限制。最大允许带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**HDX MediaStream 多媒体加速带宽限制百分比**”设置输入一个值，则最严格的设置（较低的值）将生效。

### HDX MediaStream 多媒体加速带宽限制百分比

此设置指定使用 HDX MediaStream 多媒体加速传输流式音频和视频的最大允许带宽，该带宽是总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置和**HDX MediaStream 多媒体加速带宽限制**设置输入值，则最严格的设置（较低的值）将生效。

如果配置此设置，则还必须配置**会话总带宽限制**设置，该设置指定可用于客户端会话的总带宽量。

### LPT 端口重定向带宽限制

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置；请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。

此设置指定单个用户会话中使用 LPT 端口的打印作业允许的最大带宽。允许的最大带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置和**LPT 端口重定向带宽限制百分比**设置输入值，则最严格的设置（较低的值）将应用。

### LPT 端口重定向带宽限制百分比

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置；请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。

此设置指定单个客户端会话中使用 LPT 端口的打印作业的带宽限制，该限制占总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置和**LPT 端口重定向带宽限制**设置输入值，则最严格的设置（较低的值）将应用。

如果配置此设置，则还必须配置**会话总带宽限制**设置，该设置指定可用于客户端会话的总带宽量。

### 总体会话带宽限制

此设置指定用户会话可用的总带宽量，以千比特每秒为单位。

可强制执行的最大带宽上限为 20 Mbps (20,000 Kbps)。默认情况下，未指定最大值（零）。

当客户端连接之外的其他应用程序争用有限带宽时，限制客户端连接消耗的带宽量可以提高性能。

### 打印机重定向带宽限制

此设置指定用户会话中访问客户端打印机允许的最大带宽。允许的最大带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**打印机重定向带宽限制百分比**”设置输入一个值，则应用限制性最强的设置（较低的值）。

### 打印机重定向带宽限制百分比

此设置指定了访问客户端打印机的最大允许带宽，该带宽是总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**打印机重定向带宽限制**”设置输入一个值，则应用限制性最强的设置（值较低的设置）。

如果您配置此设置，则还必须配置“**总会话带宽限制**”设置，该设置指定了客户端会话可用的总带宽量。

### TWAIN 设备重定向带宽限制

此设置指定了从已发布的应用程序控制 TWAIN 成像设备的最大允许带宽。最大允许带宽以千比特每秒为单位指定。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**TWAIN 设备重定向带宽限制百分比**”设置输入一个值，则应用限制性最强的设置（较低的值）。

### TWAIN 设备重定向带宽限制百分比

此设置指定了从已发布的应用程序控制 TWAIN 成像设备的最大允许带宽，该带宽是总会话带宽的百分比。

默认情况下，未指定最大值（零）。

如果您为此设置输入一个值，并为“**TWAIN 设备重定向带宽限制**”设置输入一个值，则应用限制性最强的设置（值较低的设置）。

如果您配置此设置，则还必须配置“**总会话带宽限制**”设置，该设置指定了客户端会话可用的总带宽量。

### 双向内容重定向策略设置

“**双向内容重定向**”部分包含用于启用或禁用客户端到主机以及主机到客户端 URL 重定向的策略设置。

服务器策略在 Studio 中设置。客户端策略从 Citrix Workspace™ 应用程序组策略对象管理模板中设置。

Citrix® 提供主机到客户端重定向和本地应用程序访问，用于客户端到 URL 重定向。但是，我们建议您对已加入域的 Windows 客户端使用双向内容重定向。

#### 允许双向内容重定向

将此策略设置为**允许**，以启用服务器 (VDA) 与客户端之间的重定向。默认情况下，它设置为**禁止**。

使用**允许重定向到客户端的 URL** 策略配置用于 VDA 到客户端重定向的 URL 列表。

> **注意：**
>
> 必须在客户端上将此策略与**双向内容重定向**策略一起设置，才能允许重定向。

#### 允许重定向到客户端的 URL

指定当允许双向内容重定向时在客户端上打开的 URL 列表。

分号 (;) 是分隔符。星号 (*) 可用作通配符。例如:

```
*.xyz.com;https://www.example.com
```

### 浏览器内容重定向策略设置

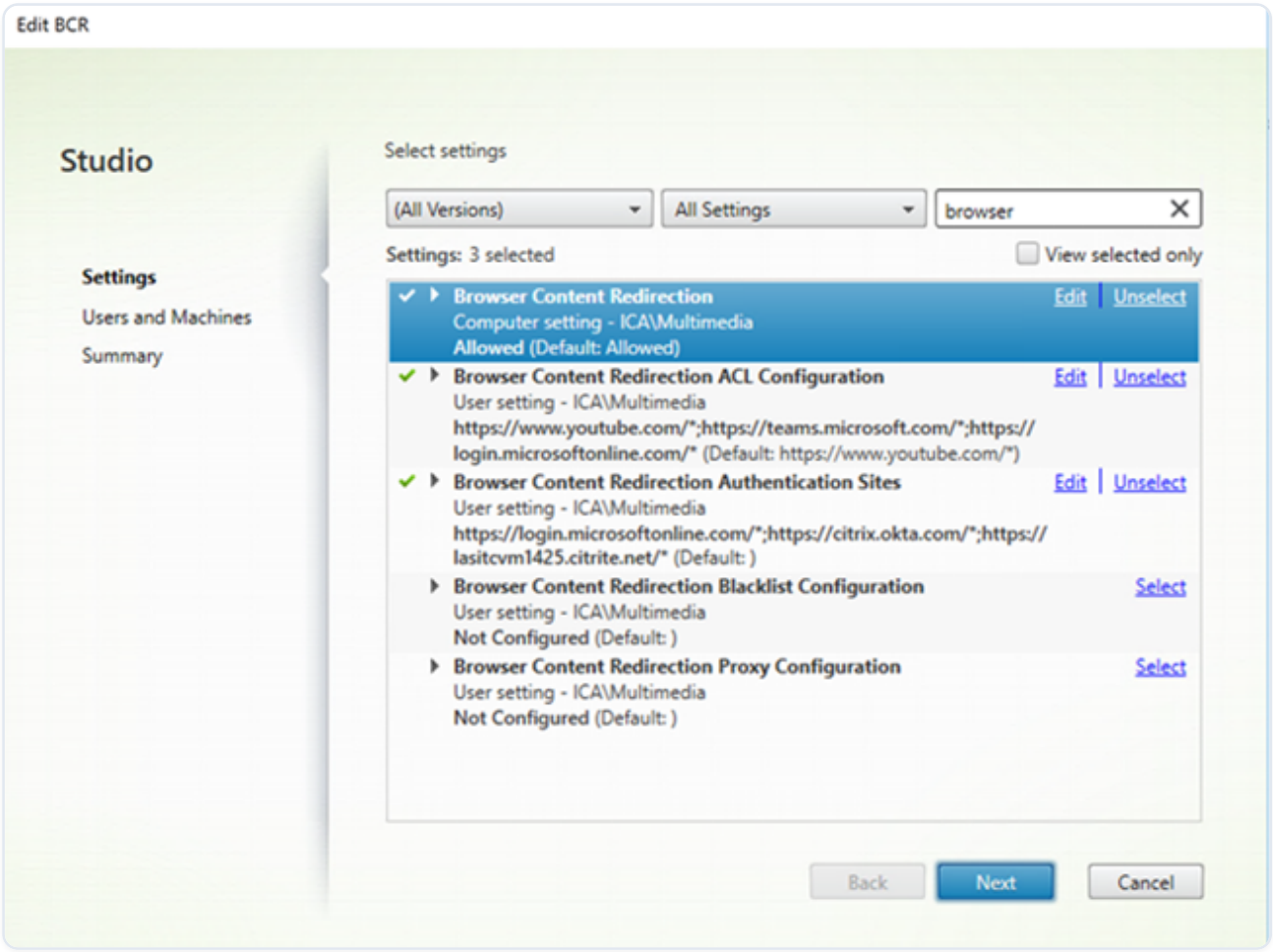
浏览器内容重定向部分包含用于配置此功能的策略设置。

浏览器内容重定向控制并优化了 Citrix Virtual Apps and Desktops™ 向用户交付任何 Web 浏览器内容（例如 HTML5）的方式。仅重定向浏览器中显示内容的可见区域。

HTML5 视频重定向和浏览器内容重定向是独立的功能。此功能不需要 HTML5 视频重定向策略即可工作。但是，Citrix HDX HTML5 视频重定向服务用于浏览器内容重定向。有关详细信息，请参阅浏览器内容重定向。

**策略设置：**

Citrix Studio 中提供了以下浏览器内容重定向功能的策略设置。这些策略可以通过 VDA 上的注册表项覆盖，但注册表项是可选的。




### TLS 和浏览器内容重定向

您可以使用浏览器内容重定向来重定向 HTTPS 网站。注入到这些网站中的 JavaScript 必须与 VDA 上运行的 Citrix HDX HTML5 视频重定向服务 (WebSocketService.exe) 建立 TLS 连接。为了实现此重定向并保持网页的 TLS 完整性，Citrix HDX HTML5 视频重定向服务会在 VDA 上的证书存储中生成两个自定义证书。

HdxVideo.js 使用安全 Web 套接字与 VDA 上运行的 WebSocketService.exe 进行通信。此进程在本地系统上运行，并执行 SSL 终止和用户会话映射。

WebSocketService.exe 正在侦听 127.0.0.1 端口 9001。

### 浏览器内容重定向

默认情况下，Citrix Workspace™ app 会尝试客户端获取和客户端渲染。当客户端获取和客户端渲染失败时，会尝试服务器端渲染。如果您还启用了浏览器内容重定向代理配置策略，Citrix Workspace app 将仅尝试服务器获取和客户端渲染。

默认情况下，此设置为“允许”。

### 浏览器内容重定向集成 Windows 身份验证支持设置

浏览器内容重定向支持使用协商方案进行身份验证的覆盖。此增强功能为与 VDA 位于同一域中配置了集成 Windows 身份验证 (IWA) 的 Web 服务器提供单点登录。

当设置为**允许**时，浏览器内容重定向覆盖会使用用户的 VDA 凭据获取协商票证。然后，用户通过单点登录向 Web 服务器进行身份验证。

当设置为**禁止**时，浏览器内容重定向覆盖不会从 VDA 请求协商票证。用户使用基本身份验证方法向 Web 服务器进行身份验证。此身份验证方法要求用户每次访问 Web 服务器时都输入其 VDA 凭据。

默认情况下，此设置为“禁用”。

### 浏览器内容重定向服务器获取 Web 代理身份验证设置

此设置通过下游 Web 代理路由源自覆盖的 HTTP 流量。下游 Web 代理使用 VDA 用户的域凭据通过 Negotiate 身份验证方案授权和验证 HTTP 流量。

您必须使用“浏览器内容重定向代理配置”策略在 PAC 文件中配置服务器获取模式的浏览器内容重定向。在 PAC 脚本中，提供通过下游 Web 代理路由覆盖流量的说明。然后配置下游 Web 代理以通过 Negotiate 身份验证方案对 VDA 用户进行身份验证。

当设置为“**允许**”时，Web 代理会响应 407 Negotiate 质询，其中包括 **Proxy-Authenticate: Negotiate** 标头。浏览器内容重定向随后使用 VDA 用户的域凭据获取 Kerberos 服务票据。此外，在后续对 Web 代理的请求中包含该服务票据。

当设置为“**禁用**”时，浏览器内容重定向会在不干扰的情况下代理覆盖与 Web 代理之间的所有 TCP 流量。覆盖使用基本身份验证凭据或任何其他可用凭据向 Web 代理进行身份验证。

默认情况下，此设置为“禁用”。

### 浏览器内容重定向访问控制列表 (ACL) 策略设置

使用此设置配置 URL 的访问控制列表 (ACL)，这些 URL 可以使用浏览器内容重定向或被拒绝访问浏览器内容重定向。

授权 URL 是允许列表中的 URL，其内容将重定向到客户端。

允许使用通配符 *，但不允许在 URL 的协议或域地址部分中使用。

允许：`http://www.xyz.com/index.html`、`https://www.xyz.com/*`、`http://www.xyz.com/*videos*`

不允许：`http://*.xyz.com/`

您可以通过在 URL 中指定路径来实现更好的粒度。例如，如果您指定 `https://www.xyz.com/sports/index.html`，则只有 index.html 页面会被重定向。

默认情况下，此设置设置为 `https://www.youtube.com/*`

有关详细信息，请参阅知识中心文章 CTX238236。

**浏览器内容重定向身份验证站点**

使用此设置配置 URL 列表。通过浏览器内容重定向重定向的站点使用此列表对用户进行身份验证。此设置指定当从允许列表中的 URL 导航离开时，浏览器内容重定向保持活动（重定向）的 URL。

一个典型的场景是依赖身份提供商 (IdP) 进行身份验证的网站。例如，网站 `www.xyz.com` 必须重定向到端点，但第三方 IdP（如 Okta (`www.xyz.okta.com`)）处理身份验证部分。管理员使用浏览器内容重定向 ACL 配置策略将 `www.xyz.com` 添加到允许列表。然后使用浏览器内容重定向身份验证站点将 `www.xyz.okta.com` 添加到允许列表。

有关详细信息，请参阅知识中心文章 CTX238236。

**浏览器内容重定向阻止列表设置**

此设置与浏览器内容重定向 ACL 配置设置协同工作。如果 URL 同时存在于浏览器内容重定向 ACL 配置设置和阻止列表配置设置中，则阻止列表配置优先，并且 URL 的浏览器内容不会被重定向。

**未经授权的 URL：** 指定阻止列表中的 URL，其浏览器内容不会重定向到客户端，而是在服务器上呈现。

允许使用通配符 *，但它不允许出现在协议或 URL 的域地址部分中。

允许：`http://www.xyz.com/index.html`、`https://www.xyz.com/*`、`http://www.xyz.com/*videos*`

不允许：`http://*.xyz.com/`

通过在 URL 中指定路径，可以实现更好的粒度。例如，如果指定 `https://www.xyz.com/sports/index.html`，则只有 index.html 位于阻止列表中。

**浏览器内容重定向代理设置**

此设置提供 VDA 上用于浏览器内容重定向的代理设置的配置选项。如果启用并使用有效的代理地址和端口号、PAC / WPAD URL 或直接/透明设置，Citrix Workspace 应用程序将仅尝试服务器获取和客户端呈现。

如果禁用或未配置并使用默认值，Citrix Workspace 应用程序将尝试客户端获取和客户端呈现。

默认情况下，此设置为“禁止”。

**显式代理的允许模式：**

`http://<hostname/ip address\>:\<port\>`

**示例：**

`http://proxy.example.citrix.com:80` `http://10.10.10.10:8080`

**PAC/WPAD 文件的允许模式：**

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

**示例：** `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

**示例：** `http://10.10.10.10/configuration/pac/wpad.dat`

**直接或透明代理的允许模式：**

在策略文本框中键入单词 **DIRECT**。

**浏览器内容重定向注册表项覆盖**

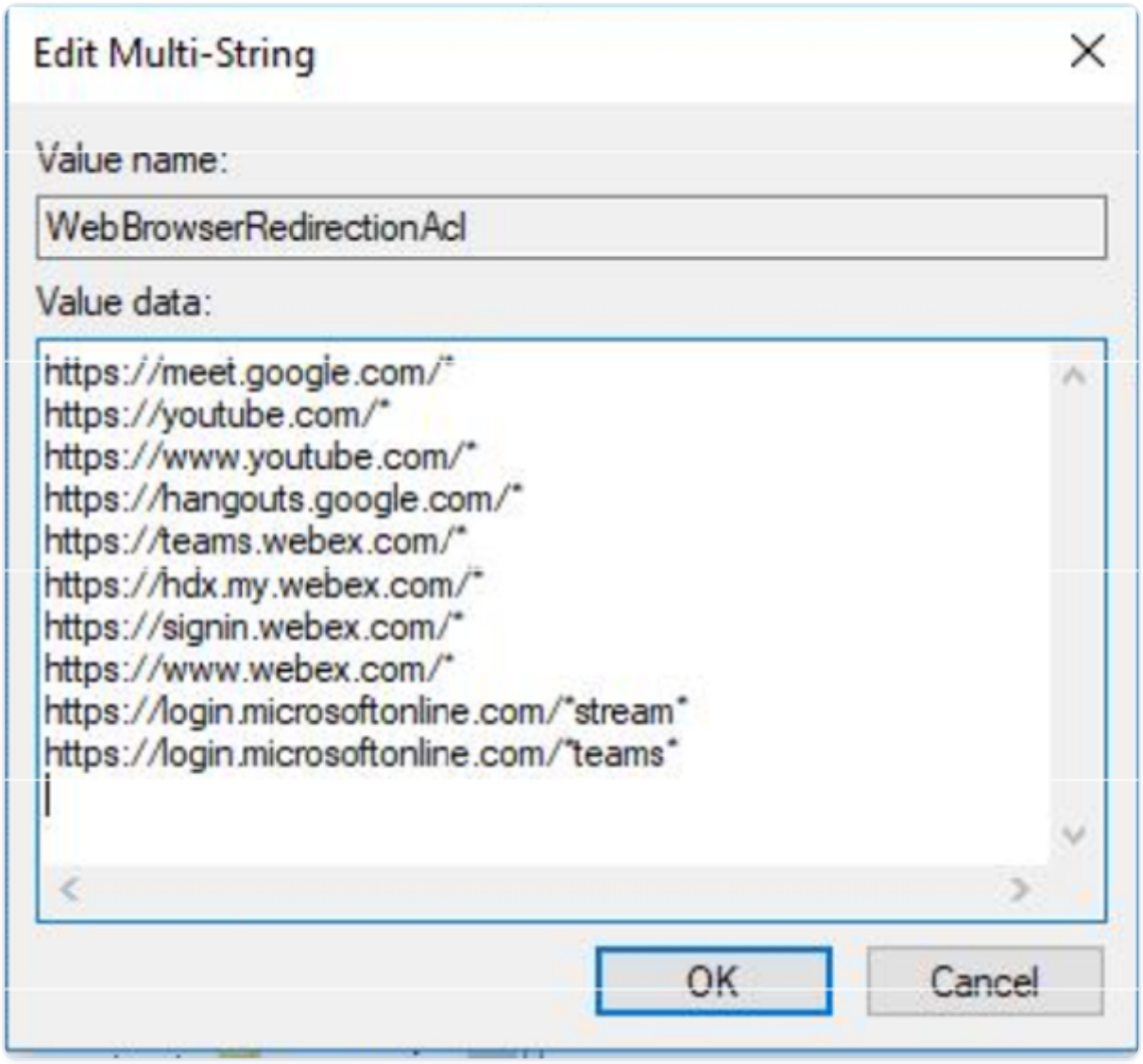
> **警告：**
>
> 不正确地编辑注册表可能导致严重问题，可能需要重新安装操作系统。Citrix 无法保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。编辑注册表之前，请务必备份注册表。

> 注册表覆盖策略设置选项：

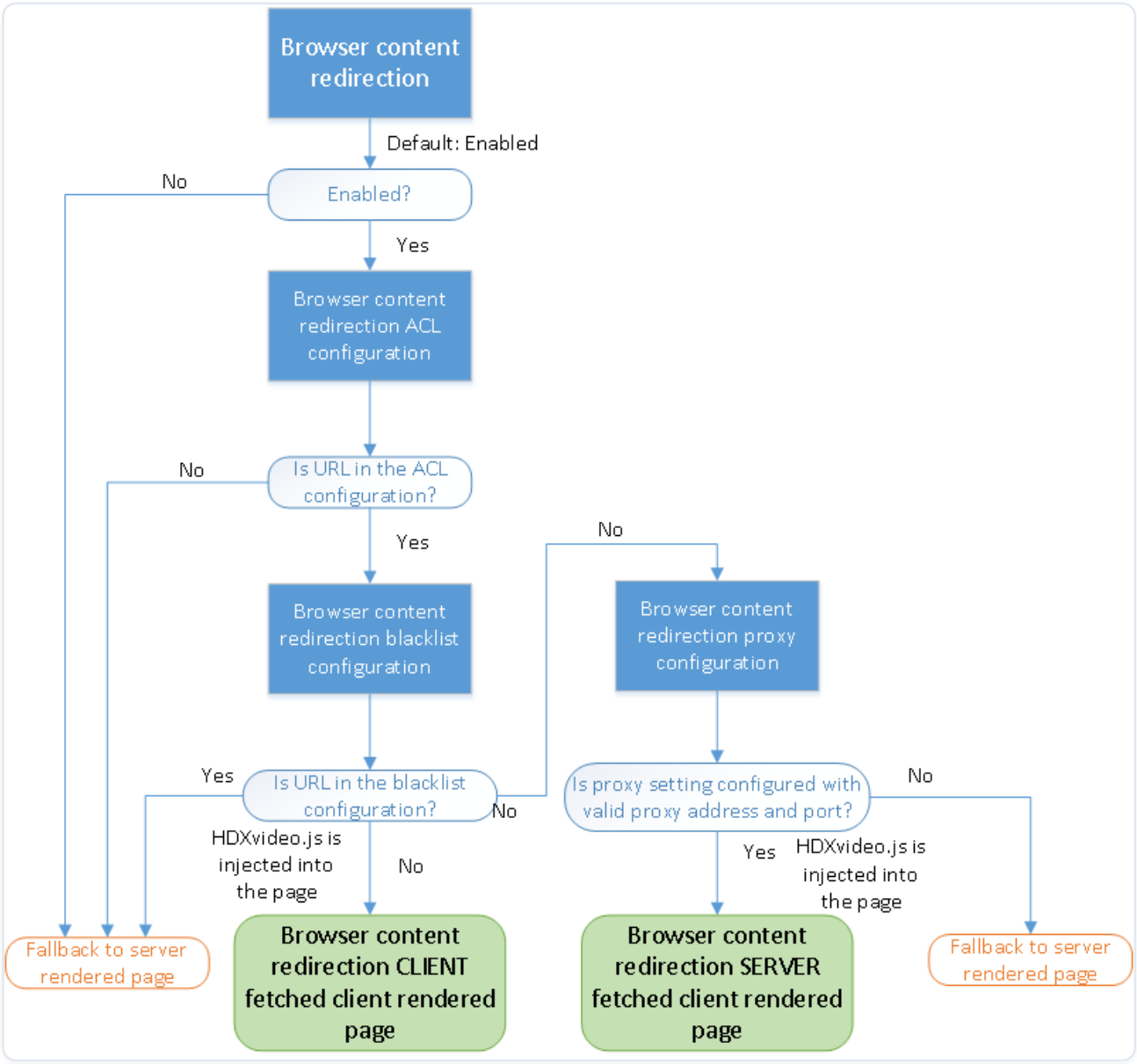
`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

| 名称 | 类型 | 值 |
| --- | --- | --- |
| WebBrowserRedirection | DWORD | 1=允许，0=禁止 |
| WebBrowserRedirectionAcl | REG_MULTI_SZ | |

| 名称 | 类型 | 值 |
| --- | --- | --- |
| WebBrowserRedirectionAuthenticationSites | REG_MULTI_SZ | |
| WebBrowserRedirectionProxyAddress | REG_SZ | `http://myproxy.citrix.com:8080` 或 `http://10.10.10.10:8888` |
| WebBrowserRedirectionBlacklist | REG_MULTI_SZ | |



### 用于浏览器内容重定向的 HDXVideo.js 插入




HdxVideo.js 通过浏览器内容重定向 Chrome 扩展程序或 Internet Explorer 浏览器帮助程序对象 (BHO) 注入到网页中。BHO 是 Internet Explorer 的一种插件模型。它为浏览器 API 提供挂钩，并允许插件访问页面的文档对象模型 (DOM) 以控制导航。

BHO 决定是否在给定页面上注入 HdxVideo.js。该决定基于上一个流程图中所示的管理策略。

在决定注入 JavaScript 并将浏览器内容重定向到客户端后，VDA 上的 Internet Explorer 浏览器中的网页将为空白。将 **document.body.innerHTML** 设置为空会移除 VDA 上网页的整个正文。该页面已准备好发送到客户端，以便在客户端上的覆盖浏览器 (Hdxbrowser.exe) 中显示。

### 客户端传感器策略设置

**客户端传感器**部分包含策略设置，用于控制在用户会话中如何处理移动设备传感器信息。

### 允许应用程序使用客户端设备的物理位置

此设置确定在移动设备会话中运行的应用程序是否允许使用用户设备的物理位置。

默认情况下，禁止使用位置信息

当此设置被禁止时，应用程序尝试检索位置信息将返回“权限被拒绝”值。

当此设置被允许时，用户可以通过拒绝 Citrix Workspace™ 应用程序访问位置的请求来禁止使用位置信息。Android 和 iOS 设备会在每个会话中首次请求位置信息时进行提示。

在开发使用“允许应用程序使用客户端设备的物理位置”设置的托管应用程序时，请考虑以下事项：

- 确保支持位置功能的应用程序不依赖于位置信息的可用性，因为：
  - 用户可能不允许访问位置信息。
  - 在应用程序运行期间，位置可能不可用或可能发生变化。
  - 用户可能从不支持位置信息的不同设备连接到应用程序会话。
- 支持位置功能的应用程序必须：
  - 默认情况下关闭位置功能。
  - 在应用程序运行期间，向用户提供一个允许或禁止该功能的选项。
  - 为用户提供清除应用程序缓存的位置数据的选项。（Citrix Workspace 应用程序不缓存位置数据。）
- 启用位置功能的应用程序必须管理位置信息的粒度。这种管理可确保所获取的数据与应用程序的用途相符。此外，还应符合所有相关司法管辖区的法规。
- 使用位置服务时，强制实施安全连接（例如，使用 TLS 或 VPN）。将 Citrix Workspace 应用程序连接到受信任的服务器。
- 考虑就位置服务的使用征求法律意见。

## 桌面用户界面策略设置

“**桌面用户界面**”部分包含控制视觉效果（例如桌面壁纸、菜单动画和拖动图像）的策略设置。这些策略设置有助于管理客户端连接中使用的带宽。通过限制带宽使用，可以提高 WAN 上的应用程序性能。

> **重要提示：**

此版本不支持传统图形模式和桌面窗口管理器重定向 (DCR)。此策略仅在以下情况下用于向后兼容：

- XenApp 7.15 LTSR
- XenDesktop 7.15 LTSR
- 以前的 VDA 版本（与 Windows 7 和 Windows 2008 R2 配合使用）。

**桌面窗口管理器重定向**

此设置指定是否使用以下各项的处理能力进行本地 DirectX 图形渲染，以便为用户提供更流畅的 Windows 桌面体验：

- 用户设备上的图形处理单元 (GPU)
- 或者，
- 用户设备上的集成图形处理器 (IGP)

启用后，**桌面窗口管理器重定向**可提供高响应的 Windows 体验，同时保持服务器上的高可扩展性。

默认情况下，**桌面窗口管理器重定向**处于禁用状态。

要取消选择**桌面窗口管理器重定向**并减少用户会话中所需的带宽，请在将此设置添加到策略时选择**已禁用**。

**桌面窗口管理器重定向图形质量**

此设置指定用于桌面窗口管理器重定向的图形质量。

默认值为“高”。

从“高”、“中”、“低”或“无损”质量中选择。

**桌面壁纸**

此设置允许或阻止在用户会话中显示壁纸。

默认情况下，用户会话可以显示壁纸。

要取消选择桌面壁纸并减少用户会话所需的带宽，请在将此设置添加到策略时选择“**禁止**”。

**菜单动画**

此设置允许或阻止在用户会话中显示菜单动画。

默认情况下，允许菜单动画。

菜单动画是 Microsoft 个人偏好设置，旨在方便访问。启用后，它会导致菜单在短时间延迟后出现，可以通过滚动或淡入方式显示。菜单底部会出现一个箭头图标。当您指向该箭头时，菜单就会出现。

如果此策略设置设置为“**允许**”并且菜单动画 Microsoft 个人偏好设置已启用，则桌面会启用菜单动画。

> **注意：**
>
> 菜单动画 Microsoft 个人偏好设置的更改会影响桌面。请考虑将桌面设置为在会话结束时丢弃更改。在这种情况下，已启用菜单动画的用户在后续会话中可能没有菜单动画。对于需要菜单动画的用户，请在桌面的主映像中启用 Microsoft 设置，或确保桌面保留用户更改。

#### 拖动时查看窗口内容

此设置允许或阻止在屏幕上拖动窗口时显示窗口内容。

默认情况下，允许查看窗口内容。

设置为 **允许** 时，拖动时整个窗口会随之移动。设置为 **禁止** 时，只有窗口轮廓会随之移动，直到您释放它。

### 最终用户监控策略设置

**最终用户监控**部分包含用于衡量会话流量的策略设置。

#### ICA® 往返计算

此设置确定是否对活动连接执行 ICA 往返计算。

默认情况下，已启用活动连接的计算。

默认情况下，每个 ICA 往返测量启动都会延迟。此延迟会持续到出现指示用户交互的某些流量为止。此延迟的长度可能不确定，旨在防止 ICA 往返测量成为 ICA 流量的唯一原因。

#### ICA 往返计算间隔

此设置指定执行 ICA 往返计算的频率（以秒为单位）。

默认情况下，每 15 秒计算一次 ICA 往返。

#### 空闲连接的 ICA 往返计算

此设置确定是否对空闲连接执行 ICA 往返计算。

默认情况下，不对空闲连接执行计算。

默认情况下，每个 ICA 往返测量启动都会延迟。此延迟会持续到出现指示用户交互的某些流量为止。此延迟的长度可能不确定，旨在防止 ICA 往返测量成为 ICA 流量的唯一原因。

### 增强桌面体验策略设置

增强桌面体验策略设置在服务器操作系统上运行会话，这些会话看起来像本地 Windows 7 桌面。

默认情况下，此设置是允许的。

如果虚拟桌面上存在带有 Windows 经典主题的用户配置文件，则此策略不会为该用户提供增强的桌面体验。假设一个用户使用 Windows 7 主题用户配置文件登录到运行 Windows Server 2012 的虚拟桌面。此外，此策略未配置或已禁用。在这种情况下，该用户会看到一条错误消息，指示无法应用主题。

在这两种情况下，重置用户配置文件都可以解决此问题。

如果您在具有活动用户会话的虚拟桌面上禁用此策略，则这些会话的界面在 Windows 7 和 Windows 经典桌面上会变得不一致。为避免这种不一致，请确保在更改此策略设置后重新启动虚拟桌面。然后删除虚拟桌面上的任何漫游配置文件。Citrix® 还建议删除虚拟桌面上的任何其他用户配置文件，以避免配置文件之间出现不一致。

假设您的环境中正在使用漫游用户配置文件。在这种情况下，请确保为所有共享配置文件的虚拟桌面启用或禁用增强桌面体验功能。

Citrix 不建议在运行服务器操作系统和客户端操作系统的虚拟桌面之间共享漫游配置文件。客户端和服务器操作系统的配置文件不同。在这两种类型之间共享漫游配置文件可能导致用户在两者之间移动时配置文件属性不一致。

## 文件重定向策略设置

“**文件重定向**”部分包含与客户端驱动器映射和客户端驱动器优化相关的策略设置。

### 自动连接客户端驱动器

此设置允许或阻止用户登录时自动连接客户端驱动器。

默认情况下，允许自动连接。

将此设置添加到策略时，请确保启用要自动连接的驱动器类型的设置。例如，要允许自动连接用户的 CD-ROM 驱动器，请配置此设置和“**客户端光驱**”设置。

以下策略设置相关：

- **客户端驱动器重定向**
- **客户端软盘驱动器**
- **客户端光驱**
- **客户端固定驱动器**
- **客户端网络驱动器**
- **客户端可移动驱动器**

**客户端驱动器重定向**

此设置启用或禁用用户设备上驱动器之间的文件重定向。

默认情况下，文件重定向已启用。

> **注意：**
>
> 客户端驱动器重定向策略设置不适用于使用通用 USB 重定向映射到会话的驱动器。
>
> 启用后，用户可以将文件保存到其所有客户端驱动器。禁用后，将阻止所有文件重定向。此配置适用于所有文件重定向设置，无论其状态如何。单独的文件重定向设置包括客户端软盘驱动器和客户端网络驱动器。

以下策略设置相关：

- **客户端软盘驱动器**
- **客户端光驱**
- **客户端固定驱动器**
- **客户端网络驱动器**
- **客户端可移动驱动器**

**客户端固定驱动器**

此设置允许或阻止用户访问或将文件保存到用户设备上的固定驱动器。

默认情况下，允许访问客户端固定驱动器。

将此设置添加到策略时，请确保“**客户端驱动器重定向**”设置存在并设置为“允许”。如果这些设置被禁用，则不会映射客户端固定驱动器，并且用户无法手动访问这些驱动器，无论“**客户端固定驱动器**”设置的状态如何。

配置“**自动连接客户端驱动器**”设置，以确保用户登录时自动连接固定驱动器。

**客户端软盘驱动器**

此设置允许或阻止用户访问或将文件保存到用户设备上的软盘驱动器。

默认情况下，允许访问客户端软盘驱动器。

将此设置添加到策略时，请确保“**客户端驱动器重定向**”设置存在并设置为“允许”。如果这些设置被禁用，客户端软盘驱动器将不会被映射，并且用户无法手动访问这些驱动器，无论“**客户端软盘驱动器**”设置的状态如何。

为确保用户登录时软盘驱动器自动连接，请配置“**自动连接客户端驱动器**”设置。

**客户端网络驱动器**

此设置允许或阻止用户通过用户设备访问文件并将其保存到网络（远程）驱动器。

默认情况下，允许访问客户端网络驱动器。

将此设置添加到策略时，请确保“**客户端驱动器重定向**”设置存在并设置为“允许”。如果这些设置被禁用，客户端网络驱动器将不会被映射，并且用户无法手动访问这些驱动器。无论“**客户端网络驱动器**”设置的状态如何，此配置都适用。

为确保用户登录时网络驱动器自动连接，请配置“**自动连接客户端驱动器**”设置。

**客户端光驱**

此设置允许或阻止用户访问文件或将其保存到以下位置：

- 用户设备上的 CD-ROM
- 用户设备上的 DVD-ROM
- 用户设备上的 BD-ROM 驱动器。

默认情况下，允许访问客户端光驱。

将此设置添加到策略时，请确保“**客户端驱动器重定向**”设置存在并设置为“**允许**”。如果这些设置被禁用，客户端光驱将不会被映射，并且用户无法手动访问这些驱动器。无论“**客户端光驱**”设置的状态如何，此配置都适用。

为确保用户登录时光驱自动连接，请配置“**自动连接客户端驱动器**”设置。

**客户端可移动驱动器**

此设置允许或阻止用户访问文件或将其保存到用户设备上的 USB 驱动器。

默认情况下，允许访问客户端可移动驱动器。

将此设置添加到策略时，请验证“**客户端驱动器重定向**”设置是否存在并设置为“允许”。如果这些设置被禁用，客户端可移动驱动器将不会被映射，并且用户无法手动访问这些驱动器。无论“**客户端可移动驱动器**”设置的状态如何，此配置都适用。

配置“**自动连接客户端驱动器**”设置，以确保用户登录时自动连接可移动驱动器。

#### 主机到客户端重定向

此设置启用或禁用文件类型关联，以便在用户设备上打开 URL 和某些媒体内容。禁用时，内容将在服务器上打开。

默认情况下，文件类型关联处于禁用状态。

启用此设置后，以下 URL 类型将在本地打开：

- HTTP
- HTTPS
- 瑞尔播放器 和 QuickTime (RTSP)
- 瑞尔播放器 和 QuickTime (RTSPU)
- 旧版 Real Player (PNM)
- 微软媒体服务器 (MMS)

#### 保留客户端驱动器盘符

此设置启用或禁用客户端驱动器映射到会话中的相同驱动器盘符。

默认情况下，不保留客户端驱动器盘符。

将此设置添加到策略时，请确保“**客户端驱动器重定向**”设置存在并设置为“允许”。

#### 只读客户端驱动器访问

此设置允许或阻止用户和应用程序执行以下操作：

- 在映射的客户端驱动器上创建文件
- 更改映射客户端驱动器上的文件
- 更改映射客户端驱动器上的文件夹

默认情况下，可以更改映射客户端驱动器上的文件和文件夹。

如果设置为“已启用”，则文件和文件夹将以只读权限访问。

将此设置添加到策略时，请确保存在**客户端驱动器重定向**设置并将其设置为“允许”。

#### 特殊文件夹重定向

此设置允许或阻止 Citrix Workspace™ 应用程序和 Web Interface 用户从会话中查看其本地“文档”和“桌面”特殊文件夹。

默认情况下，允许特殊文件夹重定向。

此设置可防止通过策略筛选的任何对象进行特殊文件夹重定向，无论其他位置存在的设置如何。当此设置被禁止时，为 StoreFront™、Web Interface 或 Citrix Workspace 应用程序指定的任何相关设置都将被忽略。

要定义哪些用户可以进行特殊文件夹重定向，请选择“**允许**”，并将此设置包含在针对您希望拥有此功能的用户进行筛选的策略中。此设置将覆盖所有其他特殊文件夹重定向设置。

阻止用户访问或将文件保存到其本地硬盘驱动器的策略设置也会阻止特殊文件夹重定向工作。出现这种情况是因为特殊文件夹重定向必须与用户设备进行交互。

将此设置添加到策略时，请确保存在**客户端固定驱动器**设置并将其设置为“允许”。

#### 使用异步写入

此设置启用或禁用异步磁盘写入。

默认情况下，异步写入处于禁用状态。

异步磁盘写入可以提高通过 WAN 进行文件传输和写入客户端磁盘的速度，WAN 通常具有相对较高的带宽和高延迟。但是，如果出现连接或磁盘故障，正在写入的客户端文件可能会处于未定义状态。如果出现此未定义状态，将弹出一个窗口通知用户受影响的文件。然后，用户可以采取补救措施，例如在重新连接时或磁盘故障得到纠正时重新启动中断的文件传输。

Citrix® 建议仅对需要远程连接且具有良好文件访问速度的用户启用异步磁盘写入。并且这些用户在连接或磁盘故障时可以轻松恢复丢失的文件或数据。

将此设置添加到策略时，请验证是否存在 **客户端驱动器重定向** 设置并将其设置为“允许”。如果此设置被禁用，则不会发生异步写入。

### 图形策略设置

“**图形**”部分包含用于控制用户会话中图像处理方式的策略设置。

#### 允许视觉无损压缩

此设置允许对图形使用视觉无损压缩，而不是真正的无损压缩。视觉无损压缩比真正的无损压缩能提高性能，但会产生肉眼无法察觉的轻微损失。此设置会更改“视觉质量”设置值的使用方式。

默认情况下，此设置为禁用状态。

### 图形状态指示器

此设置将图形状态指示器配置为在用户会话中运行。此工具允许用户查看有关活动图形模式的信息。该信息包括视频编解码器、硬件编码、图像质量以及会话中使用的显示器等详细信息。借助图形状态指示器，用户还可以启用或禁用像素完美模式。

Citrix Virtual Apps and Desktops™ 2103 及更高版本包含一个图像质量滑块，可帮助用户在图像质量和交互性之间找到适当的平衡。

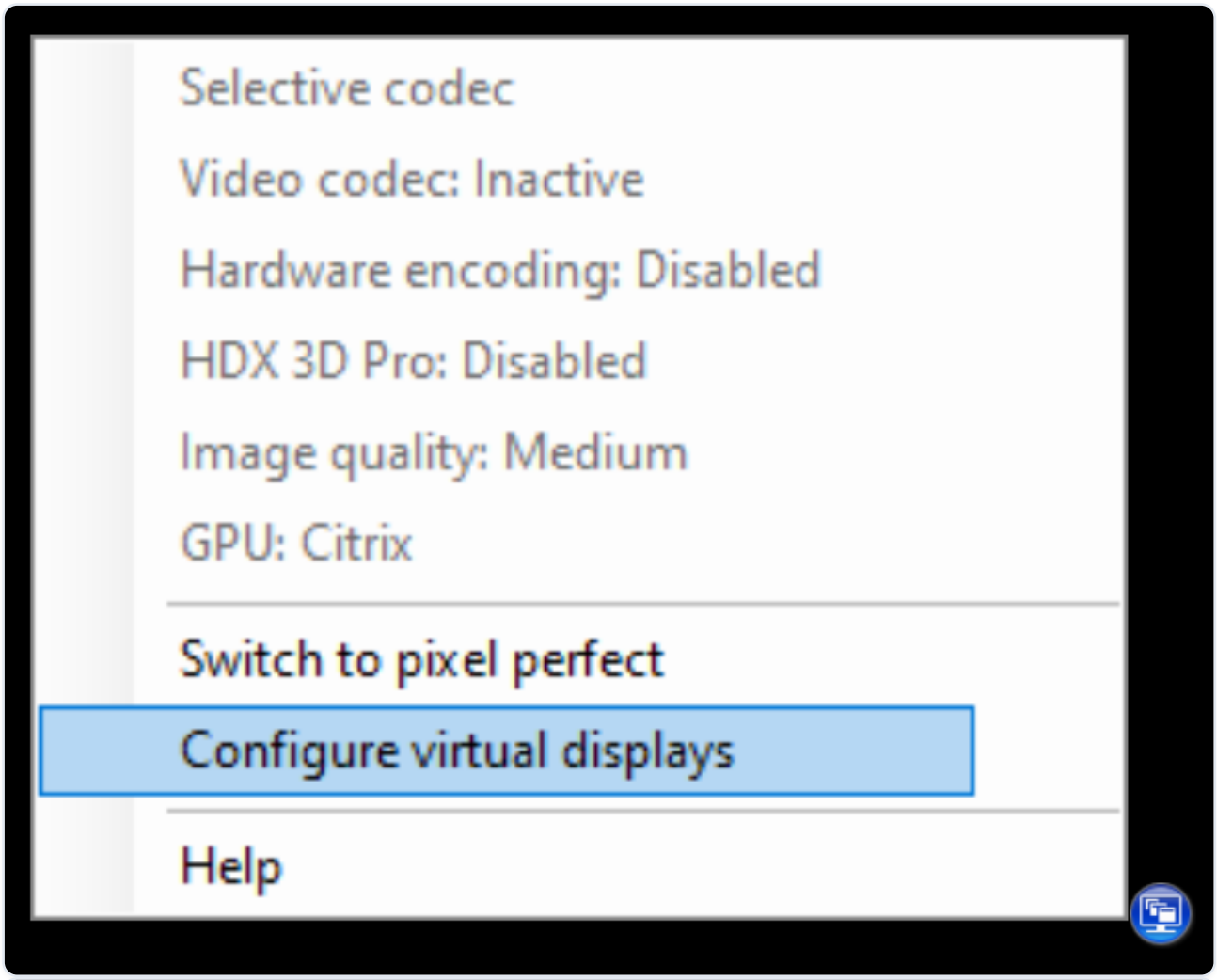
Citrix Virtual Apps and Desktops 2109 及更高版本包含通过使用图形状态指示器启动的用户界面配置虚拟显示布局的功能。

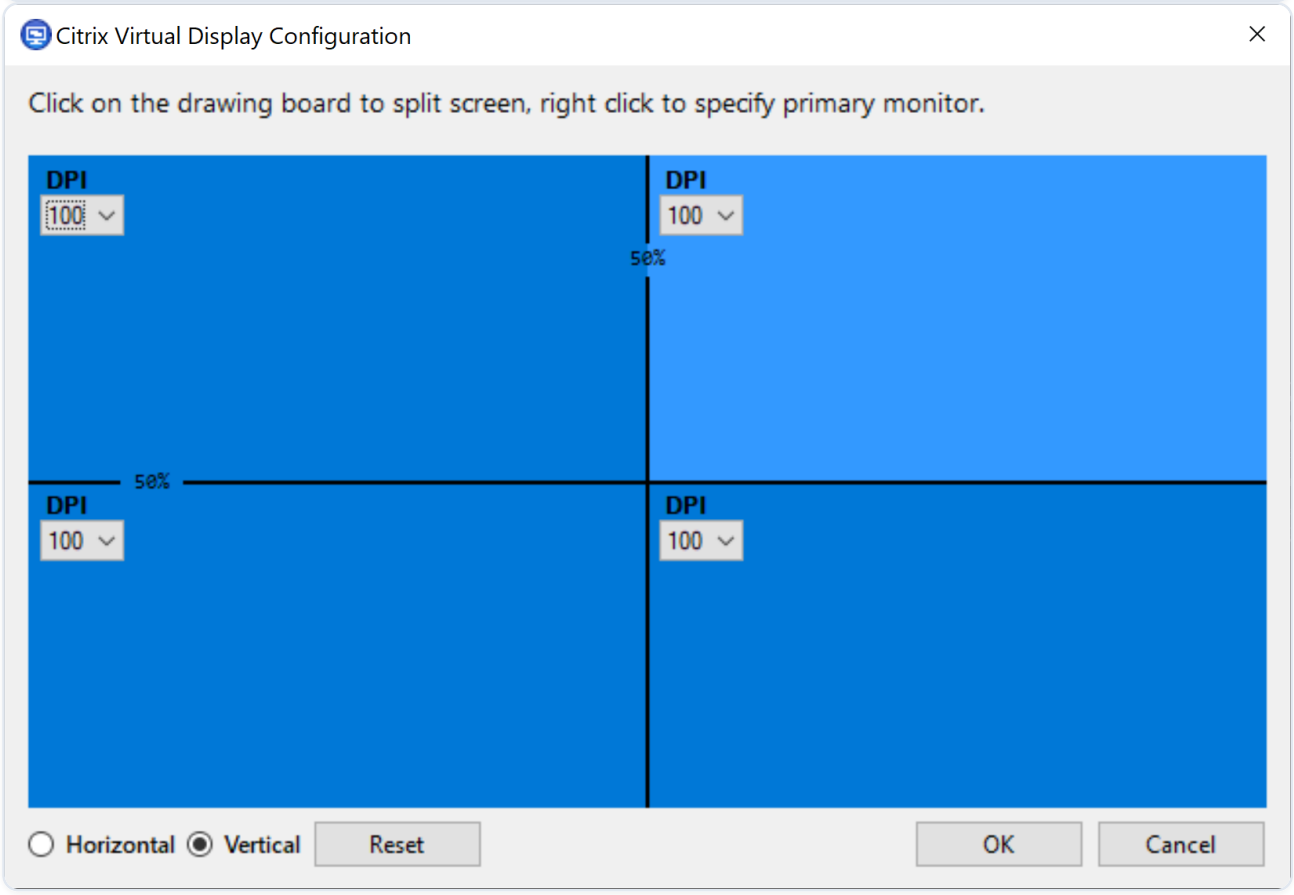
图形状态指示器取代了早期版本中的无损指示器工具。此策略为 Citrix Virtual Apps and Desktops 7.16 到 1809 版本启用了无损指示器。

### 虚拟显示布局

虚拟显示布局功能已是 Citrix Workspace™ app for Windows 的一部分，现在也已成为 VDA 的一部分。此功能允许您在实时会话中在 VDA 上定义虚拟显示器布局，并将会话显示器虚拟拆分为远程桌面上的最多八个虚拟显示器。您可以通过右键单击图形状态指示器图标并选择“**配置虚拟显示器**”选项来配置虚拟显示器，该选项将启动虚拟显示器配置 UI。在那里，您可以绘制水平或垂直线以将屏幕分成虚拟显示器。在 UI 上右键单击虚拟显示器会将其标记为主显示器。屏幕根据会话显示器分辨率的指定百分比进行拆分。您还可以为虚拟显示器设置 DPI。

定义虚拟显示器布局后，单击“**确定**”会立即应用虚拟显示布局。“**取消**”会关闭 UI，并放弃所有更改。


Selective codec
Video codec: Inactive
Hardware encoding: Disabled
HDX 3D Pro: Disabled
Image quality: Medium
GPU: Citrix
Switch to pixel perfect
Configure virtual displays
Help


Citrix Virtual Display Configuration
Click on the drawing board to split screen, right click to specify primary monitor.
DPI
100
DPI
100
50%
50%
DPI
100
DPI
100
Horizontal
Vertical
Reset
OK
Cancel

此配置仅适用于桌面会话，不影响任何已发布的应用程序。在多显示器场景中，如果虚拟显示器总数不超过支持的最大值八个虚拟显示器，则相同的配置的虚拟显示布局将应用于所有会话显示器。如果超出此限制，则虚拟显示布局将被忽略，并且不应用于任何会话显示器。

定义的虚拟显示配置按用户和客户端设备存储。此配置适用于特定用户从给定客户端进行的所有后续连接。它在会话大小调整、会话断开连接/重新连接以及会话注销/登录后仍然保留。

请勿将此功能与 Citrix Workspace 应用程序中现有的虚拟显示功能同时使用。

**屏幕共享**

此设置允许用户与其他用户共享其会话，包括屏幕内容、键盘和鼠标。

默认情况下，此设置为禁用状态。

VDA 尝试使用 TCP 端口范围内的端口来交换数据，从最低端口开始，并在每个后续连接上递增。该端口处理入站和出站流量。

默认情况下，TCP 端口范围设置为 52525-52625。

用于屏幕共享的端口必须添加到防火墙例外列表中。在安装 VDA 时，此选项显示为一个复选框。默认情况下，此选项未选中。

**显示内存限制**

此设置指定会话的最大视频缓冲区大小（以千字节为单位）。

默认情况下，显示内存限制为 65,536 千字节。

指定会话的最大视频缓冲区大小（以千字节为单位）。指定 128 到 4,194,303 之间的千字节数。最大值 4,194,303 不限制显示内存。默认情况下，显示内存为 65,536 千字节。连接使用更高的颜色深度和更高的分辨率需要更多的内存。在旧版图形模式下，如果达到内存限制，显示将根据“显示模式降级首选项”设置进行降级。

对于需要更高颜色深度和更高分辨率的连接，请增加此限制。使用以下公式计算所需的最大内存：

内存深度（字节）=（每像素位数颜色深度 / 8）x（垂直分辨率（像素））x（水平分辨率（像素））。

例如，考虑一个颜色深度为 32、垂直分辨率为 600、水平分辨率为 800 的场景。在这种情况下，所需的最大内存为 (32 / 8) x (600) x (800) = 1920000 字节，这会产生 1920 KB 的显示内存限制。

只有在启用旧版图形模式策略设置时，才可以使用 32 位以外的颜色深度。

HDX™ 仅为每个会话分配所需的显示内存量。因此，如果只有部分用户需要超出默认值，则增加显示内存限制不会对可伸缩性产生负面影响。

### 显示模式降级首选项

> **注意：**
>
> 对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。
>
> 当达到会话显示内存限制时，此设置指定是先降级颜色深度还是分辨率。

默认情况下，颜色深度会首先降级。

当达到会话内存限制时，您可以降低显示图像的质量。您可以通过选择是先降级颜色深度还是分辨率来降低此质量。当颜色深度首先降级时，显示图像使用的颜色会减少。当分辨率首先降级时，显示图像每英寸使用的像素会减少。

要在颜色深度或分辨率降级时通知用户，请配置“在显示模式降级时通知用户”设置。

### 动态窗口预览

此设置启用或禁用以下情况下的无缝窗口显示：

- 翻转-
- 三维翻转
- 任务栏预览
- Windows 预览

| WINDOWS AERO 预览选项 | 描述 |
| --- | --- |
| 任务栏预览 | 当用户将鼠标悬停在窗口的任务栏图标上时，该窗口的图像会显示在任务栏上方。 |
| Windows 预览 | 当用户将鼠标悬停在任务栏预览图像上时，窗口的全尺寸图像会显示在屏幕上。 |
| 翻转 | 当用户按下 ALT+TAB 时，每个打开的窗口都会显示小的预览图标。 |
| 三维翻转 | 当用户按下 TAB+Windows 徽标键时，打开窗口的大图像会在屏幕上层叠显示。 |

默认情况下，此设置处于启用状态。

**图像缓存**

> **注意：**

> 对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

> 此设置启用或禁用会话中图像部分的缓存和检索。按部分缓存图像并在需要时检索这些部分可实现以下目的：

- 用户设备上的滚动更流畅
- 减少用户设备上通过网络传输的数据量
- 减少用户设备所需的处理量

默认情况下，图像缓存设置处于启用状态。

> **注意：**

> 图像缓存设置控制图像的缓存和检索方式。此设置不控制图像是否缓存。如果启用了旧版图形模式设置，则会缓存图像。

**旧版图形模式 - 不受支持。仅用于向后兼容**

> **重要提示：**

> 此版本不支持旧版图形模式和桌面组合重定向 (DCR)。此策略仅用于在使用 XenApp 7.15 LTSR、XenDesktop 7.15 LTSR 以及早期 VDA 版本（与 Windows 7 和 Windows 2008 R2 结合使用）时的向后兼容性。

> 此设置会禁用富图形体验。使用此设置可恢复到旧版图形体验，从而减少通过 WAN 或移动连接的带宽消耗。XenApp 和 XenDesktop 7.13 中引入的带宽减少功能使此模式变得过时。

默认情况下，此设置处于禁用状态，用户将获得富图形体验。

旧版图形模式支持以下各项：

- Windows 7 系统
- Windows Server 2008 R2 虚拟投递代理。

旧版图形模式不支持以下各项：

- Windows 8.x 和 10 版本
- Windows Server 2012、2012 R2 和 2016 版本。

有关在 XenApp 和 XenDesktop 7.6 FP3 或更高版本中优化图形模式和策略的更多信息，请参阅 CTX202687。

**最大允许颜色深度**

> **注意：**
>
> 对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

> 此设置指定会话允许的最大颜色深度。

默认情况下，最大允许颜色深度为每像素 32 位。

此设置仅适用于 Thinwire 驱动程序和连接。它不适用于将非 ThinWire 驱动程序用作主显示驱动程序的 VDA。这些 VDA 是使用 Windows 显示驱动程序模型 (WDDM) 驱动程序作为主显示驱动程序的 VDA。对于使用 WDDM 驱动程序作为主显示驱动程序的单会话操作系统 VDA（例如 Windows 8），此设置无效。对于使用 WDDM 驱动程序的 Windows 多会话操作系统 VDA（例如 Windows Server 2012 R2），此设置可能会阻止用户连接到 VDA。

设置高颜色深度需要更多内存。要在达到内存限制时降低颜色深度，请配置**显示模式降级首选项**设置。当颜色深度降级时，显示的图像会使用较少的颜色。

**显示模式降级时通知用户**

> **注意：**
>
> 对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

> 当颜色深度或分辨率降级时，此设置会向用户显示简要说明。

默认情况下，禁用通知用户。

### 优化 3D 图形工作负载

此设置配置最适合图形密集型工作负载的相应默认设置。为工作负载侧重于图形密集型应用程序的用户启用此设置。仅当会话可用 GPU 时才应用此策略。任何明确覆盖此策略设置的默认设置的其他设置都将优先。

默认情况下，禁用优化 3D 图形工作负载。

### 排队和丢弃

> **注意：**
>
> 对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

> 此设置会丢弃被其他图像替换的排队图像。

默认情况下，排队和丢弃功能已启用。

此设置可在图形发送到用户设备时提高响应速度。配置此设置可能会导致动画因丢帧而变得卡顿。

### 使用视频编解码器进行压缩

允许在端点上提供视频解码时使用视频编解码器压缩图形。选择“**针对整个屏幕**”时，视频编解码器将作为所有内容的默认编解码器应用。选择“**针对活动变化区域**”时，视频编解码器将用于屏幕上不断变化的区域，其他数据则使用静态图像压缩和位图缓存。当端点上没有视频解码功能，或者指定“**不使用视频编解码器**”时，将使用静态图像压缩和位图缓存的组合。选择“**在首选时使用**”时，系统会根据各种因素进行选择。随着选择方法的增强，结果可能会因版本而异。

选择“**在首选时使用**”以允许系统尽力为当前场景选择适当的设置。

选择“**针对整个屏幕**”以优化用户体验和带宽，尤其是在大量使用服务器渲染的视频和 3D 图形的情况下。

选择“**针对活动变化区域**”以优化视频性能，尤其是在低带宽环境下，同时保持静态和缓慢变化内容的扩展性。多显示器部署支持此设置。

选择“**不使用视频编解码器**”以优化服务器 CPU 负载，并适用于没有大量服务器渲染视频或其他图形密集型应用程序的情况。

默认值为“**在首选时使用**”。

**对视频使用硬件编码**

此设置允许在可用时使用图形硬件，通过视频编解码器压缩屏幕元素。如果此类硬件不可用，VDA 将回退到使用软件视频编解码器的基于 CPU 的编码。

此策略设置的默认选项为“**已启用**”。

支持多显示器。

任何支持视频解码的 Citrix Workspace 应用程序都可以与硬件编码配合使用。

#### NVIDIA

对于 NVIDIA GRID GPU，多会话操作系统和单会话操作系统的 VDA 支持硬件编码。

NVIDIA GPU 必须支持 NVENC 硬件编码。有关支持的 GPU 列表，请参阅 NVIDIA 视频编解码器 SDK。

NVIDIA GRID 需要驱动程序版本 3.1 或更高版本。NVIDIA Quadro 需要驱动程序版本 362.56 或更高版本。Citrix 建议使用 NVIDIA Release R361 分支中的驱动程序。

无损文本与 NVENC 硬件编码不兼容。如果启用了无损文本，则无损文本优先于 NVENC 硬件编码。

支持对活动更改区域选择性使用 H.264 硬件编解码器。

支持视觉无损 (YUV 4:4:4) 压缩。视觉无损（图形策略设置，允许视觉无损压缩）需要 Citrix Workspace 应用程序 1808 或更高版本，或者 Citrix Receiver for Windows 4.5 或更高版本。

#### 英特尔

对于 Intel Iris Pro 图形处理器，单会话操作系统和多会话操作系统的 VDA 支持硬件编码。

支持 Intel Broadwell 处理器系列 及更高版本中的 Intel Iris Pro 图形处理器。需要 Intel Remote Displays SDK 1.0 版，可从英特尔网站下载：Remote Displays SDK。

仅当视频编解码器策略设置为整个屏幕且**优化 3D 图形工作负载**策略被禁用时，才支持无损文本。

不支持视觉无损 (YUV 4:4:4)。

英特尔编码器可为最多八个编码会话提供良好的用户体验（例如，一个用户使用八个显示器，或八个用户各使用一个显示器）。如果需要超过八个编码会话，请检查虚拟机连接了多少个显示器。管理员决定按用户或按计算机配置此策略设置，以保持良好的用户体验。

#### AMD

对于 AMD，单会话操作系统的 VDA 支持硬件编码。

AMD GPU 必须支持 RapidFire SDK。例如，AMD Radeon Pro 或 FirePro GPU。

要使编码正常工作，请安装最新的 AMD 驱动程序。您可以从 `<https://www.amd.com/en/support>` 下载这些驱动程序。

无损文本与 AMD 硬件编码不兼容。如果启用了无损文本，则无损文本优先于 AMD 硬件编码。

支持选择性使用 H.264 硬件编解码器处理活动变化的区域。

### 缓存策略设置

本节包含在客户端连接带宽受限时，在用户设备上启用图像数据缓存的策略设置。

#### 持久缓存阈值

**注意：** 对于 Virtual Delivery Agent 7.x，此策略设置仅在启用**旧版图形模式**策略设置时适用。

此设置将位图缓存到用户设备的硬盘上，从而可以重复使用以前会话中的大型常用图像。

默认情况下，阈值为每秒 3000000 位。

阈值表示低于此值时持久缓存功能生效。例如，使用默认值时，当带宽低于 3000000 bps 时，位图将缓存到用户设备的硬盘上。

### Framehawk 策略设置

> **重要提示：**
>
> 自 Citrix Virtual Apps and Desktops 7 1903 起，不再支持 Framehawk。请改用已启用(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/technical-overview/hdx/adaptive-transport.html)的 Thinwire。
>
> **Framehawk** 部分包含用于在服务器上启用和配置 Framehawk 显示通道的策略设置。

#### FRAMEHAWK 显示通道

启用后，服务器会尝试使用 Framehawk 显示通道进行用户图形和输入远程处理。该显示通道使用 UDP，可在具有高丢包率和高延迟的网络上提供更好的用户体验。但是，它也可能比其他图形模式占用更多的服务器资源和带宽。

默认情况下，Framehawk 显示通道处于禁用状态。

#### FRAMEHAWK 显示通道端口范围

此策略设置指定 VDA 用于与用户设备交换 Framehawk 显示通道数据的 UDP 端口号范围。端口号的形式为 *最低端口号或最高端口号*。VDA 会尝试使用每个端口，从最低端口号开始，并在每次后续尝试时递增。该端口处理入站和出站流量。

默认情况下，端口范围为 3224,3324。

### 本地应用访问策略设置

**本地应用访问**部分包含策略设置，用于管理用户的本地安装应用程序与托管应用程序的集成。这些策略设置管理托管桌面环境中的集成。

#### 允许本地应用访问

此设置允许或阻止用户的本地安装应用程序与托管应用程序的集成。这些策略设置管理托管桌面环境中的集成。

当用户启动本地安装的应用程序时，该应用程序似乎在其虚拟桌面中运行，即使它实际上是在本地运行。

如果您将**允许本地应用访问**策略设置设为**已启用**，则不支持浏览器内容重定向，并且客户端通知区域电池状态不会显示在桌面会话中。

默认情况下，**允许本地应用访问**被禁止。

#### URL 重定向阻止列表

此设置指定将重定向到本地 Web 浏览器并在其中启动的网站。这些网站可能包括以下内容：

- 需要区域设置信息的网站，例如 msn.com 或 newsgoogle.com
- 或者
- 包含富媒体内容的网站，在用户设备上呈现效果更好。

默认情况下，未指定任何站点。

#### URL 重定向允许列表

此设置指定将在其启动的环境中呈现的网站。

默认情况下，未指定任何站点。

### 移动体验策略设置

**移动体验**部分包含用于处理 Citrix Mobility Pack 的策略设置。

#### 自动键盘显示

此设置启用或禁用在移动设备屏幕上自动显示键盘。

默认情况下，自动显示键盘处于禁用状态。

#### 启动触摸优化桌面

此设置已禁用，不适用于 Windows 10 或 Windows Server 2016 计算机。

此设置决定了 Citrix Workspace™ 应用程序的整体界面行为。此设置允许或禁止使用针对平板电脑设备优化的触摸友好界面。

默认情况下，使用触摸友好界面。

要仅使用 Windows 界面，请将此策略设置设为“禁止”。

#### 远程组合框

此设置确定可在移动设备会话中显示的组合框类型。将此策略设置设为“允许”以显示设备原生的组合框控件。当此设置被允许时，用户可以更改适用于 iOS 的 Citrix Workspace 应用程序会话设置以使用 Windows 组合框。

默认情况下，**远程组合框**功能处于禁用状态。

### 多媒体策略设置

“**多媒体**”部分包含用于管理用户会话中流式 HTML5 和 Windows 音频和视频的策略设置。

> **警告**
>
> 不正确地编辑注册表可能会导致严重问题，可能需要您重新安装操作系统。Citrix® 无法保证可以解决因不正确使用注册表编辑器而导致的问题。使用注册表编辑器风险自负。编辑注册表之前，请务必备份注册表。

#### 多媒体策略

默认情况下，在 Delivery Controller™ 上设置的所有多媒体策略都存储在以下注册表中：

计算机策略：

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

用户策略：

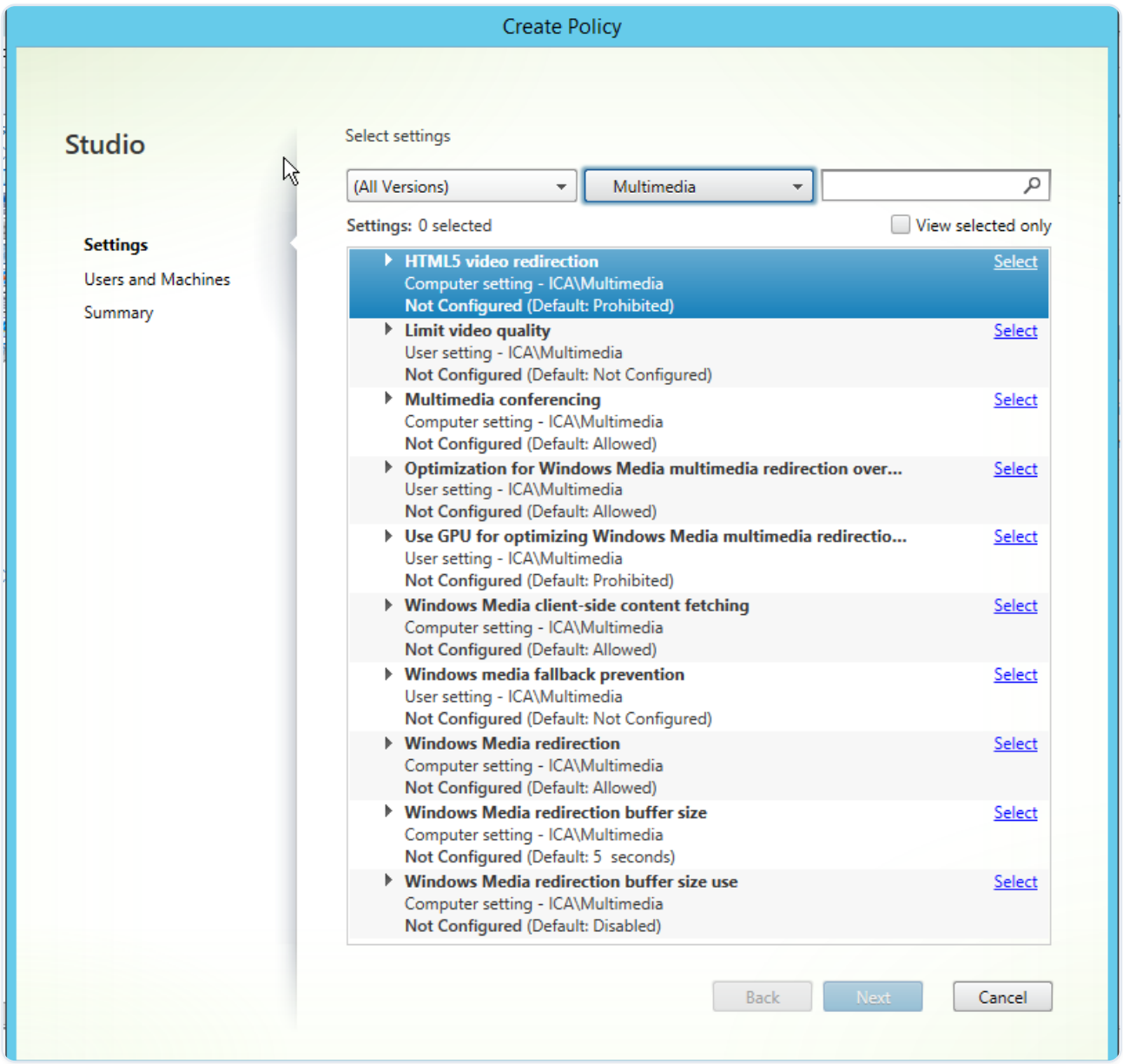
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{用户会话ID}\User\MultimediaPolicies

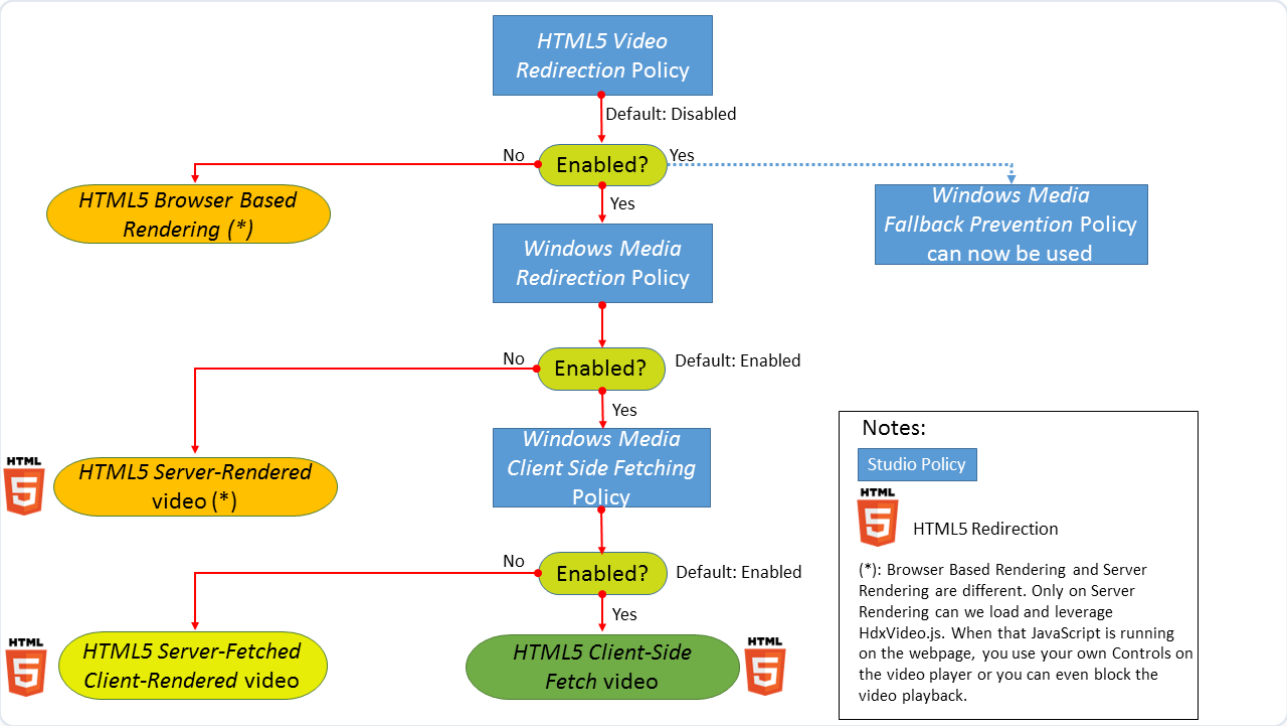
要查找当前用户会话 ID，请在 Windows 命令行中发出 **qwinsta** 命令。

### HTML5 视频重定向

控制并优化 Citrix Virtual Apps and Desktops™ 服务器向用户交付 HTML5 多媒体 Web 内容的方式。

默认情况下，此设置为禁用状态。






在此版本中，此功能仅适用于受控网页。它要求将 JavaScript 添加到提供 HTML5 多媒体内容的网页中，例如，内部培训站点上的视频。

要配置 HTML5 视频重定向：

1. 将文件 **HdxVideo.js** 从 VDA 安装的 %Program Files%/Citrix/ICA Service/HTML5 Video Redirection 复制到内部网页的位置。
2. 将此行插入到您的网页中（如果您的网页有其他脚本，请在这些脚本之前包含 **HdxVideo.js**）：

   ```
   <script src="HdxVideo.js" type="text/javascript"\></script>
   ```

**注意**：如果 HdxVideo.js 不在您的网页的同一位置，请使用 **src** 属性指定其完整路径。

假设 JavaScript 未添加到您控制的网页中，并且用户播放 HTML5 视频。在这种情况下，Citrix Virtual Apps and Desktops 默认使用服务器端渲染。

要使 HTML5 视频重定向正常工作，请允许 ***Windows Media Redirection***。此策略对于服务器提取客户端渲染是强制性的，对于客户端提取是必需的。客户端提取反过来也要求允许*Windows Media 客户端内容提取*。

Microsoft Edge 不支持此功能。

HdxVideo.js 会将其自己的控件替换浏览器 HTML5 播放器控件。要检查 HTML5 视频重定向策略是否在某个网站上生效，请将播放器控件与 **HTML5 视频重定向**策略被禁止的场景进行比较：

（策略允许时为 Citrix 自定义控件）



（策略被禁止或未配置时为本机网页控件）




支持以下视频控件：

- 播放
- 暂停
- 查找
- 重复
- 音频
- 全屏

您可以查看一个 HTML5 视频重定向测试页面。

#### TLS、HTML5 视频重定向和浏览器内容重定向

您可以使用 HTML5 视频重定向来：

- 重定向来自 HTTPS 网站的视频
- 或者
- 浏览器内容重定向以重定向整个网站

注入到这些网站中的 JavaScript 必须与在 VDA 上运行的 Citrix HDX HTML5 视频重定向服务 (WebSocketService.exe) 建立 TLS 连接。VDA 上的证书存储中的 Citrix HDX HTML5 视频重定向服务会生成两个自定义证书，用于：

- 实现视频重定向
- 维护网页的 TLS 完整性

HdxVideo.js 使用 Secure WebSockets 与在 VDA 上运行的 WebSocketService.exe 进行通信。此进程以 Local System account 运行，并执行 SSL termination 和 user session mapping。

WebSocketService.exe 正在侦听 127.0.0.1 端口 9001。

#### 限制视频质量

此设置仅适用于 Windows Media，不适用于 HTML5。它要求您启用 **Optimization for Windows Media multimedia redirection over WAN**。

此设置指定 HDX™ 连接允许的最大视频质量级别。配置后，最大视频质量将限制为指定值，从而确保在环境中保持多媒体服务质量 (QoS)。

默认情况下，此设置未配置。

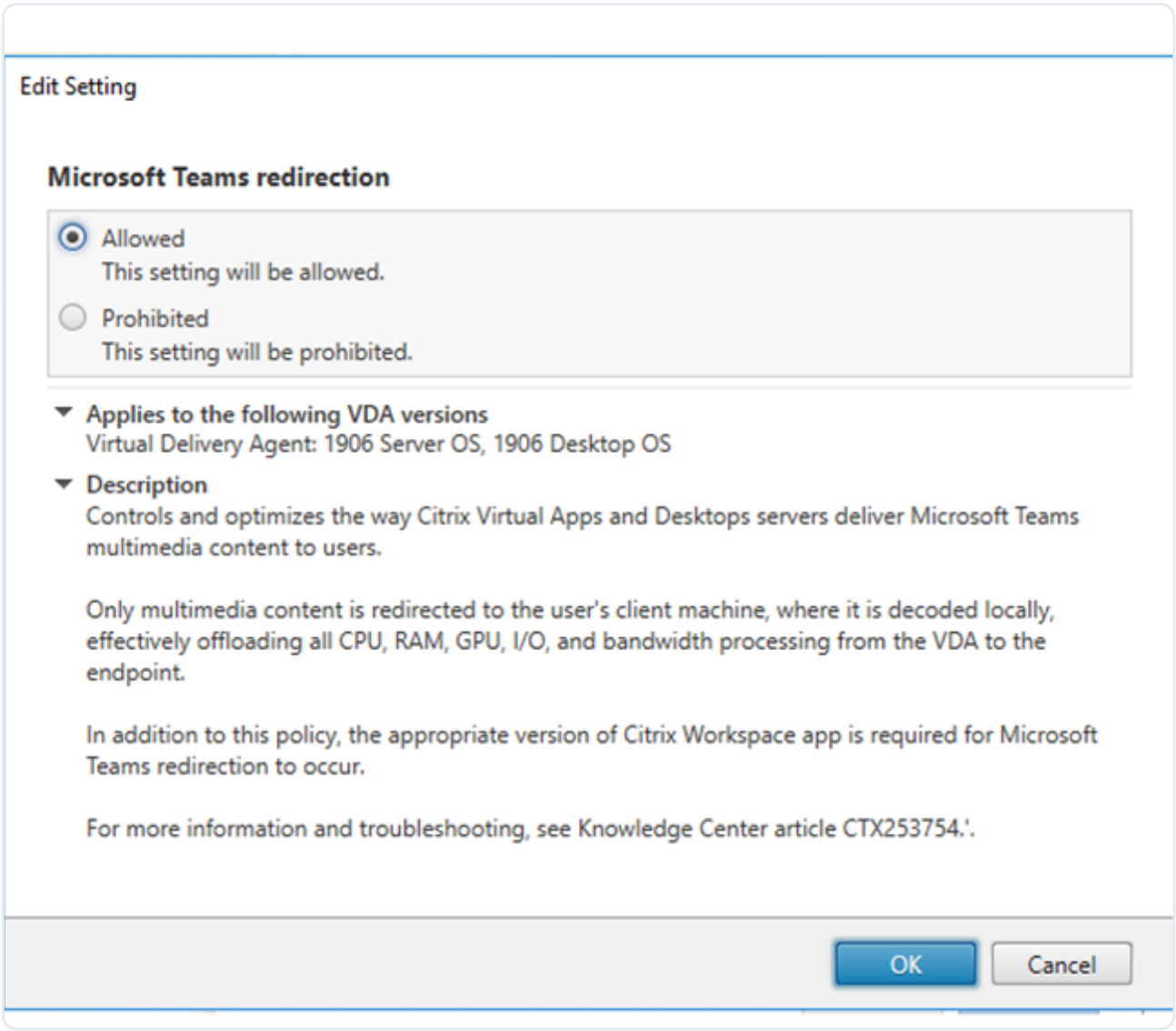
要限制允许的最大视频质量级别，请选择以下选项之一：

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

在同一服务器上同时播放多个视频会消耗大量资源，并可能影响服务器的可伸缩性。

**Microsoft Teams 重定向**

此设置基于 HDX 技术启用 Microsoft Teams 优化。




如果启用此策略，并且您使用的是受支持的 Citrix Workspace™ 应用程序版本，则此注册表项在 VDA 上设置为 **1**。Microsoft Teams 应用程序读取此项以在 VDI 模式下加载。 请注意，无需手动设置注册表项。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

名称: MSTeamsRedirSupport

值: DWORD (1 - 开，0 - 关)

> **注意：**
>
> 假设您正在使用版本 1906.2 或更高版本的 VDA，以及没有在 Studio 中提供此策略的旧版本 Controller。旧版本 Controller 的一个示例是版本 7.15。在这种情况下，HDX 优化在 VDA 上默认启用。如果 Workspace app 版本为 1907 或更高版本，Microsoft Teams 将以优化模式启

> 动。有关混合使用 7.15 LTSR Controller 和 CR VDA 的注意事项，请参阅知识中心文章 CTX205549。

> 在这种情况下，要为特定用户禁用此功能，可以覆盖注册表设置。通过使用组策略将登录脚本应用于用户的组织单位来覆盖注册表设置。

> 默认情况下，Microsoft Teams 重定向处于启用状态。

**多媒体会议**

此设置允许或阻止视频会议应用程序使用优化的网络摄像头重定向技术。

默认情况下，允许视频会议支持。

将此设置添加到策略时，请验证是否存在 **Windows Media 重定向**设置并将其设置为“允许”（默认值）。

使用**多媒体会议**时，请验证是否满足以下条件：

- 用于多媒体会议的网络摄像头的制造商提供的驱动程序已安装在客户端上。
- 在开始视频会议会话之前，将网络摄像头连接到用户设备。服务器在任何给定时间只使用一个已安装的网络摄像头。如果用户设备上安装了多个网络摄像头，服务器会尝试依次使用每个网络摄像头。此尝试会一直持续到成功创建视频会议会话为止。

当使用通用 USB 重定向来重定向网络摄像头时，不需要此策略。在这种情况下，请在 VDA 上安装网络摄像头驱动程序。

**通过 WAN 优化 Windows Media 多媒体重定向**

此设置仅适用于 Windows Media，不适用于 HTML5。此设置启用以下功能：

- 实时多媒体转码
- 允许通过降级网络将音频和视频媒体流式传输到移动设备
- 通过改进 Windows Media 内容在 WAN 上的交付方式来增强用户体验。

默认情况下，通过 WAN 交付 Windows Media 内容是经过优化的。

将此设置添加到策略时，请确保存在 **Windows Media 重定向**设置并将其设置为**允许**。

启用此设置后，将根据需要自动部署实时多媒体转码以启用媒体流。此外，即使在极端网络条件下，也能提供无缝的用户体验。

### 使用 GPU 优化通过 WAN 的 Windows Media 多媒体重定向

此设置仅适用于 Windows Media，并支持在虚拟投递代理 (VDA) 上的图形处理单元 (GPU) 中进行实时多媒体转码。它提高了服务器可伸缩性。GPU 转码仅在 VDA 具有受支持的 GPU 用于硬件加速时才可用。否则，转码将回退到 CPU。

**注意：**GPU 转码仅在 NVIDIA GPU 上受支持。

默认情况下，禁止在 VDA 上使用 GPU 优化通过 WAN 交付 Windows Media 内容。

将此设置添加到策略时，请确保存在以下设置并将其设置为“允许”：

- **Windows Media 重定向**
- **通过 WAN 优化 Windows Media 多媒体重定向设置**

### Windows Media 回退预防

此设置适用于浏览器内容重定向、HTML5 和 Windows Media。要使其支持 HTML5，请将 **HTML5 视频重定向**策略设置为**允许**。

管理员可以使用 **Windows Media 回退预防**策略设置来指定尝试向用户交付流式内容的方法。

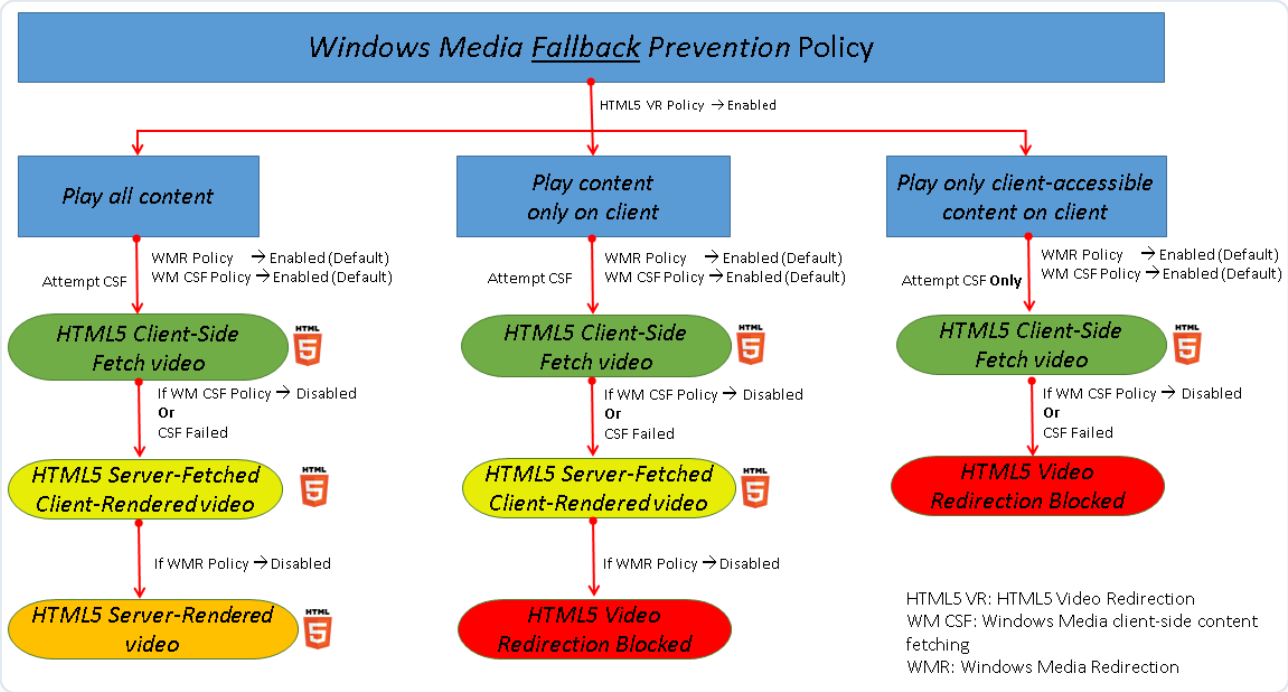
默认情况下，此设置未配置。当设置设为“未配置”时，其行为与**播放所有内容**相同。

要配置此设置，请选择以下选项之一：

- **播放所有内容**。尝试客户端内容获取，然后进行 Windows Media 重定向。如果失败，则在服务器上播放内容。
- **仅在客户端播放所有内容**。尝试客户端获取，然后进行 Windows Media 重定向。如果失败，则不播放内容。
- **仅在客户端播放客户端可访问的内容**。仅尝试客户端获取。如果失败，则不播放内容。

当内容无法播放时，播放器窗口中会显示以下错误消息（默认持续时间为 5 秒）：

```
"Company has blocked video because of lack of resources"
```




此错误消息的持续时间可以通过 VDA 上的以下注册表项进行自定义。如果注册表项不存在，则持续时间默认为 5 秒。

注册表路径因 VDA 架构而异：

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

或者

\HKLM\SOFTWARE\Citrix\HdxMediastream

注册表项：

名称: VideoLoadManagementErrDuration

类型: DWORD

范围: 1 - 直到 DWORD 限制 (默认值 = 5)

单位: 秒

### Windows Media 客户端内容获取

此设置适用于 HTML5 和 Windows Media。此设置使用户设备能够直接从互联网或内网上的源提供商流式传输多媒体文件，而不是通过 XenApp 或 XenDesktop® 主机服务器。

默认情况下，此设置为**允许**。允许此设置可改善网络使用情况并提高服务器可伸缩性。这种改进是通过将媒体上的任何处理从主机服务器移动到用户设备来实现的。它还消除了在用户设备上安装高

级多媒体框架（例如 Microsoft DirectShow 或 Media Foundation）的要求。用户设备只需具备从 URL 播放文件的能力。

将此设置添加到策略时，请确保存在 **Windows Media 重定向**设置并将其设置为**允许**。如果 **Windows Media 重定向**被禁用，则直接从源提供程序向用户设备流式传输多媒体文件也会被禁用。

**Windows Media 重定向**

此设置适用于 HTML5 和 Windows Media，并控制和优化服务器向用户交付流式音频和视频的方式。

默认情况下，此设置为**允许**。对于 HTML5，如果策略 **HTML5 视频重定向**为**禁止**，则此设置不生效。

启用此设置后，从服务器呈现的音频和视频质量会提高到与在用户设备上本地播放的音频和视频相当的水平。服务器以原始压缩形式将多媒体流式传输到客户端，并允许用户设备解压缩和呈现媒体。

Windows Media 重定向优化了使用符合 Microsoft DirectShow、DirectX Media Objects (DMO) 和 Media Foundation 标准的编解码器编码的多媒体文件。要播放给定的多媒体文件，用户设备上必须存在与多媒体文件编码格式兼容的编解码器。

默认情况下，Citrix Workspace 应用程序上禁用音频。要允许用户在 ICA® 会话中运行多媒体应用程序，请打开音频或授予用户在其 Citrix Workspace 应用程序界面中打开音频的权限。

仅当使用 Windows Media 重定向播放媒体的效果比使用基本 ICA 压缩和常规音频呈现的效果差时，才选择**禁止**。这种情况很少见，但可能在低带宽条件下发生，例如，对于关键帧频率较低的媒体。

**Windows Media 重定向缓冲区大小**

此设置为旧版设置，不适用于 HTML5。

此设置指定多媒体加速的缓冲区大小，范围为 1 到 10 秒。

默认情况下，缓冲区大小为 5 秒。

**Windows Media 重定向缓冲区大小使用**

此设置为旧版设置，不适用于 HTML5。

此设置启用或禁用使用在“**Windows Media 重定向缓冲区大小**”设置中指定的缓冲区大小。

默认情况下，不使用指定的缓冲区大小。

如果此设置被禁用，或者未配置“**Windows Media 重定向缓冲区大小**”设置，则服务器将使用默认缓冲区大小值（五秒）。

## 多流连接策略设置

**多流连接**部分包含用于管理会话中多个 ICA® 连接的服务质量 (QoS) 优先级的策略设置。

> **注意：**
>
> 如果启用了多流连接策略，则不支持 MTU 发现。

### 通过 UDP 传输音频

此设置允许或阻止在服务器上通过 UDP 传输音频。

默认情况下，服务器上允许通过 UDP 传输音频。

启用后，此设置会在服务器上打开一个 UDP 端口，以支持所有配置为使用通过 UDP 传输音频实时传输的连接。

### 音频 UDP 端口范围

此设置指定 Virtual Delivery Agent (VDA) 使用的端口号范围（最低端口号，最高端口号）。此规范有助于与用户设备交换音频数据包。VDA 尝试使用每个 UDP 端口对与用户设备交换数据，从最低端口开始，每次尝试递增两个。每个端口处理入站和出站流量。

默认情况下，此范围设置为 16500,16509。

### 多端口策略

此设置指定用于 ICA 流量的 TCP 端口，并为每个端口建立网络优先级。

默认情况下，主端口 (2598) 具有高优先级。

配置端口时，您可以分配以下优先级：

- **非常高：** 用于实时活动，例如网络摄像头会议
- **高：** 用于交互式元素，例如屏幕、键盘和鼠标
- **中：** 用于批量处理，例如客户端驱动器映射
- **低：** 用于后台活动，例如打印

每个端口都必须具有唯一的优先级。例如，您不能同时将“非常高”优先级分配给 CGP 端口 1 和 CGP 端口 3。

要从优先级中删除端口，请将端口号设置为 0。您不能删除主端口，也不能更改其优先级级别。

配置此设置时，请重新启动服务器。此设置仅在启用 **多流计算机** 设置策略设置时才生效。

### 多流计算机设置

此设置用于在服务器上启用或禁用多流。

默认情况下，多流处于禁用状态。如果您使用 Citrix SD-WAN™ 或第三方路由器来实现所需的服务质量，请配置多流计算机策略设置。

如果启用了多流，则不支持 MTU 发现（自适应传输的一项功能）。

配置此设置时，请重新启动服务器以确保更改生效。

> **重要提示：**
>
> 将此策略设置与带宽限制策略设置（例如“会话总带宽限制”）结合使用可能会产生意外结果。在策略中包含此设置时，请确保不包含带宽限制设置。

### 多流用户设置

此设置用于在用户设备上启用或禁用多流。

默认情况下，所有用户都禁用多流。如果您使用 Citrix SD-WAN 或第三方路由器来实现所需的服务质量，请配置多流用户设置。

此设置仅在启用了**多流计算机**设置策略设置的主机上生效。

> **重要提示：**
>
> 将此策略设置与带宽限制策略设置（例如“会话总带宽限制”）结合使用可能会产生意外结果。在策略中包含此设置时，请确保不包含带宽限制设置。

### 多流虚拟通道分配设置

此设置指定在使用多流时虚拟通道分配到的 ICA 流。

如果您不配置这些设置，虚拟通道将保留在其默认流中。要将虚拟通道分配给 ICA 流，请从虚拟通道名称旁边的“**流编号**”列表中选择所需的流编号（0、1、2、3）。

如果环境中使用了自定义虚拟通道，请单击“**添加**”，在“**虚拟通道**”下的文本框中指定虚拟通道名称，然后从其旁边的“**流编号**”列表中选择所需的流编号。您指定的名称必须是实际的虚拟通道名称，而不是友好名称。例如，CTXSBR 而不是 Citrix Browser Acceleration。

这些设置仅在您启用了多流计算机设置时才生效。

默认情况下，虚拟通道及其流分配如下：

- AppFlow®: 2
- 音频: 0
- 浏览器内容重定向: 2
- 客户端 COM 端口映射: 3
- 客户端驱动器映射: 2
- 客户端打印机映射: 3
- 剪贴板: 2
- CTXDND: 1 (**注意：** 这支持在 Citrix 会话和本地端点之间拖放文件。)
- DVC Plug-in（从 DVC 插件友好名称自动生成的静态 VC 名称，或管理员分配的名称）：2
- 最终用户体验监控：1
- 文件传输 (HTML5 Receiver)：2
- 通用数据传输：2
- ICA 控制：1
- 输入法编辑器：1
- 旧版客户端打印机映射 (COM1)：1, 3
- 旧版客户端打印机映射 (COM2)：2, 3
- 旧版客户端打印机映射 (LPT1)：1, 3
- 旧版客户端打印机映射 (LPT2)：2, 3
- 许可证管理：1
- Microsoft Teams/WebRTC 重定向：1
- 移动 Receiver：1
- 多点触控：1
- 端口转发: 2
- 远程音频和视频扩展 (RAVE): 2
- 无缝 (透明窗口集成): 1
- 传感器和位置: 1
- 智能卡: 1
- Thinwire 图形: 1
- 透明 UI 集成/登录状态: 2

- TWAIN 重定向: 2
- USB: 2
- 零延迟字体和键盘: 2
- 零延迟数据通道: 2

有关虚拟通道分配和优先级的更多信息，请参阅知识中心文章 CTX131001。

### 端口重定向策略设置

**端口重定向**部分包含客户端 LPT 和 COM 端口映射的策略设置。

对于 **早于 7.0** 的 Virtual Delivery Agent 版本，请使用以下策略设置配置端口重定向。对于 VDA 版本 **7.0 到 7.8**，请使用注册表配置这些设置；请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。对于 VDA 版本 **7.9**，请使用以下策略设置。

#### 自动连接客户端 COM 端口

此设置可在用户登录站点时启用或禁用用户设备上 COM 端口的自动连接。

默认情况下，客户端 COM 端口不会自动连接。

#### 自动连接客户端 LPT 端口

此设置可在用户登录站点时启用或禁用用户设备上 LPT 端口的自动连接。

默认情况下，客户端 LPT 端口不会自动连接。

#### 客户端 COM 端口重定向

此设置允许或阻止访问用户设备上的 COM 端口。

默认情况下，禁止 COM 端口重定向。

以下策略设置相关：

- COM 端口重定向带宽限制
- COM 端口重定向带宽限制百分比

#### 客户端 LPT 端口重定向

此设置允许或阻止访问用户设备上的 LPT 端口。

默认情况下，禁止 LPT 端口重定向。

LPT 端口仅供将打印作业发送到 LPT 端口的旧版应用程序使用。将打印作业发送到用户设备上的打印对象的旧版应用程序不使用这些端口。如今，大多数应用程序都可以将打印作业发送到打印机对象。此策略设置仅适用于托管打印到 LPT 端口的旧版应用程序的服务器。

请注意，尽管客户端 COM 端口重定向是双向的，但 LPT 端口重定向仅为输出，并且在 ICA 会话中仅限于 `\\client\LPT1` 和 `\\client\LPT2`。

以下策略设置相关：

- LPT 端口重定向带宽限制
- LPT 端口重定向带宽限制百分比

## 打印策略设置

“打印”部分包含用于管理客户端打印的策略设置。

### 客户端打印机重定向

此设置控制当用户登录到会话时，客户端打印机是否映射到服务器。

默认情况下，允许客户端打印机映射。如果此设置被禁用，则不会自动创建会话的 PDF 打印机。

相关策略设置：自动创建客户端打印机

### 默认打印机

此设置指定如何在会话中建立用户设备上的默认打印机。

默认情况下，用户的当前打印机用作会话的默认打印机。

要使用当前远程桌面服务或 Windows 用户配置文件设置作为默认打印机，请选择“不调整用户的默认打印机”。如果选择此选项，默认打印机不会保存在配置文件中，并且不会根据其他会话或客户端属性而更改。会话中的默认打印机是会话中自动创建的第一个打印机，它可能是：

- 本地添加到 Windows 服务器的第一个打印机，位于 **控制面板 > 设备** 和 **打印机** 中。
- 第一个自动创建的打印机（如果服务器上没有本地添加的打印机）。

您可以使用此选项通过配置文件设置向用户提供最近的打印机（称为邻近打印）。

### 打印机分配

此设置提供了“默认打印机”和“会话打印机”设置的替代方案。使用单独的“默认打印机”和“会话打印机”设置来配置站点、大型组或组织单位的行为。使用“**打印机分配**”设置将大量打印机分配给多个用户。

此设置指定如何在会话中建立列出的用户设备上的默认打印机。

默认情况下，用户的当前打印机用作会话的默认打印机。

它还指定了为每个用户设备在会话中自动创建的网络打印机。默认情况下，未指定任何打印机。

- 设置默认打印机值时：

  要使用用户设备的当前默认打印机，请选择“不调整”。

  要使用当前远程桌面服务或 Windows 用户配置文件设置作为默认打印机，请选择“不调整”。如果选择此选项，则默认打印机不会保存在配置文件中，并且不会根据其他会话或客户端属性进行更改。会话中的默认打印机是会话中第一个自动创建的打印机，它可能是：

  - 在 **控制面板 > 设备和打印机** 中本地添加到 Windows 服务器的第一个打印机。
  - 如果没有本地添加到服务器的打印机，则为第一个自动创建的打印机。

- 设置会话打印机值时：要添加打印机，请键入要自动创建的打印机的 UNC 路径。添加打印机后，您可以在每次登录时为当前会话应用自定义设置。

**打印机自动创建事件日志首选项**

此设置指定在打印机自动创建过程中记录的事件。您可以选择不记录错误或警告、仅记录错误或记录错误和警告。

默认情况下，会记录错误和警告。

警告的一个示例是，无法安装打印机的本机驱动程序，而是安装了通用打印驱动程序。在这种情况下，要使用通用打印驱动程序，请将通用打印驱动程序使用情况设置配置为“仅使用通用打印”或“仅在请求的驱动程序不可用时使用通用打印”。

**会话打印机**

此设置指定要在会话中自动创建的网络打印机。在 ICA/HDX 会话中，Citrix Print Manager 服务 (CpSvc.exe) 在会话登录期间为 **会话打印机** 策略设置中指定的每个网络打印机创建网络打印机连接。它会在会话注销期间删除打印机。默认情况下，未指定任何打印机。

在 **会话打印机** 策略设置中，网络打印机可以驻留在 Windows 打印服务器或 Citrix Universal™ Print Server 上。

- **Windows 打印服务器：** 共享一个或多个网络打印机。它还具有使用网络打印机所需的本机打印机驱动程序。
- **通用打印服务器：** 已安装 Citrix Universal Print Server 软件的 Windows 打印服务器。

使用 Windows 打印服务器时，Citrix Print Manager 服务使用本机打印机驱动程序创建网络打印机连接。Citrix Virtual Apps™ 服务器必须安装本机打印机驱动程序。

当使用 Citrix Universal Print Server 时，Citrix Print Manager 服务使用本机打印机驱动程序、Citrix Universal Printer Driver 或 Citrix Universal XPS Printer Driver 创建网络打印机连接。您使用的驱动程序由通用打印驱动程序使用策略设置控制。

所有 Windows 打印机驱动程序目前都属于 v3 或 v4 驱动程序版本。有关详细信息，请参阅 支持 Microsoft V3 和 V4 打印机驱动程序体系结构。

要添加会话打印机并验证它们是否出现在会话中，请完成以下过程：

1. 在 Citrix Studio 中，导航到“**策略**”选项卡。
2. 在“**编辑策略**”对话框中启用会话打印策略。
3. 在策略中，添加会话打印机。要添加打印机，请键入要自动创建的打印机的 UNC 路径。添加打印机后，您可以在每次登录时为当前会话应用自定义设置。会话打印机必须显示在列表中。
4. 设置策略后，已发布的应用程序可能不显示会话打印机。出现此问题的原因可能是 Citrix Virtual Apps 服务器缺少打印机驱动程序，或者策略已创建但未启用。

> **注意：**
>
> 如果打印机驱动程序未安装在 Citrix Virtual Apps 服务器上，您可能会遇到会话打印机最常见的错误，即管理员忘记在 Citrix Virtual Apps 服务器上安装打印机驱动程序。

5. 启动已发布的桌面，并在 **设备和打印机 > 控制面板** 中手动添加会话打印机。
6. 如果此操作失败，请调查 Citrix Virtual Apps 服务器与打印服务器之间的通信。考虑使用 RDP 运行测试。

**等待创建打印机**

根据是用于 Citrix Virtual Desktops™ 还是 Citrix Virtual Apps，以不同方式启用此功能。在 Delivery Controller 上使用策略在 Citrix Virtual Desktops 上启用此功能。在 Delivery Controller 上使用 PowerShell cmdlet 在 Citrix Virtual Apps 上启用此功能。

**等待创建打印机 (服务器桌面):**

此设置允许在连接到会话时延迟，以便可以自动创建客户端重定向的打印机。

默认情况下，不会发生连接延迟。

**等待创建打印机 (Citrix Virtual Apps):**

设置以下 PowerShell cmdlet 允许延迟连接到在服务器桌面上创建的虚拟应用程序，以便可以自动创建客户端重定向的打印机。

```
Set-BrokerApplication -Name <VirualAppName> -WaitForPrinterCreation $true
```

默认情况下，不会发生连接延迟。

### 客户端打印机策略设置

“**客户端打印机**”部分包含客户端打印机的策略设置，包括自动创建客户端打印机、保留打印机属性以及连接到打印服务器的设置。

#### 自动创建客户端打印机

此设置指定自动创建的客户端打印机。此设置会覆盖默认的客户端打印机自动创建设置。

默认情况下，所有客户端打印机都会自动创建。

此设置仅在存在客户端打印机重定向设置并将其设置为 **允许** 时才生效。

将此设置添加到策略时，请选择一个选项：

- **自动创建所有客户端打印机**：自动创建用户设备上的所有打印机。
- **仅自动创建客户端的默认打印机**：仅自动创建在用户设备上选择为默认打印机的打印机。
- **仅自动创建本地（非网络）客户端打印机**：仅自动创建通过 LPT、COM、USB、TCP/IP 或其他本地端口直接连接到用户设备的打印机。
- **不自动创建客户端打印机**：在用户登录时关闭所有客户端打印机的自动创建功能。选择此选项会导致远程桌面服务 (RDS) 中用于自动创建客户端打印机的设置覆盖低优先级策略中的此设置。

#### 自动创建通用型通用打印机

此设置用于启用或禁用在正在使用与通用打印兼容的用户设备的会话中自动创建通用 Citrix Universal™ Printer 对象。

默认情况下，不会自动创建通用 Universal Printer 对象。

以下策略设置相关：

- 通用打印驱动程序用法
- 通用驱动程序首选项

#### 自动创建 PDF 通用打印机

此设置用于启用或禁用为使用适用于 Windows 的 Citrix Workspace 应用程序（从 VDA 7.19 开始）、适用于 HTML5 的 Citrix Workspace 应用程序或适用于 Chrome 的 Citrix Workspace 应用程序的会话自动创建 Citrix PDF 打印机。

默认情况下，Citrix PDF 打印机不会自动创建。

#### 客户端打印机名称

此设置选择自动创建的客户端打印机的命名约定。

默认情况下，使用标准打印机名称。

选择 **标准打印机名称** 以使用诸如“会话 3 中客户端名称的 HPLaserJet 4”之类的打印机名称。

选择 **旧式打印机名称** 以使用旧式客户端打印机名称，并保留与产品 XenApp 和 XenDesktop 版本中存在的旧式打印机名称的向后兼容性。您可以将此选项与当前 Citrix Virtual Apps and Desktops 版本的产品一起使用。旧式打印机名称的示例为“Client/clientname#/HPLaserJet 4”。此选项安全性较低。

当您在从适用于 HTML5 的 Citrix Workspace™ 应用程序启动的会话中使用 Citrix PDF 打印机时，请将 **客户端打印机名称** 设置为默认值或选择 **标准打印机名称**。如果您选择 **旧式打印机名称**，则适用于 HTML5 的 Citrix Workspace 应用程序不支持 Citrix PDF 打印机选项。

#### 直接连接到打印服务器

此设置用于启用或禁用从虚拟桌面或托管应用程序的服务器到打印服务器的直接连接，以用于托管在可访问网络共享上的客户端打印机。

默认情况下，直接连接处于启用状态。

如果网络打印服务器与虚拟桌面或托管应用程序的服务器不在广域网 (WAN) 上，请启用直接连接。如果网络打印服务器与虚拟桌面或托管应用程序的服务器位于同一局域网 (LAN) 上，则直接通信可实现更快的打印。

如果网络跨越广域网 (WAN) 或具有显著延迟或有限带宽，请禁用直接连接。打印作业通过用户设备路由，并在用户设备上重定向到网络打印服务器。发送到用户设备的数据经过压缩，因此数据在广域网上传输时消耗的带宽更少。

如果两个网络打印机具有相同的名称，则使用与用户设备位于同一网络的打印机。

#### 打印机驱动程序映射和兼容性

此设置指定适用于自动创建的客户端打印机的驱动程序替换规则。

此设置配置为从自动创建的客户端打印机列表中排除 Microsoft OneNote 和 XPS Document Writer。

定义驱动程序替换规则时，可以允许或阻止使用指定驱动程序创建打印机。此外，您可以允许创建的打印机仅使用通用打印驱动程序。驱动程序替换会覆盖或映射用户设备提供的打印机驱动程序名

称，并在服务器上替换等效驱动程序。这使得服务器应用程序可以访问与服务器具有相同驱动程序但驱动程序名称不同的客户端打印机。

您可以添加驱动程序映射、编辑现有映射、覆盖映射的自定义设置、删除映射或更改列表中驱动程序条目的顺序。添加映射时，输入客户端打印机驱动程序名称，然后选择要替换的服务器驱动程序。

#### 打印机属性保留

此设置指定是否存储打印机属性以及存储位置。

默认情况下，系统会确定打印机属性是存储在用户设备上（如果可用）还是存储在用户配置文件中。

将此设置添加到策略时，请选择一个选项：

- 仅保存在客户端设备上适用于具有未保存的强制或漫游配置文件的用户设备。仅当您的场中所有服务器都运行 XenApp 5 及更高版本，并且您的用户正在使用 Citrix online plug-in 9 到 12.x 版或 Citrix Receiver 3.x 版时，才选择此选项。
- 仅保留在用户配置文件中适用于受带宽（此选项可减少网络流量）和登录速度限制的用户设备，或适用于使用旧版插件的用户。此选项将打印机属性存储在服务器上的用户配置文件中，并阻止与用户设备进行任何属性交换。将此选项与 MetaFrame Presentation Server 3.0 或更早版本以及 MetaFrame Presentation Server Client 8.x 或更早版本一起使用。请注意，这仅在使用了远程桌面服务 (RDS) 漫游配置文件时适用。
- 仅在未保存在客户端时保留在配置文件中允许系统确定打印机属性的存储位置。打印机属性存储在用户设备上（如果可用）或用户配置文件中。尽管此选项最灵活，但它也可能减慢登录时间并占用额外的带宽进行系统检查。
- 不保留打印机属性可防止存储打印机属性。

#### 保留和还原的客户端打印机

此设置启用或禁用用户设备上打印机的保留和重新创建。默认情况下，客户端打印机是自动保留和自动还原的。

保留的打印机是用户创建的打印机，它们会在下一次会话开始时重新创建或记住。当 Citrix Virtual Apps™ 重新创建保留的打印机时，它会考虑所有策略设置，但 **自动创建客户端打印机** 设置除外。

还原的打印机是管理员完全自定义的打印机，其保存状态永久附加到客户端端口。

#### CITRIX PDF 通用打印机驱动程序

Citrix PDF Universal Printer 驱动程序使用户能够打印通过托管应用程序或在 Citrix Virtual Apps and Desktops 交付的虚拟桌面上运行的应用程序打开的文档。当用户选择 **Citrix PDF 打印机** 选项时，

驱动程序会将文件转换为 PDF 并将 PDF 传输到本地设备。然后打开 PDF 以便从本地连接的打印机进行查看和打印。PDF 是 Citrix Universal Printing 支持的格式之一（除了 EMF 和 XPS）。 可以使用 Citrix 策略启用、配置和设置 PDF 打印机为默认值。适用于 Windows、Chrome 和 HTML5 的 Citrix Workspace 应用程序用户可以使用 **Citrix PDF 打印机** 选项。

> **注意：**
>
> Windows 端点需要 PDF 查看器。客户端必须具有在 Windows 上注册了文件类型关联的应用程序才能打开 PDF 文件。

### 驱动程序策略设置

**驱动程序**部分包含与打印机驱动程序相关的策略设置。

#### 自动安装内置打印机驱动程序

> **注意**
>
> 此策略在此版本中不支持 VDA。

此设置启用或禁用从 Windows 内置驱动程序集或从使用 pnputil.exe /a 在主机上暂存的驱动程序包自动安装打印机驱动程序。

默认情况下，这些驱动程序会根据需要进行安装。

#### 通用驱动程序首选项

此设置指定通用打印机驱动程序的使用顺序，从列表中的第一个条目开始。

默认情况下，首选顺序为：

- EMF
- XPS
- 打印机控制语言5c
- PCL4
- PS

您可以添加、编辑或删除驱动程序，并更改列表中驱动程序的顺序。

#### 通用打印驱动程序用法

此设置指定何时使用通用打印。

默认情况下，仅在请求的驱动程序不可用时才使用通用打印。

通用打印使用通用打印机驱动程序，而不是标准的特定型号驱动程序，这可能会简化主机上的驱动程序管理负担。通用打印驱动程序的可用性取决于用户设备、主机和打印服务器软件的功能。在某些配置中，通用打印可能不可用。

将此设置添加到策略时，请选择一个选项：

- 仅使用打印机型号专用驱动程序指定客户端打印机仅使用登录时自动创建的标准型号专用驱动程序。如果请求的驱动程序不可用，则无法自动创建客户端打印机。
- 仅使用通用打印指定不使用任何标准型号专用驱动程序。仅使用通用打印驱动程序来创建打印机。
- 仅在请求的驱动程序不可用时使用通用打印，如果可用，则使用标准型号专用驱动程序创建打印机。如果服务器上没有该驱动程序，则会自动使用相应的通用驱动程序创建客户端打印机。
- 仅在通用打印不可用时使用打印机型号专用驱动程序，如果可用，则使用通用打印驱动程序。如果服务器上没有该驱动程序，则会自动使用相应的型号专用打印机驱动程序创建客户端打印机。

### 通用打印服务器策略设置

**通用打印服务器**部分包含用于处理通用打印服务器的策略设置。

#### SSL 密码套件

此设置指定通用打印客户端用于加密打印数据流 (CGP) 连接的 SSL/TLS 密码套件集。

要控制通用打印客户端用于加密打印 Web 服务 (HTTPS/SOAP) 连接的密码套件包，请参阅 。

默认值：ALL

此设置具有以下值：ALL、COM 或 GOV。

与每个值对应的密码套件如下所示：

**ALL：**

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

**COM：**

TLS_ECDHE_RSA_AES128_CBC_SHA

**GOV：**

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

#### SSL 合规模式

此设置指定通用打印客户端用于加密打印数据流 (CGP) 连接的 NIST 特别出版物 800-52 合规级别。

默认值: 无。

此设置具有以下值：

**无。**

加密打印数据流 (CGP) 连接使用默认合规模式。

**SP800-52。**

加密打印数据流 (CGP) 连接使用 NIST 特别出版物 800-52 合规模式。

#### SSL 已启用

此设置指定通用打印客户端是否将 SSL/TLS 用于打印数据流 (CGP) 连接和 Web 服务 (HTTP/SOAP) 连接。

当您将 **通用打印服务器启用** 设置为 **启用并回退到 Windows 本机远程打印** 时，回退连接由 Microsoft Windows 网络打印提供程序建立。此设置不影响这些回退连接。

默认值: 禁用

此设置具有以下值：

**已启用。**

通用打印客户端使用 SSL/TLS 连接到通用打印服务器。

**已禁用。**

通用打印客户端使用 SSL/TLS 连接到通用打印服务器。

### SSL FIPS 模式

此设置指定通用打印客户端用于打印数据流 (CGP) 连接的 SSL/TLS 加密模块是否将在 FIPS 模式下运行。

默认值: 禁用

此设置具有以下值：

**已启用。**

FIPS 模式已开启。

**已禁用。**

FIPS 模式已关闭。

### SSL 协议版本

此设置指定通用打印客户端使用的 SSL/TLS 协议版本。

默认值：ALL

此设置具有以下值：

**ALL。**

使用 TLS 版本 1.0、1.1 或 1.2。

**TLSv1. 版本.**

使用 TLS 版本 1.0。

**TLSv1.1。**

使用 TLS 版本 1.1。

**TLSv1.2。**

使用 TLS 版本 1.2。

### SSL 通用打印服务器加密打印数据流 (CGP) 端口

此设置指定通用打印服务器加密打印数据流 (CGP) 端口的 TCP 端口号。此端口接收打印作业的数据。

默认值：443

#### SSL 通用打印服务器加密 WEB 服务 (HTTPS/SOAP) 端口

此设置指定通用打印服务器加密 Web 服务 (HTTPS/SOAP) 端口的 TCP 端口号。此端口接收打印命令的数据。

默认值: 8443

#### 启用通用打印服务器

此设置启用或禁用虚拟桌面或托管应用程序的服务器上的通用打印服务器功能。将此策略设置应用于包含虚拟桌面或托管应用程序的服务器的组织单位 (OU)。

默认情况下，通用打印服务器处于禁用状态。

将此设置添加到策略时，请选择以下选项之一：

- **启用，并回退到 Windows 本机远程打印**。如果可能，网络打印机连接由通用打印服务器提供服务。如果通用打印服务器不可用，则使用 Windows 打印提供程序。Windows 打印提供程序将继续处理以前使用 Windows 打印提供程序创建的所有打印机。
- **启用，不回退到 Windows 本机远程打印**。网络打印机连接仅由通用打印服务器提供服务。如果通用打印服务器不可用，则网络打印机连接失败。此设置有效地禁用了通过 Windows 打印提供程序的网络打印。当包含此设置的策略处于活动状态时，以前使用 Windows 打印提供程序创建的打印机将不会被创建。
- **禁用**。通用打印服务器功能已禁用。当使用 UNC 名称连接到网络打印机时，不会尝试连接通用打印服务器。远程打印机的连接将继续使用 Windows 本机远程打印功能。

#### 通用打印服务器打印数据流 (CGP) 端口

此设置指定通用打印服务器打印数据流通用网关协议 (CGP) 侦听器使用的 TCP 端口号。仅将此策略设置应用于包含打印服务器的组织单位 (OU)。

默认情况下，端口号设置为 7229。

有效端口号必须在 1 到 65535 的范围内。

#### 通用打印服务器打印流输入带宽限制 (KPBS)

此设置指定每个打印作业使用 CGP 传输到通用打印服务器的打印数据传输速率的上限（以千比特每秒为单位）。将此策略设置应用于包含虚拟桌面或托管应用程序的服务器的 OU。

默认情况下，该值为 0，表示没有上限。

#### 通用打印服务器 WEB 服务 (HTTP/SOAP) 端口

此设置指定通用打印服务器的 Web 服务 (HTTP/SOAP) 侦听器使用的 TCP 端口号。通用打印服务器是一个可选组件，它支持在网络打印场景中使用 Citrix 通用打印驱动程序。使用通用打印服务器

时，打印命令通过 HTTP 上的 SOAP 从 Citrix Virtual Apps and Desktops 主机发送到通用打印服务器。此设置修改通用打印服务器侦听传入 HTTP/SOAP 请求的默认 TCP 端口。

您必须将主机和打印服务器的 HTTP 端口配置为相同。如果您未将端口配置为相同，则主机软件将无法连接到通用打印服务器。此设置更改 Citrix Virtual Apps and Desktops 上的 VDA。此外，您必须更改通用打印服务器上的默认端口。

默认情况下，端口号设置为 8080。

有效端口号必须在 0 到 65535 的范围内。

#### 用于负载平衡的通用打印服务器

此设置列出了在评估其他 Citrix® 打印策略设置后，用于在会话启动时建立的打印机连接进行负载平衡的 Universal Print Server。为优化打印机创建时间，Citrix 建议所有打印服务器都具有相同的共享打印机集。可添加用于负载平衡的打印服务器数量没有上限。

此设置还实现了打印服务器故障转移检测和打印机连接恢复。系统会定期检查打印服务器的可用性。如果检测到服务器故障，该服务器将从负载平衡方案中移除，并且该服务器上的打印机连接将重新分配给其他可用的打印服务器。当发生故障的打印服务器恢复时，它将返回到负载平衡方案中。

单击 **验证服务器** 以检查每个服务器是否为打印服务器、服务器列表中不包含重复的服务器名称，并且所有服务器都安装了相同的共享打印机集。此操作可能需要一些时间。

#### UNIVERSAL PRINT SERVER 停止服务阈值

此设置指定负载平衡器应等待不可用的打印服务器恢复多长时间，然后才确定该服务器已永久脱机并将其负载重新分配给其他可用的打印服务器。

默认情况下，阈值设置为 180（秒）。

### 通用打印策略设置

**通用打印**部分包含用于管理通用打印的策略设置。

#### 通用打印 EMF 处理模式

此设置控制在 Windows 用户设备上处理 EMF 后台打印文件的方法。

默认情况下，EMF 记录直接后台打印到打印机。

将此设置添加到策略时，请选择一个选项：

- 重新处理打印机的 EMF 强制重新处理 EMF 后台打印文件并通过用户设备上的 GDI 子系统发送。您可以将此设置用于需要 EMF 重新处理但可能不会在会话中自动选择的驱动程序。

- 直接后台打印到打印机，与 Citrix Universal™ 打印驱动程序一起使用时，可确保 EMF 记录后台打印并传送到用户设备进行处理。通常，这些 EMF 后台打印文件会直接注入到客户端的后台打印队列中。对于与 EMF 格式兼容的打印机和驱动程序，这是最快的打印方法。

#### 通用打印图像压缩限制

此设置指定使用 Citrix 通用打印驱动程序打印的图像可用的最大质量和最小压缩级别。

默认情况下，图像压缩限制设置为最佳质量（无损压缩）。

如果选择“无压缩”，则仅对 EMF 打印禁用压缩。

将此设置添加到策略时，请选择一个选项：

- 无压缩
- 最佳质量（无损压缩）
- 高质量
- 标准质量
- 降低质量（最大压缩）

将此设置添加到包含通用打印优化默认值设置的策略时，请注意以下事项：

- 如果通用打印图像压缩限制设置中的压缩级别低于通用打印优化默认值设置中定义的级别，则图像将按照通用打印图像压缩限制设置中定义的级别进行压缩。
- 如果禁用压缩，则通用打印优化默认值设置的“所需图像质量”和“启用重量级压缩”选项在策略中不起作用。

#### 通用打印优化默认值

此设置指定为会话创建通用打印驱动程序时打印优化的默认值。

- “所需图像质量”指定应用于通用打印的默认图像压缩限制。默认情况下，启用“标准质量”，这意味着用户只能使用标准或降低质量的压缩来打印图像。
- “启用重量级压缩”启用或禁用在不损失图像质量的情况下，将带宽降低到超出“所需图像质量”设置的压缩级别。默认情况下，重量级压缩处于禁用状态。
- 图像和字体缓存设置指定是否缓存打印流中多次出现的图像和字体，以确保每个唯一的图像或字体仅发送到打印机一次。默认情况下，嵌入式图像和字体会被缓存。请注意，这些设置仅在用户设备支持此行为时才适用。
- 允许非管理员修改这些设置指定用户是否可以在会话中更改默认打印优化设置。默认情况下，不允许用户更改默认打印优化设置。

注意：所有这些选项都支持 EMF 打印。对于 XPS 打印，仅支持“所需图像质量”选项。

将此设置添加到包含通用打印图像压缩限制设置的策略时，请注意以下事项：

- 如果通用打印图像压缩限制设置中的压缩级别低于通用打印优化默认值设置中定义的级别，则图像将按照通用打印图像压缩限制设置中定义的级别进行压缩。
- 如果禁用压缩，则通用打印优化默认值设置中的“所需图像质量”和“启用重量级压缩”选项在策略中不起作用。

#### 通用打印预览首选项

此设置指定是否对自动创建或通用打印机使用打印预览功能。

默认情况下，不使用打印预览功能用于自动创建或通用打印机。

将此设置添加到策略时，请选择一个选项：

- 不对自动创建的或通用通用打印机使用打印预览
- 仅对自动创建的打印机使用打印预览
- 仅对通用通用打印机使用打印预览
- 对自动创建的打印机和通用通用打印机都使用打印预览

#### 通用打印质量限制

此设置指定在会话中生成打印输出时可用的最大每英寸点数 (dpi)。

默认情况下，“无限制”处于启用状态，这意味着用户可以选择其连接的打印机允许的最大打印质量。

如果配置了此设置，它将限制用户可用的最大打印质量（以输出分辨率表示）。打印质量本身以及用户连接的打印机的打印质量功能都将受限于配置的设置。例如，如果配置为中等分辨率 (600 DPI)，则用户只能打印最高质量为 600 DPI 的输出，并且通用打印机对话框的“高级”选项卡上的“打印质量”设置将仅显示最高为中等质量 (600 DPI) 的分辨率设置。

将此设置添加到策略时，请选择一个选项：

- 草稿 (150 DPI)
- 低分辨率 (300 DPI)
- 中分辨率 (600 DPI)
- 高分辨率 (1200 DPI)
- 无限制

## 安全策略设置

“安全”部分包含用于配置会话加密和登录数据加密的策略设置。

### SecureICA 最低加密级别

此设置指定服务器与用户设备之间发送的会话数据的最低加密级别。

**重要提示：**对于 Virtual Delivery Agent 7.x，此策略设置只能用于通过 RC5 128 位加密启用登录数据的加密。其他设置仅用于与旧版 Citrix Virtual Apps and Desktops 的向后兼容性。

对于 VDA 7.x，会话数据的加密是使用 VDA 交付组的基本设置来配置的。如果为交付组选择了“启用 Secure ICA”，则会话数据将使用 RC5（128 位）加密进行加密。如果未为交付组选择“启用 Secure ICA”，则会话数据将使用基本加密进行加密。

将此设置添加到策略时，请选择一个选项：

- 基本加密使用非 RC5 算法加密客户端连接。它可防止数据流被直接读取，但可以解密。默认情况下，服务器对客户端-服务器流量使用基本加密。
- RC5（128 位）仅登录使用 RC5 128 位加密对登录数据进行加密，并使用基本加密对客户端连接进行加密。
- RC5（40 位）使用 RC5 40 位加密对客户端连接进行加密。
- RC5（56 位）使用 RC5 56 位加密对客户端连接进行加密。
- RC5（128 位）使用 RC5 128 位加密对客户端连接进行加密。

您为客户端-服务器加密指定的设置可能会与您的环境和 Windows 操作系统中的任何其他加密设置相互作用。如果在服务器或用户设备上设置了更高优先级的加密级别，则您为已发布的资源指定的设置可能会被覆盖。

您可以提高加密级别，以进一步保护某些用户的通信和消息完整性。如果策略要求更高的加密级别，则使用较低加密级别的 Citrix Receiver 将被拒绝连接。

SecureICA 不执行身份验证或检查数据完整性。要为您的站点提供端到端加密，请将 SecureICA 与 TLS 加密结合使用。

SecureICA 不使用 FIPS 兼容算法。如果这是一个问题，请配置服务器和 Citrix Receivers 以避免使用 SecureICA。

SecureICA 使用 RFC 2040 中描述的 RC5 分组密码来实现机密性。块大小为 64 位（32 位字单元的倍数）。密钥长度为 128 位。轮数为 12。

RC5 分组密码的密钥在会话创建时进行协商。协商使用 Diffie-Hellman 算法执行。此协商使用 Diffie-Hellman 公共参数，这些参数在安装 Virtual Delivery Agent 时存储在 Windows 注册表中。公共参数不是秘密。Diffie-Hellman 协商的结果是一个密钥，RC5 分组密码的会话密钥由此密钥派生。单独的会话密钥用于用户登录和数据传输；单独的会话密钥用于往来 Virtual Delivery Agent 的流

量。因此，每个会话有四个会话密钥。密钥和会话密钥不存储。RC5 分组密码的初始化向量也派生自密钥。

### 服务器限制策略设置

“服务器限制”部分包含用于控制空闲连接的策略设置。

#### 服务器空闲计时器间隔

此设置以毫秒为单位，确定在用户没有输入的情况下，不间断的用户会话可以保持多长时间。

默认情况下，空闲连接不会断开连接（服务器空闲计时器间隔 = 0）。Citrix® 建议将此值设置为至少 60000 毫秒（60 秒）。

要显示策略，请选择**多个版本**，清除单会话操作系统版本，然后选择**服务器限制**。

> **注意**
>
> 使用此策略设置时，当会话在指定时间内处于空闲状态时，用户可能会看到一个“空闲计时器已过期”对话框。Citrix 策略设置不控制此 Microsoft 对话框消息。有关详细信息，请参阅 `<http://support.citrix.com/article/CTX118618>`。

### 会话限制策略设置

“**会话限制**”部分包含策略设置，这些设置控制会话在强制注销之前保持连接的时长。

> **重要提示：**
>
> - 本文中描述的设置不适用于运行多会话 VDA 的计算机。有关为运行多会话 VDA 的计算机配置会话时间限制的详细信息，请参阅 Microsoft KB - 会话时间限制。
> - 从 Windows Server 2012 开始，在 Microsoft KB - 会话时间限制 中提及的术语 *Terminal Services* 指的是 *Remote Desktop Service*。

#### 断开连接的会话计时器

此设置启用或禁用：

- 一个计时器，用于指定断开连接的锁定桌面在会话注销之前保持锁定的时间。

如果此计时器已启用，则断开连接的会话将在计时器到期时注销。

默认情况下，断开连接的会话不会注销。

**远程电脑访问断开连接会话计时器**

此设置启用或禁用一个计时器，该计时器在计时器到期后注销断开连接的用户会话。如果启用此设置，请使用**断开连接的会话计时器间隔**设置来指定断开连接的桌面在用户会话注销之前可以保持锁定的分钟数。

默认情况下，此设置为禁用状态。

**断开连接的会话计时器间隔**

此设置指定断开连接的锁定桌面在会话注销之前可以保持锁定的分钟数。

默认情况下，时间段为 1,440 分钟（24 小时）。

**会话连接计时器**

此设置启用或禁用一个计时器，该计时器指定用户设备与桌面之间不间断连接的最长持续时间。如果此计时器已启用，则会话将在计时器到期时断开连接或注销。Microsoft 的“**达到时间限制时结束会话**”设置决定会话的下一个状态。

默认情况下，此计时器处于禁用状态。

**会话连接计时器间隔**

此设置指定用户设备与桌面之间不间断连接的最长分钟数。

默认情况下，最长持续时间为 1,440 分钟（24 小时）。

**会话空闲计时器**

当用户未提供任何输入时，此设置用于启用或禁用：

- 一个计时器，用于指定用户设备与桌面之间不间断连接的维护时长。

当此计时器到期时，会话将进入断开连接状态，并应用**断开连接会话计时器**。如果**断开连接会话计时器**被禁用，则会话不会注销。

默认情况下，此计时器处于启用状态。

**会话空闲计时器间隔**

当用户没有输入时，此设置用于指定：

- 用户设备与桌面之间不间断连接的维护分钟数。

默认情况下，空闲连接会维护 1,440 分钟（24 小时）。

**注意：**

从 2203 LTSR CU2 版本开始，您可以为运行多会话 VDA 的计算机配置以下会话时间限制设置。

**断开连接会话计时器 – 多会话**

此设置启用或禁用一个计时器，以确定断开连接的 RDS 会话在注销之前可以持续多长时间。默认情况下，此计时器处于禁用状态，并且断开连接的会话不会注销。

**断开连接会话计时器间隔 – 多会话**

此设置确定断开连接的 RDS 会话在注销之前可以持续多少分钟。默认情况下，时间段为 1440 分钟（24 小时）。

**会话连接计时器 – 多会话**

此设置启用或禁用一个计时器，该计时器指定用户设备与终端服务器之间不间断连接的最长持续时间。默认情况下，此计时器处于禁用状态。

**会话连接计时器间隔 – 多会话**

此设置指定用户设备与 RDS 会话之间不间断连接的最长分钟数。默认情况下，最长持续时间为 1440 分钟（24 小时）。

**会话空闲计时器 – 多会话**

此设置启用或禁用计时器，以确定用户设备与终端服务器之间空闲连接的最长持续时间。默认情况下，此计时器处于禁用状态。

**会话空闲计时器间隔 – 多会话**

此设置指定用户设备与 RDS 会话之间空闲连接的分钟数。默认情况下，最长持续时间为 1440 分钟（24 小时）。

**注意：**

使用 Citrix® 策略配置的多会话计算机的计时器设置预计会覆盖通过 Microsoft 组策略配置的计时器设置。为避免意外行为，我们建议您使用这两种方法之一来配置计时器设置。

### 会话可靠性策略设置

会话可靠性部分包含用于管理会话可靠性连接的策略设置。

**会话可靠性连接**

此设置允许或阻止在网络连接丢失期间保持会话打开。会话可靠性与客户端自动重新连接功能一起，允许用户在从网络中断中恢复后自动重新连接到其 Citrix Workspace™ 应用程序会话。默认情况下，会话可靠性处于“允许”状态。

Citrix Studio 中的设置在客户端上强制执行，适用于以下情况：

- Citrix Workspace 应用程序 1808 及更高版本
- 适用于 Windows 的 Citrix Receiver 4.7 及更高版本。

Citrix Studio 策略会覆盖客户端上的 Citrix Receiver™ 组策略对象。Studio 中对这些策略的更新会将会话可靠性从服务器同步到客户端。

> **注意：**
>
> - 适用于 Windows 4.7 及更高版本的 Citrix Receiver 和适用于 Windows 的 Citrix Workspace 应用程序 - 在 Studio 中设置策略。
> - 适用于 Windows 4.7 之前的 Citrix Receiver - 在 Studio 中设置策略。同时在客户端上设置 Citrix Receiver 组策略对象模板以保持一致的行为。

> 当网络连接中断时，会话可靠性可使会话保持活动状态并显示在用户屏幕上。用户将继续看到他们正在使用的应用程序，直到网络连接恢复。

使用会话可靠性可使会话在服务器上保持活动状态。为了指示连接已丢失，用户显示会变得不透明。用户可能会在中断期间看到冻结的会话。当网络连接恢复时，用户可以恢复与应用程序的交互。会话可靠性会在不提示重新身份验证的情况下重新连接用户。

如果同时使用会话可靠性和客户端自动重新连接，这两个功能将依次工作。会话可靠性会在会话可靠性超时设置中指定的时间后关闭（或断开连接）用户会话。之后，客户端自动重新连接设置将生效，尝试将用户重新连接到断开连接的会话。

默认情况下，会话可靠性处于“允许”状态。

> **注意：**
>
> 使用 Citrix ADC 时，必须在 Citrix StoreFront > **管理 Citrix Gateway** / **安全票证颁发机构**中选择**启用会话可靠性**以代理 ICA 连接。

> 要禁用会话可靠性：

1. 启动 Citrix Studio 应用程序。
2. 打开**会话可靠性连接**策略。
3. 将策略设置为**禁止**。



**会话可靠性端口号**

此设置指定传入会话可靠性连接的 TCP 端口号。

默认情况下，端口号设置为 2598。

要更改会话可靠性端口号：

1. 启动 Citrix Studio 应用程序。
2. 打开**会话可靠性端口号**策略。
3. 编辑端口号。
4. 单击 **确定**。

**会话可靠性超时**

此设置指定时间长度（以秒为单位）。此时间是会话可靠性代理在允许会话断开连接之前等待用户重新连接的时间。

尽管您可以延长会话保持打开状态的时间，但此功能仅为方便起见，不会提示用户重新进行身份验证。会话打开的时间越长，用户无人看管设备并可能被未经授权的用户访问的可能性就越大。

默认情况下，超时设置为 180 秒（即三分钟）。

要更改会话可靠性超时：

1. 启动 思杰工作室。
2. 打开**会话可靠性超时**策略。
3. 编辑超时值。
4. 单击 **确定**。

## 会话水印策略设置

会话水印部分包含用于配置此功能的策略设置。 启用此功能会导致 VDA 计算机的网络带宽和 CPU 使用率显著增加。建议您根据可用的硬件资源为选定的 VDA 计算机配置会话水印。

**重要提示**

启用会话水印以使其他水印策略设置生效。为获得更好的用户体验，请勿启用两个以上的水印文本项。

### 启用会话水印

启用此设置后，会话显示将具有不透明的文本水印，其中显示会话特定信息。其他水印设置取决于此设置是否启用。

默认情况下，会话水印处于禁用状态。

### 包括客户端 IP 地址

启用此设置后，会话将显示当前客户端 IP 地址作为水印。

默认情况下，禁用“包括客户端 IP 地址”。

### 包括连接时间

启用此设置后，会话水印将显示连接时间。格式为 yyyy/mm/dd hh:mm。显示的时间基于系统时钟和时区。

默认情况下，禁用“包括连接时间”。

### 包括登录用户名

启用此设置后，会话将当前登录用户名显示为水印。显示格式为 USERNAME@DOMAINNAME。我们建议用户名最多为 20 个字符。当用户名超过 20 个字符时，可能会出现字符字体过小或截断，从而降低水印效果。

默认情况下，启用“包括登录用户名”。

### 包括 VDA 主机名

启用此设置后，会话将当前 ICA® 会话的 VDA 主机名显示为水印。

默认情况下，启用“包括 VDA 主机名”。

### 包括 VDA IP 地址

启用此设置后，会话将当前 ICA 会话的 VDA IP 地址显示为水印。

默认情况下，VDA IP 地址处于禁用状态。

#### 会话水印样式

此设置控制是显示单个水印文本标签还是多个标签。从“**值**”下拉菜单中选择“**多个**”或“**单个**”。

**多个**在会话中显示五个水印标签。一个在中心，四个在角落。

**单个**在会话中心显示一个水印标签。

默认情况下，会话水印样式为“多个”。

#### 水印自定义文本

此设置指定要在会话水印中显示的自定义文本字符串（例如，公司名称）。当您配置非空字符串时，它会在新行中显示文本，并附加水印中启用的其他信息。 水印自定义文本的最大长度为 25 个 Unicode 字符。如果配置的字符串较长，则会将其截断为 25 个字符。

没有默认文本。

#### 水印透明度

您可以指定水印不透明度，范围为 0 到 100。指定的值越大，水印越不透明。

默认情况下，值为 17。

### 时区控制策略设置

“时区控制”部分包含与在会话中使用本地时间相关的策略设置。

#### 为旧版客户端估算本地时间

此设置启用或禁用估算向服务器发送不准确时区信息的用户设备的本地时区。

默认情况下，服务器会在必要时估算本地时区。

此设置旨在用于不向服务器发送详细时区信息的旧版 Citrix Receiver 或 ICA 客户端。当与向服务器发送详细时区信息的 Citrix Receiver（例如受支持的 Citrix Receiver™ for Windows 版本）一起使用时，此设置无效。

#### 在会话断开连接或注销时恢复桌面操作系统时区

此设置确定当用户断开连接或注销时，单会话操作系统 VDA 的时区设置是否恢复为计算机的原始时区。如果启用此设置，则当用户断开连接或注销时，VDA 会将计算机的时区恢复为其原始设置。要使此设置生效，请将 **使用客户端本地时间** 设置为 **使用客户端时区**。

默认情况下，此设置处于启用状态。

#### 使用客户端本地时间

此设置确定用户会话的时区设置。选项包括用户会话的时区（服务器时区）或用户设备的时区（客户端时区）。

默认情况下，使用用户会话的时区。

要使此设置生效，请在组策略编辑器中启用 **允许时区重定向** 设置。该设置位于 **本地计算机策略** > **计算机配置** > **管理模板** > **Windows 组件** > **远程桌面服务** > **远程桌面会话主机** > **设备和资源重定向** 中。

如果您在运行服务器操作系统的计算机上使用单会话 VDA（以前称为工作站 VDA），请将本地用户权限 **更改时区** 配置为 **Everyone**。此用户权限可在 **本地计算机策略** > **计算机配置** > **Windows 设置** > **安全设置** > **本地策略** > **用户权限分配** 中找到。

> **注意：**
>
> 在单会话操作系统中，**用户** 包含在用户权限分配 **更改时区** 中，但在多会话操作系统中则不包含。在多会话操作系统中，时区使用以下组策略进行同步：计算机配置\管理模板\Windows 组件\远程桌面服务\远程桌面会话主机\设备和资源重定向\允许时区重定向。当服务器不是多会话操作系统 VDA 中的远程桌面会话主机（使用 `/ServerVDI` 命令安装）时，此策略不适用。在多会话操作系统中，默认情况下，用户没有更改时区的本地权限。

### TWAIN 设备策略设置

TWAIN 设备部分包含与映射客户端 TWAIN 设备（例如数码相机或扫描仪）以及优化从服务器到客户端的图像传输相关的策略设置。

> **注意：**
>
> TWAIN 2.0 可在 Citrix Receiver for Windows 4.5 中获得支持。

#### 客户端 TWAIN 设备重定向

TWAIN 设备使用 TWAIN 协议与服务器托管的图像处理应用程序通信。

此设置允许或阻止用户访问用户设备上的 TWAIN 设备。默认情况下，允许 TWAIN 设备重定向。

以下策略设置相关：

- TWAIN 压缩级别
- TWAIN 设备重定向带宽限制
- TWAIN 设备重定向带宽限制百分比

#### TWAIN 压缩级别

此设置指定从客户端到服务器的图像传输的压缩级别。使用“低”可获得最佳图像质量，使用“中”可获得良好图像质量，使用“高”可获得低图像质量。默认情况下，应用中等压缩。

### USB 设备策略设置

“**USB 设备**”部分包含用于管理 USB 设备文件重定向的策略设置。

#### 客户端 USB 设备优化规则

客户端 USB 设备优化规则可应用于设备，以禁用优化或更改优化模式。

当用户插入 USB 输入设备时，主机将检查 **USB 策略**设置是否允许该设备。如果允许该设备，主机将检查该设备的**客户端 USB 设备优化规则**。如果未指定任何规则，则设备不会进行优化。捕获模式 (04) 是签名设备的推荐模式。对于在高延迟下性能下降的其他设备，管理员可以启用交互模式 (02)。有关可用模式的说明，请参阅本文中的表格。

#### 须知

- 对于 Wacom 签名板和数位板的使用，我们建议您禁用屏幕保护程序。有关如何禁用屏幕保护程序的步骤，请参阅本节末尾。
- 对 Wacom STU 签名板和数位板系列产品优化的支持已在 Citrix Virtual Apps and Desktops™ 策略的安装中预先配置。
- 签名设备可在 Citrix Virtual Apps and Desktops 中使用，并且无需驱动程序即可用作签名设备。Wacom 提供了更多可用于进一步自定义设备的软件。请参阅 `<http://www.wacom.com/>`。
- 绘图板。某些绘图输入设备可能在 PCI/ACPI 总线上显示为 HID 设备，并且不受支持。将这些设备连接到客户端上的 USB 主机控制器，以便在 Citrix Virtual Desktops 会话中进行重定向。

策略规则采用以空格分隔的 tag=value 表达式格式。支持以下标记：

| 标记名称 | 描述 |
| --- | --- |
| 模式 | 优化模式支持 class=**03** 的输入设备。支持的模式包括：无优化 - 值 **01**。交互模式 - 值 **02**。建议用于笔式数位板和 3D Pro 鼠标等设备。捕获模式 - 值 **04**。首选用于签名板等设备。 |

| 标记名称 | 描述 |
| --- | --- |
| VID | 设备描述符中的供应商 ID，为四位十六进制数字。 |
| PID | 设备描述符中的产品 ID，为四位十六进制数字。 |
| REV | 设备描述符中的修订 ID，为四位十六进制数字。 |
| 类 | 来自设备描述符或接口描述符的类。 |
| 子类 | 来自设备描述符或接口描述符的子类。 |
| 协议 | 来自设备描述符或接口描述符的协议。 |

**示例**

Mode=00000004 VID=067B PID=1230 class=03 #在捕获模式下运行的输入设备

Mode=00000002 VID=067B PID=1230 class=03 #在交互模式下运行的输入设备（默认）

Mode=00000001 VID=067B PID=1230 class=03 #在没有任何优化的情况下运行的输入设备

Mode=00000100 VID=067B PID=1230 # 设备设置优化已禁用（默认）

Mode=00000200 VID=067B PID=1230 # 设备设置优化已启用

**禁用 Wacom 签名板设备的屏幕保护程序**

对于 Wacom 签名板和数位板的使用，Citrix® 建议您按如下方式禁用屏幕保护程序：

1. 重定向设备后，安装 **Wacom-STU-Driver**。
2. 安装 **Wacom-STU-Display MSI** 以访问签名板控制面板。
3. 转到 **控制面板 > Wacom STU Display > STU430** 或 **STU530**，然后选择您型号对应的选项卡。
4. 选择 **更改**，然后在 UAC 安全窗口弹出时选择 **是**。
5. 选择 **禁用幻灯片放映**，然后选择 **应用**。

为一种签名板型号设置此设置后，它将应用于所有型号。

**客户端 USB 设备重定向**

此设置允许或阻止将 USB 设备重定向到用户设备以及从用户设备重定向 USB 设备。

默认情况下，USB 设备不会被重定向。

**客户端 USB 设备重定向规则**

此设置指定 USB 设备的重定向规则。

默认情况下，未指定任何规则。

当用户插入 USB 设备时，主机设备会依次对照每条策略规则进行检查，直到找到匹配项。任何设备的第一个匹配项都被视为最终结果。如果第一个匹配项是“允许”规则，则设备将远程连接到虚拟桌面。如果第一个匹配项是“拒绝”规则，则设备仅可用于本地桌面。如果未找到匹配项，则使用默认规则。

策略规则采用 {Allow:|Deny:} 格式，后跟一组以空格分隔的 tag=value 表达式。支持以下标签：

| 标签名称 | 描述 |
| --- | --- |
| VID | 设备描述符中的供应商 ID |
| PID | 设备描述符中的产品 ID |
| REL | 设备描述符中的发布 ID |
| 类 | 设备描述符或接口描述符中的类 |
| 子类 | 设备描述符或接口描述符中的子类 |
| 协议 | 设备描述符或接口描述符中的协议 |

创建策略规则时，请记住：

- 规则不区分大小写。
- 规则末尾可以有一个可选注释，以 # 开头。
- 空行和纯注释行将被忽略。
- 标签必须使用匹配运算符 =（例如，VID=067B_。
- 每条规则必须另起一行，或者作为分号分隔列表的一部分。
- 请参阅 USB Implementers Forum, Inc. 网站上提供的 USB 类代码。

管理员定义的 USB 策略规则示例：

- 允许: VID=067B PID=0007 # 另一家公司，另一个闪存驱动器
- 拒绝: Class=08 subclass=05 # 大容量存储

- 要创建拒绝所有 USB 设备的规则，请使用“DENY:”而不带其他标签。

**客户端 USB 即插即用设备重定向**

此设置允许或阻止在客户端会话中使用即插即用设备，例如摄像头或销售点 (POS) 设备。

默认情况下，允许即插即用设备重定向。当设置为“允许”时，特定用户或组的所有即插即用设备都将被重定向。当设置为“禁止”时，不重定向任何设备。

**配置 USB 设备的自动重定向**

当启用 USB 支持并将 USB 用户首选项设置为自动连接 USB 设备时，USB 设备将自动重定向。

> **注意：**
>
> 在 Receiver for Windows 4.2 中，当在桌面设备模式下运行且连接栏不存在时，USB 设备也会自动重定向。在早期版本的 Citrix Receiver for Windows 中，当在桌面设备模式下运行或与虚拟机 (VM) 托管应用程序一起使用时，USB 设备也会自动重定向。

> 并非总是最好重定向所有 USB 设备。用户可以从未自动重定向的 USB 设备列表中显式重定向设备。要阻止 USB 设备被列出或重定向，请在客户端端点或 DDC 策略上使用 DeviceRules。有关更多详细信息，请参阅管理指南。

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

#### USB 设备自动重定向的用户首选项设置

策略：

1. 打开 **本地组策略编辑器**，然后转到 **管理模板 > Citrix 组件 > Citrix Receiver™ > 远程处理客户端设备 > 通用 USB 远程处理**。
2. 打开 **新建 USB 设备**，选择 **已启用**，然后单击 **确定**。
3. 打开 **现有 USB 设备**，选择 **已启用**，然后单击 **确定**。

思杰接收器：

1. 转到 **Citrix Receiver 首选项 > 连接**。
2. 确保选中以下选项：
   - 会话启动时，自动连接设备
   - 会话运行时连接新设备时，自动连接设备。
3. 单击 **确定**。

所有注册表项和策略更改都应用于 Windows 客户端设备。

#### 普通 USB 打印机重定向

普通 USB 打印机的最佳解决方案是使用专用的通用打印机驱动程序和虚拟通道来执行打印。默认情况下，普通 USB 打印机不会自动重定向。

普通打印机通过启发式方法检测，预计具有扫描功能的高级打印机（例如）可能需要使用 USB 支持进行重定向才能完全正常工作。

使用此注册表配置普通打印机是否自动重定向：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectPrinters

类型: DWORD

数据: 00000000

默认值为 0（不自动重定向）。将值更改为大于零的任何数字将启用 USB 支持以重定向普通 USB 打印机。

您还可以将 Active Directory 策略部署到此注册表项，并在两者都存在时覆盖非策略值：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectAudio

类型: DWORD

数据: 00000000

#### 普通音频设备重定向

与普通打印机类似，最佳用户体验是通过使用 ICA® 的专用音频虚拟通道从普通音频设备发送音频数据实现的。但是，您可能需要使用 USB 支持重定向某些专用设备。启发式方法用于确定哪些设备是普通音频设备。

在客户端端点上使用此注册表配置普通音频设备是否自动重定向：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectAudio

类型: DWORD

数据: 00000000

默认设置为 0 (不自动重定向)。将值更改为非零，将重定向支持 USB 的普通 USB 音频设备。

您可以使用 Active Directory 策略将此值部署到注册表项，并在两者都存在时覆盖非策略值：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectVideo

类型: DWORD

数据: 00000000

#### 普通存储设备 (大容量存储设备) 重定向

对于普通存储设备，您可以使用专用虚拟通道获得最佳用户体验，例如执行优化的客户端驱动器映射。除了简单的文件读写之外，要执行某些特殊任务，例如刻录 CD/DVD 或访问加密文件系统设备，设备可能仍需要使用通用 USB 支持进行重定向。

使用启发式方法来确定哪些设备是普通存储设备。使用此注册表项配置是否自动重定向普通存储设备：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectStorage

类型: DWORD

数据: 00000000

默认设置为 0 (不自动重定向)。将值更改为非零，将重定向使用通用 USB 支持的普通 USB 存储设备。

您还可以使用 Active Directory 策略将此值部署到以下注册表项，并在两者都存在时覆盖非策略值：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectStorage

类型: DWORD

数据: 00000000

> **注意：**
>
> 如果您使用通用 USB 支持，则无法配置对普通存储设备的只读访问，而如果使用 CDM，则可以配置。

#### 带硬件加密的 USB 闪存驱动器重定向

具有硬件加密的 USB 闪存驱动器通常由一个加密存储分区和第二个*实用程序*分区组成，该分区包含用于解锁加密分区的实用程序。对于 USB 闪存驱动器设备，请使用专用的客户端驱动器映射/动态拇指驱动器映射 HDX 虚拟通道，该通道也执行优化，以获得最佳用户体验。

对于非 Windows 客户端（例如 Linux 客户端）以及客户限制（锁定）用户访问客户端本地功能的客户端，通用 USB 重定向是必需的。通用 USB 重定向可以将任何不带硬件加密的 USB 存储设备重定向到单会话操作系统和多会话操作系统 VDA 会话。

在 Citrix Virtual Apps and Desktops 7 1808 之前，具有硬件加密的 USB 闪存驱动器无法以任何有用的方式重定向到单会话操作系统或多会话操作系统 VDA 会话。Citrix Virtual Apps and Desktops 7 1808 中引入的一项新功能增强支持将具有硬件加密的 USB 闪存驱动器通用 USB 重定向到单会话操作系统和多会话操作系统 VDA 会话。 设备重定向后，其任何驱动器都不会显示在本地客户端上。因此，如果需要解锁驱动器，请在会话中执行。此功能需要 Windows 更新 KB4074590。

#### 普通静态图像设备（扫描仪和数码相机）

对于普通静止图像设备，请使用专用的虚拟通道（例如 TWAIN 虚拟通道）以获得最佳用户体验，该通道也执行优化。这些设备必须符合行业标准。如果设备不合规或未按原始意图使用，则通用 USB 重定向可能是使用该设备的唯一方法。启发式方法用于确定哪些设备是普通静止图像设备。

使用此注册表项配置普通静态图像设备是否自动重定向：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectImage

类型: DWORD

数据: 00000000

默认设置为 0（不自动重定向）。将值更改为非零，将使用通用 USB 重定向普通 USB 静态图像设备。

您还可以使用 Active Directory 策略将此值部署到此注册表项，并在两者都存在时覆盖非策略值：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名称: AutoRedirectImage

类型: DWORD

数据: 00000000

#### 设备特定设置

用于选择 Citrix 可优化设备（例如打印机、音频、视频、存储和静止图像设备）的启发式方法并不总是与您的需求相符。您可能希望控制未在上面列出的设备的自动重定向。您可以根据设备控制自动重定向。

例如，DemoTech 2,000 条形码阅读器无需使用 USB 支持进行重定向。它的供应商标识符为 12AB，产品标识符为 5678。这些十六进制数字可以在设备管理器中找到。

为防止其自动重定向，请创建此设备特定的注册表项：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名称: AutoRedirect

类型: DWORD

数据: 00000000

值为 0 可防止设备自动重定向。非零值表示必须考虑自动重定向设备（取决于用户首选项）。供应商和产品标识符之间有一个空格字符。

您还可以使用 Active Directory 策略将此值部署到此注册表项。如果两者都存在，它将覆盖非策略值：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名称: AutoRedirect

类型: DWORD

数据: 00000000

设备特定的 AutoRedirect 设置优先于上述更通用的 AutoRedirectXXX 值。Citrix 优化设备的默认启发式算法可能会将设备误判为通用设备。因此，将设备特定的 AutoRedirect 值设置为 1 以自动重定向它。

### 虚拟通道允许列表策略设置

**虚拟通道允许列表**策略设置启用允许列表的使用，该列表指定允许在 ICA® 会话中打开哪些虚拟通道。

禁用时，允许所有虚拟通道。

启用时，仅允许 Citrix® 虚拟通道。

要使用自定义或第三方虚拟通道，请将虚拟通道添加到列表中。要将虚拟通道添加到列表中，请输入虚拟通道名称，后跟逗号，然后是访问该虚拟通道的进程路径。可以列出更多可执行路径，路径之间用逗号分隔。

例如，

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

从 Citrix Virtual Apps and Desktops™ 7 2109 开始，虚拟通道允许列表默认启用。

如果您正在使用适用于 Skype for Business 的 HDX RealTime Optimization Pack，请将虚拟通道添加到允许列表。有关详细信息，请参阅 HDX RealTime Optimization Pack 文档。

> **重要提示：**
>
> 必须重新启动 VDA 计算机才能使设置生效。
>
> 有关虚拟通道的详细信息，请参阅 ICA 虚拟通道。

### 视觉显示策略设置

视觉显示部分包含用于控制从虚拟桌面发送到用户设备的图像质量的策略设置。

#### 简单图形的首选颜色深度

此策略设置在 VDA 7.6 FP3 及更高版本中可用。8 位选项在 VDA 7.12 及更高版本中可用。

此设置可降低通过网络发送简单图形时的颜色深度。将颜色深度降低到每像素 8 位或 16 位可能会提高低带宽连接的响应速度，但会略微降低图像质量。当 Use video codec for compression 策略设置为“For the entire screen”时，不支持 8 位颜色深度。

默认的首选颜色深度为每像素 24 位。

如果在 VDA 7.11 及更早版本上应用 8 位设置，VDA 将回退到 24 位（默认）颜色深度。

**目标帧率**

此设置指定从虚拟桌面发送到用户设备的最大每秒帧数。

默认情况下，最大值为每秒 30 帧。

设置较高的每秒帧数（例如 30）可改善用户体验，但需要更多带宽。降低每秒帧数（例如 10）可在牺牲用户体验的情况下最大限度地提高服务器可伸缩性。对于 CPU 速度较慢的用户设备，请指定较低的值以改善用户体验。

支持的最大每秒帧速率为 60。

**视觉质量**

此设置指定用户设备上显示的图像所需的视觉质量。

默认情况下，此设置为“中”。

要指定图像质量，请选择以下选项之一：

- **低** - 建议用于带宽受限的网络，在这种情况下，可以牺牲视觉质量以提高交互性
- **中** - 在大多数用例中提供最佳性能和带宽效率
- **高** - 如果您需要视觉无损的图像质量，建议使用此设置
- **构建为无损** - 在网络活动高峰期向用户设备发送有损图像，并在网络活动减少后发送无损图像。此设置可提高带宽受限网络连接的性能
- **始终无损** - 当保留图像数据至关重要时，请选择“始终无损”以确保有损数据永远不会发送到用户设备。例如，在显示不允许任何质量损失的 X 射线图像时。

**动态图像策略设置**

“**动态图像**”部分包含允许您移除或更改动态图像压缩的设置。

**最低图像质量**

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

此设置指定了自适应显示可接受的最低图像质量。使用的压缩越少，显示的图像质量越高。可选择超高、很高、高、正常或低压缩。

默认情况下，此设置为正常。

#### 动态图像压缩

此设置指定是否启用自适应显示。自适应显示会根据可用带宽自动调整幻灯片放映中视频和过渡幻灯片的图像质量。启用自适应显示后，用户应能看到流畅运行的演示文稿，且质量不会降低。

默认情况下，自适应显示已启用。

对于 VDA 7.0 到 7.6 版本，此设置仅在启用旧版图形模式时适用。对于 VDA 7.6 FP1 及更高版本，此设置在启用旧版图形模式时适用，或者在禁用旧版图形模式且未使用视频编解码器压缩图形时适用。

启用旧版图形模式时，必须重新启动会话，策略更改才能生效。自适应显示与渐进式显示互斥；启用自适应显示会禁用渐进式显示，反之亦然。但是，渐进式显示和自适应显示可以同时禁用。渐进式显示作为一项旧版功能，不建议用于 XenApp 或 XenDesktop。设置渐进式阈值级别将禁用自适应显示。

#### 渐进式压缩级别

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

此设置提供细节较少但初始显示速度更快的图像。

默认情况下，不应用渐进式压缩。

由正常有损压缩设置定义的更详细图像在可用时显示。使用很高或超高压缩可改善带宽密集型图形（例如照片）的观看效果。

要使渐进式压缩有效，其压缩级别必须高于有损压缩级别设置。

注意：与渐进式压缩相关的压缩级别提高，也增强了动态图像在客户端连接上的交互性。动态图像（例如旋转的三维模型）的质量会暂时降低，直到图像停止移动，此时将应用正常的有损压缩设置。

以下策略设置相关：

- 渐进式压缩阈值
- 渐进式重量级压缩

#### 渐进式压缩阈值

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

此设置表示应用渐进式压缩的连接的最大带宽（以千比特/秒为单位）。此设置仅适用于低于此带宽的客户端连接。

默认情况下，阈值为每秒 2147483647 千比特。

以下策略设置相关：

- 渐进式压缩阈值
- 渐进式重量级压缩

#### 目标最小帧率

此设置指定了系统在低带宽条件下尝试为动态图像维持的每秒最低帧率。

默认情况下，此值设置为 10fps。

对于 VDA 7.0 到 7.6 版本，此设置仅在启用旧版图形模式时适用。对于 VDA 7.6 FP1 及更高版本，此设置在禁用或启用旧版图形模式时均适用。

### 静态图像策略设置

“**静态图像**”部分包含的设置使您能够删除或更改静态图像的压缩。

#### 额外颜色压缩

此设置启用或禁用对通过带宽受限的客户端连接传输的图像使用额外颜色压缩，通过降低显示图像的质量来提高响应速度。

默认情况下，额外颜色压缩处于禁用状态。

启用后，仅当客户端连接带宽低于“额外颜色压缩阈值”时，才应用额外颜色压缩。当客户端连接带宽高于阈值或选择“禁用”时，不应用额外颜色压缩。

#### 额外颜色压缩阈值

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用“旧版图形模式”策略设置时适用。

此设置表示连接的最大带宽（以千比特/秒为单位），低于此带宽时将应用额外颜色压缩。如果客户端连接带宽低于设定值，则在启用额外颜色压缩的情况下，将应用额外颜色压缩。

默认情况下，阈值为 8192 千比特/秒。

#### 重量级压缩

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用“旧版图形模式”策略设置时适用。

此设置启用或禁用通过使用更高级但更占用 CPU 的图形算法，在不损失图像质量的情况下，将带宽减少到超出渐进式压缩的程度。

默认情况下，重量级压缩处于禁用状态。

如果启用，重量级压缩将应用于所有有损压缩设置。它在 Citrix Workspace™ 应用程序上受支持，但对其他插件无效。

以下策略设置相关：

- 渐进式压缩级别
- 渐进式压缩阈值

#### 有损压缩级别

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

此设置控制通过带宽受限的客户端连接传输图像时使用的有损压缩程度。在这种情况下，不压缩显示图像可能会很慢。

默认情况下，选择中等压缩。

对于带宽密集型图像，为提高响应速度，请使用高压缩。在图像数据保存至关重要的情况下；例如，在显示不允许任何质量损失的 X 射线图像时，您可能不希望使用有损压缩。

相关策略设置：有损压缩阈值

#### 有损压缩阈值

注意：对于 Virtual Delivery Agent 7.x，此策略设置仅在启用旧版图形模式策略设置时适用。

此设置表示应用有损压缩的连接的最大带宽（以千比特/秒为单位）。

默认情况下，阈值为 2147483647 千比特/秒。

将“有损压缩级别”设置添加到策略中且不包含指定的阈值，可以提高通过 LAN 显示高细节位图（例如照片）的速度。

相关策略设置：有损压缩级别

### WebSockets 策略设置

WebSockets 部分包含用于使用适用于 HTML5 的 Citrix Workspace™ 应用程序访问虚拟桌面和托管应用程序的策略设置。WebSockets 功能通过在基于浏览器的应用程序和服务器之间进行双向通信来提高安全性并减少开销。此功能无需打开多个 HTTP 连接即可实现此目的。

#### WebSockets 连接

此设置允许或禁止 WebSockets 连接。

默认情况下，WebSockets 连接被禁止。

#### WebSockets 端口号

此设置标识传入 WebSocket 连接的端口。

默认情况下，值为 8008。

#### WebSockets 受信任的源服务器列表

此设置提供受信任的源服务器的逗号分隔列表（通常是适用于 Web 的 Citrix Workspace 应用程序），以 URL 形式表示。服务器仅接受源自这些地址之一的 WebSockets 连接。

默认情况下，通配符 * 用于信任所有 Citrix Workspace app for Web URL。

如果您选择在列表中键入地址，请使用以下语法：

\<protocol>://\<主机的完全限定域名>:

协议必须是 HTTP 或 HTTPS。如果未指定端口，则 HTTP 使用端口 80，HTTPS 使用端口 443。

通配符 `*` 可以在 URL 中使用，但不能作为 IP 地址的一部分（例如 10.105..）。

### WIA 设备策略设置

WIA 设备部分包含用于使用 Windows 图像采集 (WIA) 管理扫描仪重定向的策略设置。

#### WIA 重定向

WIA 设备（例如数码相机和扫描仪）通过使用 WIA 框架与服务器托管的图像处理应用程序通信。此设置允许或禁止用户访问用户设备上的 WIA 设备。默认情况下，WIA 重定向是被禁止的。

有关 WIA 兼容设备的信息，请参阅 WIA 设备。

## 通过注册表管理的 HDX™ 功能

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

> 要在服务器上打开注册表编辑器，请运行 `regedit.exe`。然后导航到注册表项以添加或编辑设置。

## 设备

### 彭博键盘

Citrix Virtual Apps and Desktops™ 支持彭博型号 4 和型号 3 右舷键盘。默认情况下，增强型彭博键盘的支持处于禁用状态。

为了启用对 Bloomberg 键盘的支持，请在启动连接之前在客户端计算机上设置以下注册表值：

- 键: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB
- 值名称: EnableBloombergHID
- 值类型: DWORD
- 值数据: 0 = 禁用, 1 = 启用

有关详细信息，请参阅彭博键盘。

### 映射的客户端驱动器

作为一项安全预防措施，当用户登录到 Citrix Virtual Apps and Desktops 时，默认情况下，服务器会映射客户端驱动器，但没有用户运行权限。为了使用户能够运行驻留在映射客户端驱动器上的可执行文件，请通过编辑服务器上的注册表来覆盖此默认设置。

要允许访问，请编辑以下注册表值（如果不存在，请创建 **CDMSettings**）：

- 键: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings
- 值名称: ExecuteFromMappedDrive
- 值类型: DWORD
- 值数据: 1 = 允许权限, 0 = 拒绝映射驱动器上的权限

更改将在您编辑注册表后连接的会话中生效。

有关详细信息，请参阅映射的客户端驱动器。

### 微软 Surface Pro 和 Surface Book 触控笔

Citrix Virtual Apps and Desktops 支持 Windows Ink 应用程序的标准笔功能。默认情况下，此功能处于启用状态。

要禁用或启用此功能，请设置以下注册表值：

- 键：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi
- 值名称: DisablePen
- 值类型: DWORD

- 值数据: 1 = 禁用, 0 = 启用

有关详细信息，请参阅 Microsoft Surface Pro 和 Surface Book 触控笔。

#### Windows 图像采集应用程序允许列表

此设置允许您控制 VDA 上的哪些应用程序可以访问 Windows 图像采集扫描仪重定向。

默认情况下，没有应用程序可以访问 Windows 图像采集。

要调整 VDA 上应用程序的 Windows 图像采集，请创建以下注册表设置：

- 键：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix
- 值名称: WIAAllowedProcesses

  选择并右键单击 **WIAAllowedProcesses**。选择**新建 > 多字符串值**，并将新值重命名为 **AllowProcesses**。
- 值数据：输入可以访问 Windows 图像采集的每个应用程序的完整路径和进程名称。每行提供一个应用程序。

对此设置的任何更改将在您下次在 VDA 上启动会话时生效。

### 常规

#### 配置自动登录到 VDA

此设置允许您在 Windows 10 单会话操作系统和多会话操作系统 VDA 上启用或禁用 **始终提示输入密码** Microsoft 策略设置。

如果启用了 **始终提示输入密码**，则用户在启动远程会话时必须在 VDA 上输入凭据。如果禁用此设置，则用户将自动连接到远程会话，而无需在 VDA 上提供凭据。

默认情况下，Microsoft 策略设置处于禁用状态。要启用或禁用 **始终提示输入密码** 设置，请在 VDA 上设置以下注册表值：

- 键: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica
- 值名称: AutoLogon
- 值类型: DWORD
- 值数据:
  - 1 - 禁用 Microsoft 策略设置，并允许用户自动登录到远程会话。
  - 0 – 启用 Microsoft 策略设置，并提示用户在启动远程会话时提供凭据。

#### 禁用超时警告

默认情况下，会话不活动或空闲的用户会在其会话自动断开连接前两分钟收到警告消息。

此设置禁用并删除针对在 Windows 2004 或更高版本的多会话操作系统上达到空闲会话超时限制的用户的警告消息。要删除警告，请在 VDA 上设置以下注册表值:

- 项: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP
- 值名称: fEnableTimeoutWarning
- 值类型: DWORD
- 值数据: 1 = 禁用警告消息, 0 = 启用警告消息

要显示警告消息，请删除注册表值或将其设置为 0。

#### EDT MTU 发现

MTU 发现允许 EDT 在建立会话时自动确定最大传输单元 (MTU)。这样做可以防止 EDT 数据包碎片化，从而避免性能下降或会话建立失败。

此设置默认启用。要禁用 EDT MTU 发现，请配置以下注册表值并重新启动 VDA。

- 项: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- 值名称: MtuDiscovery
- 值类型: DWORD
- 值数据: 0

此设置是计算机范围的，会影响所有从受支持客户端连接的会话。

### 通用内容重定向

#### 添加用于主机到客户端重定向的 URL 类型

默认情况下，我们支持重定向以下 URL 类型: HTTP、HTTPS、RTSP、RTSPU、PNM 和 MMS。您可以通过在 Windows 客户端上创建以下注册表项和值来将 URL 类型添加到列表中。

- 项：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 值名称：ExtraURLProtocols
- 值类型：REG_SZ
- 值数据：指定所需的 URL 类型，用分号分隔。包括 URL 权限部分之前的所有内容。例如：`ftp://;mailto:;customtype1://;custometype2://`

您只能为 Windows 客户端添加 URL 类型。缺少此注册表设置的客户端会拒绝重定向回 Citrix 会话。客户端必须安装并配置一个应用程序来处理指定的 URL 类型。

有关详细信息，请参阅主机到客户端重定向。

#### 客户端文件夹重定向

客户端文件夹重定向会更改客户端文件在主机端会话中的访问方式。如果您在服务器上启用客户端文件夹重定向，并且用户在用户设备上对其进行配置，则用户指定的本地卷部分将被重定向。

要在服务器上启用客户端文件夹重定向，请设置以下注册表值：

- 键：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection
- 值名称: CFROnlyModeAvailable
- 值类型: DWORD
- 值数据: 1

有关详细信息，请参阅客户端文件夹重定向。

#### 针对特定网站集的主机到客户端重定向

要针对特定网站集启用主机到客户端重定向，请在服务器 VDA 上设置以下注册表值。

- 项: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 值名称: ValidSites
- 值类型: REG_MULTI_SZ
- 值数据: 指定完全限定域名 (FQDN) 的任意组合。在单独的行上键入多个 FQDN。仅包含 FQDN，不带协议 (`http://` 或 `https://`)。FQDN 只能在最左侧位置包含星号 (`*`) 作为通配符。此通配符匹配单个域级别，这与 RFC 6125 中的规则一致。例如：

`www.example.com`

`*.example.com`

有关详细信息，请参阅主机到客户端重定向。

#### 注销和断开连接时的本地应用程序行为

默认情况下，当用户从虚拟桌面注销或断开连接时，本地应用程序会继续运行。重新连接后，如果本地应用程序在虚拟桌面上可用，则会重新集成。要配置注销和断开连接时的本地应用程序行为，请在托管桌面中设置以下注册表值:

- 键: HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies

- 值名称: Session State
- 值类型: DWORD
- 值数据:
  - 1 - 当用户注销或断开与虚拟桌面的连接时，本地应用程序将继续运行。重新连接后，如果本地应用程序在虚拟桌面中可用，它们将重新集成。
  - 3 - 当用户注销或断开与虚拟桌面的连接时，本地应用程序将关闭。

有关详细信息，请参阅 本地应用程序访问和 URL 重定向。

**从默认列表中删除用于主机到客户端重定向的 URL 类型**

要从默认重定向列表中删除 URL 类型，请在服务器 VDA 上创建以下注册表项和值。

- 项: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 值名称: DisableServerFTA
- 值类型: DWORD
- 值数据: 1
- 值名称: NoRedirectClasses
- 值类型: REG_MULTI_SZ
- 值数据: 指定以下值的任意组合：`http`、`https`、`rtsp`、`rtspu`、`pnm` 或 `mms`。在单独的行上键入多个值。例如：

`http`

`https`

`rtsp`

有关详细信息，请参阅 主机到客户端重定向。

**服务器 VDA 默认浏览器配置**

您可以启用主机到客户端重定向，以取代服务器 VDA 上的任何默认浏览器配置。如果 Web URL 未重定向，Citrix 启动器会将该 URL 传递给 `command_backup` 注册表项中配置的浏览器。此项默认指向 Internet Explorer，但您可以修改它以包含不同浏览器的路径。

- IE浏览器（默认）
  - 项: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - 值名称: Default

    - 值类型：REG_SZ
    - 值数据：`"c:\program files\internet explorer\iexplore.exe" %1`
    - 项: HKEY_CLASSES_ROOT\https\shell\open\command_backup`
    - 值名称: Default
    - 值类型：REG_SZ
    - 值数据：`"c:\program files\internet explorer\iexplore.exe" %1`
- 谷歌浏览器
    - 项: HKEY_CLASSES_ROOT\http\shell\open\command_backup
    - 值名称: Default
    - 值类型：REG_SZ
    - 值数据：`"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" %1`
    - 项: HKEY_CLASSES_ROOT\https\shell\open\command_backup
    - 值名称: Default
    - 值类型：REG_SZ
    - 值数据：`"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" %1`
- 微软 Edge 浏览器
    - 项: HKEY_CLASSES_ROOT\http\shell\open\command_backup
    - 值名称: Default
    - 值类型：REG_SZ
    - 值数据: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" %1`
    - 键: HKEY_CLASSES_ROOT\https\shell\open\command_backup
    - 值名称: 默认
    - 值类型：REG_SZ
    - 值数据: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" %1`

**已发布的应用程序的本地应用程序访问**

本地应用程序访问将本地安装的 Windows 应用程序无缝集成到托管桌面环境中，而无需在不同桌面之间切换。要提供对已发布应用程序的访问，请在服务器上设置以下注册表值：

- 键: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio

- 值名称: ClientHostedAppsEnabled
- 值类型: DWORD
- 值数据: 1 = 启用, 0 = 禁用

有关详细信息，请参阅本地应用程序访问和 URL 重定向。

## 图形

### 适用于 CUDA 或 OpenCL 应用程序的 GPU 加速

在用户会话中运行的 CUDA 和 OpenCL 应用程序的 GPU 加速默认情况下处于禁用状态。

要使用 CUDA 加速 POC 功能，请启用以下注册表设置：

- 注册表项: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper
- 值名称: CUDA
- 值类型: DWORD
- 值数据: 00000001

要使用 OpenCL 加速 POC 功能，请启用以下注册表设置：

- 注册表项: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper
- 值名称: OpenCL
- 值类型: DWORD
- 值数据: 00000001

有关详细信息，请参阅 适用于 Windows 多会话操作系统的 GPU 加速

### 渐进模式

渐进模式默认处于禁用状态。您可以使用以下注册表值更改渐进模式状态：

- 键: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 值类型: REG_DWORD
- 值名称: ProgressiveDisplay
- 值数据:

- 0 = 始终关闭 (禁用渐进模式。此值为默认值。)
- 1 = 自动 (根据网络条件切换。)
- 2 = 始终开启

有关详细信息，请参阅 渐进模式。

#### Windows 演示基础 (WPF) 渲染

HDX 3D Pro 允许在 Windows 多会话操作系统会话中运行的图形密集型应用程序在服务器的图形处理单元 (GPU) 上进行渲染。通过将 Windows Presentation Foundation (WPF) 渲染移至服务器的 GPU，图形渲染不会降低服务器 CPU 的速度。

要使用服务器的 GPU 启用 WPF 应用程序渲染，请在运行 Windows 多会话操作系统的服务器注册表中创建以下设置：

- 键: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook
- 值名称: EnableWPFHook
- 值类型: DWORD
- 值数据: 00000001

有关详细信息，请参阅适用于 Windows 多会话操作系统的 GPU 加速。

### 多媒体

#### 避免多媒体会议期间的回声

Citrix Virtual Apps and Desktops 提供回声消除选项，可最大程度地减少任何回声。此功能默认启用。要禁用回声消除，您可以更改以下注册表设置之一：

- 键：
  - 32 位: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio
  - 64 位: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio
- 值名称: EchoCancellation
- 值类型: DWORD
- 值数据: False

有关详细信息，请参阅音频功能。

### 音频限制

在客户端上安装音频设备、启用音频重定向并启动 RDS 会话后，音频文件可能无法播放音频。作为一种解决方法，请在 RDS 计算机上添加以下注册表项，然后重新启动计算机：

- 项: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig
- 值名称: EnableSvchostMitigationPolicy
- 值类型: DWORD
- 值数据: 0

有关详细信息，请参阅音频功能。

### 浏览器内容重定向和 DPI

当在用户计算机上使用浏览器内容重定向且 DPI（缩放）设置为 100% 以上时，重定向的浏览器内容屏幕显示不正确。为避免此问题，请通过在用户计算机上创建以下注册表值来禁用 Chrome 的浏览器内容重定向 GPU 加速：

- 项：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- 值名称：GPU
- 值类型: DWORD
- 值数据：0

有关详细信息，请参阅浏览器内容重定向和 DPI。

### 高清网络摄像头流式传输

服务器上的视频会议应用程序根据支持的格式类型选择网络摄像头的格式和分辨率。Citrix Virtual Apps and Desktops 支持高达 1920x1080 的网络摄像头分辨率。要禁用和启用高清网络摄像头流式传输，请添加以下注册表值：

- 项：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXRealTime
- 值名称：Enable_HighDefWebcam
- 值类型: DWORD
- 值数据:
  - 0 = 禁用高清网络摄像头流式传输
  - 1 = 启用高清网络摄像头流式传输

**高清网络摄像头分辨率**

如果媒体类型协商失败，HDX 将回退到 352x288 CIF 的默认分辨率。您可以使用客户端上的注册表项来配置默认分辨率。在设置以下注册表项之前，请确保摄像头支持指定的分辨率。

- 项：HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 宽度
  - 值名称：DefaultWidth
  - 值类型: DWORD
  - 值数据：所需的十进制宽度（例如 1280）
- 高度
  - 值名称：DefaultHeight
  - 值类型: DWORD
  - 值数据：所需高度（十进制）（例如 720）

**高清网络摄像头带宽**

与即插即用通用 USB 重定向相比，HDX 网络摄像头视频压缩使用的带宽更少，并且在 WAN 连接上运行良好。要调整带宽，请在客户端上设置以下注册表值：

- 项：HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 值名称：TargetBitrate
- 值类型: DWORD
- 值数据：350000

输入每秒位数的值。如果未指定带宽，视频会议应用程序默认使用 350000 bps。

有关详细信息，请参阅HDX 网络摄像头视频压缩。

**Microsoft Teams 回退模式**

如果 Microsoft Teams 未能在优化的 VDI 模式下加载（在 Teams/关于/版本 中显示“Citrix HDX 未连接”），VDA 将回退到旧版 HDX 技术，例如网络摄像头重定向以及客户端音频和麦克风重定向。如果您使用的 Workspace 应用程序版本/平台操作系统不支持 Microsoft Teams 优化，则回退注册表项不适用。

要控制回退机制，请在 VDA 上设置以下注册表值之一：

- 项（只需一个）：

  - **计算机设置：** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams
  - **用户设置：** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams

- 值名称：DisableFallback
- 值类型: DWORD
- 值数据：1 = 禁用回退模式，2 = 仅启用音频

如果该值不存在或设置为 0，则启用回退模式。此功能需要 Microsoft Teams 1.3.0.13565 或更高版本。有关详细信息，请参阅 Microsoft Teams 优化。

**使用 Citrix App Layering™ 对 Microsoft Teams 进行优化**

如果使用 Citrix App Layering 在不同层中管理 VDA 和 Microsoft Teams 安装，请在安装 Microsoft Teams 并设置 **ALLUSER**=1 之前，在 Windows 上部署此注册表项。

创建一个名为 **PortICA** 的空注册表项，并保留默认值名称、类型和数据。

- 注册表编辑器的 32 位版本项：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA
- 注册表编辑器的 64 位版本项：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

有关详细信息，请参阅 Microsoft Teams 优化。

**用于浏览器内容重定向的集成 Windows 身份验证单点登录**

此设置提供对与 VDA 位于同一域中配置了集成 Windows 身份验证 (IWA) 的 Web 服务器的单点登录。要启用单点登录，请将以下注册表值设置为 1：

- 键：
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream

  或

  - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\HdxMediastream
- 值名称: WebBrowserRedirectionIwaSupport
- 值类型: DWORD
- 值数据: 1

有关详细信息，请参阅集成 Windows 身份验证单点登录。

### 用户代理请求标头

用户代理标头有助于识别从浏览器内容重定向发送的 HTTP 请求。此设置在配置代理和防火墙规则时非常有用。例如，如果服务器阻止从浏览器内容重定向发送的请求，您可以创建一个包含用户代理标头的规则来绕过某些要求。只有 Windows 设备支持用户代理请求标头。

默认情况下，用户代理请求标头字符串处于禁用状态。要为客户端呈现的内容启用用户代理标头，请使用注册表编辑器。

在每个适用于 Windows 客户端的 Citrix Workspace™ 应用程序上，设置以下注册表设置之一：

- 键：
  - 32 位: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream
  - 64 位: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- 值名称: EnableCefUserAgentString
- 值类型: DWORD
- 值数据: 1

添加注册表值后，用户代理标头将包含 CitrixBCR/2102.1 文本，其中 2102.1 是适用于 Windows 的 Citrix Workspace 应用程序版本。

### 网络摄像头软件压缩

如果网络摄像头支持硬件编码，HDX 视频压缩默认使用硬件编码。硬件编码可能比软件编码消耗更多带宽。要强制使用软件压缩，请在客户端上添加以下值：

- 项：HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime
- 值名称：DeepCompress_ForceSWEncode
- 值类型: DWORD
- 值数据: 1

有关详细信息，请参阅HDX 网络摄像头视频压缩。

### 网络摄像头视频压缩

HDX 网络摄像头视频压缩将 H.264 视频直接发送到在虚拟会话中运行的视频会议应用程序。为了优化 VDA 资源，HDX 网络摄像头压缩不会对网络摄像头视频进行编码、转码和解码。此功能默认启用。

要禁用从服务器到视频会议应用程序的直接视频流，请在 VDA 中设置以下注册表值。

- 项：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime

- 值名称：OfferH264ToApp
- 值类型: DWORD
- 值数据：0

有关详细信息，请参阅HDX 网络摄像头视频压缩。

#### 网络摄像头视频压缩帧速率

要调整首选视频帧速率，请在客户端上编辑以下注册表值：

- 项：HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 值名称：FramesPerSecond
- 值类型: DWORD
- 值数据：15

如果网络摄像头不支持指定的帧速率，应用程序默认使用 15 FPS。

有关详细信息，请参阅 HDX 网络摄像头视频压缩。

## 负载管理策略设置

负载管理部分包含用于在交付 Windows 多会话操作系统计算机的服务器之间启用和配置负载管理的策略设置。

有关计算负载评估器索引的信息，请参阅 CTX202150。

### 并发登录容忍度

此设置指定服务器可接受的最大并发登录数。

默认情况下，此值设置为 2。

启用此设置后，负载平衡会尝试避免在同一时间在服务器 VDA 上有超过指定数量的活动登录。但是，此限制并未严格执行。要强制执行此限制（并导致超过指定数量的并发登录失败），请创建以下注册表项:

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit 类型: DWORD 值: 1

### CPU 使用率

此设置指定 CPU 使用率的百分比级别，服务器在此级别报告满负载。启用后，服务器报告满负载的默认值为 90%。

默认情况下，此设置已禁用，CPU 使用率将从负载计算中排除。

### CPU 使用率排除进程优先级

> **注意：**
>
> 在由 Workspace Environment Management 管理计算机的场景中，将此设置与 CPU 优先级设置一起使用可能会产生意外结果。如果您选择使用 CPU 优先级设置，建议您禁用此设置。

此设置指定优先级级别，在此级别，进程的 CPU 使用率将从 CPU 使用率负载索引中排除。

默认情况下，此值设置为 **低于正常** 或 **低**。

### 磁盘使用情况

此设置指定磁盘队列长度，在此长度下，服务器报告 75% 的满负载。启用后，磁盘队列长度的默认值为 8。

默认情况下，此设置已禁用，磁盘使用率将从负载计算中排除。

### 最大会话数

此设置指定服务器可托管的最大会话数。启用后，服务器可托管的最大会话数的默认设置为 250。

默认情况下，此设置处于启用状态。

### 内存使用情况

此设置指定服务器报告满负载时的内存使用量级别（以百分比表示）。启用后，服务器报告满负载的默认值为 90%。

默认情况下，此设置处于禁用状态，内存使用量不计入负载计算。

### 内存使用量基本负载

此设置指定了基本操作系统的内存使用量近似值，并以 MB 为单位定义了服务器被视为零负载的内存使用量。

默认情况下，此值设置为 768 MB。

# 配置文件管理策略设置

## 高级策略设置

### 访问锁定文件时的重试次数

设置访问锁定文件时的重试次数。

如果此策略已禁用，则使用默认值五次重试。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则使用默认值。

### 注销时处理 Internet Cookie 文件

某些部署会留下 `Index.dat` 未引用的额外 Internet Cookie。持续浏览后文件系统中留下的额外 Cookie 可能导致配置文件膨胀。此策略允许您启用 Profile Management 以强制处理 Index.dat 并删除额外 Cookie。此策略会增加注销时间，因此仅在遇到此问题后才启用它。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处和 .ini 文件中均未配置此策略，则不处理 Index.dat。

### 禁用自动配置

Profile Management 会检查任何 Citrix Virtual Desktops™ 环境（例如是否存在个人 vDisk），并相应地配置组策略。仅调整处于“未配置”状态的 Profile Management 策略，因此您所做的任何自定义都将保留。

此策略可加快部署速度并简化优化。您无需配置此策略。但是，在执行以下操作之一时，您可以禁用自动配置：

- 升级以保留早期版本中的设置
- 故障排除

您可以将自动配置视为一个动态配置检查器，它根据运行时环境自动配置默认策略设置。它消除了手动配置设置的需要。运行时环境包括：

- Windows 操作系统
- Windows 操作系统版本
- Citrix 虚拟桌面的存在
- 个人 vDisk 的存在

如果环境发生变化，自动配置可能会更改以下策略：

- 活动回写

- 始终缓存
- 注销时删除本地缓存的配置文件
- 删除缓存配置文件前的延迟
- 配置文件流技术

有关不同操作系统上策略的默认状态，请参阅下表：

| | 多会话操作系统 | 单会话操作系统 |
|---|---|---|
| 活动回写 | 启用 | 如果正在使用 Personal vDisk，则*禁用*；否则，启用。 |
| 始终缓存 | 已禁用 | 如果正在使用 Personal vDisk，则*禁用*；否则，启用。 |
| 注销时删除本地缓存的配置文件 | 启用 | 如果出现以下情况之一，则为*禁用*：正在使用 Personal vDisk、已分配 Citrix Virtual Desktops 或未安装 Citrix Virtual Desktops；否则，启用。 |
| 删除缓存配置文件前的延迟 | 0 秒 | 如果用户更改不是持久性的，则为 60 秒；否则，为 0 秒。 |
| 配置文件流技术 | 启用 | 如果正在使用 Personal vDisk，则*禁用*；否则，启用。 |

但是，如果禁用自动配置，则上述所有策略都默认为**禁用**。

> **重要提示：**
>
> Personal vDisk 已弃用。有关详细信息，请参阅删除 PVD、AppDisks 和不受支持的主机。

> 从 Profile Management 1909 开始，您可以在 Windows 10（版本 1607 及更高版本）和 Windows Server 2016 及更高版本上获得改进的“开始”菜单体验。此改进是通过自动配置以下策略实现的：

- 将 `Appdata\Local\Microsoft\Windows\Caches` 和 `Appdata\Local\Packages` 添加到**要镜像的文件夹**。
- 将 `Appdata\Local\Microsoft\Windows\UsrClass.Dat*` 添加到**要同步的文件**。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处和 .ini 文件中均未配置此设置，则自动配置处于启用状态。在这种情况下，如果环境发生变化，Profile Management 设置可能会随之更改。

#### 如果遇到问题，注销用户

允许您指定 Profile Management 在遇到问题时是否注销用户。

如果此策略被禁用或未配置，Profile Management 会在遇到问题时为用户提供临时配置文件。例如，用户存储不可用。

如果启用此策略，将显示错误消息并注销用户。此设置可以简化问题的故障排除。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处和 .ini 文件中均未配置此设置，则提供临时配置文件。

#### 客户体验改善计划

默认情况下，客户体验改善计划处于启用状态，通过收集匿名统计数据和使用数据来帮助提高 Citrix® 产品的质量和性能。

如果此处未配置此设置，则使用 .ini 文件中的值。

#### 启用 Outlook 搜索索引漫游

通过自动漫游 Outlook 搜索数据以及用户配置文件，允许基于用户的 Outlook 搜索体验。此功能需要在用户存储中额外空间来存储 Outlook 的搜索索引。

注销然后重新登录以使此策略生效。

#### Outlook 搜索索引数据库 – 备份和还原

允许您指定当“启用 Outlook 搜索索引漫游”策略启用时，Profile Management 在登录期间执行的操作。

如果此策略已启用，Profile Management 会在每次登录时成功装载数据库时备份搜索索引数据库。Profile Management 将备份视为搜索索引数据库的良好副本。当由于数据库损坏而导致装载搜索索引数据库的尝试失败时，Profile Management 会将搜索索引数据库还原到上次已知的良好副本。

> 注意：
>
> Profile Management 在成功保存新备份后删除以前保存的备份。备份会占用可用的 VHDX 存储空间。

#### 为配置文件容器启用多会话回写

在多会话场景中为配置文件容器启用回写。如果启用，所有会话中的更改都将回写到配置文件容器。否则，只有第一个会话中的更改会被保存，因为在配置文件容器中，只有第一个会话处于读/写模式。Citrix Profile Management 配置文件容器从 Citrix Profile Management 2103 开始支持。FSLogix Profile Container 从 Citrix Profile Management 2003 开始支持。

要将此策略用于 FSLogix Profile Container，请确保满足以下先决条件：

- FSLogix Profile Container 功能已安装并启用。
- 在 FSLogix 中，配置文件类型设置为 **尝试读写配置文件并回退到只读**。

#### 复制用户存储

允许您在每次登录和注销时将用户存储复制到多个路径，除了**用户存储路径**策略指定的路径之外。要将会话期间修改的文件和文件夹同步到用户存储，请启用主动回写。此功能目前不支持完整的容器解决方案。启用此策略会增加系统 I/O 并可能延长注销时间。

#### 启用基于凭据的用户存储访问

默认情况下，Citrix Profile Management 模拟当前用户访问用户存储。如果您不希望 Profile Management 在访问用户存储时模拟当前用户，请启用此功能。您可以将用户存储放在当前用户无权访问的存储库（例如 Azure 文件）中。

为确保 Profile Management 可以访问用户存储，请将配置文件存储服务器的凭据保存在 Workspace Environment Management™ (WEM) 或 Windows 凭据管理器中。建议您使用 Workspace Environment Management，以消除为运行 Profile Management 的每台计算机配置相同凭据的需要。如果您使用 Windows 凭据管理器，请使用本地系统帐户安全地保存凭据。

> **注意：**

> 为确保保留 NTFS 权限，您必须将整个配置文件放入配置文件容器中。

> 如果此处未配置此设置，则使用 .ini 文件中的值。如果此处和 .ini 文件中均未配置此设置，则默认禁用此设置。

#### 自定义 VHDX 文件的存储路径

Profile Management 提供以下基于 VHDX 的策略：配置文件容器、Outlook 搜索索引漫游和加速文件夹镜像。默认情况下，VHDX 文件存储在用户存储中。此策略允许您指定单独的路径来存储它们。

#### 在会话中自动重新连接 VHDX 磁盘

启用此策略后，Profile Management 可确保基于 VHDX 的策略具有高水平的稳定性。默认情况下，此策略处于启用状态。

启用此策略后，Profile Management 会监视 VHDX 策略正在使用的 VHDX 磁盘。如果任何磁盘被分离，Profile Management 会自动重新连接该磁盘。

### 基本策略设置

本部分包含与 Profile Management 的基本配置相关的策略设置。

#### 启用配置文件管理

默认情况下，为方便部署，Profile Management 不处理登录或注销。仅在执行所有其他设置任务并测试 Citrix® 用户配置文件在您的环境中的性能后，才启用 Profile Management。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则 Profile Management 不以任何方式处理 Windows 用户配置文件。

#### 已处理的组

可以使用计算机本地组和域组（本地、全局和通用）。域组必须采用以下格式指定：DOMAIN NAME\GROUP NAME。

如果此处配置了此策略，则 Profile Management 仅处理这些用户组的成员。如果禁用此策略，则 Profile Management 处理所有用户。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则处理所有用户组的成员。

#### 排除的组

您可以使用计算机本地组和域组（本地、全局和通用）来阻止处理特定的用户配置文件。以 DOMAIN NAME\ GROUP NAME 形式指定域组。

如果此处配置了此设置，则 Profile Management 将排除这些用户组的成员。如果禁用此设置，则 Profile Management 不排除任何用户。如果此处未配置此设置，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此设置，则不排除任何组的成员。

**处理本地管理员的登录**

指定是否处理 BUILTIN\Administrators 组成员的登录。如果在多会话操作系统（例如 Citrix Virtual Apps 环境）上禁用或未配置此策略，则 Profile Management 假定必须处理域用户的登录，但不处理本地管理员的登录。在单会话操作系统（例如 Citrix Virtual Desktops 环境）上，将处理本地管理员登录。此策略允许具有本地管理员权限的域用户（通常是分配了虚拟桌面的 Citrix Virtual Desktops 用户）绕过任何处理、登录并对遇到 Profile Management 问题的桌面进行故障排除。

注意：域用户的登录可能会受到组成员身份施加的限制，通常是为了确保符合产品许可。 如果禁用此策略，则 Profile Management 不处理本地管理员的登录。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不处理管理员。

**用户存储路径**

设置目录（用户存储）的路径，用户设置（注册表更改和同步文件）将保存到该目录中。

路径可以是：

- 相对路径。它必须相对于主目录（通常在 Active Directory 中配置为用户的 #homeDirectory# 属性）。
- UNC 路径。它通常指定服务器共享或 DFS 命名空间。
- 已禁用或未配置。在这种情况下，假定值为 #homeDirectory#\Windows。

此策略可以使用以下类型的变量：

- 用百分号括起来的系统环境变量（例如，%ProfVer%）。系统环境变量通常需要额外设置。
- 用哈希符号括起来的 Active Directory 用户对象属性（例如，#sAMAccountName#）。
- Profile Management 变量。有关详细信息，请参阅 Profile Management 变量产品文档。

用户环境变量不能使用，`%username%` 和 `%userdomain%` 除外。您还可以创建自定义属性来完整定义组织变量，例如位置或用户。属性区分大小写。

示例：

- `\\server\share#sAMAccountName#` 将用户设置存储到 UNC 路径 `\\server\share\JohnSmith`（如果 #sAMAccountName# 对于当前用户解析为 JohnSmith）
- `\\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!` 可能会扩展为 `\\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64`

重要提示：无论您使用何种属性或变量，请检查此策略是否扩展到包含 NTUSER.DAT 的文件夹的上一级文件夹。例如，如果此文件包含在 `\\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile` 中，请将用户存储路径设置为 `\\server\profiles$\JohnSmith.Finance\Win8x64`（而不是 \UPM_Profile 子文件夹）。

有关在指定用户存储路径时使用变量的详细信息，请参阅以下主题：

- 在多个文件服务器上共享 Citrix 用户配置文件
- 在 OU 内部和跨 OU 管理配置文件
- 使用 Profile Management 实现高可用性和灾难恢复

如果“用户存储路径”被禁用，用户设置将保存在主目录的 Windows 子目录中。

如果此策略被禁用，用户设置将保存在主目录的 Windows 子目录中。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则使用主驱动器上的 Windows 目录。

**迁移用户存储**

指定以前保存用户设置（注册表更改和同步文件）的文件夹路径（您以前使用的用户存储路径）。

如果配置了此设置，则存储在以前用户存储中的用户设置将迁移到“用户存储路径”策略中指定的当前用户存储。

该路径可以是绝对 UNC 路径，也可以是相对于主目录的路径。

在这两种情况下，您都可以使用以下类型的变量：用百分号括起来的系统环境变量和用井号括起来的 Active Directory 用户对象属性。

示例：

- 文件夹 `Windows\%ProfileVer%` 将用户设置存储在用户存储的名为 `Windows\W2K3` 的子文件夹中（如果 %ProfileVer% 是解析为 W2K3 的系统环境变量）。
- `\\server\share#SAMAccountName#` 将用户设置存储到 UNC 路径 `\\server\share\<JohnSmith>`（如果 `#SAMAccountName#` 为当前用户解析为 JohnSmith）。

在路径中，您可以使用用户环境变量，但 `%username%` 和 `%userdomain%` 除外。

如果此设置被禁用，用户设置将保存在当前用户存储中。

如果此处未配置此设置，则使用 .ini 文件中的相应设置。

如果此处或 .ini 文件中未配置此设置，则用户设置将保存在当前用户存储中。

### 活动回写

已修改的文件和文件夹（但不包括注册表项）可以在会话期间、注销前同步到用户存储。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则会启用此策略。

脱机配置文件支持

此策略允许配置文件在最早可能的机会与用户存储同步。它适用于漫游的笔记本电脑或移动设备用户。当网络断开连接时，即使在重新启动或休眠后，配置文件仍会保留在笔记本电脑或设备上。当移动用户工作时，其配置文件会在本地更新，并在网络连接重新建立后最终与用户存储同步。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则会禁用脱机配置文件。

### 活动回写注册表

将此策略与“活动回写”结合使用。已修改的注册表项可以在会话期间同步到用户存储。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会禁用活动回写注册表。

### 脱机配置文件支持

启用脱机配置文件功能。此功能适用于通常会从网络中移除的计算机，通常是笔记本电脑或移动设备，而不是服务器或台式机。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会禁用脱机配置文件支持。

## 跨平台策略设置

本节包含与配置 Profile Management 跨平台设置功能相关的策略设置。

### 启用跨平台设置

默认情况下，为方便部署，跨平台设置处于禁用状态。通过启用此策略来开启处理，但仅在对该功能进行周密规划和测试后才能这样做。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不应用任何跨平台设置。

### 跨平台设置用户组

输入一个或多个 Windows 用户组。例如，您可以使用此策略仅处理来自测试用户组的配置文件。如果配置了此策略，则 Profile Management 的跨平台设置功能将仅处理这些用户组的成员。如果此策略被禁用，则该功能将处理由“已处理组”策略指定的所有用户。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则处理所有用户组。

### 跨平台定义路径

标识从下载包复制的定义文件的网络位置。此路径必须是 UNC 路径。用户必须对此位置具有读取权限，管理员必须对此位置具有写入权限。该位置必须是服务器消息块 (SMB) 或通用 Internet 文件系统 (CIFS) 文件共享。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不应用任何跨平台设置。

### 跨平台设置存储路径

设置跨平台设置存储的路径，即保存用户跨平台设置的文件夹。用户必须对此区域具有写入权限。该路径可以是绝对 UNC 路径，也可以是相对于主目录的路径。

此区域是用户存储的公共区域，其中包含多个平台共享的配置文件数据。用户必须对此区域具有写入权限。该路径可以是绝对 UNC 路径，也可以是相对于主目录的路径。您可以使用与 **用户存储路径** 相同的变量。

如果此策略被禁用，则使用路径 Windows\PM_CP。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则使用默认值。

### 创建跨平台设置的源

如果此策略在该平台的 OU 中启用，则将该平台指定为基础平台。此策略将数据从基础平台的配置文件迁移到跨平台设置存储。

每个平台自己的配置文件集都存储在单独的 OU 中。您必须决定使用哪个平台的配置文件数据来为跨平台设置存储提供种子。这称为基本平台。如果跨平台设置存储包含没有数据的定义文件，或者单平台配置文件中的缓存数据比存储中定义的数据新，则 Profile Management 会将数据从单平台配置文件迁移到存储，除非您禁用此策略。

> **重要提示：**

> 如果此策略在多个 OU 或多个用户或计算机对象中启用，则第一个用户登录的平台将成为基础配置文件。 默认情况下，此策略处于启用状态。

## 文件系统策略设置

本节包含用于设置用户配置文件中哪些文件和目录在配置文件安装系统与用户存储之间进行同步的策略。

### 排除策略设置

本节介绍用于配置用户配置文件中哪些文件和目录从同步过程中排除的策略设置。

#### 排除列表 - 文件

同步期间忽略的文件列表。文件名必须是相对于用户配置文件 (%USERPROFILE%) 的路径。文件名和文件夹名中支持通配符，但只有文件名中的通配符会递归应用。

示例：

- `Desktop\Desktop.ini` 忽略 `Desktop` 文件夹中的文件 `Desktop.ini`
- `%USERPROFILE%*.tmp` 忽略整个配置文件中所有扩展名为 `.tmp` 的文件
- `AppData\Roaming\MyApp*.tmp` 忽略配置文件某一部分中所有扩展名为 `.tmp` 的文件
- `Downloads*\a.txt` 忽略 `Downloads` 文件夹的任何直接子文件夹中的 `a.txt`。

如果禁用此策略，则不排除任何文件。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不排除任何文件。

#### 启用默认排除列表 - 目录

同步期间忽略的默认目录列表。使用此策略可以指定 GPO 排除目录，而无需手动填写。

如果禁用此策略，Profile Management 默认不排除任何目录。

如果此处未配置此策略，Profile Management 将使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，Profile Management 默认不排除任何目录。

#### 排除列表 - 目录

同步期间忽略的文件夹列表。文件夹名称必须指定为相对于用户配置文件 (%USERPROFILE%) 的路径。文件夹名称中支持通配符，但不会递归应用。

示例：

- `Desktop` 忽略用户配置文件中的 `Desktop` 文件夹

如果此策略被禁用，则不排除任何文件夹。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不排除任何文件夹。

#### 登录排除检查

此设置配置了如果用户存储中的配置文件包含排除的文件或文件夹，Profile Management 将执行的操作。

如果此设置被禁用或设置为默认值“登录时同步排除的文件或文件夹”，则当用户登录时，Profile Management 会将用户存储中排除的文件或文件夹同步到本地配置文件。

如果此设置设置为“登录时忽略排除的文件或文件夹”，则当用户登录时，Profile Management 会忽略用户存储中排除的文件或文件夹。

如果此设置设置为“登录时删除排除的文件或文件夹”，则当用户登录时，Profile Management 会删除用户存储中排除的文件或文件夹。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在此处或 .ini 文件中配置此设置，则当用户登录时，排除的文件或文件夹会从用户存储同步到本地配置文件。

#### 大文件处理 - 要创建为符号链接的文件

为了提高登录性能并处理大文件，Profile Management 会创建符号链接，而不是复制此列表中的文件。

您可以在引用文件的策略中使用通配符；例如，`!ctx_localappdata!\Microsoft\Outlook*.OST`。

为了处理 Microsoft Outlook 的脱机文件夹文件 (`*.ost`)，请确保未将 **Outlook** 文件夹从 Profile Management 中排除。

这些文件无法在多个会话中同时访问。

### 同步策略设置

**同步**部分介绍了策略设置，用于指定用户配置文件中的哪些文件和文件夹在安装配置文件的系统与用户存储之间进行同步。

#### 要同步的目录

默认情况下，Profile Management 会在安装用户配置文件的系统与用户存储之间同步用户配置文件。如果您将某个文件夹从同步中排除，此策略允许您将该排除文件夹的子文件夹重新包含到同步中。

此列表中的路径必须相对于用户配置文件。支持文件夹名称中的通配符，但不会递归应用。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则仅同步用户配置文件中未排除的文件夹。

#### 要同步的文件

默认情况下，Profile Management 会在安装用户配置文件的系统与用户存储之间同步用户配置文件。如果您将某个文件夹从同步中排除，此策略允许您将该排除文件夹内的文件重新包含到同步中。

此列表中的路径必须相对于用户配置文件。文件名和文件夹名中都支持通配符，但只有文件名中的通配符会递归应用。通配符不能嵌套。

示例：

- `AppData\Local\Microsoft\Office\Access.qat` 指定了默认配置中排除的文件夹下的文件
- `AppData\Local\MyApp*.cfg` 指定了配置文件文件夹 `AppData\Local\MyApp` 及其子文件夹中所有扩展名为 `.cfg` 的文件

禁用此策略与启用此策略并配置空列表的效果相同。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则仅同步用户配置文件中未排除的文件。

#### 要镜像的文件夹

此策略可帮助您解决涉及任何事务性文件夹（也称为引用文件夹）的问题。该文件夹包含相互依赖的文件，其中一个文件引用其他文件。

镜像文件夹使 Profile Management 能够将事务性文件夹及其内容作为一个单一实体进行处理，从而避免配置文件膨胀。例如，您可以镜像 **Internet Explorer cookies** 文件夹，以便 Index.dat 与其索引的 Cookie 同步。在这种情况下，“后写入者优先”。因此，镜像文件夹中在多个会话中修改的文件将被最后一次更新覆盖，从而导致配置文件更改丢失。

例如，考虑用户浏览 Internet 时 Index.dat 如何引用 Cookie。如果用户有两个 Internet Explorer 会话，每个会话位于不同的服务器上，并且他们在每个会话中访问不同的站点，则来自每个站点的 Cookie 将添加到相应的服务器。当用户从第一个会话注销时（或者在会话中途，如果配置了活动回写功能），第二个会话中的 Cookie 必须替换第一个会话中的 Cookie。然而，它们会被合并，并且 Index.dat 中对 Cookie 的引用会过时。在新会话中进一步浏览会导致重复合并和 Cookie 文件夹膨胀。

每次用户注销时，通过用上次会话中的 Cookie 覆盖 Cookie，镜像 Cookie 文件夹可以解决此问题。因此，Index.dat 保持最新。

如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不镜像任何文件夹。

#### 加速文件夹镜像

启用此策略和“**要镜像的文件夹**”策略后，Profile Management 会将镜像文件夹存储在基于 VHDX 的虚拟磁盘上。它会在登录期间附加虚拟磁盘，并在注销期间分离虚拟磁盘。启用此策略可消除在用户存储和本地配置文件之间复制文件夹的需要，并加速文件夹镜像。

### 文件夹重定向策略设置

本节包含策略设置，用于指定是否将配置文件中常见的文件夹重定向到共享网络位置。

#### 授予管理员访问权限

此设置允许管理员访问用户重定向文件夹的内容。

> **注意：**
>
> 此设置向对域具有完全不受限制访问权限的管理员授予权限。

默认情况下，此设置处于禁用状态，用户被授予对其重定向文件夹内容的独占访问权限。

#### 包含域名

此设置允许将 `%userdomain%` 环境变量包含在重定向文件夹的 UNC 路径中。

默认情况下，此设置处于禁用状态，并且不将 `%userdomain%` 环境变量包含在重定向文件夹的 UNC 路径中。

### AppData(Roaming) 策略设置

本部分包含用于将 **AppData(Roaming)** 文件夹的内容重定向到共享网络位置的策略设置。

#### APPDATA(ROAMING) 路径

此设置指定将 **AppData(Roaming)** 文件夹的内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

#### APPDATA(ROAMING) 的重定向设置

此设置指定如何重定向 **AppData(Roaming)** 文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

### 联系人策略设置

本节包含用于将**联系人**文件夹内容重定向到共享网络位置的策略设置。

#### 联系人路径

此设置指定**联系人**文件夹内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

#### 联系人重定向设置

此设置指定如何重定向**联系人**文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

### 桌面策略设置

本节包含用于将 `Desktop` 文件夹的内容重定向到共享网络位置的策略设置。

#### 桌面路径

此设置指定将 **桌面** 文件夹的内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

#### 桌面的重定向设置

此设置指定如何重定向 **桌面** 文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

### 文档策略设置

本节包含用于将**文档**文件夹的内容重定向到共享网络位置的策略设置。

#### 文档路径

此设置指定**文档**文件夹中的文件重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

**文档路径**设置必须启用，不仅用于将文件重定向到**文档**文件夹，还用于将文件重定向到**音乐**、**图片**和**视频**文件夹。

#### 文档的重定向设置

此设置指定如何重定向**文档**文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

要控制如何重定向**文档**文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到“文档路径”策略设置中指定的 UNC 路径。
- 重定向到用户主目录。将内容重定向到用户主目录，通常配置为 Active Directory 中用户的 #homeDirectory# 属性。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

### 下载策略设置

本节包含用于将“**下载**”文件夹的内容重定向到共享网络位置的策略设置。

#### 下载路径

此设置指定“**下载**”文件夹中的文件重定向到的网络位置。

默认情况下，此设置为禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

#### 下载的重定向设置

此设置指定如何重定向“**下载**”文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

### 收藏夹策略设置

本节包含用于将 **收藏夹** 文件夹的内容重定向到共享网络位置的策略设置。

#### 收藏夹路径

此设置指定将 **收藏夹** 文件夹的内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

#### 收藏夹的重定向设置

此设置指定如何重定向 **收藏夹** 文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

### 音乐策略设置

本节包含用于将“**音乐**”文件夹的内容重定向到共享网络位置的策略设置。

#### 音乐路径

此设置指定“**音乐**”文件夹内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，Profile Management 不会重定向指定的文件夹。

#### 音乐的重定向设置

此设置指定如何重定向“**音乐**”文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

要控制如何重定向“**音乐**”文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到“音乐路径”策略设置中指定的 UNC 路径。
- 相对于“文档”文件夹重定向。将内容重定向到相对于“文档”文件夹的文件夹。

要将内容重定向到相对于“**文档**”文件夹的文件夹，必须启用“**文档路径**”设置。

如果此处未配置此设置，Profile Management 不会重定向指定的文件夹。

### 图片策略设置

本节包含用于将“**图片**”文件夹的内容重定向到共享网络位置的策略设置。

#### 图片路径

此设置指定“**图片**”文件夹的内容重定向到的网络位置。

默认情况下，此设置为禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

#### 图片重定向设置

此设置指定如何重定向“**图片**”文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

要控制如何重定向“**图片**”文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到“图片路径”策略设置中指定的 UNC 路径。
- 相对于“文档”文件夹重定向。将内容重定向到相对于“文档”文件夹的文件夹。

要将内容重定向到相对于“**文档**”文件夹的文件夹，必须启用“**文档路径**”设置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

### 搜索策略设置

本节包含用于将 **搜索** 文件夹的内容重定向到共享网络位置的策略设置。

#### 搜索的重定向设置

此设置指定如何重定向 **搜索** 文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，Profile Management 不会重定向指定的文件夹。

#### 搜索路径

此设置指定重定向 **搜索** 文件夹内容的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，Profile Management 不会重定向指定的文件夹。

### 开始菜单策略设置

本节包含用于将“**开始菜单**”文件夹内容重定向到共享网络位置的策略设置。

#### 开始菜单的重定向设置

此设置指定如何重定向“**开始菜单**”文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

#### 开始菜单路径

此设置指定“**开始菜单**”文件夹内容重定向到的网络位置。

默认情况下，此设置为禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

### 视频策略设置

本节包含用于将“**视频**”文件夹内容重定向到共享网络位置的策略设置。

#### 视频重定向设置

此设置指定如何重定向“**视频**”文件夹的内容。

默认情况下，内容将重定向到 UNC 路径。

要控制如何重定向“**视频**”文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到“视频路径”策略设置中指定的 UNC 路径。
- 相对于“文档”文件夹重定向。将内容重定向到相对于“文档”文件夹的文件夹。

要将内容重定向到相对于“**文档**”文件夹的文件夹，必须启用“**文档路径**”设置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

#### 视频路径

此设置指定“**视频**”文件夹内容重定向到的网络位置。

默认情况下，此设置处于禁用状态，并且未指定任何位置。

如果此处未配置此设置，则 Profile Management 不会重定向指定的文件夹。

## 日志策略设置

本部分包含配置 Profile Management 日志记录的策略设置。

### 活动目录操作

此设置启用或禁用 Active Directory 中执行的操作的详细日志记录。

默认情况下，此设置为禁用状态。

启用此设置时，请确保同时启用**启用日志记录**设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会记录错误和一般信息。

### 常见信息

此设置启用或禁用常见信息的详细日志记录。

默认情况下，此设置为禁用状态。

启用此设置时，请确保同时启用**启用日志记录**设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会记录错误和一般信息。

### 常见警告

此设置启用或禁用常见警告的详细日志记录。

默认情况下，此设置为禁用。

启用此设置时，请确保同时启用“**启用日志记录**”设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会记录错误和一般信息。

### 启用日志记录

此设置启用或禁用调试（详细日志记录）模式下的 Profile Management 日志记录。在调试模式下，详细的状态信息会记录在位于“%SystemRoot%\System32\Logfiles\UserProfileManager”的日志文件中。

默认情况下，此设置为禁用，并且仅记录错误。

Citrix® 建议仅在对 Profile Management 进行故障排除时启用此设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则仅记录错误。

### 文件系统操作

此设置启用或禁用文件系统中执行的操作的详细日志记录。

默认情况下，此设置为禁用。

启用此设置时，请确保同时启用“**启用日志记录**”设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会记录错误和一般信息。

### 文件系统通知

此设置启用或禁用文件系统通知的详细日志记录。

默认情况下，此设置为禁用。

启用此设置时，请确保也启用了“**启用日志记录**”设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会记录错误和一般信息。

**注销**

此设置启用或禁用用户注销的详细日志记录。

默认情况下，此设置为禁用。

启用此设置时，请确保也启用了“**启用日志记录**”设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会记录错误和一般信息。

**登录**

此设置启用或禁用用户登录的详细日志记录。

默认情况下，此设置为禁用。

启用此设置时，请确保同时启用**启用日志记录**设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会记录错误和常规信息。

**日志文件的最大大小**

此设置指定 Profile Management 日志文件允许的最大大小（以字节为单位）。

默认情况下，此值设置为 1048576 字节 (1 MB)。

如果您有足够的磁盘空间，Citrix 建议将此文件的大小增加到 5 MB 或更大。如果日志文件超出最大大小，则会删除现有文件备份 (.bak)，日志文件将重命名为 .bak，并创建一个新的日志文件。

日志文件在 `%SystemRoot%\System32\Logfiles\UserProfileManager` 中创建。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则使用默认值。

**日志文件路径**

此设置指定用于保存 Profile Management 日志文件的备用路径。

默认情况下，此设置处于禁用状态，日志文件保存在默认位置：%SystemRoot%\System32\Logfiles\UserProfileManager。

该路径可以指向本地驱动器或远程网络驱动器 (UNC 路径)。远程路径在大型分布式环境中可能很有用，但它们可能会产生大量网络流量，这可能不适合日志文件。对于具有持久性硬盘的预配虚拟机，请将本地路径设置为该驱动器。这可确保计算机重新启动时日志文件得以保留。对于没有持久性硬盘的虚拟机，设置 UNC 路径可让您保留日志文件，但计算机的系统帐户必须对 UNC 共享具有写入权限。对于由脱机配置文件功能管理的任何笔记本电脑，请使用本地路径。

如果日志文件使用 UNC 路径，Citrix 建议对日志文件文件夹应用适当的访问控制列表，以确保只有授权的用户或计算机帐户才能访问存储的文件。

如果此处未配置此设置，将使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，将使用默认位置 %SystemRoot%\System32\Logfiles\UserProfileManager。

**个性化用户信息**

此设置启用或禁用个性化用户信息的详细日志记录。

默认情况下，此设置处于禁用状态。

启用此设置时，请确保“**启用日志记录**”设置也已启用。

如果此处未配置此设置，将使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，将记录错误和常规信息。

**登录和注销时的策略值**

此设置启用或禁用用户登录和注销时策略值的详细日志记录。

默认情况下，此设置处于禁用状态。

启用此设置时，请确保“**启用日志记录**”设置也已启用。

如果此处未配置此设置，将使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会记录错误和一般信息。

**注册表操作**

此设置启用或禁用对注册表中执行的操作进行详细日志记录。

默认情况下，此设置为禁用状态。

启用此设置时，请确保同时启用“**启用日志记录**”设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会记录错误和一般信息。

#### 注销时的注册表差异

此设置启用或禁用对用户注销时注册表中的任何差异进行详细日志记录。

默认情况下，此设置为禁用状态。

启用此设置时，请确保同时启用“**启用日志记录**”设置。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会记录错误和一般信息。

### 配置文件处理策略设置

本部分包含指定 Profile Management 如何处理用户配置文件的策略设置。

#### 删除缓存配置文件前的延迟

此设置指定在注销时 Profile Management 删除本地缓存配置文件之前，可选的延迟时间（以分钟为单位）。

值为 0 表示在注销过程结束时立即删除配置文件。Profile Management 每分钟检查一次注销情况，因此值为 60 可确保在用户注销后一到两分钟内删除配置文件（具体取决于上次检查发生的时间）。如果您知道某个进程在注销期间会保持文件或用户注册表配置单元处于打开状态，则延长延迟会很有用。对于大型配置文件，这还可以加快注销速度。

默认情况下，此设置设为 0，Profile Management 会立即删除本地缓存的配置文件。

启用此设置时，请确保“在注销时删除本地缓存的配置文件”也已启用。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会立即删除配置文件。

#### 在注销时删除本地缓存的配置文件

此设置指定用户注销后是否删除本地缓存的配置文件。

启用此设置后，用户的本地配置文件缓存会在其注销后删除。Citrix® 建议为终端服务器启用此设置。

默认情况下，此设置处于禁用状态，用户的本地配置文件缓存在其注销后会保留。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则不会删除缓存的配置文件。

### 本地配置文件冲突处理

此设置配置了当用户配置文件同时存在于用户存储和本地 Windows 用户配置文件（而非 Citrix 用户配置文件）中时，Profile Management 的行为方式。

默认情况下，Profile Management 使用本地 Windows 配置文件，但不会对其进行任何更改。

要控制 Profile Management 的行为方式，请选择以下选项之一：

- 使用本地配置文件。Profile Management 使用本地配置文件，但不会对其进行任何更改。
- 删除本地配置文件。Profile Management 删除本地 Windows 用户配置文件，然后从用户存储中导入 Citrix 用户配置文件。
- 重命名本地配置文件。Profile Management 重命名本地 Windows 用户配置文件（用于备份），然后从用户存储中导入 Citrix 用户配置文件。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则使用现有本地配置文件。

### 现有配置文件的迁移

此设置指定了如果用户在用户存储中没有当前配置文件，则在登录期间迁移到用户存储的配置文件类型。

如果用户在用户存储中没有配置文件，Profile Management 可以在登录期间“即时”迁移现有配置文件。之后，Profile Management 会在当前会话以及配置了相同用户存储路径的任何其他会话中使用用户存储配置文件。

默认情况下，本地配置文件和漫游配置文件都会在登录期间迁移到用户存储。

要指定在登录期间迁移到用户存储的配置文件类型，请选择以下选项之一：

- 本地配置文件和漫游配置文件
- 本地
- 漫游
- 无（已禁用）

如果选择**无**，系统将使用现有 Windows 机制创建配置文件，如同在未安装 Profile Management 的环境中一样。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则会迁移现有的本地配置文件和漫游配置文件。

### 现有应用程序配置文件的自动迁移

此设置启用或禁用现有应用程序配置文件在不同操作系统之间的自动迁移。应用程序配置文件包括 `AppData` 文件夹中的应用程序数据和 `HKEY_CURRENT_USER\SOFTWARE` 下的注册表项。此设置在您希望在不同操作系统之间迁移应用程序配置文件的情况下非常有用。

例如，假设您将操作系统 (OS) 从 Windows 10 版本 1803 升级到 Windows 10 版本 1809。如果启用此设置，则在每个用户首次登录时，Profile Management 会自动将现有应用程序设置迁移到 Windows 10 版本 1809。因此，`AppData` 文件夹中的应用程序数据和 HKEY_CURRENT_USER\SOFTWARE 下的注册表项将得到迁移。

如果存在多个现有应用程序配置文件，Profile Management 将按以下优先级顺序执行迁移：

1. 相同操作系统类型的配置文件（单会话操作系统到单会话操作系统，以及多会话操作系统到多会话操作系统）。
2. 相同 Windows 操作系统系列的配置文件；例如，Windows 10 到 Windows 10，或 Windows Server 2016 到 Windows Server 2016）。
3. 早期版本操作系统的配置文件；例如，Windows 7 到 Windows 10，或 Windows Server 2012 到 Windows 2016。
4. 最接近的操作系统配置文件。

**注意：** 您必须通过在用户存储路径中包含变量“!CTX_OSNAME!”来指定操作系统的短名称。这样做可让 Profile Management 定位现有应用程序配置文件。

如果此处未配置此设置，则使用 .ini 文件中的设置。

如果此处或 .ini 文件中未配置此设置，则默认情况下禁用此设置。

### 模板配置文件路径

此设置指定了您希望 Profile Management 用作模板来创建用户配置文件的路径。

指定的路径必须是包含 NTUSER.DAT 注册表文件以及模板配置文件所需的任何其他文件夹和文件的文件夹的完整路径。

注意：路径中不要包含 NTUSER.DAT。例如，对于文件 `\\myservername\myprofiles\template\ntuser.dat`，将位置设置为 `\\myservername\myprofiles\template`。

使用绝对路径，可以是 UNC 路径，也可以是本地计算机上的路径。例如，使用后者可以在 Citrix Provisioning™ Services 映像上永久指定模板配置文件。不支持相对路径。

注意：此设置不支持扩展 Active Directory 属性、系统环境变量或 `%USERNAME%` 和 `%USERDOMAIN%` 变量。

默认情况下，此设置处于禁用状态，新用户配置文件是在用户首次登录的设备上从默认用户配置文件创建的。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则不使用任何模板。

**模板配置文件覆盖本地配置文件**

此设置允许模板配置文件在创建用户配置文件时覆盖本地配置文件。

如果用户没有 Citrix 用户配置文件，但存在本地 Windows 用户配置文件，则默认情况下使用本地配置文件（如果未禁用，则会迁移到用户存储）。启用此策略设置允许模板配置文件在创建用户配置文件时覆盖所使用的本地配置文件。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则不使用任何模板。

**模板配置文件覆盖漫游配置文件**

此设置允许模板配置文件在创建用户配置文件时覆盖漫游配置文件。

如果用户没有 Citrix 用户配置文件，但存在漫游 Windows 用户配置文件，则默认情况下使用漫游配置文件（如果未禁用，则会迁移到用户存储）。启用此策略设置后，模板配置文件可以在创建用户配置文件时覆盖所使用的漫游配置文件。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则不使用任何模板。

**用作所有登录的 Citrix 强制配置文件的模板配置文件**

此设置允许 Profile Management 将模板配置文件用作创建所有用户配置文件的默认配置文件。

默认情况下，此设置为禁用状态，新用户配置文件是根据用户首次登录的设备上的默认用户配置文件创建的。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则不使用任何模板。

## 配置文件容器策略设置

### 配置文件容器

与用户配置文件关联的大型文件夹会导致登录缓慢。Citrix Profile Management 提供了一种基于 VHDX 的配置文件解决方案，可让您指定要包含在配置文件磁盘（VHDX 文件）中的文件夹。此解决方案通过将指定文件夹映射到存储在网络上的配置文件磁盘来减少登录时间。配置文件容器在登录期间附加包含这些文件夹的配置文件磁盘，从而无需将文件夹副本保存到本地配置文件。这样做可以缩短登录时间。

### 为配置文件容器启用本地缓存

此策略为 Citrix Profile Management 配置文件容器启用本地缓存支持。如果策略设置为**已启用**，则每个本地配置文件都充当其 Citrix Profile Management 配置文件容器的本地缓存。如果正在使用配置文件流技术，则按需创建本地缓存文件。否则，它们会在用户登录期间创建。要使用本地缓存功能，请将整个用户配置文件放入其 Citrix Profile Management 配置文件容器中。

### 要从配置文件容器中排除的文件夹

要从 Citrix Profile Management 配置文件容器中排除的文件夹列表。

### 要包含在配置文件容器中的文件夹

当其父文件夹被排除时，要保留在 Citrix Profile Management 配置文件容器中的文件夹列表。

此列表中的文件夹必须是排除文件夹的子文件夹。否则，此设置不起作用。

### 要包含在配置文件容器中的文件

要包含在 Citrix Profile Management 配置文件容器中的文件列表。

此列表中的文件必须位于排除文件夹内。否则，此设置不起作用。

### 要从配置文件容器中排除的文件

要从 Citrix Profile Management 配置文件容器中排除的文件列表。

## 注册表策略设置

本节包含指定哪些注册表项包含在配置文件管理处理中或从中排除的策略设置。

### 排除列表

注销期间忽略的 HKCU 配置单元中的注册表项列表。

示例：Software\Policies

如果禁用此策略，则不排除任何注册表项。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则不排除任何注册表项。

#### 包含列表

注销期间处理的 HKCU 配置单元中的注册表项列表。

示例：Software\Adobe。

如果启用此策略，则仅处理此列表中的项。如果禁用此策略，则处理完整的 HKCU 配置单元。如果此处未配置此策略，则使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，则处理 HKCU 中的所有内容。

#### 启用默认排除列表 - Profile Management 5.5

HKCU 配置单元中未同步到用户配置文件的注册表项的默认列表。使用此策略可以指定 GPO 排除文件，而无需手动填写。

如果禁用此策略，Profile Management 默认不排除任何注册表项。如果此处未配置此策略，Profile Management 将使用 .ini 文件中的值。如果此处或 .ini 文件中未配置此策略，Profile Management 默认不排除任何注册表项。

#### NTUSER.DAT 备份

启用 NTUSER.DAT 上一个已知良好副本的备份，并在损坏时进行回滚。

如果您未在此处配置此策略，配置文件管理将使用 .ini 文件中的值。如果您未在此处或 .ini 文件中配置此策略，配置文件管理将不会备份 NTUSER.DAT。

### 流式用户配置文件策略设置

本节包含指定 Profile Management 如何处理流式用户配置文件的策略设置。

#### 始终缓存

此设置指定用户登录后，配置文件管理是否尽快缓存流式文件。用户登录后缓存文件可节省网络带宽，从而增强用户体验。

将此设置与“**配置文件流**”设置结合使用。

默认情况下，此设置处于禁用状态，并且用户登录后不会尽快缓存流式文件。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在此处或 .ini 文件中配置此设置，则此设置处于禁用状态。

### 始终缓存大小

此设置指定流式文件大小的下限（以 MB 为单位）。用户登录后，Profile Management 会尽快缓存此大小或更大的任何文件。

默认情况下，该值设置为 0（零），并使用缓存整个配置文件功能。启用缓存整个配置文件功能后，用户登录后，Profile Management 会在后台任务中从用户存储中获取所有配置文件内容。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在此处或 .ini 文件中配置此设置，则此设置处于禁用状态。

### 配置文件流技术

此设置启用和禁用 Citrix® 流式用户配置文件功能。启用后，配置文件中包含的文件和文件夹仅在用户登录后访问时才从用户存储区获取到本地计算机。挂起区域中的注册表项和文件会立即获取。

默认情况下，配置文件流式处理处于禁用状态。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在此处或 .ini 文件中配置此设置，则此设置处于禁用状态。

### 流式用户配置文件组

此设置根据 Windows 用户组指定 OU 中哪些用户配置文件是流式的。

启用后，仅流式传输指定用户组中的用户配置文件。所有其他用户配置文件都将正常处理。

默认情况下，此设置处于禁用状态，并且 OU 中的所有用户配置文件都将正常处理。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果未在此处或 .ini 文件中配置此设置，则会处理所有用户配置文件。

### 启用配置文件流式处理排除

启用配置文件流式处理排除后，配置文件管理不会流式传输排除列表中的文件夹，并且当用户登录时，所有文件夹都会立即从用户存储区获取到本地计算机。

有关详细信息，请参阅流式传输用户配置文件。

### 暂存区锁定文件的超时

此设置指定在服务器无响应时用户存储区保持锁定状态的情况下，用户文件从挂起区域写回用户存储区的天数。这可以防止挂起区域膨胀，并确保用户存储区始终包含最新文件。

默认情况下，此设置设为 1 天。

如果此处未配置此设置，则使用 .ini 文件中的值。

如果此处或 .ini 文件中未配置此设置，则使用默认值。

## 用户个性化层策略设置

要在虚拟投递代理中启用用户层的挂载，请使用配置参数指定：

- 在网络上的何处访问用户层。
- 任何新用户层磁盘可以增长到多大。

为此，以下两个策略会出现在可用策略列表中：

- 用户层存储库路径 - 在“值”字段中输入路径，格式为“\\服务器名称或地址\文件夹名称”。
- 用户层大小（GB） - 我们建议的最小默认用户层大小为 10 GB。用户层是精简配置的磁盘，会随着空间的使用而扩展到设定的大小。用户层的大小永远不会减小。

> **注意：**
>
> 增加用户层大小会影响新的用户层并扩展现有的用户层。减小层大小仅影响新的用户层。现有用户层的大小永远不会减小。

> 有关详细信息，请参阅用户个性化层。

## 虚拟投递代理策略设置

虚拟投递代理 (VDA) 部分包含用于控制 VDA 与站点控制器之间通信的策略设置。

重要提示：如果您未使用自动更新功能，VDA 需要这些设置提供的信息才能向 Delivery Controller™ 注册。由于注册需要此信息，因此您必须使用组策略编辑器配置以下设置，除非您在 VDA 安装期间提供此信息：

- 控制器注册 IPv6 网络掩码
- 控制器注册端口
- 控制器 SID
- 控制器
- 仅使用 IPv6 控制器注册
- 站点 GUID

### 控制器注册 IPv6 网络掩码

此策略设置允许管理员将 VDA 限制为仅使用首选子网（而不是全局 IP，如果已注册）。此设置指定 VDA 将注册的 IPv6 地址和网络。VDA 将仅在与指定网络掩码匹配的第一个地址上注册。此设置仅在启用“仅使用 IPv6 控制器注册”策略设置时有效。

默认情况下，此设置为空白。

### 控制器注册端口

仅当“启用控制器自动更新”设置被禁用时，才使用此设置。

此设置指定 VDA 在使用基于注册表的注册时，用于向控制器注册的 TCP/IP 端口号。

默认情况下，端口号设置为 80。

### 控制器 SID

仅当“启用控制器自动更新”设置被禁用时，才使用此设置。

此设置指定 VDA 在使用基于注册表的注册时，用于向控制器注册的以空格分隔的控制器安全标识符 (SID) 列表。这是一个可选设置，可与“控制器”设置一起使用，以限制用于注册的控制器列表。

默认情况下，此设置为空白。

### 控制器

仅当“启用控制器自动更新”设置被禁用时，才使用此设置。

此设置指定 VDA 在使用基于注册表的注册时，用于向控制器注册的以空格分隔的控制器完全限定域名 (FQDN) 列表。这是一个可选设置，可与“控制器 SID”设置一起使用。

默认情况下，此设置为空白。

### 启用控制器自动更新

此设置使 VDA 能够在安装后自动向控制器注册。

VDA 注册后，与其注册的控制器会将当前控制器 FQDN 和 SID 列表发送给 VDA。VDA 将此列表写入持久存储。每个控制器还会每 90 分钟检查一次站点数据库以获取控制器信息；如果自上次检查以来添加或删除了控制器，或者发生了策略更改，控制器会将更新的列表发送给其注册的 VDA。VDA 将接受来自其收到的最新列表中所有控制器的连接。

默认情况下，此设置处于启用状态。

### 仅使用 IPv6 控制器注册

此设置控制 VDA 用于向控制器注册的地址形式：

- 启用后，VDA 使用计算机的 IPv6 地址向控制器注册。当 VDA 与控制器通信时，它使用以下地址顺序：全局 IP 地址、唯一本地地址 (ULA)、链路本地地址（如果没有其他 IPv6 地址可用）。
- 禁用后，VDA 使用计算机的 IPv4 地址向控制器注册并进行通信。

默认情况下，此设置为禁用状态。

### 站点 GUID

仅当“启用控制器自动更新”设置被禁用时，才使用此设置。

此设置指定 VDA 在使用基于 Active Directory 的注册时，用于向控制器注册的站点的全局唯一标识符 (GUID)。

默认情况下，此设置为空白。

### HDX™ 3D Pro 策略设置

HDX 3D Pro 部分包含用于为用户启用和配置图像质量配置工具的策略设置。该工具使用户能够通过实时调整图像质量和响应能力之间的平衡来优化可用带宽的使用。

#### 启用无损

此设置指定用户是否可以使用图像质量配置工具启用和禁用无损压缩。默认情况下，用户无法选择启用无损压缩。

当用户启用无损压缩时，图像质量会自动设置为图像配置工具中可用的最大值。默认情况下，可以根据用户设备和主机的功能使用基于 GPU 或 CPU 的压缩。

#### HDX 3D Pro 质量设置

此设置指定了在图像质量配置工具中用户可用的图像质量调整范围的最小值和最大值。

指定介于 0 到 100（含）之间的图像质量值。最大值必须大于或等于最小值。

### 监视策略设置

“监视”部分包含用于进程、资源监视和应用程序故障监视的策略设置。

这些策略的范围可以根据站点、交付组、交付组类型、组织单位和标记进行定义。

### 进程和资源监视策略

CPU、内存和进程的每个数据点都从 VDA 收集并存储在监视数据库中。从 VDA 发送数据点会占用网络带宽，而存储这些数据点会占用监视数据库中大量空间。如果您不想监视特定范围（例如，特定的交付组或组织单位）的资源数据、进程数据或两者，建议禁用此策略。

#### 启用进程监视

启用此设置以允许监视在具有 VDA 的计算机上运行的进程。CPU 和内存使用情况等统计信息将发送到监视服务。这些统计信息用于 Director 中的实时通知和历史报告。

此设置的默认值为“已禁用”。

#### 启用资源监视

启用此设置以允许监视具有 VDA 的计算机上的关键性能计数器。统计信息（例如 CPU 和内存使用情况、IOPS 和磁盘延迟数据）将发送到监视服务。这些统计信息用于 Director 中的实时通知和历史报告。

此设置的默认值为“已启用”。

#### 可扩展性

CPU 和内存数据每 5 分钟从每个 VDA 推送到数据库。进程数据（如果启用）每 10 分钟推送到数据库。IOPS 和磁盘延迟数据每 1 小时推送到数据库。

#### CPU 和内存数据

CPU 和内存数据默认**启用**。数据保留值如下（白金版许可证）：

| 数据粒度 | 天数 |
| --- | --- |
| 5 分钟数据 | 1 天 |
| 10 分钟数据 | 7 天 |
| 每小时数据 | 30 天 |
| 每日数据 | 90 天 |

#### IOPS 和磁盘延迟数据

IOPS 和磁盘延迟数据默认**启用**。数据保留值如下（白金版许可证）：

| 数据粒度 | 天数 |
| --- | --- |
| 每小时数据 | 3 天 |

| 数据粒度 | 天数 |
| --- | --- |
| 每日数据 | 90 天 |

使用数据保留设置，存储一个 VDA 一年期间的 CPU、内存、IOPS 和磁盘延迟数据大约需要 276 KB 的磁盘空间。

| 计算机数量 | 所需近似存储空间 |
| --- | --- |
| 1 | 276 KB |
| 1K | 270 MB |
| 40K | 10.6 GB |

#### 进程数据

默认情况下，进程数据处于**已禁用**状态。建议根据需要在一部分计算机上启用进程数据。进程数据的默认数据保留设置如下：

| 数据粒度 | 天数 |
| --- | --- |
| 10 分钟数据 | 1 天 |
| 每小时数据 | 7 天 |

如果使用默认保留设置启用进程数据，则进程数据在一年内将占用每个 VDA 大约 1.5 MB，每个终端服务 VDA (TS VDA) 大约 3 MB。

| 计算机数量 | VDA 所需的大致存储空间 | TS VDA 所需的大致存储空间 |
| --- | --- | --- |
| 1 | 1.5 MB | 3 MB |
| 1K | 1.5 GB | 3 GB |

**注意：**

前面提供的数字不包括索引空间。所有计算均为近似值，并根据部署情况而异。

#### 可选配置

您可以修改默认保留设置以满足您的需求。但是，这会占用额外的存储空间。通过启用以下设置，您可以提高进程利用率数据的准确性。可以启用的配置包括：

#### ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

#### ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

这些配置可以通过监控 PowerShell cmdlet 启用：Set-MonitorConfiguration

### 应用程序故障监控策略

默认情况下，“**应用程序故障**”选项卡仅显示多会话操作系统 VDA 的应用程序故障。应用程序故障监控的设置可以通过以下监控策略进行修改：

#### 启用应用程序故障监控

使用此设置可配置应用程序故障监控，以监控应用程序错误或故障（崩溃和未处理的异常），或两者兼有。 通过将“**值**”设置为“**无**”来禁用应用程序故障监控。 此设置的默认值为“仅应用程序故障”。

#### 在单会话操作系统 VDA 上启用应用程序故障监控

默认情况下，仅监控多会话操作系统 VDA 上托管的应用程序的故障。要监控单会话操作系统 VDA，请将策略设置为“**允许**”。 此设置的默认值为“**禁止**”。

#### 从故障监控中排除的应用程序列表

指定不进行故障监控的应用程序列表。 默认情况下，此列表为空。

### 用于性能分析的数据收集策略

#### 用于性能分析的 VDA 数据收集

使用此策略可启用或禁用监视服务，使其不收集用于性能分析的 VDA 性能相关指标。默认情况下，此策略为**允许**。将策略设置为**禁止**可停止从 VDA 收集数据。

### 存储规划提示

**组策略**。如果您对监视资源数据或进程数据不感兴趣，可以使用组策略关闭其中一个或两者。有关详细信息，请参阅(/zh-cn/xenapp-and-xendesktop/current-release/policies/policies-create.html)的“组策略”部分。

**数据整理**。可以修改默认数据保留设置，以提前整理数据并释放存储空间。有关整理设置的详细信息，请参阅 使用 API 访问数据 中的“数据粒度和保留”。

## 虚拟 IP 策略设置

> **重要提示：**

> Windows 10 Enterprise 多会话不支持远程桌面 IP 虚拟化 (Virtual IP)，我们也不支持在 Windows 10 Enterprise 多会话上使用虚拟 IP 或虚拟环回。

> 虚拟 IP 部分包含策略设置，用于控制会话是否拥有自己的虚拟环回地址。

### 虚拟 IP 环回支持

启用此设置后，每个会话都有自己的虚拟环回地址。禁用后，会话将没有单独的环回地址。

默认情况下，此设置为禁用状态。

### 虚拟 IP 虚拟环回程序列表

此设置指定可以使用虚拟环回地址的应用程序可执行文件。将程序添加到列表时，仅指定可执行文件名称；无需指定完整路径。

默认情况下，未指定任何可执行文件。

## 使用注册表配置 COM 端口和 LPT 端口重定向设置

在 VDA 7.0 到 7.8 版本中，COM 端口和 LPT 端口设置只能使用注册表进行配置。对于早于 7.0 的 VDA 版本以及 7.9 及更高版本的 VDA，这些设置可在 Studio 中配置。有关详细信息，请参阅端口重定向策略设置和带宽策略设置。

COM 端口和 LPT 端口重定向的策略设置位于 VDA 映像或计算机上的 HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated 下。

要启用 COM 端口和 LPT 端口重定向，请按如下所示添加类型为 REG_DWORD 的新注册表项：

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

| 注册表项 | 描述 | 允许的值 |
| --- | --- | --- |
| AllowComPortRedirection | 允许或禁止 COM 端口重定向 | 1（允许）或 0（禁止） |
| LimitComBw | COM 端口重定向通道的带宽限制 | 数值 |
| LimitComBWPercent | COM 端口重定向通道的带宽限制，占总会话带宽的百分比 | 0 到 100 之间的数值 |

| 注册表项 | 描述 | 允许的值 |
| --- | --- | --- |
| AutoConnectClientComPorts | 自动连接用户设备上的 COM 端口 | 1（允许）或 0（禁止） |
| AllowLptPortRedirection | 允许或禁止 LPT 端口重定向 | 1（允许）或 0（禁止） |
| LimitLptBw | LPT 端口重定向通道的带宽限制 | 数值 |
| LimitLptBwPercent | LPT 端口重定向通道的带宽限制，占总会话带宽的百分比 | 0 到 100 之间的数值 |
| AutoConnectClientLptPorts | 自动连接用户设备上的 LPT 端口 | 1（允许）或 0（禁止） |

配置这些设置后，更改您的计算机目录以使用新的主映像或更新的物理机。用户下次注销时，桌面将使用新设置进行更新。

## Configuration Manager 2012 连接器策略设置

Configuration Manager 2012 连接器部分包含用于配置 Citrix Connector 7.5 代理的策略设置。

> **重要提示：**
>
> 警告、注销和重新启动消息策略仅适用于部署到手动管理或由 Provisioning Services 管理的多会话操作系统计算机目录。对于这些计算机目录，当有待处理的应用程序安装或软件更新时，连接器服务会提醒用户。
>
> 对于由 MCS 管理的目录，请使用 Studio 通知用户。对于手动管理的单会话操作系统目录，请使用 Configuration Manager 通知用户。对于由 Provisioning Services 管理的单会话操作系统目录，请使用 Provisioning Services 通知用户。

### 警告频率间隔

此设置定义向用户显示警告消息的间隔。

间隔使用 ddd.hh:mm:ss 格式设置，其中：

- ddd 是天数，一个可选参数，范围为 0–999。
- hh 是小时，范围为 0–23。

- mm 是分钟，范围为 0–59。
- ss 是秒，范围为 0–59。

默认情况下，间隔设置为 1 小时 (01:00:00)。

### 警告消息框正文文本

此设置包含可编辑的消息文本，用于通知用户即将进行的软件更新或需要他们注销的维护。

默认情况下，消息为：{TIMESTAMP} 保存您的工作。服务器将在 {TIMELEFT} 后离线进行维护。

### 警告消息框标题

此设置包含向用户显示的警告消息标题栏的可编辑文本。

默认情况下，标题为：“即将进行的维护”

### 警告时间段

此设置定义了警告消息在维护开始前多长时间首次出现。

时间使用 ddd.hh:mm:ss 格式设置，其中：

- ddd 表示天数，是一个可选参数，范围为 0–999。
- hh 表示小时，范围为 0–23。
- mm 表示分钟，范围为 0–59。
- ss 表示秒，范围为 0–59。

默认情况下，此设置为 16 小时 (16:00:00)，表示第一条警告消息大约在维护开始前 16 小时出现。

### 最终强制注销消息框正文

此设置包含向用户发出强制注销已开始警报的消息的可编辑文本。

默认情况下，消息为：“服务器当前正在离线进行维护”

### 最终强制注销消息框标题

此设置包含最终强制注销消息标题栏的可编辑文本。

默认情况下，标题为：Notification From IT Staff

### 强制注销宽限期

此设置定义了通知用户注销与实施强制注销以处理待定维护之间的时间段。

时间使用 ddd.hh:mm:ss 格式设置，其中：

- ddd 表示天数，是一个可选参数，范围为 0–999。
- hh 表示小时，范围为 0–23。
- mm 表示分钟，范围为 0–59。
- ss 表示秒，范围为 0–59。

默认情况下，强制注销宽限期设置为 5 分钟 (00:05:00)。

### 强制注销消息框正文

此设置包含消息的可编辑文本，该消息告知用户在强制注销开始之前保存其工作并注销。

默认情况下，消息包含以下内容：{TIMESTAMP} 保存您的工作并注销。服务器将在 {TIMELEFT} 后离线进行维护。

### 强制注销消息框标题

此设置包含强制注销消息标题栏的可编辑文本。

默认情况下，标题为：来自 IT 员工的通知

### 映像管理模式

Connector 代理自动检测其是否在由 Provisioning Services 或 MCS 管理的计算机克隆上运行。该代理会阻止 Configuration Manager 在映像管理的克隆上进行更新，并自动将更新安装到目录的主映像上。

主映像更新后，使用 Studio 协调 MCS 目录克隆的重新启动。Connector 代理会在 Configuration Manager 维护窗口期间自动协调 PVS 目录克隆的重新启动。要覆盖此行为，以便 Configuration Manager 在目录克隆上安装软件，请将“映像管理模式”更改为“已禁用”。

### 重新启动消息框正文

此设置包含可编辑文本，该消息用于通知用户服务器即将重新启动。

默认情况下，消息为：服务器当前正在脱机进行维护。

### 代理任务运行的常规时间间隔

此设置确定 Citrix Connector™ 代理任务的运行频率。

时间使用 ddd.hh:mm:ss 格式设置，其中：

- ddd 表示天数，一个可选参数，范围为 0–999。

- hh 表示小时数，范围为 0–23。
- mm 表示分钟数，范围为 0–59。
- ss 表示秒数，范围为 0–59。

默认情况下，常规时间间隔设置为 5 分钟 (00:05:00)。

# 管理

管理 Citrix Virtual Apps and Desktops™ 站点涵盖了各种项目和任务。

### 许可

创建站点时，需要与 Citrix 许可证服务器建立有效连接。之后，您可以从 Studio 完成多项许可任务，包括添加许可证、更改许可证类型或模型以及管理许可证管理员。您还可以从 Studio 访问许可证管理控制台。

### 应用程序

在交付组中管理应用程序，也可以在应用程序组中管理。

### 区域

在地理分散的部署中，您可以使用区域将应用程序和桌面置于更靠近最终用户的位置，这可以提高性能。当您安装和配置站点时，所有控制器、计算机目录和主机连接都位于一个主区域中。之后，您可以使用 Studio 创建包含这些项目的卫星区域。当您的站点拥有多个区域后，您将能够指示任何新创建的计算机目录、主机连接或添加的控制器将放置在哪个区域中。您还可以在区域之间移动项目。

### 连接和资源

如果您使用虚拟机管理程序或其他服务来托管向用户交付应用程序和桌面的计算机，则在创建站点时，您将创建与该虚拟机管理程序或其他服务的第一个连接。该连接的存储和网络详细信息构成了其资源。之后，您可以更改该连接及其资源，并创建更多连接。您还可以管理使用已配置连接的计算机。

### 本地主机缓存

当 Delivery Controller™ 与站点数据库之间的连接失败时，本地主机缓存允许站点中的连接代理操作继续进行。

### 虚拟 IP 和虚拟环回

Microsoft 虚拟 IP 地址功能为每个会话的已发布应用程序提供唯一的动态分配 IP 地址。Citrix 虚拟环回功能允许您配置依赖于与 localhost 通信的应用程序，以使用 localhost 范围内的唯一虚拟环回地址。

### 交付控制器

本文包含从站点添加和移除控制器时的注意事项和步骤。它还介绍了如何将控制器移动到另一个区域或站点，以及如何将 VDA 移动到另一个站点。

### VDA 与控制器的注册

在 VDA 帮助交付应用程序和桌面之前，它必须向控制器注册（建立通信）。控制器地址可以通过多种方式指定，本文对此进行了介绍。在站点中添加、移动和移除控制器时，VDA 拥有最新信息至关重要。

### 会话

保持会话活动对于提供最佳用户体验至关重要。多项功能可以优化会话的可靠性，减少不便、停机时间和生产力损失。

- 会话可靠性
- 客户端自动重新连接
- ICA® 保持活动
- 工作区控制
- 会话漫游

### 在 Studio 中使用搜索

当您想在 Studio 中查看有关计算机、会话、计算机目录、应用程序或交付组的信息时，请使用灵活的搜索功能。

### 标记

使用标记来标识计算机、应用程序、组和策略等项目。然后，您可以定制某些操作，使其仅应用于具有特定标记的项目。

### IPv4/IPv6

Citrix Virtual Apps and Desktops 支持纯 IPv4、纯 IPv6 以及使用重叠 IPv4 和 IPv6 网络的双栈部署。本文介绍并阐述了这些部署。它还介绍了控制 IPv4 或 IPv6 使用的 Citrix 策略设置。

### 用户配置文件

默认情况下，安装 VDA 时会自动安装 Citrix Profile Management。如果您使用此配置文件解决方案，请查阅本文以获取一般信息。有关详细信息，请参阅 Profile Management 文档。

收集 Citrix 诊断工具 (CDF) 跟踪

CDFControl 实用程序是一个事件跟踪控制器或使用者，用于捕获来自各种 Citrix 跟踪提供程序显示的 Citrix 诊断工具 (CDF) 跟踪消息。它旨在解决复杂的 Citrix 相关问题、解析筛选器支持并收集性能数据。

### 思杰洞察服务

Citrix Insight Services (CIS) 是一个 Citrix 平台，用于实现检测、遥测和业务洞察生成。

思杰 Scout

Citrix Scout 收集诊断信息并运行健康检查。您可以将结果用于 Citrix Virtual Apps and Desktops 部署中的主动维护。Citrix 通过 Citrix Insight Services 提供对诊断集合的全面自动化分析。您还可以自行或在 Citrix 支持的指导下使用 Scout 解决问题。

# 使用 Studio 为思杰虚拟应用和桌面™ 许可

在 Studio 中，如果许可证服务器与 Studio 位于同一域或受信任域中，您可以管理和跟踪许可。有关许可任务的信息，请参阅许可文档和多类型许可。

许可证激活服务 (LAS) 是一种新的基于云的许可解决方案，它提供了传统 Citrix® 旧版许可的替代方案。LAS 引入了新的激活模块，确保了无缝且现代的许可证管理方法。有关详细信息，请参阅许可证激活服务。

下表列出了支持的版本和许可模型：

| 产品 | 版本 | 许可模型 |
| --- | --- | --- |
| Citrix 虚拟应用™ | 高级版、增强版、标准版 | 并发 |
| 思杰虚拟桌面 | 高级版、增强版、标准版 | 用户/设备和并发 |

有关详细信息，请参阅并发许可证和用户/设备许可证。

## 支持的当前版本 (CR) 和长期服务版本 (LTSR)

有关支持的当前版本 (CR)、长期服务版本 (LTSR) 和最低兼容 LS 版本的信息，请参阅Citrix Virtual Apps and Desktops 当前版本文档。

> **重要提示：**

> License Server VPX 已弃用，并且将不再接收任何维护或安全修复。建议使用 11.16.6 或更早版本 License Server VPX 的客户尽快迁移到 最新版本的 Windows 版 License Server。

> 您必须是完全许可证管理员才能完成以下任务。要在 Studio 中查看许可证信息，管理员必须至少具有“读取许可”委派管理权限。内置的“完全管理员”和“只读管理员”角色具有该权限。

## 使用 Studio 从 Citrix® 下载并安装许可证

1. 在 Studio 导航窗格中选择“**配置 \> 许可**”。
2. 在“操作”窗格中选择“**分配许可证**”。
3. 输入许可证访问代码，该代码是您在购买或续订许可证后从 Citrix 收到的电子邮件中的代码。
4. 选择一个产品，然后选择“**分配许可证**”。该产品可用的许可证将被分配和下载。为特定许可证访问代码分配并下载所有许可证后，您将无法重复使用该许可证访问代码。要使用同一代码执行其他事务，请登录“我的帐户”。

## 添加存储在本地计算机或网络上的许可证

1. 在 Studio 导航窗格中选择“**配置 > 许可**”。
2. 在“操作”窗格中选择“**添加许可证**”。
3. 浏览到许可证文件并将其添加到许可证服务器。

## 更改许可证服务器

1. 在 Studio 导航窗格中选择“**配置 > 许可**”。
2. 在“操作”窗格中选择“**更改许可证服务器**”。
3. 键入许可证服务器的地址，格式为 *name:port*，其中 name 是 DNS、NetBIOS 或 IP 地址。如果未指定端口号，则使用默认端口 (27000)。

## 选择要使用的许可证类型

- 配置站点时，指定许可证服务器后，系统会提示您选择要使用的许可证类型。如果服务器上没有许可证，则会自动选择在没有许可证的情况下使用产品 30 天试用期的选项。
- 如果服务器上有许可证，则会显示其详细信息，您可以选择其中一个。或者，您可以将许可证文件添加到服务器，然后选择该文件。

## 更改产品版本和许可模型

1. 在 Studio 导航窗格中选择“**配置 > 许可**”。

2. 在“操作”窗格中选择“**编辑产品版本**”。
3. 更新相应的选项。

要访问许可证管理控制台，请在“**操作**”窗格中选择“**许可证管理控制台**”。控制台会立即显示，或者如果仪表板配置为受密码保护，系统会提示您输入许可证管理控制台凭据。有关如何使用控制台的详细信息，请参阅许可文档。

> **注意：**
>
> 在 Citrix Studio 中切换许可证时，更改最多需要 5 分钟才能显示在 Citrix Director 中。例如，如果您在 Advanced 和 Premium 之间切换，反之亦然。

## 添加许可管理员

1. 在 Studio 导航窗格中选择“**配置 > 许可**”。
2. 在中间窗格中选择“许可管理员”选项卡。
3. 在“操作”窗格中选择“**添加许可管理员**”。
4. 浏览到要添加为管理员的用户并选择权限。

## 更改许可管理员的权限或删除许可管理员

1. 在 Studio 导航窗格中选择**配置 > 许可**。
2. 在中间窗格中选择“许可管理员”选项卡，然后选择管理员。
3. 在“操作”窗格中选择**编辑许可管理员**或**删除许可管理员**。

## 添加许可管理员组

1. 在 Studio 导航窗格中选择**配置 > 许可**。
2. 在中间窗格中选择“许可管理员”选项卡。
3. 在“操作”窗格中选择**添加许可管理员组**。
4. 浏览到您希望作为许可管理员的组并选择权限。添加 Active Directory 组会向该组中的用户授予许可管理员权限。

## 更改许可管理员组的权限或删除许可管理员组

1. 在 Studio 导航窗格中选择**配置 > 许可**。
2. 在中间窗格中选择“许可管理员”选项卡，然后选择管理员组。

3. 在“操作”窗格中选择**编辑许可管理员组**或**删除许可管理员组**。

## 查看许可证信息

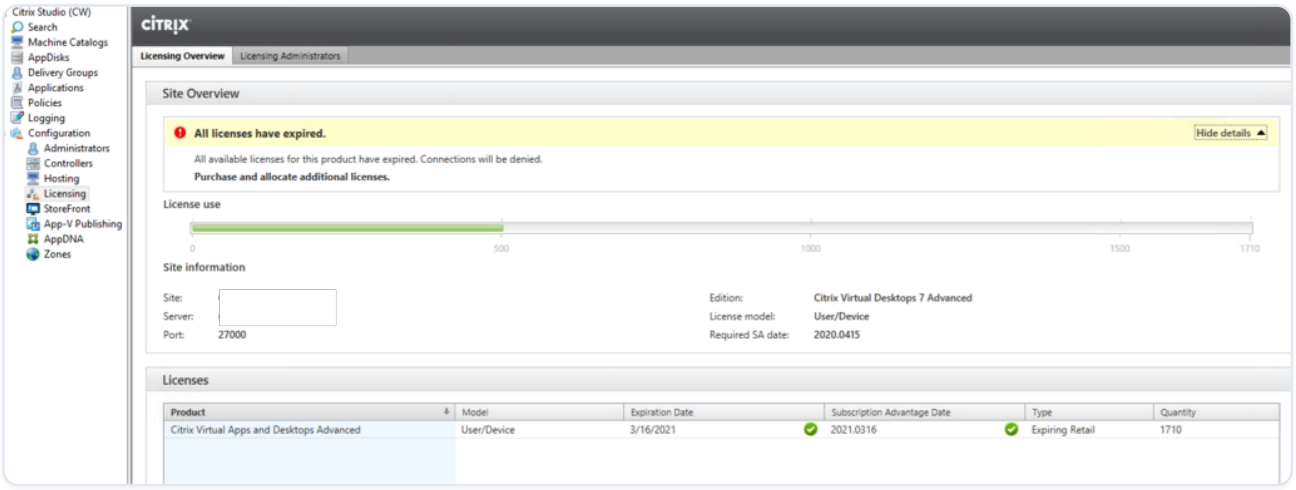
在 Studio 导航窗格中选择**配置 > 许可**。将显示站点的许可证使用情况和设置摘要，以及指定许可证服务器上当前安装的所有许可证的列表。

确保站点的许可设置（包括产品类型、许可证版本和许可模型）与您配置的许可证服务器使用的许可证匹配。如果不匹配，您可能需要下载或分配现有许可证以匹配站点的许可证设置。

## 查看许可证过期警报

Citrix Studio 从 Citrix 许可证服务器查询许可证文件的过期日期。如果许可证文件即将过期或已过期，管理员会收到警报。

您可以在 Studio 用户界面中看到警报。下图显示了 Citrix Studio UI 上显示的许可证过期警报。




## 相关链接

- 请参阅Citrix 内部部署年度和基于期限的零售许可证订阅。
- 请参阅具有混合权利的过渡和升级 (TTU)。

## 许可证激活服务

许可证激活服务 (LAS) 是一种新的基于云的许可解决方案，它提供了传统 Citrix® 旧版许可的替代方案。LAS 引入了新的激活模块，确保了无缝且现代的许可证管理方法。

LAS 简化了 Citrix 许可体验。不再需要生成、下载或安装许可证服务器上的许可证访问代码或文件。您只需升级许可证服务器并向 Citrix Cloud 注册。一旦兼容产品指向许可证服务器，它们就可以自动激活。

激活后，许可证服务器会定期与许可证激活服务通信，以保持其激活状态最新。LAS 采用云技术构建，可提高性能并确保零停机时间。如果由于任何原因许可证服务器或 LAS 无法访问，系统将进入许可证缓存模式，该模式旨在保护系统免于未授权并避免中断。有关详细信息，请参阅 许可证缓存模式。

有关 LAS 的更多详细信息，请参阅许可文档 许可证激活服务。

### 先决条件

- 将许可证服务器安装或更新到版本 11.17.2 build 53100 或更高版本。
- 许可证服务器需要可靠且持续的互联网连接。
- 桌面组级别许可证设置必须禁用。

> **注意：**

为确保 DG 级别许可已禁用，请使用 Get-brokerdesktopgroup，并且 LicenseModel 应为“None”。

> **注意：**

在开始升级到 2203 LTSR CU7 之前，请在 Delivery Controller 上安装 .NET Framework 4.8。这可确保许可兼容性检查工具正常执行并防止出现错误的许可警告。

### 注意事项

- 在 Citrix Studio 提示激活之前，所有 Delivery Controller 都必须与 LAS 兼容。单个控制器站点可以使用旧版许可证或 LAS。
- 您可以将多个许可证服务器注册到相同的 Citrix Cloud ID (CCID) 或 OrgID。但是，一个站点只能配置为指向一个许可证服务器。

### 限制

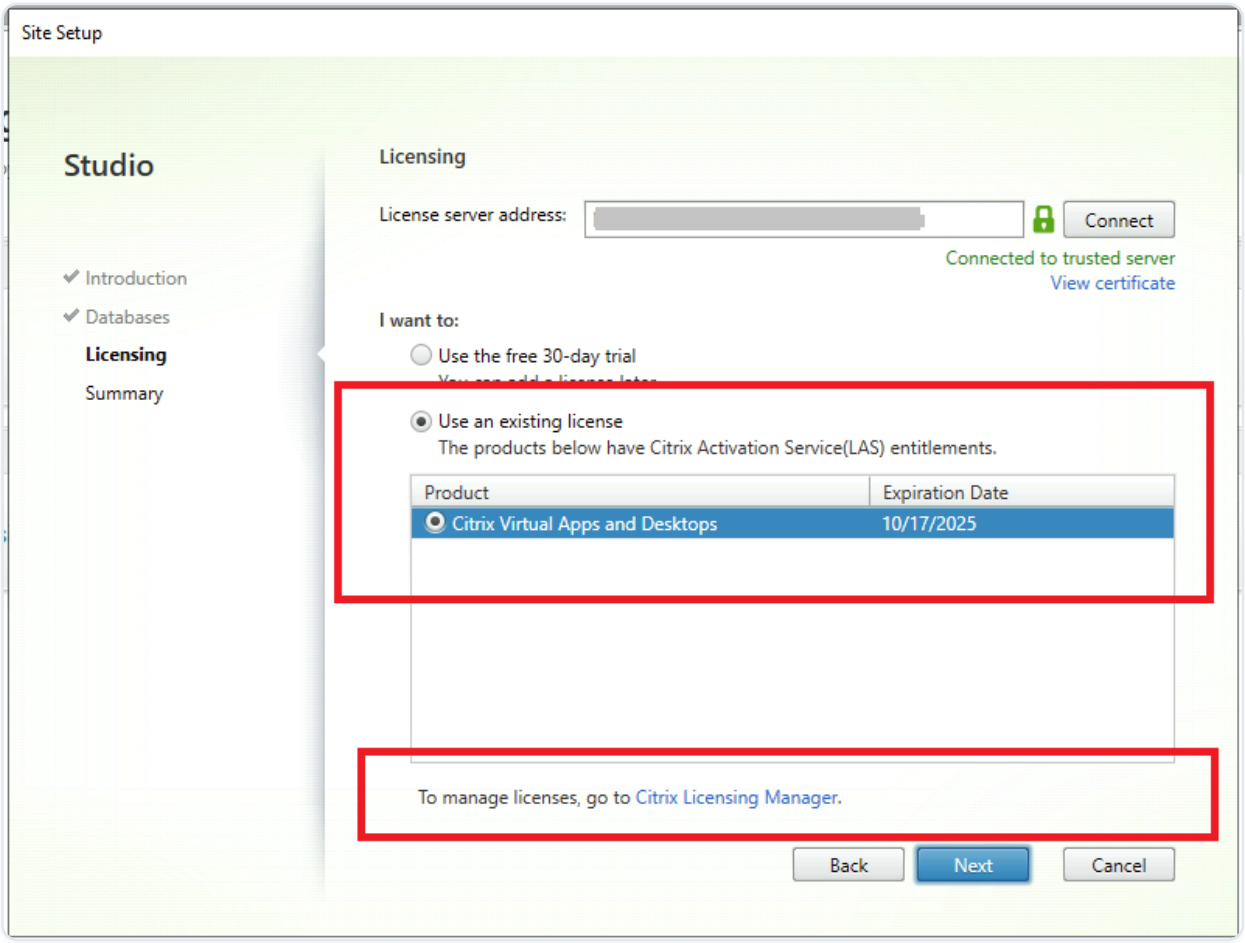
- 迁移到 LAS 会将产品版本设置为 **Premium**，并将许可证模型设置为 **Concurrent**，但这在将来可能会发生变化。请勿使用 PowerShell 修改许可证配置，因为这可能会影响注册和会话启动。
- 您可以仅使用 Citrix Studio 将您的 Citrix Virtual Apps and Desktops™ 站点从现有旧版许可证迁移到 LAS。

### 主要步骤

1. 安装或升级许可证服务器到版本 11.17.2 build 53100 或更高版本，并按照 如何为许可证激活服务配置许可证服务器 中提及的说明配置 LAS。
2. 安装 Citrix Virtual Apps and Desktops 2203 LTSR CU7 或更高版本。安装核心组件，例如 Citrix Delivery Controller、Citrix Studio 和 Citrix Director。

> **注意：**
>
> Citrix Virtual Apps and Desktops 站点中的所有 Delivery Controller 都必须与 LAS 兼容。

3. 安装所需组件后，使用 Citrix Studio 创建站点。有关创建站点的信息，请参阅创建站点。如果许可证服务器配置为使用 LAS，则 Metainstaller 会显示权利。权利会随其相应的许可证到期日期一起提供。




> **注意：**

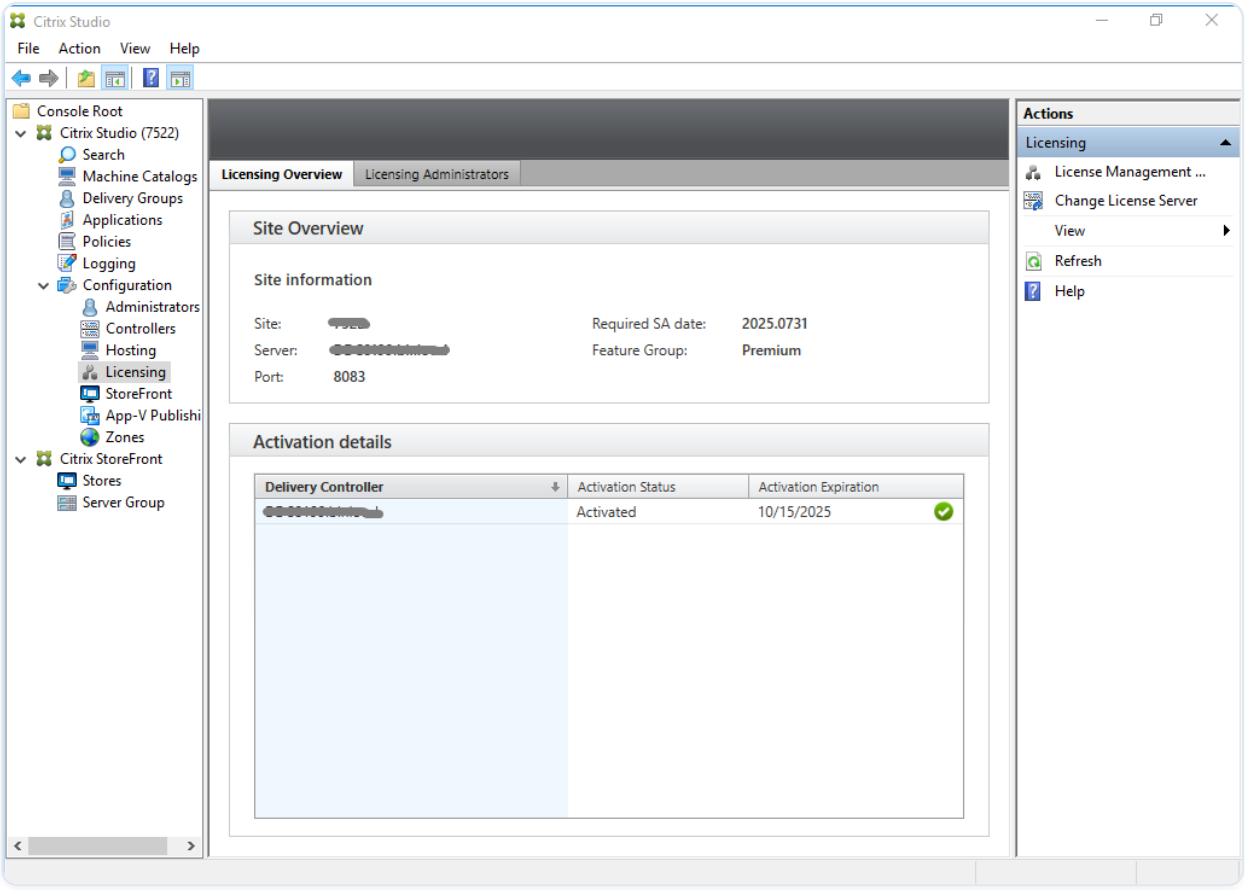
> 如果许可证服务器未升级到版本 53100 或更高版本，您将遇到许可错误。忽略这些错误并继续进行 CVAD 站点升级将导致站点无法运行。

4. 检查许可详细信息。
5. 将旧版许可迁移到 LAS。

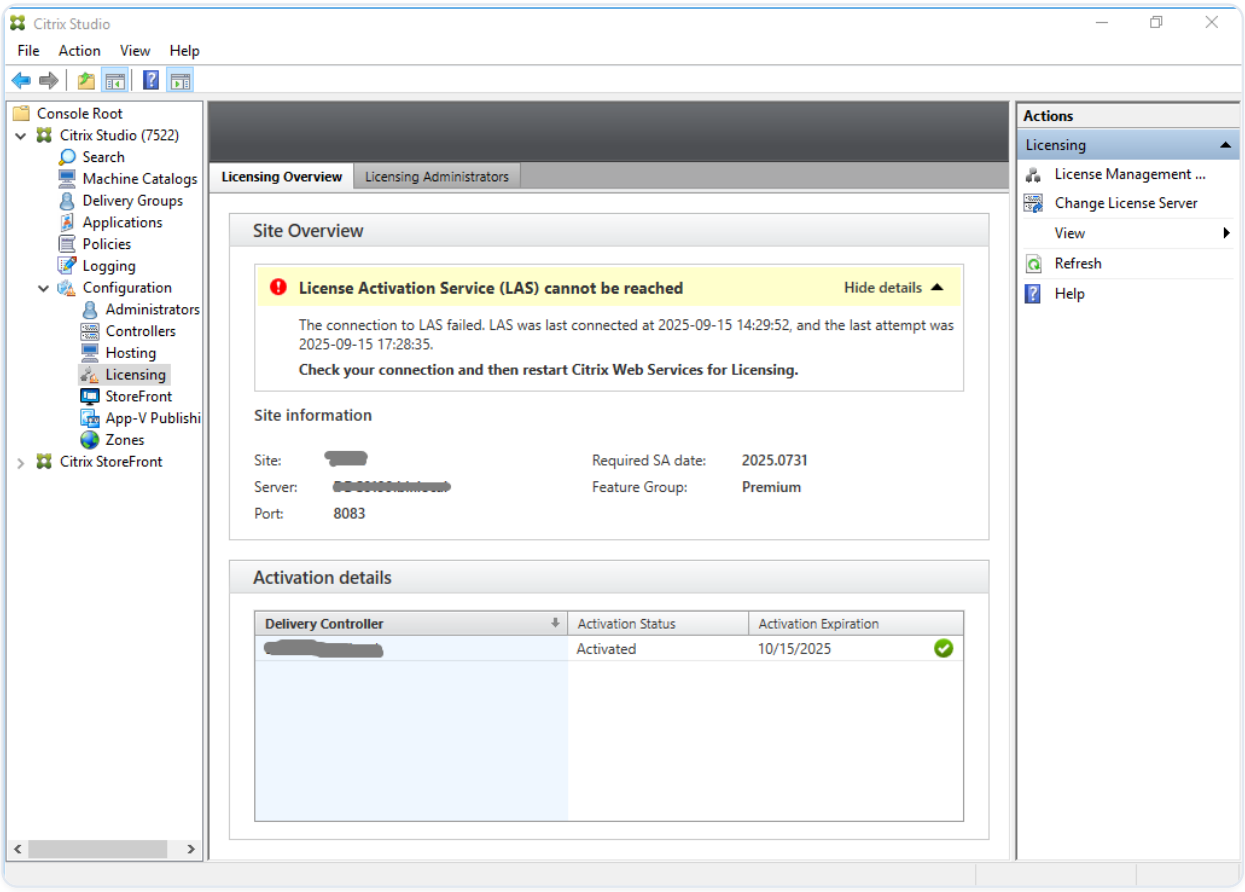
### 检查许可详细信息

创建站点后，使用 Citrix Studio 检查许可详细信息。

1. 在 Citrix Studio 中，选择**许可**节点。
2. 在**许可概述**页面上，检查 Citrix Virtual Apps and Desktops 站点是否具有相应的许可证，或者在使用 LAS 功能时许可证是否已过期。




如果 LAS 无法访问，您可能会看到错误消息：




如果您的许可证服务器仍在使用旧版许可证，并且 Citrix Virtual Apps and Desktops 站点支持 LAS，则 Citrix Studio 会提示您向 Citrix Cloud 注册许可证服务器。

注册许可证服务器以使用 LAS(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/register-license-server.png)

### 将旧版许可迁移到 LAS

如果您已将许可证服务器注册到 Citrix Cloud 并拥有必要的权利，则必须遵循以下特定顺序，将现有 Citrix Virtual Apps and Desktops 站点从旧版许可迁移到 LAS，而不会影响用户会话。

1. **升级许可证服务器：** 将许可证服务器升级到最低支持版本。
2. **升级交付控制器：** 将站点中的所有交付控制器升级到支持 LAS 的版本。
3. **删除交付组许可证分配：**
   - 在单击“**迁移到 LAS**”之前，手动删除站点级别以下的任何许可证分配（即，删除交付组级别的许可证分配）。
4. **确认分配：** 验证 LAS 分配是否准确。
5. **单击“迁移到 LAS”：**
   - 完成上述步骤后，单击“**迁移到 LAS**”。

从旧版许可证迁移到 LAS(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/migrate-to-las.png)

- 迁移到 LAS 后，Citrix Virtual Apps and Desktops 站点的**许可证版本**将设置为 **Citrix Virtual Apps and Desktops Premium**，**许可证模型**将配置为**并发**。

### 从 LAS 回滚到旧版许可

执行以下操作以从 LAS 回滚到旧版许可：

1. 运行以下 PowerShell 命令。

```
Set-ConfigSite -UseLicenseActivationService $false
```

2. 在 Citrix Studio 中配置旧版许可证。

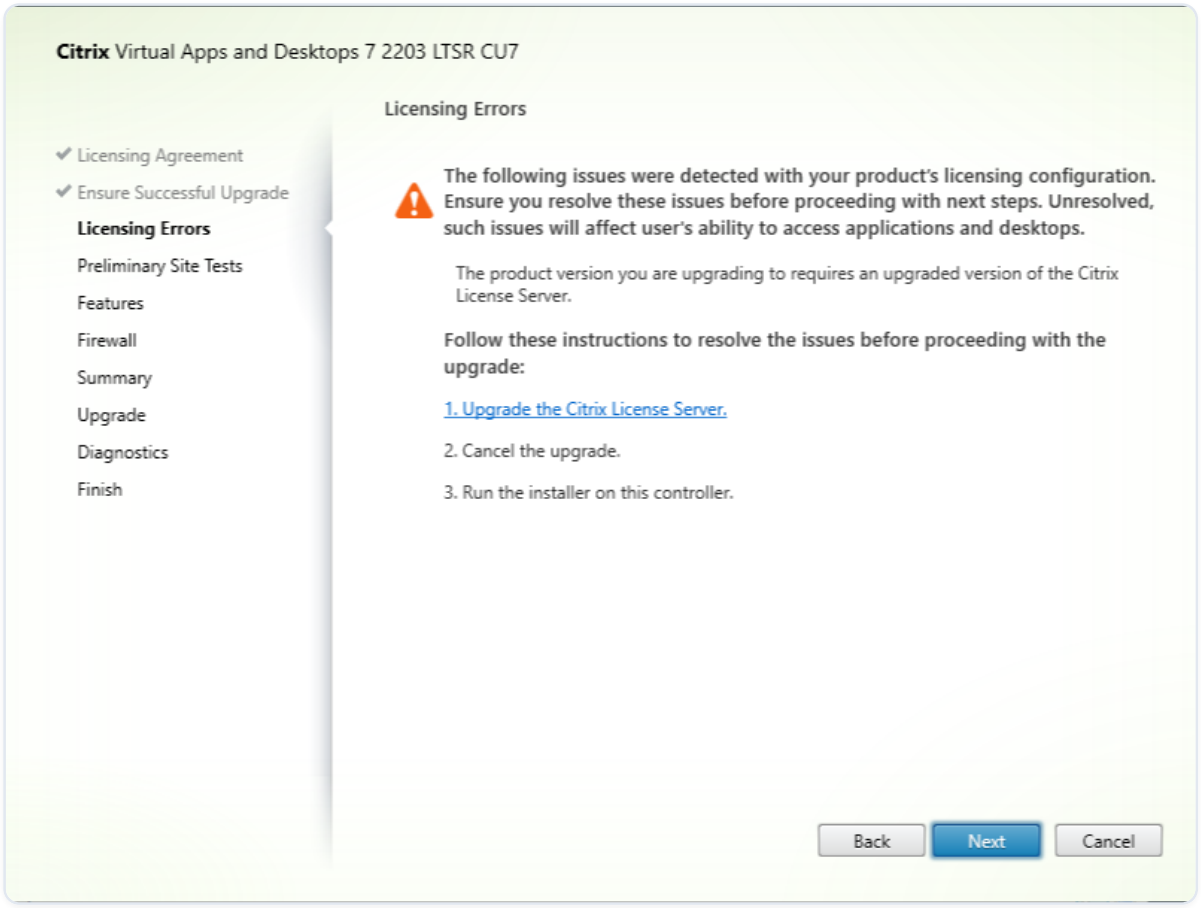
**注意：**

这些步骤仅用于临时故障排除。旧版许可证文件即将终止服务 (EOL)，并且在 April 15, 2026 之后将无法运行。为确保服务不中断，我们建议迁移到许可证激活服务 (LAS)。有关详细信息，请参阅公告。

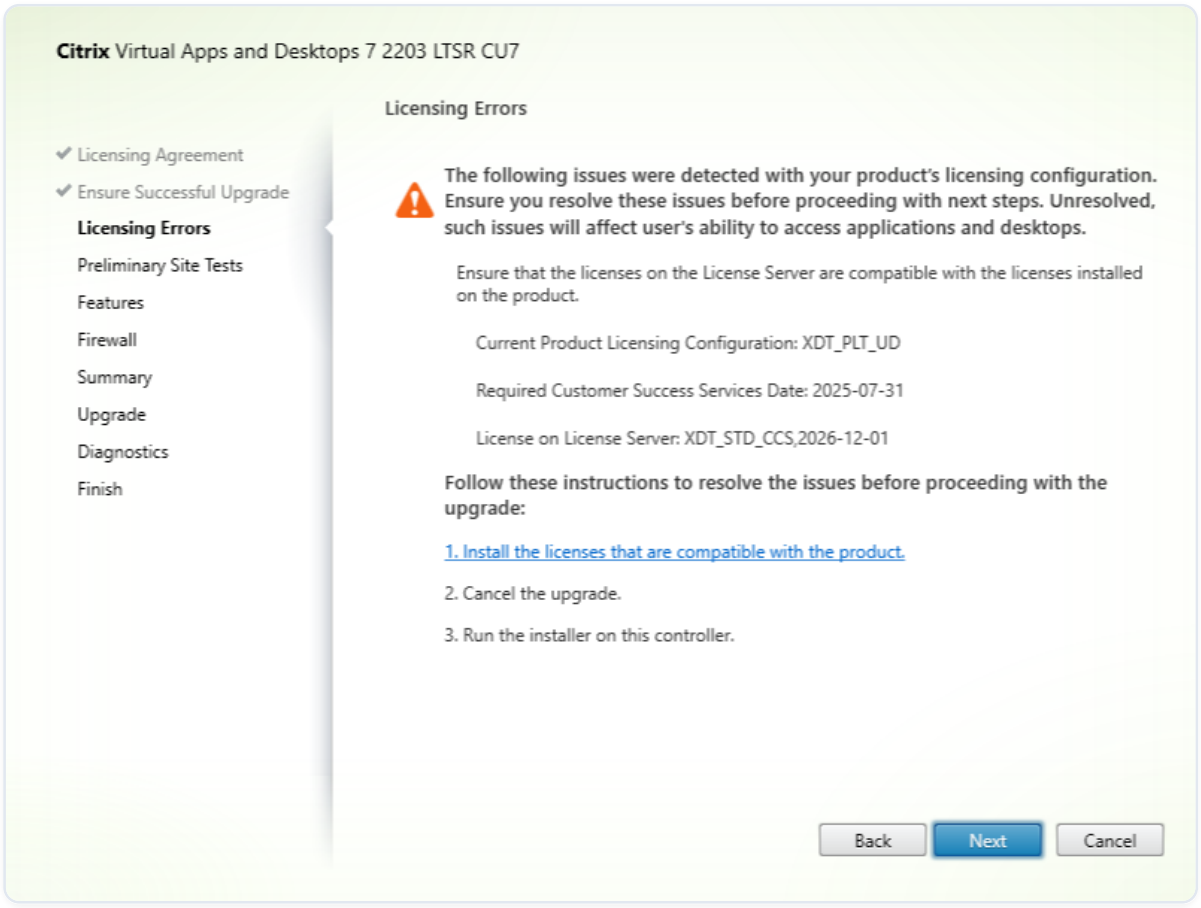
### 升级的重要注意事项

当您从任何早期版本的 Citrix Virtual Apps and Desktops 升级到 2203 LTSR CU7 及更高版本时，请将许可证服务器升级到最新版本（版本 11.2.17 build 53100 或更高版本）。

- 使用元安装程序 UI 升级时，许可错误页面上会出现以下错误：
  - 如果您未升级到最新版本的许可证服务器：




◦ 如果存在任何不兼容性，例如许可证服务器过时或许可证不可用：



- 如果您使用命令行进行升级，请运行以下命令以避免升级失败（假设您位于已装载 ISO 中的 \x64 文件夹内）：

1. 运行以下命令：

```
\x64\Licensing\CitrixLicensing.exe /quiet
```

如果您已将许可二进制文件复制到任何本地驱动器，请运行以下命令：

```
\x64\Licensing\CitrixLicensing.exe /quiet /l install.log
```

2. 运行以下命令：

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe  /components
"CONTROLLER,DESKTOPSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
```

**卸载核心组件**

在升级过程中，如果您先使用命令 `\x64\Licensing\CitrixLicensing.exe /quiet` 或 `\x64\Licensing\CitrixLicensing.exe /quiet /l install.log` 安装了许可证服务器，然后安装了核心组件，则请按照相同的顺序进行卸载：

1. 使用命令行卸载许可证服务器：

```
CitrixLicensing.exe /quiet /uninstall /l uninstall.log
```

2. 使用 GUI 或命令行卸载组件。有关信息，请参阅删除组件。

如果您使用命令行 `XenDesktopServerSetup.exe` 或 `removeall` 卸载许可证服务器和组件，请清理注册表项和剩余文件。

清理注册表项：

1. 搜索注册表项 `Citrix Licensing` 并删除该条目。通常，您可以在以下位置找到该条目：

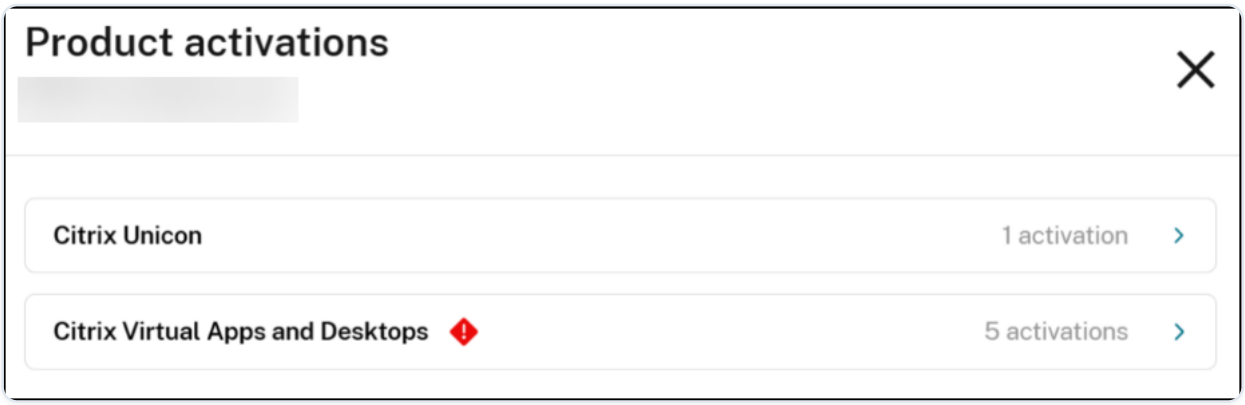
```
"Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Cur
rentVersion\Uninstall\
```

2. 删除注册表项中 **Uninstall String** 指向的文件夹。

### 故障排除

如果许可证服务器在 Citrix Cloud 中的状态显示为非绿色，请执行以下操作以了解可能存在问题的激活的详细信息：

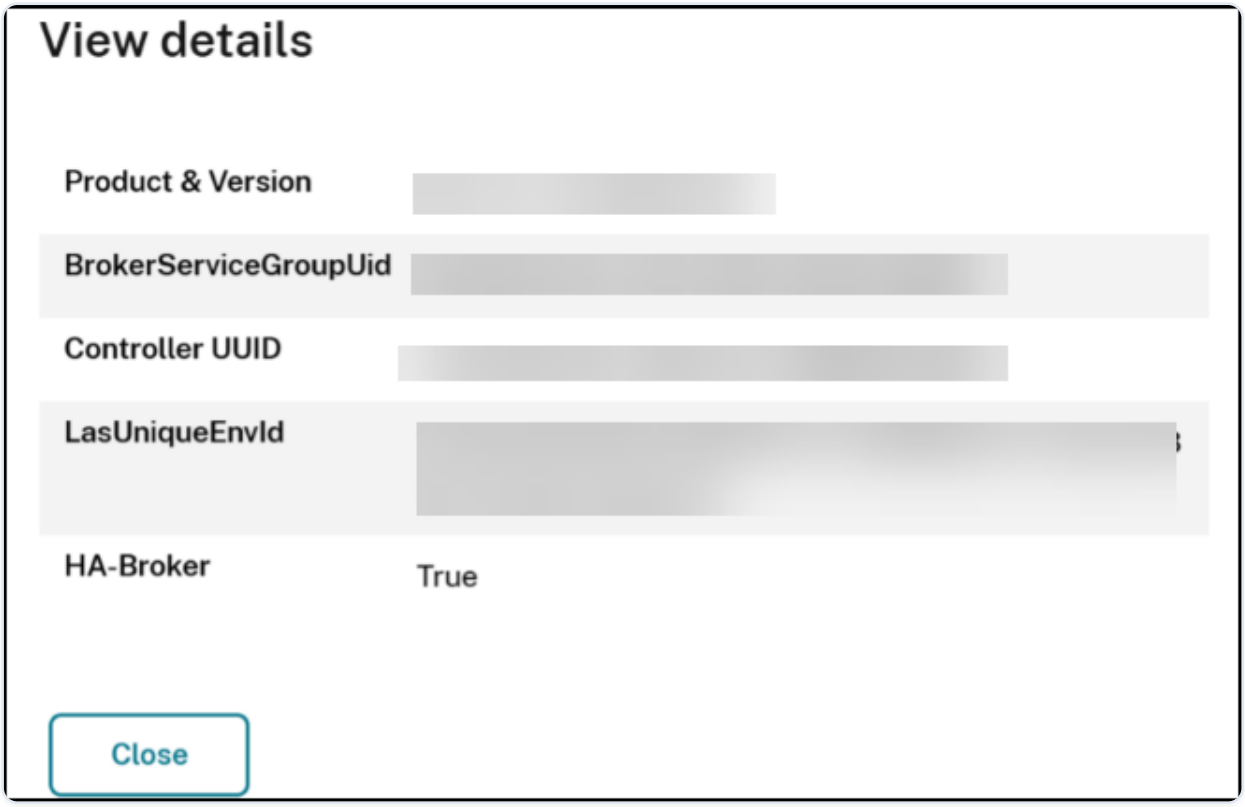
1. 在 Citrix Cloud 中，导航到 **许可 > 许可部署 > 许可服务器**。
2. 单击 Citrix Virtual Apps and Desktops 旁边的展开按钮 **>** 以查看已激活的 Delivery Controller 列表。




3. 单击激活旁边的 **View details** 以查看详细信息。

   **ID** 是用于标识激活的唯一标识符。

   提供了以下详细信息：



- **产品和版本**：产品配置为在通过 LAS 激活时使用的 Product_Edition_Model 和 Burn In Date。BurnInDate 通常是产品的发布日期。
- **BrokerServiceGroupUid**：Broker 服务组的 UID。
- **Controller UUID**：交付控制器的 UUID。
- **LasUniqueEnvId**：LAS 为激活提供的实例的唯一 ID。
- **HA-Broker**：指示它是 HA 代理还是主代理的 True 或 False。

要将已激活的主机详细信息与实际主机进行映射，请在该主机上运行以下命令。

- `Get-BrokerSite`：将屏幕上显示的 **BrokerServiceGroupUid** 值与命令的 `BrokerServiceGroupId` 输出进行比较。
- `Get-BrokerController`：将屏幕上显示的 **Controller UUID** 值与命令的 UUID 输出进行比较。

### 与许可事件相关的事件查看器日志

| 事件 ID | 描述 |
| --- | --- |
| 1112 | Citrix Broker Service 未能为用户与资源建立连接。站点的产品和版本许可配置不允许此类资源。请检查是否已为该站点选择了正确的许可证。 |
| 1150 | Citrix Broker Service 已成功联系许可证服务器。 |
| 1151 | Citrix Broker Service 无法联系许可证服务器。请确保许可证服务器正常运行，并且 XenDesktop 配置中标识许可证服务器的详细信息正确无误。 |
| 1152 | 此 XenDesktop 站点在许可证服务器上没有所需的产品许可证。使用许可证管理控制台将相关产品许可证添加到许可证服务器。 |
| 1153 | 此 XenDesktop 站点的许可证已过期。Citrix Broker 服务将从许可证服务器请求新许可证。 |
| 1154 | 此控制器已进入许可证缓存模式，因为它无法联系许可证服务器。您还有 2 小时，此控制器将停止提供桌面和应用程序会话。 |

| 事件 ID | 描述 |
| --- | --- |
| 1155 | Citrix Broker 服务现在将停止提供桌面和应用程序会话。由于持续无法与许可证服务器通信，此控制器不再处于或无法进入许可证缓存模式。请确保许可证服务器正常运行，如有必要，请使用许可证管理控制台将相关许可证添加到许可证服务器。 |
| 1156 | Citrix Broker 服务正在成功与许可证服务器通信。此控制器不再处于许可证缓存模式。 |
| 1157 | 许可证服务器上运行的版本早于 Citrix Broker 服务的版本，因此不兼容。请升级您的许可证服务器，或在您的 XenDesktop 配置中指定具有正确版本的许可证服务器位置。 |
| 1158 | Citrix Broker 服务检测到您已超出此版本在此站点许可证服务器上可用的许可证数量。许可证服务器已授予您透支许可证。 |
| 1159 | Citrix Broker 服务拒绝了桌面连接，因为此站点的最大安装许可证数量已超出。此版本安装了三个许可证，但此版本允许的最大许可证数量为两个。请从许可证服务器中删除相关许可证以符合许可证限制。 |
| 1160 | Citrix Broker 服务在管理许可证时遇到内部错误。请确保许可证服务器正常运行，并且 XenDesktop 配置中标识许可证服务器的详细信息正确无误。重新启动 Citrix Broker 服务也可能解决此问题。如果此问题仍然存在，请重新安装 Citrix XenDesktop Controller。请参阅 Citrix 知识库文章 CTX126990。 |
| 1161 | 初始化许可时出错。检查许可证服务器连接。 |
| 1162 | 停止许可时出错。检查许可证服务器连接。 |
| 1163 | 无可用连接许可证。要解决此问题，请通过关闭不需要的会话来释放许可证，或添加更多许可证。 |

| 事件 ID | 描述 |
| --- | --- |
| 1164 | 签出连接许可证时出错。检查许可证服务器连接。 |
| 1165 | 签入连接许可证时出错。检查许可证服务器连接。 |
| 1166 | 检查许可证可用性时出错。检查许可证服务器连接。 |
| 1167 | 未能启动许可。检查许可证服务器连接。 |
| 1168 | 读取许可用户通知设置时出错。检查许可证服务器连接。 |
| 1169 | 此控制器已进入开箱即用许可证缓存模式，因为在许可证服务器上未找到合适的许可证。在此控制器停止提供桌面和应用程序会话之前，您还有 2 小时。 |
| 1170 | Citrix Broker Service 已成功在许可证服务器上检测到合适的许可证。此控制器不再处于开箱即用许可证缓存模式。 |
| 1171 | 未指定许可证服务器。在指定有效的许可证服务器之前，Citrix Broker Service 无法向用户提供桌面和应用程序。您可以在 Citrix Studio 中或使用 Citrix PowerShell SDK cmdlet Set-ConfigSite 指定许可证服务器。 |
| 1172 | 检查许可证服务器适用性时出错。Citrix Broker Service 在检查计算机是否适合用作许可证服务器时收到了意外响应。请检查控制器是否可以联系到该计算机，以及该计算机上的任何防火墙是否允许来自控制器的连接。如果计算机上安装了许可证服务器，请检查其是否已正确配置和运行。 |
| 1173 | 此 XenDesktop 站点在许可证服务器上没有所需的启动许可证。使用许可证管理控制台将相关许可证添加到许可证服务器。 |

| 事件 ID | 描述 |
| --- | --- |
| 1174 | 此 XenDesktop 站点配置的产品版本不支持应用程序；应用程序资源将不可用。 |
| 1176 | 配置的产品版本不支持多会话计算机。注册被拒绝。 |
| 1177 | 配置的产品版本不支持单会话计算机。注册被拒绝。 |
| 1178 | 配置的产品版本不支持 RemotePC。注册被拒绝。 |
| 1179 | 配置的产品版本不支持预配到云系统中的计算机。注册被拒绝。 |
| 1180 | 此 XenDesktop 站点的配置产品版本不支持单会话（工作站操作系统）计算机上的应用程序。应用程序资源启动被拒绝。 |
| 1181 | 此 XenDesktop 站点的配置产品版本不支持多会话（服务器操作系统）计算机上的应用程序。应用程序资源启动被拒绝。 |
| 1182 | 此 XenDesktop 站点的配置产品版本不支持单会话（工作站操作系统）计算机上的桌面。桌面资源启动被拒绝。 |
| 1183 | 此 XenDesktop 站点配置的产品版本不支持多会话（服务器操作系统）计算机上的桌面。桌面资源启动被拒绝。 |
| 1196 | 此控制器已进入许可证突发模式，因为许可证服务器上所有可用许可证均已用尽。请添加更多许可证以解决此问题。在此控制器停止提供桌面和应用程序会话之前，您还有 2 小时。 |
| 1197 | Citrix Broker Service 现在将停止提供桌面和应用程序会话。由于许可证服务器上的许可证不足，此控制器不再处于或无法进入许可证突发模式。请使用许可证管理控制台将相关许可证添加到许可证服务器。 |

| 事件 ID | 描述 |
| --- | --- |
| 1198 | Citrix Broker Service 正在成功从许可证服务器使用许可证。服务器上有足够的许可证来满足当前需求。此控制器不再处于因许可证耗尽而导致的许可证突发模式。 |
| 1199 | Citrix Broker Service 现在将停止提供桌面和应用程序会话。由于许可证服务器上未安装任何许可证，此控制器不再处于或无法进入许可证缓存模式。请使用许可证管理控制台将相关许可证添加到许可证服务器。 |
| 1205 | 您的软件维护已过期。您的 Citrix 环境目前不受支持。请检查您的许可证服务器以查找过期许可证并将其删除。在用户开始收到警告消息之前，有 30 天的许可证缓存模式。 |
| 1206 | 许可证证书哈希无效。您的 Citrix 许可证证书哈希无效。 |
| 1300 | Citrix Broker Service 现在将停止提供桌面和应用程序会话。许可证服务器的系统时钟存在问题。 |
| 1301 | 许可证服务器的系统时钟问题已得到纠正。Citrix Broker Service 现在将恢复正常运行。 |
| 1302 | 此控制器再次未能签入或签出连接许可证。以前检测到的故障仍然存在。为避免过多的事件日志记录，服务将抑制相关消息（事件 ID 1163、1164、1165），直到问题解决。许可尝试将继续。 |
| 1303 | 此控制器不再抑制相关消息（事件 ID 1163、1164、1165）。 |
| 1304 | Citrix Broker Service 已成功联系 LAS。 |
| 1305 | Citrix Broker Service 无法联系 LAS。请确保 LAS 正常运行，并且 XenDesktop 配置中标识 LAS 的详细信息正确无误。 |

### 更多信息

有关检查站点的 LAS 状态或验证站点是否处于许可证缓存模式的信息，请参阅：

- 如何检查站点的 LAS 状态？
- 如何验证站点是否处于许可证缓存模式？

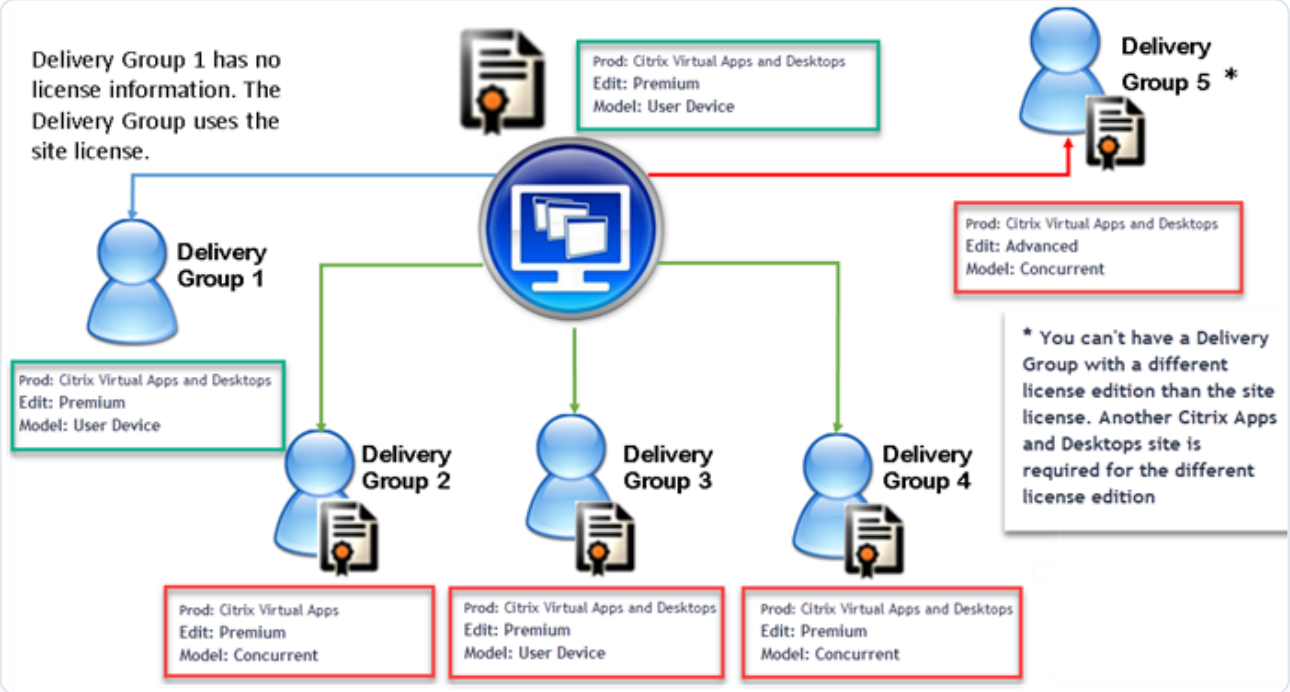
有关命令的详细信息，请参阅：

- Get-BrokerController
- Get-ConfigSite

## 多类型许可

多类型许可支持在单个 Citrix Virtual Apps and Desktops 站点上为交付组使用不同许可证类型。**类型**是产品 ID (XDT 或 MPS) 和模型 (UserDevice 或 Concurrent) 的单一组合。交付组必须使用与站点级别配置的相同产品版本 (PLT/Premium 或 ENT/Advanced)。在为您的 Citrix Virtual Apps and Desktops 部署配置多类型许可时，请注意本文末尾的特殊注意事项。

如果未配置多类型许可，则只有在为单独站点配置时才能使用不同许可证类型。交付组使用站点许可证。有关配置多类型许可时的重要通知限制，请参阅特殊注意事项。




要确定使用不同类型许可证的交付组，请使用以下 Broker PowerShell cmdlet：

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

要安装许可证，请使用：

- 思杰工作室
- 思杰许可管理器
- citrix.com

客户成功服务日期特定于每个许可证文件以及每个产品和模型。设置不同的交付组可能彼此具有不同的客户成功服务日期。

### 特殊注意事项

多类型许可具有不同于常规 Citrix Virtual Apps and Desktops™ 许可的功能。

对于配置为使用与站点配置不同类型的交付组，Director 或 Studio 不会发出警报和通知：

- 当许可证接近限制，或许可证突发模式被触发或到期时，不提供任何信息。
- 当特定组出现问题时，没有通知。

配置为多类型许可的交付组仅使用该许可类型，并且在完全使用后不会回退到站点配置。

尽管 Citrix Virtual Apps Standard 和 Citrix Virtual Desktops™ Standard 许可版本名称都表明它们是 Standard，但它们并非同一版本。多类型许可不适用于 Citrix Virtual Apps Standard 和 Citrix Virtual Desktop Standard 许可。

### 许可兼容性矩阵

此表详细说明了旧产品名称、新产品名称以及相关的特性名称。四个兼容性列指定了哪些产品和许可模型组合与多类型许可兼容。CCU 和 CCS 代表并发许可，UD 代表用户/设备许可。

| Old Name | New Name | Feature | Multi-type licensing compatibility | | | |
|---|---|---|---|---|---|---|
| | | | STD | ADV | ENT | PLT |
| Citrix XenApp Standard | Citrix XenApp Standard | MPS_STD_CCU | X | | | |
| Citrix XenApp Advanced | Citrix Virtual Apps Standard | MPS_ADV_CCU | | X | | |
| Citrix XenApp Enterprise | Citrix Virtual Apps Advanced | MPS_ENT_CCU | | | X | |
| Citrix XenApp Platinum | Citrix Virtual Apps Premium | MPS_PLT_CCU | | | | X |
| Citrix XenDesktop VDI Edition (XDT-U) | Citrix Virtual Desktops Standard- Per User/Device | XDT_STD_UD | X | | | |
| Citrix XenDesktop VDI Edition (XDT-C) | Citrix Virtual Desktops Standard - Concurrent | XDT_STD_CCS | X | | | |
| Citrix XenDesktop Enterprise Edition (XDT-C) | Citrix Virtual Apps and Desktops Advanced - Concurrent | XDT_ENT_CCS | | | X | |
| Citrix XenDesktop Enterprise Edition (XDT-U) | Citrix Virtual Apps and Desktops Advanced - Per User/Device | XDT_ENT_UD | | | X | |
| Citrix XenDesktop Platinum Edition (XDT-C) | Citrix Virtual Apps and Desktops Premium - Concurrent | XDT_PLT_CCS | | | | X |
| Citrix XenDesktop Platinum Edition (XDT-U) | Citrix Virtual Apps and Desktops Premium - Per User/Device | XDT_PLT_UD | | | | X |

### 代理 PowerShell SDK

**DesktopGroup** 对象具有这两个属性，您可以使用关联的 New-BrokerDesktopGroup 和 Set-BrokerDesktopGroup cmdlet 进行操作。

| 名称 | 值 | 限制 |
| --- | --- | --- |
| LicenseModel | 一个参数（并发或用户设备），用于指定组的许可模型。如果未指定，则使用站点范围的许可模型。 | 如果功能开关被禁用，尝试设置属性将失败。 |
| ProductCode | 一个文本字符串，XDT（适用于 Citrix Virtual Desktops）或 MPS（适用于 Citrix Virtual Apps™），用于指定该组的许可产品 ID。如果未指定，则使用站点范围的产品代码。 | 如果功能开关被禁用，尝试设置属性将失败。 |

有关 LicenseModel 和 ProductCode 的更多信息，请参阅 about_Broker_Licensing。

#### New-BrokerDesktopGroup

创建桌面组以管理桌面组的代理。有关此 cmdlet 的更多信息，请参阅 `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>`。

#### Set-BrokerDesktopGroup

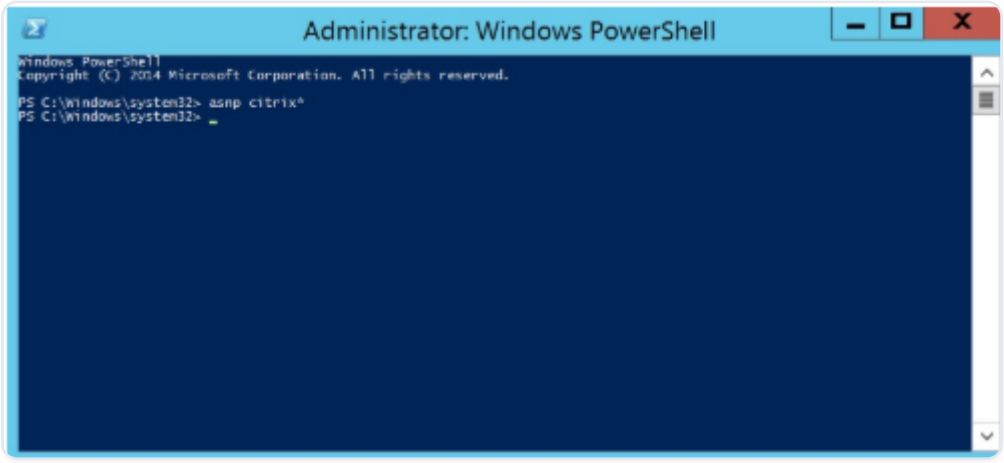
禁用或启用现有代理桌面组或更改其设置。有关此 cmdlet 的更多信息，请参阅 `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`

#### Get-BrokerDesktopGroup

检索符合指定条件的桌面组。Get-BrokerDesktopGroup cmdlet 的输出包括组的 **ProductCode** 和 **LicenseModel** 属性。如果尚未使用 New-BrokerDesktopGroup 或 Set-BrokerDesktopGroup 设置这些属性，则返回 null 值。如果为 null，则使用站点范围的许可模型和产品代码。有关此 cmdlet 的更多信息，请参阅 `<https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>`。

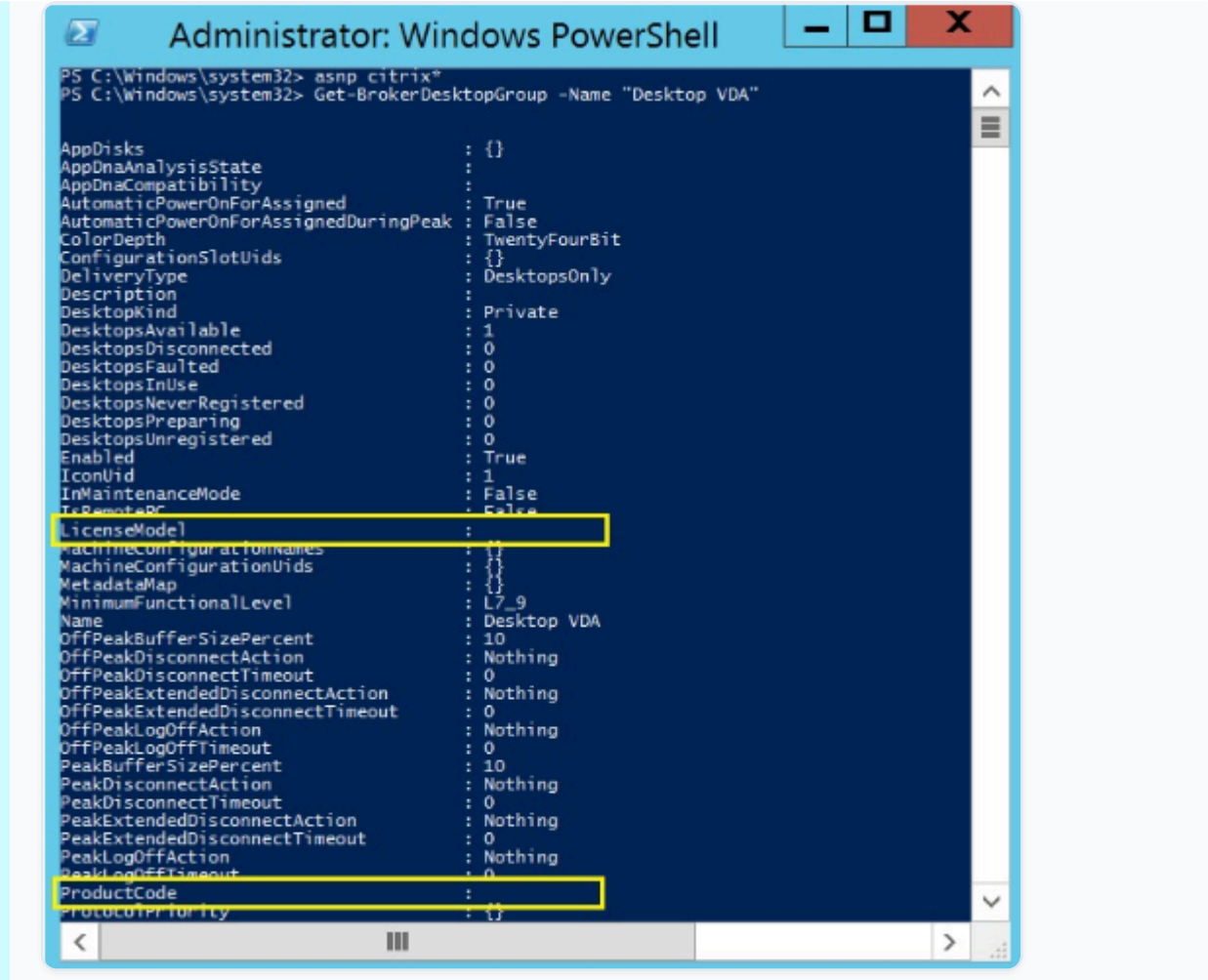
### 为每个交付组配置不同的许可产品和模型

1. 以管理员权限打开 PowerShell 并添加 Citrix 管理单元。

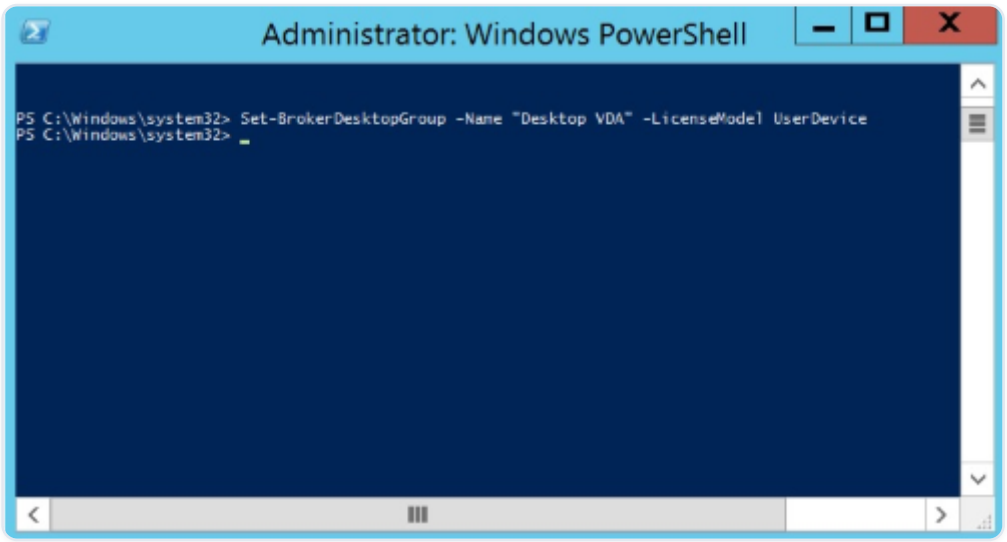



2. 运行命令 **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** 以查看当前许可证配置。查找参数 **LicenseModel** 和 **ProductCode**。如果您之前未配置这些参数，它们可能为空白。

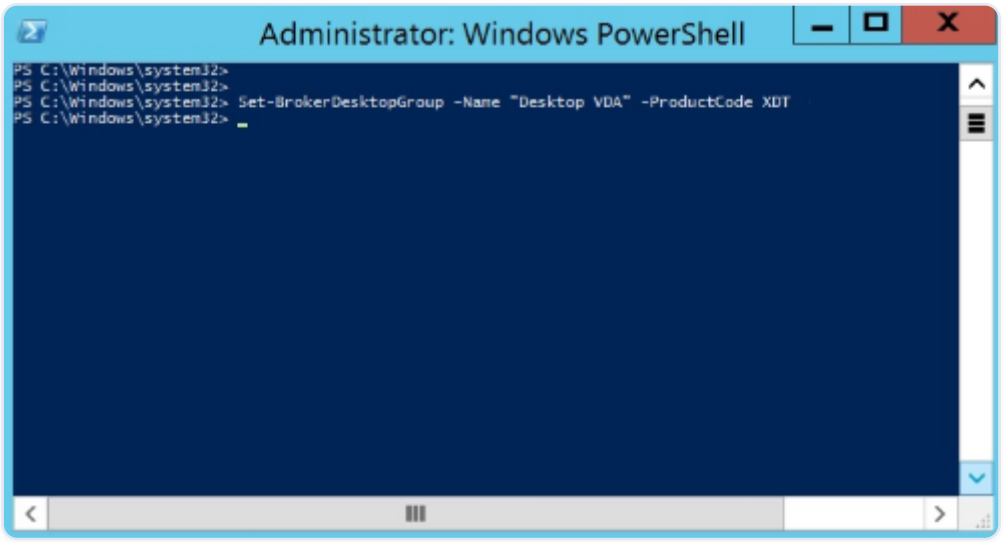
> **注意：**
>
> 如果交付组未设置许可信息，则默认为 **站点级别站点许可证**。




3. 通过运行命令更改许可模型：**Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel**。

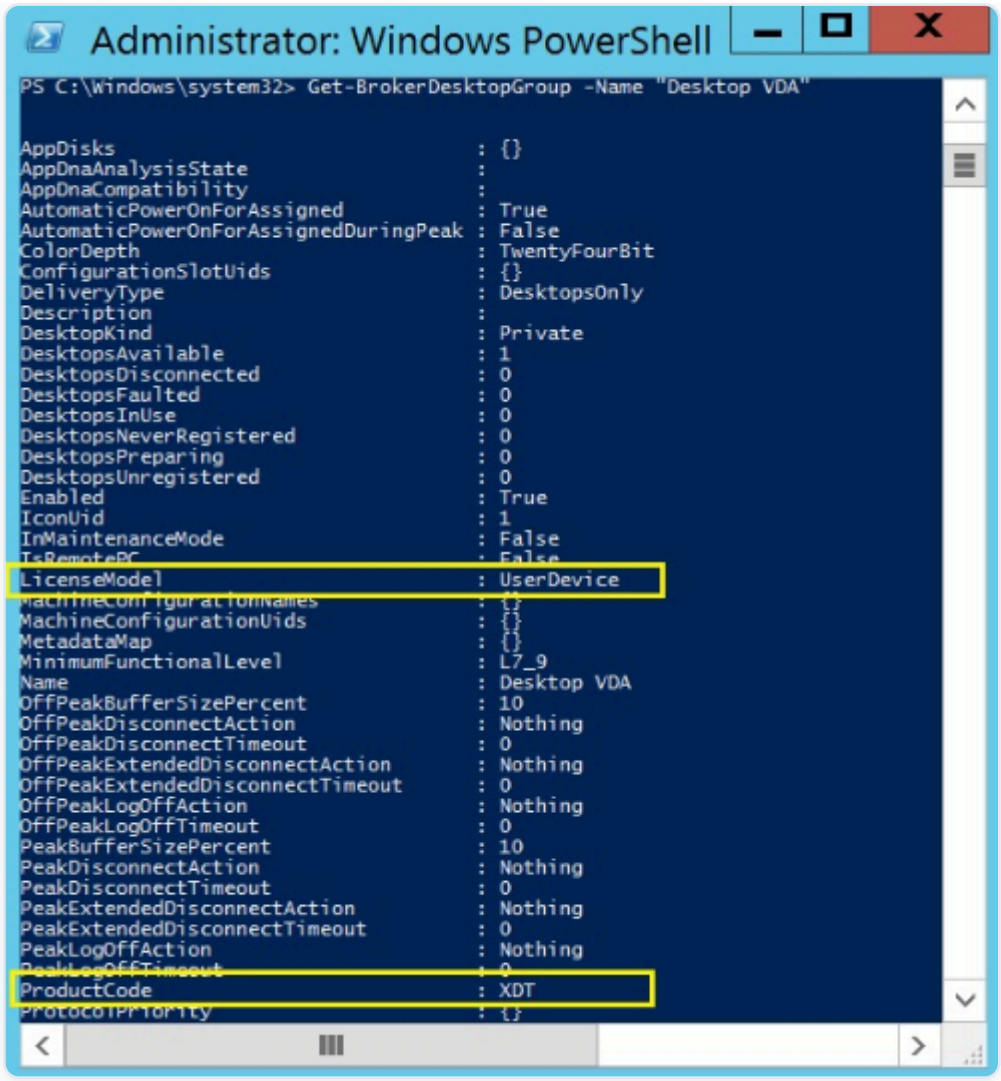


4. 通过运行以下命令更改许可证产品：**Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode**。



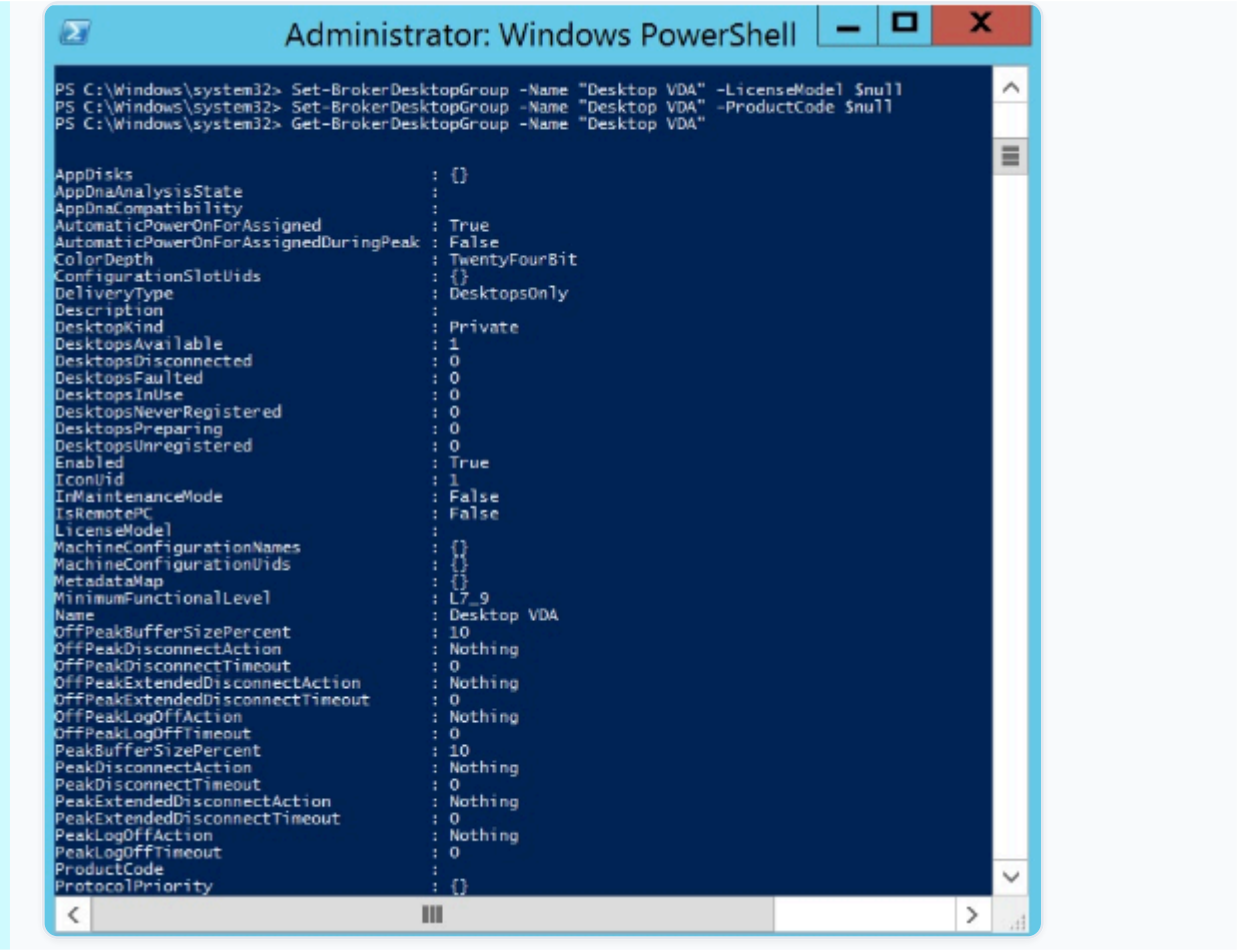

5. 输入命令 **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** 以验证更改。

> **注意：**
>
> 您不能在同一站点中混合搭配版本。例如，高级版和增强版许可证。如果您拥有不同版本的许可证，则需要多个站点。




6. 通过运行与前面步骤中描述的相同的 **Set-BrokerDesktopGroup** 命令，并将其值设置为 **$null**，来删除许可证配置。

> **注意：**
>
> Studio 不显示每个交付组的许可证配置。使用 PowerShell 查看当前配置。




## 示例

此 PowerShell cmdlet 示例说明了如何为两个现有交付组设置多类型许可，以及如何创建和设置第三个交付组。

要查看与交付组关联的许可证产品和许可证模型，请使用 **Get-BrokerDesktopGroup** PowerShell cmdlet。

1. 我们将第一个交付组设置为 XenApp® 和并发。

   **Set-BrokerDesktopGroup -Name "适用于 Citrix Virtual Apps Premium 并发版的交付组" -ProductCode MPS -LicenseModel Concurrent**

2. 我们将第二个交付组设置为 XenDesktop® 和并发。

   **Set-BrokerDesktopGroup -Name "适用于 Citrix Virtual Desktops Premium 并发版的交付组" -ProductCode XDT -LicenseModel Concurrent**

3. 我们创建并设置第三个交付组，用于 XenDesktop 和用户设备。

**New-BrokerDesktopGroup -Name "Citrix Virtual Desktops Premium UserDevice 的交付组" -PublishedName "我的桌面" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice**

# 许可常见问题解答

> **注意：**
>
> - 有关 COVID-19 大流行相关的业务连续性资源，请参阅 CTX27055。
> - 有关维护业务连续性的一般信息，请参阅 业务连续性 — 按需。
> - 有关当前 Citrix 许可证服务器的更多信息，请参阅 许可。

## Citrix® 许可

### 如何获取我的许可证文件?

我们会通过电子邮件发送许可证访问代码。使用许可证访问代码生成许可证文件有三种方法：

- 从您的 MyAccount 页面上的 `citrix.com` 访问**管理许可证**。有关详细信息，请参阅 在 citrix.com 上管理许可证。
- Citrix Studio 用于分配您的购买，许可证文件会自动安装到您的 Citrix 许可证服务器上。
- Citrix 许可证服务器中的 Citrix Licensing Manager 用于分配您的购买并安装您的许可证文件。有关详细信息，请参阅 安装许可证。

### 如何在 MyAccount 上分配许可证?

请参阅 分配许可证。

### 如何将已分配的许可证添加到许可证服务器?

请参阅 修改许可证。

### Citrix 许可使用哪些 TCP 端口?

- 许可证服务器端口号是 27000
- 供应商守护程序端口号是 7279
- 管理控制台 Web 端口是 8082
- 许可 Web 服务端口是 8083

### 什么是 Citrix 许可证服务器?

Citrix 许可证服务器是一个允许在网络中共享许可证的系统。有关详细信息，请参阅许可操作概述。

### 我可以虚拟化或群集 Citrix 许可证服务器吗?

是的。您可以虚拟化或群集 Citrix 许可证服务器。有关详细信息，请参阅群集许可证服务器。

### 如果我虚拟化 Citrix 许可证服务器，有哪些好处?

虚拟化 Citrix 许可证服务器可提供冗余解决方案。该解决方案允许在多个物理服务器之间移动，而无需停机。

### 如果我虚拟化 Citrix 许可证服务器，是否有任何限制需要考虑?

没有。

### Citrix 许可证服务器是否管理我的 Citrix Virtual Apps and Desktops™ 部署的所有许可证?

Citrix 许可证服务器管理您为 Citrix Virtual Apps™ and Desktop 收到的所有许可证，但与 Citrix Gateway 配合使用的 Premium Edition 中的许可证除外。那些安全导向的网络设备所需的内置于网络设备中的许可证服务器管理这些许可证。

### 什么是 Citrix 许可管理器?

Citrix Licensing Manager 允许从您安装了 Citrix Licensing Manager 的许可证服务器下载和分配许可证文件。Citrix Licensing Manager 是推荐的许可证服务器管理方法，具有以下功能：

- 将许可证服务器通过短代码注册到 Citrix Cloud™ 并轻松取消注册。
- 配置用户和组帐户。
- 使用控制板显示已安装、正在使用、已过期和可用的许可证以及客户成功服务日期。
- 导出许可证使用数据以用于报告。
- 配置历史使用数据保留期。默认数据保留期为 180 天。
- 使用许可证访问代码或下载的文件在许可证服务器上简化许可证文件的安装。
- 启用和禁用许可证突发模式。
- 配置客户体验改善计划 (CEIP) 和 Call Home。
- 自动或手动检查客户成功服务续订许可证，并在找到时通知您或安装许可证。
- 通知您许可证服务器状态 - 缺少启动许可证、时间问题、上传程序故障。
- 修改以下端口：
    - 许可证服务器 (默认 27000)
    - 供应商守护程序 (默认 7279)

- 许可 Web 服务 (默认 8083)

有关详细信息，请参阅 Citrix Licensing Manager。

#### Citrix 许可证管理控制台在哪里?

License Administration Console 不再受支持，已从 License Server 版本 11.16.6 中移除。我们建议您使用 Citrix Licensing Manager。

如果 License Server 与 Studio 位于同一域或受信任域中，则可以使用 Studio 管理和跟踪许可。

有关详细信息，请参阅 Citrix Licensing Manager。

#### 什么是许可证分配期?

许可证分配期是指 Citrix Virtual Apps and Desktops 许可证分配给用户或设备的期限。默认许可证分配期为 90 天。

#### 我如何知道我的组织购买了多少许可证?

所有购买的许可证都可以在 `<https://www.citrix.com>` 上的“**我的帐户**”页面中通过安全的“**管理许可证**”工具箱随时 (24x7) 查看和访问。

#### 我如何知道任何时候有多少许可证正在使用中?

Citrix Licensing Manager 和 Studio 提供实时许可证使用情况的详细信息。

#### License Server 灾难恢复和维护

有关 License Server 灾难恢复和维护的信息，请参阅 Citrix Licensing 文档中的 灾难恢复和维护。

### Citrix 虚拟应用和桌面许可

#### Citrix Virtual Apps and Desktops 如何获得许可?

Citrix Virtual Apps and Desktops 许可提供用户/设备和并发许可模式。

#### 用户/设备：

灵活的用户/设备模型与以下各项保持一致：

- 企业范围的桌面使用。
- 基础 Microsoft 桌面虚拟化许可。
- 适用于只需要偶尔访问其虚拟桌面和应用程序的客户的并发许可。

用户/设备许可允许用户从无限数量的设备访问其虚拟桌面和应用程序。设备许可允许无限数量的用户从单个设备访问其虚拟桌面和应用程序。此方法为您提供了最大的灵活性，并改进了与 Microsoft 桌面虚拟化许可的一致性。

> **重要提示：**
>
> 您无法手动将许可证分配给用户或设备。许可证服务器或云服务会分配许可证。对于用户/设备许可，一旦分配了许可证，除非在 90 天不活动之后，否则无法将其分配给其他用户。

> **并发：**
>
> 并发许可证允许任何用户和任何设备连接到无限数量的虚拟应用程序和桌面。许可证仅在活动会话期间占用。如果会话断开连接或终止，许可证将返回到池中。

有关用户/设备许可的更多信息，请参阅用户/设备许可证；有关并发许可的更多信息，请参阅并发许可证。

**在购买许可证之前，是否可以试用 Citrix Virtual Apps and Desktops?**

是的。您可以下载 Citrix Virtual Apps and Desktops 软件并以试用模式运行。试用模式允许您在本地使用 Citrix Virtual Apps and Desktops 30 天，支持 10 个连接，无需许可证。有关详细信息，请参阅评估许可证。

适用于 Citrix Cloud 的 Citrix DaaS™（以前称为 Citrix Virtual Apps and Desktops 服务）可根据批准提供试用服务。请咨询您的 Citrix 代表以获取更多详细信息。

**Citrix 如何定义 Citrix Virtual Apps and Desktops 的并发性?**

Citrix Virtual Apps and Desktops 并发模型允许任何用户和任何设备连接到无限数量的虚拟应用程序和桌面。许可证仅在活动会话期间使用。如果会话断开连接或终止，许可证将返回到池中以供重新颁发。有关详细信息，请参阅并发许可证。

**我可以在一个通用许可证服务器上部署多个版本的 Citrix Virtual Apps and Desktops 许可证吗?**

可以。许可证服务器同时管理 Citrix Virtual Apps 和 Desktops 的许可证。我们建议您安装最新版本的许可证服务器。如果您不确定您的许可证服务器版本是否为最新版本，请将其与 Citrix 下载站点上的版本号进行比较以进行验证。

### 单个站点可以使用 Citrix Virtual Apps 和 Citrix Virtual Apps and Desktops 许可证?

根据版本，单个 Citrix Virtual Apps 或 Citrix Virtual Apps and Desktops 站点可以支持两种许可模型 - 用户/设备或并发。单个 Citrix Virtual Apps 或 Citrix Virtual Apps and Desktops 站点只能支持一个版本。有关详细信息，请参阅多类型许可。

支持多类型许可的最低版本是 XenApp 和 XenDesktop 7.15 长期服务版本 (LTSR) 以及 Citrix Virtual Apps and Desktops 7 1808。

### 如果我的许可证服务器上安装了 Citrix Virtual Apps and Desktops 用户/设备或 Citrix Virtual Apps and Desktops 并发许可证，我可以选择 Citrix Virtual Apps 并发作为产品模型?

如果您将 Citrix Virtual Apps 作为 Citrix Virtual Apps and Desktops 高级版或尊享版的功能使用，则其许可模型与 Citrix Virtual Apps and Desktops 的高级版或尊享版相同。如果您已购买 Citrix Virtual Apps and Desktops，即使您计划仅使用 Citrix Virtual Apps 功能，也应将许可配置为该产品。仅当您的许可证服务器上安装了 Citrix Virtual Apps 并发独立许可证时，才应选择此产品作为产品模型。

### 每个 Citrix Virtual Apps 和 Citrix Virtual Apps and Desktops 版本都包含哪些产品组件?

有关按版本划分的完整功能矩阵，请参阅Citrix Virtual Apps and Desktops 功能。

### 如何根据 Citrix Virtual Apps and Desktops 最终用户许可协议 许可 Citrix Virtual Desktops™ 环境?

要根据 Citrix Virtual Apps and Desktops EULA 在用户/设备或并发许可模型下部署 Citrix Virtual Apps and Desktops，请将许可证文件应用到您的许可证服务器。许可证服务器随后控制并监控许可证合规性。我们建议您根据所购买的产品配置您的产品。例如，如果您购买了 Citrix Virtual Apps and Desktops 高级版但只想使用 Citrix Virtual Apps 功能，请将产品配置为 Citrix Virtual Apps and Desktops 以符合合规性。有关详细信息，请参阅产品许可证合规性中心。

### 如何根据 Citrix Virtual Apps EULA 许可 Citrix Virtual Apps 环境?

要根据 Citrix Virtual Apps EULA 在并发许可模型下部署 Citrix Virtual Apps，请将许可证文件应用到您的许可证服务器。许可证服务器随后控制并监控许可证合规性。

### Citrix Virtual Apps and Desktops 服务选项：长期服务版本 (LTSR) 或当前版本 (CR) 是否有许可要求?

Citrix Virtual Apps and Desktops 服务选项（例如长期服务版本）是客户成功服务计划的一项权益。您必须拥有有效的客户成功服务才能享受 LTSR 的权益。有关详细信息，请参阅 Citrix Virtual Apps、Citrix Virtual Apps and Desktops 和 Citrix Hypervisor 服务选项。

### 远程浏览器隔离 (RBI) 服务池化小时数如何工作?

当您购买至少 25 个服务用户时，您将获得 5000 小时的服务使用权，这些小时数在所有用户之间共享。后续购买用户权限不会增加池化小时数权益。要增加服务小时数权益，请购买附加包。

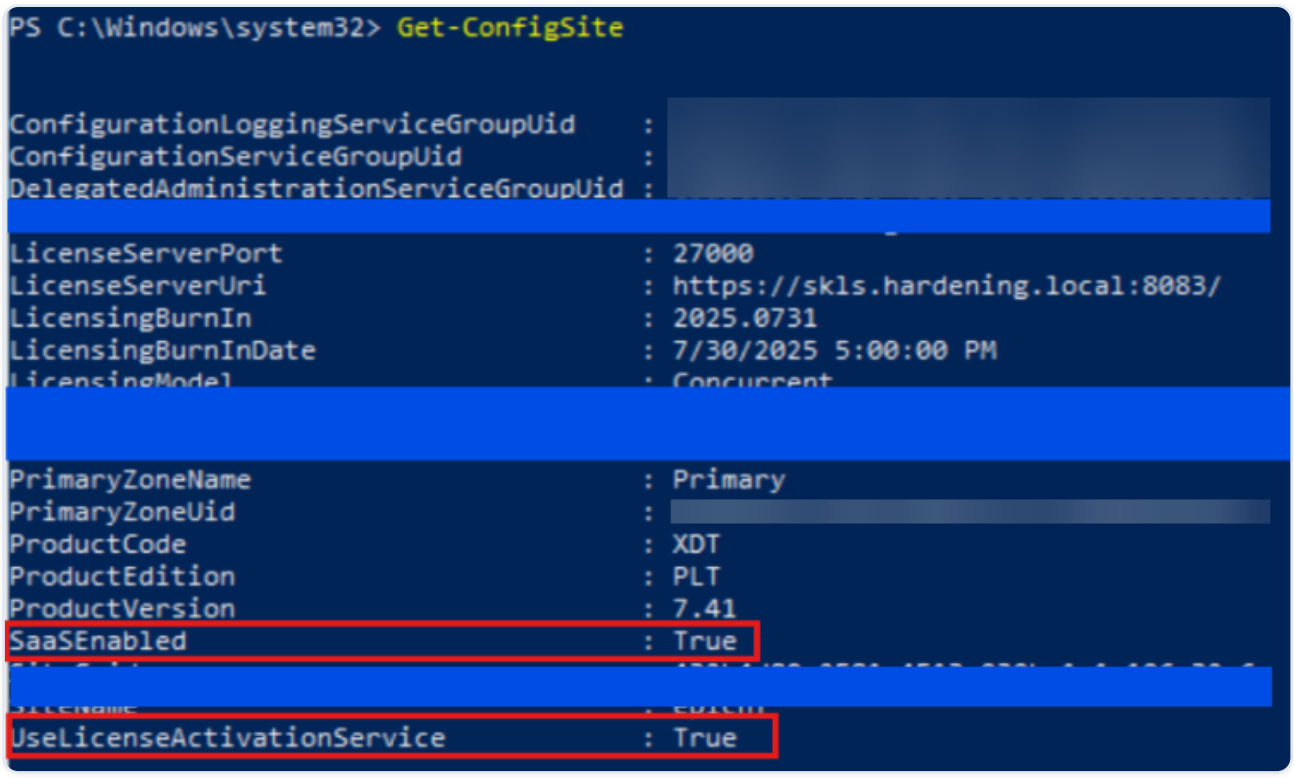
### 我可以将远程电脑访问与 CCU 许可证结合使用吗?

是的。

有关远程电脑访问的信息，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/install-configure/remote-pc-access.html)。

### 如何检查站点的 LAS 状态?

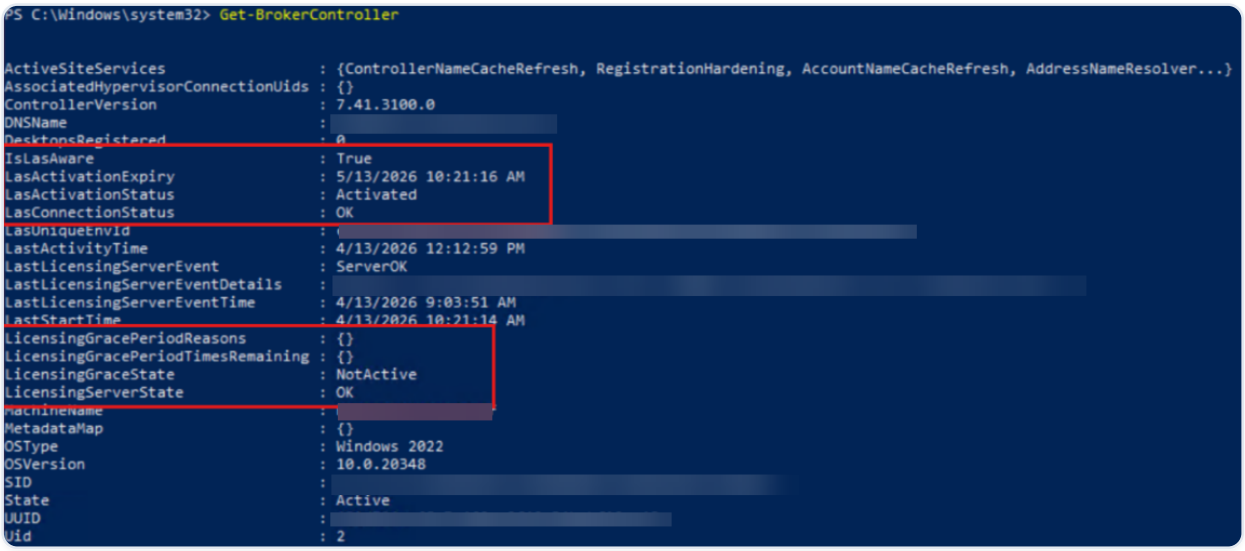
运行 `Get-configsite` 以检查 LAS 激活状态和 SaaS 位状态。



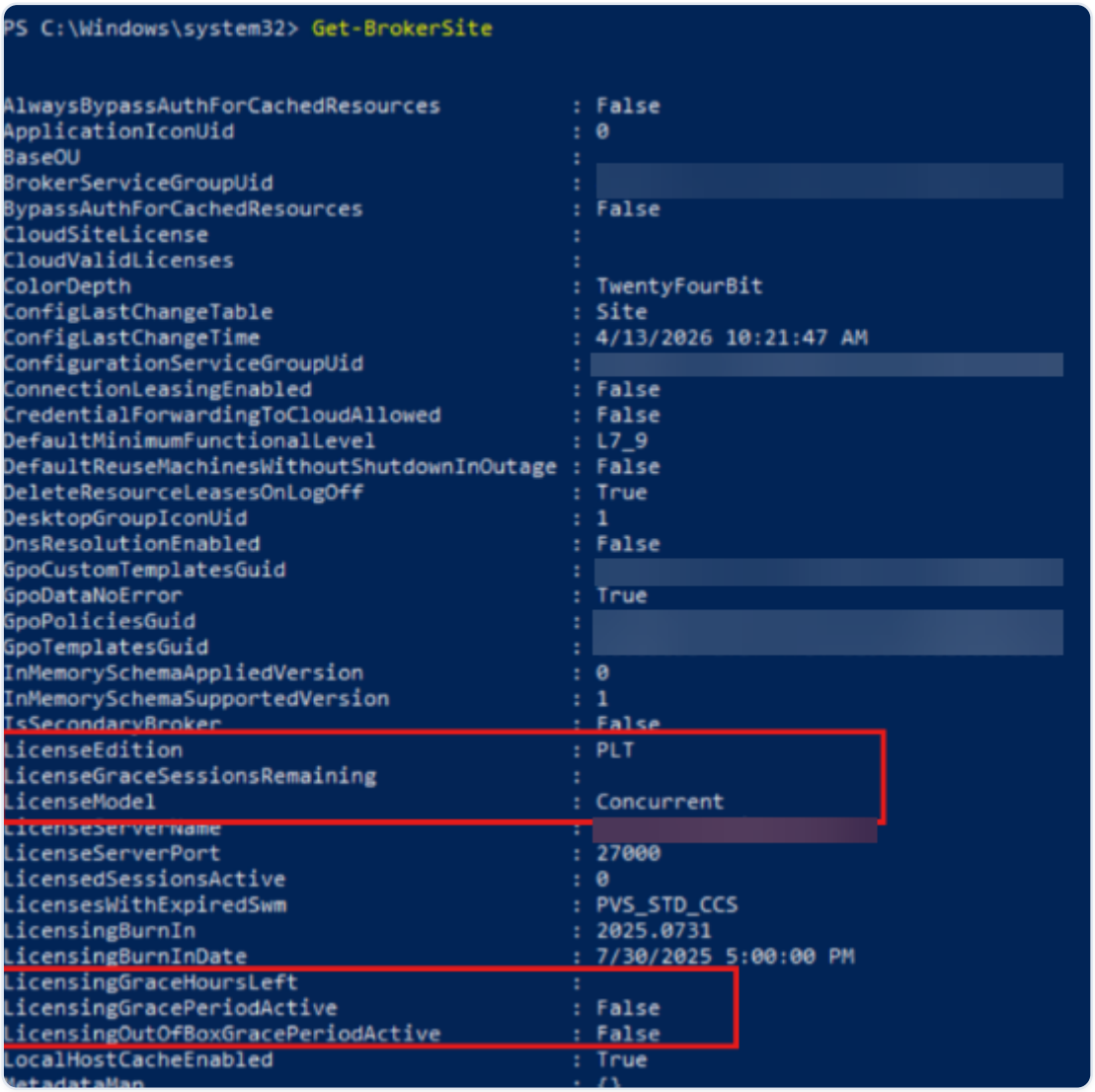

### 如何验证站点是否处于许可证缓存模式?

运行 `Get-Brokercontroller` 和 `Get-brokersite` 以获取缓存模式和剩余时间的详细信息。

- `Get-Brokercontroller` 输出：




- `Get-brokersite` 输出：




有关命令的详细信息，请参阅：

- Get-BrokerController

- Get-ConfigSite

有关 Delivery Controller 事件查看器日志中与许可相关的信息，请参阅与许可事件相关的事件查看器日志。

## 用户或设备许可证

### 思杰如何在用户/设备许可模型中向用户分配许可证?

在用户/设备许可模型中，许可证服务器将许可证分配给唯一的用户 ID。它允许该单个用户从无限数量的设备进行无限连接。如果用户连接到桌面或设备，则该用户需要分配给该用户的一个许可证才能访问虚拟桌面或应用程序。许可证服务器或云服务会分配许可证。您无法手动分配这些许可证。许可证分配给用户，而不是共享设备。许可证分配后，在 90 天不活动期过后才能分配给其他用户。有关详细信息，请参阅用户/设备许可证。

### Citrix 如何在用户/设备许可模型中定义许可设备？

许可设备需要唯一的端点设备 ID。在用户/设备模型下，设备是指您授权任何个人用于访问 Citrix Virtual Apps and Desktops 实例的任何设备。对于共享设备，单个 Citrix Virtual Apps and Desktops 用户/设备许可证可以支持共享该设备的多个用户。例如，共享设备可以是教室工作站或医院中的临床工作站。

### 我可以将我的 Citrix Virtual Desktops 标准版 并发许可证转换为用户/设备模型吗?

您无法将 Citrix Virtual Desktops 标准版 并发许可证转换为 Citrix Virtual Desktops 标准版 用户/设备许可证。同样，您也无法将 Citrix Virtual Desktops 标准版 用户/设备许可证转换为 Citrix Virtual Desktops 标准版 并发许可证。

如果您拥有 Citrix Virtual Desktops 标准版并发许可证并希望使用用户/设备许可模型，请升级到 Citrix Virtual Apps and Desktops 高级版或白金版。

| 从 | 到标准并发 | 到标准用户/设备 | 到高级用户/设备 | 到至尊版用户/设备 |
|---|---|---|---|---|
| Citrix Virtual Desktops 标准版并发许可证 | N/A | 不允许并发到用户/设备转换 | 您无法转换许可证模型，但可以升级到 Citrix Virtual Apps and Desktops 高级版或至尊版。 | 您无法转换许可证模型，但可以升级到 Citrix Virtual Apps and Desktops 高级版或至尊版。 |

| 从 | 到标准并发 | 到标准用户/设备 | 到高级用户/设备 | 到至尊版用户/设备 |
|---|---|---|---|---|
| 思杰虚拟桌面标准版用户/设备许可证 | 不允许用户/设备到并发转换 | N/A | N/A | N/A |

**并发许可与用户/设备许可有何不同?**

我们基于并发设备连接来实施并发许可。并发许可证仅在设备建立活动连接时才使用。连接结束后，并发许可证将返回到许可证池中以供立即使用。我们建议将此许可模型用于偶尔使用。用户/设备许可证在一段时间内租用，在租约到期之前其他用户无法使用。

**在用户/设备模型下，我们可以在同一企业中同时为用户和设备分配许可证?**

是的。这两种类型可以同时存在于同一企业中。许可证服务器会根据使用情况，将许可证最佳地分配给用户或设备。您无法手动分配这些许可证。

**我如何决定要许可多少用户或设备?**

评估用例要求以确定适当的许可证数量。用户/设备许可允许从无限数量的设备无限制地访问无限数量的虚拟桌面和虚拟应用程序。并发许可允许从单个设备无限制地访问无限数量的虚拟桌面和虚拟应用程序，该设备可供无限数量的用户使用。请考虑以下公式：

```
(Number of total users) – (number of users that only access exclusively

 with shared devices) + (number shared devices) = total number

 of licenses to buy.



For example, there are 1000 total users at the hospital. If 700 of them
access only

Citrix Virtual Desktops from 300 shared devices in the hospital, the
number of

licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

**在用户/设备模型下，一个获得许可的用户最多可以使用多少设备连接到我的环境?**

每个许可用户都有权使用无限数量的连接设备或离线设备。

**在用户/设备模型下，可以访问许可设备的最大用户数是多少?**

每个许可设备可以为组织内的无限数量用户提供服务。

**在用户/设备模型下，许可用户在任何给定时间可以使用的虚拟桌面或 RBI Web 应用程序的最大数量是多少?**

每个许可用户可以连接到无限数量的虚拟桌面或 Web 应用程序。

**我可以购买 Citrix Virtual Apps and Desktops 许可证来增加现有 Citrix Virtual Apps and Desktops 环境中的许可用户/设备数量?**

是的。您可以购买 Citrix Virtual Apps and Desktops 许可证来增加现有 Citrix Virtual Apps and Desktops 环境中的许可用户/设备数量。

**如何释放授权的用户/设备许可证?**

要释放授权用户/设备的分配，请根据 EULA 条款使用 `udadmin` 实用程序。许可证服务器随后会将许可证分配给下一个适当的用户/设备。有关详细信息，请参阅 显示或释放用户或设备的许可证。

**如果我超出了购买的用户/设备许可证数量，会发生什么?**

用户/设备许可证包含 10% 的透支额度，该额度在生成许可证时包含在内。透支额度也包含在已安装的许可证数量中。如果使用高峰超出已安装数量（包括透支额度），则会拒绝更多用户的访问。购买并部署新许可证以启用更多用户的访问。

如果所有许可证（包括许可证透支额度）都在使用中，则许可证突发模式允许对产品进行无限连接。许可证突发模式让您有时间确定为什么超出了最大许可证数量，并在不中断用户的情况下购买更多许可证。此期限持续到 15 天过去或您安装更多零售许可证（以先发生者为准）。有关详细信息，请参阅 许可证突发模式。

Director 显示许可证缓存模式状态。有关详细信息，请参阅 Director 控制板上的面板。

**许可用户在任何给定时间可以使用的虚拟应用程序的最大数量是多少?**

每个许可用户可以连接到无限数量的虚拟应用程序。

**如果许可用户离开我的组织，会发生什么情况?**

当现有许可用户离开您的组织时，您可以释放离职用户的许可证，而无需通知 Citrix。使用 `udadmin` 实用程序释放许可证。如果您不释放许可证，许可证服务器会在 90 天不活动后自动释放任何许可证。此信息受 EULA 中规定的条款约束。

**如果许可用户长期缺席，会发生什么情况?**

如果现有许可用户长期缺席，您可以释放许可证而无需通知 Citrix，以便该许可证可用于重新分配。使用 `udadmin` 实用程序释放许可证。

#### 如果我的组织更换了许可设备，会发生什么情况?

如果您更换现有许可设备，您可以释放许可证而无需通知 Citrix，以便该许可证可用于重新分配。使用 `udadmin` 实用程序释放许可证。

#### 如果许可设备长时间停止服务，会发生什么情况?

当现有许可设备长时间停止服务时，您可以释放许可证而无需通知 Citrix，以便该许可证可用于重新分配。使用 `udadmin` 实用程序释放许可证。如果您不释放许可证，许可证服务器会在 90 天不活动后自动释放任何许可证。此信息受 EULA 中规定的条款约束。

#### 在我将许可证分配给设备或用户之后，可以将用户许可证切换到设备许可证，反之亦然吗?

是的。此更改是自动发生的。许可证服务器根据使用模式将许可证分配给用户或设备。如果使用模式发生变化，许可证服务器可能会根据新的使用情况切换分配。许可证服务器始终以对客户最经济的方式分配许可证。此外，许可证服务器会监控许可证，以识别 90 天分配期后的**未使用**许可证。您可以将 90 天分配期后识别为未使用的许可证重新分配给其他用户或设备。

### 并发许可证

#### 在并发模型下，Citrix Virtual Apps and Desktops 许可用户在任何给定时间可以使用的虚拟桌面的最大数量是多少?

一个端点可以服务多个用户，并允许无限连接。

#### 我可以将来自旧版 Citrix Virtual Apps and Desktops 的并发许可证以及新的用户/设备或并发许可证部署到单个许可证服务器吗?

是的。您可以继续使用相同的许可证服务器以支持用户/设备或并发许可部署。

#### 我可以在单个许可证服务器上部署并发许可证和用户/设备或并发许可证?

可以。您可以继续使用同一个许可证服务器来支持并发以及用户/设备或并发许可部署。

#### Citrix Virtual Apps and Desktops Advanced 和 Premium 版本是否包含 Citrix Virtual Apps 并发许可证?

Citrix Virtual Apps and Desktops Advanced 和 Premium 用户/设备许可证仅出于兼容性目的包含并发 Citrix Virtual Apps 许可证。这些并发许可证仅适用于与用户/设备许可证不兼容的早期产品版本。用户/设备许可证中包含的并发兼容性许可证仅可用于以下版本：XenApp 6.5 之前的版本和 XenDesktop 5.0 服务包 1 之前的版本。

#### 如果我超出了购买的并发许可证数量，会发生什么?

如果所有许可证都在使用中，许可证突发模式将允许对产品进行无限制连接。许可证突发模式让您有时间确定超出最大许可证数量的原因，并在不中断用户的情况下购买更多许可证。此期限持续到 15 天过去或您安装更多零售许可证，以先发生者为准。有关详细信息，请参阅许可证突发模式。

Director 显示许可证缓存模式状态。有关详细信息，请参阅Director 控制板上的面板。

## 透支许可证

### 如何获取透支许可证?

支持用户/设备、用户或设备许可证模式的产品（不包括 Citrix Cloud）包含许可证透支功能，使您能够使用有限数量的额外许可证来防止访问被拒绝。我们提供任何透支功能作为一种便利，而不是作为许可证权利。并发许可证和服务器许可证不包含透支。任何已使用的透支许可证必须在首次使用后的 30 天内购买，但使用不限于 30 天。Citrix 保留在新产品版本中删除任何透支功能的权利。有关详细信息，请参阅许可证透支。

### 如何识别许可证透支?

您可以在 Citrix Licensing Manager 中查看使用情况信息，包括透支许可证的数量。Studio 也包含透支使用情况信息。

### 当透支许可证被使用时会发生什么?

从您已安装的许可证中分配一个许可证，以启用对您的 Citrix Virtual Apps and Desktops 环境的访问。此透支许可证提供与您的其他许可证相同的访问权限和功能。

### 当我的透支许可证被使用时，我能收到警报吗?

目前，当透支许可证被使用时，没有提供特定的警报。

### 透支许可证可以使用多久?

在首次使用后的 30 天内购买所有已使用的透支许可证。

## 其他产品特定的许可信息

- 思杰 ADC
- 思杰云
- 思杰端点管理
- 思杰网关
- 思杰 Hypervisor
- 思杰许可

# 应用程序

## 简介

如果您的部署仅使用交付组（而不使用应用程序组），则将应用程序添加到交付组。如果您还有应用程序组，通常会将应用程序添加到应用程序组。此指导可简化管理。应用程序必须始终属于至少一个交付组或应用程序组。

在“添加应用程序”向导中，您可以选择一个或多个交付组，或一个或多个应用程序组，但不能同时选择两者。尽管您以后可以更改应用程序的组关联（例如，将应用程序从应用程序组移动到交付组），但最佳实践不鼓励增加这种复杂性。将您的应用程序保留在一种类型的组中。

当您将应用程序与多个组关联时，如果您没有足够的权限在所有这些组中查看该应用程序，则可能会出现可见性问题。在这种情况下，请咨询具有更高权限的管理员，或者扩展您的范围以包括与该应用程序关联的所有组。

如果您向相同的用户发布两个同名应用程序（可能来自不同的组），请在 Studio 中更改 `Application name (for user)` 属性。否则，用户将在 Citrix Workspace™ 应用程序中看到重复的名称。

您可以在添加应用程序时或之后更改其属性（设置）。您还可以在添加应用程序时或之后更改应用程序所在的应用程序文件夹。

有关详细信息，请参阅：

- 创建交付组
- 创建应用程序组
- 标签

## 添加应用程序

您可以在创建交付组或应用程序组时添加应用程序。这些过程在创建交付组和创建应用程序组中进行了详细说明。以下过程描述了在创建组后如何添加应用程序。

须知：

- 您无法将应用程序添加到远程电脑访问交付组。
- 您不能使用“添加应用程序”向导从交付组或应用程序组中删除应用程序。这是一项单独的操作。

要添加一个或多个应用程序：

1. 在 Studio 导航窗格中选择**应用程序**，然后在“操作”窗格中选择**添加应用程序**。

2. “添加应用程序”向导启动时会显示一个**简介**页面，您可以选择在将来启动此向导时不再显示该页面。
3. 该向导将引导您完成**组**、**应用程序**和**摘要**页面。完成每个页面后，单击**下一步**，直到到达**摘要**页面。

如果要将应用程序添加到单个交付组或应用程序组，可采用步骤 1 的替代方法：

- **仅向一个交付组添加应用程序：在步骤 1 中，在 Studio 导航窗格中选择交付组**，在中间窗格中选择一个交付组，然后在“操作”窗格中选择**添加应用程序**。向导不会显示**组**页面。
- **仅向一个应用程序组添加应用程序：在步骤 1 中，在 Studio 导航窗格中选择应用程序**，在中间窗格中选择一个应用程序组，然后在“操作”窗格中应用程序组名称下选择**添加应用程序**条目。向导不会显示**组**页面。

### 组页面

此页面列出了站点中的所有交付组。如果您还创建了应用程序组，则此页面会列出应用程序组和交付组。您可以从任一组中选择，但不能同时从两组中选择。换句话说，您不能同时将应用程序添加到应用程序组和交付组。通常，如果您正在使用应用程序组，请将应用程序添加到应用程序组，而不是交付组。

添加应用程序时，请选中至少一个交付组（或应用程序组，如果可用）旁边的复选框。每个应用程序都必须始终与至少一个组关联。

### 应用程序页面

单击**添加**以显示应用程序源。

- **从“开始”菜单：** 在所选交付组中的计算机上发现的应用程序。选择此源时，将启动一个新页面，其中包含发现的应用程序列表。选中要添加的应用程序的复选框，然后单击**确定**。

  如果出现以下情况，则无法选择此源：(1) 您选择了没有关联交付组的应用程序组，(2) 您选择了关联交付组中不包含任何计算机的应用程序组，或者 (3) 您选择了不包含任何计算机的交付组。
- **手动定义：位于站点或网络中其他位置的应用程序。选择此源时，将启动一个新页面。输入可执行文件的路径、工作目录、可选命令行参数以及管理员和用户的显示名称。输入此信息后，单击确定**。
- **现有：** 以前添加到站点的应用程序。选择此源时，将启动一个新页面，其中包含发现的应用程序列表。选中要添加的应用程序的复选框，然后单击 **确定**。

  如果站点没有应用程序，则无法选择此源。

- **App-V：App-V 软件包中的应用程序。选择此源时，将启动一个新页面，您可以在其中选择 App-V 服务器或应用程序库。从结果显示中，选中要添加的应用程序的复选框，然后单击确定**。有关详细信息，请参阅 App-V。

  如果未为站点配置 App-V，则无法选择此源。

- **应用程序组**：应用程序组。选择此源时，将启动一个新页面，其中包含应用程序组列表。（尽管显示内容也列出了每个组中的应用程序，但您只能选择组，而不能选择单个应用程序。）所选组中的所有当前和未来应用程序都将添加。选中要添加的应用程序组的复选框，然后单击 **确定**。

  如果 (1) 没有应用程序组，或者 (2) 所选的交付组不支持应用程序组（例如，具有静态分配计算机的交付组），则无法选择此源。

如表中所示，如果不存在该类型的有效源，则无法选择“**添加**”列表中的某些源。不兼容的源（例如，不能将应用程序组添加到应用程序组）不包含在列表中。已经添加到您所选组的应用程序无法选择。

您可以从此页面或以后更改应用程序的属性（设置）。

默认情况下，添加的应用程序放置在名为 `Applications` 的应用程序文件夹中。您可以从此页面或稍后更改应用程序。如果您尝试添加应用程序，并且同一文件夹中存在同名应用程序，系统会提示您重命名要添加的应用程序。您可以接受提供的新名称，也可以拒绝并重命名应用程序或选择其他文件夹。例如，如果 `app` 已存在于**应用程序**文件夹中，并且您尝试将另一个名为 `app` 的应用程序添加到该文件夹，则会提供新名称 `app_1`。

### 摘要页面

如果您要添加 10 个或更少的应用程序，其名称将列在“**要添加的应用程序**”中。如果您要添加 10 个以上的应用程序，则会指定总数。

查看摘要信息，然后单击**完成**。

## 更改应用程序的组关联

添加应用程序后，您可以更改应用程序关联的交付组和应用程序组。

您可以将应用程序拖动到其他组。这是使用“操作”窗格中命令的替代方法。

如果应用程序与多个交付组或应用程序组关联，则可以使用组优先级来指定检查多个组以查找应用程序的顺序。默认情况下，所有组的优先级均为 0（最高）。相同优先级的组会进行负载平衡。

应用程序可以与包含可交付应用程序的共享（非专用）计算机的交付组关联。如果 (1) 交付组包含共享计算机且是使用早于 7.9 的 XenDesktop 7.x 版本创建的，并且 (2) 您具有 `Edit delivery`

`group` 权限，则您还可以选择包含仅交付桌面的共享计算机的交付组。提交属性对话框时，交付组类型会自动转换为 `desktops and applications`。

1. 在 Studio 导航窗格中选择**应用程序**，然后在中间窗格中选择该应用程序。
2. 在“操作”窗格中选择**属性**。
3. 选择**组**页面。
    - 要添加组，请单击**添加**并选择**应用程序组**或**交付组**。（如果您尚未创建任何应用程序组，则唯一条目为**交付组**。）然后选择一个或多个可用组。与应用程序不兼容或已与应用程序关联的组无法选择。
    - 要删除组，请选择一个或多个组，然后单击**删除**。如果删除组关联会导致应用程序不再与任何组关联，则会收到应用程序将被删除的警报。
    - 要更改组的优先级，请选择该组，然后单击**编辑优先级**。选择一个优先级值，然后单击**确定**。
4. 完成后，单击**应用**以应用更改并保持窗口打开，或单击**确定**以应用更改并关闭窗口。

## 复制、启用或禁用、重命名或删除应用程序

以下操作可用：

- **复制：** 您可能希望复制应用程序以创建具有不同参数或属性的不同版本。复制应用程序时，它会自动使用唯一的后缀重命名并放置在原始应用程序旁边。您可能还希望复制应用程序，然后将其添加到不同的组。（复制后，移动应用程序最简单的方法是拖动它。）
- **启用或禁用：** 启用和禁用应用程序与启用和禁用交付组或应用程序组是不同的操作。
- **重命名：** 您一次只能重命名一个应用程序。如果您尝试重命名应用程序，并且同一文件夹或组中已存在同名应用程序，系统会提示您指定不同的名称。
- **删除：** 删除应用程序会将其从与之关联的交付组和应用程序组中移除，但不会从最初用于添加应用程序的源中移除。删除应用程序与从交付组或应用程序组中移除应用程序是不同的操作。

要复制、启用、禁用、重命名或删除应用程序：

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个或多个应用程序，然后在“操作”窗格中选择相应的任务。
3. 出现提示时，确认操作。

## 从交付组中删除应用程序

应用程序必须与至少一个交付组或应用程序组关联（属于）。如果您尝试从交付组中删除应用程序，而此操作将删除该应用程序与任何交付组或应用程序组的关联，则系统会通知您，如果继续，该应用程序将被删除。发生这种情况时，如果您想交付该应用程序，则必须从有效源再次添加它。

1. 在 Studio 导航窗格中选择 **交付组**。
2. 选择一个交付组。在中间下部窗格的“**应用程序**”选项卡上，选择要删除的应用程序。
3. 从“操作”窗格中选择**删除应用程序**。
4. 确认删除。

## 从应用程序组中删除应用程序

应用程序必须属于至少一个交付组或应用程序组。如果您尝试从应用程序组中删除某个应用程序，而此操作将导致该应用程序不再属于任何组，则系统会通知您，如果继续操作，该应用程序将被删除。发生这种情况时，如果您想交付该应用程序，则必须从有效源再次添加它。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择应用程序组，然后选择一个或多个应用程序。
3. 在“操作”窗格中选择**从应用程序组中删除**。
4. 确认删除。

## 更改应用程序属性

您一次只能更改一个应用程序的属性。

要更改应用程序的属性：

1. 在 Studio 导航窗格中选择**应用程序**。
2. 选择一个应用程序，然后在“操作”窗格中选择**编辑应用程序属性**。
3. 选择包含要更改的属性的页面。
4. 完成后，单击 **应用** 以应用所做的任何更改并保持窗口打开，或者单击 **确定** 以应用更改并关闭窗口。

在以下列表中，页面显示在括号中。

| 属性 | 页面 |
| --- | --- |
| 应用程序在 Citrix Workspace 应用程序中显示的类别/文件夹 | 交付 |

| 属性 | 页面 |
| --- | --- |
| 命令行参数；请参阅 将参数传递给已发布的应用程序 | 位置 |
| 应用程序可用的交付组和应用程序组 | 组 |
| 描述 | 标识 |
| 文件名扩展名和文件类型关联：应用程序自动打开哪些扩展名 | 文件类型关联 |
| 图标 | 交付 |
| StoreFront™ 关键字 | 标识 |
| 限制；请参阅配置应用程序限制 | 交付 |
| 名称：用户和管理员看到的名称 | 标识 |
| 可执行文件路径；请参阅向已发布的应用程序传递参数 | 位置 |
| 用户桌面上的快捷方式：启用或禁用 | 交付 |
| 可见性：限制哪些用户可以在 Citrix Workspace 应用程序中看到该应用程序。不可见的应用程序仍然可以启动。要使其不可用且不可见，请将其添加到其他组。 | 限制可见性 |
| 工作目录 | 位置 |

应用程序更改可能要等到当前应用程序用户从其会话注销后才能生效。

## 配置应用程序限制

配置应用程序限制以帮助管理应用程序使用。例如，您可以使用应用程序限制来管理同时访问应用程序的用户数量。同样，应用程序限制可用于管理资源密集型应用程序的并发实例数量。该限制有助于保持服务器性能并防止服务质量下降。

此功能限制由 Controller 代理的应用程序启动次数（例如，来自 Citrix Workspace 应用程序和 StoreFront），而不是可通过其他方法启动的正在运行的应用程序数量。这意味着应用程序限制在管

理并发使用时协助管理员，但并非在所有情况下都提供强制执行。例如，当 Controller 处于中断模式时，无法应用应用程序限制。

默认情况下，同时运行的应用程序实例数量没有限制。有多种应用程序限制设置。您可以配置其中任何一个或所有。

- 交付组中所有用户的应用程序最大并发实例数。
- 交付组中每个用户一个应用程序实例。
- 每台计算机的最大并发应用程序实例数（仅限 PowerShell）。

如果配置了限制，当用户尝试启动超出配置限制的应用程序实例时，将生成错误消息。如果配置了多个限制，当达到第一个限制时，将报告错误。

使用应用程序限制的示例：

- **最大并发实例数限制：** 在交付组中，您将应用程序 `Alpha` 的最大并发实例数配置为 15。之后，该交付组中的用户同时运行着该应用程序的 15 个实例。如果该交付组中的任何用户现在尝试启动 `Alpha`，则会生成错误消息。`Alpha` 未启动，因为它将超出配置的并发应用程序实例限制 (15)。
- **每个用户一个实例的应用程序限制：**在另一个交付组中，您为应用程序 `Beta` 启用了每个用户一个实例的选项。用户 Tony 成功启动了应用程序 `Beta`。当天晚些时候，当该应用程序仍在 Tony 的会话中运行时，他尝试启动 `Beta` 的另一个实例。系统生成错误消息，并且 `Beta` 未启动，因为它将超出每个用户一个实例的限制。
- **最大并发实例数和每个用户一个实例的限制：** 在另一个交付组中，您为应用程序 `Delta` 配置最大并发实例数为 10 并启用每个用户一个实例的选项。之后，当该交付组中的 10 个用户各自运行着一个 `Delta` 实例时，该交付组中任何其他尝试启动 `Delta` 的用户都将收到错误消息。`Delta` 未启动。如果这 10 个当前 `Delta` 用户中的任何一个尝试启动该应用程序的第二个实例，他们将收到错误消息，并且第二个实例将不会启动。
- **每台计算机的最大并发实例数以及使用标记限制：** 应用程序 `Charlie` 具有许可和性能要求，这些要求规定了在特定服务器上可以同时运行多少个实例。这些要求还规定了在站点中所有服务器上可以同时运行多少个实例。

  每台计算机的应用程序实例限制会影响站点中的任何服务器（不仅仅是特定交付组中的计算机）。假设您的站点有三台服务器。对于应用程序 `Charlie`，您将每台计算机的应用程序实例限制配置为 2。因此，站点范围内最多允许启动六个应用程序 `Charlie` 实例。（即三台服务器上每台服务器两个 Charlie 实例的限制。）

  要将应用程序的使用限制为交付组中的某些计算机（除了限制站点中所有计算机上的实例之外）：

- 为这些计算机使用标记功能。
- 为该应用程序配置每台计算机的最大实例数限制。

如果应用程序通过 Controller 代理以外的方法启动（例如，当 Controller 处于中断模式时），并且超出了配置的限制，则用户无法启动更多实例，直到他们关闭足够的实例以不再超出限制。超出限制的实例不会被强制关闭。它们将被允许继续运行，直到其用户将其关闭。

如果禁用会话漫游，则禁用每个用户一个实例的应用程序限制。如果启用每个用户一个实例的应用程序限制，请勿配置允许在新设备上创建新会话的两个值中的任何一个。有关漫游的信息，请参阅会话。

要配置每个交付组的最大实例数限制以及每个用户一个实例的限制：

1. 在 Studio 导航窗格中选择**应用程序**，然后选择一个应用程序。
2. 在“操作”窗格中选择**编辑应用程序属性**。
3. 在**交付**页面上，选择以下选项之一。
   - **允许无限制使用应用程序**。同时运行的实例数量没有限制。这是默认设置。
   - **为应用程序设置限制**。有两种限制类型；指定其中一种或两种。
     - 指定可同时运行的最大实例数
     - 将每个用户限制为一个应用程序实例
4. 单击**确定**以应用更改并关闭对话框，或单击**应用**以应用更改并保持对话框打开。

要配置每台计算机的最大实例数限制（仅限 PowerShell）：

- 在 PowerShell 中（对于 Citrix Cloud™ 部署使用 Remote PowerShell SDK，对于本地部署使用 PowerShell SDK），输入适当的 `BrokerApplication` cmdlet 并带上 `MaxPerMachineInstances` 参数。
- 有关指导，请使用 `Get-Help` cmdlet。例如：

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

## 将参数传递给已发布的应用程序

使用应用程序属性的**位置**页面输入命令行并将参数传递给已发布的应用程序。

当您将已发布的应用程序与文件类型关联时，符号 `“%*”`（用双引号括起来的百分号和星号）将附加到应用程序命令行的末尾。这些符号用作传递给用户设备的参数的占位符。

如果已发布的应用程序未按预期启动，请验证其命令行是否包含正确的符号。默认情况下，当附加符号 `“%*”` 时，将验证用户设备提供的参数。对于使用用户设备提供的自定义参数的已发布应用程序，符号 `“%**”` 将附加到命令行以绕过命令行验证。如果您在应用程序的命令行中没有看到这些符号，请手动添加它们。

如果可执行文件的路径包含带空格的目录名称（例如 `“C:\Program Files”`），请用双引号将应用程序的命令行括起来，以指示空格属于命令行。为此，请在路径周围添加双引号，并在 `%*` 符号周围添加另一组双引号。请务必在路径的结束引号和 `%*` 符号的开始引号之间包含一个空格。

例如，已发布的应用程序 Windows Media Player 的命令行是：

```
“C:\Program Files\Windows Media Player\mplayer1.exe” “%*”
```

> **注意：**
>
> 用于启动已发布的应用程序的命令行中的最大字符数（包括参数）为 203。

## 管理应用程序文件夹

默认情况下，您添加到交付组的新应用程序将放置在名为 **Applications** 的文件夹中。您可以在创建交付组时、添加应用程序时或之后指定不同的文件夹。

须知：

- 您无法重命名或删除 Applications 文件夹，但可以将其包含的所有应用程序移动到您创建的其他文件夹中。
- 文件夹名称可以包含 1-64 个字符。允许使用空格。
- 文件夹最多可以嵌套五层。
- 文件夹不必包含应用程序。允许使用空文件夹。
- 文件夹在 Studio 中按字母顺序排列，除非您移动它们或在创建时指定了不同的位置。
- 只要每个文件夹都有不同的父文件夹，就可以有多个同名文件夹。同样，只要每个应用程序位于不同的文件夹中，就可以有多个同名应用程序。
- 您必须具有 `View Applications` 权限才能查看文件夹中的应用程序，并且必须具有 `Edit Application Properties` 权限才能删除、重命名或删除包含应用程序的文件夹中的所有应用程序。
- 以下大多数过程都要求使用 Studio 中的“操作”窗格执行操作。或者，您可以使用右键单击菜单或拖动项目。例如，如果您在不希望的位置创建或移动了文件夹，则可以将其拖放到正确的位置。

要管理应用程序文件夹，请在 Studio 导航窗格中选择**应用程序**。请使用以下列表作为指导。

- **要查看所有文件夹（不包括嵌套文件夹）：** 单击文件夹列表上方的**显示所有**。
- **要在最高级别（非嵌套）创建文件夹：选择应用程序**文件夹。要将新文件夹放置在**应用程序**以外的现有文件夹下，请选择该文件夹。然后，在“操作”窗格中选择**创建文件夹**。输入名称。
- **要移动文件夹：选择该文件夹，然后在“操作”窗格中选择移动文件夹**。一次只能移动一个文件夹，除非该文件夹包含嵌套文件夹。（移动文件夹最简单的方法是拖动它。）
- **重命名文件夹：** 选择文件夹，然后在“操作”窗格中选择**重命名文件夹**。输入名称。
- **删除文件夹：** 选择文件夹，然后在“操作”窗格中选择**删除文件夹**。删除包含应用程序和其他文件夹的文件夹时，这些对象也会被删除。删除应用程序会从交付组中移除应用程序分配。它不会将其从计算机中移除。
- **将应用程序移动到文件夹中：** 选择一个或多个应用程序。然后，在“操作”窗格中选择**移动应用程序**。选择文件夹。

在创建交付组或应用程序组时，您还可以在**应用程序**页面上将要添加的应用程序放置在文件夹中。默认情况下，添加的应用程序会进入**应用程序**文件夹。单击**更改**以选择或创建文件夹。

## 控制已发布的桌面上的应用程序的本地启动

当用户从已发布的桌面中启动已发布的应用程序时，您可以控制该应用程序是在该桌面会话中启动还是作为已发布的应用程序启动。Citrix Workspace 应用程序会在 VDA 上的 Windows 注册表中搜索应用程序的安装路径，如果存在，则启动应用程序的本地实例。否则，将启动应用程序的托管实例。如果您启动未安装在 VDA 上的应用程序，则会启动托管应用程序。有关详细信息，请参阅 vPrefer 启动。

在 PowerShell 中（在 Citrix Cloud 部署中使用远程 PowerShell SDK，或在本地部署中使用 PowerShell SDK），您可以更改此操作。

在 `New-Broker` 应用程序或 `Set-BrokerApplication` cmdlet 中，使用 `LocalLaunchDisabled` 选项。例如：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

默认情况下，此选项的值为 false（`-LocalLaunchDisabled $false`）。从已发布的桌面中启动已发布的应用程序时，该应用程序将在该桌面会话中启动。

如果将此选项的值设置为 true（`-LocalLaunchDisabled $true`），则会启动已发布的应用程序。这会从已发布的桌面（使用适用于 Windows 的 Citrix Workspace 应用程序）为已发布的应用程序创建一个单独的附加会话。

要求和限制：

- 应用程序的 `ApplicationType` 值必须为 `HostedOnDesktop`。
- 此选项仅通过相应的 PowerShell SDK 提供。它目前在 Studio 图形界面中不可用。
- 此选项最低要求：StoreFront 3.14、适用于 Windows 的 Citrix Receiver 4.11 和 Delivery Controller 7.17。

## 通用 Windows 平台应用

有关通用 Windows 平台 (UWP) 应用的信息，请参阅以下 Microsoft 文档：

- 什么是通用 Windows 平台 (UWP) 应用？
- Windows 程序包管理器

### 要求和限制

Citrix Virtual Apps and Desktops™ 支持在以下 Windows 计算机上将 UWP 应用与 VDA 结合使用：

- Windows 10 及更高版本
- Windows Server 2016 及更高版本

VDA 最低版本必须为 7.11。

使用 UWP 应用时，以下 Citrix Virtual Apps and Desktops 功能不受支持或受到限制：

- 不支持文件类型关联。
- 不支持本地应用访问。
- 动态预览：如果会话中运行的应用重叠，预览将显示默认图标。UWP 应用不支持用于动态预览的 Win32 API。
- 操作中心远程处理：UWP 应用可以使用操作中心在会话中显示消息。这些消息目前不会重定向到端点以显示给用户。

不支持从同一服务器启动 UWP 应用和非 UWP 应用。请将 UWP 应用和非 UWP 应用放置在单独的交付组或应用程序组中。

由于机器上安装的所有 UWP 应用程序都会被枚举，Citrix® 建议禁用用户对 Windows 应用商店的访问。这可以防止一个用户安装的 UWP 应用程序被其他用户访问。

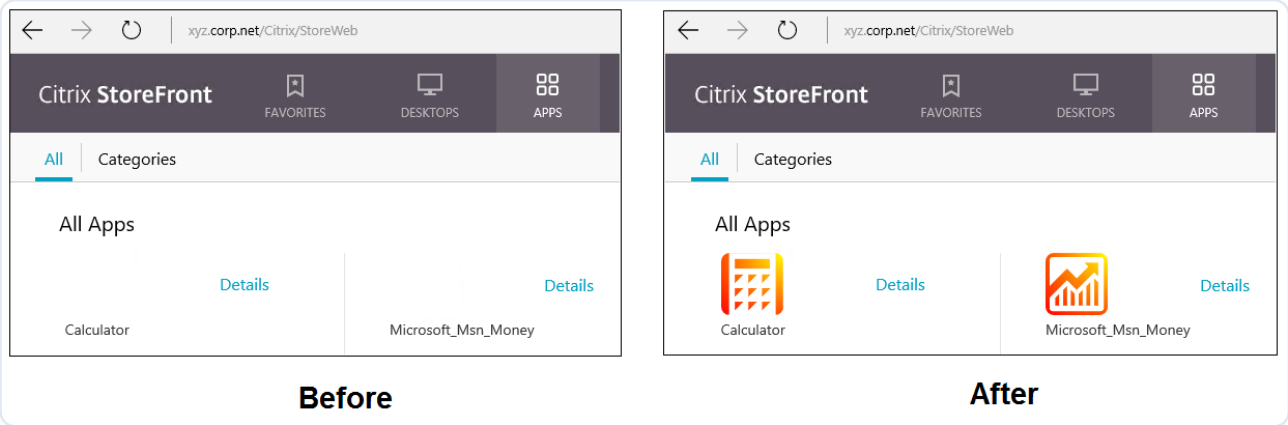
在旁加载期间，UWP 应用程序会安装在计算机上，并可供其他用户使用。当其他用户启动该应用程序时，它会被安装，并且操作系统会更新其 AppX 数据库以指示该用户“已安装”。

从以固定或无缝窗口启动的已发布的 UWP 应用启动的正常注销可能会阻止 VDA 会话关闭，并强制注销用户。发生这种情况时，VDA 会话中剩余的多个进程会阻止其正常关闭。要解决此问题，请确定哪个进程阻止 VDA 会话关闭，然后按照 CTX891671 中的指导将其添加到“LogoffCheckSysModules”注册表项值中。

UWP 应用程序的应用程序显示名称和描述可能不正确。在将应用程序添加到交付组时，请编辑并更正这些属性。

请查看 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/whats-new/known-issues.html) 以了解任何其他问题。

目前，一些 UWP 应用程序具有启用透明度的白色图标，这导致图标在 StoreFront 显示的白色背景下不可见。为避免此问题，您可以更改背景。例如，在 StoreFront 计算机上，编辑文件 `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`。在文件末尾，添加 `.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`。下图说明了此示例的更改前后对比。




在 Windows Server 2016 及更高版本上，启动 UWP 应用时也可能会启动服务器管理器。为防止出现此情况，请使用 `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon` 注册表项禁用服务器管理器在登录时自动启动。有关详细信息，请参阅 `<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`。

### 安装和发布 UWP 应用程序

默认情况下启用对 UWP 应用程序的支持。

要在 VDA（或主映像）上安装一个或多个 UWP 应用程序，请使用以下方法之一：

- 使用部署映像服务和管理 (DISM) 等工具，从适用于企业的 Windows 应用商店完成脱机安装，以将应用程序部署到桌面映像。有关详细信息，请参阅 Windows 程序包管理器。

- 旁加载应用程序。有关详细信息，请参阅 在 Windows 客户端设备中旁加载业务线 (LOB) 应用。
- 直接从适用于企业的 Windows 应用商店为每个目标用户安装 UWP 应用程序。

要在 Citrix Virtual Apps 或 Citrix Virtual Desktops™ 中添加（发布）一个或多个 UWP 应用程序，请执行以下操作：

1. UWP 应用安装到计算机后，将 UWP 应用添加到交付组或应用程序组。您可以在创建组时或之后执行此操作。在“**应用程序**”页面上，在“**添加**”菜单中，选择“**从‘开始’菜单**”。
2. 应用程序列表出现时，选择要发布的 UWP 应用。
3. 继续向导或关闭编辑对话框。

有关使用用户配置文件管理器 (UPM) 时的其他配置要求的信息，请参阅 Windows Apps - Microsoft Store。

要在 VDA 上禁用 UWP 应用的使用，请在 `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` 中添加注册表设置 **EnableUWASeamlessSupport** 并将其设置为 **0**。

### 卸载 UWP 应用

当您使用 `Remove-AppXPackage` 等命令卸载 UWP 应用时，该项目仅针对管理员卸载。要从可能已启动和使用该应用的用户计算机中删除该应用，请在每台计算机上运行删除命令。您无法通过一个命令从所有用户的计算机中卸载 AppX 包。

## 区域

跨越通过 WAN 连接的广泛分散位置的部署可能会因网络延迟和可靠性而面临挑战。有两种选项可以缓解这些挑战：

- 部署多个站点，每个站点都有自己的 SQL Server 站点数据库。

  此选项建议用于大型企业部署。多个站点是单独管理的，每个站点都需要自己的 SQL Server 站点数据库。每个站点都是一个独立的 Citrix Virtual Apps™ 部署。

- 在单个站点内配置多个区域。

  配置区域可以帮助远程区域的用户连接到资源，而无需强制其连接遍历大部分 WAN。使用区域可以通过单个 Citrix Studio 控制台、Citrix Director 和站点数据库进行有效的站点管理。这节省了在远程位置部署、配备人员、许可和运营包含独立数据库的更多站点的成本。

  区域对所有规模的部署都很有帮助。您可以使用区域使应用程序和桌面更接近最终用户，从而提高性能。一个区域可以安装一个或多个本地 Controller 以实现冗余和弹性，但这不是必需的。

站点中配置的 Controller 数量可能会影响某些操作的性能，例如向站点本身添加新的 Controller。为避免这种情况，我们建议您将 Citrix Virtual Apps 或 Citrix Virtual Desktops™ 站点中的区域数量限制为不超过 50 个。

当您的区域网络延迟超过 250 毫秒 RTT 时，我们建议您部署多个站点而不是区域。

在本文中，“本地”一词指正在讨论的区域。例如，“VDA 向本地 Controller 注册”表示 VDA 向 VDA 所在区域中的 Controller 注册。

此版本中的区域与 XenApp version 6.5 及更早版本中的区域相似，但并不完全相同。例如，在此区域实现中，没有数据收集器。站点中的所有 Controller 都与主区域中的一个站点数据库通信。此外，此版本中的故障转移和首选区域的工作方式也不同。

## 区域类型

一个站点始终有一个主区域。它还可以选择有一个或多个卫星区域。卫星区域可用于灾难恢复、地理上分散的数据中心、分支机构、云或云中的可用区。

**主区域：**

主区域的默认名称为“Primary”。此区域包含 SQL Server 站点数据库（如果使用，还包含高可用性 SQL 服务器）、Studio、Director、Citrix StoreFront™、Citrix License Server 和 Citrix Gateway。请始终将站点数据库保留在主区域中。

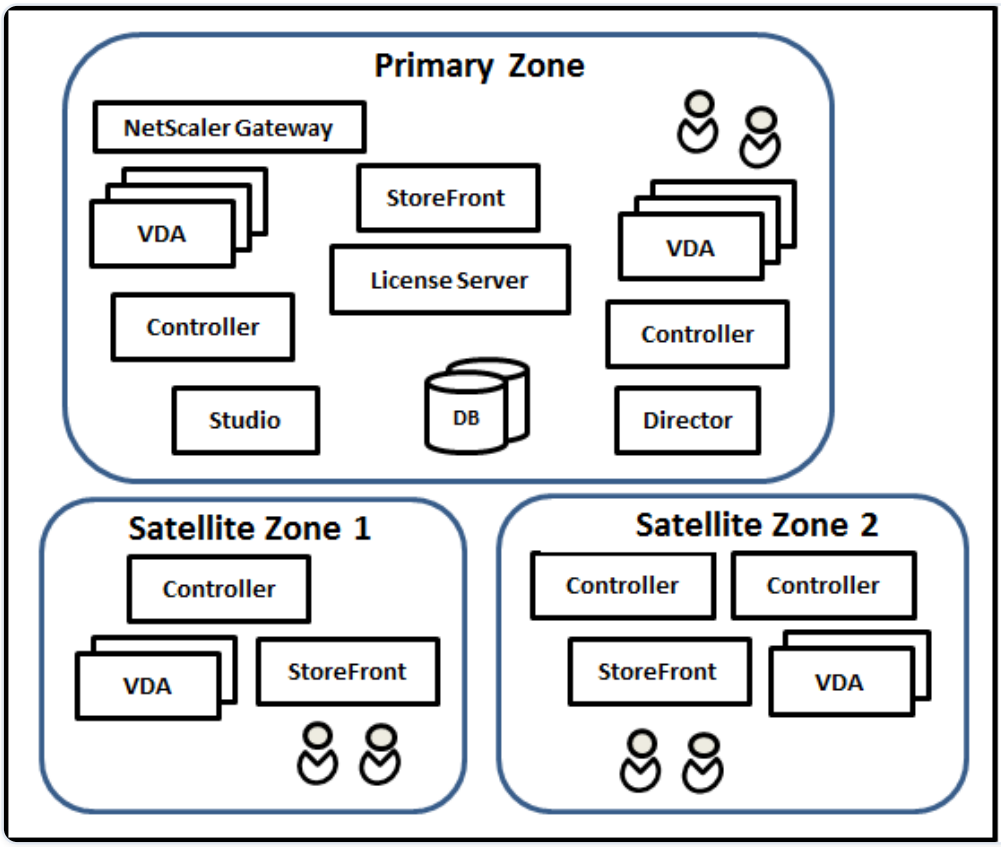
主区域应至少有两个控制器以实现冗余。主区域可以包含与数据库和基础架构紧密耦合的应用程序的 VDA。

**卫星区域：**

卫星区域包含一个或多个 VDA、控制器、StoreFront 服务器和 Citrix Gateway 服务器。在正常操作下，卫星区域中的控制器直接与主区域中的数据库通信。

卫星区域，尤其是大型卫星区域，可能还包含一个用于为该区域预配和存储计算机的管理程序。配置卫星区域时，可以将其与管理程序或其他服务连接关联。（请确保使用该连接的任何目录都在同一区域中。）

站点可以根据您的独特需求和环境拥有不同配置的卫星区域。下图说明了主区域和卫星区域的示例。




在图中：

- **主区域：**包含两个 Controller、Studio、Director、StoreFront、License Server 和站点数据库（以及高可用性 SQL Server 部署）。主区域还包含多个 VDA 和一个 Citrix Gateway。
- **卫星区域 1：带控制器的 VDA：** 卫星区域 1 包含一个控制器、VDA 和一个 StoreFront 服务器。此卫星区域中的 VDA 向本地控制器注册。本地控制器与主区域中的站点数据库和许可证服务器通信。

  如果 WAN 出现故障，本地主机缓存功能允许卫星区域中的控制器继续代理与该区域中 VDA 的连接。这种部署在办公室中可能很有效，员工可以使用本地 StoreFront 站点和本地控制器访问其本地资源。
- **卫星区域 2：带冗余控制器的 VDA：** 卫星区域 2 包含两个控制器、VDA 和一个 StoreFront 服务器。这是最具弹性的区域类型，可防止 WAN 和其中一个本地控制器同时发生故障。

## VDA 注册位置和控制器故障转移位置

在包含主区域和卫星区域的站点中，如果 VDA 的最低版本为 7.7：

- 主区域中的 VDA 向主区域中的控制器注册。主区域中的 VDA 绝不会尝试向卫星区域中的控制器注册。
- 卫星区域中的 VDA 会尽可能向本地控制器注册。（这被认为是首选控制器。）如果没有可用的本地控制器（例如，因为它们无法接受更多 VDA 注册或已发生故障），VDA 将尝试向主区域中

的控制器注册。在这种情况下，即使卫星区域中的控制器再次可用，VDA 仍会注册在主区域中。卫星区域中的 VDA 绝不会尝试向另一个卫星区域中的控制器注册。

- 当为 VDA 发现控制器启用自动更新，并且您在 VDA 安装期间指定控制器地址列表时，将从该列表中随机选择一个控制器进行初始注册（无论控制器位于哪个区域）。在该 VDA 所在的计算机重新启动后，VDA 将开始优先注册其本地区域中的控制器。
- 如果卫星区域中的控制器发生故障，它将尽可能故障转移到另一个本地控制器。如果没有可用的本地控制器，它将故障转移到主区域中的控制器。
- 如果您将控制器移入或移出某个区域，并且启用了自动更新，则两个区域中的 VDA 都会收到更新的列表，指示哪些控制器是本地的，哪些在主区域中，以便它们知道可以向谁注册并接受来自谁的连接。
- 如果您将目录移动到另一个区域，则该目录中的 VDA 将重新注册到您移动目录所在区域中的控制器。（当您将目录移动到另一个区域时，请确保此区域与具有关联主机连接的区域连接良好。如果带宽有限或延迟较高，请将主机连接移动到包含关联计算机目录的同一区域。）

如果主区域中的所有控制器都发生故障：

- Studio 无法连接到站点。
- 无法连接到主区域中的 VDA。
- 站点性能会下降，直到主区域中的控制器可用。

对于包含早于 7.7 版本的 VDA 的站点：

- 卫星区域中的 VDA 接受来自其本地区域和主区域中控制器的请求。（最低版本为 7.7 的 VDA 可以接受来自其他卫星区域的控制器请求。）
- 卫星区域中的 VDA 随机注册到主区域或本地区域中的控制器。（最低版本为 7.7 的 VDA 优先选择本地区域。）

## 区域首选项

要使用区域首选项功能，您必须使用最低 StoreFront 3.7 和 Citrix Gateway 11.0-65.x。

在多区域站点中，区域首选项功能为管理员提供了更大的灵活性，可以控制使用哪个 VDA 启动应用程序或桌面。

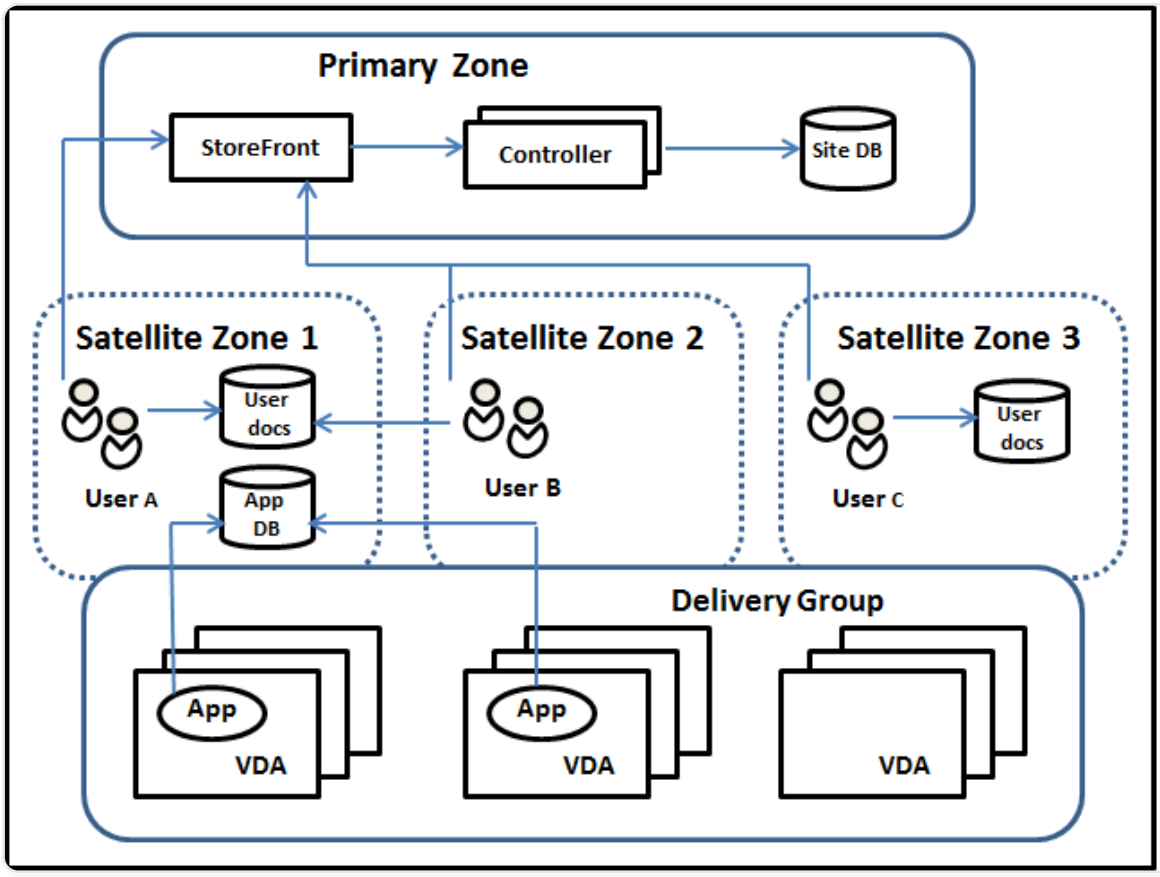
### 区域首选项的工作原理

区域首选项有三种形式。您可能希望在特定区域中使用 VDA，具体取决于：

- 应用程序数据存储的位置。这称为应用程序主目录。
- 用户主数据的位置，例如配置文件或主共享。这称为用户主目录。

- 用户的当前位置（Citrix Workspace™ 应用程序正在运行的位置）。这称为用户位置。

下图显示了一个多区域配置示例。




在此示例中，VDA 分布在三个卫星区域中，但它们都位于同一个交付组中。因此，代理可能会选择使用哪个 VDA 来处理用户启动请求。此示例表明用户可以在多个位置运行其 Citrix Workspace 应用程序端点：

- 用户 A 正在卫星区域 1 中使用运行 Citrix Workspace 应用程序的设备。
- 用户 B 正在卫星区域 2 中使用设备。
- 用户的文档可以存储在各个位置。
  - 用户 A 和 B 使用基于卫星区域 1 的共享。
  - 用户 C 使用来自卫星区域 C 的共享。
  - 其中一个已发布的应用程序使用位于卫星区域 1 的数据库。

通过为用户或应用程序配置主区域，可以将用户或应用程序与区域关联。然后，Delivery Controller™ 中的代理会使用这些关联来帮助选择在资源可用时启动会话的区域。您可以：

- 通过将用户添加到区域来配置用户的主区域。
- 通过编辑应用程序属性来配置应用程序的主区域。

用户或应用程序一次只能有一个主区域。（当由于用户组成员身份而出现多个区域成员身份时，用户可能会出现例外情况；请参阅“其他注意事项”部分。但是，即使在这种情况下，代理也只使用一个主区域。）

尽管可以配置用户和应用程序的区域首选项，但代理仅为一次启动选择一个首选区域。选择首选区域的默认优先级顺序是应用程序主区域 \> 用户主区域 \> 用户位置。您可以限制此序列；请参阅自定义区域首选项。当用户启动应用程序时：

- 如果该应用程序具有配置的区域关联（应用程序主区域），则首选区域是该应用程序的主区域。
- 如果应用程序没有配置区域关联，但用户有配置区域关联（用户主区域），则首选区域是该用户的主区域。
- 如果应用程序和用户都没有配置区域关联，则首选区域是用户运行 Citrix Workspace 应用程序实例的区域（用户位置）。如果未定义该区域，则使用随机 VDA 和区域选择。负载平衡应用于首选区域中的所有 VDA。如果没有首选区域，则负载平衡应用于交付组中的所有 VDA。

### 调整区域首选项

当您为用户或应用程序配置（或删除）主区域时，您还可以进一步限制区域首选项的使用方式。

- **强制使用用户主区域：** 在交付组中，您可以指定会话在用户的主区域（如果已配置）中启动，如果主区域没有可用资源，则不进行故障转移到其他区域。当您必须避免在区域之间复制大型配置文件或数据文件的风险时，此限制很有用。换句话说，您宁愿拒绝会话启动，也不愿在不同区域中启动会话。
- **强制应用程序主区域使用：** 同样，当您为应用程序配置主区域时，您可以指示该应用程序只能在该区域中启动，如果应用程序的主区域中没有可用资源，则不会故障转移到其他区域。
- **无应用程序主区域，并忽略配置的用户主区域：** 如果您未为应用程序指定主区域，您还可以指示在启动该应用程序时，不考虑任何已配置的用户区域。例如，您可能更希望用户使用用户位置区域首选项在其设备附近的 VDA 上运行应用程序，即使某些用户可能具有不同的主区域。

### 首选区域如何影响会话使用

当用户启动应用程序或桌面时，代理程序更倾向于使用首选区域，而不是使用现有会话。

如果启动应用程序或桌面的用户已经有一个适合所启动资源的会话（例如，可以用于应用程序的会话共享，或者已经运行所启动资源的会话），但该会话正在用户/应用程序首选区域之外的区域中的 VDA 上运行，则系统可能会创建一个新会话。这满足了在正确区域中启动（如果该区域有可用容量）的要求，优先于重新连接到该用户会话要求中不太首选区域的会话。

为防止无法再访问的孤立会话，即使现有断开连接的会话位于非首选区域，也允许重新连接到这些会话。

满足启动需求的会话的理想顺序是：

1. 重新连接到首选区域中的现有会话。
2. 重新连接到首选区域之外的区域中现有的已断开连接的会话。
3. 在首选区域中启动新会话。
4. 重新连接到首选区域之外的区域中已连接的现有会话。
5. 在首选区域之外的区域中启动新会话。

### 其他区域首选项注意事项

- 如果您为用户组（例如安全组）配置了主区域，则该组的用户（通过直接或间接成员身份）将与指定区域关联。但是，用户可以是多个安全组的成员，因此可能通过其他组成员身份配置了不同的主区域。在这种情况下，确定该用户的主区域可能会不明确。

如果用户配置了并非通过组成员身份获得的主区域，则该区域将用于区域首选项。通过组成员身份获得的任何区域关联都将被忽略。

如果用户仅通过组成员身份获得了多个不同的区域关联，代理会随机选择其中一个区域。一旦代理做出此选择，该区域将用于后续的会话启动，直到用户的组成员身份发生变化。

- 用户位置区域首选项要求 Citrix Gateway 通过其连接的端点设备检测 Citrix Workspace 应用程序。Citrix Gateway 必须配置为将 IP 地址范围与特定区域关联，并且发现的区域身份必须通过 StoreFront 传递给 Controller。

有关区域首选项的更多信息，请参阅区域首选项内部机制。

## 注意事项、要求和最佳实践

- 您可以将以下各项放置在区域中：Controller、计算机目录、主机连接、用户和应用程序。如果目录使用主机连接，请确保目录和连接位于同一区域中。（但是，如果存在低延迟高带宽连接，它们可以位于不同的区域中。）
- 当您将项目放置在卫星区域中时，这会影响站点与它们以及与它们相关的其他对象的交互方式。
    - 当 Controller 放置在卫星区域中时，假定这些计算机与同一区域中的管理程序和 VDA 具有良好的（本地）连接。然后，该卫星区域中的 Controller 将优先于主区域中的 Controller 用于处理这些管理程序和 VDA 计算机。
    - 当管理程序连接放置在卫星区域中时，假定通过该管理程序连接管理的所有管理程序也驻留在该卫星区域中。然后，该卫星区域中的 Controller 将优先于主区域中的 Controller 用于与该管理程序连接进行通信。

  - 当计算机目录放置在卫星区域中时，假定该目录中的所有 VDA 计算机都在该卫星区域中。在每个 VDA 首次注册后，Controller 列表自动更新机制激活后，本地 Controller 将优先于主区域中的 Controller 用于尝试向站点注册。
  - Citrix Gateway 实例也可以与区域关联。这是作为 StoreFront 最佳 HDX™ 路由配置的一部分完成的，而不是像此处描述的其他元素那样，作为站点配置的一部分完成的。当 Citrix Gateway 与某个区域关联时，在对该区域中的 VDA 计算机使用 HDX 连接时，将优先使用它。

- 当您创建生产站点，然后创建第一个目录和交付组时，所有项目都位于主区域中 – 在完成初始设置之前，您无法创建卫星区域。（如果您创建空站点，主区域最初将只包含一个控制器。您可以在创建目录和交付组之前或之后创建卫星区域。）
- 当您创建包含一个或多个项目的第一个卫星区域时，站点中的所有其他项目都保留在主区域中。
- 主区域默认命名为“Primary”；您可以更改该名称。尽管 Studio 显示屏会指示哪个区域是主区域，但最佳做法是为主区域使用易于识别的名称。您可以重新分配主区域（即将另一个区域设为主区域），但它应始终包含站点数据库和任何高可用性服务器。
- 始终将站点数据库保留在主区域中。
- 创建区域后，您可以稍后将项目从一个区域移动到另一个区域。这种灵活性使您能够将最适合近距离工作的项目分开。例如，将目录移动到与创建目录中计算机的连接（主机）不同的区域，可能会影响性能。在区域之间移动项目之前，请考虑潜在的意外影响。将目录及其使用的主机连接保留在同一区域中，或保留在连接良好（例如，通过低延迟和高带宽网络）的区域中。
- 为获得最佳性能，请仅在主区域中安装 Studio 和 Director。如果您希望在卫星区域中安装另一个 Studio 实例（例如，包含 Controller 的卫星区域，以便在主区域无法访问时用作故障转移），请将 Studio 作为本地发布的应用程序运行。您还可以从卫星区域访问 Director，因为它是一个 Web 应用程序。
- 理想情况下，卫星区域中的 Citrix Gateway 用于从其他区域或外部位置进入该区域的用户连接，尽管您也可以将其用于区域内的连接。
- 请记住：要使用区域首选项功能，您必须至少使用 StoreFront 3.7 和 Citrix Gateway 11.0-65.x。

### 连接质量限制

卫星区域中的控制器直接与站点数据库执行 SQL 交互。这会对卫星区域与包含站点数据库的主区域之间的链接质量施加一些限制。具体限制与部署在卫星区域中的 VDA 数量以及这些 VDA 上的用户会话数量有关。因此，只有少量 VDA 和会话的卫星区域可以使用比具有大量 VDA 和会话的卫星区域更差的数据库连接质量来运行。

有关详细信息，请参阅延迟和 SQL 阻塞查询改进。

### 延迟对代理性能的影响

尽管区域允许用户使用更高延迟的链接（前提是有本地代理），但额外的延迟不可避免地会影响最终用户体验。对于用户所做的大多数工作，他们会遇到由卫星区域中的控制器与站点数据库之间的往返通信导致的缓慢。

对于启动应用程序，在会话代理过程识别要发送会话启动请求的合适 VDA 时，会发生额外的延迟。

## 创建和管理区域

完全管理员可以执行所有区域创建和管理任务。但是，您也可以创建自定义角色，允许您创建、编辑或删除区域。在区域之间移动项目不需要与区域相关的权限（区域读取权限除外）；但是，您必须具有要移动项目的编辑权限。例如，要将目录从一个区域移动到另一个区域，您必须具有该目录的编辑权限。有关详细信息，请参阅委派管理。

**如果您使用 Citrix Provisioning™：**Citrix Provisioning 控制台不识别区域，因此 Citrix 建议使用 Studio 为卫星区域创建目录。在 Studio 中创建目录，指定正确的卫星区域。然后使用 Citrix Provisioning 控制台在该目录中预配计算机。（如果您使用 Citrix Provisioning 向导创建目录，则该目录将放置在主区域中。您以后必须使用 Studio 将其移动到卫星区域。）

### 创建区域

1. 在 Studio 导航窗格中选择**配置 \> 区域**。
2. 在“操作”窗格中选择**创建区域**。
3. 输入区域名称和描述（可选）。名称在站点内必须是唯一的。
4. 选择要放置在新区域中的项目。您可以筛选或搜索可供选择的项目列表。您也可以创建空区域；只需不选择任何项目即可。
5. 单击 **保存**。

作为此方法的替代方法，您可以在 Studio 中选择一个或多个项目，然后在“操作”窗格中选择**创建区域**。

### 更改区域名称或描述

1. 在 Studio 导航窗格中选择**配置 \> 区域**。
2. 在中间窗格中选择一个区域，然后在“操作”窗格中选择**编辑区域**。
3. 更改区域名称、描述或两者。如果更改主区域的名称，请确保该区域仍然易于识别为主区域。
4. 单击**确定**或**应用**。

### 将项目从一个区域移动到另一个区域

1. 在 Studio 导航窗格中选择**配置 \> 区域**。
2. 在中间窗格中选择一个区域，然后选择一个或多个项目。
3. 将项目拖动到目标区域，或在“操作”窗格中选择**移动项目**，然后指定要将它们移动到的区域。

确认消息会列出您选择的项目，并询问您是否确定要移动所有这些项目。

**请记住：** 当目录使用到虚拟机管理程序或其他服务的主机连接时，请将目录和连接都放在同一区域中。否则，性能可能会受到影响。如果您移动其中一个，也要移动另一个。

### 删除区域

区域必须为空才能删除。您不能删除主区域。

1. 在 Studio 导航窗格中，选择**配置 \> 区域**。
2. 在中间窗格中选择一个区域。
3. 在“操作”窗格中，选择**删除区域**。如果区域不为空（包含项目），系统会要求您选择要将这些项目移动到的区域。
4. 确认删除。

### 为用户添加主区域

为用户配置主区域也称为 *将用户添加到区域*。

1. 在 Studio 导航窗格中，选择**配置 \> 区域**，然后选择中间窗格中的一个区域。
2. 在“操作”窗格中，选择**将用户添加到区域**。
3. 在**将用户添加到区域**对话框中，单击**添加**，然后选择要添加到区域的用户和用户组。如果您指定的用户已拥有主区域，则会显示一条消息，提供两个选项：**是** = 仅添加您指定的没有主区域的用户；**否** = 返回用户选择对话框。
4. 单击 **确定**。

对于配置了主区域的用户，您可以要求会话仅从其主区域启动：

1. 创建或编辑交付组。
2. 在**用户**页面上，选中**会话必须在用户的主区域中启动（如果已配置）**复选框。

该交付组中用户启动的所有会话必须从该用户主区域中的计算机启动。如果交付组中的用户没有配置主区域，此设置将不起作用。

### 删除用户的主区域

此过程也称为从区域中删除用户。

1. 在 Studio 导航窗格中，选择**配置 \> 区域**，然后选择中间窗格中的一个区域。
2. 在“操作”窗格中，选择**从区域中删除用户**。
3. 在**将用户添加到区域**对话框中，单击**删除**，然后选择要从区域中删除的用户和组。此操作仅从区域中删除用户；这些用户仍保留在其所属的交付组和应用程序组中。
4. 在出现提示时确认删除。

### 管理应用程序的主区域

为应用程序配置主区域也称为将应用程序添加到区域。默认情况下，在多区域环境中，应用程序没有主区域。

应用程序的主区域在应用程序的属性中指定。您可以在将应用程序添加到组时或之后配置应用程序属性。

- 在创建交付组、创建应用程序组 或将应用程序添加到现有组 时，在向导的**应用程序**页面上选择**属性**。
- 要在添加应用程序后更改其属性，请在 Studio 导航窗格中选择**应用程序**。选择一个应用程序，然后在“操作”窗格中选择**编辑应用程序属性**。

在应用程序属性/设置的 **区域** 页面上：

- 如果您希望应用程序具有主区域：
  - 选择**使用选定的区域来决定**单选按钮，然后选择该区域。
  - 如果您希望应用程序仅从选定区域启动（而不是从任何其他区域启动），请选中区域选择下方的复选框。
- 如果您不希望应用程序具有主区域：
  - 选择 **不配置主区域** 单选按钮。
  - 如果您不希望代理在启动此应用程序时考虑任何已配置的用户区域，请选择单选按钮下方的复选框。在这种情况下，应用程序或用户主区域都不会用于确定此应用程序的启动位置。

## 其他涉及指定区域的操作

创建至少一个卫星区域后，您可以在添加主机连接或创建目录时指定一个区域。

通常，主区域是默认区域。使用 Machine Creation Services™ 创建目录时，将自动选择为主机连接配置的区域。

如果站点不包含卫星区域，则假定为主区域，并且不会显示区域选择框。

# 连接和资源

> **重要提示：**

> 自 Citrix Virtual Apps and Desktops™ 7 2006 起，如果您的当前部署使用了以下任何技术，则只有在移除使用这些技术的生命周期结束 (EOL) 项目后，才能将部署升级到当前版本。

> - 个人虚拟磁盘 (PvD)
> - AppDisks™
> - 公有云主机类型：Citrix CloudPlatform、Microsoft Azure Classic

> 有关详细信息，请参阅移除 PVD、AppDisks 和不受支持的主机。

> 如果您想在部署中使用公有云主机连接，则需要混合权利许可证才能完成全新安装或升级到当前版本。

当安装程序检测到一个或多个不受支持的技术或没有混合权利许可证的主机连接时，升级会暂停或停止，并显示一条解释性消息。安装程序日志中包含详细信息。有关详细信息，请参阅 升级部署。

## 混合权利许可证对主机连接的影响

根据混合权利许可证的授权，主机与公有云主机的连接会受到影响，共有以下三种情况：

- 要创建到公有云主机的新主机连接，您必须拥有混合权利许可证。
- 如果您拥有混合权利许可证但许可证已过期，则与公有云主机的现有连接将被标记为未授权并进入维护模式。当现有主机连接处于维护模式时，您无法执行以下操作：
  - 添加或修改主机连接
  - 创建目录和更新映像
  - 执行电源操作

- 当未授权的主机连接变为授权状态时，现有主机连接将重新启用。

## 简介

您可以在创建站点时选择性地创建与托管资源的第一个连接。之后，您可以更改该连接并创建其他连接。配置连接包括从支持的管理程序中选择连接类型，以及从该连接的资源中选择存储和网络。

只读管理员可以查看连接和资源详细信息。您必须是完全管理员才能执行连接和资源管理任务。有关详细信息，请参阅委派管理。

### 在何处查找有关连接类型的信息

您可以使用支持的虚拟化平台在您的 Citrix Virtual Apps 或 Citrix Virtual Desktops 环境中托管和管理计算机。(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html)文章列出了支持的类型。

有关详细信息，请参阅以下信息源：

- **Citrix Hypervisor™（以前称为 XenServer）：**
  - Citrix Hypervisor 虚拟化环境。
  - Citrix Hypervisor 的文档。
- **努坦尼克斯 阿克罗波利斯：**
  - Nutanix 虚拟化环境。
  - Nutanix 文档。
- **VMware 平台：**
  - VMware 虚拟化环境。
  - VMware 产品文档。
- **微软 Hyper-V：**
  - 微软系统中心虚拟机管理器虚拟化环境文章。
  - Microsoft 文档。
- **公共云主机连接（AWS、Microsoft Azure、Google Cloud）：**有关公共云主机的信息，请参阅设置资源类型。

> **注意：**

> 信息源将您引导至 Citrix DaaS™ 文档。如果您熟悉 Citrix DaaS 产品中的公共云主机，则本地版本存在一些差异。在 Citrix DaaS 中，管理界面称为“完整配置”。在本地 Virtual Apps and Desktops 中，管理界面称为 Citrix Studio。更新大约每四周向服务推出一次。因此，您可能会发现服务中提供的某些功能在本地版本中不可用。

## 主机存储

当存储产品由受支持的管理程序管理时，该产品将受到支持。Citrix Support 会协助这些存储产品供应商解决问题，并根据需要将这些问题记录在知识中心。

预配计算机时，数据按类型分类：

- 操作系统 (OS) 数据，包括主映像。
- 临时数据。此数据包括写入 MCS 预配计算机的所有非持久性数据、Windows 页面文件、用户配置文件数据以及与 ShareFile 同步的任何数据。每次计算机重新启动时，此数据都会被丢弃。

为每种数据类型提供单独的存储可以减少每个存储设备的负载并提高其性能，从而充分利用主机的可用资源。它还可以为不同的数据类型使用适当的存储——对于某些数据而言，持久性和弹性比其他数据更重要。

存储可以是共享的（集中放置，独立于任何主机，所有主机均可使用）或管理程序本地的。例如，中央共享存储可以是一个或多个 Windows Server 2012 群集存储卷（带或不带附加存储），或者来自存储供应商的设备。中央存储还可能提供其自身的优化，例如管理程序存储控制路径和通过合作伙伴插件的直接访问。

在本地存储临时数据可以避免遍历网络来访问共享存储。它还可以减少共享存储设备的负载。共享存储可能更昂贵，因此在本地存储数据可以降低成本。必须权衡这些优势与管理程序服务器上可用存储的充足性。

创建连接时，您可以选择两种存储管理方法之一：管理程序共享的存储，或管理程序本地的存储。

当在一个或多个 Citrix Hypervisor 主机上使用本地存储进行临时数据存储时，请确保池中的每个存储位置都具有唯一的名称。（要在 XenCenter® 中更改名称，请右键单击存储并编辑名称属性。）

### 管理程序共享的存储

管理程序共享存储方法将需要长期持久性的数据集中存储，提供集中备份和管理。该存储保存操作系统磁盘。

选择此方法时，您可以选择是否使用本地存储（在同一管理程序池中的服务器上）来存储临时计算机数据。此方法不需要像共享存储中的数据那样具有持久性或弹性，共享存储中的数据被称为*临时数据缓存*。本地磁盘有助于减少到主操作系统存储的流量。每次计算机重新启动后，此磁盘都会被

清除。该磁盘通过直写式内存缓存访问。如果将本地存储用于临时数据，则预配的 VDA 将绑定到特定的管理程序主机。如果该主机发生故障，则 VM 无法启动。

**例外**：使用群集共享卷 (CSV) 时，Microsoft System Center Virtual Machine Manager 不允许在本地存储上使用临时数据缓存磁盘。

创建连接以在本地存储临时数据，然后为每个 VM 的缓存磁盘大小和内存大小启用并配置非默认值。默认值根据连接类型量身定制，在大多数情况下都足够。有关详细信息，请参阅 创建计算机目录。

管理程序还可以通过在本地读取缓存磁盘映像来提供优化技术。例如，Citrix Hypervisor 提供了 IntelliCache™，可减少到中央存储的网络流量。

### 管理程序本地存储

管理程序本地存储方法将数据本地存储在管理程序上。使用此方法，主映像和其他操作系统数据将传输到站点中的管理程序。此过程发生在初始计算机创建和未来的映像更新中。此过程会导致管理网络上产生大量流量。映像传输也耗时，并且映像在不同时间对每个主机可用。

## 创建连接和资源

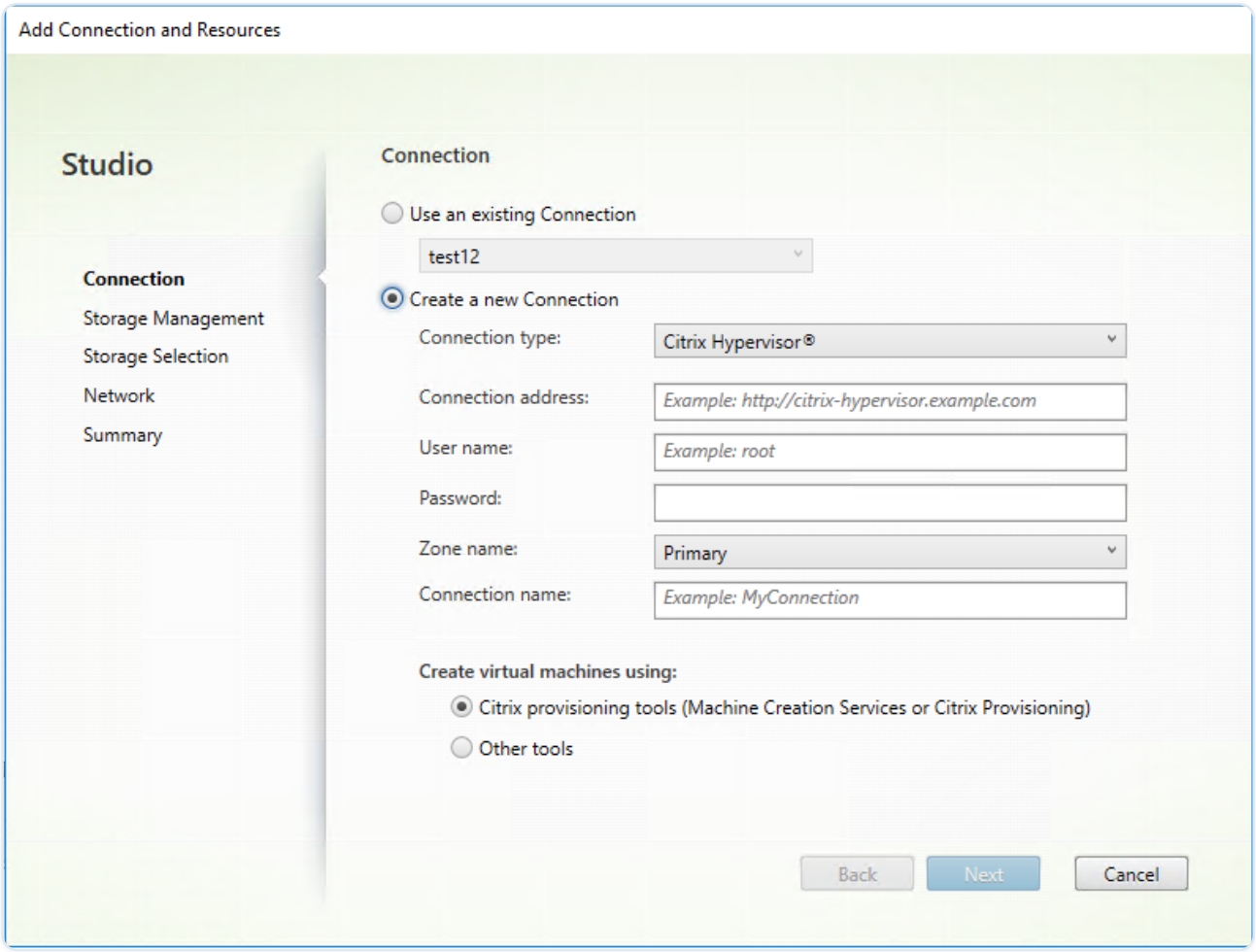
您可以在创建站点时选择性地创建第一个连接。站点创建向导包含以下部分中描述的连接相关页面。

如果您在创建站点后创建连接，请从步骤 1 开始。

> **重要提示：**
>
> 在创建连接之前，必须提供主机资源（存储和网络）。

1. 在 **Studio** 导航窗格中选择**配置 > 托管**。
2. 在**操作**窗格中选择**添加连接和资源**。
3. 向导将引导您完成以下页面（特定页面内容取决于所选的连接类型）。完成每个页面后，单击**下一步**，直到到达 **摘要** 页面。

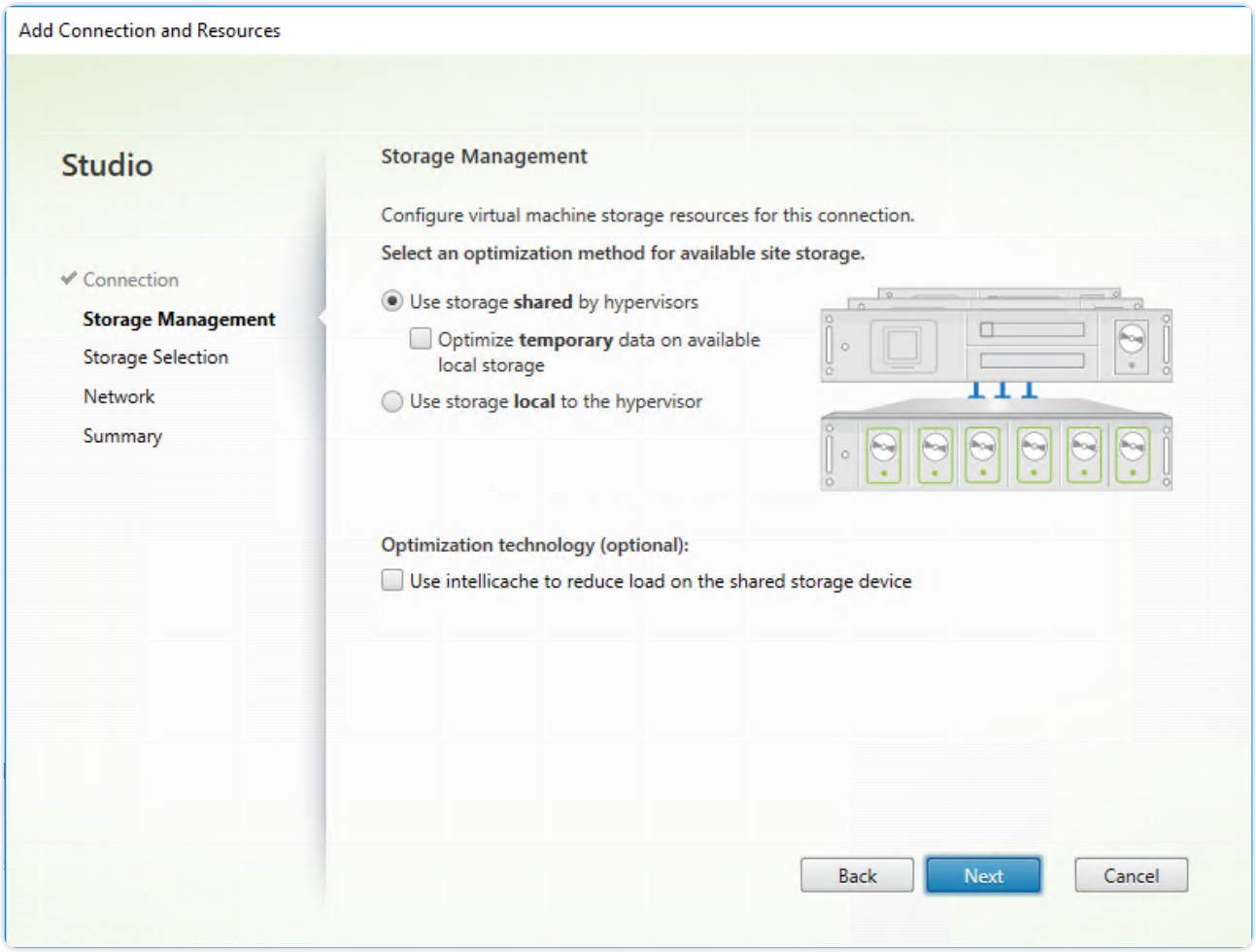
## 连接




在 **Connection** 页面上：

- 要创建连接，请选择 **创建新连接**。要基于与现有连接相同的主机配置创建连接，请选择 **使用现有连接**，然后选择相关连接。
- 在**连接类型**字段中选择您正在使用的管理程序。公共云主机连接仅在您使用混合权利许可证时才会在下拉列表中列出。
- 连接地址和凭据字段因所选连接类型而异。输入请求的信息。
- 输入连接名称。此名称显示在 Studio 中。
- 选择用于创建虚拟机的工具：Studio 工具（例如 Machine Creation Services™ 或 Citrix Provisioning）或其他工具。

# 存储管理




有关存储管理类型和方法的信息，请参阅 主机存储。

如果正在配置与 Hyper-V 或 VMware 主机的连接，请浏览并选择群集名称。其他连接类型不要求提供群集名称。

选择存储管理方法：虚拟机管理程序共享存储或虚拟机管理程序本地存储。

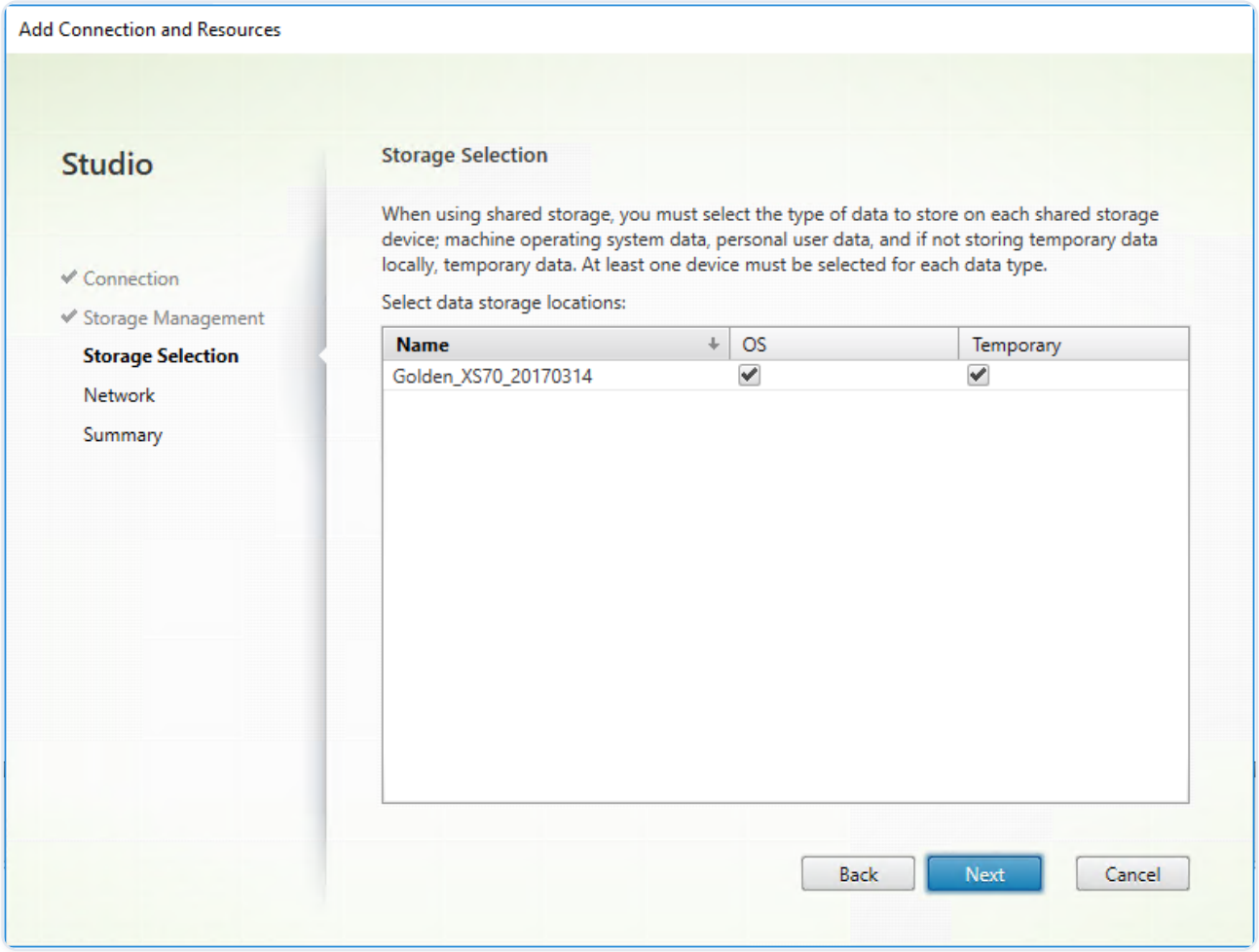
- 如果您选择管理程序共享的存储，请指明是否要将临时数据保留在可用的本地存储上。（您可以在使用此连接的计算机目录中指定非默认的临时存储大小。）**例外：** 使用群集共享卷 (CSV) 时，Microsoft System Center Virtual Machine Manager 不允许在本地存储上使用临时数据缓存磁盘。在 Studio 中配置该存储管理设置将失败。

如果您在 Citrix Hypervisor 池中使用共享存储，请指明是否要使用 IntelliCache 来减少共享存储设备上的负载。请参阅 将 IntelliCache 用于 Citrix Hypervisor 连接。

> **注意：**

> 在 XenServer®、VMware 和 SCVMM 虚拟化环境中，可以将回写缓存 (WBC) 磁盘与 OS 磁盘置于同一存储位置。为此，请勿选择**优化可用本地存储上的临时数据**。

### 存储选择




有关存储选择的详细信息，请参阅 主机存储。

为每种可用数据类型选择至少一个主机存储设备。您在上一页上选择的存储管理方法会影响此页面上可供选择的数据类型。在继续向导的下一页之前，请为每种支持的数据类型选择至少一个存储设备。

> **注意：**
>
> 在 XenServer、VMware 和 SCVMM 虚拟化环境中，如果您将可用 OS 存储列表配置为与可用临时存储列表相同，则 MCS 会将回写缓存 (WBC) 磁盘放置在与 OS 磁盘相同的存储位置。

> 如果您选择了由虚拟机管理程序共享的存储并在上一页上启用了**优化可用本地存储上的临时数据**，则**存储选择**页面的下半部分包含更多配置选项。您可以选择用于临时数据的本地存储设备。

显示当前选定的存储设备数量（在上图中，“已选择 1 个存储设备”）。将鼠标悬停在该条目上时，将显示选定的设备名称。

1. 单击**选择**以更改要使用的存储设备。
2. 在**选择存储**对话框中，选中或清除存储设备复选框，然后单击**确定**。

### 网络

在**网络**页面上，输入资源的名称。此名称将显示在 Studio 中，用于标识与连接关联的存储和网络组合。

选择虚拟机使用的一个或多个网络。

### 摘要

在**摘要**页面上，查看您的选择。完成后，单击**完成**。

**请记住**：在本地存储临时数据允许您在创建包含使用此连接的计算机的计算机目录时，为临时数据存储配置非默认值。请参阅创建计算机目录。

## 编辑连接设置

请勿使用此过程重命名连接或创建连接。这些连接是不同的操作。仅当当前主机具有新地址时才更改地址。输入不同计算机的地址会中断连接的计算机目录。

您无法更改连接的 **GPU** 设置，因为访问此资源的计算机目录必须使用适当的 GPU 专用主映像。请创建连接。

1. 在 **Studio** 导航窗格中选择**配置 \> 托管**。
2. 选择连接，然后在**操作**窗格中选择**编辑连接**。
3. 按照编辑连接时可用设置的指导进行操作。
4. 完成后，单击 **应用** 以应用所做的任何更改并保持窗口打开，或者单击 **确定** 以应用更改并关闭窗口。

**连接属性**页面：

- 要更改连接地址和凭据，请选择**编辑设置**，然后输入新信息。

- 要为 Citrix Hypervisor 连接指定高可用性服务器，请选择**编辑 HA 服务器**。Citrix 建议您选择池中的所有服务器，以便在池主服务器发生故障时允许与 Citrix Hypervisor 进行通信。

**高级**页面：

- 对于 Microsoft System Center Configuration Manager (ConfMgr) 局域网唤醒连接类型（与远程电脑访问结合使用），请输入 **ConfMgr 唤醒代理**、幻数据包和数据包传输信息。
- 限制阈值设置使您能够指定连接上允许的最大电源操作数。当电源管理设置允许同时启动过多或过少的计算机时，这些设置会有所帮助。每种连接类型都有特定的默认值，这些值适用于大多数情况，不应更改。
- **并发操作（所有类型）**设置指定两个值：此连接上可同时发生的最大绝对数量，以及使用此连接的所有计算机的最大百分比。您必须同时指定绝对值和百分比值。实际应用的限制是这两个值中较小的一个。

  例如，在包含 34 台计算机的部署中，如果“**同时操作（所有类型）**”设置为绝对值 10 和百分比值 10，则实际应用的限制为 3（即 34 的 10% 四舍五入到最接近的整数，小于 10 台计算机的绝对值）。
- “**每分钟最大新操作数**”是一个绝对数字。没有百分比值。
- 仅在 Citrix 支持代表的指导或明确的文档说明下，才可在**连接选项**字段中输入信息。

## 开启或关闭连接的维护模式

为连接开启维护模式可防止任何新的电源操作影响连接上存储的任何计算机。当计算机处于维护模式时，用户无法连接到该计算机。如果用户已连接，则维护模式将在他们注销时生效。

1. 在 **Studio** 导航窗格中选择**配置 > 托管**。
2. 选择连接。要启用维护模式，请在**操作**窗格中选择**启用维护模式**。要禁用维护模式，请选择**禁用维护模式**。

您还可以为单个计算机启用或禁用维护模式。此外，您还可以为计算机目录或交付组中的计算机启用或禁用维护模式。

## 删除连接

删除连接可能会导致大量计算机被删除和数据丢失。请确保受影响计算机上的用户数据已备份或不再需要。

删除连接之前，请确保：

- 所有用户均已从连接上存储的计算机注销。

- 没有正在运行的已断开连接的用户会话。
- 已为共用和专用计算机开启维护模式。
- 连接使用的计算机目录中的所有计算机都已关闭电源。

删除目录引用的连接后，计算机目录将变得不可用。如果此连接被目录引用，您可以选择删除该目录。在删除目录之前，请确保它未被其他连接使用。

1. 在 **Studio** 导航窗格中选择**配置 > 托管**。
2. 选择连接，然后在**操作**窗格中选择**删除连接**。
3. 如果此连接上存储有计算机，系统会询问您是否应删除这些计算机。如果需要删除，请指定如何处理关联的 Active Directory 计算机帐户。

## 重命名或测试连接

1. 在 **Studio** 导航窗格中选择**配置 > 托管**。
2. 选择连接，然后在**操作**窗格中选择**重命名连接**或**测试连接**。

## 查看连接上的计算机详细信息

1. 在 **Studio** 导航窗格中选择**配置 > 托管**。
2. 选择连接，然后在**操作**窗格中选择**查看计算机**。

上方窗格列出了通过连接访问的计算机。选择一台计算机可在下方窗格中查看其详细信息。还提供了开放会话的会话详细信息。

使用搜索功能快速查找计算机。您可以从窗口顶部的列表中选择一个已保存的搜索，或者创建一个新搜索。您可以通过键入计算机名称的全部或部分进行搜索，也可以构建一个表达式用于高级搜索。要构建表达式，请单击 **展开**，然后从属性和运算符列表中进行选择。

## 管理连接上的计算机

1. 在 **Studio** 导航窗格中选择**配置 > 主机**。
2. 选择一个连接，然后在 **操作** 窗格中选择 **查看计算机**。
3. 在 **操作** 窗格中选择以下选项之一。某些操作不可用，具体取决于计算机状态和连接主机类型。

| 操作 | 描述 |
| --- | --- |
| 启动 | 如果计算机已关机或已挂起，则启动计算机。 |

| 操作 | 描述 |
| --- | --- |
| 挂起 | 暂停计算机而不将其关闭，并刷新计算机列表。 |
| 关机 | 请求操作系统关机。 |
| 强制关机 | 强制关闭计算机电源，并刷新计算机列表。 |
| 重新启动 | 请求操作系统关机，然后再次启动计算机。如果操作系统无法执行，桌面将保持其当前状态。 |
| 启用维护模式 | 暂时停止与计算机的连接。用户无法连接到处于此状态的计算机。如果用户已连接，则维护模式将在他们注销时生效。（如上所述，您还可以为通过连接访问的所有计算机启用或禁用维护模式。） |
| 从交付组中删除 | 从交付组中删除计算机不会将其从交付组使用的计算机目录中删除。只有在没有用户连接到计算机时才能将其删除。在删除计算机时，请启用维护模式以暂时阻止用户连接。 |
| 删除 | 删除计算机后，用户将无法再访问该计算机，并且该计算机将从计算机目录中删除。在删除计算机之前，请确保所有用户数据都已备份或不再需要。仅当没有用户连接到计算机时，才能删除计算机。在删除计算机时，请启用维护模式以暂时阻止用户连接。 |

对于涉及计算机关机的操作，如果计算机未在 10 分钟内关机，则会断电。如果 Windows 在关机期间尝试安装更新，则存在在更新完成之前计算机断电的风险。

## 编辑存储

您可以显示用于存储使用连接的虚拟机的操作系统和临时数据的服务器状态。您还可以指定用于存储每种数据类型的服务器。

1. 在 **Studio** 导航窗格中选择**配置 > 主机**。
2. 选择连接，然后在 **操作** 窗格中选择**编辑存储**。
3. 在左侧窗格中，选择数据类型：操作系统或临时。

4. 选中或清除所选数据类型的一个或多个存储设备的复选框。
5. 单击 **确定**。

列表中的每个存储设备都包含其名称和存储状态。有效的存储状态值为：

- **正在使用中：** 存储正在用于创建计算机。
- **已取代：** 存储仅用于现有计算机。此存储中不会添加任何新计算机。
- **未使用：** 存储未用于创建计算机。

如果清除当前**正在使用中**的设备的复选框，其状态将更改为**已取代**。现有计算机将继续使用该存储设备（并且可以向其写入数据），因此即使该位置停止用于创建计算机，它也可能变满。

### 删除、重命名或测试资源

1. 在 **Studio** 导航窗格中选择**配置 > 主机**。
2. 选择资源，然后在 **操作** 窗格中选择相应的条目：**删除资源**、**重命名资源**或**测试资源**。

### 连接计时器

您可以使用策略设置配置三个连接计时器：

- **最长连接计时器：** 确定用户设备与虚拟桌面之间不间断连接的最长持续时间。使用**会话连接计时器**和**会话连接计时器间隔**策略设置。
- **连接空闲计时器：** 确定在用户没有输入的情况下，用户设备与虚拟桌面之间的不间断连接保持多长时间。使用**会话空闲计时器**和**会话空闲计时器间隔**策略设置。
- **断开连接计时器：** 确定断开连接的锁定虚拟桌面在会话注销前可以保持锁定的时间。使用**断开连接会话计时器**和**断开连接会话计时器间隔**策略设置。

当您更新任何这些设置时，请确保它们在您的部署中保持一致。

有关详细信息，请参阅策略设置文档。

## 本地主机缓存

为确保 Citrix Virtual Apps and Desktops 站点数据库始终可用，Citrix 建议从容错 SQL Server 部署开始，遵循 Microsoft 的高可用性最佳实践。（有关支持的 SQL Server 高可用性功能，请参阅 数据库。）但是，网络问题和中断可能导致用户无法连接到其应用程序或桌面。

当发生中断时，本地主机缓存功能允许站点中的连接代理操作继续进行。当本地 Citrix® 环境中 Delivery Controller™ 与站点数据库之间的连接失败时，就会发生中断。当站点数据库在 90 秒内无法访问时，本地主机缓存将启用。

自 XenApp and XenDesktop 7.16 起，连接租用功能（早期版本中的前身高可用性功能）已从产品中移除，不再可用。

## 数据内容

本地主机缓存包含以下信息，这些信息是主数据库中信息的子集：

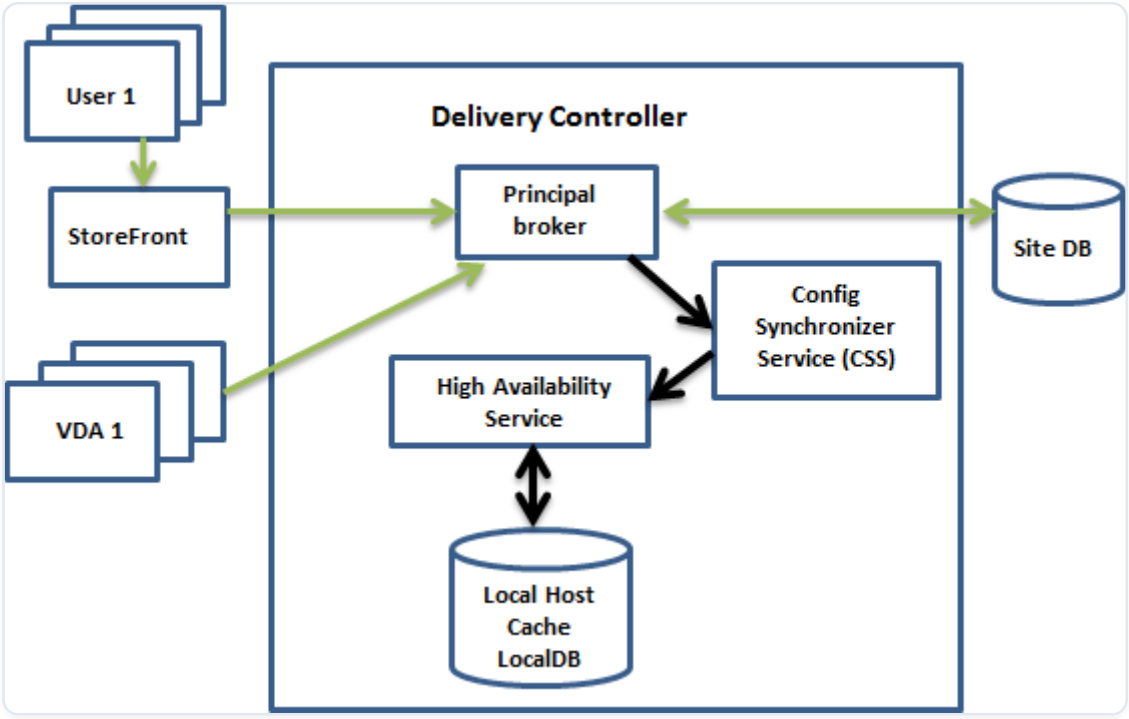
- 被授予站点发布的资源权限的用户和组的身份。
- 当前正在使用或最近使用过站点发布的资源的用户身份。
- 站点中配置的 VDA 计算机（包括远程 PC 访问计算机）的身份。
- 正在主动用于连接已发布资源的客户端 Citrix Receiver™ 计算机的身份（名称和 IP 地址）。

它还包含在主数据库不可用时建立的当前活动连接的信息：

- Citrix Receiver 执行的任何客户端计算机端点分析结果。
- 与站点相关的基础架构计算机（例如 NetScaler Gateway 和 StoreFront™ 服务器）的身份。
- 用户最近活动的日期、时间和类型。

## 工作原理

下图说明了正常运行期间本地主机缓存组件和通信路径。



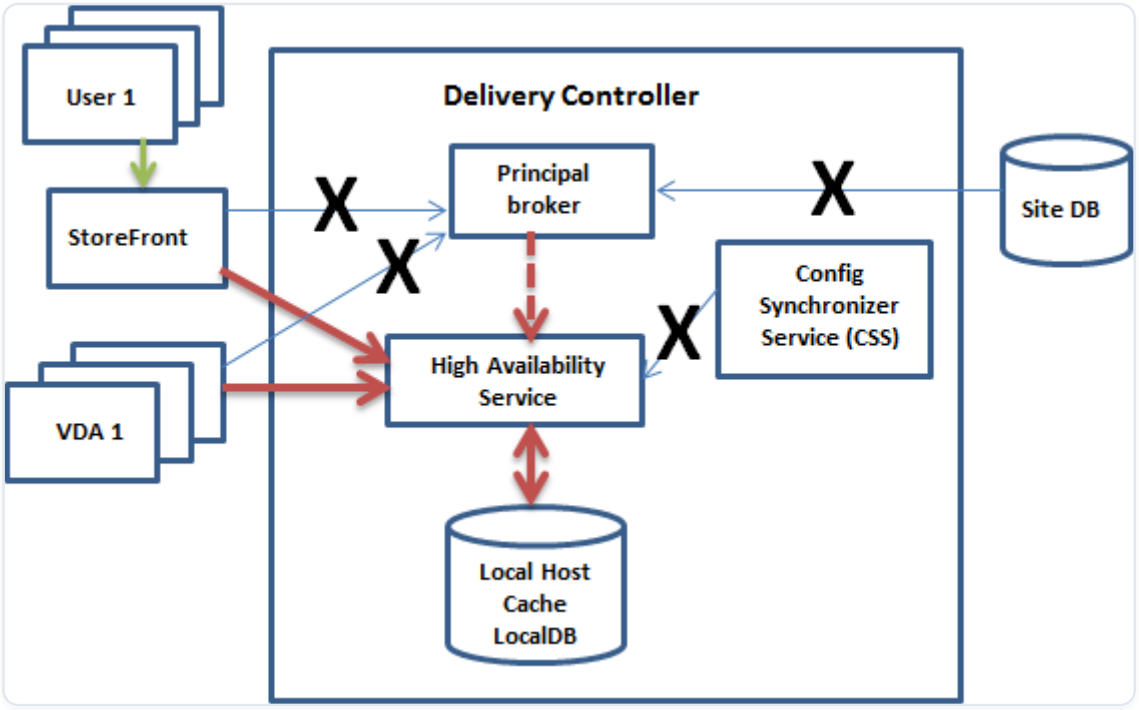
### 正常运行期间

- 控制器上的 *主代理* (Citrix Broker Service) 接受来自 StoreFront 的连接请求。代理与站点数据库通信，以将用户与已向控制器注册的 VDA 连接起来。
- Citrix 配置同步服务 (CSS) 大约每 5 分钟与代理检查一次，以查看是否进行了任何更改。这些更改可以是管理员发起的（例如更改交付组属性），也可以是系统操作（例如计算机分配）。
- 如果自上次检查以来发生了配置更改，CSS 会将信息同步（复制）到 Controller 上的辅助代理。（辅助代理也称为高可用性服务。）

  将复制所有配置数据，而不仅仅是自上次检查以来发生更改的项目。CSS 将配置数据导入到 Controller 上的 Microsoft SQL Server Express LocalDB 数据库中。此数据库称为本地主机缓存数据库。CSS 确保本地主机缓存数据库中的信息与站点数据库中的信息匹配。每次同步发生时，都会重新创建本地主机缓存数据库。

  安装 Controller 时，会自动安装 Microsoft SQL Server Express LocalDB（由本地主机缓存数据库使用）。（从命令行安装 Controller 时，可以禁止安装此项。）本地主机缓存数据库不能在 Controller 之间共享。您无需备份本地主机缓存数据库。每次检测到配置更改时，都会重新创建它。
- 如果自上次检查以来未发生任何更改，则不会复制任何数据。

下图说明了如果主代理与站点数据库失去联系（即发生中断）时通信路径的变化。




### 中断期间

中断开始时：

- 辅助代理开始侦听和处理连接请求。
- 中断开始时，辅助代理没有当前的 VDA 注册数据，但当 VDA 与其通信时，会触发注册过程。在此过程中，辅助代理还会获取有关该 VDA 的当前会话信息。
- 当辅助代理处理连接时，主代理会继续监视连接。连接恢复后，主代理会指示辅助代理停止侦听连接信息，并且主代理会恢复代理操作。下次 VDA 与主代理通信时，会触发注册过程。辅助代理会删除上次中断中所有剩余的 VDA 注册。当 CSS 得知部署中发生了配置更改时，它会恢复同步信息。

万一在同步期间发生中断，则会丢弃当前导入，并使用上次已知的配置。

事件日志 提供有关同步和中断的信息。

在中断模式下运行没有时间限制。

正常模式和中断模式之间的转换不会影响现有会话。它仅影响新会话的启动。

您也可以有意地触发中断。有关这样做的原因和方法，请参阅强制中断。

### 具有多个 Controller 的站点

除其他任务外，CSS 会定期向辅助代理提供有关区域中所有 Controller 的信息。（如果您的部署不包含多个区域，则此操作会影响站点中的所有 Controller。）拥有该信息后，每个辅助代理都会了解区域中其他 Controller 上运行的所有对等辅助代理。

辅助代理通过单独的通道相互通信。这些代理使用其运行所在计算机的 FQDN 名称的字母顺序列表来确定（选举）哪个辅助代理将在发生中断时在区域中执行代理操作。中断期间，所有 VDA 都向选定的辅助代理注册。区域中未选定的辅助代理会主动拒绝传入连接和 VDA 注册请求。

如果选定的辅助代理在中断期间发生故障，则会选举另一个辅助代理接管，并且 VDA 会向新选定的辅助代理注册。

中断期间，如果 Controller 重新启动：

- 如果该 Controller 不是选定的代理，则重新启动没有影响。
- 如果该 Controller 是选定的代理，则会选举另一个 Controller，导致 VDA 注册。重新启动的 Controller 通电后，它会自动接管代理，这会导致 VDA 再次注册。在这种情况下，注册期间的性能可能会受到影响。

如果在正常操作期间关闭 Controller，然后在中断期间将其打开，则如果该 Controller 被选为代理，则无法在该 Controller 上使用本地主机缓存。

事件日志 提供有关选举的信息。

## 中断期间不可用的功能以及其他差异

在中断模式下运行没有时间限制。但是，Citrix 建议尽快恢复连接。

中断期间：

- 您无法使用 Studio。
- 您对 PowerShell SDK 的访问权限有限。
  - 您必须首先：
    - 添加注册表项 `EnableCssTestMode`，其值为 1：`New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    - 使用端口 89：`Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ContollerDNSName, DesktopGroupName, RegistrationState`
  - 运行这些命令后，您可以访问：
    - 所有 `Get-Broker*` cmdlet。
- 无法从主机服务获取管理程序凭据。所有计算机都处于未知电源状态，并且无法发出任何电源操作。但是，主机上已开机的 VM 可用于连接请求。
- 仅当在正常操作期间发生分配时，才能使用已分配的计算机。在中断期间无法进行新的分配。
- 无法自动注册和配置远程电脑访问计算机。但是，在正常操作期间注册和配置的计算机是可用的。
- 如果资源位于不同的区域，服务器托管的应用程序和桌面用户使用的会话数可能会超过其配置的会话限制。
- 用户只能从包含当前活动/选定辅助代理的区域中的已注册 VDA 启动应用程序和桌面。在中断期间，不支持跨区域启动（从一个区域中的辅助代理到不同区域中的 VDA）。
- 如果在交付组中 VDA 的计划重启开始之前发生站点数据库中断，则重启将在中断结束时开始。这可能会导致意外结果。有关详细信息，请参阅因数据库中断而延迟的计划重启。
- 无法配置区域首选项。如果已配置，则在会话启动时不会考虑首选项。
- 会话启动不支持使用标签指定区域的标签限制。如果配置了此类标签限制，并且启用了 StoreFront 商店的高级运行状况检查 选项，则会话可能会间歇性地启动失败。

## 应用程序和桌面支持

本地主机缓存支持服务器托管的应用程序和桌面，以及静态（已分配）桌面。

本地主机缓存支持池化交付组中的桌面 VDA，具体如下：

- 默认情况下，在本地主机缓存事件期间，池化交付组（由 MCS 或 Citrix Provisioning™ 创建）中启用了 `ShutdownDesktopsAfterUse` 属性的电源管理桌面 VDA 不可用于新连接。您可以更改此默认设置，以允许这些桌面在本地主机缓存期间使用。

  但是，在中断期间，您不能依赖电源管理。（电源管理在正常操作恢复后恢复。）此外，这些桌面可能包含来自上一用户的数据，因为它们尚未重新启动。
- 要覆盖默认行为，必须在全站点范围和每个受影响的交付组中启用它。运行以下 PowerShell cmdlet。

  全站点范围：

  ```
  Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
  ```

  对于每个受影响的交付组，运行以下 PowerShell 命令：

  ```
  Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
  ```

  在站点和交付组中启用此功能不会影响配置的 `ShutdownDesktopsAfterUse` 属性在正常操作期间的工作方式。启用此功能后，VDA 在 LHC 事件完成后不会自动重新启动。池化交付组中的电源管理桌面 VDA 可以保留来自先前会话的数据，直到 VDA 重新启动。这可能发生在用户在非 LHC 操作期间从 VDA 注销时，或者可以手动触发重新启动。

> **重要提示：**

> 如果未在站点级别启用 ReuseMachinesWithoutShutdownInOutageAllowed 并在交付组级别启用 ReuseMachinesWithoutShutdownInOutage，则在本地主机缓存事件期间，所有尝试启动到池化交付组中电源管理桌面 VDA 的会话都将失败。

### RAM 大小注意事项

LocalDB 服务大约可以使用 1.2 GB RAM（数据库缓存最多 1 GB，运行 SQL Server Express LocalDB 额外 200 MB）。如果中断持续时间较长且发生大量登录（例如，12 小时内有 1 万用户），则辅助代理最多可以使用 1 GB RAM。这些内存要求是在 Controller 的正常 RAM 要求之外的，因此您可能需要增加 RAM 总容量。

如果您使用 SQL Server Express 安装作为站点数据库，则服务器将有两个 sqlserver.exe 进程。

### CPU 核心和套接字配置注意事项

Controller 的 CPU 配置，特别是可用于 SQL Server Express LocalDB 的核心数量，直接影响本地主机缓存性能，甚至比内存分配的影响更大。此 CPU 开销仅在数据库无法访问且辅助代理处于活动状态的中断期间才会出现。

尽管 LocalDB 可以使用多个核心（最多 4 个），但它仅限于单个套接字。添加更多套接字不会提高性能（例如，拥有 4 个套接字，每个套接字 1 个核心）。相反，Citrix 建议使用具有多个核心的多个套接字。在 Citrix 测试中，2x3（2 个套接字，3 个核心）配置比 4x1 和 6x1 配置提供了更好的性能。

### 存储注意事项

在中断期间，随着用户访问资源，LocalDB 会增长。例如，在以每秒 10 次登录的速度运行的登录/注销测试中，数据库每 2-3 分钟增长 1 MB。当正常操作恢复时，本地数据库会重新创建并释放空间。但是，LocalDB 安装所在的驱动器上必须有足够的可用空间，以允许数据库在中断期间增长。本地主机缓存在中断期间还会产生更多 I/O：大约每秒 3 MB 的写入，以及数十万次读取。

### 性能注意事项

在中断期间，一个辅助代理处理所有连接，因此在正常操作期间在多个 Controller 之间进行负载平衡的站点（或区域）中，选定的辅助代理可能需要在中断期间处理比正常情况多得多的请求。因此，CPU 需求会更高。站点（区域）中的每个辅助代理都必须能够处理本地主机缓存数据库和所有受影响的 VDA 带来的额外负载，因为在中断期间选定的辅助代理可能会发生变化。

VDI 限制：

- 在单区域 VDI 部署中，中断期间可有效处理多达 10,000 个 VDA。
- 在多区域 VDI 部署中，每个区域最多可处理 10,000 个 VDA，在站点中最多可处理 40,000 个 VDA，在中断期间可有效处理。例如，在中断期间，以下每个站点都可以得到有效处理：
  - 一个包含四个区域的站点，每个区域包含 10,000 个 VDA。
  - 一个包含七个区域的站点，其中一个区域包含 10,000 个 VDA，另外六个区域每个包含 5,000 个 VDA。

在中断期间，站点内的负载管理可能会受到影响。负载评估器（尤其是会话计数规则）可能会超出限制。

在所有 VDA 向辅助代理注册期间，该服务可能没有关于当前会话的完整信息。因此，在此期间的用户连接请求可能会导致启动新会话，即使可以重新连接到现有会话。此间隔（即“新”辅助代理在重新注册期间从所有 VDA 获取会话信息）是不可避免的。中断开始时已连接的会话在转换期间不受影响，但新会话和会话重新连接可能会受到影响。

每当 VDA 必须注册时，就会出现此间隔：

- 中断开始：从主代理迁移到辅助代理时。
- 中断期间辅助代理故障：从发生故障的辅助代理迁移到新选出的辅助代理时。
- 从中断中恢复：当正常操作恢复且主代理恢复控制时。

您可以通过降低 Citrix Broker Protocol 的 `HeartbeatPeriodMs` 注册表值来缩短此间隔（默认值 = 600000 毫秒，即 10 分钟）。此心跳值是 VDA 用于 ping 的间隔的两倍，因此默认值会导致每 5 分钟 ping 一次。

例如，以下命令将心跳更改为五分钟（300000 毫秒），这将导致每 2.5 分钟 ping 一次：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

更改心跳值时请务必小心。增加频率会导致控制器在正常模式和中断模式下负载增加。

无论 VDA 注册速度多快，此间隔都无法完全消除。

辅助代理之间同步所需的时间会随着对象数量（例如 VDA、应用程序、组）的增加而增加。例如，同步 5000 个 VDA 可能需要 10 分钟或更长时间才能完成。

### 与 XenApp 6.x 版本的区别

尽管此本地主机缓存实现与 XenApp 6.x 及更早版本 XenApp 版本中的本地主机缓存功能同名，但仍有显著改进。此实现更可靠，不易损坏。维护要求降至最低，例如无需定期执行 `dsmaint` 命令。从技术上讲，此本地主机缓存是完全不同的实现。

## 管理本地主机缓存

为使本地主机缓存正常工作，每个控制器上的 PowerShell 执行策略必须设置为 RemoteSigned、Unrestricted 或 Bypass。

### SQL Server Express 本地数据库

本地主机缓存使用的 Microsoft SQL Server Express LocalDB 软件在安装控制器或将控制器从 7.9 之前的版本升级时会自动安装。只有辅助代理与此数据库通信。您不能使用 PowerShell cmdlet 更改此数据库的任何内容。LocalDB 不能在控制器之间共享。

无论是否启用本地主机缓存，都会安装 SQL Server Express LocalDB 数据库软件。

为防止其安装，请使用 `XenDesktopServerSetup.exe` 命令安装或升级控制器，并包含 `/exclude "Local Host Cache Storage (LocalDB)"` 选项。但是，请记住，如果没有数据库，本地主机缓存功能将无法工作，并且您不能将其他数据库与辅助代理一起使用。

安装此 LocalDB 数据库不会影响您是否安装 SQL Server Express 作为站点数据库。

有关将早期 SQL Server Express LocalDB 版本替换为更新版本的信息，请参阅替换 SQL Server Express LocalDB。

### 产品安装和升级后的默认设置

在全新安装 Citrix Virtual Apps and Desktops（最低版本 7.16）期间，本地主机缓存处于启用状态。

升级（到版本 7.16 或更高版本）后，如果整个部署中的 VDA 少于 10,000 个，则会启用本地主机缓存。

### 启用和禁用本地主机缓存

- 要启用本地主机缓存，请输入：

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  要确定是否启用了本地主机缓存，请输入 `Get-BrokerSite`。检查 `LocalHostCacheEnabled` 属性是否为 `True`。
- 要禁用本地主机缓存，请输入：

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

请记住：从 XenApp 和 XenDesktop 7.16 开始，连接租用（在版本 7.6 中，此功能先于本地主机缓存）已从产品中移除，不再可用。

## 验证本地主机缓存是否正常工作

要验证本地主机缓存是否已正确设置并正常工作：

- 确保同步导入成功完成。检查 事件日志。
- 确保在每个 Delivery Controller 上创建了 SQL Server Express LocalDB 数据库。这确认了辅助代理可以在需要时接管。
  - 在 Delivery Controller 服务器上，浏览到 `C:\Windows\ServiceProfiles\NetworkService`。
  - 验证 `HaDatabaseName.mdf` 和 `HaDatabaseName_log.ldf` 已创建。

- 在 Delivery Controller 上 强制中断。验证本地主机缓存正常工作后，请记住将所有 Controller 恢复到正常模式。这大约需要 15 分钟。

## 事件日志

事件日志指示同步和中断发生的时间。在事件查看器日志中，中断模式被称为 *HA 模式*。*

**配置同步器服务：**

在正常操作期间，当 CSS 使用本地主机缓存代理将配置数据导入本地主机缓存数据库时，可能会发生以下事件。

- 503：Citrix 配置同步服务收到更新的配置。此事件指示同步过程的开始。
- 504：Citrix 配置同步服务导入了更新的配置。配置导入成功完成。
- 505：Citrix 配置同步服务导入失败。配置导入未成功完成。如果存在以前成功的配置，则在发生中断时会使用该配置。但是，它将与当前配置不同步。如果没有可用的以前配置，则服务在中断期间无法参与会话代理。在这种情况下，请参阅 故障排除 部分，并联系 Citrix 支持。
- 507：Citrix 配置同步服务放弃了导入，因为系统处于中断模式，并且正在使用本地主机缓存代理进行代理。服务收到了新配置，但由于发生中断而放弃了导入。这是预期行为。
- 510: 未从主配置服务接收到配置服务配置数据。
- 517: 与主代理通信时出现问题。
- 518: 配置同步脚本已中止，因为辅助代理（高可用性服务）未运行。

**高可用性服务：**

此服务也称为本地主机缓存代理。

- 3502: 发生中断，本地主机缓存代理正在执行代理操作。
- 3503: 中断已解决，正常操作已恢复。
- 3504: 指示哪个本地主机缓存代理被选中，以及参与选举的其他本地主机缓存代理。

## 强制中断

您可能希望故意强制中断。

- 如果您的网络反复出现故障。强制中断直到网络问题解决，可以防止在正常模式和中断模式之间连续转换（以及由此导致的频繁 VDA 注册风暴）。
- 测试灾难恢复计划。
- 帮助确保本地主机缓存正常工作。

- 更换或维护站点数据库服务器时。

要强制中断，请编辑包含 Delivery Controller 的每个服务器的注册表。在 `HKLM\Software\Citrix\DesktopServer\LHC` 中，创建并将 `OutageModeForced` 设置为 `REG_DWORD` 到 `1`。此设置指示本地主机缓存代理进入中断模式，无论数据库状态如何。将值设置为 `0` 会使本地主机缓存代理退出中断模式。

要验证事件，请监视 `C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService` 中的 `Current_HighAvailabilityService` 日志文件。

## 故障排除

当同步导入到本地主机缓存数据库失败并发布 505 事件时，可以使用多种故障排除工具。

**CDF 跟踪：** 包含 `ConfigSyncServer` 和 `BrokerLHC` 模块的选项。这些选项以及其他代理模块可能会识别问题。

**报告：** 如果同步导入失败，您可以生成报告。此报告会在导致错误的对象处停止。此报告功能会影响同步速度，因此 Citrix 建议在不使用时禁用它。

要启用并生成 CSS 跟踪报告，请输入以下命令：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTML 报告发布在 `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htm`。

生成报告后，输入以下命令以禁用报告功能：

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

**导出代理配置：** 提供用于调试目的的精确配置。

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

例如，`Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`。

# 虚拟 IP 和虚拟环回

> **重要提示：**

> Windows 10 Enterprise 多会话不支持远程桌面 IP 虚拟化 (Virtual IP)，我们也不支持在 Windows 10 Enterprise 多会话上使用虚拟 IP 或虚拟环回。

> 虚拟 IP 和虚拟环回功能在 Windows Server 2016 计算机上受支持。这些功能不适用于 Windows 桌面操作系统计算机。

Microsoft 虚拟 IP 地址功能为已发布的应用程序提供每个会话唯一的动态分配 IP 地址。Citrix 虚拟环回功能允许您配置依赖于与 localhost (默认为 127.0.0.1) 通信的应用程序，以使用 localhost 范围 (127.*) 内的唯一虚拟环回地址。

某些应用程序，例如 CRM 和计算机电话集成 (CTI)，使用 IP 地址进行寻址、许可、身份识别或需要唯一 IP 地址或环回地址的其他用途。其他应用程序可能绑定到静态端口，因此在多用户环境中启动应用程序的其他实例的尝试会失败，因为该端口正在使用中。为了使此类应用程序在 Citrix Virtual Apps™ 环境中正常运行，每个设备都需要一个唯一的 IP 地址。

虚拟 IP 和虚拟环回是独立的功能。您可以单独使用其中一个，也可以同时使用两者。

管理员操作概要：

- 要使用 Microsoft 虚拟 IP，请在 Windows 服务器上启用并配置它。(不需要 Citrix® 策略设置。)
- 要使用 Citrix 虚拟环回，请在 Citrix 策略中配置两个设置。

## 虚拟 IP

当在 Windows 服务器上启用和配置虚拟 IP 时，在会话中运行的每个已配置应用程序都将具有唯一的地址。用户访问 Citrix Virtual Apps 服务器上的这些应用程序的方式与访问任何其他已发布的应用程序的方式相同。在以下任一情况下，进程都需要虚拟 IP：

- 进程使用硬编码的 TCP 端口号
- 进程使用 Windows 套接字并且需要唯一的 IP 地址或指定的 TCP 端口号

要确定应用程序是否需要使用虚拟 IP 地址：

1. 从 Microsoft 获取 TCPView 工具。此工具列出所有绑定特定 IP 地址和端口的应用程序。
2. 禁用“解析 IP 地址”功能，以便您看到地址而不是主机名。

3. 启动应用程序并使用 TCPView 查看应用程序打开了哪些 IP 地址和端口，以及哪些进程名称正在打开这些端口。
4. 配置打开服务器 IP 地址 0.0.0.0 或 127.0.0.1 的任何进程。
5. 为确保应用程序不会在不同端口上打开相同的 IP 地址，请启动应用程序的另一个实例。

### Microsoft 远程桌面 (RD) IP 虚拟化工作原理

- 必须在 Microsoft 服务器上启用虚拟 IP 寻址。

  例如，在 Windows Server 2016 环境中，从“服务器管理器”中，展开 **远程桌面服务 > RD 会话主机连接** 以启用 RD IP 虚拟化功能，并配置设置以使用动态主机配置协议 (DHCP) 服务器按会话或按程序动态分配 IP 地址。有关说明，请参阅 Microsoft 文档。
- 启用该功能后，在会话启动时，服务器会从 DHCP 服务器请求动态分配的 IP 地址。
- RD IP 虚拟化功能按会话或按程序为远程桌面连接分配 IP 地址。如果您为多个程序分配 IP 地址，它们将共享一个按会话的 IP 地址。
- 为会话分配地址后，每当进行以下调用时，会话都会使用虚拟地址而不是系统的主要 IP 地址：`bind`、`closesocket`、`connect`、`WSAConnect`、`WSAAccept`、`getpeername`、`getsockname`、`sendto`、`WSASendTo`、`WSASocketW`、`gethostbyaddr`、`getnameinfo`、`getaddrinfo`。

在远程桌面会话主机配置中使用 Microsoft IP 虚拟化功能时，应用程序通过在应用程序和 Winsock 函数调用之间插入“筛选器”组件来绑定到特定的 IP 地址。应用程序随后只能看到要使用的正确 IP 地址。应用程序尝试侦听 TCP 或 UDP 通信的任何尝试都会自动绑定到其分配的虚拟 IP 地址（或环回地址）。应用程序打开的任何源连接都源自绑定到应用程序的 IP 地址。

在返回地址的函数中（例如 `GetAddrInfo()`，由 Windows 策略控制），如果请求本地主机 IP 地址，虚拟 IP 会查看返回的 IP 地址并将其更改为会话的虚拟 IP 地址。尝试通过此类名称函数获取本地服务器 IP 地址的应用程序只能看到分配给该会话的唯一虚拟 IP 地址。此 IP 地址通常用于后续的套接字调用，例如绑定或连接。有关 Windows 策略的更多信息，请参阅 Windows Server 中的 RDS IP 虚拟化。

通常，应用程序会请求绑定到端口以侦听地址 0.0.0.0。当应用程序执行此操作并使用静态端口时，您无法启动该应用程序的多个实例。虚拟 IP 地址功能还会在此类调用类型中查找 0.0.0.0，并将调用更改为侦听特定的虚拟 IP 地址，这使得多个应用程序可以在同一台计算机上的同一端口上侦听，因为它们都在侦听不同的地址。仅当在 ICA 会话中且启用了虚拟 IP 地址功能时，才会更改调用。例如，如果在不同会话中运行的应用程序的两个实例都尝试绑定到所有接口 (0.0.0.0) 和特定端口（例如 9000），它们将绑定到 VIPAddress1:9000 和 VIPAddress2:9000，并且不会发生冲突。

## 虚拟环回

启用 Citrix 虚拟 IP 回送策略设置允许每个会话拥有自己的回送地址进行通信。当应用程序在 Winsock 调用中使用 localhost 地址（默认 = 127.0.0.1）时，虚拟回送功能会简单地将 127.0.0.1 替换为 127.X.X.X，其中 X.X.X 表示会话 ID + 1。例如，会话 ID 为 7 时，地址为 127.0.0.8。万一会话 ID 超过第四个八位字节（大于 255），地址将滚动到下一个八位字节 (127.0.1.0)，最大值为 127.255.255.255。

在以下任一情况下，进程都需要虚拟回送：

- 进程使用 Windows 套接字回送 (localhost) 地址 (127.0.0.1)
- 进程使用硬编码的 TCP 端口号

对于使用回送地址进行进程间通信的应用程序，请使用虚拟回送策略设置。无需额外配置。虚拟回送不依赖于虚拟 IP，因此您无需配置 Microsoft 服务器。

- 虚拟 IP 回送支持。启用后，此策略设置允许每个会话拥有自己的虚拟回送地址。此设置默认禁用。此功能仅适用于通过“虚拟 IP 虚拟回送程序列表”策略设置指定的应用程序。
- 虚拟 IP 虚拟回送程序列表。此策略设置指定使用虚拟 IP 回送功能的应用程序。此设置仅在启用“虚拟 IP 回送支持”策略设置时适用。

### 相关功能

您可以使用以下注册表设置来确保虚拟环回优先于虚拟 IP。此功能称为首选环回。但是，请谨慎操作：

- 仅当同时启用虚拟 IP 和虚拟环回时才使用首选环回。否则，可能会出现意外结果。
- 不正确地编辑注册表可能会导致严重问题，可能需要您重新安装操作系统。Citrix 无法保证可以解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。在编辑注册表之前，请务必备份注册表。

在应用程序所在的服务器上运行 regedit。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`
- 名称: PreferLoopback, 类型: REG_DWORD, 数据: 1
- 名称: PreferLoopbackProcesses, 类型: REG_MULTI_SZ, 数据: \<进程列表\>

# 交付控制器

Delivery Controller 是服务器端组件，负责管理用户访问、代理和优化连接。Controller 还提供用于创建桌面和服务器映像的 Machine Creation Services™。

一个站点必须至少有一个 Controller。安装初始 Controller 后，您可以在创建站点时或之后添加更多 Controller。在一个站点中拥有多个 Controller 有两个主要好处。

- **冗余：** 最佳做法是，在生产站点中，始终在不同的物理服务器上至少部署两个 Controller。如果一个 Controller 出现故障，其他 Controller 可以管理连接并管理站点。
- **可扩展性：** 随着站点活动的增长，Controller 上的 CPU 利用率和数据库活动也会随之增长。额外的 Controller 使您能够处理更多用户以及更多应用程序和桌面请求，并可以提高整体响应能力。

每个 Controller 都直接与站点数据库通信。在具有多个区域的站点中，每个区域中的 Controller 都与主区域中的站点数据库通信。

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

## VDA 如何向 Controller 注册

VDA 必须先向站点中的 Delivery Controller 注册（建立通信），然后才能使用。有关 VDA 注册的信息，请参阅VDA 向 Controller 注册。

## 添加、删除或移动 Controller

要添加、删除或移动 Controller，您必须拥有 数据库 一文中列出的服务器角色和数据库角色权限。

不支持在 SQL 群集或 SQL 镜像安装中的节点上安装 Controller。

将 Delivery Controller™ 添加到站点时，请务必将该计算机的登录凭据添加到用于高可用性的任何副本 SQL Server。

如果您的部署使用数据库镜像：

- 在添加、删除或移动 Controller 之前，请确保主体数据库和镜像数据库均正在运行。此外，如果您将脚本与 SQL Server Management Studio 结合使用，请在运行脚本之前启用 SQLCMD 模式。
- 要在添加、删除或移动 Controller 后验证镜像，请运行 PowerShell `Get-configdbconnection` cmdlet。该 cmdlet 可确保在连接字符串中已将故障转移伙伴设置为镜像。

添加、删除或移动控制器后：

- 如果启用了自动更新，VDA 将在 90 分钟内收到更新的控制器列表。
- 如果未启用自动更新，请确保为所有 VDA 更新了控制器策略设置或 ListOfDDCs 注册表项。将控制器移动到另一个站点后，请在这两个站点上更新策略设置或注册表项。

### 添加控制器

您可以在创建站点时以及之后添加控制器。您不能将使用此软件的早期版本安装的控制器添加到使用此版本创建的站点。

1. 在包含受支持操作系统的服务器上运行安装程序。安装 Delivery Controller 组件以及您想要的任何其他核心组件。完成安装向导。
2. 如果您尚未创建站点，请启动 Studio。系统将提示您创建站点。在站点创建向导的“数据库”页面上，单击“选择”按钮，然后添加安装了附加 Controller 的服务器地址。

   如果您计划生成初始化数据库的脚本，请在生成脚本之前添加控制器。
3. 如果您已创建站点，请将 Studio 指向安装了附加 Controller 的服务器。单击“**扩展您的部署**”并输入站点地址。

### 删除控制器

从站点中删除 Controller 不会卸载 Citrix® 软件或任何其他组件。此操作会从数据库中删除 Controller，使其无法再用于代理连接和执行其他任务。如果您删除 Controller，以后可以将其添加回同一站点或另一个站点。一个站点至少需要一个 Controller，因此您无法删除 Studio 中列出的最后一个 Controller。

从站点中删除控制器时，不会删除控制器登录到数据库服务器的凭据。这可以避免意外删除同一计算机上其他产品服务使用的登录凭据。如果不再需要，必须手动删除登录凭据。删除登录凭据需要 `securityadmin` 服务器角色权限。

删除控制器后：

- 使用自动更新的 VDA 会重新注册到其他可用的控制器。仅当启用了自动更新机制并且 VDA 可以访问其他控制器（在与已删除控制器相同的辅助区域中，或在本地部署的主区域中）时，才会发生此重新注册。
- 更新 Citrix StoreFront 中的控制器信息。有关详细信息，请参阅管理控制器。
- 在 Citrix StoreFront 中，更新通过 Citrix Gateway 进行远程访问的安全票证颁发机构 (STA) URL。有关详细信息，请参阅管理安全票证颁发机构。
- 在 Citrix Gateway 中，更新任何虚拟服务器 STA URL。有关详细信息，请参阅Citrix Gateway。

> **重要提示：**

> 在从站点中删除控制器之前，请勿从 Active Directory 中删除该控制器。

1. 确保 Controller 已开机，以便 Studio 在不到一小时内加载。Studio 加载您要删除的 Controller 后，请在系统提示时关闭 Controller。
2. 在 Studio 导航窗格中选择“**配置 \> Controller**”，然后选择要删除的 Controller。
3. 在“操作”窗格中选择“**删除 Controller**”。如果您没有正确的数据库角色和权限，系统会提供生成脚本的选项，该脚本允许您的数据库管理员为您删除 Controller。
4. 您必须从数据库服务器中删除 Controller 的计算机帐户。删除之前，请检查其他服务是否正在使用该帐户。

使用 Studio 删除 Controller 后，流向该 Controller 的流量可能会在短时间内持续存在，以确保当前任务的正确完成。如果您想在短时间内强制删除 Controller，Citrix 建议您关闭安装它的服务器，或从 Active Directory 中删除该服务器。然后，重新启动站点上的其他 Controller，以确保不再与已删除的 Controller 进行通信。

### 将 Controller 移动到其他区域

如果您的站点包含多个区域，您可以将 Controller 移动到不同的区域。有关此移动如何影响 VDA 注册和其他操作的信息，请参阅《*区域*》文章。

1. 在 Studio 导航窗格中选择“**配置 \> Controller**”，然后选择要移动的 Controller。
2. 在“操作”窗格中选择“**移动**”。
3. 指定要将 Controller 移动到的区域。

### 将 Controller 移动到另一个站点

您无法将 Controller 移动到使用此软件的早期版本创建的站点。

1. 在 Controller 所在的站点（旧站点）上，在 Studio 导航窗格中选择“**配置 \> Controller**”。然后选择要移动的 Controller。
2. 在“操作”窗格中选择“**删除 Controller**”。如果您没有正确的数据库权限，可以生成一个脚本，允许具有这些权限的人员（例如数据库管理员）删除 Controller。一个站点至少需要一个 Controller，因此您无法删除 Studio 中列出的最后一个 Controller。
3. 在您要移动的控制器上，打开 Studio，在出现提示时重置服务，选择 **加入现有站点**，然后输入新站点的地址。

### 将 VDA 移动到其他站点

如果 VDA 是使用 Citrix Provisioning™ 预配的或是一个现有映像，则可以在升级时或将测试站点中创建的 VDA 映像移动到生产站点时，将 VDA 移动到另一个站点（从站点 1 到站点 2）。使用 Machine Creation Services (MCS) 预配的 VDA 无法从一个站点移动到另一个站点。MCS 不支持更改 VDA 检查以向 Controller 注册的 ListOfDDCs。使用 MCS 预配的 VDA 始终检查与其创建所在站点关联的 ListOfDDCs。

有两种方法可以将 VDA 移动到另一个站点：使用安装程序或 Citrix 策略。

#### 安装程序

运行安装程序并添加控制器，指定站点 2 中某个控制器的 FQDN（DNS 条目）。

仅当未使用“控制器”策略设置时，才在安装程序中指定控制器。

#### 组策略编辑器

以下示例在站点之间移动多个 VDA。

1. 在站点 1 中创建包含以下设置的策略，然后将策略筛选到交付组级别，以启动站点之间的分阶段 VDA 迁移。
    - 控制器：包含站点 2 中一个或多个控制器的 FQDN（DNS 条目）。
    - 启用控制器自动更新：设置为已禁用。
2. 交付组中的每个 VDA 都会在新策略发布后 90 分钟内收到警报。VDA 会忽略其收到的控制器列表（因为自动更新已禁用）；它会选择策略中指定的控制器之一，该策略列出了站点 2 中的控制器。
3. 当 VDA 成功向站点 2 中的控制器注册时，它会收到站点 2 的 ListOfDDCs 和策略信息，这些信息默认启用了自动更新。VDA 在站点 1 中注册的控制器不在站点 2 中的控制器发送的列表中。因此，VDA 会重新注册，从站点 2 列表中的控制器中进行选择。从那时起，VDA 会自动使用来自站点 2 的信息进行更新。

# VDA 注册

## 简介

> **注意：**

> 在本地环境中，VDA 向 Delivery Controller 注册。在 Citrix Cloud 服务环境中，VDA 向 Cloud Connector 注册。在混合环境中，一些 VDA 向 Delivery Controller 注册，而另一些则向 Cloud Connector 注册。

> VDA 必须先向站点中的一个或多个 Controller 或 Cloud Connector 注册（建立通信），然后才能使用。VDA 通过检查名为 `ListofDDCs` 的列表来查找 Controller 或 Connector。VDA 上的 `ListOfDDCs` 包含将该 VDA 指向站点上的 Controller 或 Cloud Connector 的 DNS 条目。为了实现负载平衡，VDA 会自动将连接分布到列表中的所有 Controller 或 Cloud Connector。

为什么 VDA 注册如此重要？

- 从安全角度来看，注册是一项敏感操作。您正在建立控制器或云连接器与 VDA 之间的连接。对于此类敏感操作，如果一切不完美，预期行为是拒绝连接。您实际上正在建立两个独立的通信通道：VDA 到控制器或云连接器，以及控制器或云连接器到 VDA。连接使用 Kerberos，因此时间同步和域成员资格问题是不可原恕的。Kerberos 使用服务主体名称 (SPN)，因此您不能使用负载均衡的 IP\\主机名。
- 如果 VDA 没有准确且最新的 Controller 或 Cloud Connector 信息（在您添加和删除 Controller 或 Cloud Connector 时），VDA 可能会拒绝由未列出的 Controller 或 Cloud Connector 代理的会话启动。无效条目可能会延迟虚拟桌面系统软件的启动。VDA 不会接受来自未知且不受信任的 Controller 或 Cloud Connector 的连接。

除了 `ListofDDCs` 之外，`ListOfSIDs`（安全 ID）还指示 `ListofDDCs` 中哪些计算机是受信任的。`ListofSIDs` 可用于减少 Active Directory 上的负载，或避免来自受损 DNS 服务器的潜在安全威胁。有关详细信息，请参阅 ListOfSIDs。

如果 `ListofDDCs` 指定了多个 Controller 或 Cloud Connector，VDA 会尝试以随机顺序连接它们。在本地部署中，`ListofDDCs` 还可以包含 Controller 组。VDA 会尝试连接组中的每个 Controller，然后才会转到 `ListofDDCs` 中的其他条目。

Citrix Virtual Apps and Desktops™ 在 VDA 安装期间会自动测试与已配置的 Controller 或 Cloud Connector 的连接。如果无法访问 Controller 或 Cloud Connector，则会显示错误。如果您忽略了无法联系 Controller 或 Cloud Connector 的警告（或者在 VDA 安装期间未指定 Controller 或 Cloud Connector 地址），则会显示消息提醒您。

## 配置 Controller 或 Cloud Connector 地址的方法

管理员选择 VDA 首次注册（初始注册）时要使用的配置方法。在初始注册期间，会在 VDA 上创建一个持久缓存。在后续注册期间，除非检测到配置更改，否则 VDA 会从此本地缓存中检索 Controller 或 Cloud Connector 列表。

在后续注册期间检索该列表的最简单方法是使用自动更新功能。自动更新默认启用。有关详细信息，请参阅自动更新。

有多种方法可以在 VDA 上配置 Controller 或 Cloud Connector 地址。

- 基于策略（LGPO 或 GPO）
- 基于注册表（手动、组策略首选项 (GPP)、在 VDA 安装期间指定）
- 基于 Active Directory OU（旧版 OU 发现）
- 基于 MCS (personality.ini)

在安装 VDA 时，您可以指定初始注册方法。（如果禁用自动更新，则在 VDA 安装期间选择的方法将用于后续注册。）

下图显示了 VDA 安装向导的**交付控制器**页面。

VDA 安装向导中的交付控制器页面(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vda-install-controllers-all.png)

### 基于策略 (LGPO\\GPO)

Citrix® 建议使用 GPO 进行初始 VDA 注册。它具有最高优先级。（尽管自动更新被列为最高优先级，但自动更新仅在初始注册后使用。）基于策略的注册提供了使用组策略进行配置的集中化优势。

要指定此方法，请完成以下两个步骤：

- 在 VDA 安装向导的**交付控制器**页面上，选择**稍后执行 (高级)**。即使您在 VDA 安装期间未指定控制器地址，向导也会多次提醒您指定控制器地址。（VDA 注册非常重要。）
- 通过 Citrix 策略使用 `Virtual Delivery Agent Settings > Controllers` 设置启用或禁用基于策略的 VDA 注册。（如果安全性是您的首要任务，请使用 `Virtual Delivery Agent Settings > Controller SIDs` 设置。）

此设置存储在 `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)` 下。

### 基于注册表

要指定此方法，请完成以下步骤之一：

- 在 VDA 安装向导的**交付控制器**页面上，选择**手动执行**。然后，输入已安装控制器的 FQDN，然后单击**添加**。如果您安装了更多控制器，请添加它们的地址。
- 对于命令行 VDA 安装，请使用 /controllers 选项并指定已安装的控制器或云连接器的 FQDN。

此信息存储在注册表项 `HKLM\Software\Citrix\VirtualDesktopAgent` 或 `HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent` 下的注册表值 `ListOfDDCs` 中。

您也可以手动配置此注册表项或使用组策略首选项 (GPP)。此方法可能优于基于策略的方法（例如，如果您希望对不同的控制器或云连接器进行条件处理，例如：对于以 XDW-001- 开头的计算机名称，使用 XDC-001）。

更新 `ListOfDDCs` 注册表项，其中列出了站点中所有控制器或云连接器的 FQDN。（此项等同于 Active Directory 站点 OU。）

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

如果 `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent` 注册表位置同时包含 `ListOfDDCs` 和 `FarmGUID` 键，则 `ListOfDDCs` 用于控制器或云连接器发现。如果在 VDA 安装期间指定了站点 OU，则存在 `FarmGUID`。（这可能用于旧版部署。）

（可选）更新 `ListOfSIDs` 注册表项（有关详细信息，请参阅 ListOfSIDs：

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)`

请记住：如果您还通过 Citrix 策略启用基于策略的 VDA 注册，则该策略会覆盖您在 VDA 安装期间指定的设置，因为它是一种优先级更高的方法。

### 基于 Active Directory OU（旧版）

此方法主要用于向后兼容，不建议使用。如果您仍在使用此方法，Citrix 建议更改为其他方法。

要指定此方法，请完成以下两个步骤：

- 在 VDA 安装向导的“**交付控制器**”页面上，选择“**从 Active Directory 中选择位置**”。
- 使用 `Set-ADControllerDiscovery.ps1` 脚本（在每个控制器上均可用）。此外，在每个 VDA 上配置 `FarmGuid` 注册表项以指向正确的 OU。此设置可以使用组策略进行配置。

有关详细信息，请参阅 基于 Active Directory OU 的发现。

### 基于 MCS

如果您使用 MCS 预配 VM，MCS 会设置控制器或云连接器列表。此功能与自动更新配合使用。创建目录时，MCS 会在初始预配期间将控制器或云连接器列表注入到 `Personality.ini` 文件中。自动更新会使列表保持最新。

要指定此方法，请在 VDA 安装向导的“**交付控制器**”页面上，选择“**让 Machine Creation Services™ 完成此操作**”。

### 审查和建议

最佳实践：

- 使用组策略注册方法进行初始注册。
- 使用自动更新（默认启用）以使您的控制器列表保持最新。
- 在多区域部署中，使用组策略进行初始配置（至少包含两个控制器或云连接器）。将 VDA 指向其区域本地的控制器或云连接器。使用自动更新使其保持最新。自动更新会自动优化卫星区域中 VDA 的 `ListofDDCs`。
- 在 `ListOfDDCs` 注册表项上列出多个控制器，用空格或逗号分隔，以防止在控制器不可用时出现注册问题。例如：

  ```
  DDC7x.xd.local DDC7xHA.xd.local



  32-bit: HKEY_LOCAL_MACHINE
  \Software\Citrix\VirtualDesktopAgent\ListOfDDCs



  HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs
  (REG_SZ)
  ```

- 确保 `ListofDDCs` 下列出的所有值都映射到有效的完全限定域名，以防止启动注册延迟。

## 自动更新

自动更新（在 XenApp 和 XenDesktop 7.6 中引入）默认启用。它是使 VDA 注册保持最新状态的最有效方法。尽管不用于初始注册，但自动更新软件会在初始注册发生时将 `ListofDDCs` 下载并存储在 VDA 上的持久缓存中。此过程针对每个 VDA 执行。缓存还包含计算机策略信息，这可确保策略设置在重新启动后仍保留。

使用 MCS 或 Citrix Provisioning™ 预配计算机时支持自动更新，但 Citrix Provisioning 服务器端缓存除外。服务器端缓存不是常见方案，因为自动更新缓存没有持久存储。

要指定此方法：

- 通过包含设置 `Virtual Delivery Agent Settings > Enable auto update of Controllers` 的 Citrix 策略启用或禁用自动更新。此设置默认启用。

工作原理：

- 每次 VDA 重新注册（例如，在计算机重新启动后），缓存都会更新。每个控制器或云连接器还会每 90 分钟检查一次站点数据库。如果自上次检查以来添加或删除了控制器或云连接器，或者发生了影响 VDA 注册的策略更改，则控制器或云连接器会向其注册的 VDA 发送更新列表，并且缓存会更新。VDA 接受其最近缓存列表中的所有控制器或云连接器的连接。
- 如果 VDA 收到的列表中不包含其注册的控制器或云连接器（换句话说，该控制器或云连接器已从站点中删除），则 VDA 会重新注册，从 `ListofDDCs` 中的控制器或云连接器中进行选择。

示例：

- 一个部署有三个控制器：A、B 和 C。一个 VDA 注册到控制器 B（在 VDA 安装期间指定）。
- 稍后，将两个控制器（D 和 E）添加到站点。在 90 分钟内，VDA 会收到更新列表，然后接受来自控制器 A、B、C、D 和 E 的连接。（在 VDA 重新启动之前，负载不会平均分配到所有控制器。）
- 再后来，控制器 B 被移动到另一个站点。在 90 分钟内，原始站点中的 VDA 会收到更新列表，因为自上次检查以来控制器已发生更改。最初注册到控制器 B 的 VDA（该控制器已不在列表中）会重新注册，从当前列表中的控制器（A、C、D 和 E）中进行选择。

在多区域部署中，卫星区域中的自动更新会首先自动缓存所有本地控制器。主区域中的所有控制器都缓存在备份组中。如果卫星区域中没有可用的本地控制器，则会尝试向主区域中的控制器注册。

如下例所示，缓存文件包含主机名和安全 ID (`ListofSIDs`) 列表。VDA 不查询 SID，这减少了 Active Directory 负载。

VDA 注册缓存文件示例图(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vda-registration-cache-file.png)

您可以使用 WMI 调用检索缓存文件。但是，它存储在只有 SYSTEM 帐户才能读取的位置。

> **重要提示：**
>
> 此信息仅供参考。请勿修改此文件。对本文件或文件夹的任何修改都将导致不受支持的配置。

```
Get-WmiObject -Namespace “Root\Citrix\DesktopInformation” -Class “Citrix_VirtualDesktopInfo” -Property “PersistentDataLocation”
```

如果出于安全原因（与减少 Active Directory 负载不同）需要手动配置 `ListofSIDs`，则无法使用自动更新功能。有关详细信息，请参阅 ListOfSIDs。

### 自动更新优先级的例外

尽管自动更新通常在所有 VDA 注册方法中具有最高优先级并会覆盖其他方法的设置，但存在一个例外。缓存中的 `NonAutoListOfDDCs` 元素指定了初始 VDA 配置方法。自动更新会监视此信息。如果初始注册方法发生更改，注册过程将跳过自动更新，并使用下一个最高优先级的配置方法。当您将 VDA 移动到另一个站点时（例如，在灾难恢复期间），此过程会很有帮助。

## 配置注意事项

查看常见的 VDA 注册配置。

<iframe src="https://www.youtube.com/embed/vrngwl2rc3" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
查看 VDA 注册步骤。

<iframe src="https://www.youtube.com/embed/9qpt0p609f" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
配置可能影响 VDA 注册的项目时，请考虑以下事项。

### 控制器或 Cloud Connector 地址

无论您使用哪种方法指定控制器或云连接器，Citrix 都建议使用 FQDN 地址。IP 地址不被视为受信任的配置，因为攻击 IP 比攻击 DNS 记录更容易。如果您手动填充 `ListofSIDs`，则可以在 `ListofDDCs` 中使用 IP。但是，仍建议使用 FQDN。

### 负载平衡

如前所述，VDA 会自动将连接分配到 `ListofDDCs` 中的所有控制器或 Cloud Connector。故障转移和负载平衡功能内置于 Citrix 代理协议 (CBP) 中。如果在配置中指定了多个控制器或 Cloud Connector，则注册会在需要时自动在它们之间进行故障转移。通过自动更新，所有 VDA 都会自动进行自动故障转移。

出于安全原因，您不能使用网络负载均衡器，例如 Citrix ADC。VDA 注册使用 Kerberos 相互身份验证，其中客户端 (VDA) 必须向服务 (控制器) 证明其身份。但是，控制器或 Cloud Connector 必须向 VDA 证明其身份。这意味着 VDA 和控制器或 Cloud Connector 同时充当服务器和客户端。如本文开头所述，存在两个通信通道：VDA 到控制器/Cloud Connector，以及控制器/Cloud Connector 到 VDA。

此过程中的一个组件称为服务主体名称 (SPN)，它作为属性存储在 Active Directory 计算机对象中。当 VDA 连接到 Controller 或 Cloud Connector 时，它必须指定要与谁通信。此地址是 SPN。如果您使用负载均衡 IP，相互 Kerberos 身份验证会正确识别该 IP 不属于预期的 Controller 或 Cloud Connector。

有关详细信息，请参阅：

- Kerberos 简介
- 使用 Kerberos 的相互身份验证

### 自动更新取代 CNAME

自动更新功能取代了 XenApp 和 XenDesktop 7.x 之前版本中的 CNAME (DNS 别名) 功能。从 XenApp 和 XenDesktop 7 开始，CNAME 功能已禁用。请使用自动更新而不是 CNAME。（如果您必须使用 CNAME，请参阅 CTX137960。为了使 DNS 别名一致地工作，请勿同时使用自动更新和 CNAME。）

### 控制器/云连接器组

在某些情况下，您可能希望以组的形式处理 Controller 或 Cloud Connector，其中一个组是首选组，另一个组在所有 Controller/Cloud Connector 都失败时用于故障转移。请记住，Controller 或 Cloud Connector 是从列表中随机选择的，因此分组有助于强制优先使用。

这些组旨在用于单个站点内（而非多个站点）。

使用括号指定 Controller/Cloud Connector 组。例如，对于四个 Controller（两个主用和两个备用），分组可能是：

```
(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)
```

在此示例中，第一个组中的 Controller（001 和 002）将首先处理。如果两者都失败，第二个组中的 Controller（003 和 004）将处理。

对于 XenDesktop 7.0 或更高版本，您需要执行一个额外步骤才能使用 **注册组** 功能。您需要从 Citrix Studio **禁止“启用控制器自动更新”**策略。

## ListOfSIDs

VDA 可以联系进行注册的控制器列表是 `ListofDDCs`。VDA 还必须知道要信任哪些控制器；VDA 不会自动信任 `ListofDDCs` 中的控制器。`ListofSIDs`（安全 ID）标识受信任的控制器。VDA 仅尝试向受信任的控制器注册。

在大多数环境中，`ListofSIDs` 是从 `ListofDDCs` 自动生成的。您可以使用 CDF 跟踪来读取 `ListofSIDs`。

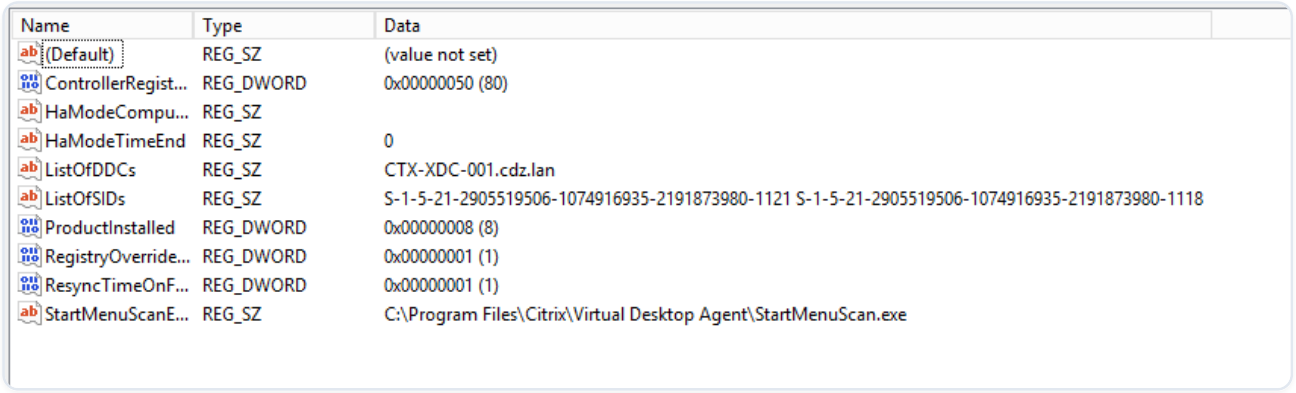
通常，无需手动修改 `ListofSIDs`。有几个例外。前两个例外不再有效，因为有更新的技术可用。

- **控制器角色分离：** 在 XenApp 和 XenDesktop 7.7 引入区域之前，当仅使用一部分控制器进行注册时，`ListofSIDs` 是手动配置的。例如，如果您使用 XDC-001 和 XDC-002 作为 XML 代理，使用 XDC-003 和 XDC-004 进行 VDA 注册，则您需要在 `ListofSIDs` 中指定所有控制器，并在 `ListofDDCs` 中指定 XDC-003 和 XDC-004。这不是典型或推荐的配置。请勿在新环境中使用此配置。请改用区域。
- **减少 Active Directory 负载：** 在 XenApp 和 XenDesktop 7.6 引入自动更新功能之前，`ListofSIDs` 用于减少域控制器上的负载。通过预填充 `ListofSIDs`，可以跳过从 DNS 名称到 SID 的解析。但是，自动更新功能消除了此工作的需要，因为此持久缓存包含 SID。Citrix 建议保持启用自动更新功能。
- **安全性：** 在某些高度安全的环境中，受信任控制器的 SID 是手动配置的，以避免来自受损 DNS 服务器的潜在安全威胁。但是，如果您这样做，则还必须禁用自动更新功能。否则，将使用持久缓存中的配置。

因此，除非有特殊原因，否则请勿修改 `ListofSIDs`。

如果必须修改 `ListofSIDs`，请在 `HKLM\Software\Citrix\VirtualDesktopAgent` 下创建名为 `ListOfSIDs (REG_SZ)` 的注册表项。该值是受信任 SID 的列表，如果有多个，请用空格分隔。

在以下示例中，一个控制器用于 VDA 注册 (`ListofDDCs`)，但两个控制器用于代理 (List OfSIDs)。



| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| ControllerRegist... | REG_DWORD | 0x00000050 (80) |
| HaModeCompu... | REG_SZ | |
| HaModeTimeEnd | REG_SZ | 0 |
| ListOfDDCs | REG_SZ | CTX-XDC-001.cdz.lan |
| ListOfSIDs | REG_SZ | S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118 |
| ProductInstalled | REG_DWORD | 0x00000008 (8) |
| RegistryOverride... | REG_DWORD | 0x00000001 (1) |
| ResyncTimeOnF... | REG_DWORD | 0x00000001 (1) |
| StartMenuScanE... | REG_SZ | C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe |

## VDA 注册期间的控制器搜索

当 VDA 尝试注册时，Broker Agent 首先在本地域中执行 DNS 查找，以确保可以访问指定的控制器。

如果初始查找未找到控制器，Broker Agent 可以启动 AD 中的回退自上而下查询。该查询会搜索所有域，并频繁重复。如果控制器地址无效（例如，管理员在安装 VDA 时输入了不正确的 FQDN），则该查询的活动可能会导致域控制器上出现分布式拒绝服务 (DDoS) 情况。

以下注册表项控制 Broker Agent 在初始搜索期间无法找到控制器时是否使用回退自上而下查询。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- 名称: `DisableDdcWildcardNameLookup`
- 类型: `DWORD`
- 值： `0` （默认）或任何非零值

当设置为 `0` 时，将启用回退搜索。如果控制器的初始搜索失败，则会启动回退自上而下搜索。这是默认行为。但是，如果设置为任何非零值，则会禁用回退搜索。如果控制器的初始搜索失败，Broker Agent 将停止查找。

## 解决 VDA 注册问题

如前所述，VDA 必须向 Delivery Controller 或 Cloud Connector 注册，才能在启动代理会话时被考虑。未注册的 VDA 可能会导致原本可用的资源利用不足。VDA 未注册的原因有很多，其中许多问题管理员都可以进行故障排除。Studio 在目录创建向导中以及创建交付组后提供故障排除信息。

- **在计算机目录创建期间识别问题：** 在目录创建向导中，添加现有计算机后，计算机帐户名称列表会指示每台计算机是否适合添加到目录。将鼠标悬停在每台计算机旁边的图标上，可显示有关该计算机的信息性消息。

  如果消息识别出有问题的计算机，您可以删除该计算机（使用**删除**按钮），或添加该计算机。例如，如果消息指示未获取有关计算机的信息（可能是因为它从未注册），您仍然可以选择添加该计算机。

  目录的功能级别控制目录中计算机可用的产品功能。使用新产品版本中引入的功能可能需要新的 VDA。设置功能级别可使该版本中引入的所有功能（以及更高版本中引入的功能，如果功能级别未更改）可用于目录中的计算机。但是，该目录中 VDA 版本较早的计算机将无法注册。
- **创建交付组后识别问题：** 创建交付组后，Studio 会显示与该组关联的计算机的详细信息。

  交付组的详细信息窗格指示应注册但未注册的计算机数量。换句话说，可能有一台或多台计算机已开机且未处于维护模式，但当前未向控制器注册。查看“未注册但应注册”的计算机时，请检查详细信息窗格中的“**故障排除**”选项卡，以了解可能的原因和建议的纠正措施。

### 有关 VDA 注册故障排除的更多信息

- 有关功能级别的更多信息，请参阅VDA 版本和功能级别。
- 有关 VDA 注册故障排除的更多信息，请参阅 CTX136668。
- 您还可以使用 Citrix Scout 运行状况检查来排查 VDA 注册和会话启动问题。有关详细信息，请参阅关于运行状况检查。

# 管理安全密钥

> **注意：**
>
> 您必须将此功能与 StoreFront™ 1912 LTSR CU2 或更高版本结合使用。
>
> 此功能允许您仅授权经批准的 StoreFront 和 Citrix Gateway 计算机与 Citrix Delivery Controllers 通信。启用此功能后，任何不包含密钥的请求都将被阻止。使用此功能可增加一层安全性，以防范源自内部网络的攻击。

使用此功能的通用工作流程如下：

1. 启用 Studio 以显示功能设置。
2. 配置站点的设置（使用 Studio 控制台或 PowerShell）。
3. 配置 StoreFront 中的设置（使用 PowerShell）。
4. 配置 Citrix ADC 中的设置（使用 PowerShell）。

## 启用 Studio 以显示功能设置

默认情况下，安全密钥的设置在 Studio 中是隐藏的。要启用 Studio 显示这些设置，请按如下方式使用 PowerShell SDK：

要启用此功能，请执行以下步骤：

1. 运行 Citrix 虚拟应用和桌面™ 远程 PowerShell SDK。
2. 在命令窗口中，运行以下命令：
   - `Add-PSSnapIn Citrix*`。此命令添加 Citrix 管理单元。
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManagementEnabled" -Value "True"`

有关远程 PowerShell SDK 的详细信息，请参阅SDK 和 API。

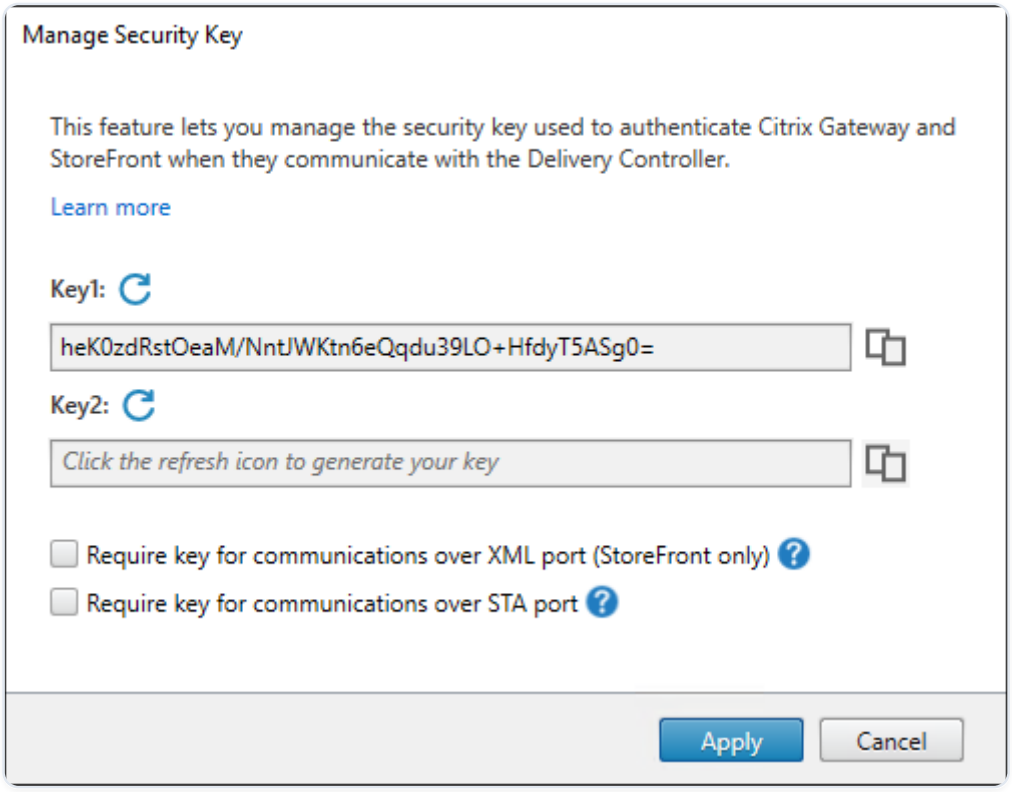
## 配置站点的设置

您可以使用 Studio 控制台或 PowerShell 在 Studio 中配置设置。

### 使用 Studio 控制台

在您(#enable-studio-to-show-the-feature-settings)后，转到**Studio > 配置 > 管理安全密钥**。您可能需要单击**刷新**才能显示**管理安全密钥**选项。

单击**管理安全密钥**后，将显示**管理安全密钥**窗口。




**重要提示：**

- 有两个可用的密钥。您可以对通过 XML 和 STA 端口进行的通信使用相同密钥或不同密钥。我们建议您一次只使用一个密钥。未使用的密钥仅用于密钥轮换。
- 请勿单击刷新图标来更新已在使用的密钥。否则，服务将中断。

单击刷新图标以生成新密钥。

**要求通过 XML 端口进行通信时使用密钥（仅限 StoreFront）**。如果选中此选项，则要求使用密钥对通过 XML 端口进行的通信进行身份验证。StoreFront 通过此端口与 Citrix Cloud 通信。有关更改 XML 端口的信息，请参阅知识中心文章 CTX127945。

**要求通过 STA 端口进行通信时使用密钥**。如果选中此选项，则要求使用密钥对通过 STA 端口进行的通信进行身份验证。Citrix Gateway 和 StoreFront 通过此端口与 Citrix Cloud 通信。有关更改 STA 端口的信息，请参阅知识中心文章 CTX101988。

应用更改后，单击**关闭**以退出**管理安全密钥**窗口。

### 使用 PowerShell

以下是与 Studio 操作等效的 PowerShell 步骤。

1. 运行 Citrix 虚拟应用和桌面 远程 PowerShell SDK。
2. 在命令窗口中，运行以下命令：
   - `Add-PSSnapIn Citrix*`
3. 运行以下命令以生成密钥并设置 Key1：
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. 运行以下命令以生成密钥并设置 Key2：
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. 运行以下一个或两个命令以启用密钥用于身份验证通信：
   - 要通过 XML 端口验证通信：
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - 要通过 STA 端口验证通信：
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

有关指导和语法，请参阅 PowerShell 命令帮助。

## 在 StoreFront 中配置设置

在 Studio 中完成配置后，您需要使用 PowerShell 在 StoreFront 中配置相关设置。

在 StoreFront 服务器上，运行以下 PowerShell 命令：

要配置用于通过 XML 端口进行通信的密钥，请使用命令。例如：

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]
```

```
Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

为以下参数输入相应的值：

- `Path to store`
- `Resource feed name`
- `secret`

要配置通过 STA 端口进行通信的密钥，请使用 `New-STFSecureTicketAuthority` 和 `Set-STFRoamingGateway` 命令。例如：

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

为以下参数输入相应的值：

- `Gateway name`
- `STA URL`
- `Secret`

有关指导和语法，请参阅 PowerShell 命令帮助。

## 在 Citrix ADC 中配置设置

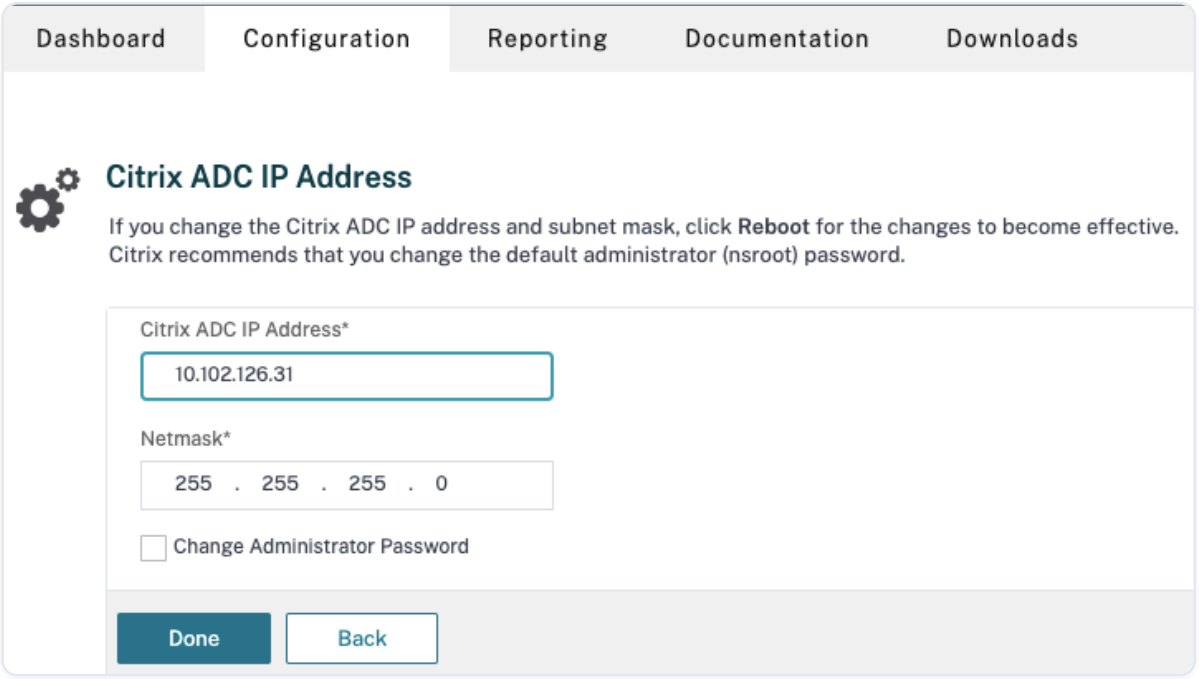
**注意：**

除非您使用 Citrix ADC 作为网关，否则无需在 Citrix ADC 中配置此功能。如果您使用 Citrix ADC，请按照以下步骤操作。

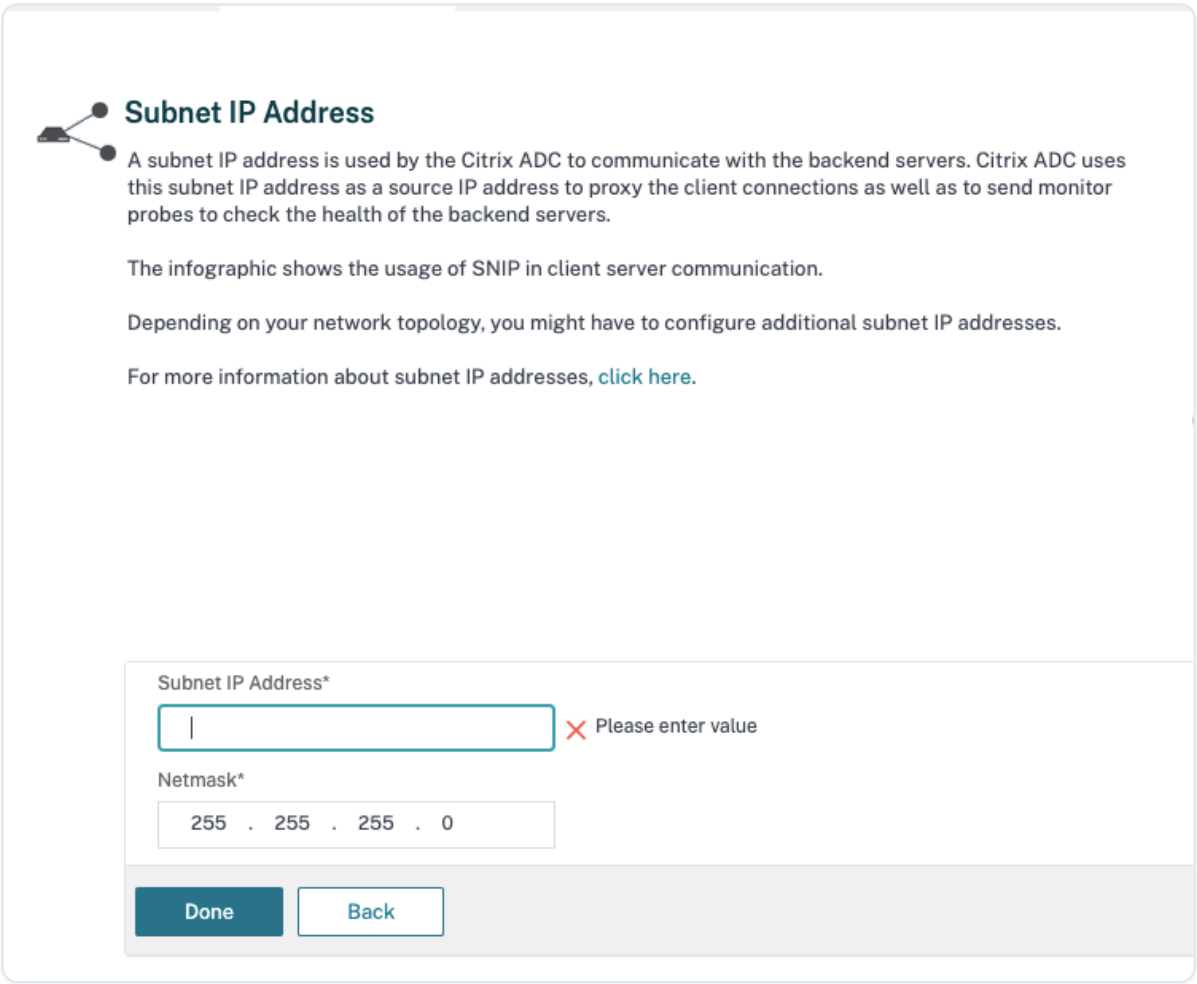
1. 确保已完成以下先决条件配置：

   - 已配置以下 Citrix ADC 相关 IP 地址。

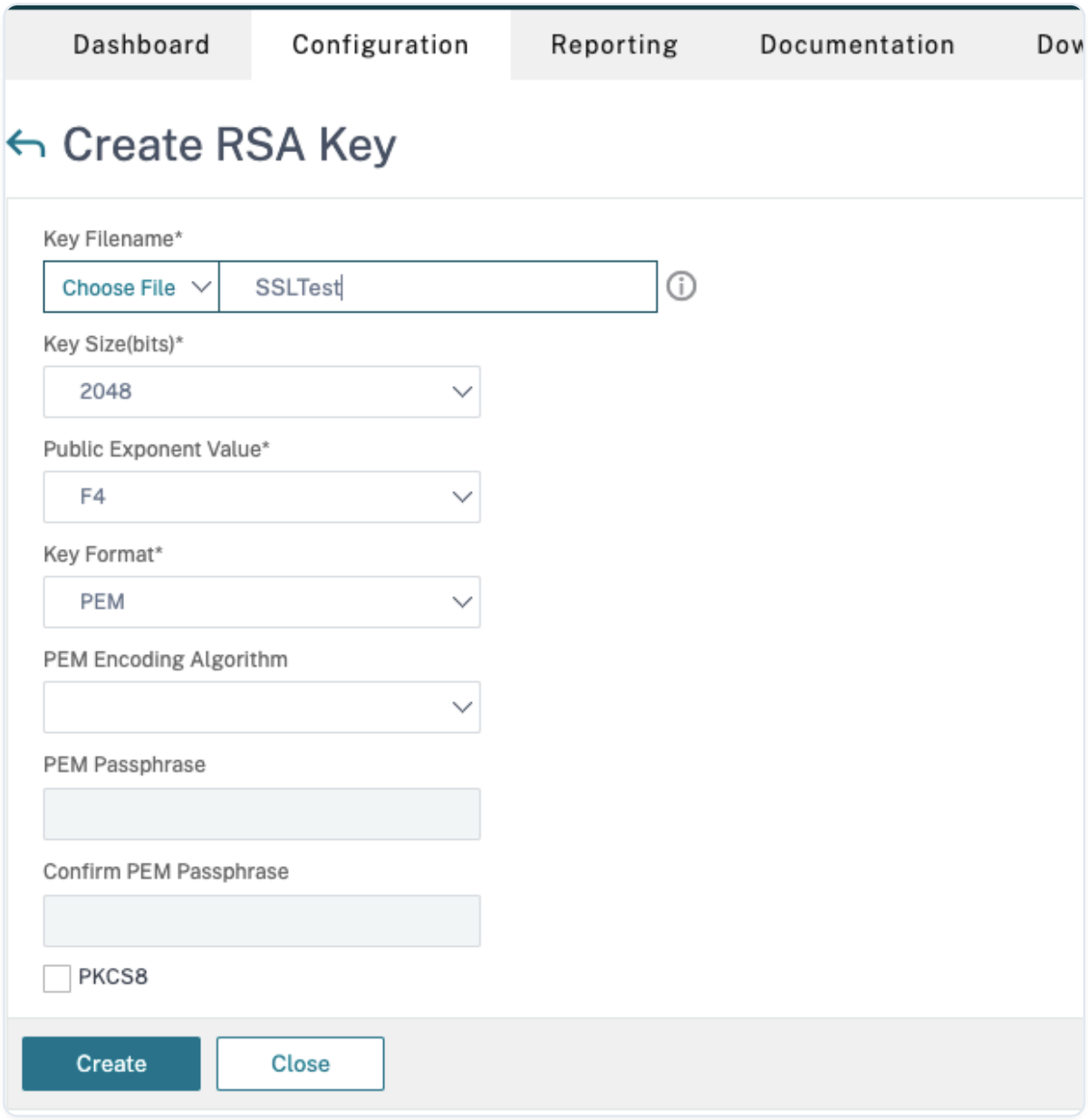
     - 用于访问 Citrix ADC 控制台的 Citrix ADC 管理 IP (NSIP) 地址。有关详细信息，请参阅配置 NSIP 地址。



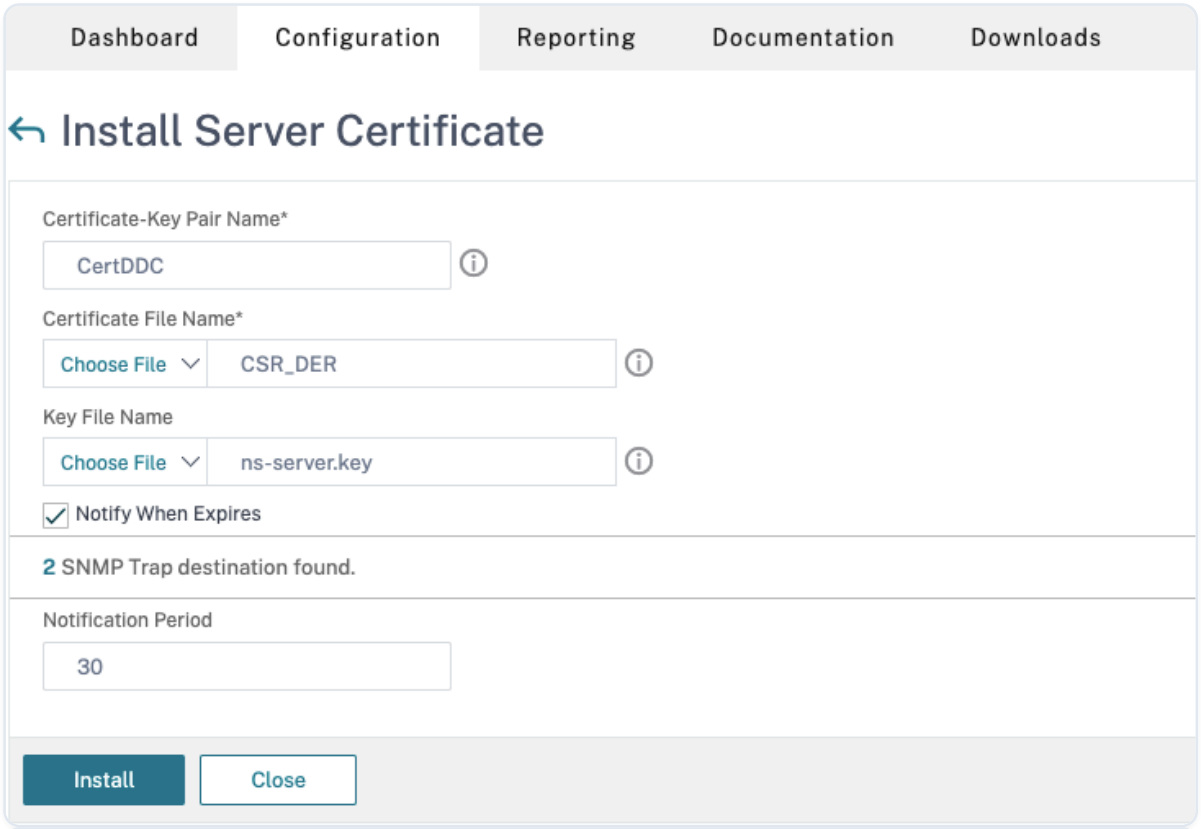

     - 子网 IP (SNIP) 地址，用于启用 Citrix ADC 设备与后端服务器之间的通信。有关详细信息，请参阅 配置子网 IP 地址。
     - Citrix Gateway 虚拟 IP 地址和负载均衡器虚拟 IP 地址，用于登录 ADC 设备以启动会话。有关详细信息，请参阅 创建虚拟服务器。

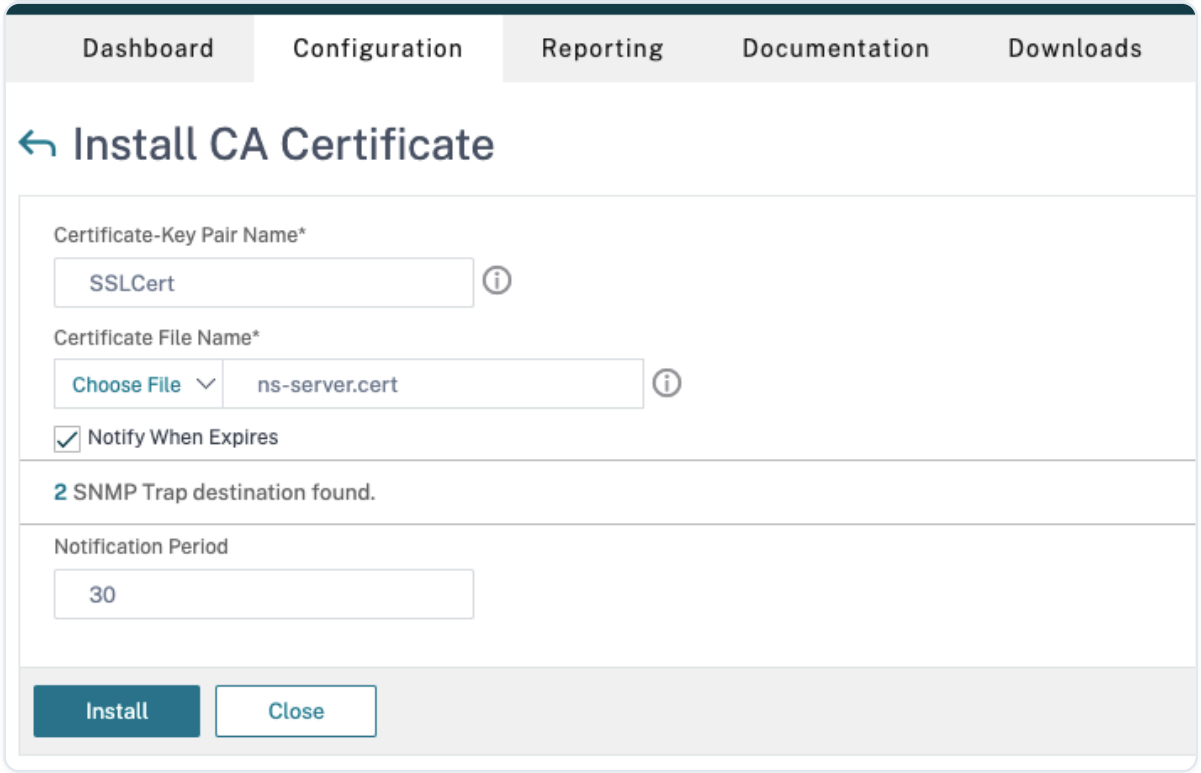



- Citrix ADC 设备中所需的模式和功能已启用。
  - 要启用这些模式，请在 Citrix ADC GUI 中转到 **System > Settings > Configure Mode**。
  - 要启用这些功能，请在 Citrix ADC GUI 中转到 **System > Settings > Configure Basic Features**。
- 证书相关配置已完成。
  - 证书签名请求 (CSR) 已创建。有关详细信息，请参阅 创建证书。

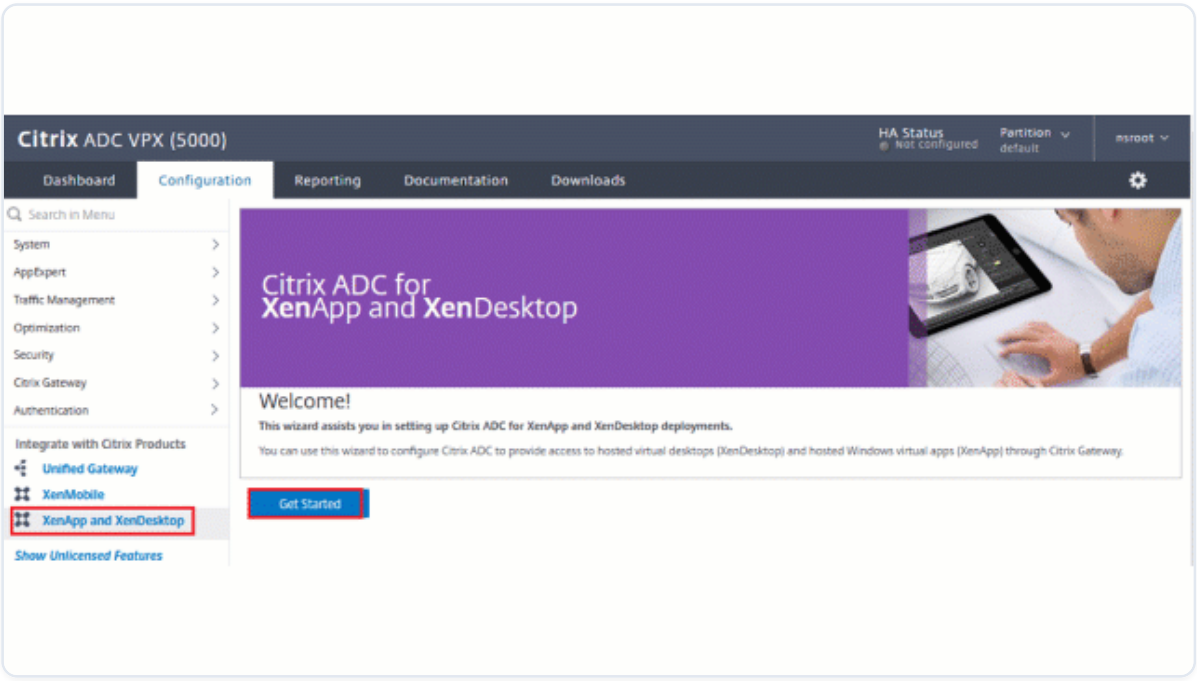



◦ 服务器证书、CA 证书和根证书已安装。有关详细信息，请参阅 安装、链接和更新。



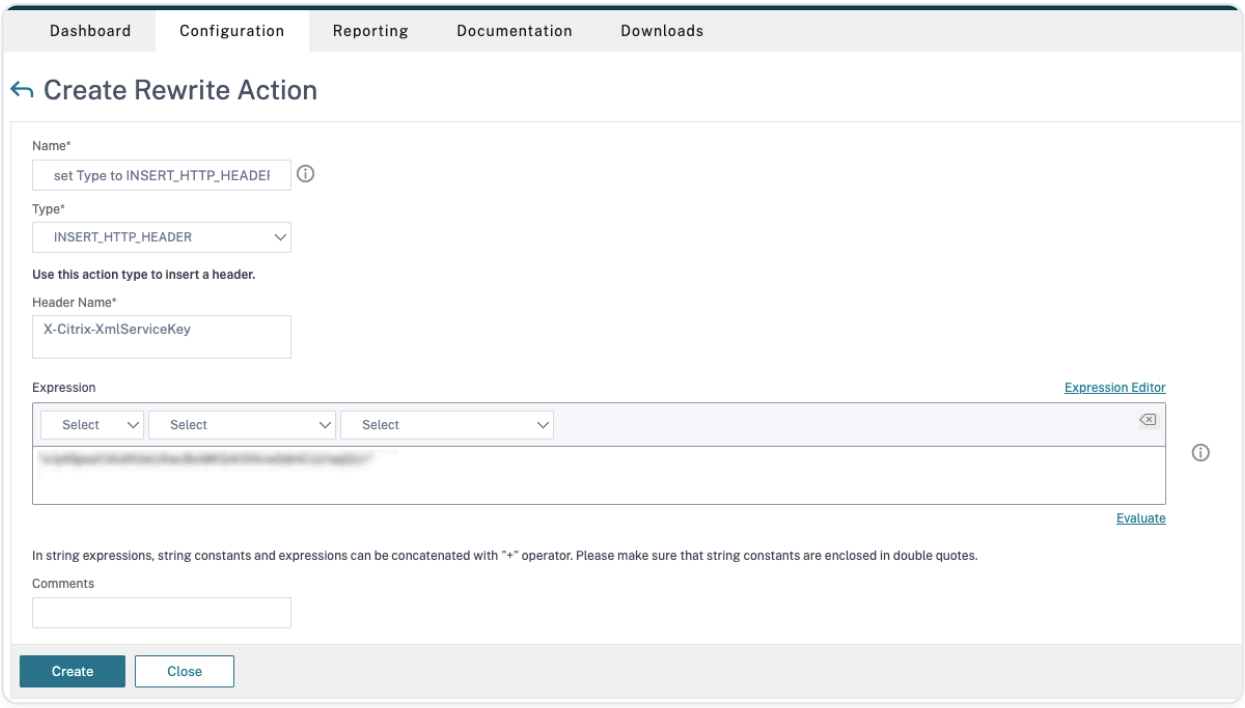

- 已为 Citrix Virtual Desktops 创建 Citrix Gateway。通过单击**测试 STA 连接**按钮测试连接，以确认虚拟服务器在线。有关详细信息，请参阅(/zh-cn/citrix-adc/current-release/solutions/deploy-xa-xd.html)。




2. 添加重写操作。有关详细信息，请参阅 配置重写操作。

   a. 请转到 **AppExpert > Rewrite > Actions**。

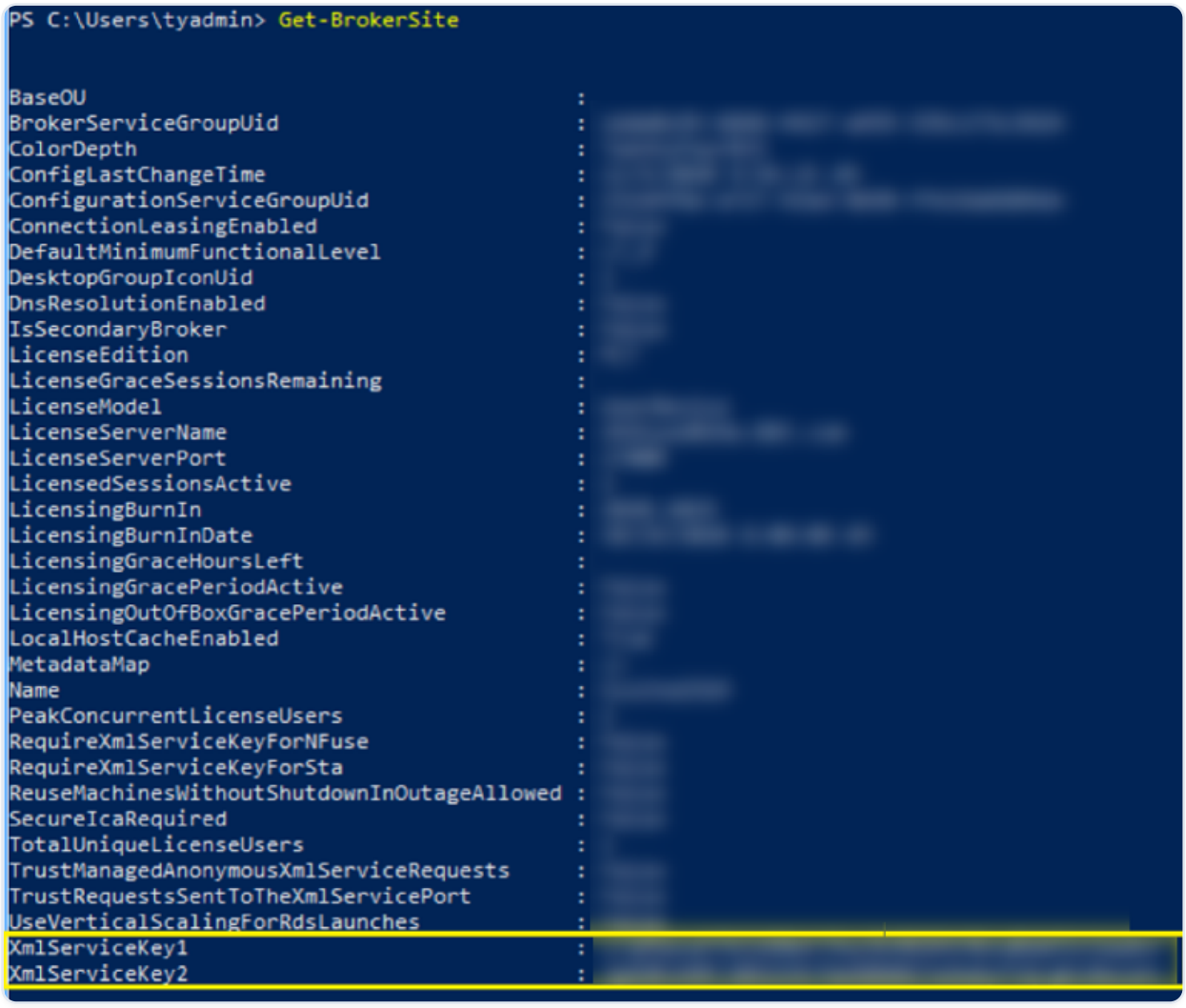
   b. 单击**添加**以添加重写操作。您可以将该操作命名为“set Type to INSERT_HTTP_HEADER”。




   a. 在 **类型** 中，选择 **INSERT_HTTP_HEADER**。

   b. 在 **标头名称** 中，输入 X-Citrix-XmlServiceKey。

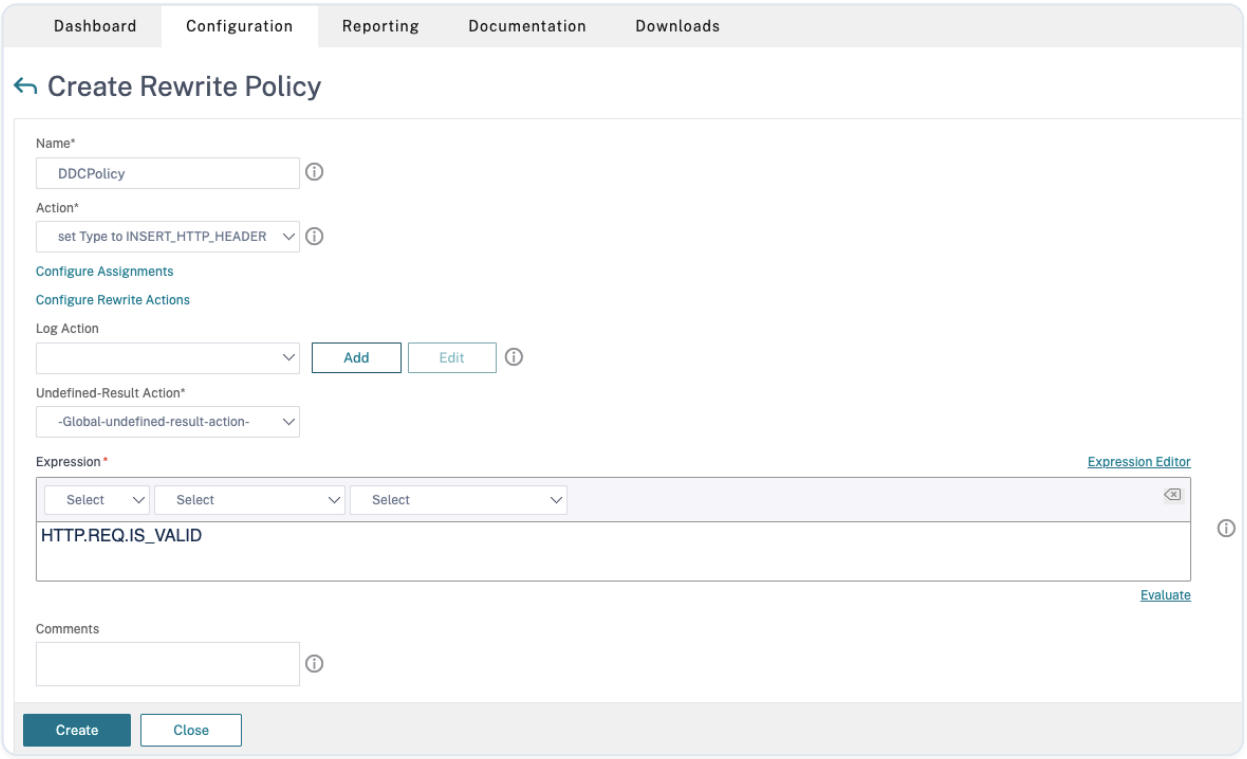
   c. 在 **表达式** 中，添加 `<XmlServiceKey1 value>` 并带引号。您可以从您的 Desktop Delivery Controller™ 配置中复制 XmlServiceKey1 值。




3. 添加重写策略。有关详细信息，请参阅配置重写策略。

   a. 请转到 **AppExpert > Rewrite > Policies**。

   b. 单击**添加**以添加策略。




a. 在 **操作** 中，选择上一步中创建的操作。

b. 在 **表达式** 中，添加 HTTP.REQ.IS_VALID。

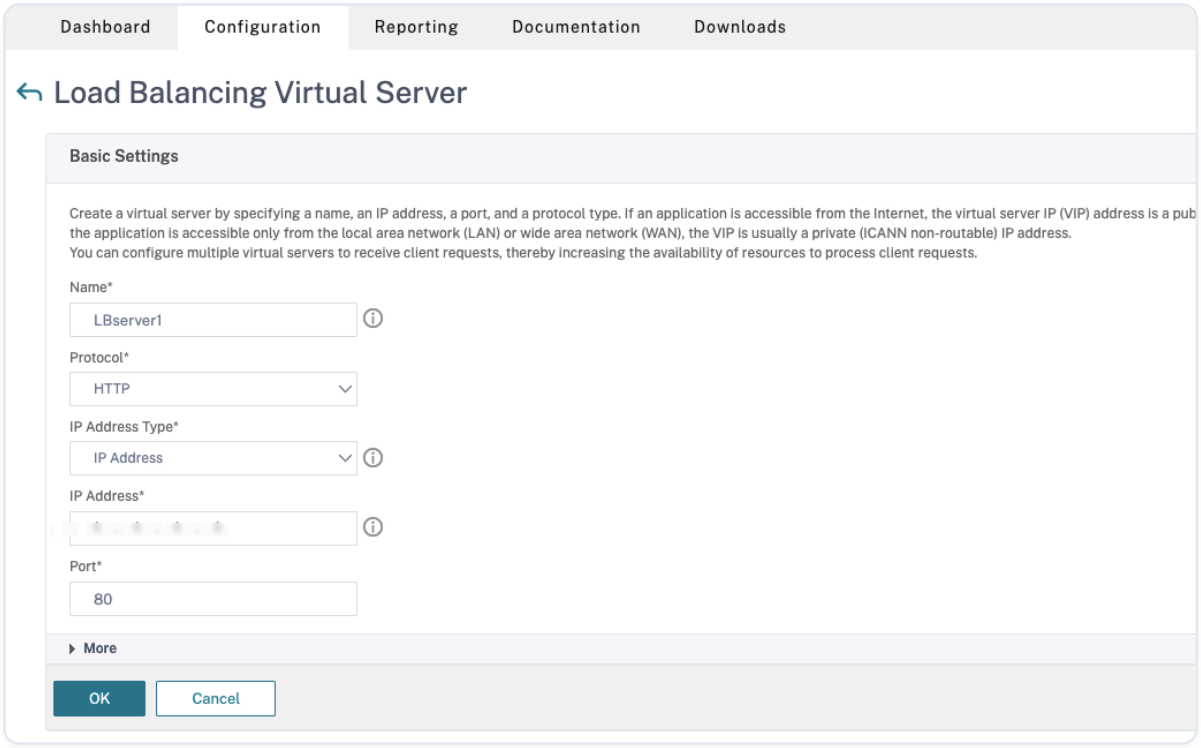
c. 单击**确定**。

4. 设置负载平衡。您必须为每个 STA 服务器配置一个负载平衡虚拟服务器。否则会话将无法启动。

   有关详细信息，请参阅设置基本负载平衡。

   a. 创建负载平衡虚拟服务器。

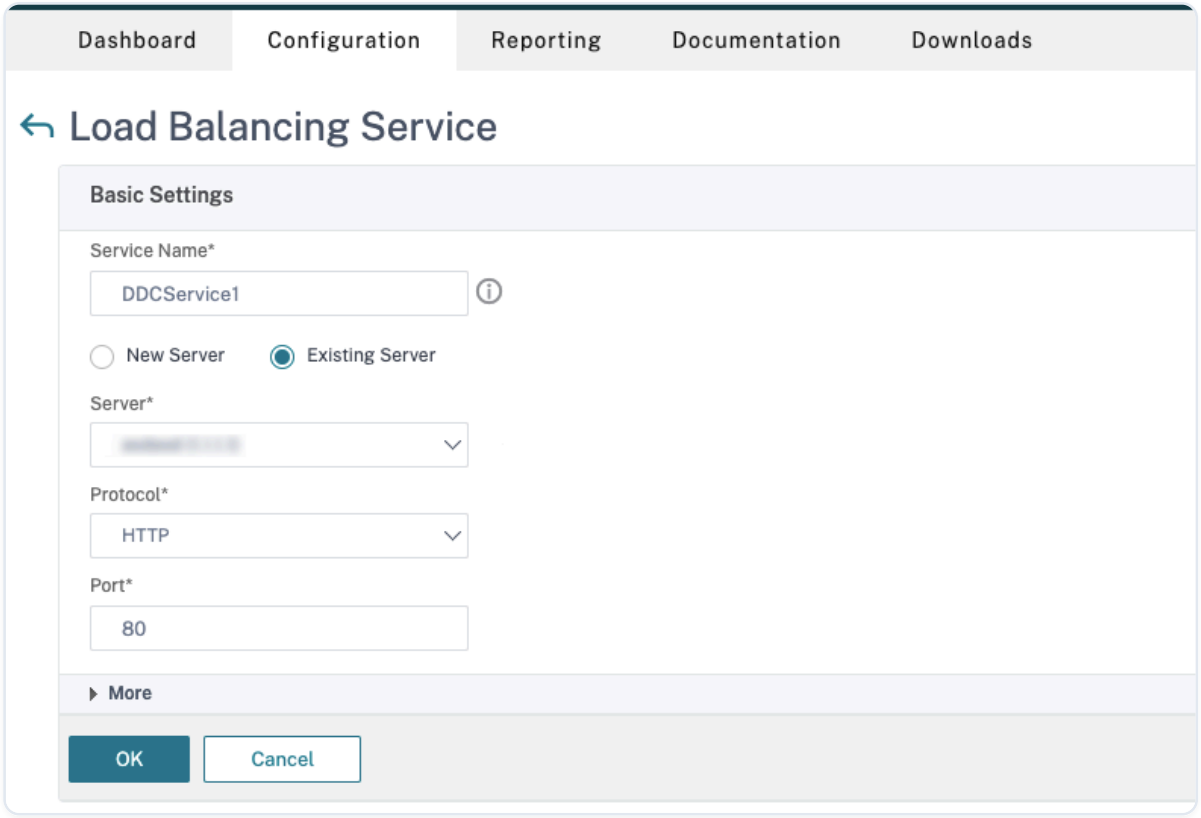
      - 转到 **流量管理 > 负载平衡 > 服务器**。
      - 在**虚拟服务器**页面上，单击**添加**。




- 在 **协议** 中，选择 **HTTP**。
- 添加负载平衡虚拟 IP 地址，并在 **端口** 中选择 **80**。
- 单击**确定**。

b. 创建负载平衡服务。

- 转到 **流量管理 > 负载平衡 > 服务**。



- 在 **现有服务器** 中，选择上一步中创建的虚拟服务器。
- 在 **协议** 中，选择 **HTTP**，并在 **端口** 中选择 **80**。
- 单击 **确定**，然后单击 **完成**。

c. 将服务绑定到虚拟服务器。

- 选择之前创建的虚拟服务器，然后单击**编辑**。
- 在“**服务和服务组**”中，单击“**无负载平衡虚拟服务器服务绑定**”。

绑定服务到虚拟服务器(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-bind-service-to-lbvserver.png)

- 在**服务绑定**中，选择之前创建的服务。
- 单击“**绑定**”。

d. 将之前创建的重写策略绑定到虚拟服务器。

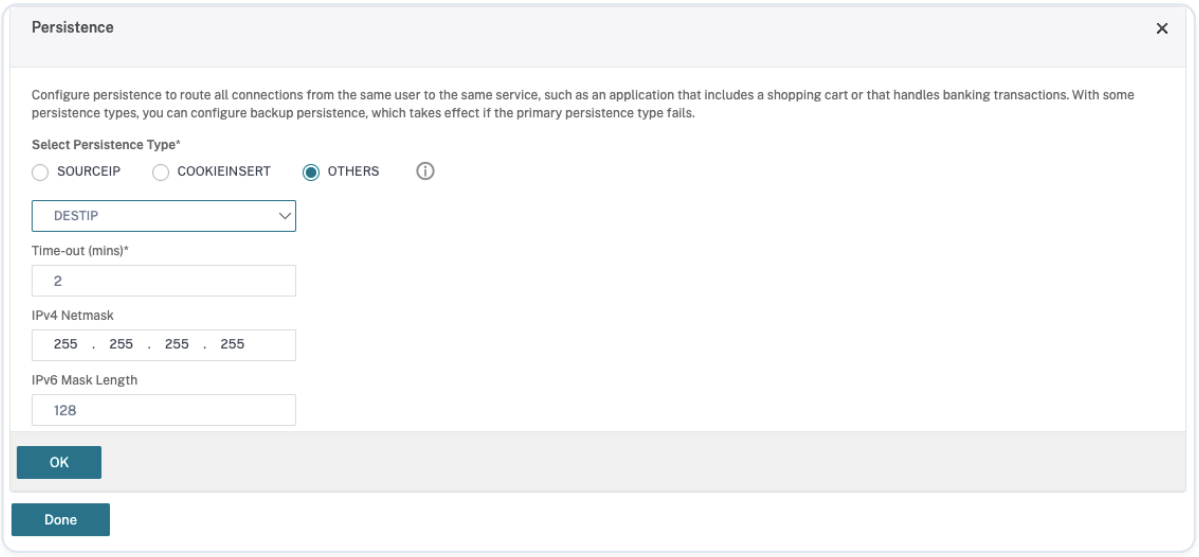
- 选择之前创建的虚拟服务器，然后单击**编辑**。
- 在“**高级设置**”中，单击“**策略**”，然后在“**策略**”部分单击“**+**”。

绑定重写策略(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-bind-rewrite-policy.png)

- 在“**选择策略**”中，选择“**重写**”，并在“**选择类型**”中，选择“**请求**”。
- 单击“**继续**”。
- 在“**选择策略**”中，选择之前创建的重写策略。
- 单击“**绑定**”。
- 点击 **完成**。

e. 如有必要，为虚拟服务器设置持久性。

- 选择之前创建的虚拟服务器，然后单击**编辑**。
- 在**高级设置**中，单击**持久性**。




- 选择持久性类型为**其他**。
- 选择 **DESTIP** 以根据虚拟服务器选择的服务 IP 地址（目标 IP 地址）创建持久性会话
- 在 **IPv4 子网掩码**中，添加与 DDC 相同的网络掩码。
- 单击 **确定**。

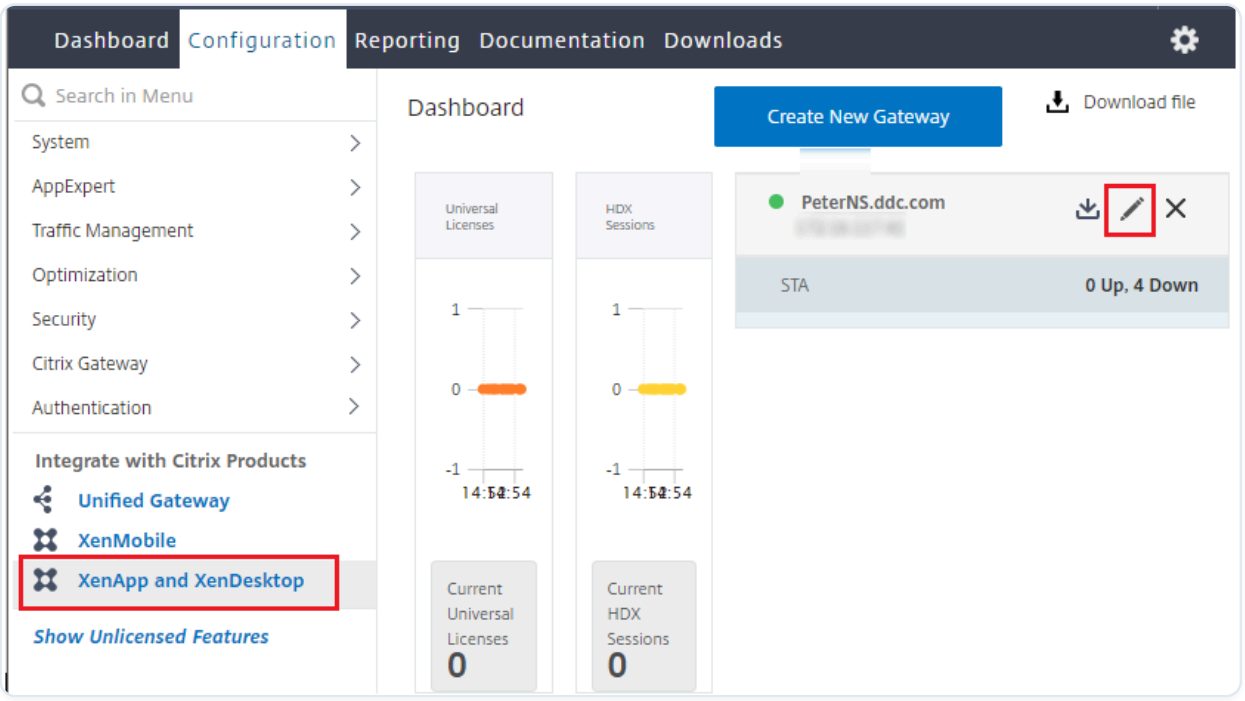
f. 对其他虚拟服务器也重复这些步骤。

### 如果 Citrix ADC 设备已配置 Citrix Virtual Desktops™，则进行配置更改

如果您已使用 Citrix Virtual Desktops 配置了 Citrix ADC 设备，则要使用安全 XML 功能，必须进行以下配置更改。

- 在会话启动之前，更改网关的**安全票证颁发机构 URL**，以使用负载平衡虚拟服务器的 FQDN。
- 确保 `TrustRequestsSentToTheXmlServicePort` 参数设置为 False。默认情况下，`TrustRequestsSentToTheXmlServicePort` 参数设置为 False。但是，如果客户已为 Citrix Virtual Desktops 配置了 Citrix ADC，则 `TrustRequestsSentToTheXmlServicePort` 设置为 True。

1. 在 Citrix ADC GUI 中，转到**配置 > 与 Citrix 产品集成**，然后单击 **XenApp and XenDesktop®**。
2. 选择网关实例，然后单击编辑图标。




3. 在 StoreFront 窗格中，单击编辑图标。

   编辑 StoreFront 详细信息(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/edit-storefront-details.png)

4. 添加 **安全票证颁发机构 URL**。

   - 如果启用了安全 XML 功能，则 STA URL 必须是负载平衡服务的 URL。
   - 如果禁用了安全 XML 功能，则 STA URL 必须是 STA 的 URL（DDC 的地址），并且 DDC 上的 TrustRequestsSentToTheXmlServicePort 参数必须设置为 True。

   添加 STA URL(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/add-sta-urls.png)

# 会话

保持会话活动对于提供最佳用户体验至关重要。由于网络不可靠、网络延迟高度可变以及无线设备的范围限制而失去连接，可能导致用户沮丧。在设备之间快速切换并在每次登录时访问相同的应用程序，对于许多移动工作人员（例如医护人员）来说是优先事项。

本文介绍的功能可优化会话的可靠性，减少不便、停机时间和生产力损失；使用这些功能，移动用户可以在设备之间快速轻松地漫游。

您还可以将用户从会话中注销、断开会话以及配置会话预启动和会话保持；请参阅 管理交付组。

## 会话可靠性

会话可靠性在网络连接中断时保持会话处于活动状态并显示在用户屏幕上。用户将继续看到他们正在使用的应用程序，直到网络连接恢复。

此功能对于使用无线连接的移动用户特别有用。例如，使用无线连接的用户进入铁路隧道并暂时失去连接。通常，会话会断开连接并从用户屏幕上消失，用户必须重新连接到断开的会话。借助会话可靠性，会话在计算机上保持活动状态。为了指示连接丢失，用户的显示屏会冻结，光标会变成旋转的沙漏，直到隧道另一侧的连接恢复。用户在中断期间可以继续访问显示屏，并在网络连接恢复时恢复与应用程序的交互。会话可靠性会在不提示重新身份验证的情况下重新连接用户。

Citrix Workspace™ 应用程序用户无法覆盖控制器设置。

您可以将会话可靠性与传输层安全性 (TLS) 结合使用。TLS 仅加密在用户设备和 Citrix Gateway 之间发送的数据。

使用以下策略设置启用和配置会话可靠性：

- “会话可靠性连接”策略设置允许或阻止会话可靠性。
- “会话可靠性超时”策略设置默认为 180 秒（即三分钟）。尽管您可以延长会话可靠性保持会话打开的时间，但此功能旨在方便用户。因此，它不会提示用户重新进行身份验证。随着您延长会话保持打开的时间，用户可能会分心并离开用户设备的可能性会增加。这些操作可能会使会话可供未经授权的用户访问。
- 传入的会话可靠性连接使用端口 2598，除非您在“会话可靠性端口号”策略设置中更改端口号。
- 为防止用户在不重新进行身份验证的情况下重新连接到中断的会话，请使用自动客户端重新连接功能。您可以配置“自动客户端重新连接身份验证”策略设置，以在用户重新连接到中断的会话时提示他们重新进行身份验证。

如果您同时使用会话可靠性和自动客户端重新连接，这两个功能将按顺序工作。会话可靠性会在您在“会话可靠性超时”策略设置中指定的时间量后关闭或断开用户会话。之后，“自动客户端重新连接”策略设置生效，尝试将用户重新连接到断开的会话。

## 客户端自动重新连接

借助自动客户端重新连接功能，Citrix Workspace 应用程序可以检测 ICA® 会话的意外断开连接，并自动将用户重新连接到受影响的会话。在服务器上启用此功能后，用户无需手动重新连接即可继续工作。

对于应用程序会话，Citrix Workspace 应用程序会尝试重新连接到会话，直到成功重新连接或用户取消重新连接尝试。

对于桌面会话，Citrix Workspace 应用程序会尝试在指定的时间段内重新连接到会话，除非重新连接成功或用户取消重新连接尝试。默认情况下，此时间段为五分钟。要更改此时间段，请在用户设备上编辑以下注册表设置（其中 `seconds` 是不再尝试重新连接会话的秒数）。

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

使用以下策略设置启用和配置自动客户端重新连接：

- **自动客户端重新连接：** 在连接中断后，启用或禁用 Citrix Workspace 应用程序的自动重新连接。
- **自动客户端重新连接身份验证：** 启用或禁用自动重新连接后对用户身份验证的要求。
- **自动客户端重新连接日志记录：** 启用或禁用事件日志中重新连接事件的日志记录。默认情况下，日志记录处于禁用状态。启用后，服务器的系统日志会捕获有关成功和失败的自动重新连接事件的信息。每个服务器都在其自己的系统日志中存储有关重新连接事件的信息。站点不提供所有服务器的重新连接事件的组合日志。

自动客户端重新连接包含一个基于加密用户凭据的身份验证机制。当用户首次登录时，服务器会加密并将用户凭据存储在内存中。服务器还会创建并向 Citrix Workspace 应用程序发送一个包含加密密钥的 Cookie。Citrix Workspace 应用程序将密钥提交给服务器以进行重新连接。服务器解密凭据并将其提交给 Windows 登录以进行身份验证。当 Cookie 过期时，用户必须重新进行身份验证才能重新连接到会话。

如果您启用了自动客户端重新连接身份验证设置，则不使用 Cookie。相反，当 Citrix Workspace 应用程序尝试自动重新连接时，会向用户显示一个请求凭据的对话框。

为了最大限度地保护用户凭据和会话，请对客户端和站点之间的所有通信使用加密。

通过使用 icaclient.adm 文件，在适用于 Windows 的 Citrix Workspace 应用程序上禁用自动客户端重新连接。有关详细信息，请参阅适用于 Windows 版本的 Citrix Workspace 应用程序文档。

连接设置也会影响自动客户端重新连接：

- 默认情况下，如前所述，通过站点级别的策略设置启用自动客户端重新连接。不需要用户重新身份验证。但是，如果服务器的 ICA TCP 连接配置为在通信链接中断时重置会话，则不会发生自动重新连接。自动客户端重新连接仅在服务器在连接中断或超时时断开会话的情况下才有效。在此上下文中，ICA TCP 连接是指用于 TCP/IP 网络上会话的服务器虚拟端口（而不是实际网络连接）。
- 默认情况下，服务器上的 ICA TCP 连接设置为断开具有中断或超时连接的会话。断开的会话在系统内存中保持完整，并可供 Citrix Workspace 应用程序重新连接。

- 连接可以配置为重置或注销具有中断或超时连接的会话。当会话被重置时，尝试重新连接会启动一个新会话。应用程序将重新启动，而不是将用户恢复到正在使用的应用程序中的相同位置。
- 如果服务器配置为重置会话，则自动客户端重新连接会创建一个新会话。此过程要求用户输入其凭据才能登录到服务器。
- 如果 Citrix Workspace 应用程序或插件提交了不正确的身份验证信息，自动重新连接可能会失败，这可能发生在攻击期间，或者服务器确定自检测到断开连接以来已过去太长时间。

## ICA 保持活动

启用 ICA 保持活动功能可防止断开的连接被终止。启用后，如果服务器检测到没有活动，此功能可防止远程桌面服务断开该会话。没有活动的示例包括没有时钟变化、没有鼠标移动、没有屏幕更新。服务器每隔几秒发送一次保持活动数据包，以检测会话是否处于活动状态。如果会话不再处于活动状态，服务器会将该会话标记为已断开连接。

> **重要提示：**
>
> ICA 保持活动仅在您不使用会话可靠性时才有效。会话可靠性有其自己的机制来防止断开的连接被终止。仅为不使用会话可靠性的连接配置 ICA 保持活动。

> ICA 保持活动设置会覆盖在 Windows 组策略中配置的保持活动设置。

使用以下策略设置启用和配置 ICA 保持活动：

- **ICA 保持活动超时：** 指定用于发送 ICA 保持活动消息的时间间隔（1-3600 秒）。如果您希望网络监控软件在断开连接不频繁的环境中关闭非活动连接，并且允许用户重新连接到会话不是问题，请勿配置此选项。

  默认间隔为 60 秒：ICA 保持活动数据包每 60 秒发送到用户设备。如果用户设备在 60 秒内没有响应，ICA 会话的状态将变为已断开连接。
- **ICA 保持活动：** 发送或阻止发送 ICA 保持活动消息。

## 工作区控制

工作区控制允许桌面和应用程序随用户从一个设备移动到另一个设备。这种漫游能力使用户只需登录即可从任何地方访问所有桌面或打开的应用程序，而无需在每个设备上重新启动桌面或应用程序。例如，工作区控制可以帮助医院中的医护人员，他们需要在不同工作站之间快速移动，并在每次登录时访问同一组应用程序。如果您配置工作区控制选项以允许此操作，这些工作人员可以从一个客户端设备断开多个应用程序，然后重新连接以在不同的客户端设备上打开相同的应用程序。

工作区控制影响以下活动：

- **登录：** 默认情况下，工作区控制允许用户在登录时自动重新连接到所有正在运行的桌面和应用程序，从而无需手动重新打开它们。通过工作区控制，用户可以打开已断开连接的桌面或应用程序，以及在另一个客户端设备上处于活动状态的任何桌面或应用程序。从桌面或应用程序断开连接会使其在服务器上继续运行。如果您有漫游用户，他们必须在一个客户端设备上保持某些桌面或应用程序运行，同时在另一个客户端设备上重新连接到其桌面或应用程序的子集，您可以配置登录重新连接行为，使其仅打开用户之前断开连接的桌面或应用程序。
- **重新连接：** 登录到服务器后，用户可以随时通过单击“重新连接”来重新连接到其所有桌面或应用程序。默认情况下，“重新连接”会打开已断开连接的桌面或应用程序，以及当前在另一个客户端设备上运行的任何桌面或应用程序。您可以配置“重新连接”以仅打开用户之前断开连接的那些桌面或应用程序。
- **注销：** 对于通过 StoreFront™ 打开桌面或应用程序的用户，您可以配置“**注销**”命令，以将用户从 StoreFront 和所有活动会话中注销，或者仅从 StoreFront 中注销。
- **断开连接：** 用户可以一次性断开所有正在运行的桌面和应用程序的连接，而无需单独断开每个连接。

工作区控制仅适用于通过 Citrix StoreFront 连接访问桌面和应用程序的 Citrix Workspace 应用程序用户。默认情况下，虚拟桌面会话的工作区控制处于禁用状态，但对托管应用程序启用。已发布的桌面与这些桌面中运行的任何已发布的应用程序之间默认不发生会话共享。

当用户移动到新的客户端设备时，用户策略、客户端驱动器映射和打印机配置会相应地更改。策略和映射根据用户登录会话的客户端设备应用。例如，医护人员从急诊室的设备注销，然后登录到 X 射线实验室的工作站。适用于 X 射线实验室会话的策略、打印机映射和客户端驱动器映射会在会话启动时生效。

您可以自定义用户更改位置时向其显示的打印机。您还可以控制用户是否可以打印到本地打印机、用户远程连接时消耗的带宽量以及其打印体验的其他方面。

有关为用户启用和配置工作区控制的信息，请参阅 StoreFront 文档。

## 会话漫游

默认情况下，会话会随用户在客户端设备之间漫游。当用户启动会话然后移动到另一台设备时，将使用相同的会话，并且应用程序在两台设备上都可用。无论设备如何或是否存在当前会话，应用程序都会随之移动。通常，分配给应用程序的打印机和其他资源也会随之移动。

虽然此默认行为提供了许多优点，但在所有情况下可能并不理想。您可以使用 PowerShell SDK 阻止会话漫游。

示例 1：一名医务人员正在使用两台设备，在一台台式电脑上填写保险表格，并在平板电脑上查看患者信息。

- 如果启用了会话漫游，两个应用程序都会显示在两台设备上（在一台设备上启动的应用程序在所有正在使用的设备上都可见）。这可能不符合安全要求。
- 如果禁用了会话漫游，患者记录不会显示在台式电脑上，并且保险表格不会显示在平板电脑上。

示例 2：一位生产经理在他的办公室电脑上启动了一个应用程序。设备名称和位置决定了该会话可用的打印机和其他资源。当天晚些时候，他去隔壁大楼的办公室开会，会议需要使用打印机。

- 当启用会话漫游时，生产经理可能无法访问会议室附近的打印机，因为他之前在办公室启动的应用程序导致分配了该位置附近的打印机和其他资源。
- 当禁用会话漫游时，当他登录到另一台机器（使用相同的凭据）时，会启动一个新会话，并且附近的打印机和资源将可用。

### 配置会话漫游

要配置会话漫游，请使用以下授权策略规则 cmdlet 和“SessionReconnection”属性。可选地，您还可以指定“LeasingBehavior”属性。

对于桌面会话：

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

对于应用程序会话：

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

其中 `value` 可以是以下之一：

- **始终：** 会话始终漫游，无论客户端设备以及会话是连接还是断开。这是默认值。
- **仅断开连接：** 仅重新连接到已断开连接的会话；否则，启动新会话。（会话可以通过先断开连接，或使用 Workspace Control 显式漫游，在客户端设备之间漫游。）永远不会使用来自其他客户端设备的活动连接会话。而是启动一个新会话。
- **仅限相同端点：** 用户为其使用的每个客户端设备获取一个唯一的会话。这会完全禁用漫游。用户只能重新连接到会话中以前使用过的同一设备。

下面介绍了“LeasingBehavior”属性。

**其他设置的影响：**

禁用会话漫游受交付组中应用程序属性中的应用程序限制**每个用户只允许一个应用程序实例**的影响。

- 如果禁用会话漫游，则禁用“只允许一个实例...”应用程序限制。
- 如果启用“只允许一个实例...”应用程序限制，则不要配置允许在新设备上创建新会话的两个值中的任何一个。

### 登录间隔

如果包含桌面 VDA 的虚拟机在登录过程完成之前关闭，您可以为该过程分配更多时间。7.6 及更高版本的默认值为 180 秒（7.0-7.5 版本的默认值为 90 秒）。

在计算机上（或在计算机目录中使用的主映像上），设置以下注册表项：

项：`HKLM\SOFTWARE\Citrix\PortICA`

- 值: `AutoLogonTimeout`
- 类型: `DWORD`
- 指定一个十进制时间（以秒为单位），范围为 0-3600。

如果您更改了主映像，请更新目录。

此设置仅适用于具有桌面 VDA 的虚拟机。Microsoft 控制具有服务器 VDA 的计算机上的登录超时。

## 在 Studio 中使用搜索

使用搜索功能查看有关特定计算机、会话、计算机目录、应用程序或交付组的信息。

1. 在 Studio 导航窗格中选择**搜索**。

   您不能使用搜索框在计算机目录或交付组选项卡中进行搜索。请使用导航窗格中的“搜索”节点。

   要在显示中显示其他搜索条件，请单击“搜索”下拉字段旁边的加号。通过单击减号按钮删除搜索条件。
2. 输入名称或使用下拉列表选择其他搜索选项以查找所需项目。
3. （可选）通过选择**另存为**来保存搜索。该搜索将显示在**已保存的搜索**列表中。

或者，单击**展开搜索**图标（双向下尖括号）以显示搜索属性菜单。您可以通过从菜单中的属性构建表达式来执行高级搜索。

增强搜索的技巧：

- 要显示可在其中搜索和排序的显示中包含的其他特征，请右键单击任意列并选择**选择列**。
- 要查找连接到计算机的用户设备，请使用“**客户端 (IP)**”和“**是**”，然后输入设备 IP 地址。
- 要查找活动会话，请使用“**会话状态**”、“**是**”和“**已连接**”。
- 要列出交付组中的所有计算机，请在导航窗格中选择**交付组**，然后选择该组，然后在“操作”窗格中选择**查看计算机**。

# 标签

## 简介

标签是用于标识项目（例如计算机、应用程序、桌面、交付组、应用程序组和策略）的字符串。创建标签并将其添加到项目后，您可以自定义某些操作，使其仅应用于具有指定标签的项目。

- 在 Studio 中定制搜索显示。

  例如，要仅显示已针对测试人员优化的应用程序，请创建一个名为“test”的标记，然后将其添加（应用）到这些应用程序。现在，您可以使用“test”标记筛选 Studio 搜索。

- 从应用程序组发布应用程序或从交付组发布特定桌面时，仅考虑所选交付组中的一部分计算机。这称为*标签限制*。

  通过标签限制，您可以将现有计算机用于多个发布任务，从而节省部署和管理更多计算机的成本。标签限制可以看作是对交付组中的计算机进行细分（或分区）。其功能与 XenApp 7.x 之前的版本中的辅助角色组类似，但并不完全相同。

  使用带有标签限制的应用程序组或桌面有助于隔离和排查交付组中一部分计算机的问题。

- 为交付组中的一部分计算机安排定期重新启动。

  对计算机使用标签限制可让您使用新的 PowerShell cmdlet 为交付组中的一部分计算机配置多个重新启动计划。有关示例和详细信息，请参阅 管理交付组。

- 定制 Citrix® 策略在具有（或不具有）指定标记的交付组、交付组类型或 OU 中的部分计算机上的应用（分配）。

  例如，如果您只想将 Citrix 策略应用于功能更强大的工作站，请为这些计算机添加一个名为“high power”的标记。然后，在“创建策略”向导的**分配策略**页面上，选择该标记和**启用**复选框。您还可以向交付组添加标记，然后将 Citrix 策略应用于该组。有关详细信息，请参阅创建策略。

您可以将标签应用于：

- 计算机

- 应用程序
- 计算机目录（仅限 PowerShell；请参阅 计算机目录上的标签）
- 交付组
- 应用程序组

在 Studio 中创建或编辑以下内容时，可以配置标记限制：

- 共享交付组中的桌面
- 应用程序组

> **重要提示：**
>
> 标签可以显式应用于计算机，也可以显式应用于计算机目录或交付组级别。当标签应用于计算机目录或交付组级别时，该目录或交付组中的所有计算机都会隐式继承该标签。这些继承的标签无法在计算机级别删除。要移除标签效果，必须从计算机目录或交付组级别移除该标签。

## 桌面或应用程序组的标签限制

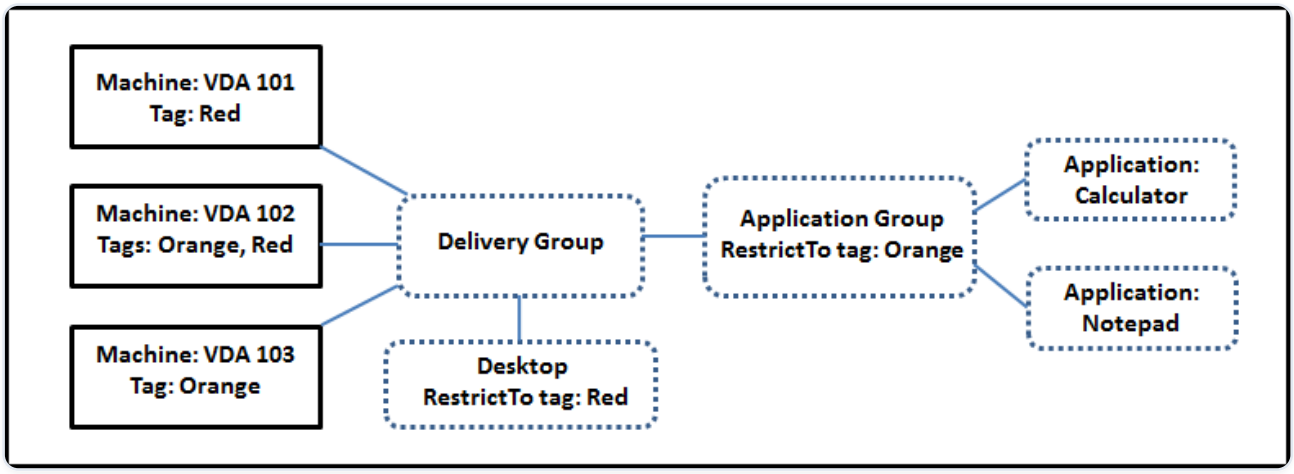
标签限制涉及以下几个步骤：

- 创建标签，然后将其添加（应用）到计算机。
- 创建或编辑具有标签限制的组（换句话说，“将启动限制为具有标签 x 的计算机”）。

标签限制扩展了代理的计算机选择过程。代理从关联的交付组中选择一台计算机，选择过程受访问策略、配置的用户列表、区域首选项和启动就绪状态以及标签限制（如果存在）的约束。对于应用程序，代理会按优先级顺序回退到其他交付组，并对每个考虑的交付组应用相同的计算机选择规则。

### 示例 1：简单布局

本示例介绍了一种简单布局，该布局使用标签限制来限制哪些计算机可用于某些桌面和应用程序启动。该站点有一个共享交付组、一个已发布的桌面和一个配置了两个应用程序的应用程序组。



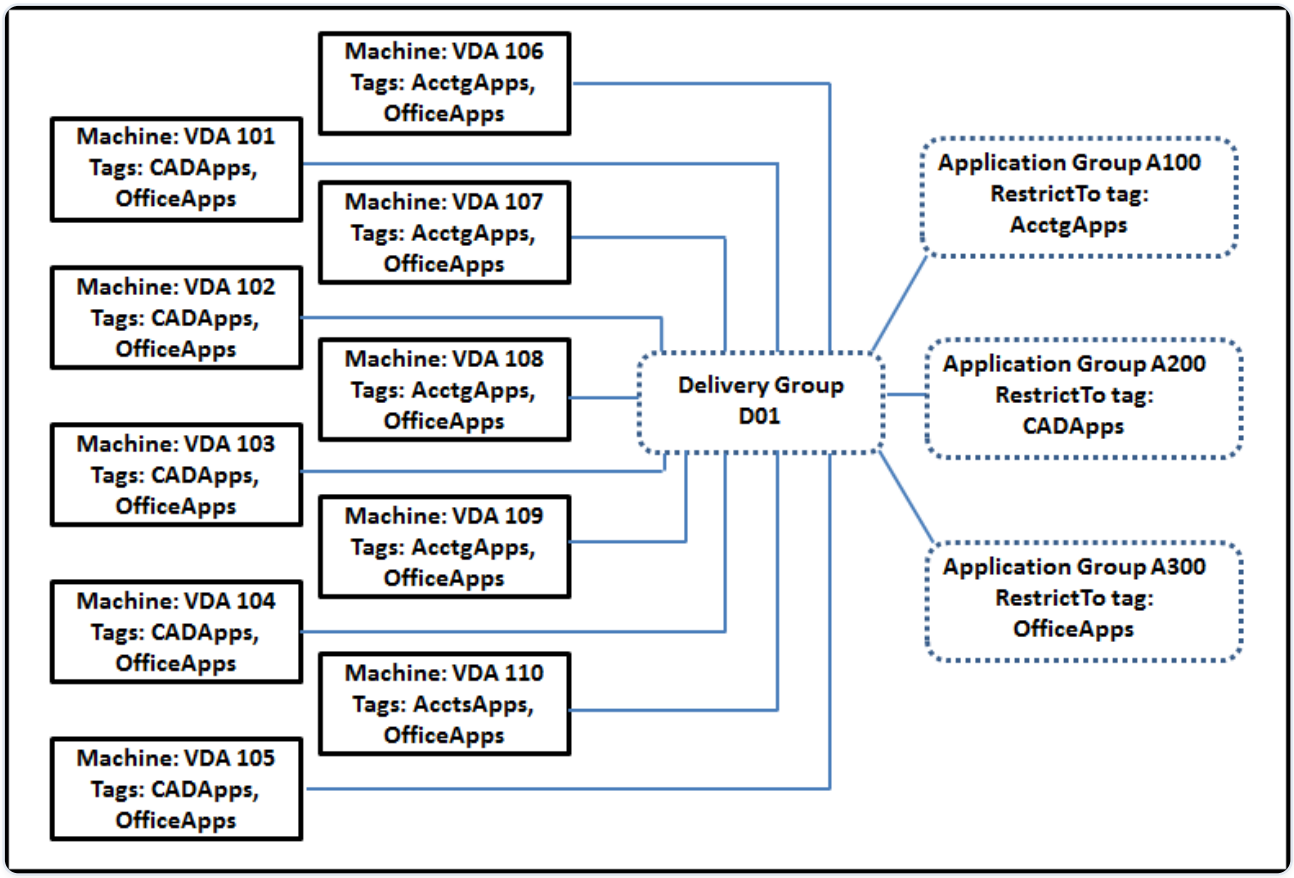

- 已将标签添加到三台计算机（VDA 101-103）中的每台计算机。
- 共享交付组中的桌面是使用名为“Red”的标签限制创建的。桌面只能在该交付组中具有“Red”标签的计算机上启动：VDA 101 和 102。
- 应用程序组是使用“Orange”标签限制创建的，因此其每个应用程序（计算器和记事本）只能在该交付组中具有“Orange”标签的计算机上启动：VDA 102 和 103。

计算机 VDA 102 具有两个标签（Red 和 Orange），因此可以考虑用于启动应用程序和桌面。

### 示例 2：更复杂的布局

本示例包含多个使用标签限制创建的应用程序组。这样，与仅使用交付组相比，可以使用更少的计算机交付更多的应用程序。

如何配置示例 2 显示了在此示例中用于创建和应用标签，然后配置标签限制的步骤。




此示例使用 10 台计算机 (VDA 101-110)、一个交付组 (D01) 和三个应用程序组 (A100、A200、A300)。通过为每台计算机应用标记，然后在创建每个应用程序组时指定标记限制：

- 组中的会计用户可以在五台计算机 (VDA 101–105) 上访问他们所需的应用程序
- 组中的 CAD 设计人员可以在五台计算机 (VDA 106-110) 上访问他们所需的应用程序
- 组中需要 Office 应用程序的用户可以在 10 台计算机 (VDA 101-110) 上访问 Office 应用程序

仅使用 10 台计算机，且只有一个交付组。如果仅使用交付组（不使用应用程序组），则需要两倍的计算机，因为一台计算机只能属于一个交付组。

## 管理标签和标签限制

通过 Studio 中的**管理标记**操作，可以对选定项目创建、添加（应用）、编辑和删除标记。

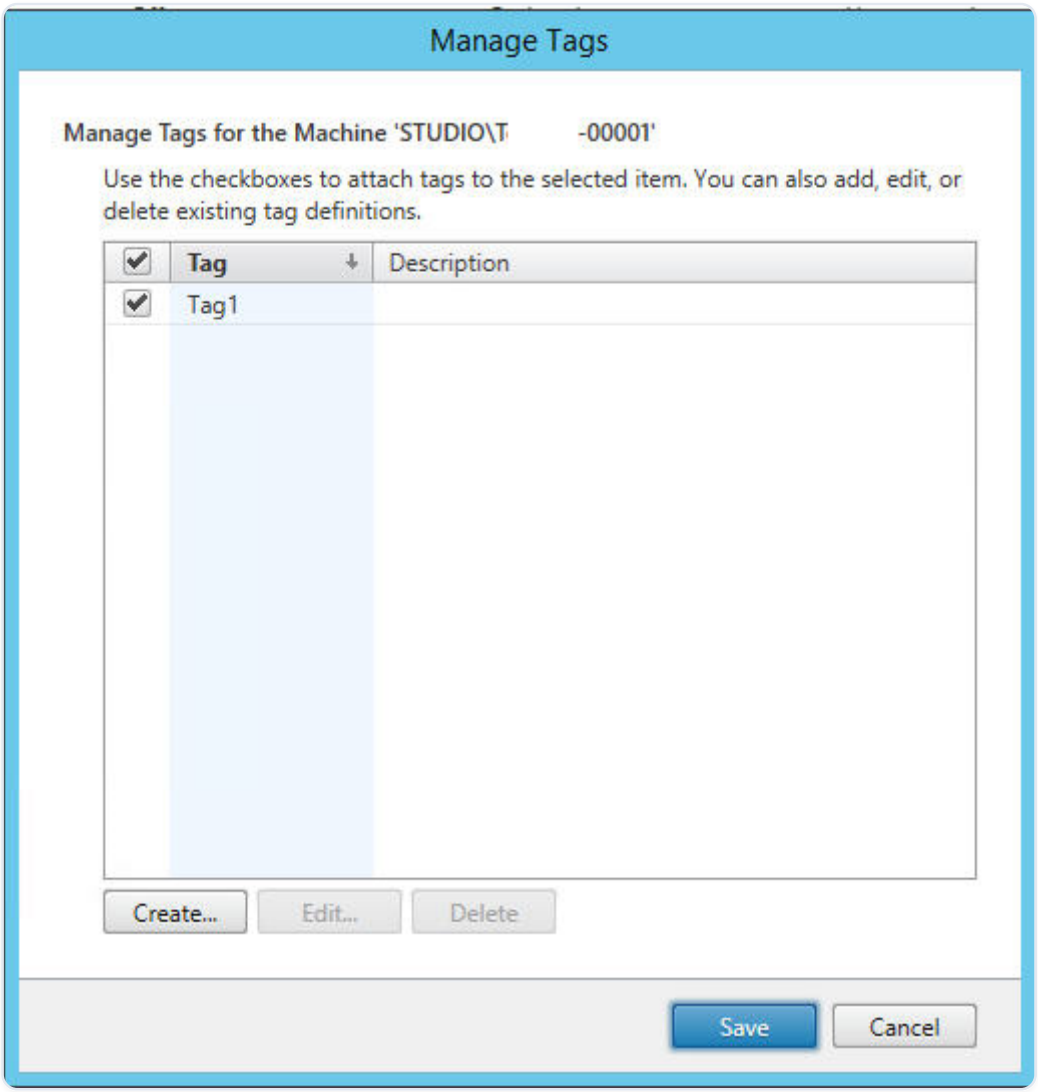
（例外：用于策略分配的标记通过 Studio 中的**管理标记**操作创建、编辑和删除。但是，标记是在创建策略时应用（分配）的。有关详细信息，请参阅创建策略。）

在交付组中创建或编辑桌面以及创建和编辑应用程序组时，将配置标签限制。

### 在 Studio 中使用“管理标记”对话框

在 Studio 中，选择要应用标记的项目（一台或多台计算机、应用程序、桌面、交付组或应用程序组），然后在“操作”窗格中选择**管理标记**。该对话框列出了站点中已创建的所有标记，而不仅仅是您选择的项目的标记。

- 包含复选标记的复选框表示该标签已添加到所选项目。（在下面的屏幕截图中，所选计算机已应用名为“Tag1”的标签。）
- 如果您选择了多个项目，则包含连字符的复选框表示部分（但并非所有）选定项目已添加该标签。




以下操作可从**管理标签**对话框中获取。请务必查看使用标签时的注意事项。

- **创建标签：**

  点击“**创建**”。输入名称和描述。标签名称必须唯一且不区分大小写。然后点击“**确定**”。（创建标签不会自动将其应用于您选择的任何项目。使用复选框应用标签。）

- **添加（应用）一个或多个标签：**

选中标签名称旁边的复选框。如果您选择了多个项目，并且标签旁边的复选框包含连字符（表示部分而非全部选定项目已应用该标签），则将其更改为复选标记会影响所有选定的计算机。

如果您尝试将标签添加到一个或多个计算机，并且该标签在应用程序组中用作限制，则会收到警告，指出此操作可能导致这些计算机可用于启动。如果这是您的意图，请继续。

- **删除一个或多个标签：**

  清除标签名称旁边的复选框。如果您选择了多个项目，并且标签旁边的复选框包含连字符（表示部分而非全部选定项目已应用该标签），则清除该复选框会从所有选定的计算机中删除该标签。

  如果您尝试从将某个标签用作限制的计算机中删除该标签，则会收到警告，指出此操作可能会影响哪些计算机被考虑用于启动。如果这是您的意图，请继续。

- **编辑标签：**

  选择一个标签，然后点击“**编辑**”。输入新名称、新描述或两者。您一次只能编辑一个标签。

- **删除一个或多个标签：**

  选择标签，然后点击“**删除**”。“删除标签”对话框会显示当前有多少项目正在使用所选标签（例如“2 台计算机”）。点击一个项目以显示更多信息。例如，点击“2 台计算机”项目会显示已应用该标签的两台计算机的名称。确认是否要删除这些标签。

  您不能使用 Studio 删除用作限制的标记。首先，编辑应用程序组并删除标记限制或选择其他标记。

在“管理标记”对话框中完成后，单击**保存**。

要查看计算机是否应用了任何标记：在导航窗格中选择**交付组**。在中间窗格中选择一个交付组，然后在“操作”窗格中选择**查看计算机**。在中间窗格中选择一台计算机，然后在**详细信息**窗格中选择**标记**选项卡。

### 管理标签限制

配置标签限制是一个多步骤过程：首先创建标签并将其添加/应用到计算机。然后，将限制添加到应用程序组或桌面。

- **创建并应用标签：**

  创建标签，然后使用前面描述的“**管理标签**”操作将其添加（应用）到受标签限制影响的计算机。

- **将标签限制添加到应用程序组：**

  创建或编辑应用程序组。在“**交付组**”页面上，选择“**将启动限制到具有该标签的计算机**”，然后从列表中选择该标签。

- **更改或删除应用程序组上的标签限制：**

  编辑组。在“**交付组**”页面上，可以从列表中选择其他标签，也可以通过清除“**将启动限制到具有该标签的计算机**”来完全删除标签限制。

- **将标签限制添加到桌面：**

  创建或编辑交付组。在“**桌面**”页面上，单击“**添加**”或“**编辑**”。在“添加桌面”对话框中，选择“**将启动限制到具有该标签的计算机**”，然后从菜单中选择该标签。

- **更改或删除交付组上的标签限制：**

  编辑组。在“桌面”页面上，单击“**编辑**”。在对话框中，可以从列表中选择其他标签，也可以通过清除“**将启动限制到具有该标签的计算机**”来完全删除标签限制。

### 使用标签时的注意事项

应用于项目的标记可用于不同的目的，因此请记住，添加、删除和移除标记可能会产生意外影响。您可以使用标记在 Studio 搜索字段中对计算机显示进行排序。在配置应用程序组或桌面时，可以将同一标记用作限制。该标记将启动考虑范围限制为仅包含具有该标记的指定交付组中的计算机。

当您尝试将标签添加到计算机，而该标签已配置为桌面或应用程序组的标签限制时，将显示警告。添加该标签可能会使计算机可用于启动其他应用程序或桌面。如果这是您的预期，请继续。如果不是，您可以取消操作。

例如，假设您创建了一个具有“Red”标签限制的应用程序组。稍后，您在该应用程序组使用的相同交付组中添加了其他几台计算机。如果您随后尝试将“Red”标签添加到这些计算机，Studio 会显示一条类似以下内容的警告消息：“标签‘Red’用作以下应用程序组的限制。添加此标签可能会使选定的计算机能够在此应用程序组中启动应用程序。”然后，您可以确认或取消将该标签添加到这些额外的计算机。

同样，如果应用程序组使用标签来限制启动，Studio 会警告您，在您编辑该组以将其作为限制删除之前，无法删除该标签。（如果允许您删除用作应用程序组中限制的标签，则可能导致允许应用程序在与该应用程序组关联的交付组中的所有计算机上启动。）如果标签用作桌面启动的限制，则同样禁止删除该标签。在您编辑交付组中的应用程序组或桌面以删除该标签限制后，即可删除该标签。

并非所有计算机都可能具有相同的应用程序集。一个用户可以属于多个应用程序组，每个组都有不同的标签限制以及来自交付组的不同或重叠的计算机集。下表列出了如何确定计算机注意事项。

| 当应用程序已添加到 | 所选交付组中的这些计算机被视为可用于启动 |
| --- | --- |
| 一个没有标签限制的应用程序组 | 任何计算机。 |

| 当应用程序已添加到 | 所选交付组中的这些计算机被视为可用于启动 |
| --- | --- |
| 一个具有标签限制 A 的应用程序组 | 已应用标签 A 的计算机。 |
| 两个应用程序组，一个具有标签限制 A，另一个具有标签限制 B | 具有标签 A 和标签 B 的计算机。如果没有可用，则为具有标签 A 或标签 B 的计算机。 |
| 两个应用程序组，一个具有标签限制 A，另一个没有标签限制 | 具有标签 A 的计算机。如果没有可用，则为任何计算机。 |

如果您在计算机重新启动计划中使用了标签限制，则您所做的任何影响标签应用或限制的更改都会影响下一个计算机重新启动周期。它不会影响更改进行中正在进行的任何重新启动周期。

### 如何配置示例 2

以下序列展示了创建和应用标签，然后为第二个示例中所示的应用程序组配置标签限制的步骤。

VDA 和应用程序已安装在计算机上，并且已创建交付组。

创建标签并将其应用于计算机：

1. 在 Studio 中，选择交付组 D01，然后在“操作”窗格中选择 **View Machines**（查看计算机）。
2. 选择计算机 VDA 101-105，然后在“操作”窗格中选择 **Manage Tags**（管理标签）。
3. 在“管理标签”对话框中，单击 **Create**，然后创建名为 `CADApps` 的标签。单击 **OK**。
4. 再次单击 **Create**，然后创建名为 OfficeApps 的标签。单击 **OK**。
5. 在 **Manage Tags** 对话框中，通过启用每个标签名称（`CADApps` 和 `OfficeApps`）旁边的复选框，将新创建的标签添加（应用）到选定的计算机。完成后，关闭对话框。
6. 选择交付组 D01，在“操作”窗格中选择 **View Machines**（查看计算机）。
7. 选择计算机 VDA 106-110，然后在“操作”窗格中选择 **Manage Tags**（管理标签）。
8. 在 **Manage Tags** 对话框中，单击 **Create**。创建名为 `AcctgApps` 的标签。单击 **OK**。
9. 通过单击每个标签名称旁边的复选框，将新创建的 `AcctgApps` 标签和 `OfficeApps` 标签应用于选定的计算机，然后关闭对话框。

创建具有标签限制的应用程序组。

1. 在 Studio 中，在导航窗格中选择 **Applications**（应用程序），然后在“操作”窗格中选择 **Create Application Group**（创建应用程序组）。此时将启动“创建应用程序组”向导。
2. 在向导的 **Delivery Groups** 页面上，选择交付组 D01。选择 **Restrict launches to machines with tag**，然后从列表中选择 `AcctgApps` 标签。

3. 完成向导，指定会计用户和会计应用程序。（添加应用程序时，选择**从“开始”菜单**源，该源会在具有 `AcctgApps` 标记的计算机上搜索应用程序。）在**摘要**页面上，将组命名为 `A100`。
4. 重复上述步骤以创建应用程序组 `A200`，指定具有 `CADApps` 标记的计算机以及相应的用户和应用程序。
5. 重复步骤以创建应用程序组 `A300`，指定具有 `OfficeApps` 标记的计算机以及相应的用户和应用程序。

### 计算机目录上的标记

您可以在计算机目录上使用标签。创建标签然后将其应用于目录的总体顺序与前面所述相同。但是，将标签应用于目录仅通过 PowerShell 界面支持。您不能使用 Studio 将标签应用于目录或从目录中删除标签。Studio 中的目录显示不指示是否应用了标签。

摘要：您可以使用 Studio 或 PowerShell 创建或删除用于目录的标签。使用 PowerShell 将标签应用于目录。

以下是一些将标记与目录结合使用的示例：

- 交付组包含来自多个目录的计算机，但您希望某个操作（例如重新启动计划）仅影响特定目录中的计算机。将标记应用于该目录即可实现此目的。
- 在应用程序组中，您希望将应用程序会话限制为特定目录中的计算机。将标记应用于该目录即可实现此目的。

受影响的 PowerShell cmdlet：

- 您可以将目录对象传递给 `Add-BrokerTag` 和 `Remove-BrokerTag` 等 cmdlet。
- `Get-BrokerTagUsage` 显示有多少个目录包含标记。
- `Get-BrokerCatalog` 具有一个名为 `Tags` 的属性。

例如，以下 cmdlet 将名为 `fy2018` 的标签添加到名为 `acctg` 的目录中：`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`。（该标签之前已使用 Studio 或 PowerShell 创建。）

有关更多指导和语法，请参阅 PowerShell cmdlet 帮助。

## 更多信息

博客文章：如何将桌面分配给特定服务器。

# IPv4/IPv6 支持

此版本支持纯 IPv4、纯 IPv6 以及使用重叠 IPv4 和 IPv6 网络的双栈部署。

以下组件仅支持 IPv4。所有其他组件均支持 IPv4 和 IPv6。

- Citrix 置备™
- 思杰虚拟机监控程序™
- 不受**仅使用 IPv6 控制器注册**策略设置控制的虚拟投递代理 (VDA)

IPv6 通信通过两个与 VDA 连接相关的 Citrix® 策略设置进行控制。

- **强制使用 IPv6 的主要设置：**仅使用 IPv6 控制器注册。

  此策略设置控制 VDA 用于向 Delivery Controller 注册的地址形式。

  启用后，VDA 将使用按以下优先级选择的单个 IPv6 地址向 Controller 注册并与之通信：全局 IP 地址、唯一本地地址 (ULA)、链路本地地址（仅当没有其他 IPv6 地址可用时）。

  禁用后，VDA 将使用计算机的 IPv4 地址向 Controller 注册并与之通信。这是默认值。

  如果团队频繁使用 IPv6 网络，请根据已启用**仅使用 IPv6 控制器注册**策略设置的映像或组织单位 (OU) 为这些用户发布桌面和应用程序。

  如果团队频繁使用 IPv4 网络，请根据已禁用**仅使用 IPv6 控制器注册**策略设置的映像或 OU 为这些用户发布桌面和应用程序。

- **定义 IPv6 网络掩码的从属设置：**控制器注册 IPv6 网络掩码。

  一台计算机可以有多个 IPv6 地址。此策略设置允许管理员将 VDA 限制为仅使用首选子网（如果已注册），而不是全局 IP。此设置指定 VDA 注册的网络。VDA 仅注册与指定网络掩码匹配的第一个地址。

  此设置仅在启用**仅使用 IPv6 控制器注册策略**设置时有效。默认值 = 空字符串

## 部署注意事项

如果您的环境同时包含 IPv4 和 IPv6 网络，请为仅限 IPv4 的客户端以及可以访问 IPv6 网络的客户端创建单独的交付组配置。考虑使用命名、手动 Active Directory 组分配或 SmartAccess 筛选器来区分用户。

如果连接在 IPv6 网络上启动，然后您尝试从仅具有 IPv4 访问权限的客户端再次连接，则会话重新连接可能会失败。

# 用户配置文件

默认情况下，在安装 Virtual Delivery Agent 时，Citrix Profile Management 会在主映像上静默安装，但您不必将 Profile Management 用作配置文件解决方案。

为了满足用户不同的需求，您可以使用 Citrix Virtual Apps and Desktops™ 策略将不同的配置文件行为应用于每个交付组中的计算机。例如，一个交付组可能需要 Citrix 强制配置文件（其模板存储在一个网络位置），而另一个交付组可能需要存储在另一个位置并包含多个重定向文件夹的 Citrix 漫游配置文件。

- 如果组织中的其他管理员负责 Citrix Virtual Apps and Desktops 策略，请与他们合作，确保他们在您的 Delivery Groups 中设置任何与配置文件相关的策略。
- Profile Management 策略还可以在组策略、Profile Management .ini 文件中以及在各个虚拟机本地进行设置。定义配置文件行为的这些多种方式按以下顺序读取：

  a. 组策略（.adm 或 .admx 文件）

  b. 策略节点中的 Citrix Virtual Apps and Desktops 策略

  c. 用户连接到的虚拟机上的本地策略

  d. 配置文件管理 .ini 文件

  例如，如果您在组策略和策略节点中配置相同的策略，系统将读取组策略中的策略设置并忽略 Citrix Virtual Apps and Desktops 策略设置。

无论您选择哪种配置文件解决方案，Director 管理员都可以访问诊断信息并对用户配置文件进行故障排除。有关详细信息，请参阅 Director 文档。

## 自动配置

桌面类型会根据 Virtual Delivery Agent 安装自动检测，并且除了您在 Studio 中所做的配置选择之外，还会相应地设置 Profile Management 默认值。

Profile Management 调整的策略显示在下表中。任何非默认策略设置都将保留，并且不会被此功能覆盖。有关每个策略的信息，请查阅 Profile Management 文档。创建配置文件的计算机类型会影响调整的策略。主要因素是计算机是持久的还是预配的，以及它们是多用户共享还是专用于单个用户。

持久系统具有某种类型的本地存储，其内容在系统关闭时预计会持久存在。持久系统可能会采用 SAN 等存储技术来模拟本地磁盘。相比之下，预配系统是“即时”从基本磁盘和某种身份磁盘创建的。本地存储通常由 RAM 磁盘或网络磁盘模拟，后者通常由具有高速链路的 SAN 提供。预配技术

通常是 Citrix Provisioning 或 Machine Creation Services™（或第三方等效产品）。有时，预配系统具有持久本地存储。这些系统被归类为持久系统。

这两个因素共同定义了以下计算机类型：

- **持久和专用** -- 示例包括使用 Machine Creation Services 创建的具有静态分配和持久本地存储的单会话操作系统计算机、使用 VDI-in-a-Box 创建的具有持久存储的桌面、物理工作站和笔记本电脑
- **持久和共享** -- 示例包括使用 Machine Creation Services 创建的多会话操作系统计算机
- **预配和专用** -- 示例包括使用 Citrix Provisioning™ 创建的具有静态分配但没有持久存储的单会话操作系统计算机
- **预配和共享** -- 示例包括使用 Citrix Provisioning 创建的具有随机分配的单会话操作系统计算机，以及使用 VDI-in-a-Box 创建的没有持久存储的桌面

以下配置文件管理策略设置是针对不同计算机类型的建议准则。它们在大多数情况下都适用，但您可能需要根据部署要求进行调整。

> **重要提示：**
>
> **注销时删除本地缓存的配置文件**、**配置文件流技术**和**始终缓存**由自动配置功能强制执行。请手动调整其他策略。

### 持久性计算机

| 策略 | 持久且专用 | 持久且共享 |
| --- | --- | --- |
| 在注销时删除本地缓存的配置文件 | 已禁用 | 启用 |
| 配置文件流技术 | 已禁用 | 启用 |
| 始终缓存 | 已启用（注 1） | 已禁用（注 2） |
| 活动回写 | 已禁用 | 已禁用（注 3） |
| 处理本地管理员的登录 | 启用 | 已禁用（注 4） |

### 预配的计算机

| 策略 | 预配和专用 | 预配和共享 |
| --- | --- | --- |
| 在注销时删除本地缓存的配置文件 | 已禁用（注 5） | 启用 |
| 配置文件流技术 | 启用 | 启用 |
| 始终缓存 | 已禁用（注 6） | 已禁用 |
| 活动回写 | 启用 | 启用 |
| 处理本地管理员的登录 | 启用 | 已启用（注 7） |

1. 由于此计算机类型已禁用**配置文件流**，因此**始终缓存**设置始终被忽略。
2. 禁用**始终缓存**。但是，您可以通过启用此策略并使用它来定义文件大小限制（以 MB 为单位），确保在登录后尽快将大文件加载到配置文件中。任何达到或超过此大小的文件都将尽快在本地缓存。
3. 禁用**活动回写**，除非是为了保存漫游于 Citrix Virtual Apps 服务器之间的用户配置文件中的更改。在这种情况下，请启用此策略。
4. 禁用**处理本地管理员登录**，托管共享桌面除外。在这种情况下，请启用此策略。
5. 禁用**注销时删除本地缓存的配置文件**。此设置会保留本地缓存的配置文件。由于计算机在注销时会重置但会分配给单个用户，因此如果配置文件已缓存，登录速度会更快。
6. 禁用**始终缓存**。但是，您可以通过启用此策略并使用它来定义文件大小限制（以 MB 为单位），确保在登录后尽快将大文件加载到配置文件中。任何达到或超过此大小的文件都将尽快在本地缓存。
7. 启用**处理本地管理员登录**，漫游于 Citrix Virtual Apps and Desktops 服务器之间的用户配置文件除外。在这种情况下，请禁用此策略。

## 文件夹重定向

文件夹重定向允许您将用户数据存储在配置文件存储位置以外的网络共享上。文件夹重定向可减小配置文件大小并缩短加载时间，但可能会影响网络带宽。文件夹重定向不要求使用 Citrix 用户配置文件。您可以选择自行管理用户配置文件，并仍然重定向文件夹。

在 Studio 中使用 Citrix 策略配置文件夹重定向。

- 确保用于存储重定向文件夹内容的网络位置可用并具有正确的权限。将验证位置属性。

- 重定向文件夹在网络上设置，其内容在用户登录时从用户的虚拟桌面填充。

仅使用 Citrix 策略或 Active Directory 组策略对象配置文件夹重定向，不要同时使用两者。同时使用两种策略引擎配置文件夹重定向可能会导致不可预测的行为。

## 高级文件夹重定向

在具有多个操作系统 (OS) 的部署中，您可能希望用户的部分配置文件由每个 OS 共享。配置文件的其余部分不共享，仅由一个 OS 使用。为了确保跨 OS 的一致用户体验，您需要为每个 OS 提供不同的配置，即高级文件夹重定向。例如，在两个 OS 上运行的应用程序的不同版本可能需要读取或编辑共享文件，因此您决定将其重定向到两个版本都可以访问的单个网络位置。或者，由于两个 OS 中 **“开始”菜单** 文件夹的内容结构不同，您决定只重定向一个文件夹，而不是两个。此方法将每个 OS 上的 **“开始”菜单** 文件夹及其内容分开，从而确保用户获得一致的体验。

如果您的部署需要高级文件夹重定向，则必须了解用户配置文件数据的结构，并确定其中哪些部分可以在 OS 之间共享。除非正确使用文件夹重定向，否则可能会导致不可预测的行为。

若要在高级部署中重定向文件夹：

- 为每个 OS 使用单独的交付组。
- 了解您的虚拟应用程序（包括虚拟桌面上的应用程序）存储用户数据和设置的位置，并了解数据的结构。
- 对于可以安全漫游的共享配置文件数据（因为它在每个 OS 中结构相同），请在每个交付组中重定向包含文件夹。
- 对于无法漫游的非共享配置文件数据，请仅在其中一个桌面组中重定向包含文件夹，通常是使用最频繁的 OS 或数据最相关的 OS。或者，对于无法在 OS 之间漫游的非共享数据，请将两个系统上的包含文件夹重定向到单独的网络位置。

### 高级部署示例

该部署包含在 Windows 10 桌面上运行的应用程序（包括 Microsoft Outlook 和 Internet Explorer 的版本）以及由 Windows Server 2019 交付的应用程序（包括 Outlook 和 Internet Explorer 的其他版本）。您已经为这两个 OS 设置了两个交付组。用户希望在这两个应用程序的两个版本中访问相同的 **“联系人”** 和 **“收藏夹”** 集。

**重要提示：** 以下决定和建议适用于所描述的 OS 和部署。在您的组织中，您选择重定向的文件夹以及是否决定共享它们取决于您特定部署的各种独特因素。

- 使用应用于交付组的策略，您可以选择以下文件夹进行重定向。

| 文件夹 | 在 WINDOWS 10 中重定向？ | 在 WINDOWS SERVER 2019 中重定向？ |
|---|---|---|
| 我的文档 | 是 | 是 |
| 应用程序数据 | 否 | 否 |
| 联系人 | 是 | 是 |
| 桌面 | 是 | 否 |
| 下载 | 否 | 否 |
| 收藏夹 | 是 | 是 |
| 链接 | 是 | 否 |
| 我的音乐 | 是 | 是 |
| 我的图片 | 是 | 是 |
| 我的视频 | 是 | 是 |
| 搜索 | 是 | 否 |
| 保存的游戏 | 否 | 否 |
| 开始菜单 | 是 | 否 |

- 对于共享的重定向文件夹：
  - 在分析了不同版本的 Outlook 和 Internet Explorer 保存的数据结构后，您决定可以安全地共享“**联系人**”和“**收藏夹**”文件夹。
  - 您知道“**我的文档**”、“**我的音乐**”、“**我的图片**”和“**我的视频**”文件夹的结构在所有操作系统中都是标准的。因此，可以安全地将这些文件夹存储在每个交付组的相同网络位置。
- 对于非共享的重定向文件夹：
  - 您不会在 Windows Server 交付组中重定向“桌面”、“链接”、“搜索”或“**开始菜单**”文件夹，因为这些文件夹中的数据在两个操作系统中的组织方式不同。因此，无法共享。
  - 为确保此非共享数据的可预测行为，您仅在 Windows 10 交付组中重定向它。用户在日常工作中更频繁地使用 Windows 10。用户仅偶尔访问 Windows Server 交付的应用程序。此外，在这种情况下，非共享数据与桌面环境而非应用程序环境更相关。例如，桌面快捷方式存储

在 **Desktop** 文件夹中，如果它们源自 Windows 10 计算机而不是 Windows Server 计算机，则可能很有用。

- 对于未重定向的文件夹：
  - 您不希望用用户下载的文件使服务器变得混乱，因此选择不重定向“下载”文件夹
  - 来自单个应用程序的数据可能会导致兼容性和性能问题，因此您决定不重定向“应用程序数据”文件夹

有关文件夹重定向的更多信息，请参阅 文件夹重定向、脱机文件和漫游用户配置文件概述。

### 文件夹重定向和排除项

在 Citrix Profile Management 中（但不在 Studio 中），一项性能增强功能允许您使用排除项阻止处理文件夹。如果使用此功能，请勿排除任何重定向的文件夹。文件夹重定向和排除功能协同工作。确保不排除任何重定向的文件夹，可让 Profile Management 将它们移回配置文件文件夹结构中，并在您以后决定不重定向它们时保留数据完整性。有关排除项的更多信息，请参阅 包含和排除项目。

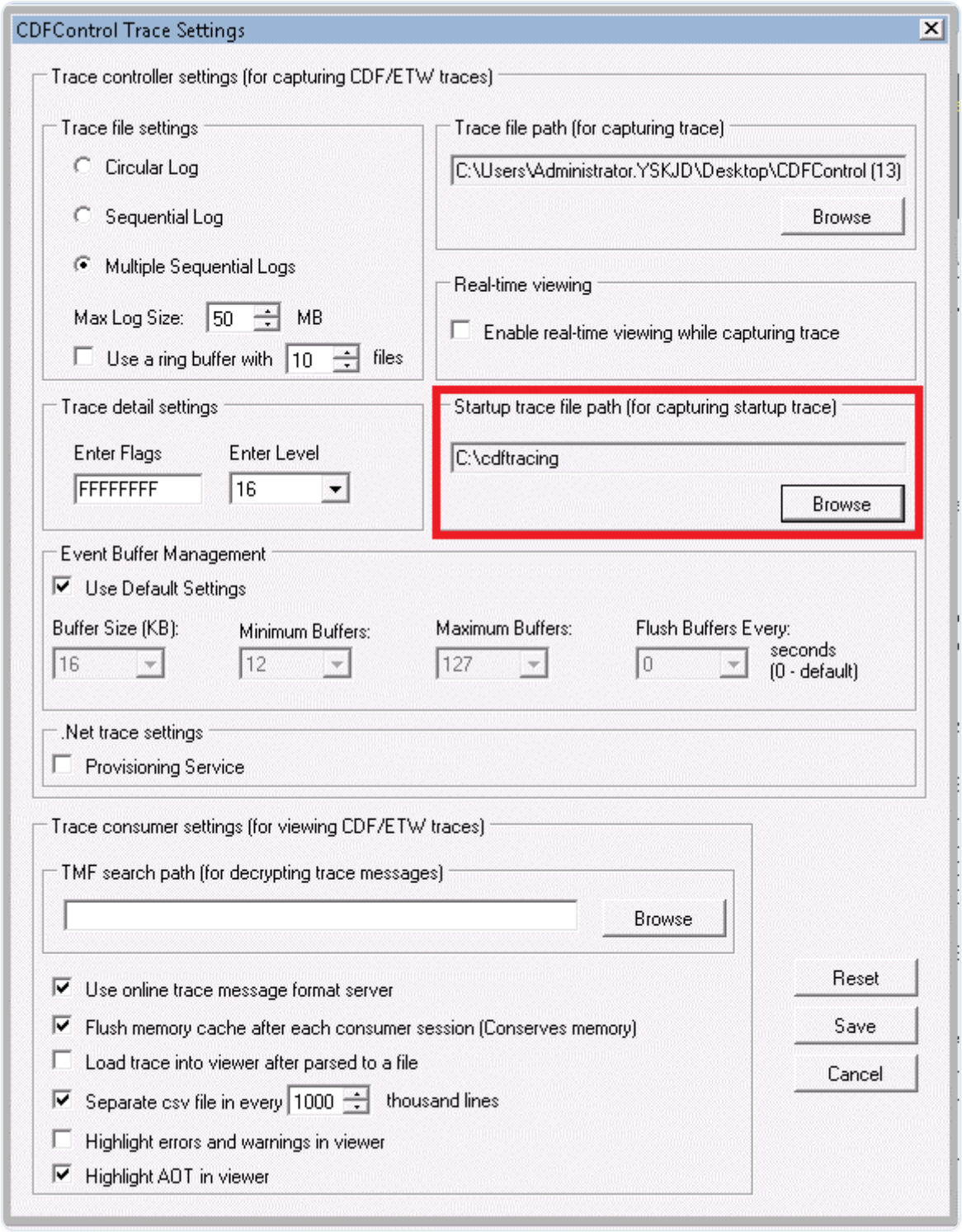
## 在系统启动时收集 Citrix 诊断工具 (CDF) 跟踪

CDFControl 实用程序是一个事件跟踪控制器或使用者，用于捕获来自各种 Citrix 跟踪提供程序的 Citrix 诊断工具 (CDF) 跟踪消息。它旨在解决复杂的 Citrix 相关问题、解析筛选器支持并收集性能数据。要下载 CDFControl 实用程序，请参阅 CTX111961。

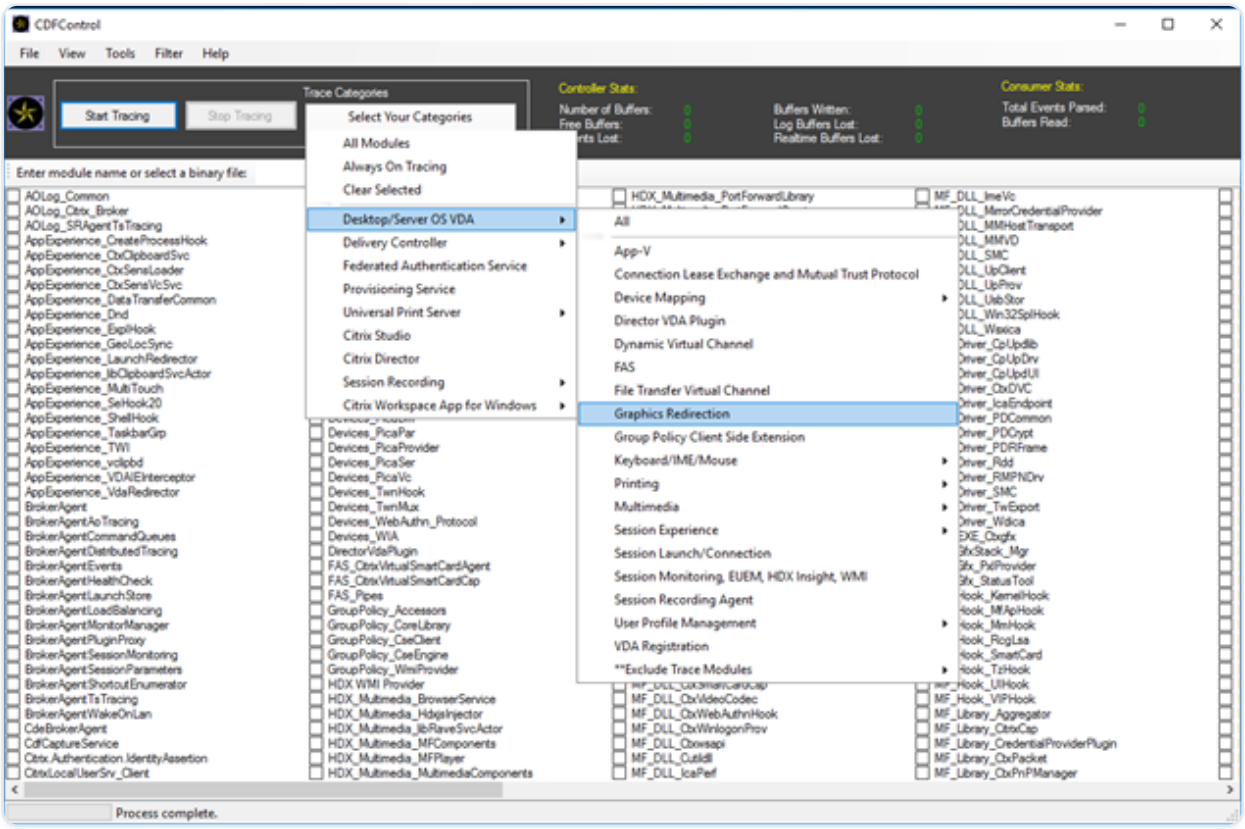
### 在系统启动时收集跟踪

使用以下过程在系统启动时收集 CDF 跟踪。您需要管理员权限。

1. 启动 **CDFControl**，然后从**工具**菜单中选择**选项**。
2. 在**用于捕获启动跟踪的启动跟踪文件路径**部分中指定跟踪文件路径。然后单击**保存**。




3. 选择 Citrix 支持建议的**跟踪类别**。（在以下示例中，选择了**图形重定向**。该选择仅为示例。我们建议您为正在排查的特定问题启用提供程序。）




4. 选择**启动跟踪**，然后从**工具**菜单中选择**启用**。

   选择**启用**后，动画栏开始滚动。此活动不影响过程。继续执行下一步。

5. 启用**启动跟踪**后，关闭 **CDFControl 实用程序**并重新启动系统。
6. 启动 **CDFControl** 实用程序。系统重新启动并出现错误后，通过从**工具**菜单中选择**启动跟踪**并单击**禁用**来禁用启动跟踪。
7. 转到步骤 2 中指定的跟踪文件路径，并收集跟踪日志文件 (.etl) 进行分析。

# Citrix 洞察服务

Citrix Insight Services (CIS) 是一个 Citrix 平台，用于生成仪器数据、遥测数据和业务洞察。其仪器数据和遥测功能使技术用户（客户、合作伙伴和工程师）能够自我诊断和修复问题，并优化其环境。有关 CIS 及其工作原理的详细信息和最新信息，请参阅 `<https://cis.citrix.com>`（需要 Citrix 帐户凭据）。

所有上传到 Citrix 的信息均用于故障排除和诊断目的，以及改进产品的质量、可靠性和性能，但须遵守：

- Citrix Insight Services 策略，请参阅 `<https://cis.citrix.com/legal>`
- Citrix 隐私策略，请参阅 `<https://www.cloud.com/privacy-policy>`

此 Citrix Virtual Apps and Desktops™ 版本支持以下技术。

- Citrix Virtual Apps and Desktops 安装和升级分析
- Citrix 客户体验改善计划 (CEIP)
- Citrix 回传
- Citrix 侦察兵

除了 CIS 和 Citrix Analytics 之外（且独立于它们）：当您安装（或升级）Studio 时，Google Analytics 会自动收集（并随后上传）。安装 Studio 后，您可以使用注册表项 `HKLM\Software\Citrix\DesktopStudio\GAEnabled` 更改此设置。值为 1 启用收集和上传，0 禁用收集和上传。

## 安装和升级分析

当您使用完整产品安装程序部署或升级 Citrix Virtual Apps and Desktops 组件时，有关安装过程的匿名信息会在您安装/升级组件的计算机上收集和存储。此数据用于帮助 Citrix 改进客户的安装体验。

信息本地存储在 `%ProgramData%\Citrix\CTQs` 下。

在完整产品安装程序的图形界面和命令行界面中，此数据的自动上传默认启用。

- 您可以在注册表设置中更改默认值。如果您在安装/升级之前更改注册表设置，则在使用完整产品安装程序时将使用该值。
- 如果您使用命令行界面安装/升级，可以通过在命令中指定一个选项来覆盖默认设置。

**控制自动上传：**

- 控制安装/升级分析数据自动上传的注册表设置（默认值 = 1）：
  - 位置：`HKLM:\Software\Citrix\MetaInstall`
  - 名称：SendExperienceMetrics
  - 值：0 = 禁用，1 = 启用
- 使用 PowerShell，以下 cmdlet 可禁用安装/升级分析数据的自动上传：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
SendExperienceMetrics -PropertyType DWORD -Value 0
```

- 要使用 XenDesktopServerSetup.exe 或 XenDesktopVDASetup.exe 命令禁用自动上传，请包含 `/disableexperiencemetrics` 选项。

要使用 XenDesktopServerSetup.exe 或 XenDesktopVDASetup.exe 命令启用自动上传，请包含 `/sendexperiencemetrics` 选项。

## Citrix 客户体验改善计划

当您参与 Citrix 客户体验改善计划 (CEIP) 时，匿名统计数据和使用信息将发送给 Citrix，以帮助 Citrix 改进 Citrix 产品的质量和性能。有关详细信息，请参阅 https://more.citrix.com/XD-CEIP。

### 在站点创建或升级期间注册

创建站点（安装第一个 Delivery Controller™ 后）时，您将自动注册 CEIP。首次数据上传大约在创建站点七天后进行。您可以在创建站点后的任何时间停止参与。在 Studio 导航窗格（**产品支持**选项卡）中选择**配置**节点，然后按照指导操作。

当您升级 Citrix Virtual Apps and Desktops 部署时：

- 如果您从不支持 CEIP 的版本升级，系统会询问您是否要参与。
- 如果您从支持 CEIP 的版本升级，并且已启用参与，则 CEIP 将在升级后的站点中启用。
- 如果您从支持 CEIP 的版本升级，并且已禁用参与，则 CEIP 在升级后的站点中处于禁用状态。
- 如果您从支持 CEIP 的版本升级，并且参与状态未知，系统会询问您是否要参与。

收集的信息是匿名的，因此上传到 Citrix Insight Services 后无法查看。

### 安装 VDA 时的注册

默认情况下，当您安装 Windows VDA 时，会自动注册 CEIP。您可以在注册表设置中更改此默认值。如果您在安装 VDA 之前更改注册表设置，则会使用该值。

控制 CEIP 自动注册的注册表设置（默认值 = 1）：

位置：`HKLM:\Software\Citrix\Telemetry\CEIP` 名称：Enabled 值：0 = 禁用，1 = 启用

默认情况下，`Enabled` 属性在注册表中是隐藏的。当它未指定时，自动上传功能处于启用状态。

使用 PowerShell，以下 cmdlet 可禁用 CEIP 注册：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled
-PropertyType DWORD -Value 0
```

收集的运行时数据点会定期作为文件写入输出文件夹（默认 %programdata%/Citrix/VdaCeip）。

首次数据上传大约在您安装 VDA 七天后进行。

### 安装其他产品和组件时的注册

您还可以在安装相关 Citrix 产品、组件和技术时参与 CEIP，例如 Citrix Provisioning™、AppDNA、Citrix License Server、适用于 Windows 的 Citrix Workspace™ 应用程序、Universal Print Server 和 Session Recording。有关安装和参与默认值的详细信息，请参阅其文档。

## Citrix 回传

当您在 Citrix Virtual Apps and Desktops 中安装某些组件和功能时，系统会提供参与 Citrix Call Home 的机会。Call Home 会收集诊断数据，然后定期将包含该数据的遥测包直接上传到 Citrix Insight Services（通过默认端口 443 上的 HTTPS），以进行分析和故障排除。

在 Citrix Virtual Apps and Desktops 中，Call Home 作为名为 Citrix Telemetry Service 的后台服务运行。有关详细信息，请参阅 https://more.citrix.com/XD-CALLHOME。

Call Home 调度功能在 Citrix Scout 中也可用。有关详细信息，请参阅 Citrix Scout。

### 收集的内容

Citrix Diagnostic Facility (CDF) 跟踪会记录对故障排除有用的信息。Call Home 会收集一部分 CDF 跟踪，这些跟踪在排查常见故障（例如 VDA 注册和应用程序/桌面启动）时会很有帮助。此技术称为始终开启跟踪 (AOT)。AOT 日志保存在磁盘上的 C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOT 中。

Call Home 不会收集任何其他 Windows 事件跟踪 (ETW) 信息，也无法配置为收集此类信息。

Call Home 还会收集其他信息，例如：

- Citrix Virtual Apps and Desktops 在 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` 下创建的注册表。
- Citrix 命名空间下的 Windows Management Instrumentation (WMI) 信息。
- 正在运行的进程列表。
- 存储在 `%PROGRAMDATA%\Citrix\CDF` 中的 Citrix 进程的崩溃转储。
- 安装和升级信息。这可以包括完整的产品元安装程序日志、失败的 MSI 日志、MSI 日志分析器的输出、StoreFront™ 日志、许可兼容性检查日志以及初步站点升级测试的结果。

跟踪信息在收集时会进行压缩。Citrix Telemetry Service 最多保留 10 MB 的压缩近期跟踪信息，最长时间限制为八天。

- 压缩数据可让 Call Home 在 VDA 上保持较小的占用空间。
- 跟踪保存在内存中，以避免在预配的计算机上产生 IOP。

- 跟踪缓冲区使用循环机制在内存中保留跟踪。

Call Home 收集 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/manage-deployment/call-home-datapoints.html) 中列出的关键数据点。

### 配置和管理摘要

您可以在使用完整产品安装向导时或之后，使用 PowerShell cmdlet 注册 Call Home。注册后，默认情况下，诊断信息会在当地时间每周日凌晨 3:00 左右收集并上传到 Citrix。上传时间会从指定时间开始随机化，持续两小时。这意味着使用默认计划的上传会在凌晨 3:00 到 5:00 之间进行。

如果您不想定期上传诊断信息（或者您想更改计划），您可以使用 PowerShell cmdlet 手动收集和上传诊断信息，或将其存储在本地。

当您注册计划的 Call Home 上传以及手动将诊断信息上传到 Citrix 时，您需要提供 Citrix 帐户或 Citrix Cloud™ 凭据。Citrix 会将这些凭据交换为上传令牌，该令牌用于识别客户并上传数据。凭据不会被保存。

上传发生时，通知将通过电子邮件发送到与 Citrix 帐户关联的地址。

如果您在安装组件时启用了 Call Home，则可以 (#disable-call-home)。

### 先决条件

- 计算机必须运行 PowerShell 3.0 或更高版本。
- Citrix Telemetry Service 必须在计算机上运行。
- 系统变量 `PSModulePath` 必须设置为 Telemetry 的安装路径，例如 `C:\Program Files\Citrix\Telemetry Service\`。

### 在组件安装期间启用 Call Home

**在 VDA 安装或升级期间：** 当您使用完整产品安装程序中的图形界面安装或升级 Virtual Delivery Agent 时，系统会询问您是否要参与 Call Home。有两个选项：

- 参与 Call Home。
- 不参与 Call Home。

如果您正在升级 VDA 并且之前已注册 Call Home，则该向导页面不会出现。

**在 Controller 安装或升级期间：** 当您使用图形界面安装或升级 Delivery Controller 时，系统会询问您是否要参与 Call Home。有三个选项：

当您安装 Controller 时，如果该服务器应用了包含策略设置“作为服务登录”的 Active Directory GPO，则无法在安装向导的 Call Home 页面上配置信息。有关详细信息，请参阅 CTX218094。

如果您正在升级 Controller 并且之前已注册 Call Home，则不会询问您是否参与。

### PowerShell cmdlet 命令

PowerShell 帮助提供了全面的语法，包括这些常见用例中未使用的 cmdlet 和参数的说明。

要使用代理服务器进行上传，请参阅 配置代理服务器。

- **启用计划上传：** 诊断集合会自动上传到 Citrix。如果您不输入用于自定义计划的其他 cmdlet，则使用默认计划。

  ```
  $cred = Get-Credential

  Enable-CitrixCallHome -Credential $cred
  ```

  要确认已启用计划上传，请输入 `Get-CitrixCallHome`。如果已启用，则返回 `IsEnabled=True` 和 `IsMasterImage=False`。

- **为从主映像创建的计算机启用计划上传：** 在主映像中启用计划上传可省去配置计算机目录中创建的每台计算机的麻烦。

  `Enable-CitrixCallHome -Credential $cred -MasterImage`

  要确认已启用计划上传，请输入 **Get-CitrixCallHome**。如果已启用，则返回 `IsEnabled=True` 和 `IsMasterImage=True`。

- **创建自定义计划：** 为诊断集合和上传创建每日或每周计划。

  ```
  $timespan = New-TimeSpan –Hours hours -Minutes minutes

  Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
  -UploadFrequency {Daily|Weekly}
  ```

**示例：**

以下 cmdlet 创建了一个计划，用于在每天晚上 10:20 捆绑和上传数据。Hours 参数使用 24 小时制。当 `UploadFrequency` 参数值为 Daily 时，如果指定了 `DayOfWeek` 参数，则会忽略它。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

要确认计划，请输入 `Get-CitrixCallHomeSchedule`。在前面的示例中，它返回 `StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`。

以下 cmdlet 创建了一个计划，用于在每个星期三晚上 10:20 捆绑和上传数据。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed
-UploadFrequency Weekly
```

要确认计划，请输入 `Get-CitrixCallHomeSchedule`。在前面的示例中，它返回 `StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`。

## 禁用 Call Home

您可以使用 PowerShell cmdlet 或通过 Citrix Scout 禁用 Call Home。

即使禁用 Call Home 计划上传，AOT 日志也会收集并保存到磁盘。（禁用计划上传时，AOT 日志不会自动上传到 Citrix。）您可以禁用 AOT 日志的收集和本地存储。

### 使用 PowerShell 禁用 Call Home

运行以下 cmdlet 后，诊断数据将不会自动上传到 Citrix。（您仍然可以使用 Citrix Scout 或遥测 PowerShell cmdlet 上传诊断数据。）

`Disable-CitrixCallHome`

要确认 Call Home 已禁用，请输入 `Get-CitrixCallHome`。如果已禁用，则返回 `IsEnabled=False` 和 `IsMasterImage=False`。

### 使用 Citrix Scout 禁用收集计划

要使用 Citrix Scout 禁用诊断收集计划，请按照 Schedule collections 中的指导进行操作。在步骤 3 中，单击 **Off** 以取消所选计算机的计划。

### 禁用 AOT 日志收集

运行以下 cmdlet（将 `Enabled` 字段设置为 `false`）后，将不会收集 AOT 日志。

```
Enable-CitrixTrace -Listen‘{“trace”:{“enabled”:false,“persistDirectory”:“C:\Users\Public”,”maxSizeBytes”:1000000, “sliceDurationSeconds”:300}}’
```

`Listen` 参数包含 JSON 格式的参数。

### 为 Call Home 上传配置代理服务器

在启用 Call Home 的计算机上完成以下任务。以下过程中的示例图包含服务器地址和端口 10.158.139.37:3128。您的信息将有所不同。

1. 在浏览器中添加代理服务器信息。在 Internet Explorer 中，选择 **Internet Options \> Connections \> LAN settings**（Internet 选项 \> 连接 \> 局域网设置）。选择 **Use a proxy server for your LAN**（为 LAN 使用代理服务器）并输入代理服务器地址和端口号。
2. 在 PowerShell 中，运行 `netsh winhttp import proxy source=ie`。

   ```
   PS C:\Users\administrator.JLGXH> netsh winhttp import proxy source=ie

   Current WinHTTP proxy settings:

       Proxy Server(s) :  10.108.124.245:8080
       Bypass List     :  (none)
   ```

3. 使用文本编辑器编辑 TelemetryService.exe 配置文件，该文件位于 `C:\Program Files\Citrix\Telemetry Service`。添加红色框中显示的信息。

   ```
   TelemetryService.exe - Notepad
   File  Edit  Format  View  Help
   <?xml version="1.0" encoding="utf-8"?>
   <configuration>
       <startup>
                   <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1" />
       </startup>
       <runtime>
         <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
           <dependentAssembly>
             <assemblyIdentity name="Newtonsoft.Json" culture="neutral" publicKeyToken="30ad4fe6b2a6aeed" />
             <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="9.0.0.0" />
           </dependentAssembly>
           <probing privatePath="TelemetryModule" />
         </assemblyBinding>
       </runtime>
   <system.net>
   <defaultProxy>
   <proxy bypassonlocal="false" usesystemdefault="true" proxyaddress="http://10.108.124.245:8080" />
   </defaultProxy>
   </system.net>

   </configuration>
   ```

4. 重新启动遥测服务。

在 PowerShell 中运行 Call Home cmdlet。

### 手动收集和上传诊断信息

您可以使用 CIS 网站将诊断信息包上传到 CIS。您还可以使用 PowerShell cmdlet 收集诊断信息并将其上传到 CIS。

要使用 CIS 网站上传捆绑包：

1. 使用您的 Citrix 帐户凭据登录 Citrix Insight Services。
2. 选择 **My Workspace**。
3. 选择 **Healthcheck**，然后导航到数据所在位置。

CIS 支持多个用于管理数据上传的 PowerShell cmdlet。本文档涵盖了两种常见情况的 cmdlet：

- 使用 `Start-CitrixCallHomeUpload` cmdlet 手动收集诊断信息包并将其上传到 CIS。（该捆绑包不会在本地保存。）
- 使用 `Start-CitrixCallHomeUpload` cmdlet 手动收集数据并在本地存储诊断信息包。这允许您预览数据。稍后，使用 `Send-CitrixCallHomeBundle` cmdlet 手动将该捆绑包的副本上传到 CIS。（您最初保存的数据仍保留在本地。）

PowerShell 帮助提供了全面的语法，包括这些常见用例中未使用的 cmdlet 和参数的说明。

当您输入 cmdlet 将数据上传到 CIS 时，系统会提示您确认上传。如果 cmdlet 在上传完成之前超时，请在系统事件日志中检查上传状态。如果服务已在执行上传，则上传请求可能会被拒绝。

**收集数据并将捆绑包上传到 CIS：**

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string]
[-Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploadHeader string] [-AppendHeaders string] [-Collect string]
[<CommonParameters>]
```

**收集数据并将其本地保存：**

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
strings] [<CommonParameters>]
```

以下参数有效：

- **Credential**： 将上传定向到 CIS。

- **InputPath：** 要包含在捆绑包中的 zip 文件的位置。这可能是 Citrix 支持请求的附加文件。请务必包含 .zip 扩展名。
- **OutputPath：** 诊断信息的保存位置。在本地保存 Call Home 数据时，此参数是必需的。
- **Description and Incident Time：** 关于上传的自由格式信息。
- **SRNumber：** Citrix 技术支持事件编号。
- **Name：** 标识捆绑包的名称。
- **UploadHeader：** 指定上传到 CIS 的上传标头的 JSON 格式字符串。
- **AppendHeaders：** 指定上传到 CIS 的附加标头的 JSON 格式字符串。
- **Collect：** JSON 格式字符串，用于指定要收集或省略的数据，格式为 {'collector': {'enabled':Boolean}}，其中 Boolean 为 true 或 false。 有效的收集器值为：
  - 'Windows 管理规范'
  - '进程'
  - '注册表'
  - '崩溃报告'
  - '跟踪'
  - '文件'
  - 'msi' 文件
  - '本地数据'
  - '站点数据'
  - 'sfb' 文件

  默认情况下，除 'sfb' 之外的所有收集器均已启用。

  'sfb' 收集器旨在按需使用，以诊断 Skype for Business 问题。除了 'enabled' 参数之外，'sfb' 收集器还支持 'account' 和 'accounts' 参数来指定目标用户。使用以下形式之一：

  - "-收集 " `{'sfb':{'account':'domain\user1'}}` "
  - "-收集 " `{'sfb':{'accounts':['domain\user1', 'domain\user2']}}` "
- **常见参数：**请参阅 PowerShell 帮助。

**上传以前本地保存的数据：**

`Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<CommonParameters>]`

`Path` 参数指定了先前保存的捆绑包的位置。

**示例：**

以下 cmdlet 请求将 Call Home 数据（不包括来自 WMI 收集器的数据）上传到 CIS。此数据与 Citrix Provisioning VDA 的注册失败有关，该失败在下午 2:30 记录，对应 Citrix 支持案例 123456。除了 Call Home 数据外，文件“`c:\Diagnostics\ExtraData.zip`”也包含在上传的捆绑包中。

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:
\Diagnostics\ExtraData.zip" -Description "Registration failures with
Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name
"RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}"
-UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

以下 cmdlet 保存与 Citrix 支持案例 223344 相关的 Call Home 数据，该案例记录于上午 8:15。数据保存在网络共享上的文件 mydata.zip 中。除了 Call Home 数据外，文件“`c:\Diagnostics\ExtraData.zip`”也将包含在保存的捆绑包中。

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \
\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"
-Description "Diagnostics for incident number 223344" -IncidentTime "8:15"
-SRNumber 223344
```

以下 cmdlet 上传您之前保存的数据捆绑包。

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

## 思杰 Scout

### 简介

Citrix Scout 收集诊断信息并运行运行状况检查。您可以使用结果来维护您的 Citrix Virtual Apps and Desktops™ 部署。Citrix 通过 Citrix Insight Services 提供诊断收集的全面自动化分析。您还可以自行或在 Citrix 支持的指导下使用 Scout 解决问题。

您可以将收集文件上传到 Citrix 以进行分析并获得 Citrix 支持的指导。或者，您可以将收集文件保存在本地以供自己查看，然后稍后将收集文件上传到 Citrix 进行分析。

Scout 提供以下过程：

- **收集：** 对您在站点中选择的计算机运行一次性诊断收集。然后，您可以将文件上传到 Citrix 或将其保存在本地。
- **跟踪和重现：** 在您选择的计算机上启动手动跟踪。然后，您在这些计算机上重现问题。重现问题后，跟踪将停止。Scout 然后收集其他诊断信息并将文件上传到 Citrix，或将文件保存在本地。
- **计划：** 计划在您选择的计算机上每天或每周在指定时间进行诊断收集。文件会自动上传到 Citrix。
- **运行状况检查：** 运行检查以评估站点及其组件的运行状况和可用性。您可以对 Delivery Controller、Virtual Delivery Agent (VDA)、StoreFront™ 服务器和 Citrix 许可证服务器运行运行状况检查。如果在检查期间发现问题，Scout 会提供详细报告。每次 Scout 启动时，它都会检查更新的运行状况检查脚本。如果有新版本可用，Scout 会自动下载它们，以便在下次运行运行状况检查时使用。

> **注意：**
>
> **跟踪和重现**、**计划**和**运行状况检查**过程目前不适用于 Linux VDA。

> 本文中描述的图形界面是使用 Scout 的主要方式。或者，您可以使用 PowerShell 配置一次性或计划的诊断收集和上传。请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/manage-deployment/cis.html#citrix-call-home)。

运行 Scout 的位置：

- 在本地部署中，从 Delivery Controller™ 运行 Scout 以捕获诊断信息或对一个或多个 Virtual Delivery Agent (VDA)、Delivery Controller、StoreFront 服务器和许可证服务器运行检查。您还可以从 VDA 运行 Scout 以收集本地诊断信息。
- 在使用 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）的 Citrix Cloud 环境中，从 VDA 运行 Scout 以收集本地诊断信息。

Scout 应用程序的日志存储在 `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log` 中。此文件可用于故障排除。

观看 Citrix Scout 演示。

<iframe src="https://www.youtube.com/embed/2y9k07r8i0" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

### 收集了哪些信息

Scout 收集的诊断信息包括 Citrix 诊断工具 (CDF) 跟踪日志文件。还包括 CDF 跟踪的一个子集，称为“始终开启跟踪 (AOT)”。AOT 信息在排查常见问题（例如 VDA 注册和应用程序/桌面启动）时会很有帮助。不收集其他 Windows 事件跟踪 (ETW) 信息。

收集内容包括：

- Citrix Virtual Apps and Desktops 在 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` 下创建的注册表项。
- **Citrix 命名空间**下的 Windows 管理规范 (WMI) 信息。
- 正在运行的进程。
- 存储在 `%PROGRAMDATA%\Citrix\CDF` 中的 Citrix 进程的崩溃转储。
- Citrix 策略信息，采用 CSV 格式。
- 安装和升级信息。收集内容可包括完整的产品元安装程序日志、失败的 MSI 日志、MSI 日志分析器的输出、StoreFront 日志、许可兼容性检查日志以及初步站点升级测试的结果。

关于跟踪信息：

- 跟踪信息在收集时会进行压缩，以保持在计算机上的占用空间较小。
- 在每台计算机上，Citrix Telemetry Service 最多保留八天的压缩近期跟踪信息。
- 从 Citrix Virtual Apps and Desktops 7 1808 开始，AOT 跟踪默认保存到本地磁盘。（在早期版本中，跟踪保存在内存中。）默认路径 = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`。
- 从 Citrix Virtual Apps and Desktops 7 1811 开始，保存到网络共享的 AOT 跟踪会与其他诊断信息一起收集。
- 您可以使用 `Enable-CitrixTrace` cmdlet 或 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen` 注册表字符串修改最大大小（默认值 = 10 MB）和切片持续时间。
- 跟踪会追加到文件中，直到文件达到 `MaxSize` 的 10%。

有关 Scout 收集的数据点的列表，请参阅Call Home 关键数据点。

### Scout 配置

可以将 Scout 配置为在 Linux VDA 上运行。有关 Linux VDA 和遥测的更多信息，请参阅与 Citrix Telemetry Service 集成

Linux VDA 可能会自动更改 `ctxtelemetry` 套接字端口或遥测服务端口。如果是这样，您必须手动配置端口。

1. 导航到 C:\Program Files\Citrix\Telemetry Service
2. 打开 ScoutUI.exe.config 文件。
3. 将 LinuxVDATelemetryServicePort 或 LinuxVDATelemetryWakeupPort 的值更改为在 Linux VDA 上配置的值：

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. 保存更改并关闭文件。
2. 再次打开 Scout 以确保它加载最新配置。

## 关于运行状况检查

运行状况检查数据存储在 `C:\ProgramData\Citrix\TelemetryService\` 下的文件夹中。

### 站点运行状况检查

站点运行状况检查包含在环境测试服务中，该服务提供对 FlexCast Management Architecture (FMA) 服务的全面评估。除了检查服务可用性外，这些检查还会查找其他运行状况指标，例如数据库连接。

站点运行状况检查在 Delivery Controller 上运行。根据您的站点大小，这些检查可能需要长达一小时才能完成。

#### DELIVERY CONTROLLER 配置检查

作为站点健康检查的一部分，Delivery Controller 配置检查会根据 Citrix 对 Virtual Apps and Desktops 站点的建议，验证是否存在以下问题：

- 一个或多个 Delivery Controller 处于失败状态。
- 站点中只有一个 Delivery Controller。
- Delivery Controller 版本不同。

除了满足健康检查的权限和要求外，Delivery Controller 配置检查还需要：

- 至少有一个 Controller 已开机。
- 在控制器上运行的代理服务。
- Controller 与站点数据库之间的连接正常。

### VDA 健康检查

VDA 健康检查可识别常见的 VDA 注册、会话启动和时区重定向问题的可能原因。

对于 VDA 上的注册，Scout 会检查：

- VDA 软件安装
- VDA 计算机域成员身份
- VDA 通信端口可用性
- VDA 服务状态
- Windows 防火墙配置
- 与 Controller 的通信
- 与 Controller 的时间同步
- VDA 注册状态

对于 VDA 上的会话启动，Scout 会检查：

- 会话启动通信端口可用性
- 会话启动服务状态
- 会话启动 Windows 防火墙配置
- VDA 远程桌面服务客户端访问许可证
- VDA 应用程序启动路径
- 会话启动注册表设置

对于 VDA 上的时区重定向，Scout 会检查：

- Windows 修补程序安装
- Citrix 修补程序安装
- Microsoft 组策略设置
- Citrix 组策略设置

对于 VDA 上的配置文件管理，Scout 会检查：

- 虚拟机管理程序检测
- 预配检测
- Citrix 虚拟应用和桌面
- 个人 vDisk 配置

- 用户存储
- 配置文件管理服务状态检测
- Winlogon.exe 挂钩测试

要对配置文件管理运行检查，您必须在 VDA 上安装并启用配置文件管理。有关配置文件管理配置检查的更多信息，请参阅知识中心文章 CTX132805。

**StoreFront 运行状况检查**

StoreFront 检查验证：

- Citrix Default Domain 服务正在运行
- Citrix Credential Wallet 服务正在运行
- 从 StoreFront 服务器到 Active Directory 端口 88 的连接
- StoreFront 服务器到 Active Directory 端口 389 的连接
- 基本 URL 具有有效的 FQDN
- 可以从基本 URL 检索到正确的 IP 地址
- IIS 应用程序池正在使用 .NET 4.0
- 证书是否绑定到主机 URL 的 SSL 端口
- 证书链是否完整
- 证书是否已过期
- 证书是否即将过期（30 天内）

**许可证服务器检查**

许可证服务器检查验证：

- Delivery Controller 到许可证服务器的连接
- 许可证服务器防火墙远程访问状态
- Citrix 许可服务状态
- 许可证服务器宽限期状态
- 许可证服务器端口连接
- Citrix 供应商守护程序 (CITRIX) 是否正在运行
- 系统时钟是否同步
- Citrix 许可服务是否在本地服务帐户下运行
- `CITRIX.opt` 文件的存在

- 客户成功服务资格日期
- Citrix 许可证服务器更新
- 许可证服务器证书是否在 Delivery Controller 的受信任根存储中

除了满足运行运行状况检查的 权限和要求 之外，许可证服务器还必须加入域。否则，将无法发现许可证服务器。

### 运行运行状况检查

运行状况检查过程包括选择计算机、开始检查，然后查看结果报告。

1. 启动 Scout。从计算机的“**开始**”菜单中，选择“**Citrix > Citrix Scout**”。在打开的页面上，单击“**运行状况检查**”。
2. 选择计算机。单击“**查找计算机**”以发现计算机。“**选择计算机**”页面列出了在此站点中发现的所有 VDA、Delivery Controller 和许可证服务器。您可以按计算机名称筛选显示。选中要从中收集诊断信息的每台计算机旁边的复选框，然后单击“**继续**”。

   要添加其他组件类型（例如 StoreFront 服务器和 VDA 计算机），请参阅 手动添加计算机 和 导入 VDA 计算机。您无法手动添加 Citrix Provisioning™ 服务器或许可证服务器。

   Scout 会自动在每台选定的计算机上启动验证测试，确保其符合 验证测试 中列出的条件。如果验证失败，则会在“**状态**”列中发布一条消息，并且该计算机的复选框将被清除。您可以：

   - 解决问题，然后再次选中该计算机的复选框。这将触发验证测试的重试。
   - 跳过该计算机（取消选中其复选框）。不会对该计算机运行运行状况检查。

   验证测试完成后，单击“**继续**”。
3. 对选定的计算机运行运行状况检查。摘要列出了运行测试的计算机（您选择的通过验证测试的计算机）。单击“**开始检查**”。

   检查期间和检查之后：

   - “**状态**”列指示计算机的当前检查状态。
   - 要停止所有正在进行的检查，请单击页面右下角的“**停止检查**”。（您无法取消单个计算机的运行状况检查，只能取消所有选定计算机的运行状况检查。已完成检查的计算机的信息将保留。）.
   - 当所有选定计算机的检查完成后，右下角的“**停止检查**”按钮将变为“**完成**”。
   - 如果检查失败，可以单击“**操作**”列中的“**重试**”。
   - 如果检查完成且未发现任何问题，则“**操作**”列为空。

- 如果检查发现问题，请单击“**查看详细信息**”以显示结果。
- 所有选定计算机的检查完成后，请勿单击“**返回**”。（如果单击，检查结果将丢失。）

4. 检查完成后，单击“**完成**”返回 Scout 启动页面。

#### 运行状况检查结果

对于生成报告的 Citrix 检查，报告包含：

- 生成结果报告的时间和日期
- 已检查的计算机
- 检查在目标计算机上查找的条件

### 权限和要求

权限：

- 要收集诊断信息：
  - 对于要从中收集诊断信息的每台计算机，您必须是本地管理员和域用户。
  - 您必须具有在每台计算机的 LocalAppData 目录中写入的权限。
- 要运行运行状况检查：
  - 您必须是域用户组的成员。
  - 您必须是完全管理员，或者具有对站点具有只读和 **运行环境测试** 权限的自定义角色。
  - 将脚本执行策略设置为至少 `RemoteSigned` 以允许脚本运行。例如：`Set-ExecutionPolicy RemoteSigned`。**注意：** 其他脚本执行权限也可以。
- 启动 Scout 时使用 **以管理员身份运行**。

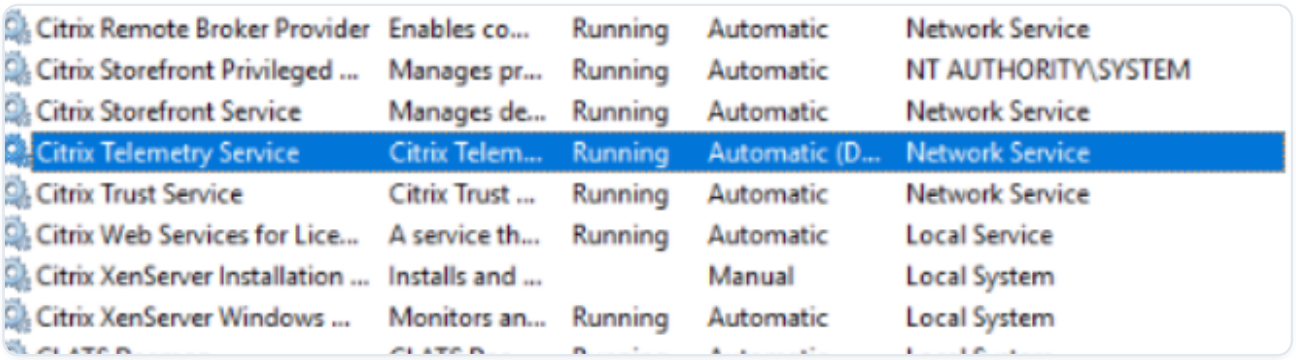
对于您从中收集诊断信息或运行运行状况检查的每台计算机：

- Scout 必须能够与计算机通信。
- 必须启用文件和打印机共享。
- 必须启用 PSRemoting 和 WinRM。计算机还必须运行 PowerShell 3.0 或更高版本。
- 计算机上必须运行 Citrix Telemetry Service。
- 计算机上必须启用 Windows Management Infrastructure (WMI) 访问。
- 要设置诊断信息收集计划，计算机必须运行 兼容的 Scout 版本。

请勿在路径名中指定的用户名称中使用美元符号 ($)。这会阻止诊断信息的收集。

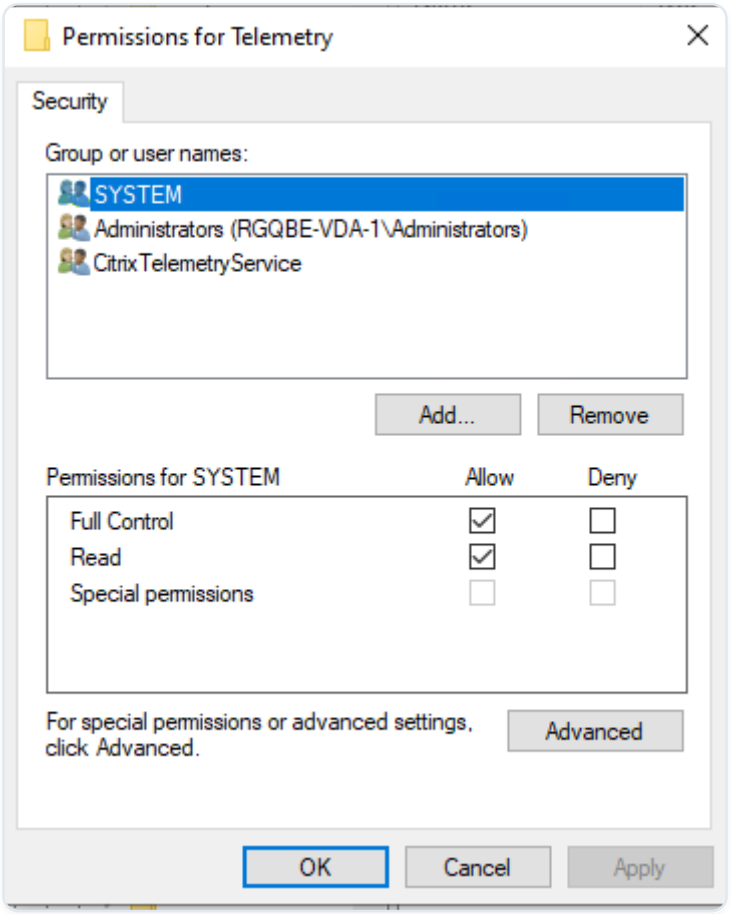
Scout 会对您选择的计算机运行验证测试，以确保满足这些要求。

适用于 Windows 的 Telemetry Service 在 Network Service 上运行。

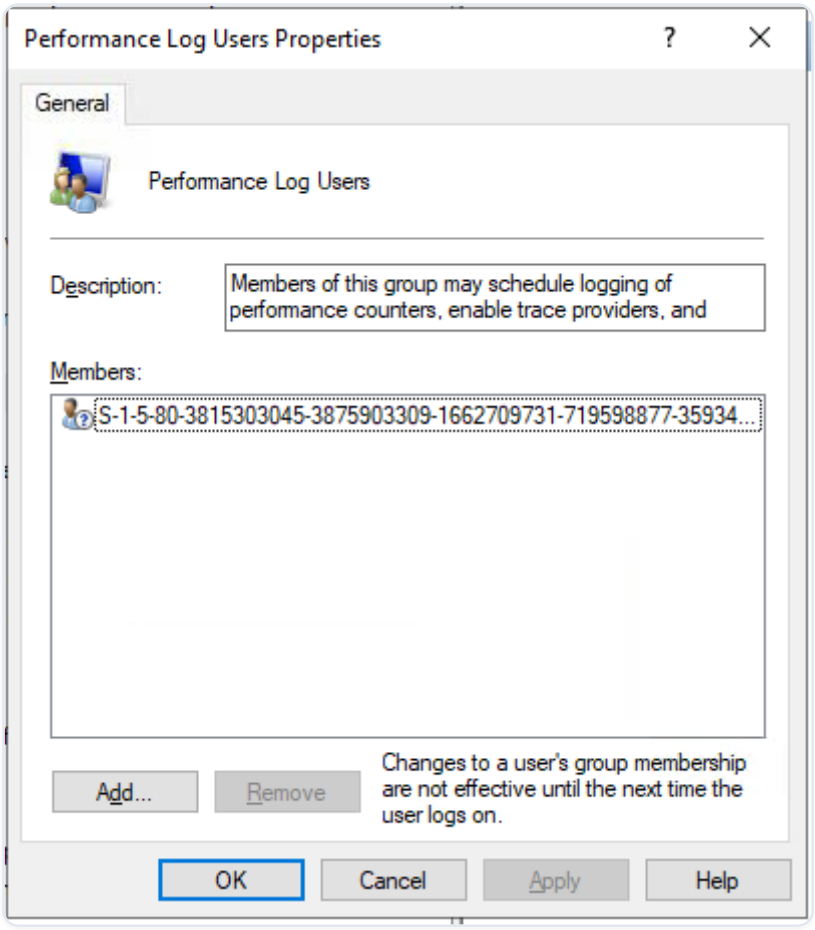



AOT Trace Folder 保存到 `C:\ProgramData\Citrix\TelemetryService\CitrixAOT`。

只有 Administrator group、System 和 Telemetry Service SID 中的用户才有权访问 `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry` 注册表。




卸载 Telemetry Service 后，Telemetry Service SID 仍保留在 Performance Log Users group 中，但您可以手动将其删除。




### 验证测试

在诊断信息收集或运行状况检查开始之前，将为每台选定的计算机自动运行验证测试。这些测试可确保满足要求。如果某台计算机的测试失败，Scout 将显示一条消息，其中包含建议的纠正措施。

- **Scout 无法访问此计算机** - 请确保：
  - 计算机已开机。
  - 网络连接正常工作。（这可能包括验证您的防火墙是否已正确配置。）
  - 文件和打印机共享已启用。有关说明，请参阅 Microsoft 文档。
- **启用 PSRemoting 和 WinRM** - 您可以同时启用 PowerShell 远程处理和 WinRM。使用**以管理员身份运行**，运行 `Enable-PSRemoting` cmdlet。有关详细信息，请参阅 Microsoft cmdlet 帮助。
- **Scout 需要 PowerShell 3.0（最低版本）** - 在计算机上安装 PowerShell 3.0（或更高版本），然后启用 PowerShell 远程处理。
- **无法访问此计算机上的 LocalAppData 目录** - 确保帐户具有在此计算机上的 LocalAppData 目录中写入的权限。
- **无法找到 Citrix Telemetry Service** - 确保 Citrix Telemetry Service 已安装并在计算机上启动。

- **无法获取计划** - 将计算机升级到 XenApp 和 XenDesktop 7.14（最低版本）。
- **WMI 未在计算机上运行** - 确保已启用 Windows Management Instrumentation (WMI) 访问。
- **WMI 连接被阻止** - 在 Windows 防火墙服务中启用 WMI。
- **需要更高版本的 Citrix Telemetry Service** - （仅针对“收集”和“跟踪与重现”检查版本。）升级计算机上的 Telemetry Service 版本（请参阅 安装和升级）。如果您不升级该服务，则该计算机将不包括在**收集**或**跟踪与重现**操作中。
- **Scout 无法连接到此计算机上的 systemd 套接字** - 请确保：
  - 端口 7503 已打开。验证 systemd ctxtelemetry.socket 是否正在计算机上的端口 7503 上侦听。如果 ctxtelemetry.socket 端口已更改，则端口可能不同。请参阅 Scout 配置 以调整端口。
  - 网络连接正常工作。（这可能包括验证您的防火墙是否已正确配置。）
- **Linux VDA 遥测服务未在此计算机上启动** - 确保：
  - 端口 7502 已打开。验证 Linux VDA 遥测服务是否已安装并在此计算机上启动。如果遥测服务端口已更改，则端口可能不同。请参阅Scout 配置 以调整端口。
  - 网络连接正常工作。（这可能包括验证您的防火墙是否已正确配置。）

## 版本兼容性

此版本的 Scout (3.x) 旨在 Citrix Virtual Apps and Desktops（或最低 XenApp and XenDesktop 7.14）控制器和 VDA 上运行。

| 功能 | 思科特 2.23 | 思科特 3.0 |
| --- | --- | --- |
| 支持 Citrix 虚拟应用和桌面（以及 XenApp 和 XenDesktop 7.14 到 7.18） | 是 | 是 |
| 支持 XenDesktop 5.x、7.1–7.13 | 是 | 否 |
| 支持 XenApp 6.x、7.5 到 7.13 | 是 | 否 |
| 随产品提供 | 7.1–7.13 | 从 7.14 开始 |
| 可从 CTX 文章下载 | 是 | 否 |
| 捕获 CDF 跟踪 | 是 | 是 |

| 功能 | 思科特 2.23 | 思科特 3.0 |
| --- | --- | --- |
| 捕获始终开启的跟踪 (AOT) | 否 | 是 |
| 允许收集诊断数据 | 最多同时 10 台计算机（默认） | 无限制（取决于资源可用性） |
| 允许将诊断数据发送到 Citrix | 是 | 是 |
| 允许将诊断数据保存到本地 | 是 | 是 |
| 支持 Citrix Cloud™ 凭据 | 否 | 是 |
| 支持 Citrix 凭据 | 是 | 是 |
| 支持用于上传的代理服务器 | 是 | 是 |
| 调整计划 | N/A | 是 |
| 脚本支持 | 命令行（仅限本地控制器） | 使用 Call Home cmdlet 的 PowerShell（安装了遥测服务的任何计算机） |
| 运行状况检查 | 否 | 是 |
| 数据掩码 | 否 | 从 3.17 开始 |

### 安装和升级

默认情况下，当您安装或升级 VDA 或 Controller 时，Scout 会作为 Citrix Telemetry Service 的一部分自动安装或升级。

如果您在安装 VDA 时省略了 Citrix Telemetry Service，或者稍后删除了该服务，请从 Citrix Virtual Apps and Desktops 安装介质上的 `x64\Virtual Desktop Components` 或 `x86\Virtual Desktop Components` 文件夹运行 `TelemetryServiceInstaller_xx.msi`。

当您选择“**收集**”或“**跟踪和重现**”操作时，如果某台计算机运行的是旧版 Citrix Telemetry Service，您会收到通知。Citrix 建议使用最新支持的版本。如果您未在该计算机上升级 Telemetry Service，则该计算机不会包含在“**收集**”或“**跟踪和重现**”操作中。要升级 Telemetry Service，请使用与安装它相同的过程。

### 上传授权

如果您计划将诊断集合上传到 Citrix，则必须拥有 Citrix 或 Citrix Cloud 帐户。（这些是您用于访问 Citrix 下载或访问 Citrix Cloud Control Center 的凭据。）验证您的帐户凭据后，将颁发一个令牌。

- 如果您使用 Citrix 帐户进行身份验证，则令牌颁发过程不可见。您只需输入您的帐户凭据。Citrix 验证凭据后，您便可以在 Scout 向导中继续操作。
- 如果您使用 Citrix Cloud 帐户进行身份验证，则单击链接以使用默认浏览器通过 HTTPS 访问 Citrix Cloud。输入 Citrix Cloud 凭据后，将显示令牌。复制令牌，然后将其粘贴到 Scout 中。然后您可以在 Scout 向导中继续操作。

令牌存储在运行 Scout 的计算机本地。要使该令牌在下次运行“**收集**”或“**跟踪和重现**”时可用，请选中“**存储令牌并在将来跳过此步骤**”复选框。

每次在 Scout 启动页面上选择“**计划**”时，都必须重新授权。创建或更改计划时，不能使用存储的令牌。

#### 使用代理进行上传

如果要使用代理服务器将集合上传到 Citrix，可以指示 Scout 使用为浏览器 Internet 属性配置的代理设置。或者，您可以指定代理服务器的 IP 地址和端口号。

### 查找计算机

对于“**收集**”、“**跟踪和重现**”和“**计划**”过程，Scout 会列出其自动发现的 Controller 和 VDA。

当您从 Delivery Controller 运行 Scout Health Check 时，单击**查找计算机**以发现计算机，包括 Delivery Controller、VDA、许可证服务器和 StoreFront 服务器。

当您从非 Delivery Controller 的已加入域的计算机运行 Scout Health Check 时，Scout 无法自动发现计算机。您需要手动添加计算机或导入 VDA 计算机。

### 手动添加计算机

在 Scout 列出其发现的 Controller 和 VDA 后，您可以手动添加部署中的其他计算机，例如 StoreFront 服务器、许可证服务器和 Citrix Provisioning 服务器。

运行运行状况检查时：

- 域中的 Citrix 许可证服务器会自动发现。您无法手动添加许可证服务器。
- 运行状况检查目前不支持 Citrix Provisioning 服务器。

在列出已发现计算机的任何 Scout 页面上，单击**+ 添加计算机**。键入要添加的计算机的 FQDN，然后单击**继续**。根据需要重复此操作以添加其他计算机。（尽管输入 DNS 别名而不是 FQDN 可能看起来有效，但运行状况检查可能会失败。）

手动添加的计算机始终显示在计算机列表的顶部，位于已发现计算机的上方。

识别手动添加的计算机的一种简单方法是行右端的红色删除按钮。只有手动添加的计算机才有该按钮。已发现的计算机没有。

要删除手动添加的计算机，请单击行右端的红色按钮。确认删除。重复此操作以删除其他手动添加的计算机。

Scout 会记住手动添加的计算机，直到您将其删除。当您关闭并重新打开 Scout 时，手动添加的计算机仍会显示在列表顶部。

在 StoreFront 服务器上使用**跟踪和重现**时，不会收集 CDF 跟踪。但是，会收集所有其他跟踪信息。

### 导入 VDA 计算机

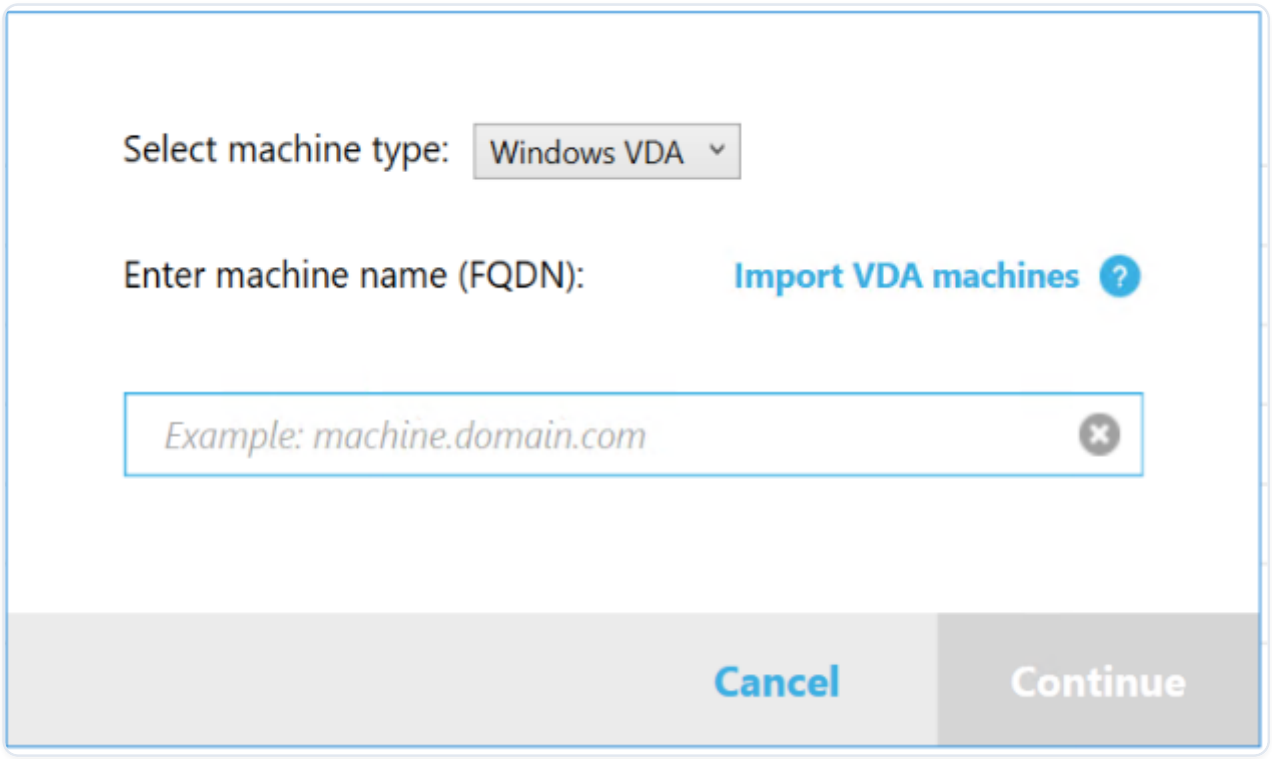
运行运行状况检查时，您可以导入部署中的 VDA 计算机。

1. 在 Delivery Controller 或 Connector 上，使用 PowerShell 命令生成计算机列表文件。在 Connector 上，您必须输入 Citrix 凭据并在弹出对话框中选择客户。

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
   ```

2. 将 machineList.txt 文件复制到您要启动 Scout Health Check 的已加入域的计算机。
3. 在 Scout Health Check 页面上，单击 **添加计算机**。
4. 选择 **Windows VDA** 计算机类型。
5. 单击 **导入 VDA 计算机**。
6. 选择 machineList.txt 文件。
7. 单击 **打开**。

导入的 VDA 计算机将列在 Scout Health Check 页面上。




### 收集诊断信息

**收集** 过程包括选择计算机、启动诊断信息收集，然后将包含收集信息的文件上传到 Citrix 或将其保存到本地。

1. 启动 Scout。从计算机的 **开始** 菜单中，选择 **Citrix > Citrix Scout**。在打开的页面上，单击 **收集**。
2. 选择计算机。

   - 在 Controller 上，**选择计算机** 页面列出了站点中的所有 VDA 和 Controller。您可以按计算机名称筛选显示。要手动添加其他计算机（例如 StoreFront 或 Citrix Provisioning 服务器），请参阅 手动添加计算机。
   - 在其他组件（例如 VDA 服务器）上，**选择计算机** 页面仅列出本地计算机。不支持手动添加计算机。

   选择要从中收集诊断信息的每台计算机旁边的复选框，然后单击“**继续**”。

   Scout 会自动在每台选定的计算机上启动验证测试，确保其符合 (#verification-tests) 中列出的条件。如果验证失败，**状态**列中会显示一条消息，并且该计算机的复选框将被取消选中。您可以选择：

   - 解决问题，然后再次选中该计算机的复选框。这将触发验证测试的重试。
   - 跳过该计算机（使其复选框保持未选中状态）。将不会从该计算机收集诊断信息。

   验证测试完成后，单击“**继续**”。

3. 收集诊断信息。摘要列出了所有已收集诊断信息的计算机（您选择并通过验证测试的计算机）。单击“**开始收集**”。

   收集期间：

   - **状态**列指示计算机的当前收集状态。
   - 要停止单个计算机上正在进行的收集，请在该计算机的**操作**列中单击“**取消**”。
   - 要停止所有正在进行的收集，请单击页面右下角的“**停止收集**”。已完成收集的计算机的诊断信息将保留。要恢复收集，请在每台计算机的**操作**列中单击“**重试**”。
   - 当所有选定计算机的收集完成后，右下角的“**停止收集**”按钮将变为“**继续**”。
   - 要再次收集诊断信息，请在该计算机的**操作**列中单击“**再次收集**”。较新的收集会覆盖较早的收集。
   - 如果收集失败，您可以在**操作**列中单击“**重试**”。只有成功的收集才会上传或保存。
   - 所有选定计算机的收集完成后，请勿单击“**返回**”。（如果单击，收集将丢失。）

   收集完成后，单击“**继续**”。

4. 保存或上传收集的数据。选择是将文件上传到 Citrix，还是将其保存到本地计算机。

   如果您选择立即上传文件，请继续执行步骤 5。

   如果您选择将文件保存到本地：

   - 将显示 Windows **保存**对话框。导航到所需位置。
   - 本地保存完成后，将显示文件的路径名并提供链接。您可以查看该文件。您可以稍后将文件上传到 Citrix。请参阅 CTX136396。

   单击 **Done** 返回 Scout 启动页面。您无需完成此过程中的任何其他步骤。

5. 对上传进行身份验证，并可选择指定代理。有关详细信息，请参阅 上传授权。

   - 如果您尚未通过 Scout 进行身份验证，请继续执行此步骤。
   - 如果您已通过 Scout 进行身份验证，则默认使用存储的授权令牌。如果这是您想要执行的操作，请选择此选项并单击 **Continue**。系统不会提示您输入此收集的凭据。继续执行步骤 6。
   - 如果您之前已进行身份验证，但想要重新授权并获取新令牌，请单击 **Change/Reauthorize** 并继续执行此步骤。

   选择是使用 Citrix 凭据还是 Citrix Cloud 凭据来验证上传。单击 **Continue**。凭据页面仅在您未使用存储的令牌时显示。

   在凭据页面上：

- 如果要为文件上传使用代理服务器，请单击 **Configure proxy**。您可以指示 Scout 使用为浏览器 Internet 属性配置的代理设置。或者，您可以输入代理服务器的 IP 地址和端口号。关闭代理对话框。
- 对于 Citrix Cloud 帐户，请单击 **Generate token**。您的默认浏览器将启动到 Citrix Cloud 页面，其中显示一个令牌。复制令牌，然后将其粘贴到 Scout 页面上。
- 对于 Citrix 帐户，请输入您的凭据。

完成后，点击“**继续**”。

6. 输入有关上传的信息。

   - 名称字段包含所收集诊断文件的默认名称。这对于大多数收集来说已足够，尽管您可以更改名称。（如果删除默认名称并使名称字段为空，则将使用默认名称。）
   - （可选）指定一个 8 位数的 Citrix 支持案例编号。
   - 在可选的“**描述**”字段中，描述问题并指明问题发生的时间（如果适用）。

   完成后，点击“**开始上传**”。

   上传期间，页面左下角会显示已完成上传的近似百分比。要取消正在进行的上传，请点击“**停止上传**”。

   上传完成后，将显示其位置的 URL 并提供链接。您可以点击该链接转到 Citrix 位置以查看上传分析，也可以复制该链接。

   点击“**完成**”返回 Scout 启动页面。

### 跟踪和重现

“**跟踪和重现**”过程包括选择计算机、启动跟踪、重现问题、完成诊断收集，然后将文件上传到 Citrix 或将其保存到本地。

此过程类似于标准“**收集**”过程。但是，它允许您在计算机上启动跟踪，然后在这些计算机上重新创建问题。所有诊断收集都包含 AOT 跟踪信息。此过程添加 CDF 跟踪以帮助进行故障排除。

1. 启动 Scout。从计算机的“**开始**”菜单中，选择“**Citrix > Citrix Scout**”。在启动页面上，点击“**跟踪和重现**”。
2. 选择计算机。“**选择计算机**”页面列出了站点中的所有 VDA 和控制器。您可以按计算机名称筛选显示。选中要从中收集跟踪和诊断的每台计算机旁边的复选框。然后点击“**继续**”。

   要手动添加其他计算机（例如 StoreFront 或 Citrix Provisioning 服务器），请参阅手动添加计算机。

Scout 会自动在每台选定的计算机上启动验证测试，确保它符合 验证测试 中列出的条件。如果某台计算机的验证失败，**状态**列中会显示一条消息，并且该计算机的复选框会被取消选中。您可以选择：

- 解决问题，然后再次选中该计算机的复选框。这将触发验证测试的重试。
- 跳过该计算机（使其复选框保持未选中状态）。不会从该计算机收集诊断信息和跟踪。

验证测试完成后，单击**继续**。

3. 启动跟踪。摘要列出了所有从中收集跟踪的计算机。单击**开始跟踪**。

   在一台或多台选定的计算机上，重现您遇到的问题。在此过程中，跟踪收集会继续。重现问题后，在 Scout 中单击**继续**。这将停止跟踪。

   停止跟踪后，指示您是否在跟踪期间重现了问题。

4. 从计算机收集诊断信息。单击**开始收集**。收集期间：

   - “**状态**”列指示计算机的当前收集状态。
   - 要停止单台计算机上正在进行的收集，请在该计算机的**操作**列中单击**取消**。
   - 要停止所有正在进行的收集，请单击页面右下角的**停止收集**。已完成收集的计算机的诊断信息将保留。要恢复收集，请在每台计算机的**操作**列中单击**重试**。
   - 当所有选定计算机的收集完成后，右下角的**停止收集**按钮将变为**继续**。
   - 要再次从计算机收集诊断信息，请在该计算机的**操作**列中单击**再次收集**。新的收集会覆盖之前的收集。
   - 如果收集失败，您可以在**操作**列中单击**重试**。只有成功的收集才会上传或保存。
   - 所有选定计算机的收集完成后，请勿单击**返回**。（如果单击，收集的数据将丢失。）

   收集完成后，点击“**继续**”。

5. 保存或上传收集。选择是将文件上传到 Citrix 还是本地保存。

   如果您选择现在上传文件，请继续执行步骤 6。

   如果您选择将文件保存到本地：

   - 将出现一个 Windows 保存对话框。选择所需位置。
   - 本地保存完成后，将显示并链接文件的路径名。您可以查看该文件。请记住：您可以稍后从 Citrix 上传文件；有关 Citrix Insight Services，请参阅 CTX136396。

   点击“**完成**”返回 Scout 启动页面。您无需完成此过程中的任何其他步骤。

6. 对上传进行身份验证并可选地指定代理。有关此过程的详细信息，请查看 上传授权。

- 如果您尚未通过 Scout 进行身份验证，请继续执行此步骤。
- 如果您已通过 Scout 进行身份验证，则默认使用存储的授权令牌。如果这是您想要执行的操作，请选择此选项并点击“**继续**”。系统不会提示您输入此收集的凭据。继续执行步骤 7。
- 如果您之前已进行身份验证，但想重新授权并获取新令牌，请点击“**更改/重新授权**”并继续执行此步骤。

选择您是要使用 Citrix 凭据还是 Citrix Cloud 凭据来验证上传。点击“**继续**”。凭据页面仅在您未使用存储令牌时显示。

在凭据页面上：

- 如果您想为文件上传使用代理服务器，请点击“**配置代理**”。您可以指示 Scout 使用为浏览器 Internet 属性配置的代理设置。或者，您可以输入代理服务器的 IP 地址和端口号。关闭代理对话框。
- 对于 Citrix Cloud 帐户，点击“**生成令牌**”。您的默认浏览器将启动到 Citrix Cloud 页面，其中显示一个令牌。复制该令牌，然后将其粘贴到 Scout 页面上。
- 对于 Citrix 帐户，输入您的凭据。

完成后，单击 **继续**。

7. 提供有关上传的信息。

   输入上传详细信息：

   - 名称字段包含所收集诊断文件的默认名称。这对于大多数收集来说已足够，尽管您可以更改名称。（如果删除默认名称并使名称字段为空，则会使用默认名称。）
   - （可选）指定一个 8 位数的 Citrix 支持案例编号。
   - 在可选的“描述”字段中，描述问题并指明问题发生的时间（如果适用）。

   完成后，单击 **开始上传**。

   上传期间，页面左下角会显示上传完成的大致百分比。要取消正在进行的上传，请单击 **停止上传**。

   上传完成后，将显示其位置的 URL 并提供链接。您可以点击该链接前往 Citrix 位置查看上传分析，也可以复制该链接。

   单击 **完成** 返回 Scout 启动页面。

### 启用附加日志收集

**启用附加日志收集** 功能允许您将跟踪和重现功能与更多工具（例如 perfmon、Netsh、DebugView 和 Wireshark）结合使用。

> **注意：**
>
> 这仅适用于本地计算机。

> 要设置附加日志收集：

1. 启动 Citrix Scout。
2. 单击“**设置**”齿轮图标。
3. 单击“**使用更多工具启用附加日志收集**”。
4. 单击 **保存**。

要收集附加日志：

1. 在 Scout 主页上，单击“**跟踪和重现**”。
2. 在“**选择计算机**”页面上，单击本地计算机右侧的齿轮图标。
3. 在“**选择日志记录所需的工具：**”页面上，单击“**下载工具**”。
4. 在“**下载工具**”页面上，选择要使用的工具，然后单击“**下载**”。然后将下载这些工具，Wireshark 除外。Wireshark 只能手动下载和安装。 注意：如果您选择手动下载其他工具，则必须将下载的 .zip 文件的内容提取到 `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\<toolname>`。例如，如果您下载 DebugView.zip 文件，则需要将该文件的内容解压缩到 `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\`。
5. 在“**选择日志记录所需的工具：**”页面上，单击“**刷新状态**”。所有选定的工具在“状态”列下显示为“**存在**”。
6. 选择用于日志记录的工具，然后单击“**下一步**”。
7. 按照跟踪和重现 说明进行操作。
8. 完成后，检查 zip 文件中的日志。日志已压缩到 *CDCLogs* 文件夹中。

> **注意：**

如果选择 Procmon 工具进行跟踪，则 Process Monitor 日志可能会快速增长。请确保仅选择所需的工具。您还可以在 *%temp%\Scout-CDC-Log* 下监视日志的大小。

### 安排收集

**注意：**

您目前可以安排收集，但不能安排运行状况检查。

计划过程包括选择计算机，然后设置或取消计划。计划的收集会自动上传到 Citrix。（您可以使用 PowerShell 界面在本地保存计划的收集。请参阅 Citrix Call Home。）

1. 启动 Scout。从计算机的“开始”菜单中，选择 **Citrix > Citrix Scout**。在打开的页面上，单击“**计划**”。
2. 选择计算机。列出了站点中的所有 VDA 和控制器。您可以按计算机名称筛选显示。

   当您使用图形界面安装 VDA 和控制器时，如果您设置了 Call Home 计划（请参阅 Citrix Call Home），Scout 默认会显示这些设置。您可以使用此版本的 Scout 首次启动计划的收集，或更改以前配置的计划。

   尽管您在组件安装期间按每台计算机启用了/禁用了 Call Home，但在 Scout 中配置的计划会影响您选择的所有计算机。

   选中要从中收集诊断信息的每台计算机旁边的复选框，然后单击“**继续**”。

   要手动添加其他计算机（例如 StoreFront 或 Citrix Provisioning 服务器），请参阅 手动添加计算机。

   Scout 会自动对每台选定的计算机启动验证测试，确保其符合 验证测试 中的条件。如果某台计算机的验证失败，则会在“**状态**”列中发布一条消息，并且该计算机的复选框将被取消选中。您可以选择：

   - 解决问题，然后再次选中该计算机的复选框。这将触发验证测试的重试。
   - 跳过该计算机（使其复选框保持未选中状态）。不会从该计算机收集诊断信息（或跟踪）。

   验证测试完成后，单击“**继续**”。

   摘要页面列出了应用了计划的计算机。单击“**继续**”。
3. 设置计划。指明您希望何时收集诊断信息。请记住：该计划会影响所有选定的计算机。

- 要为选定的计算机配置每周计划，请单击“**每周**”。选择星期几。输入收集开始的时间（24 小时制）。
- 要为选定的计算机配置每日计划，请单击“**每日**”。输入收集开始的时间（24 小时制）。
- 要取消所选计算机的现有计划（而不是替换为另一个计划），请单击“**关闭**”。这将取消之前为这些计算机配置的任何计划。

单击“**继续**”。

4. 对上传进行身份验证，并可选择指定代理。有关此过程的详细信息，请查看上传授权。请记住：在使用 Scout 计划时，不能使用存储的令牌进行身份验证。

   选择是使用 Citrix 凭据还是 Citrix Cloud 凭据来验证上传。单击“**继续**”。

   在凭据页面上：

   - 如果要使用代理服务器进行文件上传，请单击“**配置代理**”。您可以指示 Scout 使用为浏览器 Internet 属性配置的代理设置。或者，您可以输入代理服务器的 IP 地址和端口号。关闭代理对话框。
   - 对于 Citrix Cloud 帐户，请单击“**生成令牌**”。您的默认浏览器将启动到 Citrix Cloud 页面，其中显示一个令牌。复制该令牌，然后将其粘贴到 Scout 页面上。
   - 对于 Citrix 帐户，请输入您的凭据。

   完成后，单击“**继续**”。

   查看已配置的计划。单击“**完成**”返回 Scout 启动页面。

   在收集过程中，每台选定计算机的 Windows 应用程序日志都包含有关收集和上传的条目。

### 数据屏蔽

使用 Citrix Scout 收集的诊断信息可能包含安全敏感信息。Citrix Scout 数据屏蔽功能允许您在将诊断文件上传到 Citrix 之前屏蔽其中的敏感数据。

Scout 数据屏蔽配置为屏蔽 IP 地址、计算机名称、域名、用户名、虚拟机管理程序名称、交付组名称、目录名称、应用程序名称和 SID。

> **注意：**

> CDF 跟踪已加密，无法屏蔽。

> Linux VDA 日志已压缩为 `.tar.gz2` 格式，无法屏蔽。

#### 收集新诊断信息并执行数据掩码

要使用 Citrix Scout 数据掩码功能，请从命令行启动 Scout。

1. 在 Windows 中，以管理员身份打开命令提示符。
2. 转到 Scout 的安装目录：`cd C:\Program Files\Citrix\Telemetry Service`。
3. 启动 Scout：`ScoutUI.exe datamasking`。
4. 单击“**收集**”或“**跟踪和重现**”以收集诊断信息。
5. 收集完成后，选择“**启用数据掩码**”。此选项默认启用。
6. 配置数据掩码。您可以使用默认规则或自定义规则。
7. 选择是上传还是保存诊断信息集合。
   - 如果选择“**将诊断信息集合上传到 Citrix**”，则会将已掩码的诊断文件上传到 Citrix。
   - 如果选择“**将诊断信息集合保存到本地计算机**”，则原始诊断信息和已掩码的诊断信息都将保存到指定位置。

#### 对现有诊断信息执行数据掩码

1. 在 Windows 中，以管理员身份打开命令提示符。
2. 转到 Scout 的安装目录：`cd C:\Program Files\Citrix\Telemetry Service`。
3. 直接在数据掩码模式下启动 Scout：`ScoutUI.exe datamasking filePath`。
4. 选择“启用数据屏蔽”以继续。此选项默认启用。
5. 配置数据屏蔽。您可以使用默认规则运行数据屏蔽，也可以自定义规则。
6. 选择是上传还是保存诊断集合。
   - 如果您选择**将诊断集合上传到 Citrix**，则屏蔽的诊断文件将上传到 Citrix。
   - 如果您选择**将诊断集合保存到本地计算机**，则原始诊断和屏蔽诊断都将保存到指定位置。

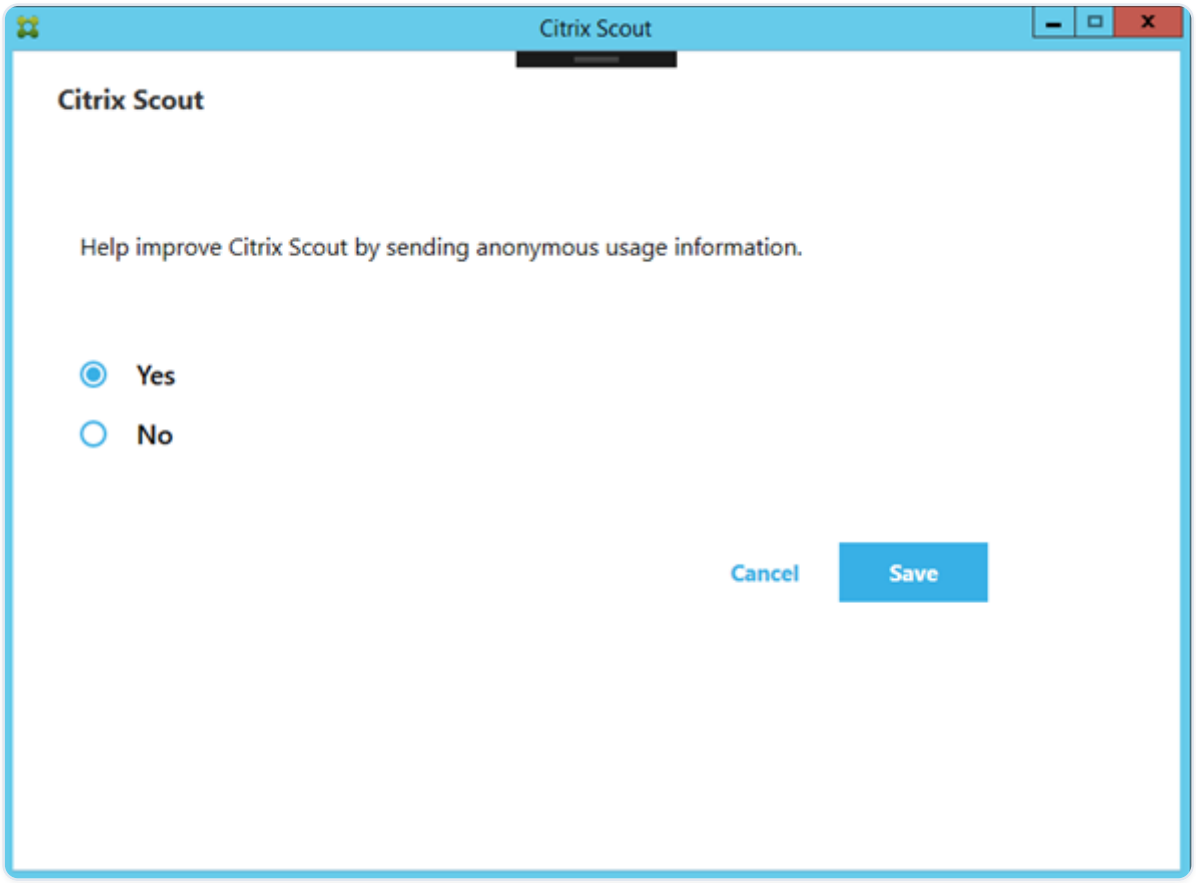
#### 屏蔽数据文件和映射文件位置

上传或保存诊断集合后，单击链接以打开原始诊断和屏蔽诊断，并打开映射信息文件。

### 使用情况数据收集

当您使用 Scout 时，Citrix 会使用 Google Analytics 收集匿名使用情况数据，以用于未来的产品功能和改进。数据收集默认启用。

要更改使用情况数据收集和上传，请单击 Scout UI 中的**设置**齿轮。然后，您可以通过选择**是**或**否**来选择是否发送信息，然后单击**保存**。




## Call Home 关键数据点

Call Home 收集以下关键数据点。

(M) = 仅在手动收集期间捕获 (PowerShell cmdlet `Start-CitrixCallHomeUpload`)

| 文件名 | 类别 | 数据组 |
| --- | --- | --- |
| | | |
| | | 计算机 |
| | | XD站点 |
| | | 站点信息 |
| | | Broker 数据库信息 (M) |
| | | 已安装的数据库版本 (M) |

| | | |
|---|---|---|
| | | Broker 服务状态 (M) |
| | | 已注册的服务实例 (M) |
| | | Broker 许可证测试 (M) |
| | | 活动 HDX™ 会话 (M) |
| | | Broker 管理员 |
| | | Broker 管理员权限 |
| | | RDS 配置（包括 LicensingSettings、SessionSettings、SpecifiedLicenseServers 和 RegisteredLicenseServers） |
| | | 监控服务 (M)（包括 MonitorConfiguration、MonitorDataStore、MonitorDBConnection、MonitorDBSchemaVersion、MonitorService、MonitorServiceAddedCapability、MonitorServiceInstance、MonitorServiceStatus 和 MonitorInstalledDBVersion） |
| | | 配置日志记录 |
| | | 连接日志 |
| | | 管理程序连接 (M) |
| | | 代理管理程序连接 |
| | | 管理程序警报 |
| | | 目录 |
| | | 多会话操作系统代理 (M) |
| | | 单会话操作系统代理 (M) |

| | | |
|---|---|---|
| | | 已发布的应用程序 |
| | | 交付组 |
| | | 已配置的交付代理 |

| | | |
|---|---|---|
| | | Citrix 已安装组件 |
| | | Citrix 代理服务信息 |
| | | 代理服务配置文件 |
| | | 计算机创建服务™ 配置文件 |
| | | 主机服务配置文件 |
| | | AD 身份服务配置文件 |
| | | 配置服务配置文件 |
| | | 配置日志服务配置文件 |
| | | 委派管理服务配置文件 |
| | | 环境测试服务配置文件 |
| | | 监视服务配置文件 |
| | | Storefront™ 服务配置文件 |
| | | 工作站代理配置文件 |
| | | Citrix VDA 信息 |
| | | Citrix XD 热修复 |
| | | Citrix_VirtualChannel_Graphics_Enum |
| | | Citrix_VirtualChannel_Flash_Enum |

| | | |
|---|---|---|
| | | Citrix_VirtualChannel_Printer_Enum |

| | | |
|---|---|---|
| | | 计算机 |
| | | BIOS |
| | | 内存信息 |
| | | 处理器 |
| | | PnP 设备 |
| | | 设备 |
| | | 磁盘驱动器 |
| | | 逻辑驱动器 |
| | | 页面文件使用情况 |
| | | 网络适配器 |
| | | 网络适配器配置 |
| | | ipConfig |
| | | 视频控制器 |
| | | IDE 控制器 |
| | | SCSI 控制器 |

| | | |
|---|---|---|
| | | HKLM:\Software\Wow6432Node\Citrix |
| | | HKLM:\System\CurrentControlSet\Control\Citrix |

| | | |
|---|---|---|
| | | HKLM:\SOFTWARE\Policies\Citrix |
| | | HKLM:\Software\Microsoft\Cryptography |
| | | HKLM:\Software\Wow6432Node\Microsoft\Cryptography |
| | | HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Windows |
| | | HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon |
| | | HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer |
| | | HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer |
| | | HKLM:\SYSTEM\CurrentControlSet\Control\Print\Environments |
| | | HKLM:\系统\当前控制集\控制\会话管理器 |
| | | HKLM:\系统\当前控制集\控制\终端服务器 |
| | | HKCU:\Control Panel\Desktop |

| | | |
|---|---|---|
| | | HKLM:\SOFTWARE\Classes\ShockwaveFlash.ShockwaveFlash\CurVer |
| | | HKLM:\SYSTEM\CurrentControlSet\Control\SystemInformation |
| | | HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem |
| | | HKLM:\SYSTEM\CurrentControlSet\Control\Windows |
| | | HKLM:\SYSTEM\CurrentControlSet\Control\TimeZoneInformation |

| | | |
|---|---|---|
| | | 驱动程序 |
| | | 环境变量 |
| | | 操作系统 |
| | | 进程 |
| | | 服务 |
| | | 服务包 |
| | | 组策略结果 |
| | | Microsoft 热修复程序 |
| | | 网络统计 |
| | | PNP 驱动程序 |

| | | |
|---|---|---|
| | | 系统事件日志 |

| | | |
|---|---|---|
| | | AOT（始终开启的跟踪） |
| | | 崩溃转储 |

| | | |
|---|---|---|
| | | 运行时间 |
| | | 内存 |
| | | 计算机系统 |
| | | 处理器 |
| | | 视频控制器 |
| | | 磁盘驱动器 |
| | | 浏览器信息 |
| | | 重启次数 |
| | | 内存使用情况 |
| | | 磁盘使用情况 |
| | | ICA 会话分辨率 |
| | | ICA 颜色深度 |
| | | 元安装程序-客户体验改善计划-机器 ID |

| | | |
|---|---|---|
| | | 存储数量 |
| | | 服务器组中的服务器数量 |
| | | 每个存储的 Delivery Controller™ 数量 |
| | | HTTPS 已启用 |
| | | 为 Citrix Receiver™ 启用经典体验 |

| | | |
|---|---|---|
| | | 适用于 Citrix 接收器的 HTML5 接收器设置 |
| | | 为 Citrix Receiver 启用工作区控制 |
| | | Store 的远程访问已启用 |
| | | 网关数量 |
| | | 用于集成 NetScaler® 身份验证的显式 JSON 服务 |

# 监控

管理员和技术支持人员可以使用各种功能和工具监控 Citrix Virtual Apps and Desktops™ 站点。使用这些工具，您可以监控：

- 用户会话和会话使用情况
- 登录性能
- 连接和计算机，包括故障
- 负载评估
- 历史趋势
- 基础结构

## 思杰监控台

Director 是一款实时 Web 工具，可用于监控和故障排除，并为最终用户执行支持任务。

有关详细信息，请参阅 Director 文章。

## 配置日志记录

配置日志记录允许管理员跟踪对站点的管理更改。配置日志记录可以帮助管理员在进行配置更改后诊断和排除问题，协助变更管理和跟踪配置，并报告管理活动。

您可以从 Studio 查看和生成有关已记录信息的报告。您还可以在 Director 中使用趋势视图查看已记录的项目，以提供配置更改的通知。此功能对于无权访问 Studio 的管理员很有用。

趋势视图提供了一段时间内配置更改的历史数据，以便管理员可以评估对站点进行了哪些更改、何时进行的以及由谁进行的，从而找出问题的根源。此视图将配置信息分为三类：

- 连接故障
- 失败的单会话计算机
- 失败的多会话计算机

有关如何启用和配置配置日志记录的详细信息，请参阅配置日志记录。 Director文章介绍了如何从该工具查看日志信息。

# 事件日志

Citrix Virtual Apps and Desktops 中的服务会记录发生的事件。事件日志用于监视和排查操作。

有关详细信息，请参阅事件日志。各个功能文章也可能包含事件信息。

# 配置日志记录

配置日志记录是一项功能，可将站点配置更改和管理活动捕获到数据库中。此功能默认启用。您可以使用记录的内容来：

- 在配置更改后诊断和解决问题。日志提供了一个跟踪线索。
- 协助变更管理并跟踪配置。
- 报告管理活动。

您可以从 Citrix Studio 设置配置日志记录首选项、显示配置日志以及生成 HTML 和 CSV 报告。您可以按日期范围和全文搜索结果筛选配置日志显示。强制日志记录（启用时）会阻止进行配置更改，除非这些更改可以被记录。获得适当权限后，您可以从配置日志中删除条目。您不能使用配置日志记录功能编辑日志内容。

配置日志记录使用 PowerShell SDK 和配置日志记录服务。配置日志记录服务在站点中的每个控制器上运行。如果一个控制器发生故障，另一个控制器上的服务会自动处理日志记录请求。

默认情况下，配置日志记录功能处于启用状态，并使用在创建站点时创建的数据库（站点配置数据库）。您可以为数据库指定不同的位置。配置日志记录数据库支持与站点配置数据库相同的高可用性功能。

对配置日志记录的访问通过委派管理进行控制，具有“编辑日志记录首选项”和“查看配置日志”权限。

配置日志在创建时即已本地化。例如，以英语创建的日志将以英语读取，无论读者的区域设置如何。

## 记录了什么

从 Studio、Director 和 PowerShell 脚本启动的配置更改和管理活动都会被记录。记录的配置更改示例包括处理（创建、编辑、删除、分配）：

- 计算机目录
- 交付组（包括更改电源管理设置）
- 管理员角色和范围
- 主机资源和连接

- 通过 Studio 的 Citrix 策略

记录的管理更改示例包括：

- 虚拟机或用户桌面的电源管理
- Studio 或 Director 向用户发送消息

以下操作不会被记录：

- 自主操作，例如池管理虚拟机的电源开启。
- 通过组策略管理控制台 (GPMC) 实现的策略操作；使用 Microsoft 工具查看这些操作的日志。
- 通过注册表、直接访问数据库或来自 Studio、Director 或 PowerShell 以外的源进行的更改。
- 部署初始化时，当第一个配置日志记录服务实例向配置服务注册时，配置日志记录才可用。因此，配置的早期阶段不会被记录（例如，获取和应用数据库架构时，初始化管理程序时）。

## 管理配置日志记录

默认情况下，配置日志记录使用创建站点时创建的数据库（也称为站点配置数据库）。Citrix 建议您将配置日志记录数据库（和监视数据库）放置在单独的位置，原因如下：

- 配置日志记录数据库的备份策略可能与站点配置数据库的备份策略不同。
- 为配置日志记录（和监视服务）收集的数据量可能会对站点配置数据库的可用空间产生不利影响。
- 它将三个数据库的单点故障分离开来。

不支持配置日志记录的产品版本在 Studio 中没有“日志记录”节点。

## 启用和禁用配置日志记录以及强制日志记录

默认情况下，配置日志记录处于启用状态，强制日志记录处于禁用状态。

1. 在 Studio 导航窗格中选择 **日志记录**。
2. 在“操作”窗格中选择 **首选项**。配置日志记录对话框包含数据库信息，并指示配置日志记录和强制日志记录是启用还是禁用。
3. 选择所需操作：

   要启用配置日志记录，请选择 **启用**。这是默认设置。如果无法写入数据库，则日志记录信息将被丢弃，但操作会继续。

   要禁用配置日志记录，请选择 **禁用**。如果以前启用了日志记录，则现有日志仍可通过 PowerShell SDK 读取。

要启用强制日志记录，请选择 **当数据库不可用时阻止更改站点配置**。除非可以将配置更改或通常记录的管理活动写入配置日志记录数据库，否则不允许进行此类更改或活动。仅当启用配置日志记录时（即选择 **启用** 时），才能启用强制日志记录。如果配置日志记录服务失败且未使用高可用性，则假定为强制日志记录。在这种情况下，通常会记录的操作将不会执行。

要禁用强制日志记录，请选择 **当数据库不可用时允许更改站点配置**。即使无法访问配置日志记录数据库，也允许进行配置更改和管理活动。这是默认设置。

## 更改配置日志记录数据库位置

当强制日志记录启用时，您无法更改数据库位置，因为位置更改包括一个无法记录的短暂断开连接间隔。

1. 使用受支持的 SQL Server 版本创建数据库服务器。
2. 在 Studio 导航窗格中选择 **日志记录**。
3. 在“操作”窗格中选择 **首选项**。
4. 在“日志记录首选项”对话框中，选择 **更改日志记录数据库**。
5. 在“更改日志记录数据库”对话框中，指定包含新数据库服务器的服务器位置。有关有效格式，请参阅 (/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/technical-overview/databases.html#database-address-formats)。
6. 要允许 Studio 创建数据库，请单击 **确定**。出现提示时，单击 **确定**，数据库将自动创建。Studio 尝试使用当前 Studio 用户的凭据访问数据库。如果失败，系统会提示您输入数据库用户的凭据。然后，Studio 会将数据库架构上传到数据库。（凭据仅在数据库创建期间保留。）
7. 要手动创建数据库，请单击**生成数据库脚本**。生成的脚本包含手动创建数据库的说明。在上传架构之前，请确保数据库为空，并且至少有一个用户有权访问和更改数据库。

以前数据库中的配置日志记录数据不会导入到新数据库。检索日志时，无法从两个数据库聚合日志。新配置日志记录数据库中的第一个日志条目指示发生了数据库更改，但它不标识以前的数据库。

## 显示配置日志内容

启动配置更改和管理活动时，Studio 和 Director 创建的高级操作将列在 Studio 的上方中间窗格中。一个高级操作会产生一个或多个服务和 SDK 调用，这些是低级操作。在上方窗格中选择高级操作时，下方窗格会显示低级操作。

如果操作在完成之前失败，则日志操作可能未在数据库中完成。例如，开始记录将没有相应的停止记录。在这种情况下，日志会指示信息缺失。当您根据时间范围显示日志时，如果日志中的数据符

合条件，则会显示不完整的日志。例如，如果请求过去五天的所有日志，并且存在一个日志，其开始时间在过去五天内但没有结束时间，则该日志也会被包括在内。

使用调用 PowerShell cmdlet 的脚本时，如果您在未指定父高级操作的情况下创建低级操作，配置日志记录会创建一个替代高级操作。

要显示配置日志内容，请在 Studio 导航窗格中选择 **日志记录**。默认情况下，中心窗格按时间顺序（最新条目在前）列出日志内容，并按日期分隔。您可以：

- 按列标题排序显示。
- 通过指定日期间隔或在 **搜索** 框中输入文本来筛选显示。要在使用搜索后返回标准显示，请清除 **搜索** 框中的文本。

## 生成报告

您可以生成包含配置日志数据的 CSV 和 HTML 报告。

- CSV 报告包含指定时间间隔内的所有日志记录数据。数据库中的分层数据被展平为单个 CSV 表。数据在文件中没有优先级。不使用任何格式，也不假定人类可读性。该文件（名为 MyReport）以通用可消费格式包含数据。CSV 文件通常用于存档数据或作为 Microsoft Excel 等报告或数据操作工具的数据源。
- HTML 报告以人类可读的形式提供指定时间间隔内的日志记录数据。它提供了一个结构化、可导航的视图，用于查看更改。HTML 报告包含两个文件，分别名为 Summary 和 Details。Summary 列出高级操作：每个操作发生的时间、执行者和结果。单击每个操作旁边的**详细信息**链接会将您带到 Details 文件中的低级操作，其中提供了更多信息。

要生成配置日志报告，请在 Studio 导航窗格中选择 **日志记录**，然后在“操作”窗格中选择 **创建自定义报告**。

- 选择报告的日期范围。
- 选择报告格式：CSV、HTML 或两者。
- 浏览到要保存报告的位置。

## 删除配置日志内容

要删除配置日志，您必须具有特定的委派管理和 SQL Server 数据库权限。

- **委派管理：** 您必须具有允许读取部署配置的委派管理角色。完全管理员角色具有此权限。自定义角色必须在“其他权限”类别中选择“只读”或“管理”。

要在删除配置日志数据之前创建备份，自定义角色还必须在“日志记录权限”类别中选择“只读”或“管理”。

- **SQL Server 数据库：** 您必须具有有权从数据库中删除记录的 SQL Server 登录名。有两种方法可以执行此操作：
  - 使用具有 sysadmin 服务器角色的 SQL Server 数据库登录名，该角色允许您在数据库服务器上执行任何活动。或者，`serveradmin` 或 `setupadmin` 服务器角色允许您执行删除操作。
  - 如果您的部署需要更高的安全性，请使用映射到有权从数据库中删除记录的数据库用户的非 sysadmin 数据库登录名。
    a. 在 SQL Server Management Studio 中，创建一个服务器角色不是“sysadmin”的 SQL Server 登录名。
    b. 将登录名映射到数据库中的用户。SQL Server 会自动在数据库中创建一个与登录名同名的用户。
    c. 在“数据库角色成员身份”中，为数据库用户指定至少一个角色成员：`ConfigurationLoggingSchema_ROLE` 或 `dbowner`。

    有关详细信息，请参阅 SQL Server Management Studio 文档。

要删除配置日志：

1. 在 Studio 导航窗格中选择 **日志记录**。
2. 在“操作”窗格中选择 **删除日志**。
3. 系统会询问您是否要在删除日志之前创建日志备份。如果您选择创建备份，请浏览到保存备份存档的位置。备份将创建为 CSV 文件。

配置日志清除后，日志删除是发布到空日志的第一项活动。该条目提供有关谁在何时删除了日志的详细信息。

# 事件日志

以下文章列出并描述了 Citrix Virtual Apps and Desktops 中服务可以记录的事件。

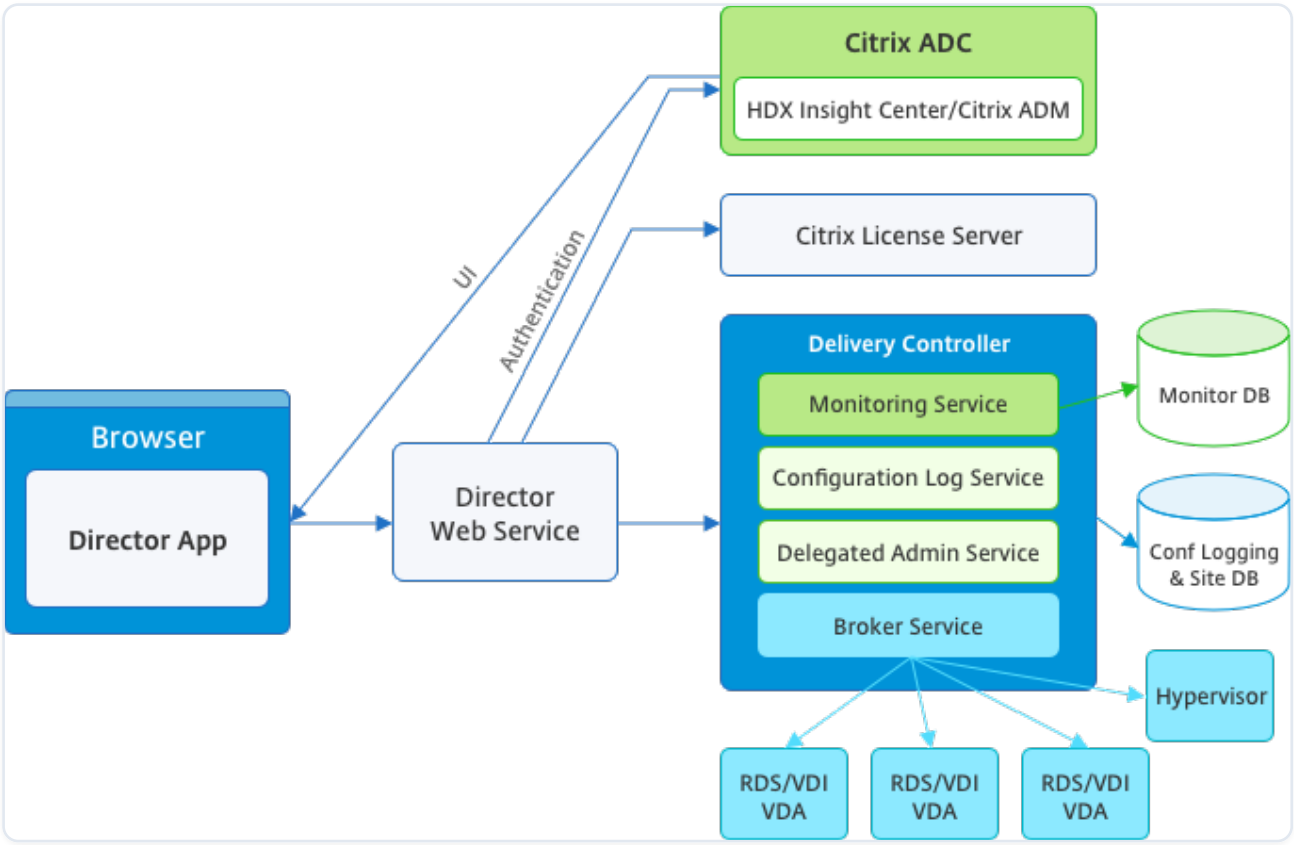
此信息并非详尽无遗。读者应查阅各个功能文章以获取更多事件信息。

- Citrix Broker 服务事件
- Citrix FMA 服务 SDK 事件
- Citrix Configuration 服务事件

- Citrix 委派管理服务事件

# 导向器

Director 是一个用于 Citrix Virtual Apps and Desktops 的监控和故障排除控制台。




Director 可以访问：

- 来自 Broker Agent 的实时数据，使用与 Analytics、Performance Manager 和 Network Inspector 集成的统一控制台。以下分析由 Citrix ADM 提供支持，用于识别您的 Citrix Virtual Apps™ 或 Desktops 环境中由于网络造成的瓶颈：
  - 用于健康状况和容量保障的性能管理
  - 历史趋势和网络分析
- 存储在 Monitor 数据库中的历史数据，用于访问 Configuration Logging 数据库。
- 来自 Citrix Gateway 的 ICA® 数据，使用 Citrix ADM。
  - 深入了解 Citrix Virtual Apps 或 Desktops 的虚拟应用程序、桌面和用户的最终用户体验。
  - 将网络数据与应用程序数据和实时指标关联起来，以实现有效的故障排除。
  - 与 Citrix Virtual Desktop 7 Director 监控工具集成。

Director 使用故障排除控制板，提供 Citrix Virtual Apps 或 Desktops 站点的实时和历史健康状况监控。此功能允许您实时查看故障，从而更好地了解最终用户的体验。

有关 Director 功能与 Delivery Controller (DC)、VDA 和任何其他相关组件兼容性的更多信息，请参阅 功能兼容性矩阵。

> **注意：**

> 随着 Meltdown 和 Spectre 推测执行侧信道漏洞的披露，Citrix 建议您安装相关的缓解补丁。这些补丁可能会影响 SQL Server 性能。有关更多信息，请参阅 Microsoft 支持文章：保护 SQL Server 免受 Spectre 和 Meltdown 侧信道漏洞攻击。Citrix 建议您在生产环境中推出补丁之前，测试规模并规划工作负载。

> Director 默认作为网站安装在 Delivery Controller 上。有关先决条件和其他详细信息，请参阅本版本的系统要求文档。有关 Director 安装和配置的具体信息，请参阅安装和配置 Director。

# 登录 Director

Director 网站位于 https 或 `http://<Server FQDN>/Director`。

如果多站点部署中的某个站点出现故障，则在尝试连接到该故障站点时，登录时间会稍长一些。

# 将 Director 与 PIV 智能卡身份验证结合使用

Director 现在支持基于个人身份验证 (PIV) 的智能卡身份验证登录。此功能对于使用基于智能卡的身份验证进行访问控制的组织和政府机构非常有用。 智能卡身份验证需要在 Director 服务器和 Active Directory 中进行特定配置。配置步骤详见配置 PIV 智能卡身份验证。

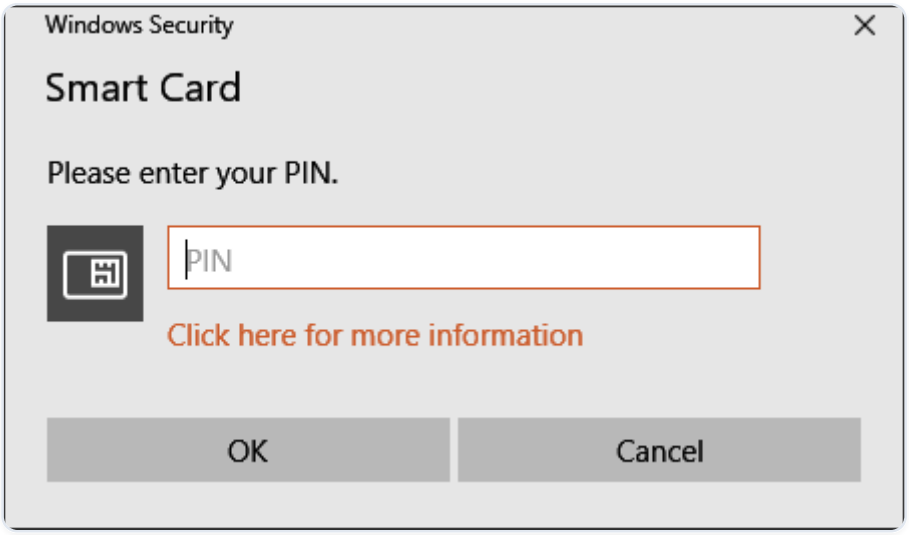
> **注意：**

> 智能卡身份验证仅支持来自同一 Active Directory 域的用户。

> 完成所需配置后，您可以使用智能卡登录 Director：

1. 将智能卡插入智能卡读卡器。
2. 打开浏览器并访问 Director URL，`https://<directorfqdn>/Director`。
3. 从显示的列表中选择一个有效的用户证书。

4. 输入您的智能卡令牌。




5. 身份验证成功后，您无需在 Director 登录页面上输入额外凭据即可访问 Director。

# 将 Director 与集成 Windows 身份验证结合使用

通过集成 Windows 身份验证 (IWA)，加入域的用户可以直接访问 Director，而无需在 Director 登录页面上重新输入其凭据。使用集成 Windows 身份验证和 Director 的先决条件是：

- 在托管 Director 的 IIS 网站上启用集成 Windows 身份验证。安装 Director 时，会启用匿名身份验证和表单身份验证。为了支持集成 Windows 身份验证和 Director，请禁用匿名身份验证并启用 Windows 身份验证。对于非域用户的身份验证，表单身份验证必须保持启用状态。

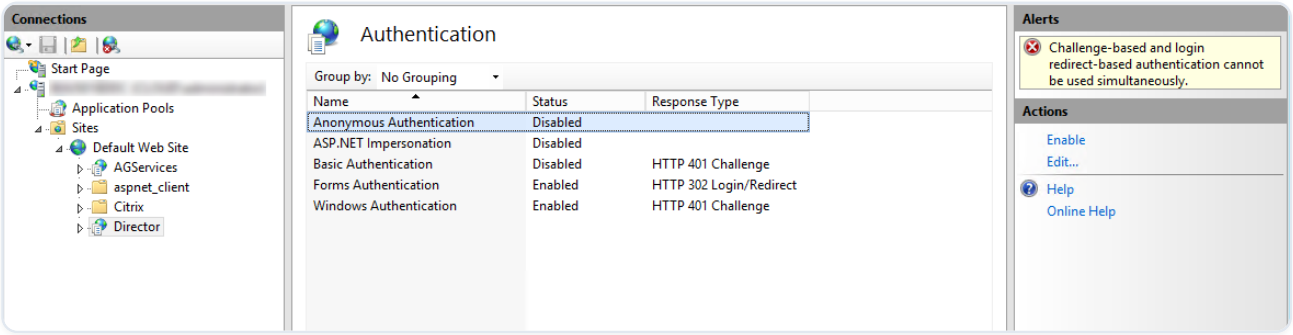
  a. 启动 IIS 管理器。

  b. 转至 **站点** \> **Default Web Site** \> **Director**。

  c. 选择**身份验证**。

  d. 右键单击**匿名身份验证**，然后选择**禁用**。

  e. 右键单击**Windows 身份验证**，然后选择**启用**。




- 为 Director 计算机配置 Active Directory 委派权限。仅当 Director 和 Delivery Controller™ 安装在不同的计算机上时才需要进行配置。

a. 在 Active Directory 计算机上，打开 Active Directory 管理控制台。
b. 在 Active Directory 管理控制台中，导航到 **域名** \> **计算机**。选择 Director 计算机。
c. 右键单击并选择**属性**。
d. 在“属性”中，选择**委派**选项卡。
e. 选择选项**信任此计算机以委派给任何服务（仅限 Kerberos）**。

- 用于访问 Director 的浏览器必须支持集成 Windows 身份验证。Firefox 和 Chrome 中可能需要额外的配置步骤。有关详细信息，请参阅浏览器文档。
- 监控服务必须运行 Microsoft .NET Framework 4.5.1 或 Director 系统要求中列出的更高版本。有关详细信息，请参阅系统要求。

当用户从 Director 注销或会话超时时，将显示登录页面。在登录页面上，用户可以将身份验证类型设置为**自动登录**或**用户凭据**。

# 界面视图

Director 提供针对特定管理员量身定制的不同界面视图。产品权限决定了显示的内容和可用的命令。

例如，技术支持管理员会看到一个针对技术支持任务量身定制的界面。Director 允许技术支持管理员搜索报告问题的用户，并显示与该用户相关的活动。例如，用户应用程序和进程的状态。他们可以通过执行以下操作快速解决问题：结束无响应的应用程序或进程、在用户计算机上执行影子操作、重新启动计算机或重置用户配置文件。

相比之下，完全管理员可以查看和管理整个站点，并可以对多个用户和计算机执行命令。仪表板提供了部署关键方面的概述，例如会话状态、用户登录和站点基础结构。信息每分钟更新一次。如果出现问题，会自动显示有关已发生的故障数量和类型的详细信息。

有关 Director 中各种角色及其权限的详细信息，请参阅委派管理和 Director

# 由 Google Analytics 收集使用数据

Director 服务在安装 Director 后开始使用 Google Analytics 收集使用数据。收集有关趋势页面使用情况和 OData API 调用分析的统计信息。分析数据收集符合 Citrix 隐私策略。安装 Director 时，数据收集默认启用。

要选择退出 Google Analytics 数据收集，请编辑安装 Director 的计算机上的注册表项。如果注册表项不存在，请创建并将其设置为所需值。更改注册表项值后，请刷新 Director 实例。

**注意：**不正确使用注册表编辑器可能会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证可以解决因不正确使用注册表编辑器而导致的问题。使用注册表编辑器风险自负。Citrix 建议您在更改 Windows 注册表之前对其进行备份。

位置：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名称：DisableGoogleAnalytics

值：0 = 启用（默认），1 = 禁用

您可以使用以下 PowerShell cmdlet 禁用 Google Analytics 的数据收集功能：

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

# 新功能指南

Director 具有产品内指南，该指南使用 Pendo 深入了解 Director 当前版本中发布的新功能。快速概述与适当的产品内消息相结合，可帮助您了解产品中的新增功能。

要选择退出此功能，请按照以下说明在安装 Director 的计算机上编辑注册表项。如果注册表项不存在，请创建并将其设置为所需值。更改注册表项值后，刷新 Director 实例。

**注意：**

不正确地使用注册表编辑器会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证能够解决因不正确使用注册表编辑器而导致的问题。请自行承担使用注册表编辑器的风险。Citrix 建议您在更改 Windows 注册表之前对其进行备份。

位置：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名称：DisableGuidedHelp

值：0 = 启用（默认），1 = 禁用

您可以使用以下 PowerShell cmdlet 禁用产品内指南：

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



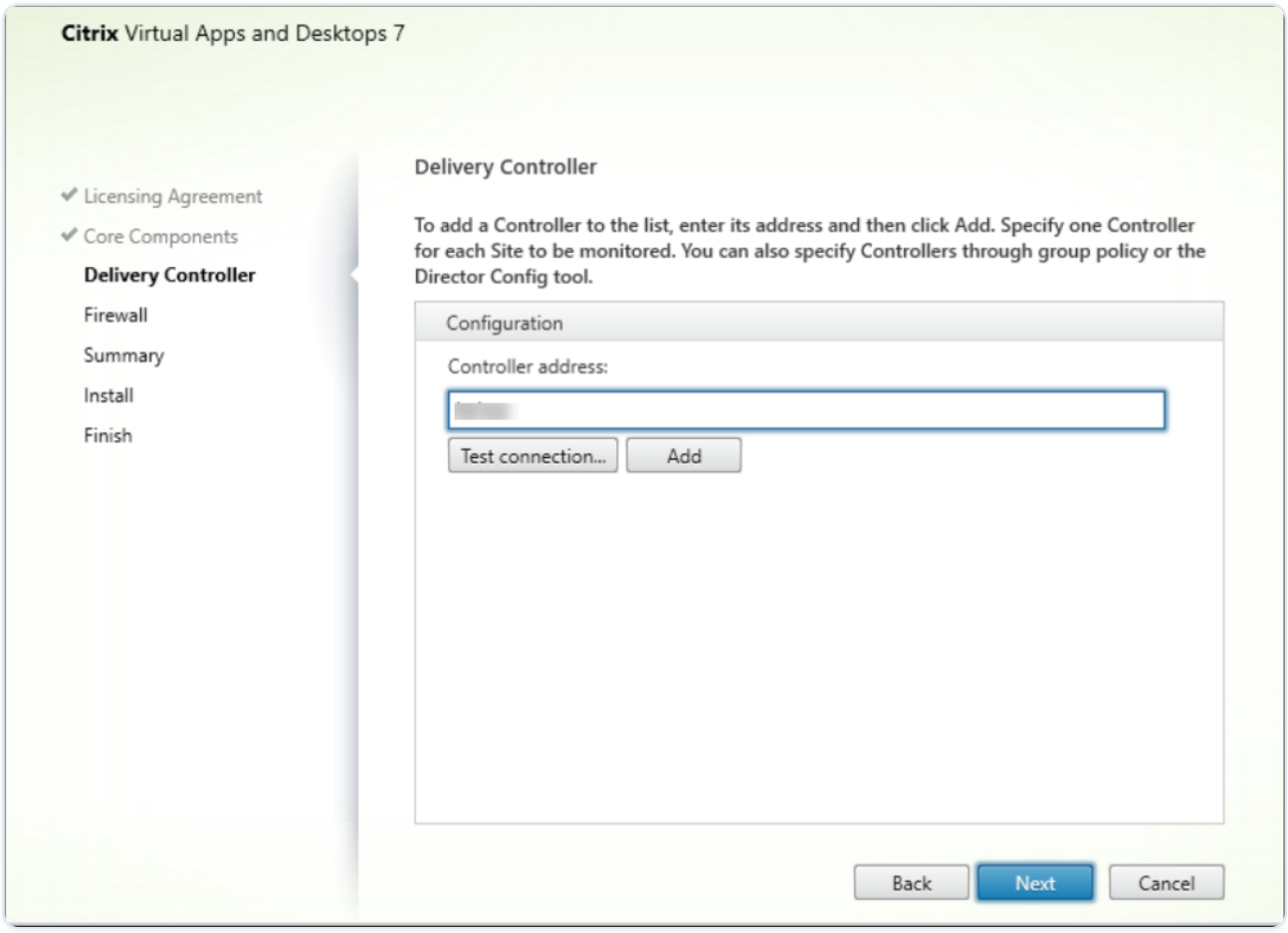
New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

# 安装和配置

## 安装 Director

使用适用于 Citrix Virtual Apps and Desktops 的完整产品 ISO 安装程序安装 Director，该安装程序会检查必备条件、安装所有缺失的组件、设置 Director 网站并执行基本配置。有关必备条件和其他详细信息，请参阅本版本的 系统要求 文档。此版本的 Director 不兼容 6.5 之前的 Virtual Apps 部署或 7 之前的 Virtual Desktops 部署。 ISO 安装程序提供的默认配置可处理典型部署。如果安装期间未包含 Director，请使用 ISO 安装程序添加 Director。要添加任何其他组件，请重新运行 ISO 安装程序并选择要安装的组件。有关使用 ISO 安装程序的信息，请参阅安装文档中的 安装核心组件。Citrix 建议您仅使用完整产品 ISO 安装程序进行安装，而不是 .MSI 文件。

当 Director 安装在 Controller 上时，它会自动将 localhost 配置为服务器地址，并且 Director 默认与本地 Controller 通信。要将 Director 安装在远离 Controller 的专用服务器上，系统会提示您输入 Controller 的 FQDN 或 IP 地址。




**注意：**

单击“**添加**”以添加要监视的 Controller。

Director 默认与指定的 Controller 通信。对于您监视的每个站点，仅指定一个 Controller 地址。如果您指定的 Controller 出现故障，Director 会自动发现同一站点中的所有其他 Controller 并回退到这些 Controller。

**注意：**

Director 不在 Controller 之间进行负载平衡。

为保护浏览器与 Web 服务器之间的通信安全，Citrix® 建议您在托管 Director 的 IIS 网站上实施 TLS。有关说明，请参阅 Microsoft IIS 文档。启用 TLS 不需要 Director 配置。

# 部署和配置 Director

当 Director 用于包含多个站点的环境中时，请务必同步安装了 Controller、Director 和其他核心组件的所有服务器上的系统时钟。否则，这些站点可能无法在 Director 中正确显示。

> **重要提示：**
>
> 为保护通过网络以纯文本形式发送的用户名和密码的安全，请仅允许使用 HTTPS 连接 Director，而不允许使用 HTTP。某些工具能够读取 HTTP（未加密）网络数据包中的纯文本用户名和密码，这可能会给用户带来潜在的安全风险。

## 配置权限

要登录 Director，具有 Director 权限的管理员必须是 Active Directory 域用户，并且必须具有以下权限：

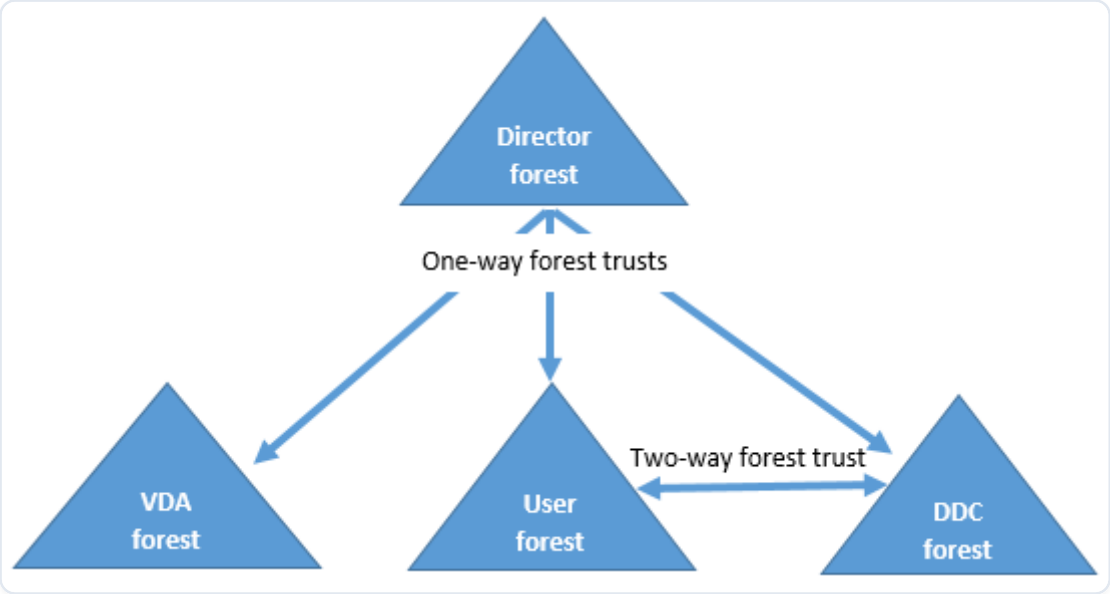
- 在所有要搜索的 Active Directory 林中具有读取权限（请参阅 高级配置）。
- 已配置的委派管理员角色（请参阅 委派管理和 Director）。
- 要对用户进行影子操作，必须使用 Microsoft 组策略为 Windows 远程协助配置管理员。此外：
  - 安装 VDA 时，请确保在所有用户设备上启用 Windows 远程协助功能（默认情况下处于选中状态）。
  - 在服务器上安装 Director 时，请确保已安装 Windows 远程协助（默认情况下处于选中状态）。但是，默认情况下，它在服务器上处于禁用状态。Director 无需启用此功能即可向最终用户提供帮助。Citrix 建议禁用此功能以提高服务器的安全性。
  - 要使管理员能够启动 Windows 远程协助，请通过使用适用于远程协助的相应 Microsoft 组策略设置授予他们所需的权限。有关信息，请参阅 CTX127388：如何为 Desktop Director 启用远程协助。

# 高级配置

Director 支持跨林配置的多林环境，其中用户、交付控制器 (DC)、VDA 和 Director 位于不同的林中。这需要正确设置林之间的信任关系和配置设置。

## 多林环境中的推荐配置

推荐配置要求在林之间创建具有域范围身份验证的出站和入站林信任关系。




来自 Director 的信任关系使您能够排查位于不同林中的用户会话、VDA 和交付控制器中的问题。

Director 支持多林所需的高级配置通过在 Internet 信息服务 (IIS) 管理器中定义的设置进行控制。

> **重要提示：**
>
> 在 IIS 中更改设置时，Director 服务会自动重启并注销用户。
>
> 要使用 IIS 配置高级设置，请执行以下操作：

1. 打开 Internet 信息服务 (IIS) 管理器控制台。
2. 在默认网站下，转到 Director 网站。
3. 双击“**应用程序设置**”。
4. 双击某个设置以对其进行编辑。
5. 单击“**添加**”以添加新设置。

Director 使用 Active Directory 搜索用户并查找更多用户和计算机信息。默认情况下，Director 搜索以下域或林：

- 管理员帐户是成员。
- Director Web 服务器是成员（如果不同）。

Director 尝试使用 Active Directory 全局目录在林级别执行搜索。如果您没有在林级别搜索的权限，则仅搜索域。

搜索或查找来自其他 Active Directory 域或林的数据需要您明确设置要搜索的域或林。在 IIS 管理器中，将以下应用程序设置配置到 Director 网站：

```
Connector.ActiveDirectory.Domains = (user),(server)
```

值属性 user 和 server 分别表示 Director 用户（管理员）和 Director 服务器的域。

要启用来自额外域或林的搜索，请将域的名称添加到列表中，如本例所示：

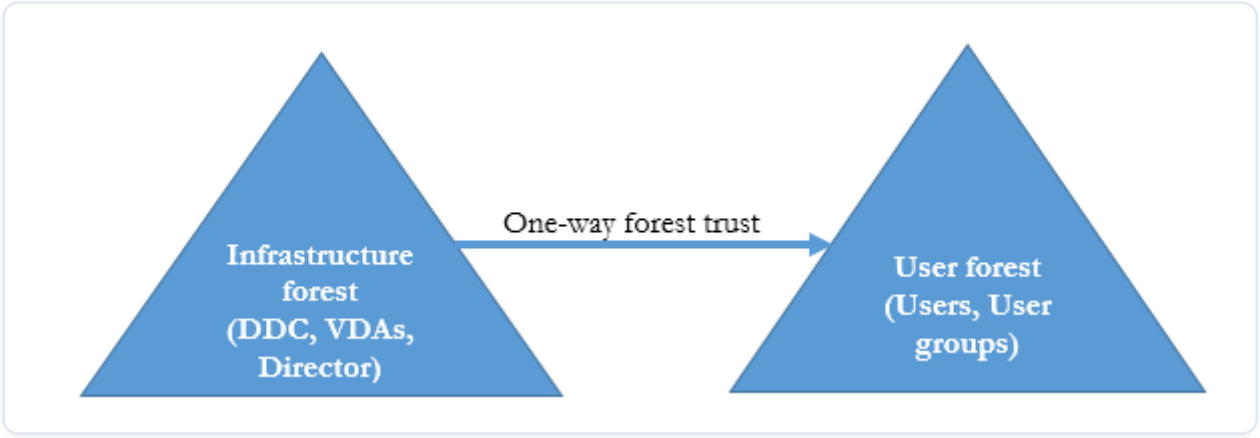
```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

对于列表中的每个域，Director 都会尝试在林级别执行搜索。如果您没有在林级别搜索的权限，则仅搜索域。

### 域本地组配置

大多数 Citrix 服务提供商 (CSP) 具有类似的环境设置，包括基础架构林中的 VDA、DC 和 Director。用户或用户组记录属于客户林。从基础架构林到客户林存在单向出站信任。

CSP 管理员通常在基础架构林中创建一个域本地组，并将客户林中的用户或用户组添加到此域本地组。




Director 可以支持这样的多林设置，并监控使用域本地组配置的用户的会话。

1. 在 IIS 管理器中，将以下应用程序设置添加到 Director 网站：

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true
   ```

```
DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
```

\<domain1\>\<domain2\> 是域本地组所在的林的名称。

2. 在 Citrix Studio 中将域本地组分配给交付组。
3. 重启 IIS 并重新登录 Director，以使更改生效。现在，Director 可以监视并显示这些用户的会话。

### 将站点添加到 Director

如果 Director 已安装，请将其配置为与多个站点配合使用。要进行配置，请在每个 Director 服务器上使用 IIS 管理器控制台更新应用程序设置中的服务器地址列表。

将每个站点中 Controller 的地址添加到以下设置：

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAController 和 SiteBController 是来自两个不同站点的 Delivery Controller 的地址。

### 禁用活动管理器中正在运行的应用程序的可见性

默认情况下，Director 中的活动管理器会显示用户会话的所有正在运行的应用程序列表。所有有权访问 Director 中活动管理器功能的管理员都可以查看此信息。对于委派管理员角色，这包括完全管理员、交付组管理员和技术支持管理员。

为了保护用户隐私及其正在运行的应用程序，您可以禁用“**应用程序**”选项卡以列出正在运行的应用程序。

**警告：**

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

1. 在 VDA 上，修改 `HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed` 处的注册表项。默认情况下，该项设置为 1。将值更改为 0，这意味着不从 VDA 收集信息，因此不在活动管理器中显示。

2. 在安装了 Director 的服务器上，修改控制正在运行的应用程序可见性的设置。默认情况下，该值为“true”，允许在“应用程序”选项卡中显示正在运行的应用程序。将值更改为“false”以禁用可见性。此选项仅影响 Director 中的活动管理器，而不影响 VDA。 修改以下设置的值：UI.TaskManager.EnableApplications = false

> **重要提示：**
>
> 要禁用正在运行的应用程序视图，请同时进行这两项更改，以确保数据不会显示在活动管理器中。

## 配置 PIV 智能卡身份验证

本文列出了在 Director 服务器和 Active Directory 中启用智能卡身份验证功能所需的配置。

> **注意：**
>
> 智能卡身份验证仅支持来自同一 Active Directory 域的用户。

### Director 服务器配置

在 Director 服务器上执行以下配置步骤：

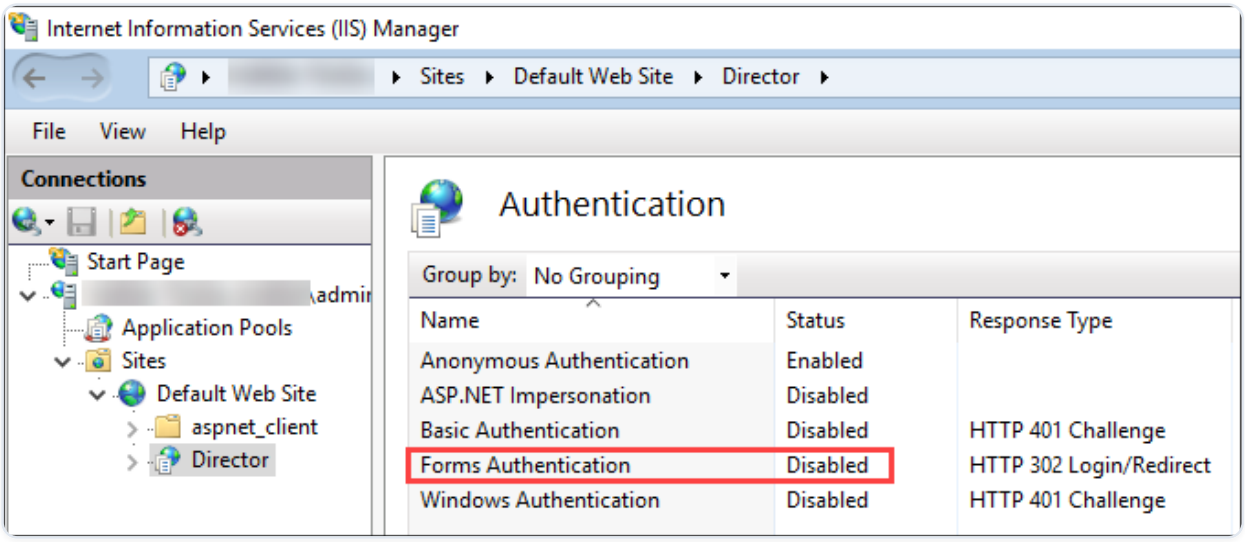
1. 安装并启用客户端证书映射身份验证。请遵循 Microsoft 文档 客户端证书映射身份验证 中的“**使用 Active Directory 进行客户端证书映射身份验证**”说明。
2. 在 Director 站点上禁用表单身份验证。

   启动 IIS 管理器。

   转至“**站点**” \> “**默认网站**” \> “**Director**”。

   选择“**身份验证**”。

   右键单击“**表单身份验证**”，然后选择“**禁用**”。



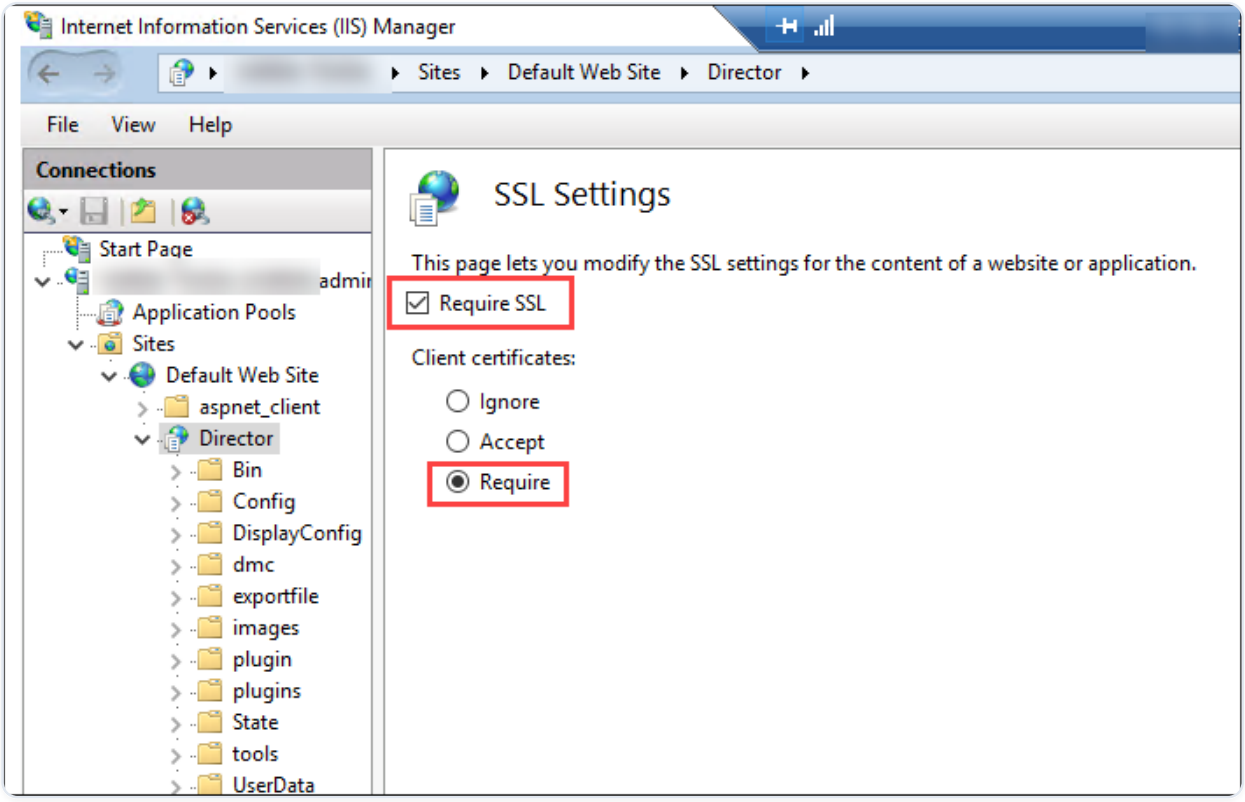

3. 为客户端证书身份验证配置 Director URL，使用更安全的 https 协议（而不是 HTTP）。

   a. 启动 IIS 管理器。

   b. 转至“**站点**” \> “**默认网站**” \> “**Director**”。

   c. 选择 **SSL Settings**。

   d. 选择 **要求 SSL** 和 **客户端证书** \> **要求**。




4. 更新 web.config。打开 web.config 文件（位于 `c:\inetpub\wwwroot\Director`）并使用文本编辑器打开。

在 `<system.webServer>` 父元素下，将以下代码片段添加为第一个子元素：

```
&lt;defaultDocument>

   &lt;files>

       &lt;add value="LogOn.aspx"/>

   &lt;/files>

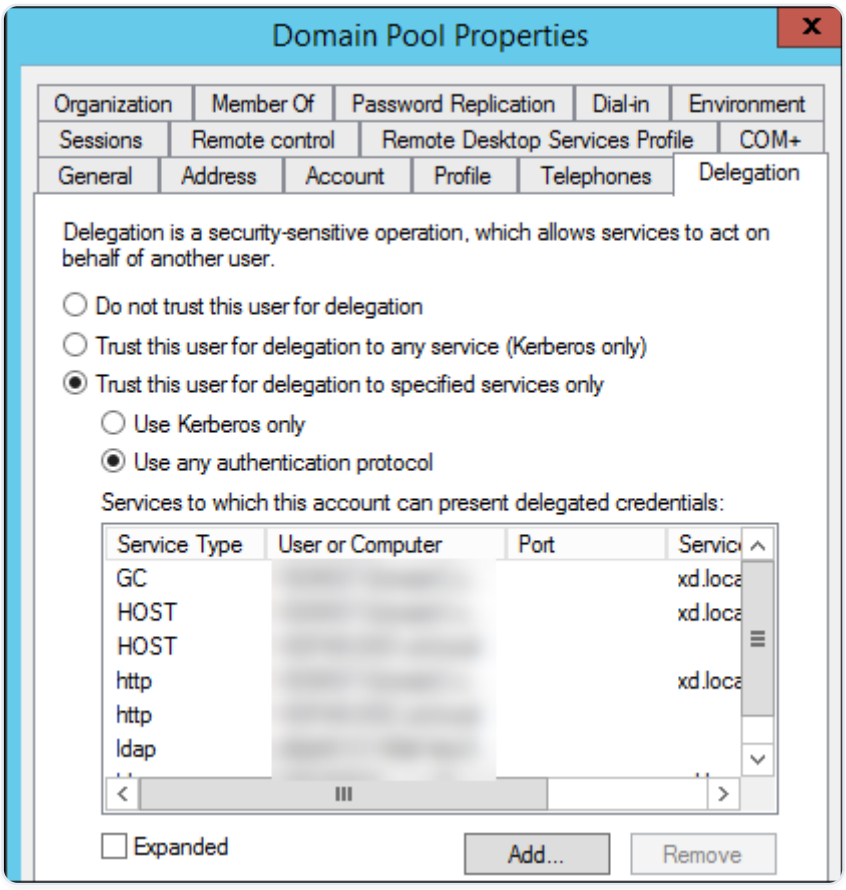
&lt;/defaultDocument>
```

### 活动目录配置

默认情况下，Director 应用程序使用 **Application Pool** 标识属性运行。智能卡身份验证需要委派，因此 Director 应用程序标识必须在服务主机上具有可信计算基 (TCB) 权限。

Citrix 建议您为应用程序池标识创建一个单独的服务帐户。根据 MSDN Microsoft 文章中的说明创建服务帐户并分配 TCB 权限，该文章是 Protocol Transition with Constrained Delegation Technical Supplement。

将新创建的服务帐户分配给 Director 应用程序池。下图显示了示例服务帐户 Domain Pool 的属性对话框。

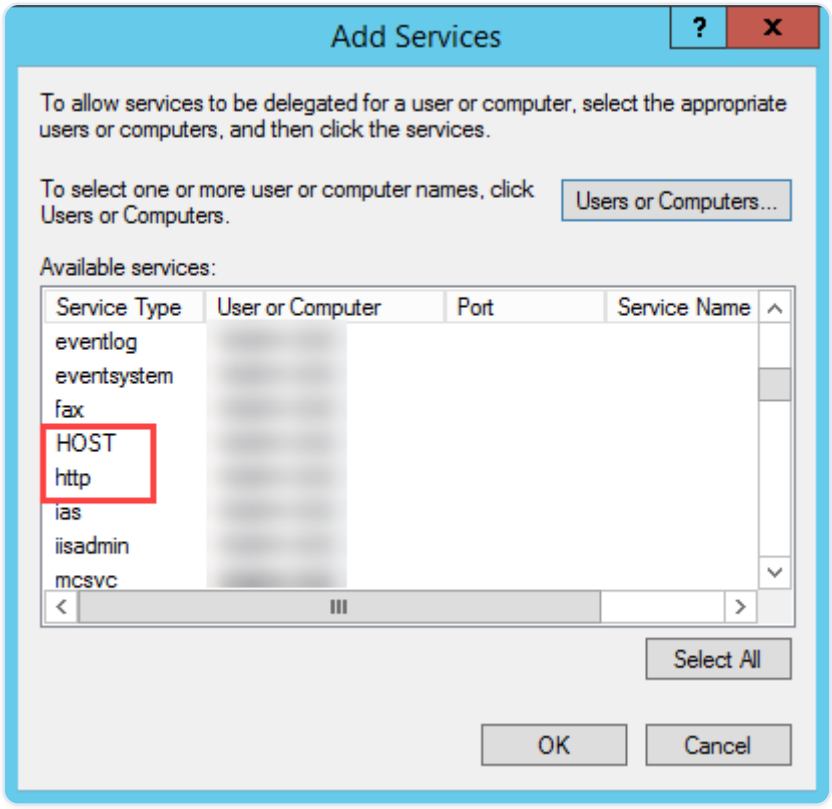



为此帐户配置以下服务：

- 交付控制器™：HOST, HTTP
- Director 配置：HOST, HTTP
- 活动目录：GC、LDAP

要配置，

1. 在用户帐户属性对话框中，单击“**添加**”。
2. 在“**添加服务**”对话框中，单击“用户”或“计算机”。
3. 选择 Delivery Controller 主机名。
4. 从“**可用服务**”列表中，选择 HOST 和 HTTP **服务类型**。




同样，为 **Director** 和 **Active Directory** 主机添加服务类型。

### Firefox 浏览器配置

要使用 Firefox 浏览器，请安装 OpenSC 0.17.0 中提供的 PIV 驱动程序。有关安装和配置说明，请参阅 在 Firefox 中逐步安装 OpenSC PKCS#11 模块。 有关 Director 中智能卡身份验证功能用法的信息，请参阅 Director 文章中的 将 Director 与基于 PIV 的智能卡身份验证结合使用 部分。

## 配置网络分析

> **注意：** 此功能的可用性取决于您组织的许可证和您的管理员权限。

> Director 与 Citrix ADM 集成，以提供网络分析和性能管理：

- 网络分析使用 Citrix ADM 中的 HDX™ Insight 报告，提供网络的应用程序和桌面上下文视图。借助此功能，Director 可为您的部署提供 ICA 流量的高级分析。
- 性能管理提供历史数据保留和趋势报告。通过历史数据保留而非实时评估，您可以创建趋势报告，包括容量和运行状况趋势。

在 Director 中启用此功能后，HDX Insight 报告会向 Director 提供更多信息：

- “趋势”页面中的“网络”选项卡显示了整个部署中应用程序、桌面和用户的延迟和带宽影响。
- “用户详细信息”页面显示了特定用户会话的延迟和带宽信息。

**限制：**

- 在“趋势”视图中，不收集早于 7 版本的 VDA 的 HDX 连接登录数据。对于早期 VDA，图表数据显示为 0。

要启用网络分析，您必须在 Director 中安装和配置 Citrix ADM。Director 需要 Citrix ADM 版本 11.1 Build 49.16 或更高版本。MAS 是在 Citrix XenServer 上运行的虚拟设备。通过网络分析，Director 可以通信并收集与您的部署相关的信息。

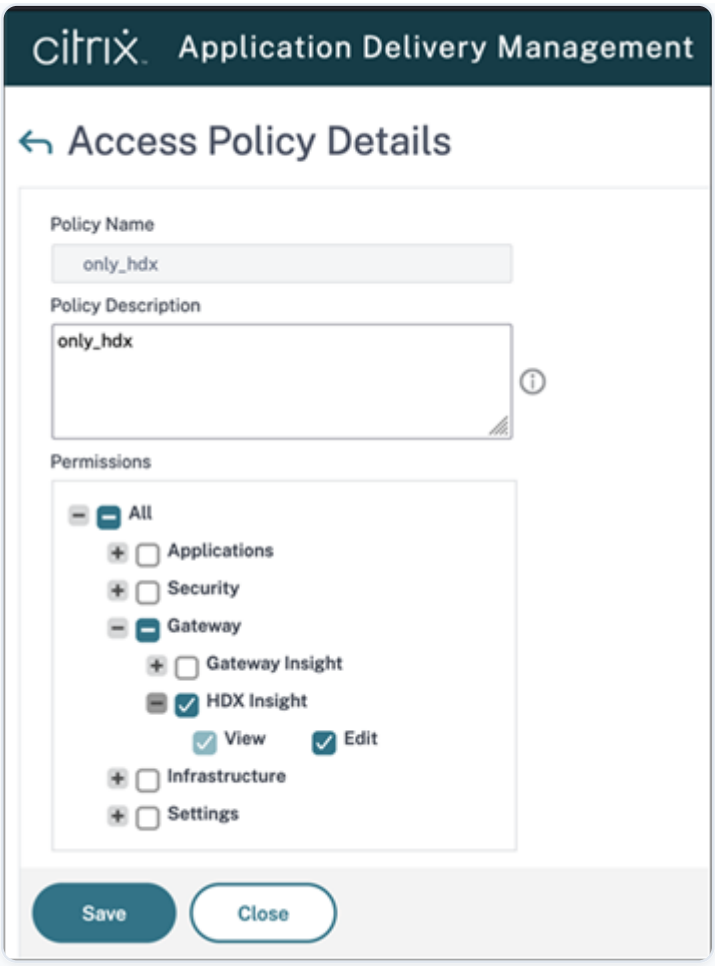
有关详细信息，请参阅 Citrix ADM 文档。

> **注意：** Citrix NetScaler Insight Center 已于 15 May 2018 达到其维护终止日期。请参阅 Citrix 产品矩阵。将 Director 与 Citrix ADM 集成以进行网络分析。要将您的 NetScaler Insight Center 迁移到 Citrix ADM，请参阅 从 NetScaler Insight Center 迁移到 Citrix ADM。

1. 在安装 Director 的服务器上，在 `C:\inetpub\wwwroot\Director\tools` 中找到 DirectorConfig 命令行工具，然后从命令提示符处使用参数 /configNetScaler 运行它。
2. 出现提示时，输入 Citrix ADM 计算机名称（FQDN 或 IP 地址）、用户名、密码、HTTPS 连接类型（优先于 HTTP），然后选择 Citrix ADM 集成。
3. 要验证更改，请注销并重新登录。

> **注意：**

> 出于安全原因，建议为 ADM 与 Director 集成创建一个自定义角色，该角色仅具有访问 HDX Insight 的足够权限。




有关详细信息，请参阅配置访问策略。

## 委派管理和 Director

委派管理使用三个概念：管理员、角色和作用域。权限基于管理员的角色和该角色的作用域。例如，管理员可能被分配了帮助台管理员角色，其作用域仅涉及一个站点的最终用户。

有关创建委派管理员的信息，请参阅主委派管理文章。

管理权限决定了向管理员显示的 Director 界面以及他们可以执行的任务。权限决定：

- 管理员可以访问的视图，统称为一个视图。
- 管理员可以查看和交互的桌面、计算机和会话。
- 管理员可以执行的命令，例如影子跟进用户会话或启用维护模式。

内置角色和权限还决定了管理员如何使用 Director：

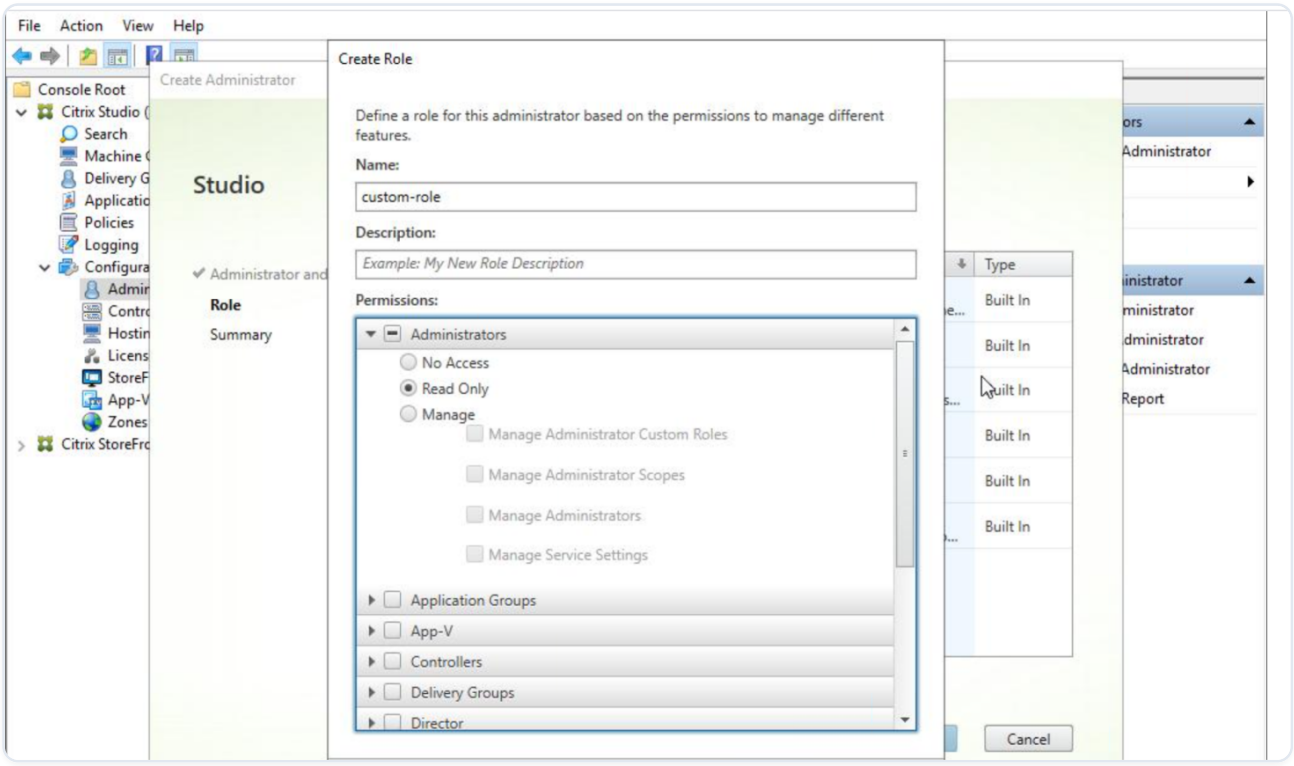
| 管理员角色 | DIRECTOR 中的权限 |
| --- | --- |
| 完全管理员 | 完全访问所有视图，并可以执行所有命令，包括影子跟进用户会话、启用维护模式和导出趋势数据。 |
| 交付组管理员 | 完全访问所有视图，并可以执行所有命令，包括影子跟进用户会话、启用维护模式和导出趋势数据。 |
| 只读管理员 | 可以访问所有视图并查看指定范围内的所有对象和全局信息。可以从 HDX™ 通道下载报告，并可以使用“趋势”视图中的“导出”选项导出趋势数据。无法执行任何其他命令或更改视图中的任何内容。 |
| 帮助台管理员 | 只能访问“技术支持”和“用户详细信息”视图，并且只能查看管理员被委派管理的对象。可以影子用户会话并为该用户执行命令。可以执行维护模式操作。可以对单会话操作系统计算机使用电源控制选项。无法访问“控制板”、“趋势”、“警报”或“筛选器”视图。无法对多会话操作系统计算机使用电源控制选项。 |
| 计算机目录管理员 | 只能访问“计算机详细信息”页面（基于计算机的搜索）。 |
| 主机管理员 | 无访问权限。Director 不支持此管理员，无法查看数据。 |

### 为 Director 管理员配置自定义角色

在 Studio 中，您还可以配置 Director 专用的自定义角色，以更紧密地匹配您的组织要求并更灵活地委派权限。例如，您可以限制内置的技术支持管理员角色，以便此管理员无法注销会话。

如果创建具有 Director 权限的自定义角色，则还必须为该角色授予其他通用权限：

- Delivery Controller™ 登录 Director 的权限 - 至少在管理员节点中具有只读访问权限
- 交付组权限，用于在 Director 中查看与这些交付组相关的数据 - 至少具有只读访问权限

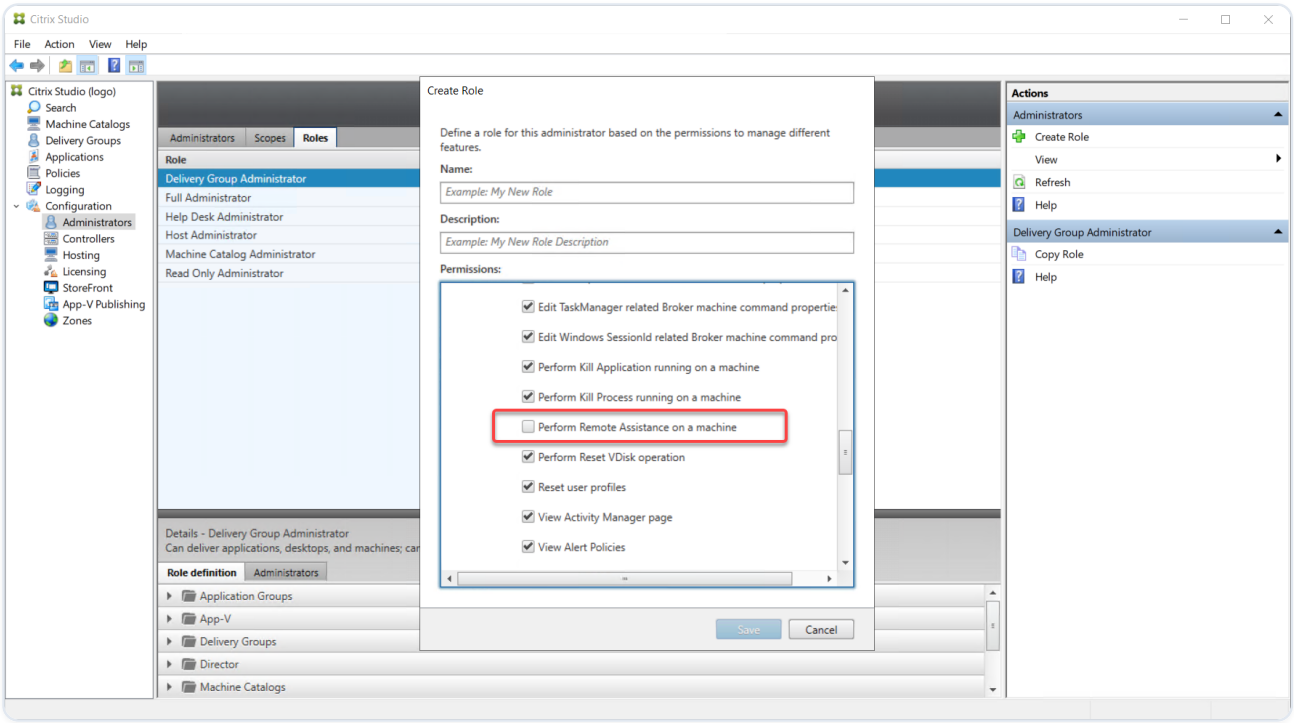



或者，您可以通过复制现有角色并为不同视图添加额外权限来创建自定义角色。例如，您可以复制帮助台角色并添加查看仪表板或筛选器页面的权限。

选择自定义角色的 Director 权限，其中包括：

- 执行终止在计算机上运行的应用程序
- 执行终止在计算机上运行的进程
- 在计算机上执行远程协助
- 重置用户配置文件
- 查看客户端详细信息页面
- 查看仪表板页面
- 查看筛选器页面
- 查看计算机详细信息页面
- 查看趋势页面
- 查看用户详细信息页面

在此示例中，影子会话（在计算机上执行远程协助）已关闭。




权限可能依赖于其他权限才能在 UI 上生效。例如，选择“**执行终止在计算机上运行的应用程序**”权限仅在角色具有权限的那些面板中启用“**结束应用程序**”功能。您可以选择以下面板权限：

- 查看筛选器页面
- 查看用户详细信息页面
- 查看计算机详细信息页面
- 查看客户端详细信息页面

此外，在其他组件的权限列表中，请考虑交付组的以下权限：

- 使用交付组成员身份启用/禁用计算机的维护模式。
- 使用交付组成员身份对 Windows 桌面计算机执行电源操作。
- 使用交付组成员身份对计算机执行会话管理。

# 保护 Director 部署

本文重点介绍了部署和配置 Director 时可能影响系统安全的方面。

## 配置 微软互联网信息服务 (IIS)

您可以使用受限的 IIS 配置来配置 Director。

### 应用程序池回收限制

您可以设置以下应用程序池回收限制：

- 虚拟内存限制：4,294,967,295

- 私有内存限制：StoreFront™ 服务器的物理内存大小
- 请求限制：4,000,000,000

**文件名扩展名**

您可以禁止未列出的文件扩展名。

Director 在请求筛选中需要以下文件扩展名：

- .aspx 扩展名
- .css 扩展名
- .html 文件
- .js
- ． png
- .svc 文件
- .gif 文件
- .json 文件
- 点woff
- woff2 文件
- “.ttf”

Director 在请求筛选中需要以下 HTTP 谓词。您可以禁止未列出的谓词。

- GET
- POST
- HEAD

Director 不需要：

- ISAPI 筛选器
- ISAPI 扩展
- CGI 程序
- FastCGI 程序

> **重要提示：**

- Director 需要完全信任。请勿将全局 .NET 信任级别设置为“高”或更低。
- Director 维护一个单独的应用程序池。要修改 Director 设置，请选择 Director 站点并进行修改。

### 配置用户权限

安装 Director 后，其应用程序池将获得以下权限：

- **作为服务登录**登录权限
- **调整进程的内存配额、生成安全审核**和**替换进程级令牌**权限

上述权限和特权是创建应用程序池时的正常安装行为。

您无需更改这些用户权限。Director 不使用这些特权，并且这些特权会自动禁用。

### Director 通信

在生产环境中，请使用 Internet 协议安全 (IPsec) 或 HTTPS 协议来保护 Director 与服务器之间传输的数据。

IPsec 是一组 Internet 协议标准扩展，可提供经过身份验证和加密的通信，并具有数据完整性和重放保护功能。由于 IPsec 是一组网络层协议，因此更高级别的协议无需修改即可使用它。HTTPS 使用传输层安全 (TLS) 协议来提供强大的数据加密。

**注意：**

- Citrix® 强烈建议您将 Director 控制台的访问权限限制在内部网络中。
- Citrix 强烈建议您不要在生产环境中启用对 Director 的不安全连接。
- 来自 Director 的安全通信需要为每个连接单独配置。
- 不建议使用 SSL 协议。请改用更安全的 TLS 协议。
- 使用 TLS 而非 IPsec 保护您与 Citrix ADC 的通信。

要保护 Director 与 Citrix Virtual Apps and Desktops 服务器之间的通信（用于监视和报告），请参阅 数据访问安全。

要保护 Director 与 Citrix ADC 之间的通信（用于 Citrix Insight），请参阅 配置网络分析。

要保护 Director 和许可证服务器之间的通信，请参阅保护许可证管理控制台。

### Director 安全隔离

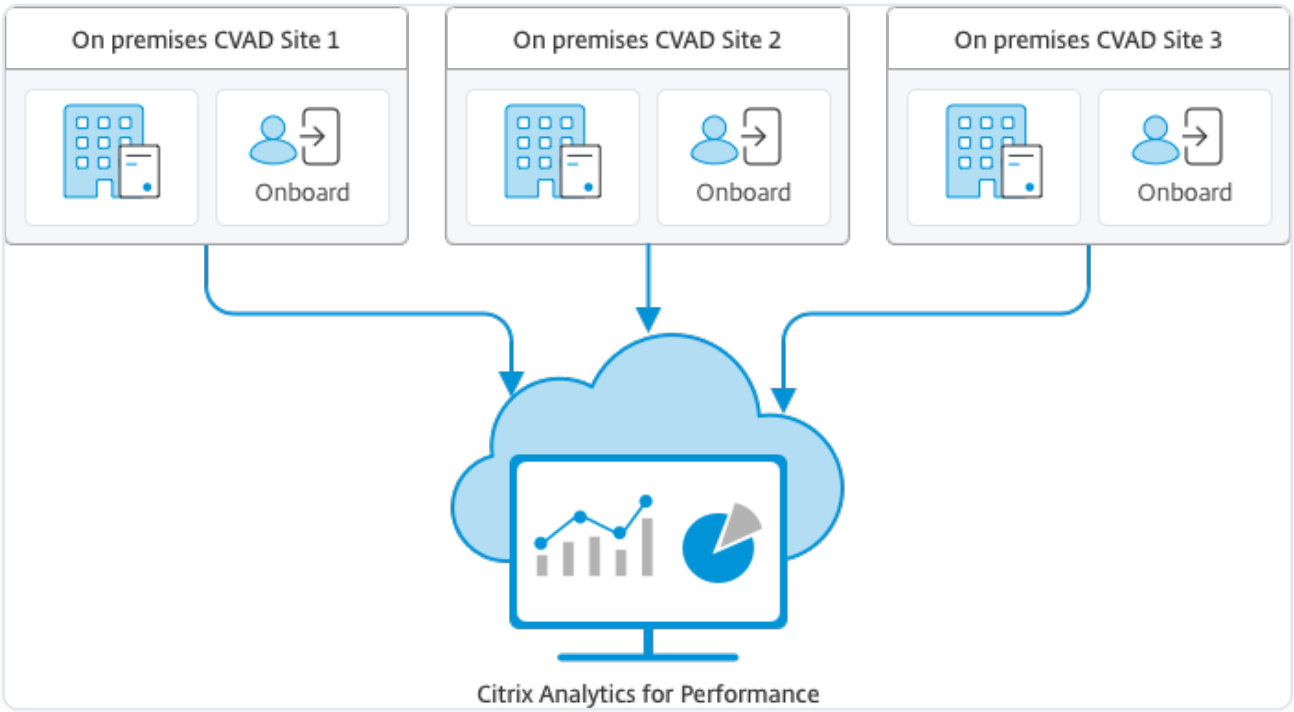
您可以将任何 Web 应用程序与 Director 部署在同一 Web 域（域名和端口）中。但是，这些 Web 应用程序中的任何安全风险都可能降低 Director 部署的安全性。如果需要更高程度的安全隔离，Citrix 建议您将 Director 部署在单独的 Web 域中。

## 使用 Citrix Analytics for Performance™ 配置本地站点

Citrix Analytics for Performance（性能分析）是 Citrix Analytics 云服务提供的综合性能监控解决方案。性能分析提供基于性能指标的高级洞察和分析。性能分析可帮助您监控和查看组织中一个或多个 Citrix Virtual Apps and Desktops™ 站点的使用情况和性能指标。

有关性能分析的更多信息，请参阅性能分析文章。

您可以将站点的性能数据发送到 Citrix Cloud™ 上的 Citrix Analytics for Performance，以利用其高级性能分析功能。要查看和使用性能分析，您必须首先在 **Director** 的“**分析**”选项卡中，使用 Citrix Analytics for Performance 配置本地站点。




性能分析以安全方式访问数据，并且不会将任何数据从 Citrix Cloud 传输到本地环境。

### 先决条件

要从 Director 配置 Citrix Analytics for Performance，无需安装任何新组件。请确保满足以下要求：

- 您的 Delivery Controller 和 Director 版本为 1912 CU2 或更高版本。有关详细信息，请参阅功能兼容性列表。

**注意：**

- 如果 Delivery Controller 运行的 Microsoft .NET Framework 版本低于 4.8，则从 Director 使用 Citrix Analytics for Performance 配置本地站点可能会失败。解决方法是将 Delivery Controller 中的 .NET Framework 升级到版本 4.8。LCM-9255。
- 当您从 Director 使用 Citrix Analytics for Performance 配置运行 Citrix Virtual Apps and Desktops 2012 版本的本地站点时，配置可能会在几个小时后或在 Delivery Controller 中重新启动 Citrix Monitor Service 后失败。“分析”选项卡在这种情况下会显示“未连接”状态。解决方法是在 Delivery Controller 的注册表中创建 Encryption 文件夹，位置：HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor，文件夹名称：Encryption。确保 CitrixMonitor 帐户对 Encryption 文件夹具有完全控制访问权限。重新启动 Citrix Monitor Service。DIR-14324。

- 只有完全管理员才能访问“**分析**”选项卡以执行此配置。
- 为了让性能分析访问性能指标，所有 Delivery Controller 和安装了 Director 的计算机都必须具有出站 Internet 访问权限。具体而言，请确保可以访问以下 URL：
  - Citrix 密钥注册：`https://*.citrixnetworkapi.net/`
  - 思杰云：`https://*.citrixworkspacesapi.net/`
  - 思杰分析：`https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` 如果交付控制器和 Director 计算机位于内网中，并且出站 Internet 访问通过代理服务器，请确保以下事项：
- 代理服务器必须允许上述 URL 列表。
- 在 Director 的 web.config 和 citrix.monitor.exe.config 文件中添加以下配置。确保将此配置添加到 **configuration** 标签内：

```
&lt;system.net>

    &lt;defaultProxy>

        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>
```

```
&lt;/system.net>
```

- Director web.config 位于安装 Director 的计算机上的 `C:\inetpub\wwwroot\Director\web.config`。
- citrix.monitor.exe.config 位于安装交付控制器的计算机上的 `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config`。

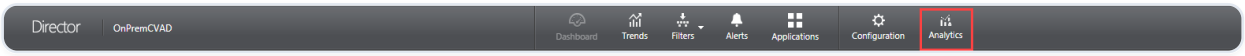
此设置由 Microsoft 在 IIS 上提供。有关详细信息，请参阅 `https://docs.microsoft.com/zh-cn/dotnet/framework/network-programming/proxy-configuration`。 配置文件中的 **defaultproxy** 字段控制 Director 和监视服务的出站访问。配置和与 Performance Analytics 的通信要求将 **defaultproxy** 字段设置为 **true**。现有策略可能会将此字段设置为 false。在这种情况下，您必须手动将此字段设置为 true。在进行更改之前，请备份配置文件。重新启动 Delivery Controller™ 上的监视服务以使更改生效。

- 您拥有 Citrix Analytics for Performance 的有效 Citrix Cloud 授权。
- 您的 Citrix Cloud 帐户是具有产品注册体验权限的管理员帐户。有关管理员权限的详细信息，请参阅修改管理员权限。

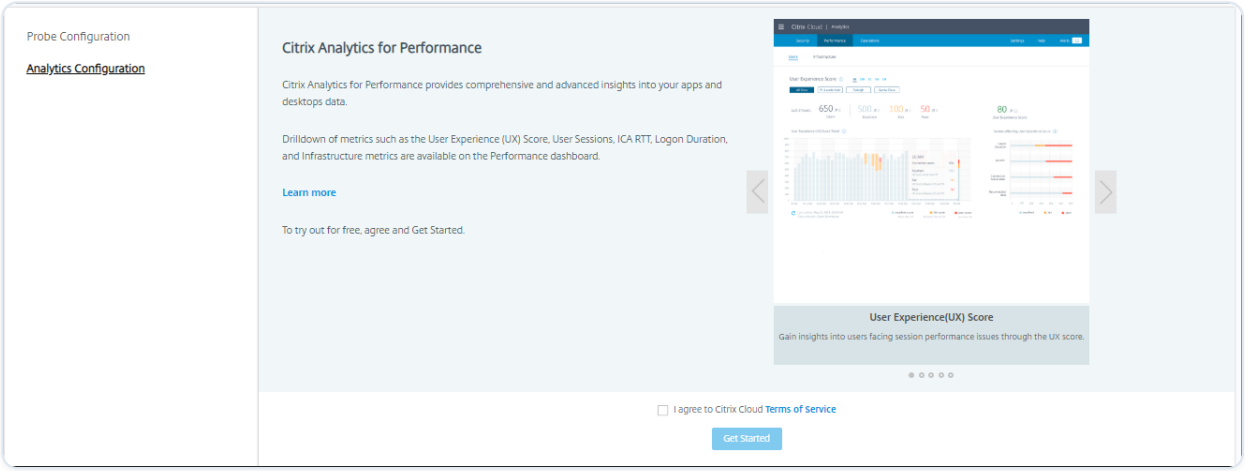
### 配置步骤

验证先决条件后，请执行以下操作：

1. 以完全管理员身份登录 Director，然后选择要使用 Performance Analytics 配置的站点。
2. 单击 **Analytics** 选项卡。此时将显示“**配置**”页面。

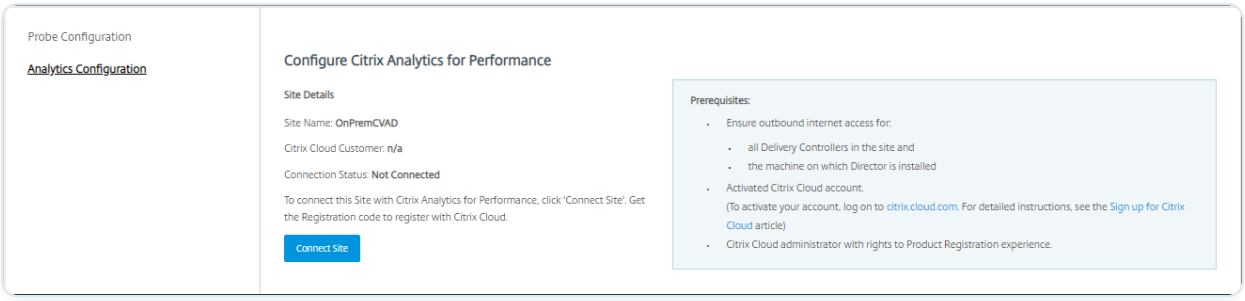



3. 查看步骤，选择服务条款，然后单击“**开始**”。




4. 查看先决条件并确保满足这些条件。查看站点详细信息。

5. 单击“**连接站点**”以开始配置过程。




6. 将生成一个唯一的 8 位注册码，用于将此站点注册到 Citrix Cloud。

   注册码(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-onboarding5.png)

7. 单击**复制代码**以复制代码，然后单击**在 Citrix Cloud 上注册**。
8. 您将被重定向到 Citrix Cloud 中的注册 URL。使用您的 Citrix Cloud 凭据登录并选择您的客户。
9. 在 Citrix Cloud 的“产品注册”页面中粘贴复制的注册代码。单击**继续**进行注册。查看注册详细信息，然后单击**注册**。

   在 Citrix Cloud 中注册(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-onboarding6.png)

10. 您的本地站点已在 Citrix Cloud 中注册。现在，从 **Director** 中，单击**分析**选项卡中的**转到分析**。

    转到分析(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-onboarding7.png)

11. Performance Analytics 在浏览器的新选项卡中打开。 Performance Analytics 仪表板(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-onboarding-pa-dashboard.png)

    如果您的 Citrix Cloud 会话已过期，您可能会被重定向到 Citrix.com 或 My Citrix 帐户登录页面。

12. 要向 Performance Analytics 注册多个站点，请从 Director 为每个站点重复上述配置步骤。所有已配置站点的指标都显示在 Performance Analytics 仪表板上。

    如果每个站点运行多个 Director 实例，请从任意一个 Director 实例进行配置。连接到该站点的所有其他 Director 实例将在配置过程后的下一次刷新时更新。

13. 要将您的站点与 Citrix Cloud 断开连接，请单击**断开站点连接**。此选项将删除现有配置。

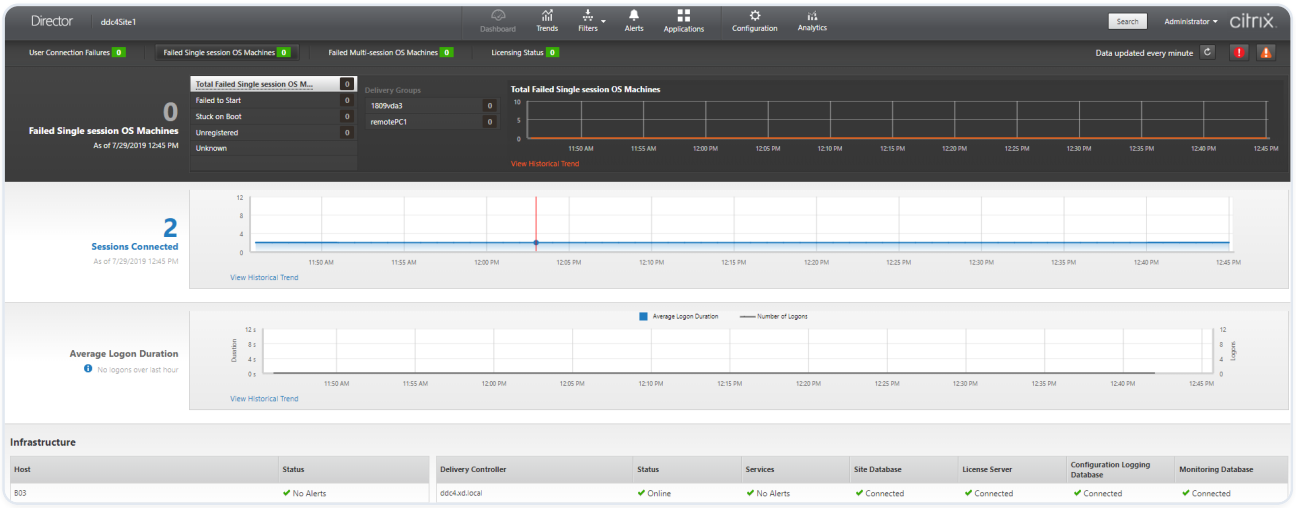
> **注意：**
>
> 首次配置站点时，来自站点的事件可能需要一些时间（大约一小时）才能处理完毕；这会导致 Performance Analytics 仪表板上指标的显示出现延迟。此后，事件会定期刷新。

> 断开连接后，旧帐户的数据传输会持续一段时间，直到新帐户的事件传输完毕。数据传输停止后大约一小时内，与旧帐户相关的分析仍会显示在 Performance Analytics 仪表板上。

> Citrix Analytics 服务授权到期后，最多需要一天时间才能停止向 Performance Analytics 发送站点指标。

# 站点分析

在拥有完整管理员权限的情况下，当您打开 Director 时，仪表板提供了一个集中位置来监控站点的运行状况和使用情况。




如果当前没有故障，并且在过去 60 分钟内没有发生故障，则面板将保持折叠状态。当出现故障时，特定的故障面板会自动显示。

> **注意：**
>
> 根据您组织的许可证和您的管理员权限，某些选项或功能可能不可用。

## Director 控制板上的面板

### 用户连接故障

过去 60 分钟内的连接故障。单击总数旁边的类别可查看该类型故障的指标。在相邻的表中，该数字按交付组细分。连接故障包括因达到应用程序限制而导致的故障。有关应用程序限制的详细信息，请参阅应用程序。

### 失败的单会话操作系统计算机或失败的多会话操作系统计算机

过去 60 分钟内按交付组细分的总故障。故障按类型细分，包括启动失败、卡在启动中和未注册。对于多会话操作系统计算机，故障还包括计算机达到最大负载。

### 许可状态

许可证服务器警报显示许可证服务器发送的警报以及解决警报所需的操作。需要许可证服务器版本 11.12.1 或更高版本。交付控制器警报显示控制器所见的许可状态详细信息，并由控制器发送。需要适用于 XenApp 7.6 或 XenDesktop 7.6 或更高版本的控制器。您可以在 Studio 中设置警报阈值。在 **Delivery Controllers** > **Details** > **Product Editions** > **PLT** 中显示的许可状态表示 **Premium** 而不是 **Platinum**。

### 宽限状态

Director 显示以下宽限状态之一。此信息从交付控制器中获取。

1. **未激活：** 未处于任何类型的许可证缓存模式。适用正常的许可限制。
2. **紧急宽限：** 当许可证服务器无法访问或在代理连接时无法获取许可证信息时生效。用户不受影响。Director 中显示的错误在许可证服务器可访问之前无法消除。
3. **宽限期已过期：** 紧急许可证缓存模式已过期。

有关详细信息，请参阅 许可证透支 和 许可证突发模式。

### 已连接会话

过去 60 分钟内所有交付组的已连接会话。

### 平均登录持续时间

最近 60 分钟的登录数据。左侧的大数字是该小时内的平均登录持续时间。早于 XenDesktop 7.0 的 VDA 的登录数据不包括在此平均值中。有关详细信息，请参阅 诊断用户登录问题。

### 基础结构

列出站点的基础架构——主机和控制器。对于来自 Citrix Hypervisor 或 VMware 的基础架构，您可以查看性能警报。例如，您可以配置 XenCenter，使其在托管服务器或虚拟机上的 CPU、网络 I/O 或磁盘 I/O 使用率超过指定阈值时生成性能警报。默认情况下，警报重复间隔为 60 分钟，但您也可以配置此项。有关详细信息，请参阅 Citrix Hypervisor 产品文档 中的 XenCenter 性能警报部分。

> **注意：**

> 如果特定指标没有显示图标，则表示您使用的主机类型不支持此指标。例如，System Center Virtual Machine Manager (SCVMM) 主机、AWS 和 CloudStack 不提供运行状况信息。

> 继续使用以下选项（在以下部分中进行了说明）来排查问题：

- 控制用户计算机电源
- 阻止连接到计算机

## 监视会话

如果会话断开连接，它仍然处于活动状态，并且其应用程序会继续运行，但用户设备不再与服务器通信。

| 操作 | 描述 |
| --- | --- |
| 查看用户当前连接的计算机或会话 | 在“活动管理器”和“用户详细信息”视图中，查看用户当前连接的计算机或会话以及该用户有权访问的所有计算机和会话的列表。要访问此列表，请单击用户标题栏中的会话切换器图标。有关详细信息，请参阅 恢复会话。 |
| 查看所有交付组中连接会话的总数 | 在“控制板”的“**已连接会话**”窗格中，查看过去 60 分钟内所有交付组的已连接会话总数。然后单击大总数，这将打开“筛选器”视图，您可以在其中根据选定的交付组和范围以及跨交付组的使用情况显示图形会话数据。 |
| 结束空闲会话 | “会话筛选器”视图显示与所有活动会话相关的数据。根据关联用户、交付组、会话状态和超过阈值时间段的空闲时间筛选会话。从筛选列表中，选择要注销或断开连接的会话。有关详细信息，请参阅 应用程序故障排除。 |
| 查看更长时间段的数据 | 在“趋势”视图中，选择“**会话**”选项卡，以深入查看更长时间段内（即早于最近 60 分钟的会话总数）已连接和已断开连接会话的更具体使用数据。要查看此信息，请单击“**查看历史趋势**”。 |

> **注意：**

如果用户设备运行的是旧版虚拟投递代理 (VDA)（例如早于版本 7 的 VDA 或 Linux VDA），Director 无法显示有关会话的完整信息。相反，它会显示一条消息，指示信息不可用。

**桌面分配规则限制：** Citrix Studio 允许将多个桌面分配规则 (DAR) 分配给交付组中单个 VDA 的不同用户或用户组。StoreFront™ 根据登录用户的 DAR，显示具有相应**显示名称**的已分配桌面。但是，Director 不支持 DAR，并且无论登录用户是谁，都使用交付组名称显示已分配的桌面。因此，您无法在 Director 中将特定桌面映射到计算机。 您可以使用以下 PowerShell 命令将 StoreFront 中显示的已分配桌面映射到 Director 中显示的交付组名称：

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq
"\&lt;Name on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property
Name, Uid
```

### 会话传输协议

在“**会话详细信息**”面板中查看当前会话的 HDX 连接类型所使用的传输协议。此信息适用于在 VDA 7.13 或更高版本上启动的会话。

传输协议(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/sessions-transport-protocol.png)

- 对于 **HDX™** 连接类型，
  - 如果 HDX 连接使用 EDT，则协议显示为 **UDP**。
  - 如果 HDX 连接使用 TCP，则协议显示为 **TCP**。
- 对于 **RDP** 连接类型，协议显示为 **n/a**。

当自适应传输配置后，会话传输协议会根据网络状况在 EDT（通过 UDP）和 TCP 之间动态切换。如果无法使用 EDT 建立 HDX 会话，则会回退到 TCP 协议。

有关自适应传输配置的更多信息，请参阅自适应传输。

## 导出报告

您可以导出趋势数据以生成常规使用情况和容量管理报告。导出支持 PDF、Excel 和 CSV 报告格式。PDF 和 Excel 格式的报告包含以图表形式表示的趋势。CSV 格式的报告包含可用于生成视图或存档的表格数据。

要导出报告：

1. 转到“**趋势**”选项卡。

2. 设置筛选条件和时间段，然后单击“**应用**”。趋势图和表格将填充数据。
3. 单击**导出**，然后输入报告的名称和格式。

Director 根据您选择的筛选条件生成报告。如果更改筛选条件，请在单击**导出**之前单击**应用**。

> **注意：**
>
> 导出大量数据会导致 Director 服务器、Delivery Controller 和 SQL 服务器上的内存和 CPU 消耗显著增加。为实现最佳导出性能，支持的并发导出操作数量和可导出的数据量已设置为默认限制。

### 支持的导出限制

导出的 PDF 和 Excel 报告包含所选筛选条件的完整图表。但是，所有报告格式中的表格数据都会在超出表中行数或记录数的默认限制后被截断。支持的默认记录数是根据报告格式定义的。

您可以通过在 Internet Information Services (IIS) 中配置 Director 应用程序设置来更改默认限制。

| 报告格式 | 默认支持的记录数 | DIRECTOR 应用程序设置中的字段 | 支持的最大记录数 |
|---|---|---|---|
| PDF | 500 | UI.ExportPdfDrilldownLimit | 5000 |
| 艾赛尔 | 100,000 | UI.ExportExcelDrilldownLimit | 100,000 |
| CSV | 100,000（在**会话**选项卡中为 10,000,000） | UI.ExportCsvDrilldownLimit | 100,000 |

要更改可导出记录数的限制：

1. 打开 IIS 管理器控制台。
2. 在默认网站下，转到 Director 网站。
3. 双击 **应用程序设置**。
4. 根据需要编辑或添加以下字段的设置：UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit 或 UI.ExportCsvDrilldownLimit。

在 Application Settings 中添加这些字段值将覆盖默认值。

> **警告：**
>
> 将字段值设置为大于支持的最大记录数可能会影响导出性能，并且不受支持。

### 错误处理

本节提供有关处理您在导出操作期间可能会遇到的错误的信息。

- **Director 已超时**

此错误可能由于网络问题，或 Director 服务器上或 Monitor Service 的资源使用率过高而发生。

默认超时持续时间为 100 秒。要增加 Director Service 的超时持续时间，请在 Internet Information Services (IIS) 的 Director 应用程序设置中设置 **Connector.DataServiceContext.Timeout** 字段的值：

1. 打开 IIS 管理器控制台。
2. 在默认网站下，转到 Director 网站。
3. 双击“**应用程序设置**”。
4. 编辑值 **Connector.DataServiceContext.Timeout**。

- **Monitor 已超时**

此错误可能由于网络问题，或 Monitor Service 的资源使用率过高或在 SQL 服务器上而发生。

要增加 Monitor Service 的超时持续时间，请在 Delivery Controller 上运行以下 PowerShell 命令：

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds &lt;timeout value>
```

- **最大并发导出或预览操作正在进行**

Director 支持一个导出或预览实例。如果出现“**最大并发导出或预览操作正在进行**”错误，请稍后重试下一次导出操作。

可以增加并发导出或预览操作的数量，但这可能会影响 Director 的性能，并且不受支持：

1. 打开 IIS 管理器控制台。

2. 在默认网站下，转到 Director 网站。
3. 双击“**应用程序设置**”。
4. 编辑值 **UI.ConcurrentExportLimit**。

- **Director 中磁盘空间不足**

每个导出操作在 Windows Temp 文件夹中最多需要 2 GB 硬盘空间。在 Director 服务器上清理空间或添加更多硬盘空间后，重试导出。

## Monitor 热修复程序

要查看安装在特定计算机 VDA（物理或虚拟机）上的热修复程序，请选择**计算机详细信息**视图。

## 控制用户计算机电源状态

要控制在 Director 中选择的计算机的状态，请使用电源控制选项。这些选项适用于单会话操作系统计算机，但可能不适用于多会话操作系统计算机。

**注意：**

此功能不适用于物理计算机或使用远程电脑访问的计算机。

| 命令 | 功能 |
| --- | --- |
| **重新启动** | 执行 VM 的有序（软）关机，并在重新启动 VM 之前单独停止所有正在运行的进程。例如，选择在 Director 中显示为“启动失败”的计算机，然后使用此命令重新启动它们。 |
| **强制重新启动** | 重新启动 VM，而不首先执行任何关机过程。此命令的工作方式与拔下物理服务器电源，然后重新插入并重新打开电源相同。 |
| **关机** | 执行 VM 的有序（软）关机。所有正在运行的进程都将单独停止。 |
| **强制关机** | 关闭 VM，而不首先执行任何关机过程。此命令的工作方式与拔下物理服务器电源相同。它可能无法始终关闭所有正在运行的进 |

| 命令 | 功能 |
| --- | --- |
| | 程，如果以这种方式关闭 VM，则存在数据丢失的风险。 |
| **挂起** | 挂起正在运行的 VM 的当前状态，并将该状态存储在默认存储库中的文件中。此选项允许您关闭 VM 的主机服务器，稍后，在重新启动它之后，恢复 VM，使其返回到原始运行状态。 |
| **恢复** | 恢复已挂起的 VM 并将其还原到其原始运行状态。 |
| **启动** | 在 VM 关闭时启动它（也称为冷启动）。 |

如果电源控制操作失败，请将鼠标悬停在警报上，将显示一个弹出消息，其中包含有关故障的详细信息。

## 阻止连接到计算机

使用维护模式暂时阻止新连接，同时由相应的管理员对映像执行维护任务。

在计算机上启用维护模式后，在禁用该模式之前，不允许建立新连接。如果用户当前已登录，则维护模式会在所有用户注销后立即生效。对于未注销的用户，请发送消息通知他们计算机将在特定时间关闭，并使用电源控制强制关闭计算机。

1. 选择计算机，例如从“用户详细信息”视图中选择，或在“筛选器”视图中选择一组计算机。
2. 选择**维护模式**，然后打开该选项。

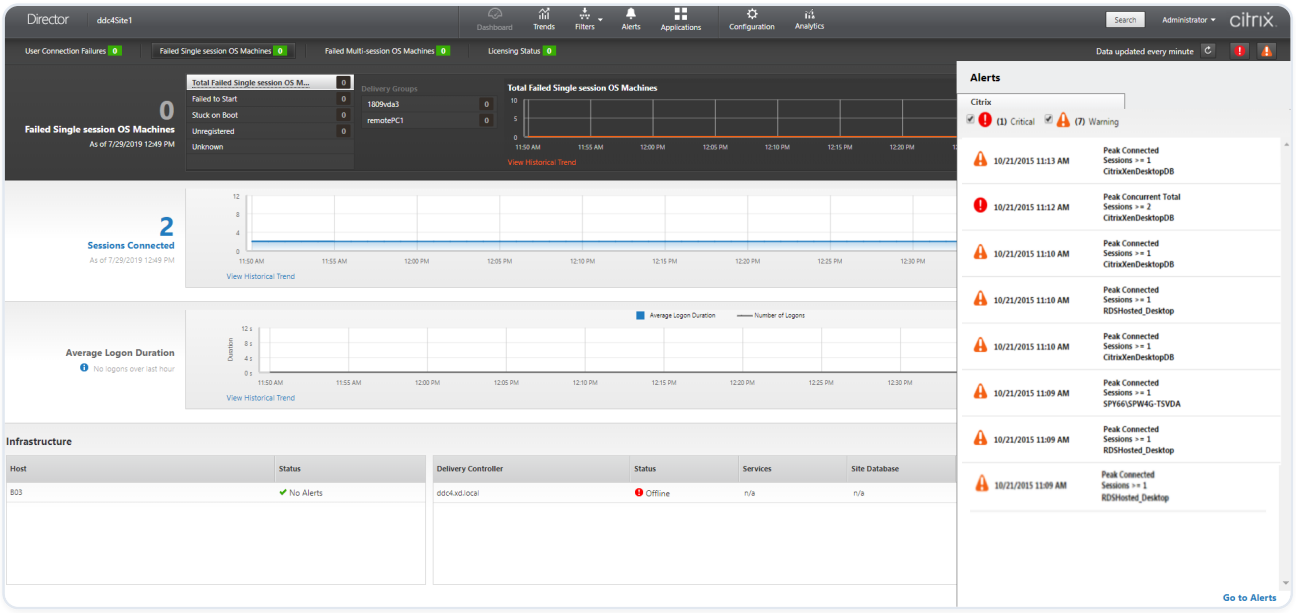
如果用户尝试连接到处于维护模式的已分配桌面，将显示一条消息，指示桌面不可用。在禁用维护模式之前，无法建立新连接。

## 应用程序分析

“**应用程序**”选项卡在一个统一视图中显示基于应用程序的分析，以帮助高效分析和管理应用程序性能。您可以深入了解站点上发布的所有应用程序的运行状况和使用信息。它显示了诸如探测结果、每个应用程序的实例数以及与已发布应用程序相关的故障和错误等指标。有关详细信息，请参阅**应用程序故障排除**中的应用程序分析部分。

# 警报和通知

警报在 Director 的仪表板和其他高级视图中显示，带有警告和严重警报符号。警报适用于 **Premium** 许可站点。警报每分钟自动更新；您也可以按需更新警报。

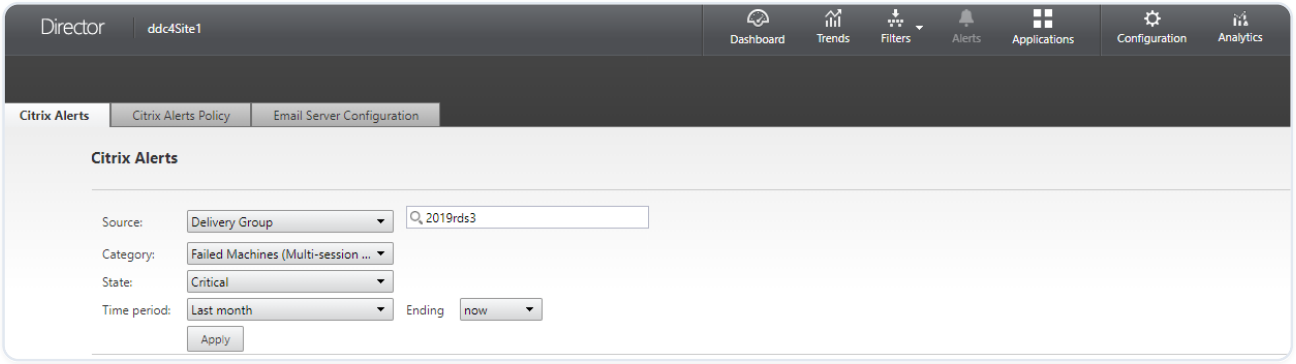



警告警报（琥珀色三角形）表示某个条件的警告阈值已达到或超出。

严重警报（红色圆形）表示某个条件的严重阈值已达到或超出。

您可以通过从侧边栏中选择警报、单击侧边栏底部的“**转到警报**”链接或从 Director 页面顶部选择“**警报**”来查看有关警报的更详细信息。

在“警报”视图中，您可以筛选和导出警报。例如，过去一个月内特定交付组的失败多会话操作系统计算机，或特定用户的所有警报。有关详细信息，请参阅导出报告。




## Citrix® 警报

Citrix 警报是 Director 中监视的源自 Citrix 组件的警报。您可以在 Director 中通过“**警报**”\>“**Citrix 警报策略**”配置 Citrix 警报。作为配置的一部分，您可以设置当警报超出您已设置的阈值时，通过电子邮件将通知发送给个人和组。有关设置 Citrix 警报的更多信息，请参阅创建警报策略。

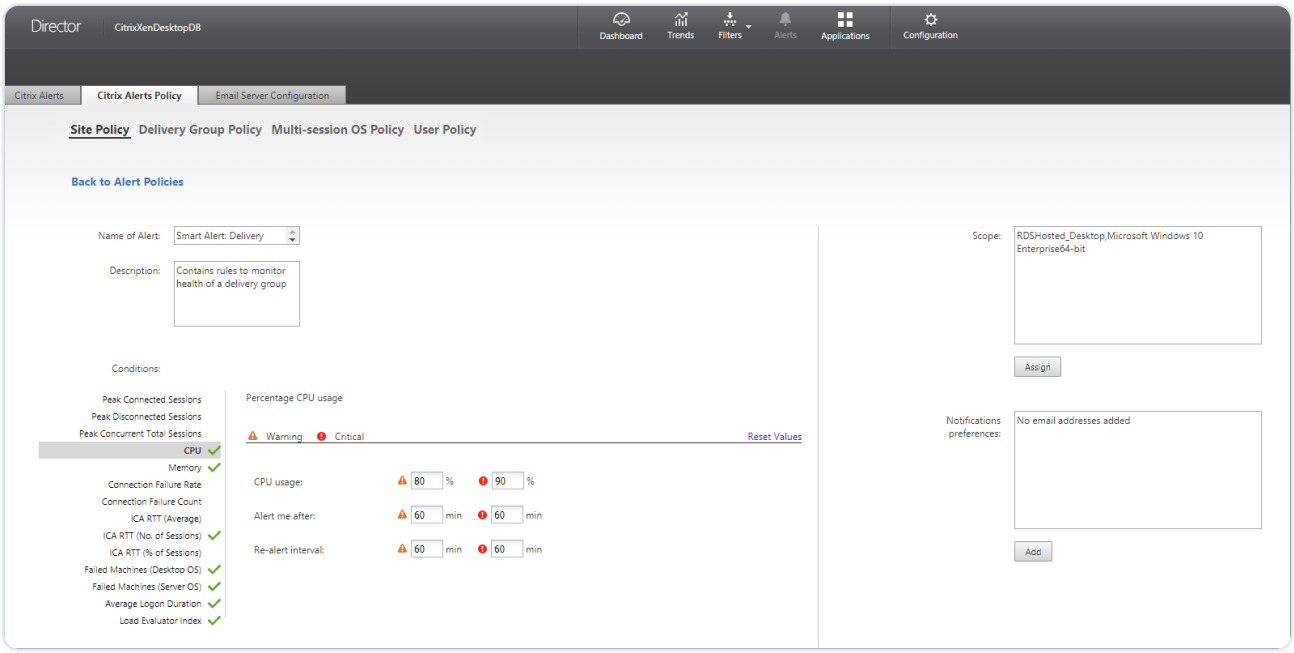
> **注意：**
>
> 确保您的防火墙、代理或 Microsoft Exchange Server 不会阻止电子邮件警报。

### 智能警报策略

针对交付组和多会话操作系统 VDA 范围提供了一组具有预定义阈值的内置警报策略。此功能需要 Delivery Controller 7.18 或更高版本。您可以在“**警报**”\>“**Citrix 警报策略**”中修改内置警报策略的阈值参数。 当您的站点中定义了至少一个警报目标（交付组或多会话操作系统 VDA）时，将创建这些策略。此外，这些内置警报会自动添加到新的交付组或多会话操作系统 VDA。

如果您升级 Director 和您的站点，则会沿用您之前 Director 实例中的警报策略。仅当 Monitor 数据库中不存在相应的警报规则时，才会创建内置警报策略。

有关内置警报策略的阈值，请参阅警报策略条件部分。

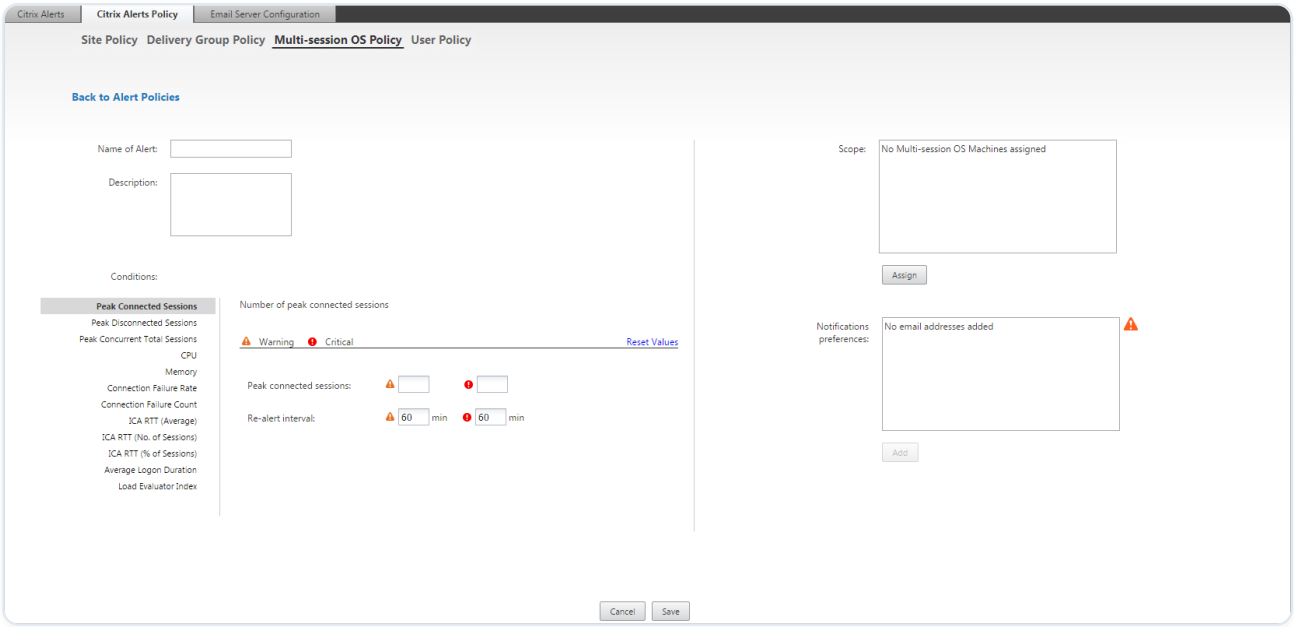



### SCOM 警报

SCOM 警报显示来自 Microsoft System Center 2012 Operations Manager (SCOM) 的警报信息，以便在 Director 中提供更全面的数据中心运行状况和性能指示。有关详细信息，请参阅配置 SCOM 警报集成部分。

在展开侧边栏之前，警报图标旁边显示的警报数量是 Citrix 警报和 SCOM 警报的总和。

## 创建警报策略




要创建新的警报策略，例如，在满足特定会话计数条件时生成警报：

1. 转到**警报** \> **Citrix 警报策略**，然后选择例如“多会话操作系统策略”。
2. 单击“**创建**”。
3. 命名并描述策略，然后设置触发警报必须满足的条件。例如，为峰值连接会话、峰值断开连接会话和峰值并发总会话指定警告和严重计数。警告值不得大于严重值。有关详细信息，请参阅警报策略条件。
4. 设置重新警报间隔。如果警报条件仍然满足，警报将在此时间间隔再次触发，并且，如果警报策略中已设置，则会生成电子邮件通知。已解除的警报不会在重新警报间隔生成电子邮件通知。
5. 设置范围。例如，为特定的交付组设置。
6. 在“通知首选项”中，指定当警报触发时应通过电子邮件通知谁。您必须在“**电子邮件服务器配置**”选项卡上指定电子邮件服务器，才能在“警报策略”中设置电子邮件通知首选项。
7. 单击 **保存**。

在范围中定义了 20 个或更多交付组的策略，其配置可能需要大约 30 秒才能完成。在此期间会显示加载指示器。

为多达 20 个唯一交付组（总共 1000 个交付组目标）创建 50 个以上的策略可能会导致响应时间增加（超过 5 秒）。

将包含活动会话的计算机从一个交付组移动到另一个交付组可能会触发使用计算机参数定义的错误交付组警报。

### 警报策略条件

下面列出了警报类别、建议的缓解警报措施以及（如果已定义）内置策略条件。内置警报策略的警报和重新警报间隔为 60 分钟。

#### 峰值连接会话

- 检查 Director 会话趋势视图以查看连接会话峰值。
- 检查以确保有足够的容量来适应会话负载。
- 如果需要，添加新计算机

#### 峰值断开连接会话

- 检查 Director 会话趋势视图以查看断开连接会话峰值。
- 检查以确保有足够的容量来容纳会话负载。
- 如有需要，添加新计算机。
- 如有需要，注销断开连接的会话。

#### 并发会话总数峰值

- 在 Director 中检查 Director 会话趋势视图以查看并发会话峰值。
- 检查以确保有足够的容量来容纳会话负载。
- 如有需要，添加新计算机。
- 如有需要，注销断开连接的会话。

#### CPU

CPU 使用率百分比表示 VDA 上的整体 CPU 消耗，包括进程的 CPU 消耗。您可以从相应 VDA 的**计算机详细信息**页面获取有关单个进程的 CPU 利用率的更多见解。

- 转至**计算机详细信息 > 查看历史利用率 > 前 10 个进程**，确定占用 CPU 的进程。确保已启用进程监视策略以启动进程级别资源使用情况统计信息的收集。
- 如有必要，结束进程。
- 结束进程会导致未保存的数据丢失。
- 如果一切按预期工作，将来请添加额外的 CPU 资源。

> **注意：**

> 策略设置“**启用资源监视**”默认允许监视安装了 VDA 的计算机上的 CPU 和内存性能计数器。如果此策略设置被禁用，则不会触发包含 CPU 和内存条件的警报。有关详细信息，请参阅监视策略设置

> **智能策略条件：**

- **范围：**交付组、多会话操作系统范围
- **阈值：**警告 - 80%，严重 - 90%

#### 内存

内存使用百分比指示 VDA 上的总体内存消耗，包括进程的内存消耗。您可以从相应 VDA 的“**计算机详细信息**”页面更深入地了解单个进程的内存使用情况。

- 转至**计算机详细信息 > 查看历史利用率 > 前 10 个进程**，确定占用内存的进程。确保已启用进程监视策略以启动进程级别资源使用情况统计信息的收集。
- 如有必要，结束该进程。
- 结束进程会导致未保存的数据丢失。
- 如果一切按预期工作，将来请添加额外的内存。

> **注意：**

> 策略设置“**启用资源监视**”默认允许监视安装了 VDA 的计算机上的 CPU 和内存性能计数器。如果此策略设置被禁用，则不会触发包含 CPU 和内存条件的警报。有关详细信息，请参阅监视策略设置

> **智能策略条件：**

- **范围：**交付组、多会话操作系统范围
- **阈值：** 警告 - 80%，严重 - 90%

#### 连接失败率

过去一小时内连接失败的百分比。

- 根据尝试连接总数中的失败总数计算。
- 检查 Director 连接失败趋势视图以查看从配置日志记录的事件。
- 确定应用程序或桌面是否可访问。

### 连接失败计数

过去一小时内连接失败的数量。

- 检查 Director 连接失败趋势视图，查看配置日志中记录的事件。
- 确定应用程序或桌面是否可访问。

### ICA® RTT（平均）

平均 ICA 往返时间。

- 检查 Citrix ADM 以获取 ICA RTT 的详细信息，从而确定根本原因。有关详细信息，请参阅 Citrix ADM 文档。
- 如果 Citrix ADM 不可用，请检查 Director 用户详细信息视图中的 ICA RTT 和延迟，并确定是网络问题还是应用程序或桌面问题。

### ICA RTT（会话数）

超过阈值 ICA 往返时间的会话数。

- 检查 Citrix ADM 以获取 ICA RTT 较高的会话数。有关详细信息，请参阅 Citrix ADM 文档。
- 如果 Citrix ADM 不可用，请与网络团队协作以确定根本原因。

  **智能策略条件：**

  - **范围：** 交付组、多会话操作系统范围
  - **阈值：** 警告 - 5 个或更多会话持续 300 毫秒，严重 - 10 个或更多会话持续 400 毫秒

### ICA RTT（会话百分比）

超过平均 ICA 往返时间的会话百分比。

- 检查 Citrix ADM 以获取 ICA RTT 较高的会话数。有关详细信息，请参阅 Citrix ADM 文档。
- 如果 Citrix ADM 不可用，请与网络团队协作以确定根本原因。

### ICA RTT（用户）

应用于指定用户启动的会话的 ICA 往返时间。如果至少一个会话中的 ICA RTT 大于阈值，则会触发警报。

### 失败的计算机（单会话操作系统）

失败的单会话操作系统计算机数量。故障可能由于各种原因发生，如 Director 控制板和筛选器视图中所示。

- 运行 Citrix Scout 诊断以确定根本原因。有关详细信息，请参阅 解决用户问题。

**智能策略条件：**

- **范围：** 交付组范围
- **阈值：**警告 - 1，严重 - 2

### 失败的计算机（多会话操作系统）

失败的多会话操作系统计算机数量。故障可能由于各种原因发生，如 Director 控制板和筛选器视图中所示。

- 运行 Citrix Scout 诊断以确定根本原因。

**智能策略条件：**

- **范围：** 交付组、多会话操作系统范围
- **阈值：**警告 - 1，严重 - 2

### 平均登录持续时间

过去一小时内发生的登录的平均登录持续时间。

- 检查 Director 控制板以获取有关登录持续时间的最新指标。在短时间内大量用户登录可能会增加登录持续时间。
- 检查登录的基线和细分以缩小原因范围。有关详细信息，请参阅诊断用户登录问题

**智能策略条件：**

- **范围：** 交付组、多会话操作系统范围
- **阈值：** 警告 - 45 秒，严重 - 60 秒

### 登录持续时间（用户）

过去一小时内指定用户的登录持续时间。

### 负载评估器指数

过去 5 分钟内负载评估器指数的值。

- 在 Director 中检查可能具有峰值负载（最大负载）的多会话操作系统计算机。查看“控制板”（故障）和“趋势负载评估器索引”报告。

**智能策略条件：**

- **范围：** 交付组、多会话操作系统范围
- **阈值：** 警告 - 80%，严重 - 90%

### 管理程序警报监控

Director 显示警报以监控管理程序运行状况。来自 Citrix Hypervisor™ 和 VMware vSphere 的警报有助于监控管理程序参数和状态。还会监控与管理程序的连接状态，以便在主机群集或池重新启动或不可用时提供警报。

要接收管理程序警报，请确保在 Citrix Studio 中创建了托管连接。有关详细信息，请参阅连接和资源。只有这些连接会受到监控以获取管理程序警报。下表描述了管理程序警报的各种参数和状态。

| 警报 | 支持的管理程序 | 触发条件 | 条件 | 配置 |
| --- | --- | --- | --- | --- |
| CPU 使用率 | 思杰 Hypervisor, 威睿 vSphere | 管理程序 | 达到或超出 CPU 使用率警报阈值 | 警报阈值必须在管理程序中配置。 |
| 内存使用情况 | 思杰 Hypervisor, 威睿 vSphere | 管理程序 | 内存使用情况警报阈值已达到或超出 | 警报阈值必须在管理程序中配置。 |
| 网络使用情况 | 思杰 Hypervisor, 威睿 vSphere | 管理程序 | 网络使用情况警报阈值已达到或超出 | 警报阈值必须在管理程序中配置。 |
| 磁盘使用情况 | 威睿 vSphere | 管理程序 | 磁盘使用情况警报阈值已达到或超出 | 警报阈值必须在管理程序中配置。 |
| 主机连接或电源状态 | 威睿 vSphere | 管理程序 | 管理程序主机已重新启动或不可用 | 警报在 VMware vSphere 中预先构建。无需额外配置。 |
| 管理程序连接不可用 | 思杰 Hypervisor, 威睿 vSphere | 交付控制器™ | 与管理程序（池或群集）的连接已丢失、已断电或已重新启动。只要连接不可用，此警报就会每小时生成一次。 | 警报已与 Delivery Controller 预先构建。无需额外配置。 |

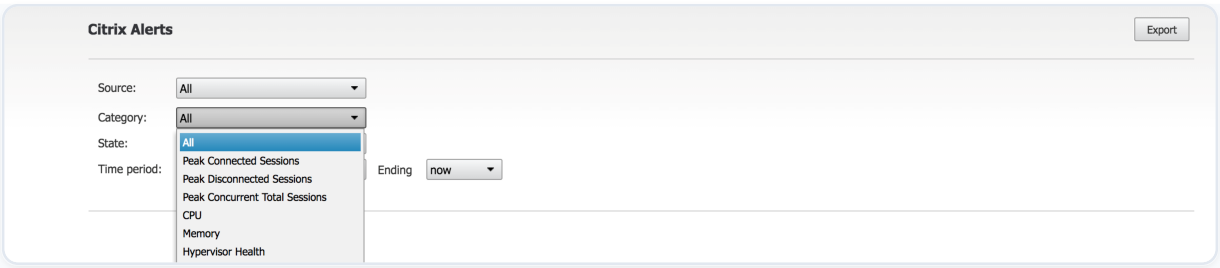
**注意：**

有关配置警报的更多信息，请参阅 Citrix XenCenter 警报 或查看 VMware vCenter 警报文档。

可以在 **Citrix 警报策略 > 站点策略 > 管理程序运行状况**下配置电子邮件通知首选项。管理程序警报策略的阈值条件只能从管理程序配置、编辑、禁用或删除，而不能从 Director 配置、编辑、禁用或删除。但是，修改电子邮件首选项和解除警报可以在 Director 中完成。

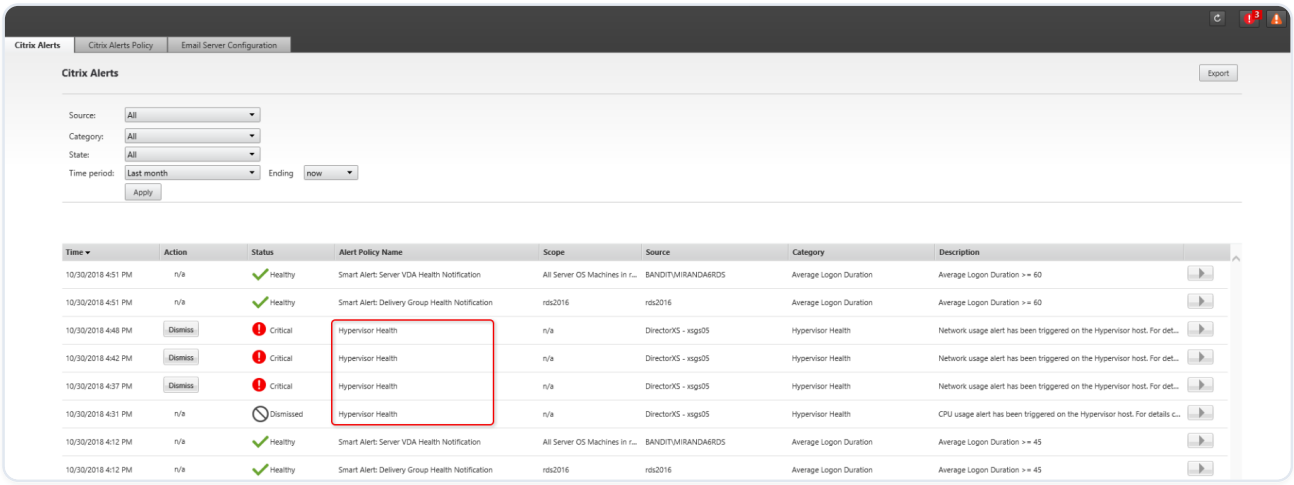
**重要提示：**

- 由管理程序触发的警报会在 Director 中获取并显示。但是，管理程序警报生命周期/状态的变化不会反映在 Director 中。
- 在管理程序控制台中处于正常、已解除或已禁用状态的警报会继续显示在 Director 中，并且必须明确解除。
- 在 Director 中解除的警报不会在管理程序控制台中自动解除。




已添加一个名为“**管理程序运行状况**”的新警报类别，以仅筛选管理程序警报。一旦达到或超过阈值，这些警报就会显示。管理程序警报可以是：

- 严重—已达到或超过管理程序警报策略的严重阈值
- 警告—已达到或超过管理程序警报策略的警告阈值
- 已解除—警报不再显示为活动警报




此功能需要 Delivery Controller 7 1811 或更高版本。如果您使用的是旧版 Director，但站点版本为 7 1811 或更高版本，则仅显示管理程序警报计数。要查看警报，您必须升级 Director。

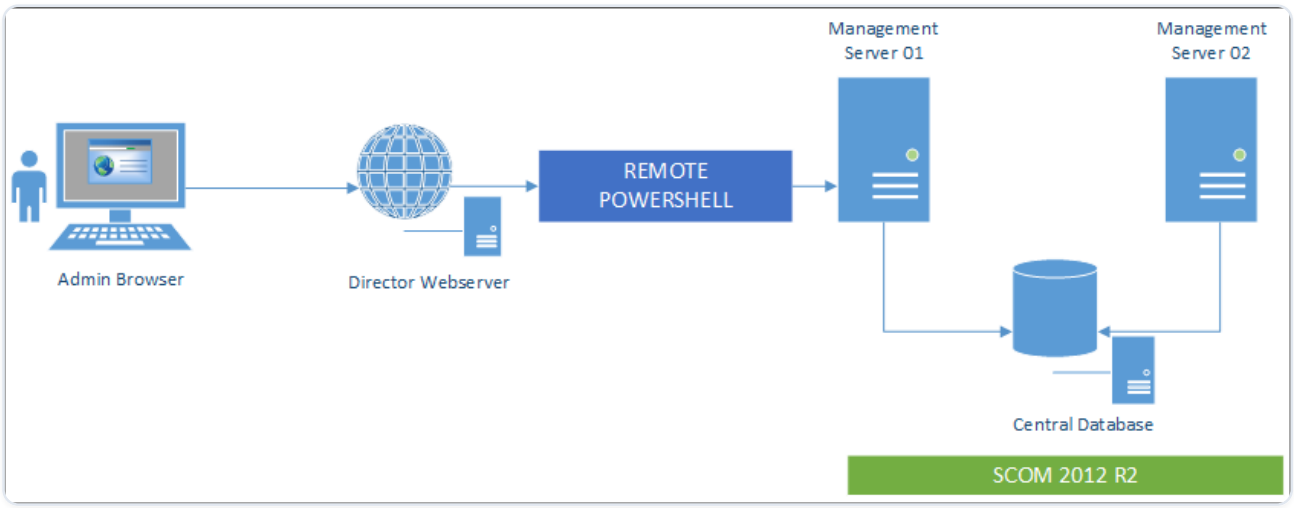
## 配置 SCOM 警报集成

SCOM 与 Director 集成后，您可以在 Director 的控制板和其他高级视图中查看来自 SCOM 的警报信息。

SCOM 警报与 Citrix 警报一起显示在屏幕上。您可以从侧栏中的 SCOM 选项卡访问并深入查看 SCOM 警报。

您可以查看长达一个月的历史警报，对筛选后的信息进行排序、筛选，并将其导出为 CSV、Excel 和 PDF 报告格式。有关详细信息，请参阅导出报告。

SCOM 集成使用远程 PowerShell 3.0 或更高版本从 SCOM 管理服务器查询数据，并在用户的 Director 会话中维护持久的运行空间连接。Director 和 SCOM 服务器必须具有相同的 PowerShell 版本。




SCOM 集成的要求如下：

- Windows 服务器 2012 R2

- System Center 2012 R2 操作管理器
- PowerShell 3.0 或更高版本（Director 和 SCOM 服务器上的 PowerShell 版本必须匹配）
- 四核 CPU，16 GB RAM（推荐）
- 必须在 Director 的 web.config 文件中配置 SCOM 的主管理服务器。您可以使用 DirectorConfig 工具执行此操作。

Citrix 建议将 Director 管理员帐户配置为 SCOM 操作员角色，以便在 Director 中检索完整的警报信息。如果无法做到这一点，可以使用 DirectorConfig 工具在 web.config 文件中配置 SCOM 管理员帐户。

Citrix 进一步建议，每个 SCOM 管理服务器配置的 Director 管理员不要超过 10 个，以确保最佳性能。

在 Director 服务器上：

1. 键入 **Enable-PSRemoting** 以启用 PowerShell 远程处理。
2. 将 SCOM 管理服务器添加到 TrustedHosts 列表。打开 PowerShell 提示符并执行以下命令：
   - 获取 TrustedHosts 的当前列表

     Get-Item WSMAN:\localhost\Client\TrustedHosts
   - 将 SCOM 管理服务器的 FQDN 添加到 TrustedHosts 列表中。\<Old Values\> 表示从 Get-Item cmdlet 返回的现有条目集。

     Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "\<SCOM 管理服务器的 FQDN\>, \<旧值\>"
3. 使用 DirectorConfig 工具配置 SCOM。

   C:\inetpub\wwwroot\Director\tools\Director配置.exe /配置scom

在 SCOM 管理服务器上：

1. 将 Director 管理员分配给 SCOM 管理员角色。
   a. 打开 SCOM 管理控制台，然后转到 **Administration** \> **Security** \> **User Roles**。
   b. 在“用户角色”中，您可以创建新用户角色或修改现有用户角色。SCOM 操作员角色分为四类，它们定义了对 SCOM 数据的访问性质。例如，“只读”角色看不到“管理”窗格，也无法发现或管理规则、计算机或帐户。“操作员”角色是完全管理员角色。

   > **注意：**

> 如果 Director 管理员被分配到非操作员角色，则以下操作不可用：
>
> - 如果配置了多个管理服务器且主管理服务器不可用，则 Director 管理员无法连接到辅助管理服务器。主管理服务器是在 Director web.config 文件中配置的服务器，与上述步骤 3 中使用 DirectorConfig 工具指定的服务器相同。辅助管理服务器是主服务器的对等管理服务器。
> - 筛选警报时，Director 管理员无法搜索警报源。这需要操作员级别的权限。

c. 要修改任何用户角色，请右键单击该角色，然后单击 **Properties**。

d. 在“用户角色属性”对话框中，您可以从指定的用户角色中添加或删除 Director 管理员。

2. 将 Director 管理员添加到 SCOM 管理服务器上的 Remote Management Users 组。这允许 Director 管理员建立远程 PowerShell 连接。
3. 键入 **Enable-PSRemoting** 以启用 PowerShell 远程处理。
4. 设置 WS-Management 属性限制：

   a. 修改 MaxConcurrentUsers：

      在 CLI 中：

      ```
      winrm set winrm/config/winrs @{MaxConcurrentUsers = "20"}
      ```

      在 PS 中：

      ```
      Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
      ```

   b. 修改 MaxShellsPerUser：

      在 CLI 中：

      ```
      winrm set winrm/config/winrs @{MaxShellsPerUser="20"}
      ```

      在 PS 中：

```
Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
```

   a. 修改 MaxMemoryPerShellMB：

      在 CLI 中：

`winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}`

在 PS 中：

`Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024`

5. 为确保 SCOM 集成在混合域环境中正常工作，请设置以下注册表项。

路径：
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

密钥：LocalAccountTokenFilterPolicy

类型：DWord

值：1

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

SCOM 集成设置完成后，您可能会看到消息“无法获取最新的 SCOM 警报。有关详细信息，请查看 Director 服务器事件日志”。服务器事件日志有助于识别和纠正问题。原因可能包括：

- Director 或 SCOM 计算机上的网络连接丢失。
- SCOM 服务不可用或过于繁忙而无法响应。
- 由于配置用户的权限发生更改，导致授权失败。
- Director 在处理 SCOM 数据时出现错误。
- Director 和 SCOM 服务器之间的 PowerShell 版本不匹配。

## 筛选数据以排查故障

当您单击仪表板上的数字或从“筛选器”菜单中选择预定义筛选器时，“筛选器”视图将打开以显示基于所选计算机或故障类型的数据。

预定义筛选器无法编辑，但您可以将预定义筛选器另存为自定义筛选器，然后对其进行修改。此外，您还可以创建所有交付组中计算机、连接、会话和应用程序实例的自定义筛选视图。

1. 选择一个视图：

    - **计算机**。选择单会话操作系统计算机或多会话操作系统计算机。这些视图显示已配置计算机的数量。多会话操作系统计算机选项卡还包括负载评估器索引，该索引指示性能计数器的分布以及将鼠标悬停在链接上时会话计数的工具提示。

- **会话**。您还可以从“会话”视图中查看会话计数。使用空闲时间度量来识别空闲时间超过阈值时段的会话。
- **连接**。按不同时间段筛选连接，包括最近 60 分钟、最近 24 小时或最近 7 天。
- **应用程序实例**。此视图显示服务器和单会话操作系统 VDA 上所有应用程序实例的属性。多会话操作系统 VDA 上的应用程序实例可使用会话空闲时间度量。

> **注意：**
>
> 如果您在安装了 Windows 10 1809 计算机的 VDA 上启动了桌面会话，Director 中的活动管理器有时可能会将 Microsoft Edge 和 Office 显示为正在主动运行的应用程序，而实际上它们仅在后台运行。

2. 对于**筛选依据**，选择条件。
3. 根据需要，使用每个视图的附加选项卡来完成筛选。
4. 根据需要选择额外的列，以进一步排查故障。
5. 保存并命名您的筛选器。
6. 要从多个 Director 服务器访问筛选器，请将筛选器存储在可从这些服务器访问的共享文件夹中：
   - 共享文件夹必须对 Director 服务器上的帐户具有修改权限。
   - 必须将 Director 服务器配置为访问共享文件夹。要进行配置，请运行 **IIS 管理器**。在**站点 \> 默认网站 \> Director\ > 应用程序设置**中，修改 **Service.UserSettingsPath** 设置以反映共享文件夹的 UNC 路径。
7. 要稍后打开筛选器，请从**筛选器**菜单中选择筛选器类型（计算机、会话、连接或应用程序实例），然后选择已保存的筛选器。
8. 单击**导出**以将数据导出到 CSV 格式文件。最多可导出 100,000 条记录的数据。此功能在 Delivery Controller™ 1808 版及更高版本中可用。
9. 如果需要，对于**计算机**或**连接**视图，请对筛选列表中选择的所有计算机使用电源控制。对于“会话”视图，请使用会话控制或发送消息选项。
10. 在“**计算机**”和“**连接**”视图中，单击失败的计算机或连接的“**失败原因**”以获取故障的详细说明以及建议的故障排除操作。计算机和连接故障的失败原因和建议操作可在 Citrix Director 7.12 失败原因故障排除指南 中找到。
11. 在“**计算机**”视图中，单击计算机名称链接以转到相应的“**计算机详细信息**”页面。此页面显示计算机的详细信息，提供电源控制，并显示 CPU、内存、磁盘监视和 GPU 监视图表。此外，单击“

**查看历史利用率**”以查看计算机的资源利用率趋势。有关详细信息，请参阅对计算机进行故障排除。

12. 在“**应用程序实例**”视图中，根据大于阈值时间段的“**空闲时间**”进行排序或筛选。选择要结束的空闲应用程序实例。注销或断开应用程序实例会结束同一会话中的所有活动应用程序实例。有关详细信息，请参阅 排查应用程序故障。如果 Director、Delivery Controller 和 VDA 的版本为 7.13 或更高版本，则可以使用“应用程序实例”筛选页面和“会话”筛选页面中的空闲时间测量值。

> **注意：** Citrix Studio 允许将多个桌面分配规则 (DAR) 分配给交付组中不同用户或用户组的单个 VDA。StoreFront™ 根据登录用户的 DAR 显示分配的桌面以及相应的显示名称。但是，Director 不支持 DAR，并且无论登录用户是谁，都使用交付组名称显示分配的桌面。因此，您无法在 Director 中将特定桌面映射到计算机。要将 StoreFront 中显示的分配桌面映射到 Director 中显示的交付组名称，请使用以下 PowerShell 命令：

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq "\<Name
on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

## 监控站点的历史趋势

“趋势”视图可访问每个站点的以下参数的历史趋势信息：

- 会话
- 连接失败
- 计算机故障
- 登录性能
- 负载评估
- 容量管理
- 计算机使用情况
- 资源利用率
- 每个站点的网络分析。

要查找此信息，请单击“**趋势**”菜单。

放大钻取功能允许您通过放大某个时间段（单击图表中的数据点）并向下钻取以查看与趋势相关的详细信息来浏览趋势图表。此功能使您能够更好地了解受影响的人员或内容的详细信息。

要更改每个图表的默认范围，请对数据应用不同的筛选器。

选择您需要历史趋势信息的时间段。时间段的可用性取决于您的 Director 部署，具体如下：

- 高级许可站点中提供最长可达去年（365 天）的趋势报告。
- 高级许可站点中提供最长可达上个月（31 天）的趋势报告。
- 在非高级和非高级许可站点中，提供最长可达最近 7 天的趋势报告。

**注意：**

- 在所有 Director 部署中，当时间段设置为上个月（**截止到当前**）或更短时，会话、故障和登录性能趋势信息以图表和表格形式提供。如果时间段选择为具有自定义结束日期的上个月或去年，则趋势信息以图表形式提供，而不是以表格形式提供。
- Monitor Service 的清理保留值控制趋势数据的可用性。默认值可在数据粒度和保留中找到。高级许可站点的客户可以将其清理保留更改为所需的保留天数。
- IIS 管理器中的以下参数控制可供选择的自定义结束日期范围。但是，所选日期的数据可用性取决于所测量特定指标的清理保留设置。

| 参数 | 默认值 |
| --- | --- |
| UI.TrendsLast2HoursRange | 3 |
| UI.TrendsLast24HoursRange | 32 |
| UI.TrendsLast7DaysRange | 32 |
| UI.TrendsLastMonthRange | 365 |

### 可用趋势

**查看会话趋势：** 在**会话**选项卡中，选择交付组和时间段，以查看有关并发会话计数的更详细信息。

**会话自动重新连接**列显示会话中的自动重新连接次数。当会话可靠性或客户端自动重新连接策略生效时，将启用自动重新连接。当端点上发生网络中断时，以下策略将生效：

- 会话可靠性生效（默认情况下为 3 分钟），Citrix Receiver™ 或 Citrix Workspace™ 应用程序会尝试连接到 VDA。

- 客户端自动重新连接在 3 到 5 分钟之间生效，客户端会尝试连接到 VDA。

两次重新连接都会被捕获并显示给用户。重新连接发生后，此信息最多可能需要 5 分钟才能显示在 Director UI 上。

自动重新连接信息可帮助您查看和排查存在中断的网络连接。它还可以分析具有无缝体验的网络。您可以查看在筛选器中选择的特定交付组或时间段的重新连接次数。深入分析可提供其他信息，例如会话可靠性或客户端自动重新连接、时间戳、端点 IP 以及安装了 Workspace 应用程序的计算机的端点名称。

默认情况下，日志按事件时间戳降序排序。此功能适用于适用于 Windows 的 Citrix Workspace 应用程序、适用于 Mac 的 Citrix Workspace 应用程序、适用于 Windows 的 Citrix Receiver 和适用于 Mac 的 Citrix Receiver。此功能需要 Delivery Controller™ 7 1906 或更高版本以及 VDA 1906 或更高版本。

有关会话重新连接的详细信息，请参阅会话。

有关策略的详细信息，请参阅客户端自动重新连接策略设置和会话可靠性策略设置。

有时，自动重新连接数据可能不会显示在 Director 中，原因如下：

- Workspace 应用程序未将自动重新连接数据发送到 VDA。
- VDA 未将数据发送到监视服务。
- Delivery Controller 丢弃 VDA 有效负载，因为它们可能没有相应的会话。

> **注意：**
>
> 有时，如果设置了某些 Citrix Gateway 策略，客户端 IP 地址可能无法正确获取。

> **查看连接失败趋势：** 在“失败”选项卡中，选择连接、计算机类型、失败类型、交付组和时间段，以查看包含有关站点中用户连接失败的更详细信息的图表。

**查看计算机故障趋势：** 在“**单会话操作系统计算机故障**”选项卡或“多会话操作系统计算机”选项卡中，选择故障类型、交付组和时间段，以查看包含站点中计算机故障的更详细信息的图表。

**查看登录性能趋势：** 在“**登录性能**”选项卡中，选择交付组和时间段，以查看包含站点中用户登录时间持续时间的更详细信息以及登录次数是否影响性能的图表。此视图还显示登录阶段的平均持续时间，例如代理持续时间和 VM 启动时间。 此数据专门用于用户登录，不包括尝试从断开连接的会话重新连接的用户。 图表下方的表格显示按用户会话划分的登录持续时间。您可以选择要显示的列，

并按任意列对报告进行排序。 有关详细信息，请参阅(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/director/troubleshoot-deployments/user-issues/user-logon.html)

**查看负载评估趋势：** 在“**负载评估器索引**”选项卡中，查看包含有关在多会话操作系统计算机之间分配的负载的更详细信息的图表。此图表的筛选器选项包括交付组或交付组中的多会话操作系统计算机、多会话操作系统计算机（仅当选择了交付组中的多会话操作系统计算机时可用）和范围。

**查看托管应用程序使用情况：** 此功能的可用性取决于您组织的许可证。 在“**容量管理**”选项卡中，选择“**托管应用程序使用情况**”选项卡。选择交付组和时间段，以查看显示并发使用高峰的图表和显示基于应用程序的使用情况的表格。在“基于应用程序的使用情况”表格中，您可以选择特定的应用程序以查看详细信息以及正在使用或已使用该应用程序的用户列表。

**查看单会话和多会话操作系统使用情况：** “趋势”视图按站点和交付组显示单会话操作系统的使用情况。当您选择“**站点**”时，将按交付组显示使用情况。当您选择“交付组”时，将按用户显示使用情况。“趋势”视图还按站点、交付组和计算机显示多会话操作系统的使用情况。当您选择“**站点**”时，将按交付组显示使用情况。当您选择“交付组”时，将按计算机和用户显示使用情况。当选择“计算机”时，将按用户显示使用情况。

**查看虚拟机使用情况：** 在“**计算机使用情况**”选项卡中，选择“**单会话操作系统计算机或多会话操作系统计算机**”以获取 VM 使用情况的实时视图，从而使您能够快速评估站点的容量需求。 单会话操作系统可用性 - 按整个站点或特定交付组的可用性显示单会话操作系统计算机 (VDI) 的当前状态。 多会话操作系统可用性 - 按整个站点或特定交付组的可用性显示多会话操作系统计算机的当前状态。

> **注意：** “可用计数器”中显示的计算机数量包括处于维护模式的计算机。

> **查看资源利用率：** 在“**资源利用率**”选项卡中，选择“**单会话操作系统计算机或多会话操作系统计算机**”以获取每个 VDI 计算机的 CPU 和内存使用情况以及 IOPS 和磁盘延迟的历史趋势数据，从而更好地进行容量规划。 此功能需要 Delivery Controller 和 VDA **版本 7.11** 或更高版本。 图表显示平均 CPU、平均内存、平均 IOPS、磁盘延迟和并发会话峰值的数据。您可以深入到计算机，并查看消耗 CPU 的前 10 个进程的数据和图表。

> **注意：**
>
> 此表中列出的进程过多可能会消耗大量数据，从而影响性能。为避免这种情况，仅列出平均 CPU 或平均内存超过 1% 的进程。因此，该表有时可能列出少于 10 个进程。

按交付组和时间段进行筛选。CPU、内存使用情况和并发会话峰值图表可用于最近 2 小时、24 小时、7 天、月和年。平均 IOPS 和磁盘延迟图表可用于最近 24 小时、月和年。

**注意：**

- 必须将“监视”策略设置“**启用进程监视**”设置为“**允许**”才能在“历史计算机利用率”页面上的“前 10 个进程”表中收集和显示数据。默认情况下，该策略设置为“**禁止**”。默认情况下会收集所有资源利用率数据。可以使用“**启用资源监视**”策略设置禁用此功能。图表下方的表格显示每台计算机的资源利用率数据。有关详细信息，请参阅(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/policies/reference/virtual-delivery-agent-policy-settings/monitoring-policy-settings.html)。
- 平均 IOPS 显示每日平均值。峰值 IOPS 计算为所选时间范围内的 IOPS 平均值中的最高值。（IOPS 平均值是 VDA 上每小时收集的 IOPS 的每小时平均值）。

**查看网络分析数据：** 此功能的可用性取决于您组织的许可证和您的管理员权限。此功能需要 Delivery Controller **版本 7.11** 或更高版本。

在“**网络**”选项卡中，监视您的网络分析，该分析提供用户、应用程序和桌面的网络上下文视图。借助此功能，Director 通过 Citrix ADM 中的 HDX Insight 报告提供部署中 ICA 流量的高级分析。有关详细信息，请参阅(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/director/install-and-configure/hdx-insight.html)

**查看应用程序故障：** “**应用程序故障**”选项卡显示与 VDA 上已发布的应用程序相关的故障。

此功能需要 Delivery Controller 和 VDA **7.15 版**或更高版本。支持运行 Windows Vista 及更高版本的单会话操作系统 VDA，以及运行 Windows Server 2008 及更高版本的多会话操作系统 VDA。 有关详细信息，请参阅历史应用程序故障监视。

默认情况下，仅显示来自多会话操作系统 VDA 的应用程序故障。您可以使用监视策略设置应用程序故障的监视。有关详细信息，请参阅监视策略设置。

**查看应用程序探测结果：**“应用程序探测结果”选项卡显示已在“配置”页面中配置为探测的应用程序的探测结果。此处记录了应用程序启动失败时所处的启动阶段。

此功能需要 Delivery Controller 和 VDA **7.18 版**或更高版本。有关详细信息，请参阅应用程序探测。

**创建自定义报告：**“自定义报告”选项卡提供了一个用户界面，用于生成包含来自监视数据库的实时和历史数据的表格格式的自定义报告。

此功能需要 Delivery Controller **7.12 版**或更高版本。

在以前保存的自定义报告查询列表中，您可以单击**运行并下载**以 CSV 格式导出报告，单击**复制 OData**以复制和共享相应的 OData 查询，或者单击**编辑**以编辑查询。 您可以根据计算机、连接、会话或应用程序实例创建自定义报告查询。根据计算机、交付组或时间段等字段指定筛选条件。指定自定义报告中所需的其他列。预览显示报告数据的示例。保存自定义报告查询会将其添加到已保存查询的列表中。

您可以基于复制的 OData 查询创建自定义报告查询。为此，请选择“OData 查询”选项并粘贴复制的 OData 查询。您可以保存生成的查询以供以后执行。

> **注意：** 使用 OData 查询生成的预览和导出报告中的列名未本地化，而是以英文显示。

图表上的旗帜图标表示该特定时间范围内的重要事件或操作。将鼠标悬停在旗帜上并单击以列出事件或操作。

**注意：**

- 对于早于 7 的 VDA，不收集 HDX™ 连接登录数据。对于较早的 VDA，图表数据显示为 0。
- 在 Citrix Studio 中删除的交付组在 Director 趋势筛选器中仍可供选择，直到与其相关的数据被清除。选择已删除的交付组会显示可用数据的图表，直到保留期结束。但是，表格不显示数据。
- 将包含活动会话的计算机从一个交付组移动到另一个交付组会导致新交付组的**资源利用率和负载评估器索引**表显示从旧交付组和新交付组整合的指标。

# 排查部署故障

作为帮助台管理员，您可以搜索报告问题的用户，并显示与该用户关联的会话或应用程序的详细信息。同样，搜索报告问题的计算机或端点。通过监视相关指标并执行适当的操作来快速解决问题。

可用操作包括：

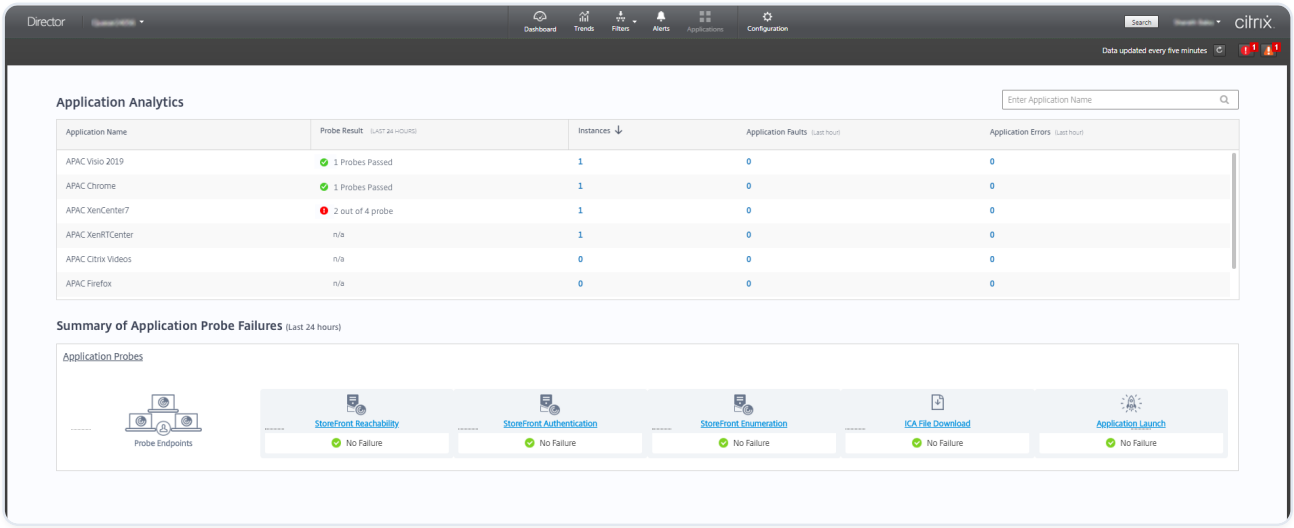
- 结束无响应的应用程序或进程
- 在用户计算机上执行影子操作

- 注销无响应的会话
- 重新启动计算机
- 将计算机置于维护模式
- 重置用户配置文件

# 排除应用程序故障

## 应用程序分析

“**应用程序**”视图在一个单一的综合视图中显示基于应用程序的分析，以帮助有效分析和管理应用程序性能。您可以深入了解站点上发布的所有应用程序的运行状况和使用情况信息。默认视图有助于识别运行靠前的应用程序。 此功能需要 Delivery Controllers 7.16 或更高版本以及 VDA 7.15 或更高版本。




“**探测结果**”列显示过去 24 小时内运行的应用程序探测结果。单击探测结果链接可在“**趋势**” \> “**应用程序探测结果**”页面中查看更多详细信息。有关如何配置应用程序探测的更多详细信息，请参阅应用程序探测。

“**实例**”列显示应用程序的使用情况。它指示当前正在运行的应用程序实例数（包括已连接和已断开连接的实例）。要进一步进行故障排除，请单击“**实例**”字段以查看相应的“**应用程序实例**”筛选器页面。在此处，您可以选择要注销或断开连接的应用程序实例。

> **注意：**
>
> 对于自定义范围管理员，Director 不显示在应用程序组下创建的应用程序实例。要查看所有应用程序实例，您必须是完全管理员。有关详细信息，请参阅知识中心文章 CTX256001。

> 使用“**应用程序故障**”和“**应用程序错误**”列监视站点中已发布应用程序的运行状况。这些列显示了过去一小时内启动相应应用程序时发生的故障和错误的聚合数量。单击“**应用程序故障**”或“**应用程序错误**”字段，以在“**趋势**” \> “**应用程序故障**”页面上查看与所选应用程序对应的故障详细信息。

应用程序故障策略设置控制故障和错误的可用性及显示。有关策略以及如何修改这些策略的详细信息，请参阅“**监视策略**”设置中的应用程序故障监视策略。

### 实时应用程序监视

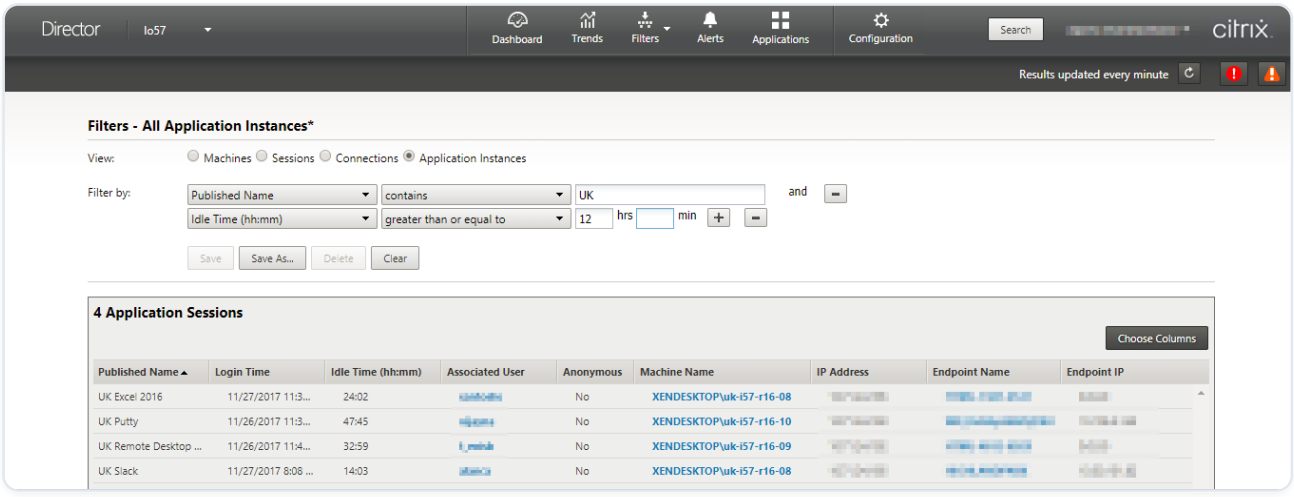
您可以使用空闲时间指标来识别空闲时间超出特定时间限制的实例，从而排除应用程序和会话故障。

基于应用程序故障排除的典型用例存在于医疗保健领域，员工共享应用程序许可证。在此类情况下，您必须结束空闲会话和应用程序实例，以清除 Citrix Virtual Apps and Desktops™ 环境、重新配置性能不佳的服务器或维护和升级应用程序。

“**应用程序实例**”筛选器页面列出服务器和单会话操作系统 VDA 上的所有应用程序实例。对于多会话操作系统 VDA 上已空闲至少 10 分钟的应用程序实例，将显示相关的空闲时间度量。

> **注意：** 应用程序实例指标适用于所有许可证版本的站点。

> 使用此信息识别空闲时间超出特定时间段的应用程序实例，并根据需要注销或断开连接它们。为此，请选择**筛选器 \> 应用程序实例**，然后选择一个预保存的筛选器，或者选择**所有应用程序实例**并创建自己的筛选器。

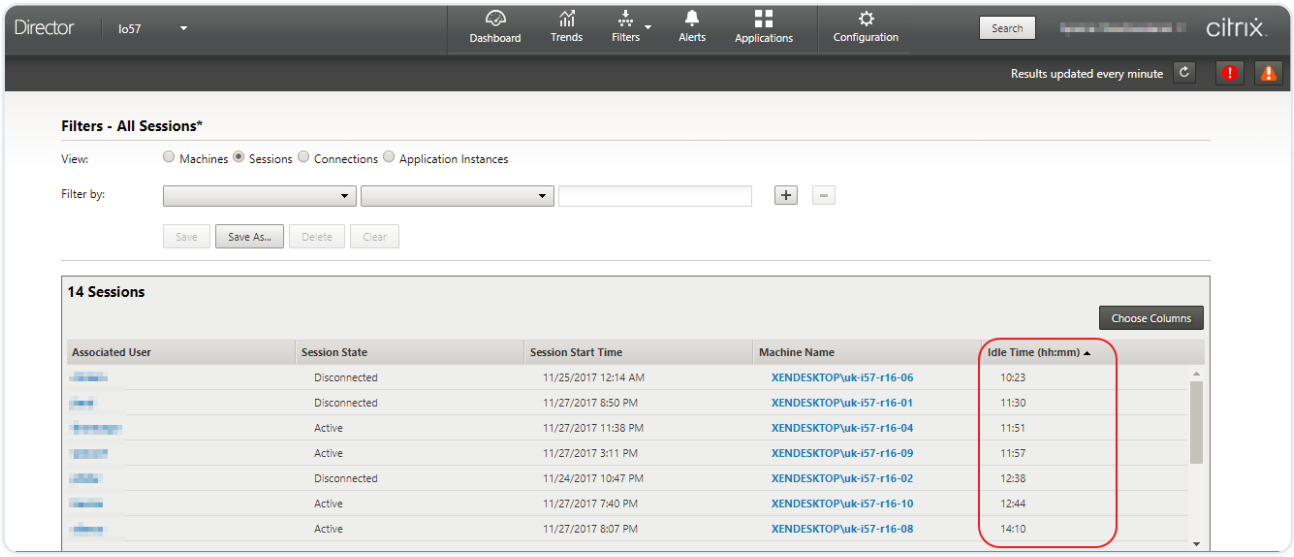



筛选器示例如下。在“**筛选依据**”条件中，选择“**已发布名称**”（应用程序的）和“**空闲时间**”。然后，将“**空闲时间**”设置为“**大于或等于**”特定时间限制，并保存筛选器以供重复使用。从筛选列表中，选择应

用程序实例。选择发送消息的选项，或者从“**会话控制**”下拉列表中选择“**注销**”或“**断开连接**”以结束实例。

> **注意：** 注销或断开应用程序实例会注销或断开当前会话，从而结束属于同一会话的所有应用程序实例。

> 您可以使用会话状态和会话空闲时间指标从“**会话**”筛选器页面识别空闲会话。按“**空闲时间**”列排序或定义筛选器以识别超出特定时间限制的空闲会话。对于空闲时间至少为 10 分钟的多会话操作系统 VDA 上的会话，会列出空闲时间。




当会话或应用程序实例出现以下情况时，“**空闲时间**”显示为“**不适用**”

- 空闲时间未超过 10 分钟，
- 在单会话操作系统 VDA 上启动，或者
- 在运行版本 7.12 或更早版本的 VDA 上启动。

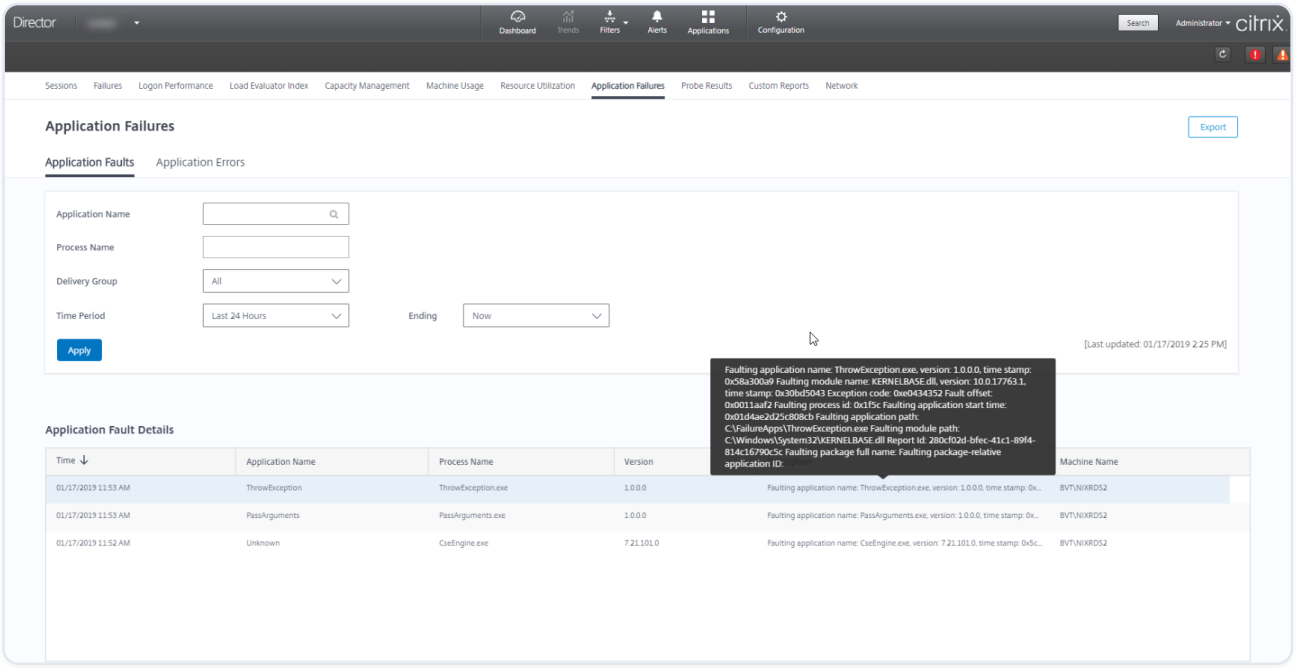
### 历史应用程序故障监视

“**趋势**”-\>“**应用程序故障**”选项卡显示与 VDA 上已发布的应用程序相关的故障。

Premium 和 Advanced 许可站点可查看过去 2 小时、24 小时、7 天和 1 个月的应用程序故障趋势。其他许可证类型可查看过去 2 小时、24 小时和 7 天的应用程序故障趋势。将监视以“应用程序错误”为源记录到事件查看器中的应用程序故障。单击“**导出**”以生成 CSV、Excel 或 PDF 格式的报告

应用程序故障监视的清理保留设置 GroomApplicationErrorsRetentionDays 和 GroomApplicationFaultsRetentionDays 默认为一天，适用于 Premium 和非 Premium 许可站点。您可以使用 PowerShell 命令更改此设置：

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```




故障根据其严重性显示为“**应用程序故障**”或“**应用程序错误**”。“应用程序故障”选项卡显示与功能或数据丢失相关的故障。应用程序错误表示不立即相关的问题；它们表示可能导致未来问题的状况。

您可以根据“**已发布应用程序名称**”、“**进程名称**”或“**交付组**”以及“**时间段**”筛选故障。该表显示故障或错误代码以及故障的简要说明。详细故障说明以工具提示形式显示。

> **注意：** 当无法派生相应的应用程序名称时，已发布的应用程序名称将显示为“未知”。这通常发生在启动的应用程序在桌面会话中失败，或者由于依赖的可执行文件导致未处理的异常而失败时。

默认情况下，仅监视托管在多会话操作系统 VDA 上的应用程序的故障。您可以通过监视组策略修改监视设置：“启用应用程序故障监视”、“启用单会话操作系统 VDA 上的应用程序故障监视”和“从故障监视中排除的应用程序列表”。有关详细信息，请参阅监视策略设置中的应用程序故障监视策略。

**趋势 \> 应用程序探测结果**页面显示站点中过去 24 小时和 7 天内运行的应用程序探测结果。有关如何配置应用程序探测的更多详细信息，请参阅应用程序探测。

### 应用程序探测

应用程序探测可自动检查站点中发布的 Citrix Virtual Apps™ 的运行状况。应用程序探测的结果可在 Director 中查看。

要求：

- Delivery Controller 运行版本 7.18 或更高版本。
- 运行探测代理的端点计算机是安装了 Citrix Receiver for Windows 4.8 或更高版本，或者 Citrix Workspace app for Windows（以前称为 Citrix Receiver for Windows）1808 或更高版本的 Windows 计算机。不支持适用于统一 Windows 平台 (UWP) 的 Workspace 应用程序。
- Director 和 StoreFront™ 支持默认的基于表单的身份验证。

运行应用程序探测所需的用户帐户/权限：

- 在每个端点计算机上用于探测的唯一 StoreFront 用户。StoreFront 用户无需是管理员；探测可以在非管理员上下文中运行。
- 具有 Windows 管理员权限的用户帐户，用于在端点计算机上安装和配置 Citrix 探测代理
- 具有以下权限的完全管理员用户帐户或自定义角色。将现有用户帐户重新用于应用程序探测可能会导致用户从其活动会话中注销。
    - 交付组权限：
        - 只读
    - Director 权限：
        - 创建\\编辑\\删除警报电子邮件服务器配置 - 如果电子邮件服务器尚未配置
        - 创建\\编辑\\删除探测配置
        - 查看配置页面
        - 查看趋势页面

**配置应用程序探测**

您可以安排应用程序探测在非高峰时段跨多个地理区域运行。全面的探测结果有助于在用户遇到问题之前，对与应用程序、托管计算机或连接相关的问题进行故障排除。

Citrix Probe Agent 2103 版支持站点聚合。可以从聚合站点枚举和启动应用程序和桌面。配置探测代理时，选择“**Workspace (StoreFront) 站点聚合已启用**”选项以启用从聚合站点枚举应用程序和桌面。支持以下站点组合：

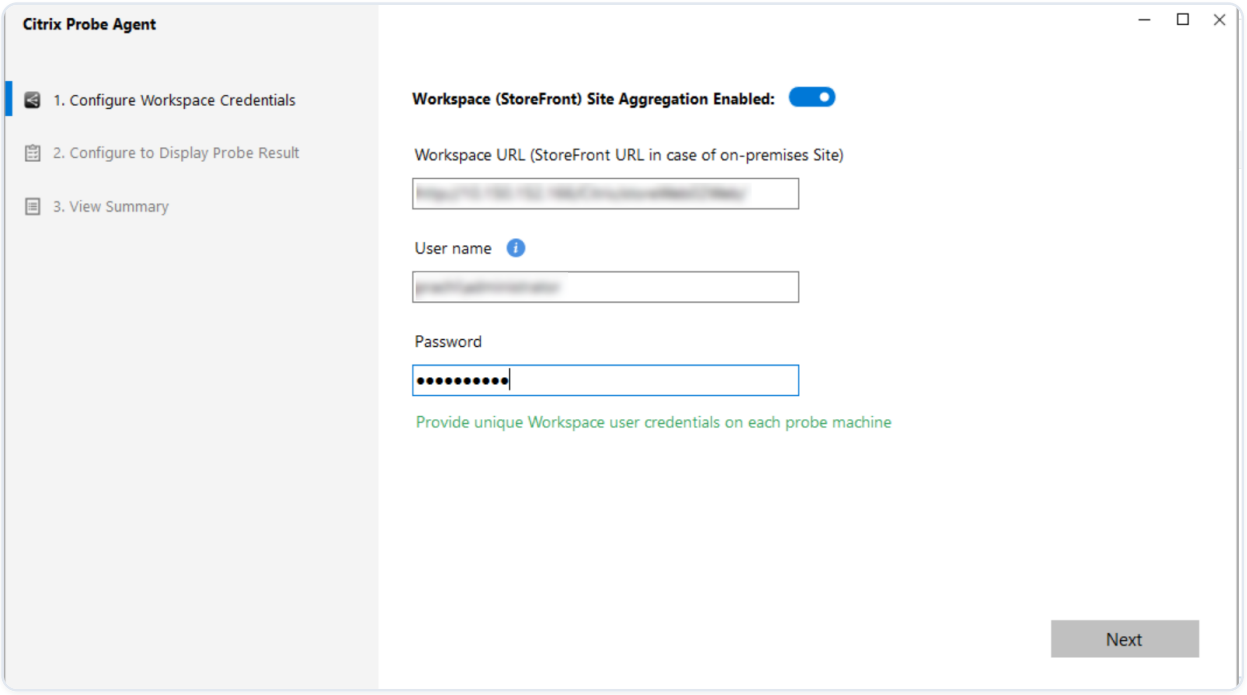
- 具有一个 StoreFront URL 的多个本地站点。
- 具有 StoreFront 或 Workspace URL 的本地和云站点。
- 具有一个 Workspace URL 的多个云站点。

> **注意：**
>
> 您必须创建单独的管理员或用户来配置只能访问一个站点的探测。

### 步骤 1：安装和配置 CITRIX PROBE AGENT

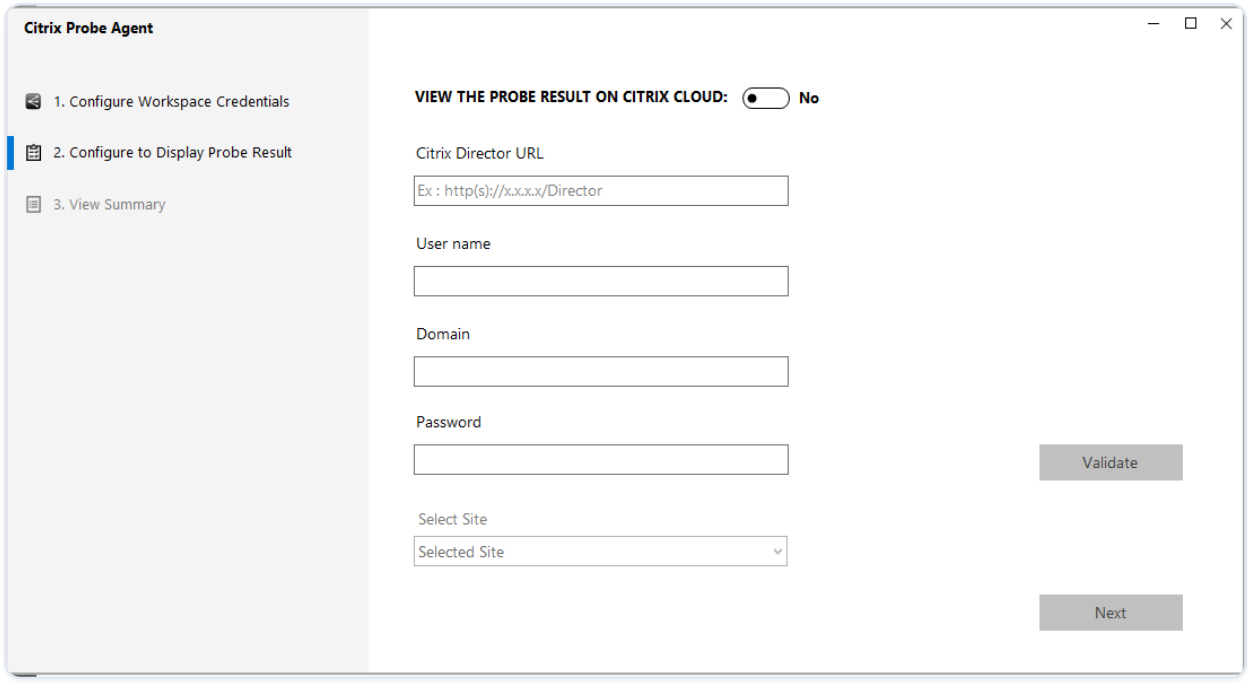
Citrix 探测代理是一个 Windows 可执行文件，它模拟用户通过 StoreFront 实际启动应用程序的过程。它根据 Director 中的配置测试应用程序启动，并将结果报告回 Director。

1. 确定要运行应用程序探测的端点计算机。
2. 具有管理权限的用户可以在端点计算机上安装和配置 Citrix 探测代理。从 `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>` 下载 Citrix 探测代理可执行文件
3. 启动代理并配置您的 StoreFront Receiver for Web 凭据。在每个端点计算机上配置一个唯一的 StoreFront 用户。凭据经过加密并安全存储。




> **注意：**
>
> 要从网络外部访问要探测的站点，请在 StoreFront URL 字段中键入 Citrix Gateway 的登录 URL。Citrix Gateway 会自动将请求路由到相应的站点 StoreFront URL。此功能适用于 Citrix Gateway 12.1 及更高版本（RfWebUI 主题）以及 Delivery Controllers 1811 及更高版本。

4. 在“**配置以显示探测结果**”选项卡中，输入您的 Director 凭据，然后单击“**验证**”。




5. 选择您的站点，然后单击**下一步**。

### 步骤 2: 在 DIRECTOR 中配置应用程序探测

**限制：**

如果从启用了交互式登录消息横幅的 Windows VDA 启动测试应用程序，探测将失败。这是因为在等待接受交互式登录消息时会发生超时。 要在服务器 VDA 上禁用登录消息。转到“计算机配置”>“Windows 设置”>“安全设置”>“本地策略”>“安全选项”。

删除以下字段中的文本并更新 Microsoft 策略。

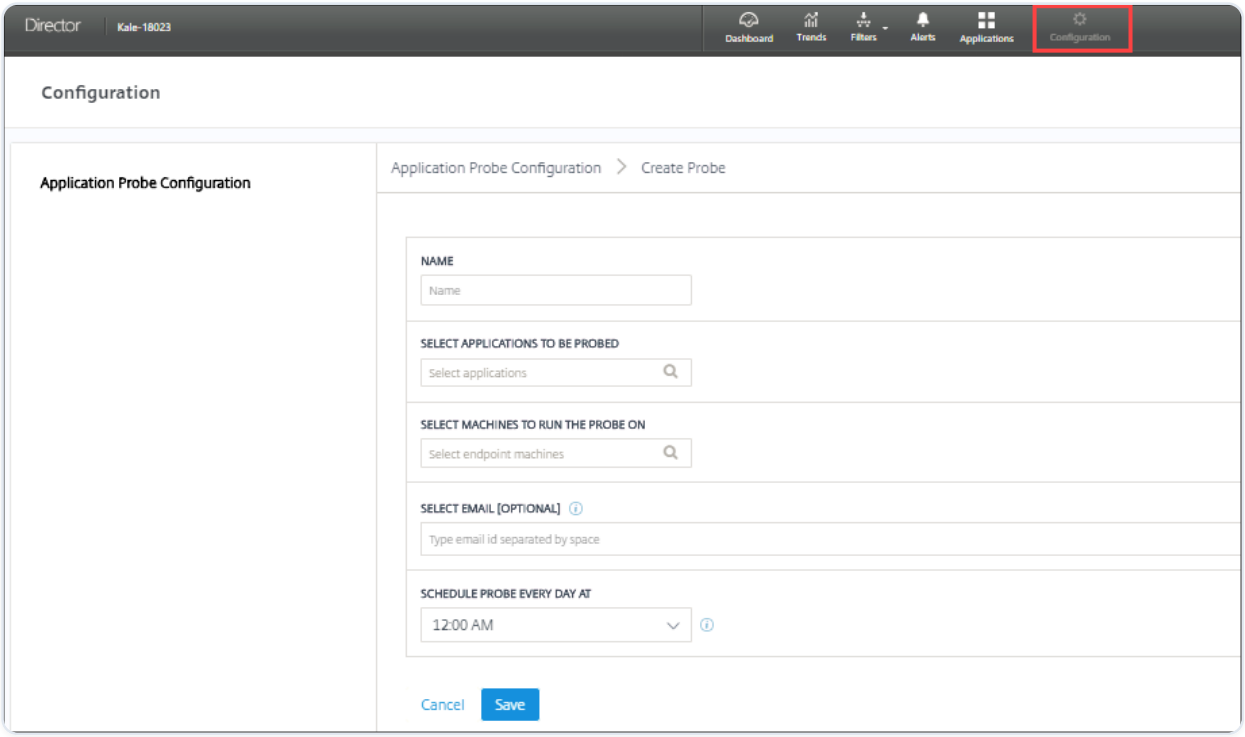
- 交互式登录：尝试登录用户的消息文本
- 交互式登录：尝试登录用户的消息标题

将探测用户分配给此已禁用交互式登录消息横幅的特定服务器 VDA，以确保探测可以越过“应用程序启动”状态。

> 有关详细信息，请参阅 `<https://learn.microsoft.com/zh-cn/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`。

1. 转到 **配置** \> **应用程序探测配置**。
2. 创建探测并选择：
   - 要探测的应用程序，
   - 必须运行探测的端点计算机，
   - 发送失败探测结果的电子邮件地址（在**警报** -\> **电子邮件服务器配置**中配置您的电子邮件服务器），和
   - 探测必须运行的一天中的时间（根据端点计算机的本地时区）。

   在 Director 中配置后，代理需要 10 分钟才能准备好开始探测。然后，它会在下一个小时开始运行配置的探测。




### 步骤 3：探测执行

代理根据其定期从 Director 获取的探测配置运行应用程序探测。它使用 StoreFront 串行启动选定的应用程序。代理通过 Monitor 数据库将结果报告回 Director。故障在五个特定阶段报告：

- **StoreFront 可达性** - 配置的 StoreFront URL 不可达。
- **StoreFront 身份验证** - 配置的 StoreFront 凭据无效。

- **StoreFront 枚举** - StoreFront 枚举应用程序列表不包含要探测的应用程序。
- **ICA® 下载** - ICA 文件不可用。
- **应用程序启动** – 应用程序无法启动。

#### 步骤 4：查看探测结果

您可以在**应用程序**页面中查看最新的探测结果。

Director 应用程序分析页面(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-app-analytics.png)

要进一步排查故障，请点击探测结果链接，在 **趋势** \> **应用程序探测结果** 页面上查看更多详细信息。

Director 应用程序探测结果(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-app-probing-trends.png)

此页面上提供过去 24 小时或过去 7 天时间段的整合探测结果数据。您可以查看探测失败的阶段。您可以根据特定应用程序、探测失败阶段或端点计算机筛选表格。

### 桌面探测

桌面探测可自动检查在站点中发布的 Citrix Virtual Desktops™ 的运行状况。桌面探测的结果可在 Director 中查看。

在 Director 的“配置”页面中，配置要探测的桌面、运行探测的端点计算机以及探测时间。代理使用 StoreFront™ 测试所选桌面的启动，并将结果报告回 Director。探测结果显示在 Director UI 中——“应用程序”页面上显示最近 24 小时的数据，历史探测数据则显示在 **趋势 > 探测结果 > 桌面探测结果** 页面上。在此，您可以查看探测失败发生的阶段 - StoreFront 可达性、StoreFront 身份验证、StoreFront 枚举、ICA 下载或桌面启动。故障报告将发送到配置的电子邮件地址。您可以安排桌面探测在非高峰时段跨多个地理区域运行。全面的结果有助于在用户遇到问题之前主动排查与预配桌面、托管计算机或连接相关的问题。桌面探测适用于高级版许可站点。此功能需要 Delivery Controllers 7 1906 或更高版本以及 Probe Agent 1903 或更高版本。

要求：

- Delivery Controller™ 运行版本 1906 或更高版本。
- 运行探测代理的端点计算机是安装了 Citrix Receiver for Windows 4.8 或更高版本，或 Citrix Workspace app for Windows（以前称为 Citrix Receiver for Windows）1906 或更高版本的 Windows 计算机。不支持适用于统一 Windows 平台 (UWP) 的 Workspace 应用程序。
- Director 和 StoreFront 支持默认的基于表单的身份验证。

运行桌面探测所需的用户帐户或权限：

- 每个端点计算机上用于探测的唯一 StoreFront 用户。StoreFront 用户无需是管理员；探测可以在非管理员上下文中运行。
- 具有 Windows 管理员权限的用户帐户，用于在端点计算机上安装和配置 Citrix Probe Agent
- 具有以下权限的完全管理员用户帐户或自定义角色。将普通用户帐户重新用于桌面探测可能会导致用户从其活动会话中注销。
    - 交付组权限：
        - 只读
    - Director 权限：
        - 创建、编辑、删除警报电子邮件服务器配置 - 如果电子邮件服务器尚未配置
        - 创建、编辑、删除探测配置
        - 查看配置页面
        - 查看趋势页面

**配置桌面探测**

您可以安排桌面探测在非高峰时段跨多个地理区域运行。全面的探测结果有助于在用户遇到问题之前排查与桌面、托管计算机或连接相关的问题。

Citrix Probe Agent 2103 版支持站点聚合。可以从聚合站点枚举和启动应用程序和桌面。配置探测代理时，选择“**Workspace (StoreFront) 站点聚合已启用**”选项以启用从聚合站点枚举应用程序和桌面。支持以下站点组合：

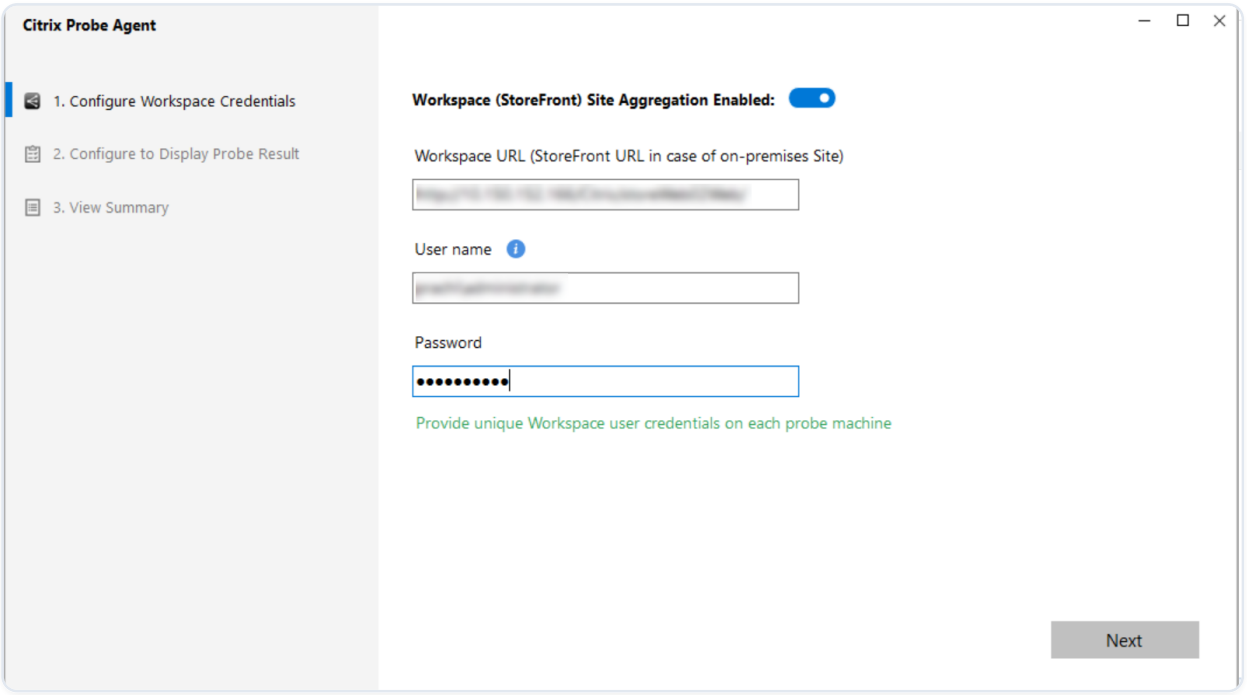
- 具有一个 StoreFront URL 的多个本地站点。
- 具有 StoreFront 或 Workspace URL 的本地和云站点。
- 具有一个 Workspace URL 的多个云站点。

> **注意：**
>
> 您必须创建单独的管理员或用户来配置只能访问一个站点的探测。

#### 步骤 1：安装和配置 CITRIX PROBE AGENT

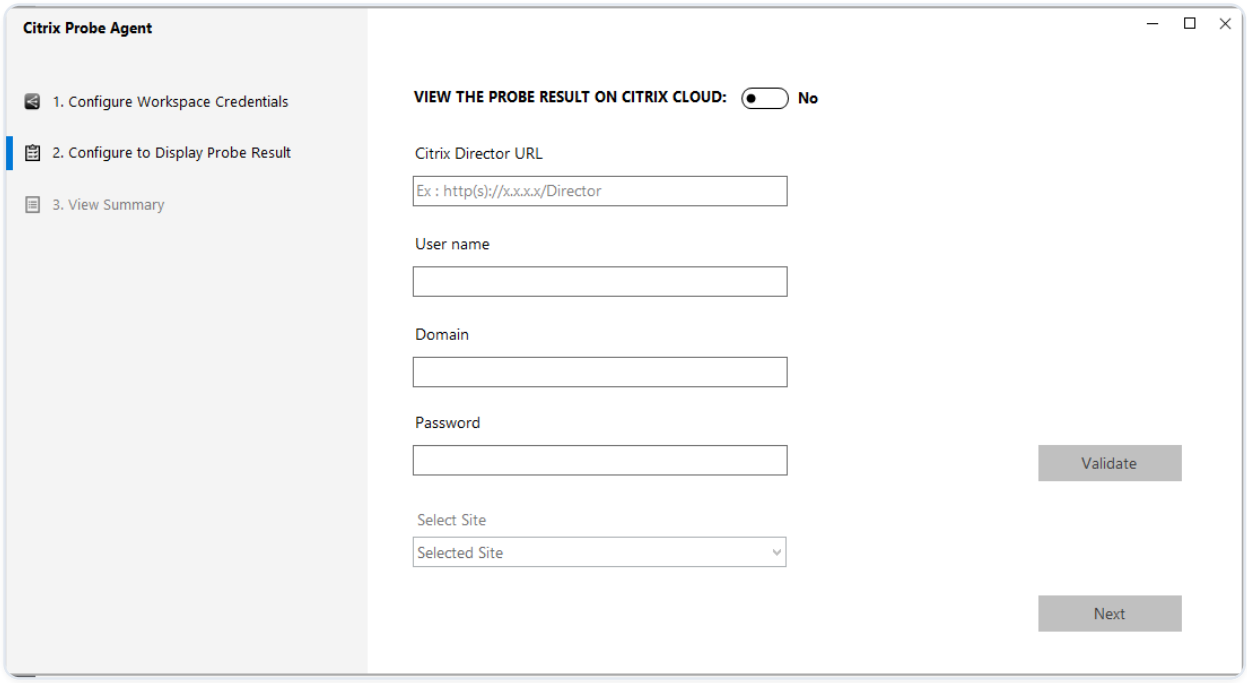
Citrix Probe Agent 是一个 Windows 可执行文件，它模拟用户通过 StoreFront 实际启动桌面的过程。它根据 Director 中的配置测试桌面启动，并将结果报告回 Director。

1. 识别要运行桌面探测的端点计算机。
2. 具有管理权限的用户可以在端点计算机上安装和配置 Citrix 探测代理。在 `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>` 下载 Citrix 探测代理可执行文件。
3. 启动代理并配置您的 StoreFront Receiver for Web 凭据。在每台端点计算机上配置一个唯一的 StoreFront 用户。凭据经过加密并安全存储。




> **注意：**
>
> - 要从网络外部访问要探测的站点，请在 StoreFront URL 字段中键入 Citrix Gateway 登录页面 URL。Citrix Gateway 会自动将请求路由到相应的站点 StoreFront URL。此功能适用于 Citrix Gateway 12.1 或更高版本以及 Delivery Controllers 1811 或更高版本。
> - 您必须为配置的唯一 StoreFront 用户启用交互式登录。

4. 在“**配置以显示探测结果**”选项卡中，输入您的 Director 凭据，然后单击“**验证**”。




5. 选择您的站点，然后单击**下一步**。

### 步骤 2：在 DIRECTOR 中配置桌面探测

**限制：**

如果从启用了交互式登录消息横幅的 Windows VDA 启动桌面测试，探测将失败。这是因为等待接受交互式登录消息会导致超时。 要在服务器 VDA 上禁用登录消息。转到“计算机配置”>“Windows 设置”>“安全设置”>“本地策略”>“安全选项”。

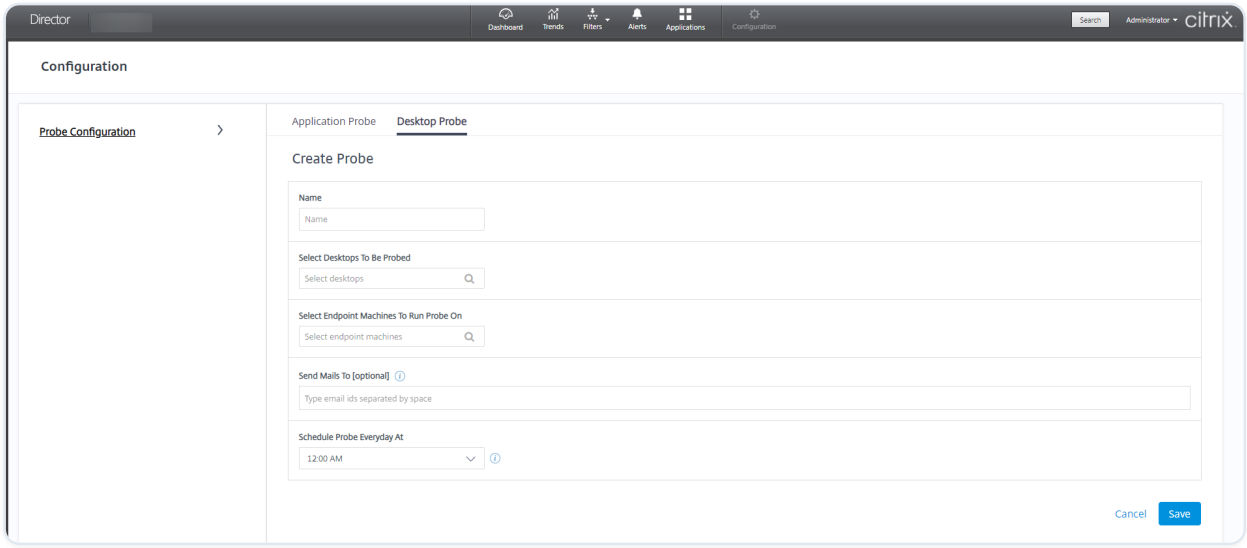
删除以下字段中的文本并更新 Microsoft 策略。

- 交互式登录：尝试登录用户的消息文本
- 交互式登录：尝试登录用户的消息标题

将探测用户分配给此已禁用交互式登录消息横幅的特定服务器 VDA，以确保探测能够通过桌面启动状态。

有关详细信息，请参阅 `<https://learn.microsoft.com/zh-cn/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`。

1. 转到 **配置** > **桌面探测配置**。
2. 要创建探测，请输入详细信息并单击 **Save**。




**注意：**

在 **Alerts** > **Email Server Configuration** 中配置您的电子邮件服务器。

桌面探测配置完成后，代理需要 10 分钟才能准备好开始探测。然后，它会在下一个小时开始运行配置的探测。

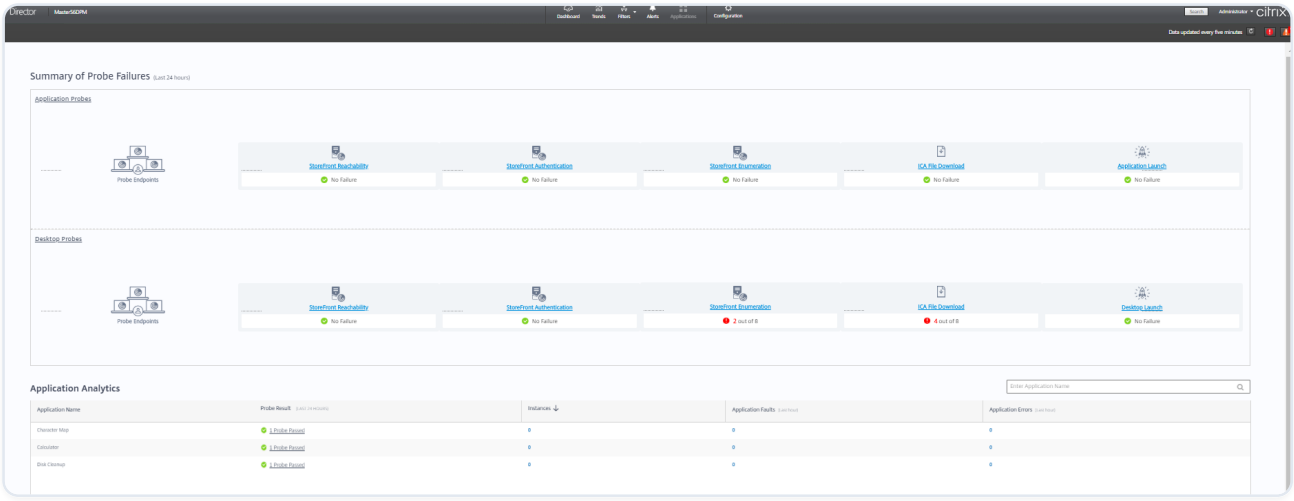
### 步骤 3：探测执行

代理根据其定期从 Director 获取的探测配置运行桌面探测。它使用 StoreFront 串行启动选定的桌面。代理通过 Monitor 数据库将结果报告回 Director。故障在五个特定阶段报告：

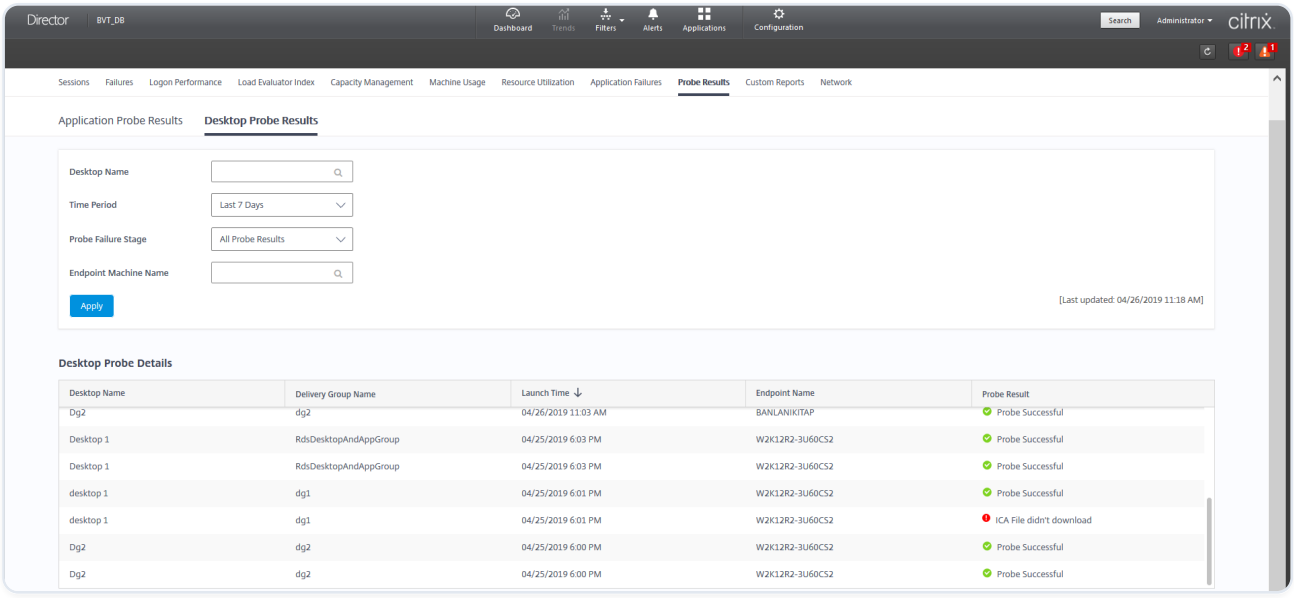
- **StoreFront 可达性** - 配置的 StoreFront URL 不可达。
- **StoreFront 身份验证** - 配置的 StoreFront 凭据无效。
- **StoreFront 枚举** - StoreFront 枚举桌面列表中不包含要探测的桌面。
- **ICA® 下载** - ICA 文件不可用。
- **桌面启动** – 无法启动桌面。

### 步骤 4：查看探测结果

您可以在**桌面**页面中查看最新的探测结果。




要进一步进行故障排除，请单击探测结果链接以在**趋势** >**探测结果** > **桌面探测结果**页面上查看更多详细信息。




此页面上提供了过去 24 小时或过去 7 天的合并探测结果数据。您可以查看探测失败的阶段。您可以按特定桌面、探测失败阶段或端点计算机筛选表格。

## 排查计算机故障

> **注意：**
>
> **Citrix Health Assistant** 是一款用于排查未注册 VDA 中配置问题的工具。该工具可自动执行多项运行状况检查，以识别 VDA 注册失败以及会话启动和时区重定向配置中问题的可能根本原因。知识中心文章 Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch 包含 **Citrix Health Assistant** 工具的下载和使用说明。

> Director 控制台中的“**筛选器 > 计算机**”视图显示了站点中配置的计算机。“多会话操作系统计算机”选项卡包含负载评估器索引，该索引指示性能计数器的分布以及将鼠标悬停在链接上时会话计数的工具提示。

单击失败计算机的“**故障原因**”列，以获取故障的详细描述以及建议的故障排除操作。计算机和连接故障的故障原因及建议操作可在 Citrix Director 7.12 故障原因疑难解答指南 中找到。

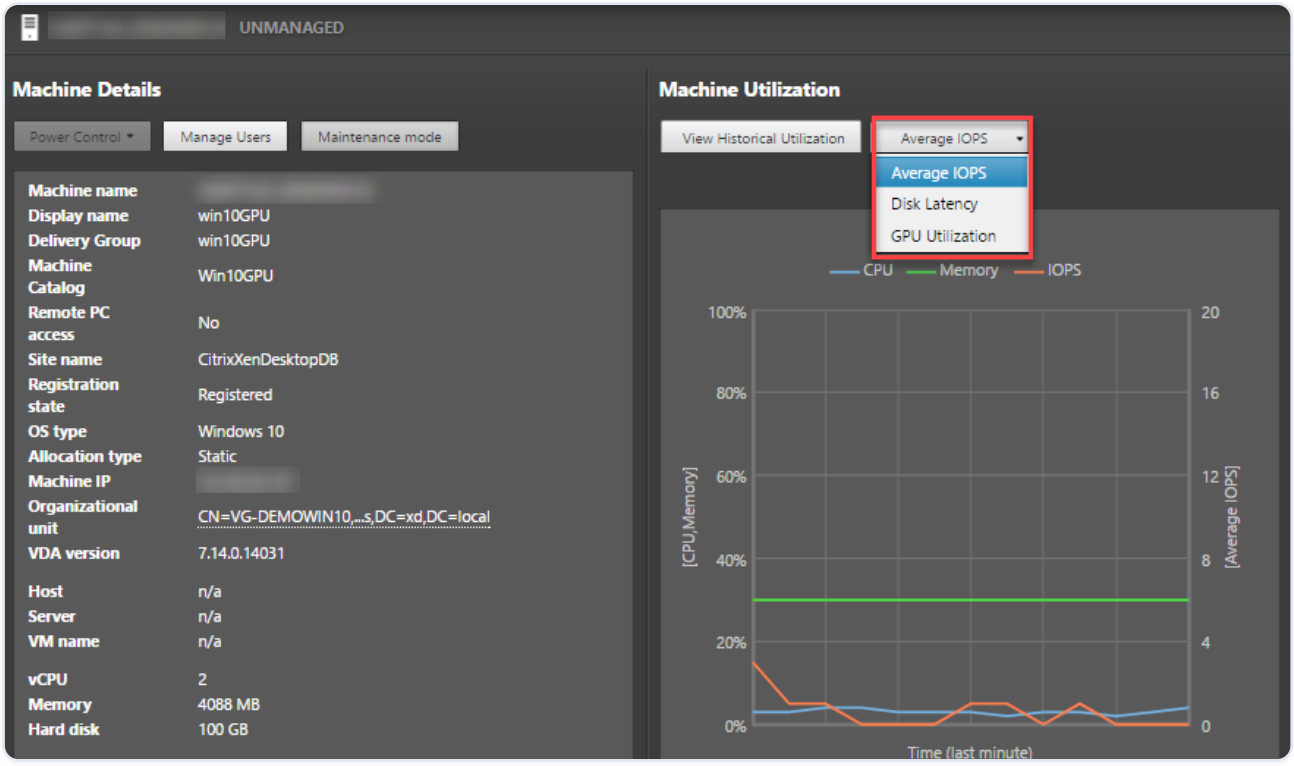
单击计算机名称链接可转到“**计算机详细信息**”页面。

“计算机详细信息”页面列出了计算机详细信息、基础结构详细信息以及应用于计算机的热修复程序详细信息。

### 基于计算机的实时资源利用率

“**计算机利用率**”面板显示 CPU 和内存的实时利用率图表。此外，对于具有 Delivery Controller 和 VDA 版本 **7.14** 或更高版本的站点，还提供磁盘和 GPU 监视图表。

磁盘监视图表、平均 IOPS 和磁盘延迟是重要的性能测量指标，可帮助您监视和排查与 VDA 磁盘相关的问题。平均 IOPS 图表显示磁盘的平均读写次数。选择**磁盘延迟**可查看数据请求与数据从磁盘返回之间的延迟图表，以毫秒为单位。



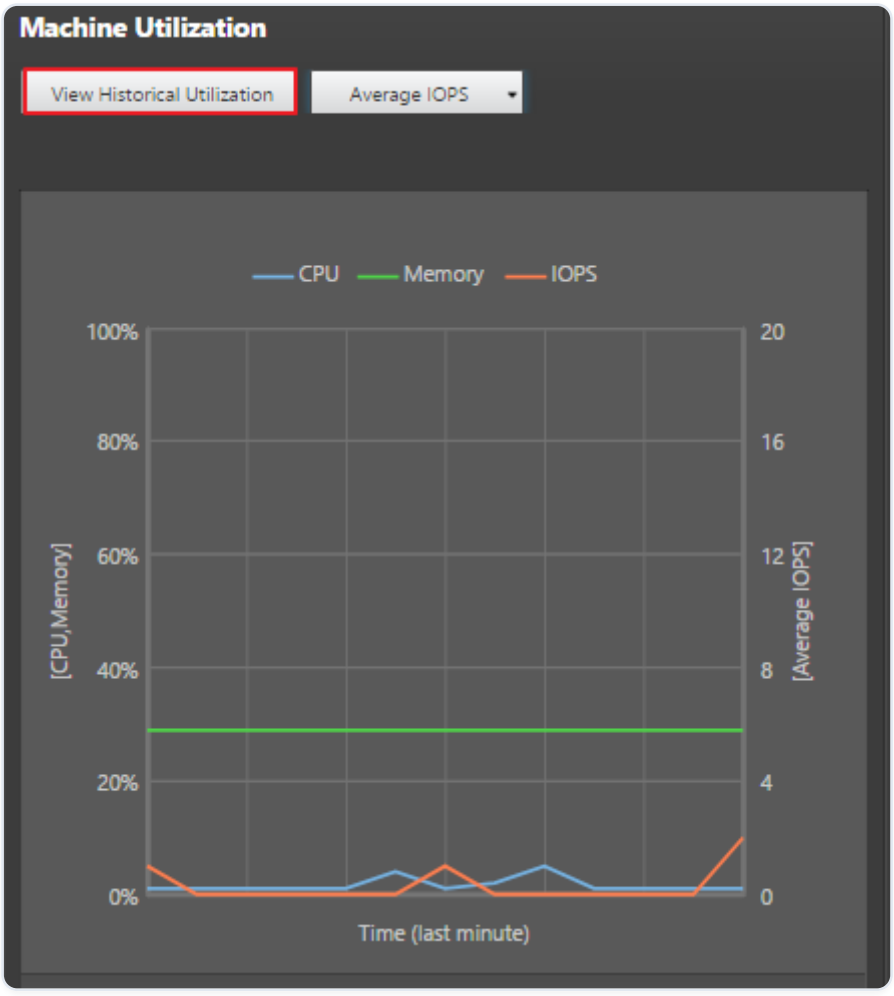

选择“**GPU 利用率**”以查看 GPU、GPU 内存以及编码器和解码器的百分比利用率，从而解决服务器或单会话操作系统 VDA 上的 GPU 相关问题。GPU 利用率图表仅适用于运行 64 位 Windows 且配备 NVIDIA Tesla M60 GPU 并运行显示驱动程序版本 369.17 或更高版本的 VDA。 VDA 必须启用 HDX™ 3D Pro 才能提供 GPU 加速。有关详细信息，请参阅适用于 Windows 单会话操作系统的

GPU 加速和适用于 Windows 多会话操作系统的 GPU 加速。 当 VDA 访问多个 GPU 时，利用率图表会显示从各个 GPU 收集的 GPU 指标的平均值。GPU 指标是针对整个 VDA 收集的，而不是针对单个进程。

### 基于计算机的历史资源利用率

在“**计算机利用率**”面板中，单击“**查看历史利用率**”以查看所选计算机上的资源历史使用情况。 利用率图表包括 CPU、内存、并发会话峰值、平均 IOPS 和磁盘延迟的关键性能计数器。

> **注意：**
>
> 必须将监视策略设置“**启用进程监视**”设置为“允许”才能在“历史计算机利用率”页面上的“前 10 个进程”表中收集和显示数据。默认情况下禁止收集。
>
> 默认情况下会收集 CPU 和内存利用率、平均 IOPS 以及磁盘延迟数据。您可以使用“**启用资源监视**”策略设置禁用此收集。

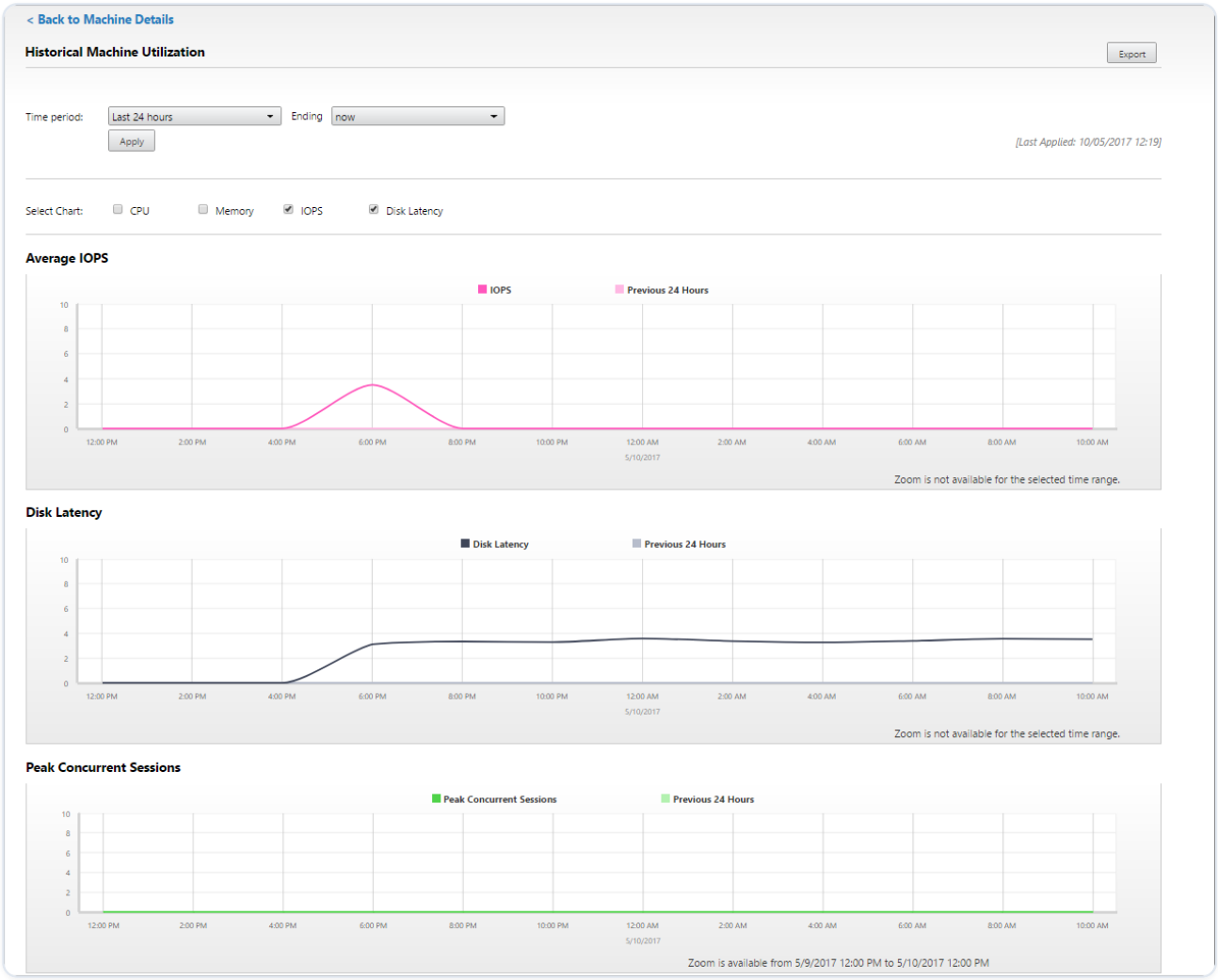



1. 在“**计算机详细信息**”视图的“**计算机利用率**”面板中，选择“**查看历史利用率**”。

2. 在“**历史计算机利用率**”页面中，设置“**时间段**”以查看过去 2 小时、24 小时、7 天、月或年的使用情况。

> **注意：**
>
> 平均 IOPS 和磁盘延迟使用情况数据仅适用于截至目前的过去 24 小时、月和年。不支持自定义结束时间。

3. 单击“**应用**”并选择所需的图表。
4. 将鼠标悬停在图表的不同部分上，以查看所选时间段的更多信息。




例如，如果您选择“**最近 2 小时**”，则基线周期是所选时间范围之前的 2 小时。查看最近 2 小时和基线时间的 CPU、内存和会话趋势。如果您选择“**上个月**”，则基线周期是上个月。选择查看上个月和基线时间的平均 IOPS 和磁盘延迟。

1. 单击“**导出**”以导出所选时间段的资源利用率数据。有关详细信息，请参阅“监视部署”中的 导出报告 部分。

2. 在图表下方，表格列出了基于 CPU 或内存利用率排名前 10 位的进程。您可以按任意列进行排序，这些列显示选定时间范围内的应用程序名称、用户名、会话 ID、平均 CPU、峰值 CPU、平均内存和峰值内存。IOPS 和磁盘延迟列无法排序。

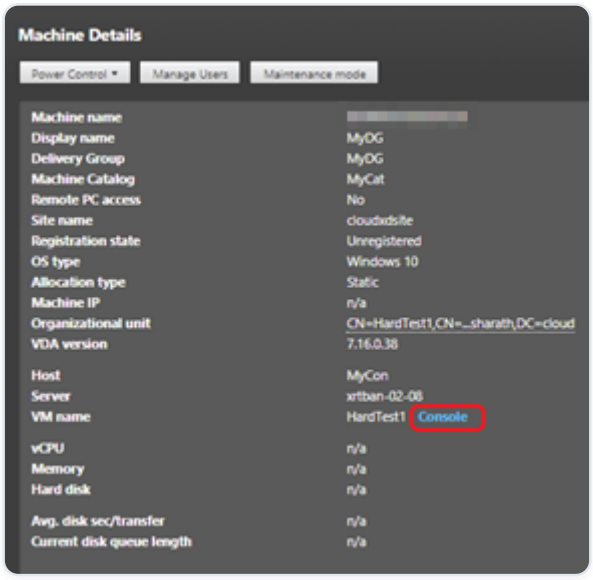
   > **注意：**
   >
   > 系统进程的会话 ID 显示为“0000”。

3. 要查看特定进程的资源消耗历史趋势，请深入查看任意排名前 10 位的进程。

### 计算机控制台访问

您可以直接从 Director 访问托管在 XenServer 7.3 版及更高版本上的单会话和多会话操作系统计算机的控制台。这样，您无需 XenCenter 即可排查 XenServer 托管的 VDA 上的问题。要使用此功能，需要满足以下条件：

- 需要 7.16 版或更高版本的 Delivery Controller。
- 托管计算机的 XenServer 必须是 7.3 版或更高版本，并且必须可从 Director UI 访问。




要排查计算机问题，请单击相应“计算机详细信息”面板中的**控制台**链接。在您提供的主机凭据通过身份验证后，计算机控制台将在单独的选项卡中打开，使用基于 Web 的 VNC 客户端 noVNC。您现在可以通过键盘和鼠标访问控制台。

> **注意：**

- Internet Explorer 11 不支持此功能。
- 如果计算机控制台上的鼠标指针未对齐，请参阅 CTX230727，了解解决此问题的步骤。
- Director 在新选项卡中启动控制台访问，请确保您的浏览器设置允许弹出窗口。
- 出于安全原因，Citrix® 建议您在浏览器上安装 SSL 证书。

### Microsoft RDS 许可证运行状况

您可以在多会话操作系统计算机的“**计算机详细信息**”和“**用户详细信息**”页面中的“计算机详细信息”面板中查看 Microsoft RDS 许可证的状态。




将显示以下消息之一：

- 许可证可用
- 配置不正确（警告）
- 许可证错误（错误）
- VDA 版本不兼容（错误）

**注意：**

处于宽限期且具有有效许可证的计算机的 Microsoft RDS 许可证运行状况状态以绿色显示“**许可证可用**”消息。请在许可证过期前续订。

对于警告和错误消息，将鼠标悬停在信息图标上可查看下表中提供的其他信息。

| 消息类型 | DIRECTOR 中的消息 |
| --- | --- |
| 错误 | 适用于 VDA 7.16 及更高版本。 |
| 错误 | 不允许新的 RDS 连接。 |
| 错误 | Microsoft RDS 许可证已超出其宽限期。 |
| 错误 | 未为所需的操作系统级别配置具有按设备客户端访问许可类型的许可证服务器。 |
| 错误 | 配置的许可证服务器与具有按设备客户端访问许可类型的 RDS 主机操作系统级别不兼容。 |
| 警告 | 个人终端服务器在 Citrix Virtual Apps and Desktops™ 部署中不是有效的 RDS 许可类型。 |
| 警告 | 远程桌面管理在 Citrix Virtual Apps and Desktops 部署中不是有效的许可类型。 |
| 警告 | 未配置 RDS 许可类型。 |
| 警告 | 使用按用户客户端访问 RDS 许可类型时，域控制器或许可证服务器不可访问。 |
| 警告 | 使用按设备客户端访问许可类型时，由于所需操作系统级别的许可证服务器不可访问，因此无法确定客户端设备许可证。 |

**注意：**

此功能仅适用于 Microsoft RDS CAL（客户端访问许可证）。

# 解决用户问题

使用 Director 的**帮助台**视图（**活动管理器**页面）查看有关用户的信息：

- 检查有关用户的登录、连接和应用程序的详细信息。
- 对用户的计算机进行影子会话。
- 录制 ICA® 会话。
- 使用下表中的建议操作对问题进行故障排除，如果需要，将问题上报给相应的管理员。

## 故障排除技巧

| 用户问题 | 建议 |
| --- | --- |
| 登录时间过长或间歇性/反复失败 | 诊断用户登录问题 |
| 会话启动时间过长或间歇性/反复失败 | 诊断会话启动问题 |
| 应用程序运行缓慢或无响应 | 解决应用程序故障 |
| 连接失败 | 恢复桌面连接 |
| 会话运行缓慢或无响应 | 恢复会话 |
| 录制会话 | 录制会话 |
| 视频运行缓慢或质量不佳 | 运行 HDX 通道系统报告 |

> **注意：** 为确保计算机未处于维护模式，请从“用户详细信息”视图中检查“计算机详细信息”面板。

## 搜索技巧

在“搜索”字段中键入用户名时，Director 会在 Active Directory 中搜索所有配置为支持 Director 的站点中的用户。

当您在“搜索”字段中键入多用户计算机名称时，Director 会显示指定计算机的“计算机详细信息”。

在“搜索”字段中键入端点名称时，Director 会使用连接到特定端点的未经身份验证（匿名）和已通过身份验证的会话，这有助于对未经身份验证的会话进行故障排除。确保端点名称是唯一的，以便对未经身份验证的会话进行故障排除。

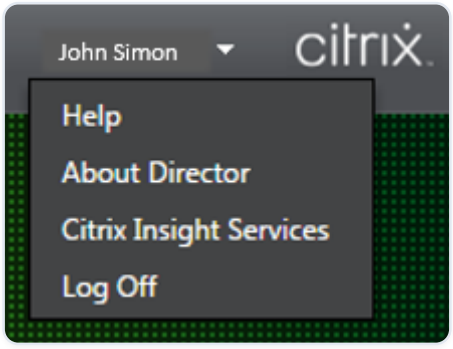
搜索结果还包括当前未在使用或未分配到计算机的用户。

- 搜索不区分大小写。
- 部分输入会生成可能的匹配项列表。
- 键入两部分名称（用户名、姓氏和名字或显示名称）的几个字母后，用空格分隔，结果将包含两个字符串的匹配项。例如，如果键入 jo rob，结果可能包括“John Robertson”或 Robert, Jones 等字符串。

要返回登录页面，请单击 **Director 徽标**。

### 访问 Citrix 洞察服务

您可以从 Director 中的**用户**下拉列表中访问 Citrix Insight Services (CIS)，以获取额外的诊断见解。CIS 中可用的数据来自包括 Call Home 和 Citrix Scout 在内的源。




#### 将故障排除信息上传到 Citrix 技术支持

从单个 Delivery Controller™ 或 VDA 运行 Citrix Scout，以捕获关键数据点和 Citrix Diagnostics Facility (CDF) 跟踪，从而对选定的计算机进行故障排除。Scout 能够将数据安全地上传到 CIS 平台，以协助 Citrix 技术支持进行故障排除。Citrix 技术支持使用 CIS 平台来缩短解决客户报告问题所需的时间。

Scout 随 Citrix Virtual Apps and Desktops™ 组件一起安装。根据 Windows 版本，当您安装或升级到 Citrix Virtual Apps and Desktops 时，Scout 会出现在 Windows“开始”菜单或“开始”屏幕中。

要启动 Scout，请从“开始”菜单或“开始”屏幕中选择 Citrix \> Citrix Scout。

有关使用和配置 Scout 以及常见问题解答的信息，请参阅 CTX130147。

### 诊断会话启动问题

除了 诊断用户登录问题 部分中提到的登录过程阶段之外，Director 还显示会话启动持续时间。这在**用户详细信息**页面和**计算机详细信息**页面上分为 Workspace App 会话启动持续时间和 VDA 会话启动持续时间。这两个持续时间进一步包含各个阶段，其启动持续时间也一并显示。此数据有助于您了解和排查会话启动持续时间过长的问题。此外，会话启动中涉及的每个阶段的时间持续时间有助于排查与各个阶段相关的问题。例如，如果驱动器映射时间过长，您可以检查 GPO 或脚本中是否正

确映射了所有有效驱动器。此功能适用于 Delivery Controller 7 1906 及更高版本以及 VDA 1903 及更高版本。

### 先决条件

确保满足以下先决条件才能显示会话启动持续时间数据：

- Delivery Controller™ 7 1906 或更高版本。
- VDA 1903 或更高版本。
- Citrix End User Experience Monitoring (EUEM) 服务必须在 VDA 上运行。

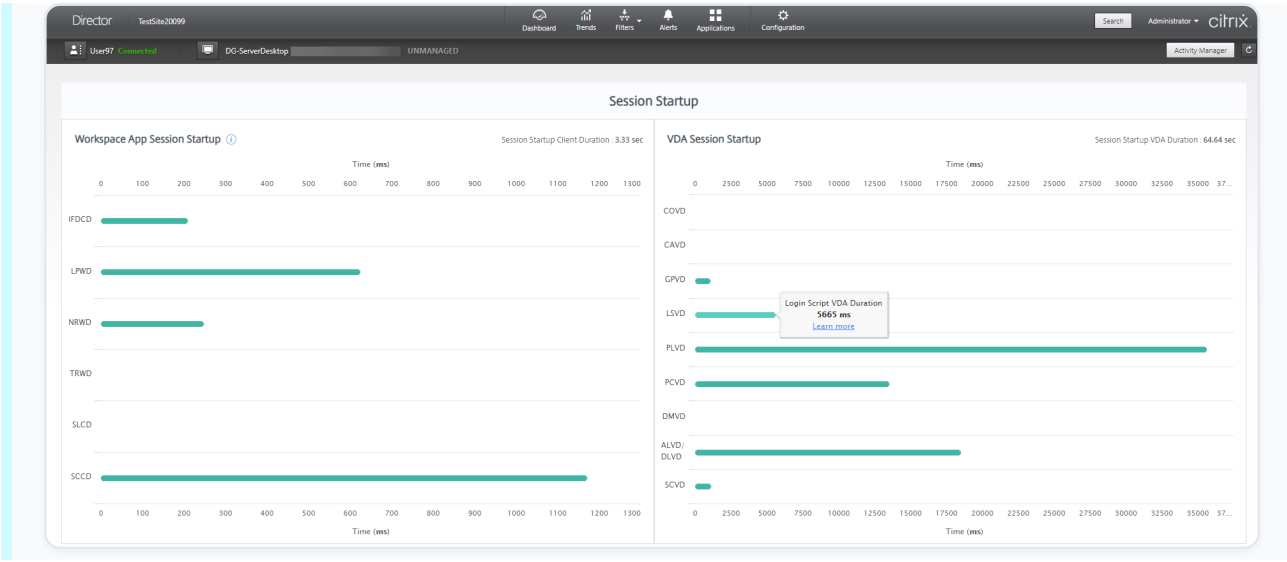
### 限制

当 Director 显示会话启动持续时间数据时，存在以下限制。

- 会话启动持续时间仅适用于 HDX™ 会话。
- 对于从 iOS 和 Android OS 启动的会话，仅提供 VDA 启动持续时间。
- 仅当从浏览器启动时检测到 Workspace App 时，ICA® 文件下载持续时间 (IFDCD) 才可用。
- 对于从 macOS 启动的会话，IFDCD 仅适用于 Workspace App 1902 或更高版本。
- 对于从 Windows OS 启动的会话，IFDCD 适用于 Workspace app 1902 及更高版本。对于早期版本，IFDCD 仅显示从浏览器启动且检测到 Workspace app 的应用程序。

**注意：**

- 如果满足先决条件后会话启动持续时间显示出现问题，请按照 CTX130320 中所述查看 Director 服务器和 VDA 日志。 对于共享会话（在同一会话中启动多个应用程序），Workspace App 启动指标将显示最新连接或最新应用程序启动的数据。
- VDA 会话启动中的某些指标不适用于重新连接。在这种情况下，将显示一条消息。




## Workspace 应用程序会话启动阶段

### 会话启动客户端持续时间 (SSCD)

当此指标较高时，表示存在导致启动时间过长的客户端问题。查看后续指标以确定问题的可能根本原因。SSCD 尽可能接近请求时间（鼠标点击）开始计时。它在客户端设备和 VDA 之间的 ICA 连接建立时结束。在共享会话的情况下，此持续时间会小得多，因为与创建到服务器的新连接相关的大部分设置成本都不会发生。在下一层级，有几个详细指标可用。

### ICA 文件下载持续时间 (IFDCD)

这是客户端从服务器下载 ICA 文件所需的时间。整个过程如下：

1. 用户点击 Workspace 应用程序中的资源（应用程序或桌面）。
2. 用户的请求通过 Citrix Gateway（如果已配置）发送到 StoreFront™，后者将请求发送到 Delivery Controller。
3. Delivery Controller 为请求找到一台可用计算机，并将计算机信息和其他详细信息发送到 StoreFront。此外，StoreFront 从安全票证颁发机构请求并接收一次性票证。
4. StoreFront 生成一个 ICA 文件，并通过 Citrix Gateway（如果已配置）将其发送给用户。

IFDCD 表示完成整个过程（步骤 1-4）所需的时间。当客户端收到 ICA 文件时，IFDCD 持续时间停止计时。

LPWD 是此过程的 StoreFront 组件。

如果 IFDCD 较高（但 LPWD 正常），则启动的服务器端处理成功，但客户端设备和 StoreFront 之间存在通信问题。这通常是由于两台计算机之间的网络问题造成的。因此，您可以首先排查潜在的网络问题。

#### 启动页面 WEB 服务器持续时间 (LPWD)

这是在 StoreFront 上处理启动页面 (launch.aspx) 所需的时间。如果 LPWD 较高，则 StoreFront 上可能存在瓶颈。

可能的原因包括：

- StoreFront 上的高负载。尝试通过检查 Internet Information Services (IIS) 日志和监控工具、任务管理器、性能监视器等来找出导致速度变慢的原因。
- StoreFront 在与 Delivery Controller 等其他组件通信时遇到问题。检查 StoreFront 和 Delivery Controller 之间的网络连接是否缓慢，或者某些 Delivery Controller 是否已关闭或过载。

#### 名称解析 WEB 服务器持续时间 (NRWD)

这是 Delivery Controller 将已发布的应用程序/桌面名称解析为 VDA 计算机 IP 地址所需的时间。

当此指标较高时，表示 Delivery Controller 解析已发布的应用程序名称到 IP 地址所需的时间较长。

可能的原因包括客户端出现问题、Delivery Controller 出现问题（例如 Delivery Controller 过载）或它们之间的网络链接出现问题。

#### 票证响应 WEB 服务器持续时间 (TRWD)

此持续时间表示从安全票证颁发机构 (STA) 服务器或 Delivery Controller 获取票证（如有必要）所需的时间。当此持续时间较高时，表示 STA 服务器或 Delivery Controller 过载。

#### 会话查找客户端持续时间 (SLCD)

此持续时间表示查询每个会话以托管所请求的已发布应用程序所需的时间。在客户端执行检查，以确定现有会话是否可以处理应用程序启动请求。所使用的方法取决于会话是新建的还是共享的。

#### 会话创建客户端持续时间 (SCCD)

此持续时间表示从 wfica32.exe（或类似的等效文件）启动到建立连接所需的时间。

### VDA 会话启动阶段

#### 会话启动 VDA 持续时间 (SSVD)

此持续时间是高级别的服务器端连接启动指标，它涵盖了 VDA 执行整个启动操作所需的时间。当此指标较高时，表示存在 VDA 问题导致会话启动时间增加。这包括 VDA 执行整个启动操作所花费的时间。

#### 凭据获取 VDA 持续时间 (COVD)

VDA 获取用户凭据所需的时间。

如果用户未能及时提供凭据，此持续时间可能会人为增加。因此，它不包含在 VDA 启动持续时间中。仅当使用手动登录并显示服务器端凭据对话框（或在登录开始前显示法律声明）时，此时间才可能显著。

#### 凭据身份验证 VDA 持续时间 (CAVD)

这是 VDA 针对身份验证提供程序验证用户凭据所需的时间。它们可以是 Kerberos、Active Directory 或安全支持提供程序接口 (SSPI)。

#### 组策略 VDA 持续时间 (GPVD)

此持续时间是登录期间应用组策略对象所需的时间。

#### 登录脚本执行 VDA 持续时间 (LSVD)

这是 VDA 运行用户登录脚本所需的时间。

考虑将用户或组的登录脚本设置为异步。考虑优化任何应用程序兼容性脚本或改用环境变量。

#### 配置文件加载 VDA 持续时间 (PLVD)

这是 VDA 加载用户配置文件所需的时间。

如果此持续时间较长，请考虑您的用户配置文件配置。漫游配置文件的大小和位置会导致会话启动缓慢。当用户登录到启用了终端服务漫游配置文件和主文件夹的会话时，漫游配置文件内容和对该文件夹的访问会在登录期间进行映射。这会占用额外的资源。有时，这会消耗大量的 CPU 使用率。考虑使用带有重定向个人文件夹的 **终端服务主** 文件夹来缓解此问题。通常，考虑使用 Citrix Profile Management 在 Citrix 环境中管理用户配置文件。如果您正在使用 Citrix Profile Management 并且登录时间较慢，请检查您的防病毒软件是否正在阻止 Citrix Profile Management 工具。

#### 打印机创建 VDA 持续时间 (PCVD)

这是 VDA 同步映射用户客户端打印机所需的时间。如果配置设置为异步执行打印机创建，则不会记录 PCVD 的值，因为它不影响会话启动的完成。

映射打印机所花费的时间过长通常是打印机自动创建策略设置的结果。用户客户端设备上本地添加的打印机数量以及您的打印配置会直接影响会话启动时间。会话启动时，Citrix Virtual Apps and Desktops™ 必须在客户端设备上创建每个本地映射的打印机。考虑重新配置打印策略，以减少创建的打印机数量，尤其是在用户拥有许多本地打印机时。为此，请在 Delivery Controller 和 Citrix Virtual Apps and Desktops 中编辑“打印机自动创建”策略。

#### 驱动器映射 VDA 持续时间 (DMVD)

这是 VDA 映射用户客户端驱动器、设备和端口所花费的时间。

确保您的基本策略包含禁用未使用的虚拟通道的设置。例如，音频或 COM 端口映射，以优化 ICA 协议并提高整体会话性能。

#### 应用程序/桌面启动 VDA 持续时间 (ALVD/DLVD)

此阶段是 Userinit 和 Shell 持续时间的组合。当用户登录到 Windows 计算机时，winlogon 会运行 userinit.exe。Usernit.exe 运行登录脚本，重新建立网络连接，然后启动 Explorer.exe。Userinit 表示从 userinit.exe 启动到虚拟桌面或应用程序用户界面启动之间的时间。Shell 持续时间是指从用户界面初始化到用户获得键盘和鼠标控制之间的时间。

#### 会话创建 VDA 持续时间 (SCVD)

此时间包括 VDA 上会话创建时间中的任何杂项延迟。

## 诊断用户登录问题

使用登录持续时间数据排查用户登录问题。

登录持续时间仅针对使用 HDX 首次连接到桌面或应用程序时进行测量。此数据不包括尝试使用远程桌面协议连接或从断开连接的会话重新连接的用户。具体而言，当用户最初使用非 HDX 协议连接并使用 HDX 重新连接时，不测量登录持续时间。

在用户详细信息视图中，持续时间显示为数值。在此数值下方，显示登录发生的时间以及登录过程各阶段的图表。

当用户登录到 Citrix Virtual Apps and Desktops™ 时，Monitor Service 会跟踪登录过程的各个阶段。这些阶段从用户通过 Citrix Workspace™ 应用程序连接时开始，直到桌面准备就绪可供使用。

左侧的大数字是总登录时间。这是通过将建立连接和从 Delivery Controller™ 获取桌面所花费的时间与对虚拟桌面进行身份验证和登录所花费的时间相结合计算得出的。持续时间信息以秒（或秒的分数）为单位显示。

### 先决条件

请确保满足以下先决条件，以便显示登录持续时间数据和深入分析：

1. 在 VDA 上安装 **赛睿用户配置文件管理器** 和 **赛睿用户配置文件管理器 WMI 插件**。
2. 确保 Citrix Profile Management Service 正在运行。
3. 对于 XenApp 和 XenDesktop 7.15 及更早版本站点，请禁用 GPO 设置“**不处理旧版运行列表**”。
4. 必须启用审核进程跟踪才能进行交互式会话深入分析。
5. 对于 GPO 深入分析，请增加组策略操作日志的大小。

> **注意：**

- 登录持续时间仅在默认 Windows 外壳程序 (explorer.exe) 上受支持，而不支持自定义外壳程序。
- 仅当在 Remote PC Access 安装期间将 **Citrix User Profile Manager** 和 **Citrix User Profile Manager WMI Plugin** 作为额外组件安装时，Remote PC Access 的登录持续时间才可用。有关详细信息，请参阅 Remote PC Access 配置和序列注意事项 中的步骤 4。

### 排查用户登录问题的步骤

1. 在**用户详细信息**视图中，使用登录持续时间面板排查登录状态。
   - 如果用户正在登录，视图会反映登录过程。
   - 如果用户已登录，登录持续时间面板会显示用户登录到当前会话所花费的时间。
2. 检查登录过程的各个阶段。

### 登录过程阶段

#### 代理

决定为用户分配哪个桌面所花费的时间。

#### VM 启动

如果会话需要启动计算机，VM 启动是启动虚拟机所需的时间。

#### HDX 连接

完成从客户端到虚拟机的 HDX 连接设置所需步骤的时间。

#### 身份验证

完成远程会话身份验证所需的时间。

#### GPO

如果在虚拟机上启用了组策略设置，这是登录期间应用组策略对象所需的时间。当您将鼠标悬停在 GPO 栏上时，会显示一个工具提示，其中包含根据 CSE（客户端扩展）应用每个策略所花费时间的详细信息。(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-gpo-drilldown.png) 单击**详细钻取**可查看包含策略状态和相应 GPO 名称的表。钻取中的持续时间仅表示 CSE 处理时间，不计入总 GPO 时间。您可以复制钻取表以进行进一步故障排除或在报告中使用。策略的 GPO 时间是从事件查看器日志中检索的。日志可能会根据为操作日志分配的内存（默认大小为 4 MB）而被覆盖。有关增加操作日志大小的更多信息，请参阅 Microsoft TechNet 文章 配置事件日志。

#### 登录脚本

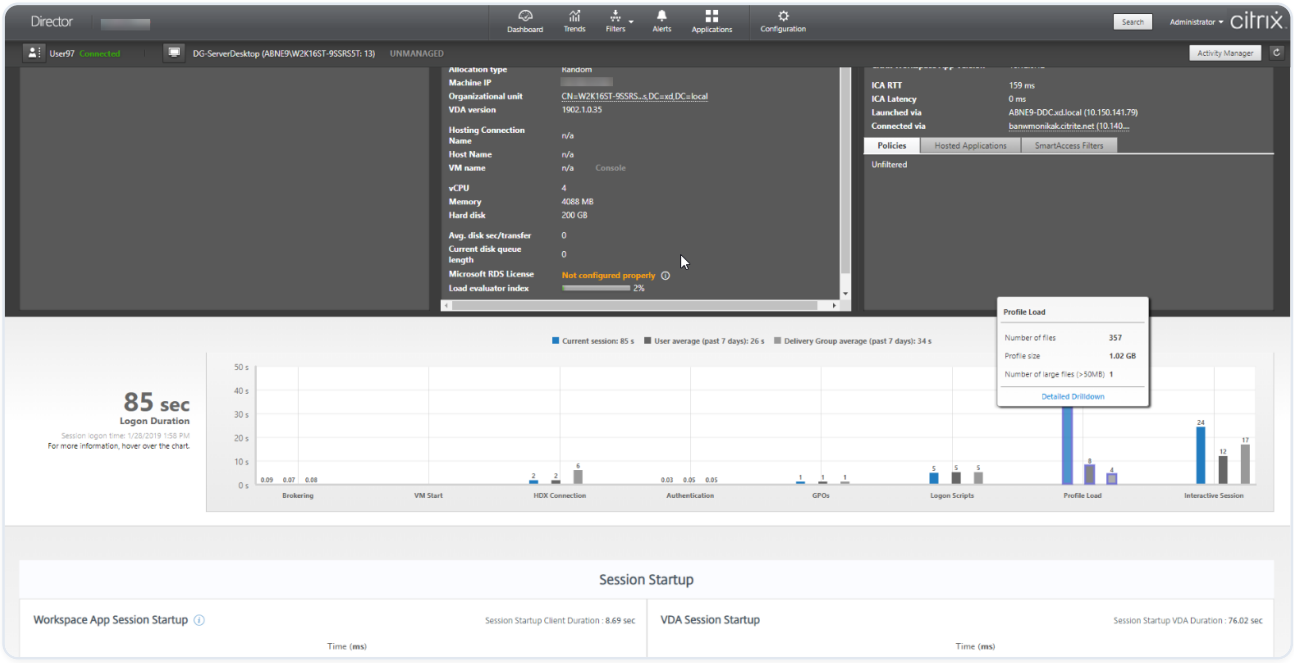
如果为会话配置了登录脚本，则这是运行登录脚本所需的时间。

### 配置文件加载

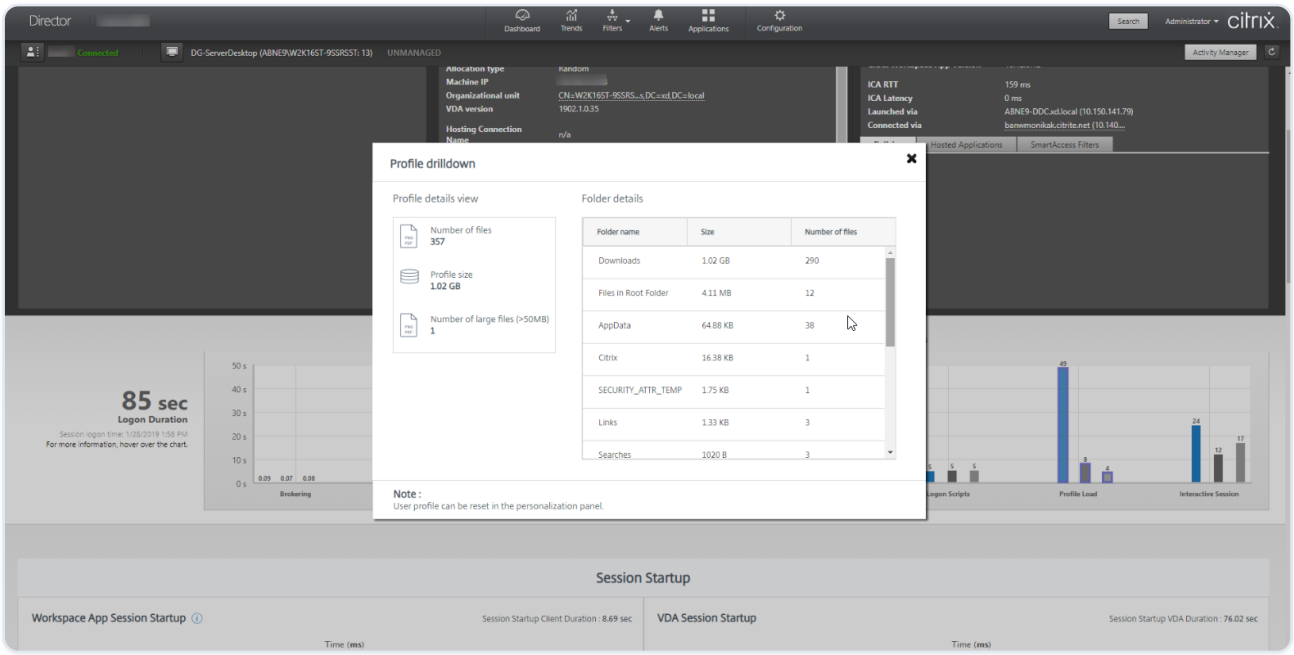
如果为用户或虚拟机配置了配置文件设置，则这是配置文件加载所需的时间。

如果配置了 Citrix Profile Management，配置文件加载栏会包含 Citrix Profile Management 处理用户配置文件所花费的时间。此信息有助于管理员排查配置文件处理持续时间过长的问题。配置 Profile Management 后，配置文件加载栏会显示增加的持续时间。此增加是由此增强功能引起的，并不表示性能下降。此增强功能适用于 VDA 1903 或更高版本。

将鼠标悬停在“配置文件加载”栏上会显示一个工具提示，其中显示当前会话的用户配置文件详细信息。




单击**详细钻取**可进一步钻取配置文件根文件夹（例如，C:/Users/username）中的每个单独文件夹、其大小以及文件数量（包括嵌套文件夹中的文件）。



配置文件深入分析功能适用于 Delivery Controller 7 1811 或更高版本以及 VDA 1811 或更高版本。使用配置文件深入分析信息，您可以解决配置文件加载时间过长的问题。您可以：

- 重置用户配置文件
- 通过删除不需要的大文件来优化配置文件
- 减少文件数量以减少网络负载
- 使用配置文件流

默认情况下，配置文件根目录中的所有文件夹都显示在向下钻取中。要隐藏文件夹可见性，请在 VDA 计算机上编辑以下注册表值：

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

1. 在 VDA 上，在 HKEY_LOCAL_MACHINE\Software\Citrix\Director\ 下添加新的注册表值 **ProfileFoldersNameHidden**。
2. 将值设置为 1。此值必须是 DWORD（32 位）值。现在已禁用文件夹名称可见性。
3. 要使文件夹名称再次可见，请将值设置为 0。

> **注意：** 您可以使用 GPO 或 PowerShell 命令在多台计算机上应用注册表值更改。有关使用 GPO 部署注册表更改的更多信息，请参阅博客。

附加信息

- 配置文件深入分析不考虑重定向的文件夹。
- 根文件夹中的 NTUser.dat 文件可能对最终用户不可见。但是，它们包含在配置文件向下钻取中，并显示在“**根文件夹**”的文件列表中。
- AppData 文件夹中的某些隐藏文件不包含在配置文件钻取中。
- 由于某些 Windows 限制，文件数量和配置文件大小数据可能与“个性化”面板中的数据不匹配。

### 交互式会话

这是用户配置文件加载后，将键盘和鼠标控制权“移交”给用户所需的时间。它通常是登录过程所有阶段中最长的持续时间，计算方式为：**交互式会话持续时间 = 桌面就绪事件时间戳（VDA 上的 EventId 1000）- 用户配置文件加载事件时间戳（VDA 上的 EventId 2）**。交互式会话有三个子阶段：Pre-userinit、Userinit 和 Shell。将鼠标悬停在交互式会话上可查看显示以下内容的工具提示：

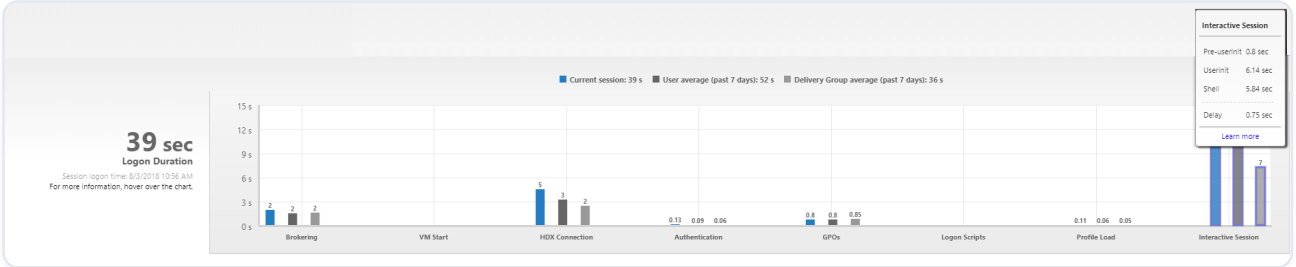
- 子阶段
- 每个子阶段所用的时间
- 这些子阶段之间的总累计时间延迟
- 文档链接。

> **注意：**
>
> 此功能适用于 VDA 1811 及更高版本。如果您在早于 7.18 的站点上启动了会话，然后升级到 7.18 或更高版本，则会显示“由于服务器错误，向下钻取不可用”消息。但是，如果您在升级后启动了会话，则不会显示错误消息。

> 要查看每个子阶段的时间持续时间，请在 VM (VDA) 上启用“审核进程跟踪”。当“审核进程跟踪”被禁用（默认）时，将显示 Pre-userinit 的时间持续时间以及 Userinit 和 Shell 的组合时间持续时间。您可以通过组策略对象 (GPO) 启用“审核进程跟踪”，如下所示：

1. 创建 GPO 并使用 GPO 编辑器对其进行编辑。
2. 转到 **计算机配置 > Windows 设置 > 安全设置 > 本地策略 > 审核策略**。
3. 在右侧窗格中，双击**审核进程跟踪**。
4. 选择**成功**，然后单击“确定”。
5. 将此 GPO 应用于所需的 VDA 或组。

有关审核进程跟踪以及启用或禁用它的详细信息，请参阅 Microsoft 文档中的审核进程跟踪。




“用户详细信息”视图中的“登录持续时间”面板。

- **交互式会话 – Pre-userinit：** 交互式会话中与组策略对象和脚本重叠的部分。可以通过优化 GPO 和脚本来缩短此子阶段。
- **交互式会话 – Userinit：** 当用户登录到 Windows 计算机时，Winlogon 会运行 userinit.exe。Userinit.exe 运行登录脚本，重新建立网络连接，然后启动 Windows 用户界面 Explorer.exe。交互式会话的此子阶段表示从 Userinit.exe 启动到虚拟桌面或应用程序用户界面启动之间的时间。
- **交互式会话 – Shell：** 在上一阶段，Userinit 启动 Windows 用户界面的初始化。Shell 子阶段捕获从用户界面初始化到用户获得键盘和鼠标控制之间的时间。
- **延迟：** 这是 **Pre-userinit 和 Userinit** 子阶段与 **Userinit 和 Shell** 子阶段之间的累计时间延迟。

总登录时间并非这些阶段的精确总和。例如，某些阶段并行发生，而在某些阶段，会发生更多处理，这可能导致登录持续时间长于总和。 总登录时间不包括 ICA® 空闲时间，即 ICA 文件下载与应用程序的 ICA 文件启动之间的时间。 要启用在应用程序启动时自动打开 ICA 文件，请将浏览器配置为在下载 ICA 文件时自动启动 ICA 文件。有关详细信息，请参阅 CTX804493。

> **注意：** 登录持续时间图表以秒为单位显示登录阶段。任何小于一秒的持续时间值都显示为亚秒值。大于一秒的值四舍五入到最接近的 0.5 秒。该图表设计为将最高的 Y 轴值显示为 200 秒。任何大于 200 秒的值都会在条形图上方显示实际值。

**故障排除技巧**

要识别图表中的异常或意外值，请将当前会话每个阶段所花费的时间与该用户过去七天的平均持续时间以及此交付组中所有用户过去七天的平均持续时间进行比较。

根据需要上报。例如，如果虚拟机启动缓慢，问题可能出在管理程序中，因此您可以将其上报给管理程序管理员。或者，如果代理时间缓慢，您可以将问题上报给站点管理员，以检查交付控制器上的负载平衡。

检查异常差异，包括：

- 缺少（当前）登录条
- 当前持续时间与此用户的平均持续时间之间存在重大差异。原因包括：
  - 安装了新应用程序。
  - 发生了操作系统更新。
  - 进行了配置更改。
  - 用户配置文件大小过大。在这种情况下，配置文件加载时间较长。
- 用户登录数据（当前和平均持续时间）与交付组平均持续时间之间存在重大差异。

如有需要，单击“**重新启动**”以观察用户的登录过程，从而排查虚拟机启动或代理等问题。

### 影子用户

在 Director 中，使用影子用户功能直接查看或操作用户的虚拟机或会话。您可以跟踪 Windows 或 Linux VDA。用户必须连接到您要跟踪的计算机。通过检查用户标题栏中列出的计算机名称来验证这一点。

Director 会在新选项卡中启动影子会话，请更新浏览器设置以允许来自 Director URL 的弹出窗口。

从“**用户详细信息**”视图访问影子功能。选择用户会话，然后在“活动管理器”视图或“会话详细信息”面板中单击“**影子**”。

#### 跟踪 Linux VDA

影子功能适用于版本 7.16 或更高版本的 Linux VDA，这些 VDA 运行 RHEL7.3 或 Ubuntu 16.04 版 Linux 发行版。

> **注意：**
>
> - VDA 必须可从 Director UI 访问，影子功能才能正常工作。因此，影子功能仅适用于与 Director 客户端位于同一内网中的 Linux VDA。
> - Director 使用 FQDN 连接到目标 Linux VDA。确保 Director 客户端可以解析 Linux VDA 的 FQDN。
> - VDA 必须安装 python websockify 和 x11vnc 软件包。
> - noVNC 连接到 VDA 使用 WebSocket 协议。默认情况下，使用 **ws://** WebSocket 协议。出于安全原因，Citrix 建议您使用安全的 **wss://** 协议。在每个 Director 客户端和 Linux VDA 上安装 SSL 证书。

> 按照 会话跟踪 中的说明配置 VDA 以进行影子操作。

1. 单击“**影子**”后，影子连接将初始化，并且用户设备上将显示确认提示。
2. 指示用户单击“**是**”以开始共享计算机或会话。
3. 管理员只能查看影子会话。

#### 跟踪 Windows VDA

Windows VDA 会话使用 Windows 远程协助进行影子化。在安装 VDA 时启用**用户 Windows 远程协助**功能。有关详细信息，请参阅启用或禁用功能。

1. 单击**影子化**后，影子化连接将初始化，并出现一个对话框，提示您打开或保存 .msrc 事件文件。
2. 如果未默认选择，请使用远程协助查看器打开事件文件。用户设备上将出现确认提示。
3. 指示用户单击“**是**”以开始机器或会话共享。
4. 如需更多控制，请要求用户共享键盘和鼠标控制。

#### 简化 MICROSOFT INTERNET EXPLORER 浏览器以进行影子化

配置您的 Microsoft Internet Explorer 浏览器，使其使用远程协助客户端自动打开下载的 Microsoft 远程协助 (.msra) 文件。

为此，您必须在组策略编辑器中启用“自动提示文件下载”设置：

计算机配置 \> 管理模板 \> Windows 组件 \> Internet Explorer \> Internet 控制面板 \> 安全页 \> Internet 区域 \> 自动提示文件下载。

默认情况下，此选项对本地 Intranet 区域中的站点启用。如果 Director 站点不在本地 Intranet 区域中，请考虑手动将该站点添加到此区域。

### 向用户发送消息

在 Director 中，向连接到一个或多个计算机的用户发送消息。使用此功能可发送有关管理操作的即时通知，例如即将进行的桌面维护、计算机注销和重新启动以及配置文件重置。

1. 在“活动管理器”视图中，选择用户，然后单击“详细信息”。
2. 在“用户详细信息”视图中，找到“会话详细信息”面板，然后单击“发送消息”。
3. 在“主题”和“消息”字段中键入您的消息信息，然后单击“发送”。

如果消息发送成功，Director 中将显示一条确认消息。该消息将显示在用户的计算机中。

如果消息发送失败，Director 中将显示一条错误消息。根据错误消息排查问题。完成后，再次键入主题和消息文本，然后再次单击“**重试**”。

### 解决应用程序故障

在**活动管理器**视图中，单击“应用程序”选项卡。您可以查看此用户有权访问的所有计算机上的所有应用程序，包括当前连接计算机的本地和托管应用程序，以及每个应用程序的状态。

> **注意：**
>
> 如果“应用程序”选项卡显示为灰色，请联系具有启用该选项卡权限的管理员。

> 此列表仅包含在会话中启动的应用程序。

对于多会话操作系统计算机和单会话操作系统计算机，应用程序会针对每个断开连接的会话列出。如果用户未连接，则不显示任何应用程序。

| 操作 | 描述 |
| --- | --- |
| 结束无响应的应用程序 | 选择无响应的应用程序，然后单击“结束应用程序”。应用程序终止后，请用户再次启动它。 |
| 结束无响应的进程 | 如果您具有所需权限，请单击“进程”选项卡。选择与应用程序相关或占用大量 CPU 资源或内存的进程，然后单击“结束进程”。但是，如果您没有终止进程所需的权限，则尝试结束进程会失败。 |
| 重新启动用户计算机 | 仅对于单会话操作系统计算机，对于选定的会话，单击“重新启动”。或者，从“计算机详细信息”视图中，使用电源控件重新启动或关闭计算机。指示用户再次登录，以便您可以重新检查应用程序。对于多会话操作系统计算机，重新启动选项不可用。请改为注销用户，然后让用户再次登录。 |
| 将计算机置于维护模式 | 如果计算机映像需要维护（例如修补程序或其他更新），请将计算机置于维护模式。在“计算机详细信息”视图中，单击“详细信息”并打开维护模式选项。上报给相应的管理员。 |

### 恢复桌面连接

在 Director 中，检查用户标题栏中当前计算机的用户连接状态。

如果桌面连接失败，将显示导致失败的错误，这有助于您决定如何进行故障排除。

| 操作 | 描述 |
| --- | --- |
| 确保计算机未处于维护模式 | 在“用户详细信息”页面上，确保维护模式已关闭。 |
| 重新启动用户计算机 | 选择计算机，然后单击**重新启动**。如果用户计算机无响应或无法连接，请使用此选项。例 |

| 操作 | 描述 |
| --- | --- |
| | 如，当计算机使用的 CPU 资源异常高，导致 CPU 无法使用时。 |

### 恢复会话

如果会话断开连接，它仍然处于活动状态，并且其应用程序会继续运行，但用户设备不再与服务器通信。

在“用户详细信息”视图中，在“**会话详细信息**”面板中排除会话故障。您可以查看当前会话的详细信息，由会话 ID 指示。

| 操作 | 描述 |
| --- | --- |
| 结束无响应的应用程序或进程 | 单击“**应用程序**”选项卡。选择任何无响应的应用程序，然后单击“**结束应用程序**”。同样，选择任何无响应的相应进程，然后单击“**结束进程**”。此外，结束占用异常高内存或 CPU 资源的进程，这可能会导致 CPU 无法使用。 |
| 断开 Windows 会话 | 单击“**会话控制**”，然后选择“**断开连接**”。此选项仅适用于已代理的多会话操作系统计算机。对于未代理的会话，此选项处于禁用状态。 |
| 从用户会话注销 | 单击“**会话控制**”，然后选择“**注销**”。 |

要测试会话，用户可以尝试重新登录。您还可以跟踪用户以更密切地监视此会话。

### 生成 HDX™ 通道系统报告

在**用户详细信息**视图中，检查用户计算机上 **HDX** 面板中 HDX 通道的状态。此面板仅在用户计算机使用 HDX 连接时可用。

如果出现消息指示信息当前不可用，请等待一分钟以刷新页面，或选择**刷新**按钮。HDX 数据更新所需时间比其他数据稍长。

单击错误或警告图标以获取更多信息。

> 提示：
>
> 您可以通过单击标题栏左上角的左右箭头，在同一对话框中查看其他通道的信息。

HDX 通道系统报告主要由 Citrix 支持部门用于进一步进行故障排除。

1. 在 HDX 面板中，单击下载系统报告。
2. 您可以查看或保存 .xml 报告文件。
    - 要查看 .xml 文件，请单击打开。.xml 文件将显示在与 Director 应用程序相同的窗口中。
    - 要保存 .xml 文件，请单击保存。将出现“另存为”窗口，提示您选择 Director 计算机上的位置以下载文件。

## 重置用户配置文件

**注意：**

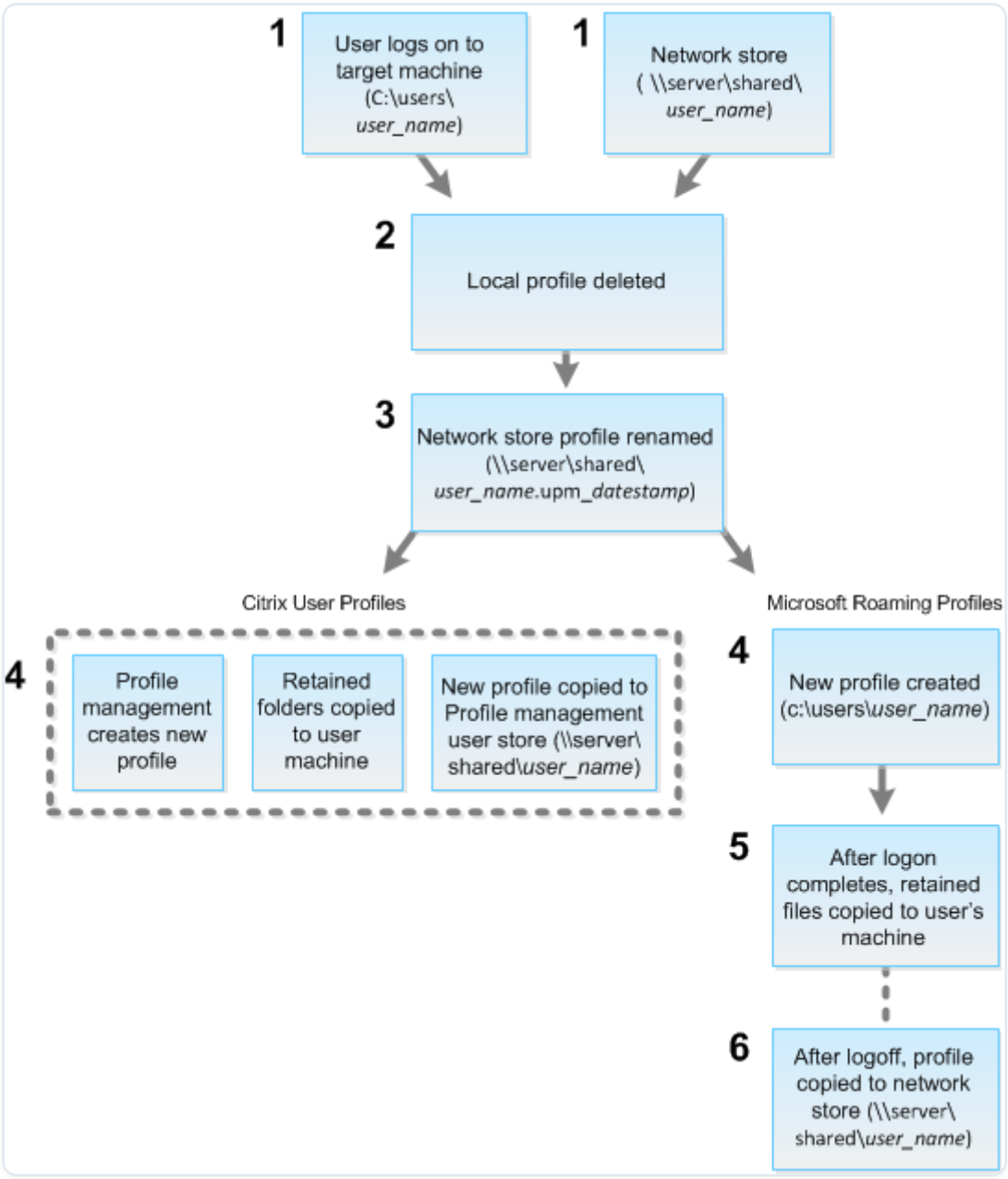
重置配置文件时，用户的文件夹和文件将保存并复制到新配置文件。但是，大多数用户配置文件数据会丢失（例如，注册表会被重置，应用程序设置可能会被删除）。

从 Profile Management 2106 开始，基于 Citrix Management 配置文件容器的用户配置文件解决方案提供了重置功能。

### 重置配置文件的处理方式

任何 Citrix 用户配置文件或 Microsoft 漫游配置文件都可以重置。用户注销后，如果您选择重置命令（在 Director 中或使用 PowerShell SDK），Director 会首先识别正在使用的用户配置文件并发出相应的重置命令。Director 通过 Profile Management 接收信息，包括配置文件大小、类型和登录时间等信息。

此图说明了用户登录后重置用户配置文件的过程。




Director 发出的重置命令指定了配置文件类型。然后，Profile Management 服务会尝试重置该类型的配置文件，并查找相应的网络共享（用户存储）。如果用户由 Profile Management 处理，但收到漫游配置文件命令，则该命令将被拒绝（反之亦然）。

1. 如果存在本地配置文件，则将其删除。
2. 网络配置文件已重命名。
3. 下一步操作取决于要重置的配置文件是 Citrix 用户配置文件还是 Microsoft 漫游配置文件。

   对于 Citrix 用户配置文件，新配置文件是使用 Profile Management 导入规则创建的。文件夹会复制回网络配置文件，用户可以正常登录。如果重置时使用了漫游配置文件，则漫游配置文件中的任何注册表设置都将保留在重置配置文件中。如有必要，您可以配置 Profile Management，使模板配置文件覆盖漫游配置文件。

对于 Microsoft 漫游配置文件，Windows 会创建一个配置文件，当用户登录时，文件夹会复制回用户设备。当用户再次注销时，新配置文件会复制到网络存储。

### 在 Director 中重置用户配置文件

如果您使用的是 Citrix Virtual Desktops™ (桌面 VDA)，请执行以下操作：

1. 在 **Director** 中，搜索要重置其配置文件的用户，然后选择此用户的会话。
2. 单击“**重置配置文件**”。
3. 指示用户从所有会话注销。
4. 指示用户重新登录。 从用户配置文件保存的文件夹和文件将复制到新配置文件中。

如果您使用的是 Citrix Virtual Desktops (服务器 VDA)，则需要登录才能执行配置文件重置。然后，用户需要注销并重新登录才能完成配置文件重置。

> **重要提示：**

> 如果用户在多个平台（例如 Windows 8 和 Windows 7）上拥有配置文件，请指示用户首先重新登录到用户报告为问题的同一桌面或应用程序。此登录操作可确保重置正确的配置文件。如果配置文件是 Citrix 用户配置文件，则在用户桌面出现时，配置文件已重置。如果配置文件是 Microsoft 漫游配置文件，则文件夹还原可能仍会短暂进行。用户必须保持登录状态，直到还原完成。

> 如果配置文件未成功重置（例如，用户无法成功重新登录到计算机或某些文件丢失），则必须手动还原原始配置文件。

请注意以下事项：

- 如果用户存储作为用户配置文件解决方案启用，则新配置文件包含原始用户配置文件中的以下个人文件夹：
  - 桌面
  - Cookie 文件
  - 收藏夹
  - 文档
  - 图片
  - 音乐

- 视频

- 如果 Citrix Management 配置文件容器作为整个用户配置文件解决方案启用，则新配置文件不包含上述个人文件夹。
- 在 Windows 8 及更高版本中，重置配置文件时，Cookie 不会复制到新配置文件。

### 手动恢复失败重置后的配置文件

1. 指示用户从所有会话注销。
2. 如果存在本地配置文件，请将其删除。
3. 在网络共享上找到存档文件夹，该文件夹的名称附加了日期和时间，即带有 .upm_datestamp 扩展名的文件夹。
4. 删除当前配置文件名称。即，不带 upm_datestamp 扩展名的那个。
5. 使用原始配置文件名称重命名存档文件夹。即，删除日期和时间扩展名。您已将配置文件恢复到其原始的、重置前的状态。

### 使用 PowerShell SDK 重置配置文件

您可以使用 Broker PowerShell SDK 重置配置文件。

#### NEW-BROKERMACHINECOMMAND

创建一个排队等待传送到特定用户、会话或计算机的命令。有关此 cmdlet 的更多信息，请参阅 `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>`。

#### 示例

有关如何使用 PowerShell cmdlet 重置配置文件的详细信息，请参阅以下示例：

重置配置文件管理配置文件

- 假设您要重置 user1 的配置文件。使用 New-BrokerMachineCommand PowerShell 命令。例如：

  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **重要提示：**

> `CommandData $byteArray` 必须采用以下格式：`<SID>[,<backup path>]`。如果您未提供备份路径，配置文件管理将生成一个以当前日期和时间命名的备份文件夹。

> 重置 Windows 漫游配置文件

- 假设您想重置 user1 的漫游配置文件。使用 New-BrokerMachineCommand PowerShell 命令。例如：
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

## 录制会话

您可以使用 Director 中**用户详细信息**和**计算机详细信息**屏幕上的会话录制控件来录制 ICA® 会话。此功能适用于 **Premium** 站点的客户。

要使用 DirectorConfig 工具在 Director 上配置会话录制，请参阅创建和激活录制策略中的**配置 Director 以使用会话录制服务器**部分。 仅当登录用户具有修改会话录制策略的权限时，Director 中才提供会话录制控件。此权限可以在会话录制授权控制台中设置，如创建和激活录制策略中所述。

> **注意：** 通过 Director 或会话录制策略控制台对会话录制设置所做的更改将从后续 ICA 会话开始生效。

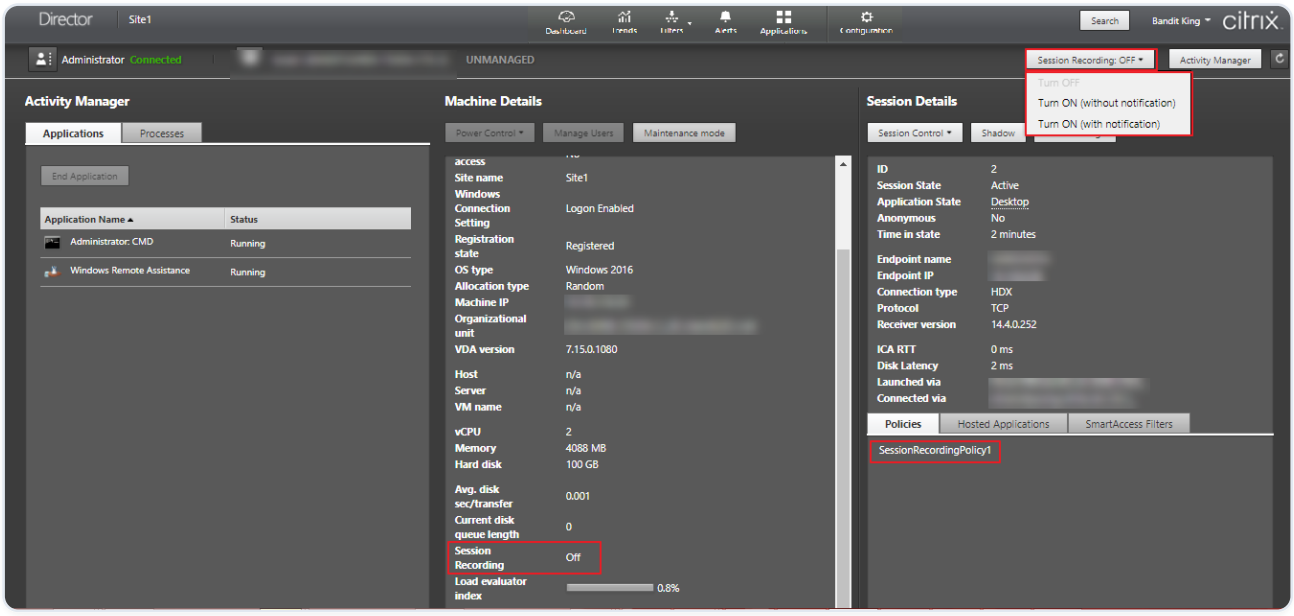
### Director 中的会话录制控件

您可以在**活动管理器**或**用户详细信息**屏幕上为特定用户启用会话录制。后续会话将为所有受支持服务器上的特定用户录制。

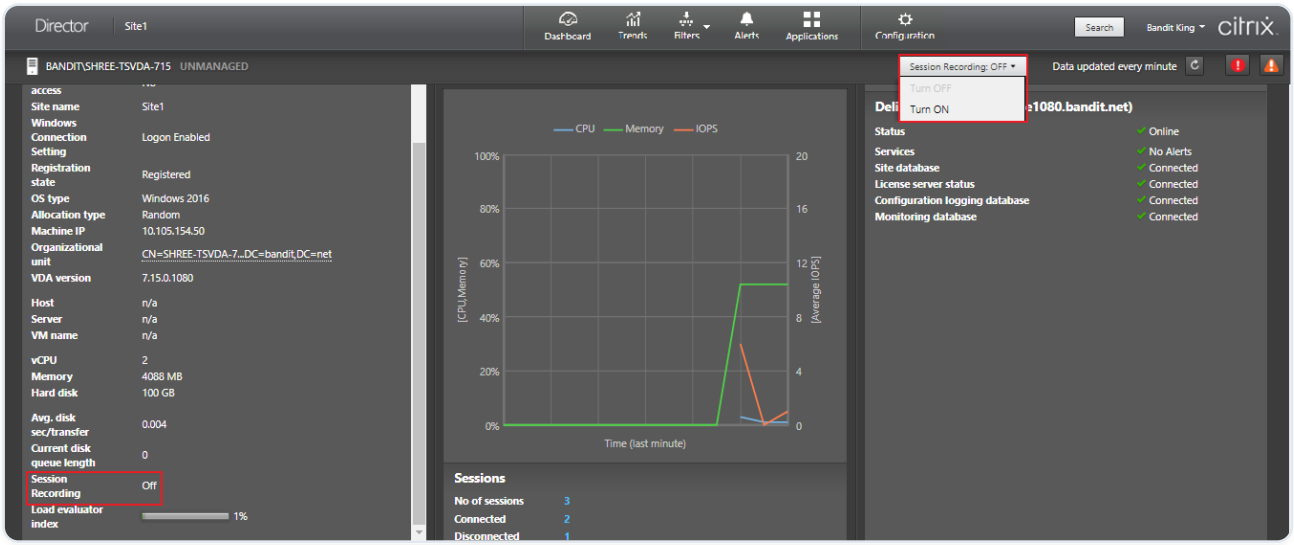
您可以：

- 启用（带通知）- 用户在登录 ICA 会话时会收到会话正在录制的通知。
- 启用（无通知）- 会话在不通知用户的情况下静默录制。
- 关闭 - 禁用为用户录制会话。

**策略**面板显示活动会话录制策略的名称。




您可以从“计算机详细信息”页面为特定计算机启用会话录制。该计算机上的后续会话将被录制。**计算机详细信息**面板显示该计算机的会话录制策略状态。




# 功能兼容性矩阵

Citrix Director 7 2203 与以下版本兼容：

- Citrix Virtual Apps and Desktops™ 7 2112 及更高版本
- Citrix 虚拟应用和桌面 7 1912 LTSR

在每个站点中，尽管您可以将 Director 与早期版本的交付控制器™ 结合使用，但最新版本 Director 中的所有功能可能无法使用。Citrix 建议 Director、交付控制器和 VDA 保持相同版本。

> **注意：**

升级交付控制器后，当您打开 Studio 时，系统会提示您升级站点。有关详细信息，请参阅 升级部署 中的“**升级顺序**”部分。

Director 升级后首次登录时，系统会对配置的站点执行版本检查。如果任何站点运行的 Controller 版本早于 Director 版本，Director 控制台上会显示一条消息，建议升级站点。此外，只要站点版本早于 Director 版本，Director 控制板上就会一直显示一条说明，指示此版本不匹配。

**注意：**

早期版本的 Citrix Director 不显示应用于在最新 VDA 版本上运行的用户会话的策略。Citrix Director 1912 及更早版本不显示应用于在 VDA 2003 及更高版本上运行的用户会话的策略。请使用 Citrix Director 2003 及更高版本来查看这些策略。

下面列出了 Director 的特定功能，以及所需的 Delivery Controller (DC)、VDA 和其他依赖组件的最低版本以及许可证版本。

| DIRECTOR 版本 | 功能 | 依赖项 - 所需最低版本 | 版本 |
| --- | --- | --- | --- |
| 1909 | 使用 Citrix Analytics for Performance 配置本地站点(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/director/install-and-configure/onboarding.html) | DC 7 1906 和 VDA 1906 | 所有 |
| 1906 | 会话自动重新连接 | DC 7 1906 和 VDA 1906 | 所有 |
| 1906 | 会话启动持续时间 | DC 7 1906 和 VDA 1903 | 所有 |
| 1906 | 桌面探测 | 交付控制器 7 1906 和 Citrix 探测代理 1903 | 高级版 |

| DIRECTOR 版本 | 功能 | 依赖项 - 所需最低版本 | 版本 |
|---|---|---|---|
| 7.9 及更高版本 | 配置文件加载中的 Citrix Profile Management 持续时间 | VDA 1903 | 所有 |
| 1811 | 配置文件深入分析 | DC 7 1811 和 VDA 1811 | 所有 |
| 1811 | 管理程序警报监控 | DC 7 1811 | 高级版 |
| 1811 | 应用程序探测 | DC 7 1811 和 Citrix 应用程序探测代理 1811 | 高级版 |
| 1811 | Microsoft RDS 许可证运行状况 | DC 7 1811 和 VDA 7.16 | 所有 |
| 1808 | 筛选器数据导出 | DC 7 1808 | 所有 |
| 1808 | 交互式会话深入分析 | DC 7 1808 和 VDA 1808 | 所有 |
| 1808 | GPO 深入分析 | DC 7 1808 和 VDA 1808 | 所有 |
| 1808 | 使用 OData API 获取计算机历史数据 | DC 7 1808 | 所有 |
| 7.18 | 应用程序探测 | DC 7.18 | 高级版（以前称为白金版） |
| 7.18 | 智能警报策略 | DC 7.18 | 高级版（以前称为白金版） |
| 7.18 | 健康助手链接 | 无 | 所有 |
| 7.18 | 交互式会话深入分析 | 无 | 所有 |
| 7.17 | PIV 智能卡身份验证 | 无 | 所有 |
| 7.16 | 应用程序分析 | DC 7.16 和 VDA 7.15 | 所有 |

| DIRECTOR 版本 | 功能 | 依赖项 - 所需最低版本 | 版本 |
|---|---|---|---|
| 7.16 | OData API 版本 4 | DC 7.16 | 所有 |
| 7.16 | Shadow Linux VDA 用户 | VDA 7.16 | 所有 |
| 7.16 | 域本地组支持 | 无 | 所有 |
| 7.16 | 计算机控制台访问 | DC 7.16 | 所有 |
| 7.15 | 应用程序故障监控 | DC 7.15 和 VDA 7.15 | 所有 |
| 7.14 | 以应用程序为中心的故障排除 | DC 7.13 和 VDA 7.13 | 所有 |
| 7.14 | 磁盘监控 | DC 7.14 和 VDA 7.14 | 所有 |
| 7.14 | GPU 监控 | DC 7.14 和 VDA 7.14 | 所有 |
| 7.13 | 会话详细信息面板上的传输协议 | DC 7.x 和 VDA 7.13 | 所有 |
| 7.12 | 用户友好的连接和计算机故障描述 | DC 7.12 和 VDA 7.x | 所有 |
| 7.12 | 企业版中增加的历史数据可用性 | DC 7.12 和 VDA 7.x | 企业 |
| 7.12 | 自定义报告 | DC 7.12 和 VDA 7.x | 高级版（以前称为白金版） |
| 7.11 | 资源利用率报告 | DC 7.11 和 VDA 7.11 | 所有 |
| 7.11 | CPU、内存和 ICA RTT 条件的警报扩展 | DC 7.11 和 VDA 7.11 | 高级版（以前称为白金版） |
| 7.11 | 导出报告改进 | DC 7.11 和 VDA 7.x | 所有 |
| 7.11 | 与 Citrix ADM 集成 | DC 7.11、VDA 7.x 和 MAS 版本 11.1 Build 49.16 | 高级版（以前称为白金版） |
| 7.9 | 登录持续时间细分 | DC 7.9 和 VDA 7.x | 所有 |

| DIRECTOR 版本 | 功能 | 依赖项 - 所需最低版本 | 版本 |
| --- | --- | --- | --- |
| 7.7 | 主动监控和警报 | DC 7.7 和 VDA 7.x | 高级版（以前称为白金版） |
| 7.7 | SCOM 集成(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/director/site-analytics/alerts-notifications.html#configure-scom-alerts-integration) | DC 7.7、VDA 7.x、SCOM 2012 R2 和 PowerShell 3.0 | 高级版（以前称为白金版） |
| 7.7 | Windows 身份验证集成 | DC 7.x 和 VDA 7.x | 所有 |
| 7.7 | 单会话和多会话操作系统使用情况 | DC 7.7 和 VDA 7.x | 高级版（以前称为白金版） |
| 7.6.300 | 支持 Framehawk 虚拟通道 | DC 7.6 和 VDA 7.6 | 所有 |
| 7.6.200 | 会话录制集成 | DC 7.6 和 VDA 7.x | 高级版（以前称为白金版） |
| 7 | HDX Insight 集成 | 交付控制器 7.6、虚拟投递代理 7.x 以及 Citrix ADM | 高级版（以前称为白金版） |

# 数据粒度和保留

## 数据值聚合

监视服务收集各种数据，包括用户会话使用情况、用户登录性能详细信息、会话负载平衡详细信息以及连接和计算机故障信息。数据根据其类别以不同方式进行聚合。了解使用 OData 方法 API 呈现的数据值的聚合对于解释数据至关重要。例如：

- 连接会话和计算机故障在一段时间内发生。因此，它们以该时间段内的最大值形式显示。
- 登录持续时间是时间长度的度量，因此以该时间段内的平均值形式显示。
- 登录计数和连接故障是该时间段内发生次数的计数，因此以该时间段内的总和形式显示。

## 并发数据评估

会话必须重叠才能被视为并发。但是，当时间间隔为 1 分钟时，该分钟内的所有会话（无论是否重叠）都被视为并发。间隔的大小如此之小，以至于计算精度所涉及的性能开销不值得其增加的价值。如果会话发生在同一小时内，但不在同一分钟内，则不认为它们重叠。

## 汇总表与原始数据的关联

数据模型以两种不同的方式表示指标：

- 汇总表以每分钟、每小时和每天的时间粒度表示指标的聚合视图。
- 原始数据表示在会话、连接、应用程序和其他对象中跟踪的单个事件或当前状态。

尝试跨 API 调用或在数据模型本身中关联数据时，了解以下概念和限制非常重要：

- **部分间隔无汇总数据。** 指标汇总旨在满足长期历史趋势的需求。这些指标被聚合到汇总表中以形成完整间隔。在数据收集的开始（最旧的可用数据）和结束时，没有部分间隔的汇总数据。当查看一天的聚合（Interval=1440）时，这意味着第一个和最近的不完整天数没有任何数据。尽管这些部分间隔可能存在原始数据，但它们从不进行汇总。您可以通过从特定汇总表中提取最小和最大 SummaryDate 来确定特定数据粒度的最早和最晚聚合间隔。SummaryDate 列表示间隔的开始。Granularity 列表示聚合数据间隔的长度。
- **按时间关联。** 指标按照上一节所述，聚合到汇总表中以形成完整间隔。它们可用于历史趋势，但原始事件在状态上可能比为趋势分析而汇总的数据更具时效性。任何基于时间的汇总数据与原始数据比较都必须考虑到，对于可能发生的部分间隔或时间段的开始和结束，没有汇总数据。
- **丢失和延迟事件。** 如果事件丢失或延迟到聚合周期，聚合到汇总表中的指标可能略有不准确。尽管 Monitor Service 尝试维护准确的当前状态，但它不会回溯时间来重新计算汇总表中丢失或延迟事件的聚合。
- **连接高可用性。** 在连接高可用性期间，当前连接的汇总数据计数中会出现空白，但会话实例仍将在原始数据中运行。
- **数据保留期。** 汇总表中的数据保留计划与原始事件数据的计划不同。数据可能因已从汇总表或原始表中清除而丢失。不同粒度的汇总数据，其保留期也可能不同。较低粒度的数据（分钟）比较高粒度的数据（天）清除得更快。如果由于清除而导致某个粒度的数据丢失，则可以在更高粒度中找到它。由于 API 调用仅返回请求的特定粒度，因此某个粒度没有数据并不意味着同一时间段内更高粒度的数据不存在。
- **时区。** 指标以 UTC 时间戳存储。汇总表按小时时区边界进行聚合。对于不属于小时边界的时区，数据聚合的位置可能存在一些差异。

## 粒度和保留

Director 检索的聚合数据的粒度是所请求的时间 (T) 跨度的函数。规则如下：

- 0 \< T \<= 1 小时 - 使用每分钟粒度
- 0 \< T \<= 30 天 - 使用每小时粒度
- T \> 31 天 - 使用每日粒度

未聚合的数据来自原始会话和连接信息。此数据增长迅速，因此有其自己的清除设置。清除可确保仅保留长期相关的有用数据。清除可确保更好的性能，同时保持报告所需的粒度。Premium 许可站点的客户可以将其清除保留期更改为所需的保留天数，否则将使用默认值。如果与站点数据库失去连接，Monitor Service 将使用下表中指定的 Premium 授权的默认保留天数。

要访问这些设置，请在 Delivery Controller™ 上运行以下 PowerShell 命令：

```
asnp Citrix.*

 Get-MonitorConfiguration

 Set-MonitorConfiguration -<setting name> <value>
```

| # | 设置名称 | 受影响的架构表 | MONITOR 页面中受影响的表和图表 | PREMIUM 的保留天数 | ADVANCED 的保留天数 |
|---|---|---|---|---|---|
| 1 | GroomSessionsRetentionDays | MonitorData.Session 和 Monitordata.Connection 表 | 此设置会影响“趋势”页面上的会话详细信息、按用户会话划分的登录持续时间、基于应用程序的使用情况表。 | 90 | 31 |
| 2 | GroomFailuresRetentionDays | MonitorData.MachineFailureLog 和 MonitorData.ConnectionFailureLog | 趋势页面：此设置会影响故障选项卡上的图表和表格。 | 90 | 31 |

| # | 设置名称 | 受影响的架构表 | MONITOR 页面中受影响的表和图表 | PREMIUM 的保留天数 | ADVANCED 的保留天数 |
|---|---|---|---|---|---|
| 3 | GroomLoadIndexesRetentionDays | MonitorData.LoadIndex | 此设置会影响“趋势”页面上“负载评估器索引”选项卡中显示的数据。 | 3 | 3 |
| 4 | GroomDeletedRetentionDays | LifecycleState 为 “Deleted”的 MonitorData.Machine、MonitorData.Catalog、MonitorData.DesktopGroup 和 MonitorData.Hypervisor 实体。此设置还会删除任何相关的 Session、SessionDetail、Summary、Failure 或 LoadIndex 记录。 | LifecycleState 为 “Deleted”的 Machine、Catalog、DesktopGroup 和 Hypervisor 实体。此设置还会删除任何相关的 Session、SessionDetail、Summary、Failure 或 LoadIndex 记录。 | 90 | 31 |
| 5 | GroomSummariesRetentionDays | MonitorData.DesktopGroupSummary、MonitorData.FailureLogSummary 和 MonitorData | 此设置影响“趋势”页面上的所有图表数据。 | 365 | 31 |

| # | 设置名称 | 受影响的架构表 | MONITOR 页面中受影响的表和图表 | PREMIUM 的保留天数 | ADVANCED 的保留天数 |
|---|---|---|---|---|---|
| | | .LoadIndexSummary | | | |
| 6 | GroomMachineHotfixLogRetentionDays | MonitorData.Hotfix | 此设置影响“计算机详细信息”页面上显示的 VDA 热修复数据。 | 90 | 31 |
| 7 | GroomMinuteRetentionDays | 所有摘要表 | 此设置影响“趋势”页面上显示的“最近 2 小时”时间段的图表。 | 3 | 3 |
| 8 | GroomHourlyRetentionDays | 所有摘要表 | 这会影响“趋势”页面上显示的每周图表。 | 32 | 31 |
| 9 | GroomApplicationInstanceRetentionDays | MonitorData.ApplicationInstance | 此设置会影响“容量管理”选项卡上的图表和表格以及“趋势”页面上的应用程序使用情况表。 | 90 | 不适用 |
| 10 | GroomNotificationLogRetentionDays | MonitorData.NotificationLog | 此设置会影响在 Monitor 上显示的警报。 | 90 | 不适用 |
| 11 | GroomResourceUsageR | MonitorData.Resourceutilization | 此设置会影响在“历史计算机利用率”计算机详 | 3 | 3 |

| # | 设置名称 | 受影响的架构表 | MONITOR 页面中受影响的表和图表 | PREMIUM 的保留天数 | ADVANCED 的保留天数 |
|---|---|---|---|---|---|
| | awDataRetentionDays | | 细信息页面中看到的 CPU 和内存图表。 | | |
| 12 | GroomResourceUsageMinuteDataRetentionDays | MonitorData.ResourceUtilizationSummary | 此设置会影响在“历史计算机利用率”计算机详细信息页面中看到的“最近 2 小时”时间段的 CPU 和内存图表。 | 7 | 7 |
| 13 | GroomResourceUsageHourDataRetentionDays | MonitorData.Resourceutilizationsummary | 此设置影响“历史计算机利用率”计算机详细信息页面中显示的 CPU 和内存图表。 | 30 | 30 |
| 14 | GroomResourceUsageDayDataRetentionDays | MonitorData.Resourceutilizationsummary | 此设置影响趋势页面上“资源利用率”计算机中以及特定计算机的“计算机利用率”页面中显示的 CPU 和内存图表。 | 365 | 31 |
| 15 | GroomProcessUsageR | MonitorData.ProcessUtilization | 此设置影响在计算机历史使用情况页面上显示 | 1 | 1 |

| # | 设置名称 | 受影响的架构表 | MONITOR 页面中受影响的表和图表 | PREMIUM 的保留天数 | ADVANCED 的保留天数 |
|---|---|---|---|---|---|
| | awDataRetentionDays | | 的每进程资源趋势信息。 | | |
| 16 | GroomProcessUsageMinuteDataRetentionDays | MonitorData.ProcessUtilizationMinuteSummary | 此设置影响在历史计算机利用率页面上显示的“最近 2 小时”每进程的 CPU 和内存使用情况图表。 | 3 | 3 |
| 17 | GroomProcessUsageHourDataRetentionDays | MonitorData.ProcessUtilizationHourSummary | 此设置影响计算机历史使用情况页面上显示的每个进程的 CPU 和内存使用趋势。 | 7 | 7 |
| 18 | GroomProcessUsageDayDataRetentionDays | MonitorData.ProcessUtilizationDaySummary | 此设置影响计算机历史使用情况页面上显示的每个进程的 CPU 和内存使用趋势。 | 30 | 30 |
| 19 | GroomSessionMetricsDataRetentionDays | MonitorData.Sessionmetrics | 此设置影响用户详细信息页面上“会话性能”选项卡中显示的所有图表。 | 1 | 1 |
| 20 | GroomMachineMetricDat | MonitorData.Machinemetrics | 此设置影响趋势页面上“资源利用 | 3 | 3 |

| # | 设置名称 | 受影响的架构表 | MONITOR 页面中受影响的表和图表 | PREMIUM 的保留天数 | ADVANCED 的保留天数 |
|---|---|---|---|---|---|
| | aRetentionDays | | 率”选项卡中的图表和表格。 | | |
| 21 | GroomMachineMetricDaySummaryDataRetentionDays | MonitorData.MachineMetricDaySummary | 此设置会影响趋势页面上“资源利用率”选项卡中的图表和表格。 | 365 | 31 |
| 22 | GroomApplicationErrorsRetentionDays | MonitorData.ApplicationError | 此设置会影响应用程序页面上“应用程序错误”列中显示的错误详细信息。 | 1 | 1 |
| 23 | GroomApplicationFaultsRetentionDays | MonitorData.Applicationfailure | 此设置会影响应用程序页面上“应用程序故障”列。 | 1 | 1 |

**注意：**

修改 Monitor Service 数据库中的值需要重新启动服务才能使新值生效。建议仅在 Citrix 支持部门的指导下对 Monitor Service 数据库进行更改。

GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays 和 GroomSessionMetricsDataRetentionDays 设置的默认值限制为 1，而 GroomProcessUsageMinuteDataRetentionDays 的默认值限制为 3。用于设置这些值的 PowerShell 命令已被禁用，因为进程使用数据往往会快速增长。 此外，基于许可证的保留设置如下：

- **高级许可站点 -** 所有设置的清理保留期限制为 1000 天（Citrix 建议 365 天）。
- **进阶许可站点 -** 所有设置的清理保留期限制为 31 天。
- **所有其他站点 -** 所有设置的清理保留期限制为 7 天。

**例外：**

- GroomApplicationInstanceRetentionDays 只能在高级许可站点中设置。
- GroomApplicationErrorsRetentionDays 和 GroomApplicationFaultsRetentionDays 在高级许可站点中限制为 31 天。

长期保留数据会对表大小产生以下影响：

- **每小时数据。** 如果允许每小时数据在数据库中保留长达两年，则一个包含 1000 个交付组的站点可能导致数据库按如下方式增长：

  1000 个交付组 x 24 小时/天 x 365 天/年 x 2 年 = 17,520,000 行数据。如此大量的数据在聚合表中对性能的影响是巨大的。鉴于仪表板数据是从此表中提取的，因此对数据库服务器的要求可能很高。过多的数据量可能会对性能产生显著影响。
- **会话和事件数据。** 每次启动会话并建立连接/重新连接时收集的数据。对于大型站点（10 万用户），此数据增长迅速。例如，两年内这些表的数据量将超过 1 TB，需要高端企业级数据库。

# Citrix Director 故障原因和故障排除

下表描述了各种故障类别、原因以及解决问题所需采取的操作。有关详细信息，请参阅 枚举、错误代码和说明。

## 连接故障错误

| 类别 | 原因 | 问题 | 操作 |
| --- | --- | --- | --- |
| N/A | [0] 未知。此错误代码未映射。 | 监控服务无法根据 Brokering 服务共享的信息确定报告的启动或连接失败的原因。 | 在控制器上收集 CDF 日志并联系 Citrix 支持。 |
| [0] 无 | [1] 无 | 无 | N/A |
| [2] MachineFailure | [2] SessionPreparation | 从交付控制器到 VDA 的会话准备请求失败。可能的原因：控 | 有关导致控制器与 VDA 之间通信问题的常见问题，请参阅知 |

| 类别 | 原因 | 问题 | 操作 |
| --- | --- | --- | --- |
| | | 制器与 VDA 之间的通信问题、Broker Service 在创建准备请求时遇到的问题，或导致 VDA 不接受请求的网络问题。 | 识中心文章 Citrix Virtual Apps and Desktops 中 Virtual Delivery Agent 与交付控制器注册故障排除 中列出的故障排除步骤。 |
| [2] MachineFailure | [3] RegistrationTimeout | VDA 已开机，但在尝试向交付控制器注册时发生超时。 | 验证 Citrix Broker Service 是否在交付控制器上运行，以及 Desktop 服务是否在 VDA 上运行。如果已停止，请启动它们。 |
| [1] 客户端连接失败 | [4] 连接超时 | VDA 准备好启动会话后，客户端未能连接到 VDA。会话已成功代理，但在等待客户端连接到 VDA 时发生超时。可能的原因：防火墙设置、网络中断或阻止远程连接的设置。 | 检查 Director 控制台，查看客户端当前是否有活动连接，这意味着没有用户受到影响。如果不存在会话，请检查客户端和 VDA 上的事件日志以查找任何错误。解决客户端和 VDA 之间的任何网络连接问题。 |
| [4] 无可用许可证 | [5] 许可 | 许可请求失败。可能的原因：许可证数量不足，或者许可证服务器已停机超过 30 天。 | 验证许可证服务器是否在线且可访问。解决与许可证服务器的任何网络连接问题，或者如果许可证服务器出现故障，请重新启动它。验证环境中是否有足够的许可证，并在必要时分配更多许可证。 |
| [1] 客户端连接失败 | [6] 票证 | 票证处理期间发生故障，表明客户端与 VDA 的连接与代理请 | 根据交付组中定义的用户组，验证用户是否具有对应用程序或 |

| 类别 | 原因 | 问题 | 操作 |
| --- | --- | --- | --- |
| | | 求不匹配。启动请求票证由 Broker 准备并随 ICA® 文件一起交付。当用户尝试启动会话时，VDA 会使用 Broker 验证 ICA 文件中的启动票证。可能的原因：ICA 文件已损坏或用户正在尝试进行未经授权的连接。 | 桌面的访问权限。指示用户重新启动应用程序或桌面，以确定这是否是一次性问题。如果问题再次发生，请检查客户端设备事件日志以查找错误。验证用户尝试连接的 VDA 是否已注册。如果未注册，请检查 VDA 上的事件日志并解决任何注册问题。 |
| [1] 客户端连接失败 | [7] 其他 | 客户端最初联系 VDA 后但在完成连接序列之前，会话已从 VDA 报告为已终止。 | 验证会话是否未在启动前由用户终止。尝试重新启动会话，如果问题仍然存在，请收集 CDF 日志并联系 Citrix 支持。 |
| [1] 客户端连接失败 | [8] 一般故障 | 会话启动失败。可能的原因：在代理仍在启动或初始化时请求了代理启动，或者在启动的代理阶段发生内部错误。 | 验证 Citrix Broker Service 正在运行，然后重试启动会话。 |
| [5] 配置 | [9] 维护模式 | VDA 或 VDA 所属的交付组已设置为维护模式。 | 确定是否需要维护模式。如果不需要，请在相关交付组或计算机上禁用维护模式，并指示用户尝试重新连接。 |
| [5] 配置 | [10] 应用程序已禁用 | 最终用户无法访问该应用程序，因为它已被管理员禁用。 | 如果应用程序旨在用于生产环境，请启用该应用程序并指示用户重新连接。 |

| 类别 | 原因 | 问题 | 操作 |
| --- | --- | --- | --- |
| [4] 无可用许可证 | [11] 许可证功能被拒绝 | 正在使用的功能不在现有许可证的涵盖范围内。 | 请联系 Citrix 销售代表，确认现有 Citrix Virtual Apps and Desktops™ 许可证版本和类型所涵盖的功能。 |
| [3] 无可用容量 | [13] 会话限制已达 | 所有 VDA 都在使用中，没有容量来托管更多会话。可能的原因：所有 VDA 都在使用中（对于单会话操作系统 VDA），或者所有 VDA 都已达到配置的最大并发会话数（对于多会话操作系统 VDA）。 | 验证是否有任何 VDA 处于维护模式。如果不需要，请禁用维护模式以释放更多容量。考虑增加 Citrix 策略设置中**最大会话数**的值，以允许每个服务器 VDA 承载更多会话。考虑添加更多多会话操作系统 VDA。考虑添加更多单会话操作系统 VDA。 |
| [5] 配置 | [14] 不允许的协议 | 不允许使用 ICA 和 RDP 协议。 | 在交付控制器上运行 **Get-BrokerAccessPolicyRule** PowerShell 命令，并验证 **AllowedProtocols** 值是否列出了所有所需的协议。此问题仅在配置错误时发生。 |
| [5] 配置 | [15] 资源不可用 | 用户尝试连接的应用程序或桌面不可用。此应用程序或桌面可能不存在，或者没有可用的 VDA 来运行它。可能的原因：应用程序或桌面已取消发布，或者托管应用程序或桌面的 VDA 已达到最大负载，或 | 验证应用程序或桌面是否仍已发布，并且 VDA 未处于维护模式。确定多会话操作系统 VDA 是否已满载。如果是，请预配更多多会话操作系统 VDA。验证是否有可用于连接的单会话操作系统 VDA。如有必 |

| 类别 | 原因 | 问题 | 操作 |
| --- | --- | --- | --- |
| | | 者应用程序或桌面已设置为维护模式。 | 要，请预配更多单会话操作系统 VDA。 |
| [5] 配置 | [16] ActiveSessionReconnectDisabled | ICA 会话处于活动状态并连接到其他端点。但是，由于**活动会话重新连接**已禁用，客户端无法连接到活动会话。 | 在交付控制器上，验证**活动会话重新连接**是否已启用。验证注册表中的 **DisableActiveSessionReconnect** 值（位于 **HKEY_LOCAL_MACHINE\Software\Citrix\Desktop\Server** 下）是否设置为 0。 |
| [2] MachineFailure | [17] NoSessionToReconnect | 客户端尝试重新连接到特定会话，但该会话已终止。 | 重试工作区控制重新连接。 |
| [2] MachineFailure | [18] SpinUpFailed | VDA 无法启动以进行会话启动。这是虚拟机管理程序报告的问题。 | 如果计算机仍处于关机状态，请尝试从 Citrix Studio 启动计算机。如果失败，请检查虚拟机管理程序连接和权限。如果 VDA 是 PVS 预配的计算机，请在 PVS 控制台中验证计算机是否正在运行。如果没有，请验证是否为计算机分配了个人虚拟磁盘，然后登录到虚拟机管理程序以重置 VM。 |
| [2] MachineFailure | [19] 已拒绝 | 交付控制器向 VDA 发送请求，要求其准备好接受来自最终用户的连接，但 VDA 主动拒绝了此请求。 | 通过 ping 验证交付控制器和 VDA 是否可以成功通信。如果不能，请解决任何防火墙或网络路由问题。 |

| 类别 | 原因 | 问题 | 操作 |
| --- | --- | --- | --- |
| [2] MachineFailure | [20] 配置集失败 | 交付控制器在会话启动期间未将所需的配置数据（例如策略设置和会话信息）发送到 VDA。可能的原因：控制器与 VDA 之间的通信问题、Broker Service 在创建配置集请求时遇到的问题，或导致 VDA 不接受请求的网络问题。 | - |
| [3] NoCapacityAvailable | [21] MaxTotalInstancesExceeded | 已达到应用程序的最大实例数。无法在 VDA 上打开应用程序的其他实例。此问题与应用程序限制功能有关。 | 如果许可允许，请考虑将应用程序设置“**限制同时运行的实例数**”增加到更高的值。 |
| [3] NoCapacityAvailable | [22] MaxPerUserInstancesExceeded | 用户尝试打开应用程序的多个实例，但应用程序配置为每个用户只允许一个应用程序实例。此问题与应用程序限制功能有关。 | 默认情况下，每个用户只允许一个应用程序实例。如果需要每个用户多个实例，请考虑清除应用程序设置中的“**限制每个用户一个实例**”设置。 |
| [1] ClientConnectionFailure | [23] 通信错误 | 交付控制器尝试向 VDA 发送信息（例如准备连接的请求），但在通信尝试期间发生错误。这可能是由网络中断引起的。 | 如果已启动，请重新启动 VDA 上的 Desktop 服务以重新启动注册过程，并验证 VDA 是否成功注册。通过应用程序事件日志中的详细信息，确认为 VDA 配置的交付控制器是否准确。 |
| [3] 无可用容量 | [100] 无可用计算机监视服务将 [12] 无可 | 分配用于启动会话的 VDA 处于无效状态或 | 验证 VDA 是否在交付组中。如果不在， |

| 类别 | 原因 | 问题 | 操作 |
| --- | --- | --- | --- |
| | 用桌面 转换为此错误代码。 | 不可用。可能的原因：VDA 的电源状态未知或不可用，VDA 自上次用户会话以来未重新启动，当前会话需要启用会话共享但会话共享已禁用，或者 VDA 已从交付组或站点中删除。 | 请将其添加到相应的交付组。验证是否有足够的 VDA 已注册并处于就绪状态，以便能够启动用户请求的已发布共享桌面或应用程序。验证托管 VDA 的虚拟机管理程序未处于维护模式。 |
| [2] 计算机故障 | [101] 计算机无法运行。监视服务将 [12] 无可用桌面 转换为此错误代码。 | VDA 未运行。可能的原因：VDA 已从交付组中删除，VDA 未注册，VDA 电源状态不可用，或者 VDA 遇到内部问题。 | 验证 VDA 是否在交付组中。如果不在，请将其添加到相应的交付组。验证 VDA 在 Citrix Studio 中显示为已开机。如果多台计算机的电源状态未知，请解决与虚拟机管理程序连接或主机故障的任何问题。验证托管 VDA 的虚拟机管理程序未处于维护模式。解决这些问题后，重新启动 VDA。 |

## 计算机故障类型

| 错误代码 | 错误代码 ID | 问题 | 操作 |
| --- | --- | --- | --- |
| 未知 | - | - | - |
| 未注册 | 3 | - | - |
| 最大容量（在 Director 控制台上表示为最大负载） | 4 | 计算机报告自身已达到最大容量，即最大负载指数 | 确保所有管理程序都已开机。通过增加管理程序容量或添加更多管理程序，向受影响的交付组添加更多计算机。 |

| 错误代码 | 错误代码 ID | 问题 | 操作 |
| --- | --- | --- | --- |
| 启动卡住 | 2 | 虚拟机未完成其启动序列，且未与管理程序通信。 | 确保虚拟机在管理程序上成功启动。检查虚拟机上的其他消息，例如操作系统问题。确保虚拟机上安装了管理程序工具。确保虚拟机上安装了 VDA。 |
| 启动失败 | 1 | 虚拟机在管理程序上尝试启动时遇到问题。 | 检查管理程序日志。 |
| 无 | 0 | - | - |

## 计算机注销原因（适用于故障类型为“未注册”或“未知”时）

| 错误代码 | 错误代码 ID | 问题 | 操作 |
| --- | --- | --- | --- |
| 代理关机 | 0 | VDA 正常关机。 | 如果您不希望 VDA 根据现有电源管理策略处于关闭状态，请开启 VDA。检查事件日志中的任何错误。 |
| 代理挂起 | 1 | VDA 处于休眠或睡眠模式。 | 将 VDA 退出休眠模式。考虑通过电源设置禁用 Citrix Virtual Apps and Desktops VDA 的休眠功能。 |
| IncompatibleVersion | 100 | 由于 Citrix 协议版本不匹配，VDA 无法与交付控制器通信。 | 统一 VDA 和交付控制器的版本。 |
| AgentAddressResolutionFailed | 101 | 交付控制器无法解析 VDA 的 IP 地址。 | 验证 VDA 计算机帐户是否存在于 AD 中。如果不存在，请创建它。验证 DNS 中 VDA 的名称和 IP 地址是否准确。如果 |

| 错误代码 | 错误代码 ID | 问题 | 操作 |
| --- | --- | --- | --- |
| | | | 不准确，请更正。如果问题普遍存在，请验证交付控制器上的 DNS 设置。通过运行 `nslookup` 命令，验证控制器上的 DNS 解析。 |
| [Cloud]:AgentAddressResolutionFailed | 101 | 交付控制器无法解析 VDA 的 IP 地址。 | 验证 VDA 计算机帐户是否存在于 AD 中。如果不存在，请创建它。验证 DNS 中 VDA 的名称和 IP 地址是否准确。如果不准确，请更正。 |
| AgentNotContactable | 102 | 交付控制器与 VDA 之间发生通信问题。 | 使用 ping 验证交付控制器和 VDA 是否可以成功通信。如果不能，请解决任何防火墙或网络问题。有关导致控制器和 VDA 之间通信问题的常见问题，请参阅知识中心文章 Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) 中列出的故障排除步骤。 |
| [Cloud]: AgentNotContactable | 102 | 交付控制器和 VDA 之间发生通信问题。 | 有关导致控制器和 VDA 之间通信问题的常见问题，请参阅知识中心文章 Troubleshooting Virtual Delivery |

| 错误代码 | 错误代码 ID | 问题 | 操作 |
| --- | --- | --- | --- |
| | | | Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) 中列出的故障排除步骤。请联系 Citrix 支持。 |
| AgentWrongActiveDirectoryOU | 103 | 发生了 Active Directory 发现配置错误。VDA 注册表中配置的特定于站点的 OU（其中站点控制器信息存储在 AD 中）属于不同的站点。 | 确保 Active Directory 配置正确，或检查注册表设置。 |
| EmptyRegistrationRequest | 104 | 从 VDA 发送到交付控制器的注册请求为空。这可能是由于 VDA 软件安装损坏造成的。 | 重新启动 VDA 上的 Desktop 服务以重新启动注册过程，并通过应用程序事件日志验证 VDA 是否正确注册。 |
| MissingRegistrationCapabilities | 105 | VDA 版本与交付控制器不兼容。 | 升级 VDA 或移除 VDA，然后重新安装。 |
| MissingAgentVersion | 106 | VDA 版本与交付控制器不兼容。 | 如果问题影响所有计算机，请重新安装 VDA 软件。 |
| InconsistentRegistrationCapabilities | 107 | VDA 无法将其功能告知 Broker。这可能是由于 VDA 和交付控制器版本不兼容造成的。注册功能随每个版本而变化，其表达形式与注册请求不匹配。 | 使 VDA 和交付控制器版本保持一致。 |

| 错误代码 | 错误代码 ID | 问题 | 操作 |
| --- | --- | --- | --- |
| NotLicensedForFeature | 108 | 您尝试使用的功能未获得许可。 | 检查您的 Citrix 许可版本，或移除 VDA，然后重新安装。 |
| [Cloud]: NotLicensedForFeature | 108 | 您尝试使用的功能未获得许可。 | 请联系 Citrix 支持。 |
| 不支持的凭据安全版本 | 109 | VDA 和交付控制器未采用相同的加密机制。 | 使 VDA 和交付控制器版本保持一致。 |
| 无效注册请求 | 110 | VDA 向 Broker 发出了注册请求，但请求内容已损坏或无效。 | 有关导致控制器和 VDA 之间出现通信问题的常见问题，请参阅知识中心文章 在 Citrix Virtual Apps and Desktops 中对 Virtual Delivery Agent 与交付控制器的注册进行故障排除 (CTX136668) 中列出的故障排除步骤。 |
| 单多会话不匹配 | 111 | VDA 的操作系统类型与计算机目录或交付组不兼容。 | 将 VDA 添加到正确的计算机目录类型或包含相同操作系统计算机的交付组。 |
| 目录功能级别过低 | 112 | 计算机目录设置的 VDA 功能级别高于已安装的 VDA 版本。 | 验证 VDA 的计算机目录功能级别是否与 VDA 的功能级别匹配。升级或降级计算机目录以使其与 VDA 匹配。 |
| 桌面组功能级别过低 | 113 | 交付组设置的 VDA 功能级别高于已安装的 VDA 版本。 | 验证 VDA 的交付组功能级别是否与 VDA 的功能级别匹配。升级或降级计算机目录 |

| 错误代码 | 错误代码 ID | 问题 | 操作 |
| --- | --- | --- | --- |
| | | | 以使其与 VDA 匹配。 |
| 关机 | 200 | VDA 未正常关机。 | 如果 VDA 应该处于开机状态，请尝试从 Citrix Studio 启动 VDA，并验证其是否正常启动和注册。排查任何启动或注册问题。VDA 重新启动后，查看其事件日志以帮助确定关机的根本原因。 |
| 代理拒绝设置更新 | 203 | Citrix 策略等设置已更改或更新，但在将更新发送到 VDA 时发生错误。如果更新与已安装的 VDA 版本不兼容，则可能会发生这种情况。 | 如有必要，请升级 VDA。检查所应用的更新是否与 VDA 版本兼容。 |
| SessionPrepareFailure | 206 | Broker 未完成对 VDA 上运行的会话的审核。 | 如果普遍存在，请在交付控制器上重新启动 Citrix Broker Service。 |
| [Cloud]: SessionPrepareFailure | 206 | Broker 未完成对 VDA 上运行的会话的审核。 | 联系 Citrix 支持。 |
| ContactLost | 207 | 交付控制器与 VDA 失去连接。这可能是由网络中断引起的。 | 验证 Citrix Broker Service 是否在交付控制器上运行，以及 Desktop service 是否在 VDA 上运行。如果已停止，请启动它们。如果已启动，请重新启动 VDA 上的 Desktop service 以重新启动注册过程，并验证 VDA 是否成功 |

| 错误代码 | 错误代码 ID | 问题 | 操作 |
| --- | --- | --- | --- |
| | | | 注册。通过应用程序事件日志中的详细信息，确认为 VDA 配置的交付控制器是否准确。使用 ping 验证交付控制器和 VDA 是否可以成功通信。如果不能，请解决任何防火墙或网络问题。 |
| [Cloud]: ContactLost | 207 | 交付控制器与 VDA 失去连接。这可能是由网络中断引起的。 | 验证 Desktop service 是否在 VDA 上运行。如果已停止，请启动它。 |
| BrokerRegistrationLimitReached | 301 | 交付控制器已达到允许并发注册的 VDA 的最大配置数量。默认情况下，交付控制器允许 10,000 个并发 VDA 注册。 | 考虑将交付控制器添加到站点或创建站点。您还可以通过 **HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\MaxWorkers** 注册表项增加允许并发注册到交付控制器的 VDA 数量。有关详细信息，请参阅知识中心文章 Citrix Virtual Apps and Desktops 使用的注册表项条目 (CTX117446)。增加此数量可能需要控制器更多的 CPU 和内存资源。 |
| 设置创建失败 | 208 | Broker 未构建要发送到 VDA 的一组设置和配置。如果 Broker 无法收集数据，则注册失败，VDA 变为未注册状态。 | 检查交付控制器上的事件日志以查找任何错误。如果日志中没有明显的特定问题，请重新启动 Broker 服务。Broker 服务重 |

| 错误代码 | 错误代码 ID | 问题 | 操作 |
| --- | --- | --- | --- |
| | | | 新启动后，重新启动受影响 VDA 上的 Desktop 服务并验证它们是否成功注册。 |
| [Cloud]: 设置创建失败 | 208 | Broker 未构建要发送到 VDA 的一组设置和配置。如果 Broker 无法收集数据，则注册失败，VDA 变为未注册状态。 | 重新启动受影响 VDA 上的 Desktop 服务并验证它们是否成功注册。联系 Citrix 支持。 |
| 发送设置失败 | 204 | Broker 未将设置和配置数据发送到 VDA。如果 Broker 可以收集数据但无法发送，则注册失败。 | 如果仅限于单个 VDA，请重新启动 VDA 上的 Desktop 服务以强制重新注册，并通过应用程序事件日志验证 VDA 是否成功注册。排除发现的任何错误。请参阅知识中心文章 Citrix Virtual Apps and Desktops 中 Virtual Delivery Agent 与交付控制器注册故障排除 (CTX136668) 中列出的故障排除步骤，以了解导致控制器和 VDA 之间通信问题的常见问题。 |
| 代理请求 | 2 | 发生未知错误。 | 联系 Citrix 支持。 |
| 桌面重启 | 201 | 发生未知错误。 | 联系 Citrix 支持。 |
| 桌面已移除 | 202 | 发生未知错误。 | 联系 Citrix 支持。 |
| 会话审计失败 | 205 | 发生未知错误。 | 联系 Citrix 支持。 |
| UnknownError | 300 | 发生未知错误。 | 请联系 Citrix 支持。 |

| 错误代码 | 错误代码 ID | 问题 | 操作 |
| --- | --- | --- | --- |
| RegistrationStateMismatch | 302 | 发生未知错误。 | 请联系 Citrix 支持。 |
| 未知 | - | 发生未知错误。 | 请联系 Citrix 支持。 |

# 第三方通知

此版本的 Citrix Virtual Apps and Desktops™ 可能包含根据以下文档中定义的条款获得许可的第三方软件：

- Citrix Virtual Apps and Desktops 第三方通知 （PDF 下载）
- FlexNet Publisher 2017 (11.15.0.0) 的非商业软件披露 （PDF 下载）
- FlexNet Publisher 文档补充：FlexNet Publisher 11.15.0 中使用的第三方和开源软件 （PDF 下载）

# SDK 和 API

此版本提供了多个 SDK 和 API。要访问这些 SDK 和 API，请转到 Build anything with Citrix。在此处，选择 **Citrix Workspace** 以访问 Citrix Virtual Apps and Desktops 及其相关组件的编程信息。

> **注意：**
>
> Citrix Virtual Apps and Desktops™ SDK 和 Citrix Group Policy SDK 可以作为模块或管理单元安装。多个组件 SDK（例如 Citrix Licensing、Citrix Provisioning 和 StoreFront）仅使用管理单元进行安装。
>
> 此产品支持 PowerShell 版本 3 到 5。

## Citrix 虚拟应用和桌面 SDK

当您安装 Delivery Controller™ 或 Studio 时，此 SDK 会自动作为 PowerShell 模块安装。这使您无需添加管理单元即可使用此 SDK 的 cmdlet。（如果您选择将此 SDK 作为管理单元安装，下面提供了说明。）

### 权限

您必须使用具有 Citrix 管理权限的身份运行 shell 或脚本。尽管 Controller 上本地管理员组的成员自动拥有完全管理权限以允许安装 Citrix Virtual Apps 或 Citrix Virtual Desktops™，但 Citrix 建议在正常操作中，您创建具有适当权限的 Citrix 管理员，而不是使用本地管理员帐户。

### 访问并运行 cmdlet

1. 在 PowerShell 中启动 shell：打开 Studio，选择 **PowerShell** 选项卡，然后单击 **Launch PowerShell**。
2. 要在脚本中使用 SDK cmdlet，请在 PowerShell 中设置执行策略。有关 PowerShell 执行策略的信息，请参阅 Microsoft 文档。
3. 如果要使用管理单元（而不是模块），请使用 `Add-PSSnapin`（或 `asnp`）cmdlet 添加管理单元。

V1 和 V2 表示管理单元的版本。XenDesktop 5 管理单元是版本 1。Citrix Virtual Apps and Desktops 以及更早的 XenDesktop 7 版本管理单元是版本 2。例如，要安装 Citrix Virtual Apps and Desktops 管理单元，请键入 `Add-PSSnapin Citrix.ADIdentity.Admin.V2`。要导入所有 cmdlet，请键入：`Add-PSSnapin Citrix.*.Admin.V*`

您现在可以使用 cmdlet 和帮助文件了。

- 要访问此 SDK 的帮助文件，请在 Categories 列表中选择产品或组件，然后选择 **Citrix Virtual Apps and Desktops SDK**。
- 有关 PowerShell 指南，请参阅 Windows PowerShell Integrated Scripting Environment (ISE)。

# 组策略 SDK

Citrix Group Policy SDK 使您能够显示和配置组策略设置和筛选器。此 SDK 使用 PowerShell 提供程序创建一个虚拟驱动器，该驱动器对应于计算机和用户设置以及筛选器。该提供程序作为 `New-PSDrive` 的扩展出现。

要使用组策略 SDK，必须安装 Studio 或 Citrix Virtual Apps and Desktops SDK。

Citrix 组策略 PowerShell 提供程序可作为模块或管理单元使用。

- 要使用该模块，无需执行额外操作。
- 要添加管理单元，请键入 `Add-PSSnapin citrix.common.grouppolicy`。

要访问帮助，请键入：`help New-PSDrive -path localgpo:/`。

要创建虚拟驱动器并加载设置，请键入 `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>`，其中 Controller 字符串是您要连接并从中加载设置的站点中 Controller 的完全限定域名。

# 监控服务 OData

Monitor API 允许使用 OData API 的版本 3 或 4 访问 Monitor Service 数据。您可以根据从 Monitor Service 数据查询的数据创建自定义监视和报告仪表板。OData V.4 基于 ASP.NET Web API，并支持聚合查询。

有关详细信息，请参阅 Monitor Service OData API。

# __index__

## 监控站点的历史趋势

“趋势”视图可访问每个站点的以下参数的历史趋势信息：

- 会话
- 连接失败
- 计算机故障
- 登录性能
- 负载评估
- 容量管理
- 计算机使用情况
- 资源利用率
- 每个站点的网络分析。

要查找此信息，请单击“**趋势**”菜单。

放大钻取功能允许您通过放大某个时间段（单击图表中的数据点）并向下钻取以查看与趋势相关的详细信息来浏览趋势图表。此功能使您能够更好地了解受影响的人员或内容的详细信息。

要更改每个图表的默认范围，请对数据应用不同的筛选器。

选择您需要历史趋势信息的时间段。时间段的可用性取决于您的 Director 部署，具体如下：

- 高级许可站点中提供最长可达去年（365 天）的趋势报告。
- 高级许可站点中提供最长可达上个月（31 天）的趋势报告。
- 在非高级和非高级许可站点中，提供最长可达最近 7 天的趋势报告。

> **注意：**

- 在所有 Director 部署中，当时间段设置为上个月（**截止到当前**）或更短时，会话、故障和登录性能趋势信息以图表和表格形式提供。如果时间段选择为具有自定义结束日期的上个月或去年，则趋势信息以图表形式提供，而不是以表格形式提供。
- Monitor Service 的清理保留值控制趋势数据的可用性。默认值可在数据粒度和保留中找到。高级许可站点的客户可以将其清理保留更改为所需的保留天数。
- IIS 管理器中的以下参数控制可供选择的自定义结束日期范围。但是，所选日期的数据可用性取决于所测量特定指标的清理保留设置。

| 参数 | 默认值 |
| --- | --- |
| UI.TrendsLast2HoursRange | 3 |
| UI.TrendsLast24HoursRange | 32 |
| UI.TrendsLast7DaysRange | 32 |
| UI.TrendsLastMonthRange | 365 |

## 可用趋势

**查看会话趋势：** 在**会话**选项卡中，选择交付组和时间段，以查看有关并发会话计数的更详细信息。

**会话自动重新连接**列显示会话中的自动重新连接次数。当会话可靠性或客户端自动重新连接策略生效时，将启用自动重新连接。当端点上发生网络中断时，以下策略将生效：

- 会话可靠性生效（默认情况下为 3 分钟），Citrix Receiver™ 或 Citrix Workspace™ 应用程序会尝试连接到 VDA。
- 客户端自动重新连接在 3 到 5 分钟之间生效，客户端会尝试连接到 VDA。

两次重新连接都会被捕获并显示给用户。重新连接发生后，此信息最多可能需要 5 分钟才能显示在 Director UI 上。

自动重新连接信息可帮助您查看和排查存在中断的网络连接。它还可以分析具有无缝体验的网络。您可以查看在筛选器中选择的特定交付组或时间段的重新连接次数。深入分析可提供其他信息，例如会话可靠性或客户端自动重新连接、时间戳、端点 IP 以及安装了 Workspace 应用程序的计算机的端点名称。

默认情况下，日志按事件时间戳降序排序。此功能适用于适用于 Windows 的 Citrix Workspace 应用程序、适用于 Mac 的 Citrix Workspace 应用程序、适用于 Windows 的 Citrix Receiver 和适用于 Mac 的 Citrix Receiver。此功能需要 Delivery Controller™ 7 1906 或更高版本以及 VDA 1906 或更高版本。

有关会话重新连接的详细信息，请参阅会话。

有关策略的详细信息，请参阅客户端自动重新连接策略设置和会话可靠性策略设置。

有时，自动重新连接数据可能不会显示在 Director 中，原因如下：

- Workspace 应用程序未将自动重新连接数据发送到 VDA。
- VDA 未将数据发送到监视服务。
- Delivery Controller 丢弃 VDA 有效负载，因为它们可能没有相应的会话。

> **注意：**
>
> 有时，如果设置了某些 Citrix Gateway 策略，客户端 IP 地址可能无法正确获取。

> **查看连接失败趋势：** 在“失败”选项卡中，选择连接、计算机类型、失败类型、交付组和时间段，以查看包含有关站点中用户连接失败的更详细信息的图表。

**查看计算机故障趋势：** 在“**单会话操作系统计算机故障**”选项卡或“多会话操作系统计算机”选项卡中，选择故障类型、交付组和时间段，以查看包含站点中计算机故障的更详细信息的图表。

**查看登录性能趋势：** 在“**登录性能**”选项卡中，选择交付组和时间段，以查看包含站点中用户登录时间持续时间的更详细信息以及登录次数是否影响性能的图表。此视图还显示登录阶段的平均持续时间，例如代理持续时间和 VM 启动时间。 此数据专门用于用户登录，不包括尝试从断开连接的会话重新连接的用户。 图表下方的表格显示按用户会话划分的登录持续时间。您可以选择要显示的列，并按任意列对报告进行排序。 有关详细信息，请参阅(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/director/troubleshoot-deployments/user-issues/user-logon.html)

**查看负载评估趋势：** 在“**负载评估器索引**”选项卡中，查看包含有关在多会话操作系统计算机之间分配的负载的更详细信息的图表。此图表的筛选器选项包括交付组或交付组中的多会话操作系统计算机、多会话操作系统计算机（仅当选择了交付组中的多会话操作系统计算机时可用）和范围。

**查看托管应用程序使用情况：** 此功能的可用性取决于您组织的许可证。 在“**容量管理**”选项卡中，选择“**托管应用程序使用情况**”选项卡。选择交付组和时间段，以查看显示并发使用高峰的图表和显示基

于应用程序的使用情况的表格。在“基于应用程序的使用情况”表格中，您可以选择特定的应用程序以查看详细信息以及正在使用或已使用该应用程序的用户列表。

**查看单会话和多会话操作系统使用情况：** “趋势”视图按站点和交付组显示单会话操作系统的使用情况。当您选择“**站点**”时，将按交付组显示使用情况。当您选择“交付组”时，将按用户显示使用情况。“趋势”视图还按站点、交付组和计算机显示多会话操作系统的使用情况。当您选择“**站点**”时，将按交付组显示使用情况。当您选择“交付组”时，将按计算机和用户显示使用情况。当选择“计算机”时，将按用户显示使用情况。

**查看虚拟机使用情况：** 在“**计算机使用情况**”选项卡中，选择“**单会话操作系统计算机或多会话操作系统计算机**”以获取 VM 使用情况的实时视图，从而使您能够快速评估站点的容量需求。 单会话操作系统可用性 - 按整个站点或特定交付组的可用性显示单会话操作系统计算机 (VDI) 的当前状态。 多会话操作系统可用性 - 按整个站点或特定交付组的可用性显示多会话操作系统计算机的当前状态。

> **注意：** “可用计数器”中显示的计算机数量包括处于维护模式的计算机。

> **查看资源利用率：** 在“**资源利用率**”选项卡中，选择“**单会话操作系统计算机或多会话操作系统计算机**”以获取每个 VDI 计算机的 CPU 和内存使用情况以及 IOPS 和磁盘延迟的历史趋势数据，从而更好地进行容量规划。 此功能需要 Delivery Controller 和 VDA **版本 7.11** 或更高版本。 图表显示平均 CPU、平均内存、平均 IOPS、磁盘延迟和并发会话峰值的数据。您可以深入到计算机，并查看消耗 CPU 的前 10 个进程的数据和图表。

> **注意：**
>
> 此表中列出的进程过多可能会消耗大量数据，从而影响性能。为避免这种情况，仅列出平均 CPU 或平均内存超过 1% 的进程。因此，该表有时可能列出少于 10 个进程。

> 按交付组和时间段进行筛选。CPU、内存使用情况和并发会话峰值图表可用于最近 2 小时、24 小时、7 天、月和年。平均 IOPS 和磁盘延迟图表可用于最近 24 小时、月和年。

> **注意：**
>
> - 必须将“监视”策略设置“**启用进程监视**”设置为“**允许**”才能在“历史计算机利用率”页面上的“前 10 个进程”表中收集和显示数据。默认情况下，该策略设置为“**禁止**”。默认情况下会收集所

有资源利用率数据。可以使用“**启用资源监视**”策略设置禁用此功能。图表下方的表格显示每台计算机的资源利用率数据。有关详细信息，请参阅(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/policies/reference/virtual-delivery-agent-policy-settings/monitoring-policy-settings.html)。

- 平均 IOPS 显示每日平均值。峰值 IOPS 计算为所选时间范围内的 IOPS 平均值中的最高值。（IOPS 平均值是 VDA 上每小时收集的 IOPS 的每小时平均值）。

**查看网络分析数据：** 此功能的可用性取决于您组织的许可证和您的管理员权限。此功能需要 Delivery Controller **版本 7.11** 或更高版本。

在“**网络**”选项卡中，监视您的网络分析，该分析提供用户、应用程序和桌面的网络上下文视图。借助此功能，Director 通过 Citrix ADM 中的 HDX Insight 报告提供部署中 ICA 流量的高级分析。有关详细信息，请参阅(/zh-cn/citrix-virtual-apps-desktops/2203-ltsr/director/install-and-configure/hdx-insight.html)

**查看应用程序故障：** “**应用程序故障**”选项卡显示与 VDA 上已发布的应用程序相关的故障。

此功能需要 Delivery Controller 和 VDA **7.15 版**或更高版本。支持运行 Windows Vista 及更高版本的单会话操作系统 VDA，以及运行 Windows Server 2008 及更高版本的多会话操作系统 VDA。 有关详细信息，请参阅历史应用程序故障监视。

默认情况下，仅显示来自多会话操作系统 VDA 的应用程序故障。您可以使用监视策略设置应用程序故障的监视。有关详细信息，请参阅监视策略设置。

**查看应用程序探测结果：**“应用程序探测结果”选项卡显示已在“配置”页面中配置为探测的应用程序的探测结果。此处记录了应用程序启动失败时所处的启动阶段。

此功能需要 Delivery Controller 和 VDA **7.18 版**或更高版本。有关详细信息，请参阅应用程序探测。

**创建自定义报告：**“自定义报告”选项卡提供了一个用户界面，用于生成包含来自监视数据库的实时和历史数据的表格格式的自定义报告。

此功能需要 Delivery Controller **7.12 版**或更高版本。

在以前保存的自定义报告查询列表中，您可以单击**运行并下载**以 CSV 格式导出报告，单击**复制 OData**以复制和共享相应的 OData 查询，或者单击**编辑**以编辑查询。 您可以根据计算机、连接、会话或应用程序实例创建自定义报告查询。根据计算机、交付组或时间段等字段指定筛选条件。指定自定义报告中所需的其他列。预览显示报告数据的示例。保存自定义报告查询会将其添加到已保存查询的列表中。

您可以基于复制的 OData 查询创建自定义报告查询。为此，请选择“OData 查询”选项并粘贴复制的 OData 查询。您可以保存生成的查询以供以后执行。

**注意：** 使用 OData 查询生成的预览和导出报告中的列名未本地化，而是以英文显示。

图表上的旗帜图标表示该特定时间范围内的重要事件或操作。将鼠标悬停在旗帜上并单击以列出事件或操作。

**注意：**

- 对于早于 7 的 VDA，不收集 HDX™ 连接登录数据。对于较早的 VDA，图表数据显示为 0。
- 在 Citrix Studio 中删除的交付组在 Director 趋势筛选器中仍可供选择，直到与其相关的数据被清除。选择已删除的交付组会显示可用数据的图表，直到保留期结束。但是，表格不显示数据。
- 将包含活动会话的计算机从一个交付组移动到另一个交付组会导致新交付组的**资源利用率和负载评估器索引**表显示从旧交付组和新交付组整合的指标。