

# 在 Horizon 7 中配置远程桌面功能

2019 年 7 月

VMware Horizon 7 7.9



vmware®

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

如果您对本文档有任何意见或建议, 请将反馈信息发送至:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**威睿信息技术(中国)有限公司**  
北京办公室  
北京市  
朝阳区新源南路 8 号  
启皓北京东塔 8 层 801  
[www.vmware.com/cn](http://www.vmware.com/cn)

上海办公室  
上海市  
淮海中路 333 号  
瑞安大厦 804-809 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

广州办公室  
广州市  
天河路 385 号  
太古汇一座 3502 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

# 目录

|   |   |    |
|---|---|----|
| 1 | 在 Horizon 7 中配置远程桌面功能                     | 8  |
| 2 | 配置远程桌面功能                                  | 9  |
|   | 配置 Unity Touch                            | 10 |
|   | Unity Touch 的系统要求                         | 10 |
|   | 配置 Unity Touch 显示的收藏的应用程序                 | 10 |
|   | 为多播流或单播流配置 Flash URL 重定向                  | 12 |
|   | Flash URL 重定向的系统要求                        | 13 |
|   | 验证是否安装了 Flash URL 重定向功能                   | 14 |
|   | 设置提供多播或单播流的网页                             | 15 |
|   | 为 Flash URL 重定向设置客户端设备                    | 15 |
|   | 禁用或启用 Flash URL 重定向                       | 16 |
|   | 配置 Flash 重定向                              | 16 |
|   | Flash 重定向的系统要求                            | 17 |
|   | 安装并配置 Flash 重定向                           | 18 |
|   | 使用 Windows 注册表设置配置 Flash 重定向              | 20 |
|   | 配置 HTML5 多媒体重定向                           | 21 |
|   | HTML5 多媒体重定向的系统要求                         | 21 |
|   | 安装和配置 HTML5 多媒体重定向                        | 22 |
|   | 安装适用于 Chrome 的 VMware Horizon HTML5 重定向扩展 | 24 |
|   | 安装适用于 Edge 的 VMware Horizon HTML5 重定向扩展   | 25 |
|   | 配置地理位置重定向                                 | 25 |
|   | 地理位置重定向的系统要求                              | 25 |
|   | 安装和配置地理位置重定向                              | 26 |
|   | 启用 VMware Horizon 地理位置重定向 IE 插件           | 28 |
|   | 启用 VMware Horizon 地理位置重定向 Chrome 插件       | 28 |
|   | 使用实时音频-视频配置 Microsoft Teams               | 29 |
|   | 配置实时音频-视频                                 | 30 |
|   | 实时音频-视频的配置选择                              | 30 |
|   | 实时音频-视频的系统要求                              | 31 |
|   | 确保使用的是实时音频-视频而非 USB 重定向                   | 31 |
|   | 选择首选网络摄像头和麦克风                             | 32 |
|   | 配置实时音频-视频组策略设置                            | 39 |
|   | 实时音频-视频带宽                                 | 42 |
|   | 配置扫描仪重定向                                  | 42 |
|   | 扫描仪重定向的系统要求                               | 42 |
|   | 扫描仪重定向的用户操作                               | 43 |

|   |    |
|---|----|
| 配置扫描仪重定向组策略设置   | 44 |
| 配置串行端口重定向   | 47 |
| 串行端口重定向的系统要求  | 48 |
| 串行端口重定向的用户操作  | 49 |
| 有关配置串行端口重定向的准则  | 50 |
| 配置串行端口重定向组策略设置  | 50 |
| 配置 USB 到串口适配器   | 53 |
| 管理对 Windows Media 多媒体重定向 (MMR) 功能的访问                        | 54 |
| 启用 Horizon 7 中的多媒体重定向                                       | 54 |
| Windows Media MMR 的系统要求                                     | 55 |
| 确定是否基于网络延迟使用 Windows Media MMR                              | 56 |
| 管理对客户端驱动器重定向的访问   | 57 |
| 在 Unified Access Gateway 实施中使用客户端驱动器重定向                     | 57 |
| 使用组策略禁用客户端驱动器重定向  | 57 |
| 使用组策略配置驱动器盘符行为  | 58 |
| 使用注册表设置配置客户端驱动器重定向  | 58 |
| 配置拖放功能  | 60 |
| 配置简单设备方向 (SDO) 传感器重定向                                       | 60 |
| 配置会话协作  | 61 |
| 配置适用于 Skype for Business 的 VMware Virtualization Pack       | 62 |
| 收集日志以排除 Skype for Business 故障                               | 67 |
| 配置 VMware Integrated Printing 重定向                           | 67 |
| 为 USB 重定向、Windows Media Player MMR 重定向或客户端驱动器重定向激活 BEAT 侧通道 | 70 |

### 3 配置 URL 内容重定向 72

|   |    |
|---|----|
| 了解 URL 内容重定向                                  | 72 |
| URL 内容重定向要求                                   | 73 |
| 在 Cloud Pod 架构环境中使用 URL 内容重定向                 | 74 |
| 安装具有 URL 内容重定向功能的 Horizon Agent               | 74 |
| 配置代理到客户端重定向                                   | 74 |
| 将 URL 内容重定向 ADMX 模板添加到 GPO                    | 75 |
| URL 内容重定向组策略设置                                | 76 |
| URL 内容重定向规则的语法                                | 78 |
| URL 内容重定向支持的正则表达式规则                           | 79 |
| 代理到客户端重定向组策略示例                                | 80 |
| 配置客户端到代理重定向                                   | 81 |
| 安装具有 URL 内容重定向功能的适用于 Windows 的 Horizon Client | 82 |
| 使用 vdmutil 命令行实用程序                            | 82 |
| “--agentURLPattern” 选项的语法                     | 84 |
| 创建本地 URL 内容重定向设置                              | 84 |
| 创建全局 URL 内容重定向设置                              | 86 |

|  |            |
|--|------------|
| 将 URL 内容重定向设置分配给用户或组                         | 88         |
| 测试 URL 内容重定向设置                               | 89         |
| 管理 URL 内容重定向设置                               | 90         |
| 使用组策略设置配置客户端到代理重定向                           | 91         |
| URL 内容重定向限制                                  | 91         |
| 不支持的 URL 内容重定向功能                             | 91         |
| 在 Windows 上安装并启用适用于 Chrome 的 URL 内容重定向帮助程序扩展 | 92         |
| 在 Mac 上启用适用于 Chrome 的 URL 内容重定向帮助程序          | 93         |
| <br>   |            |
| <b>4 将 USB 设备与远程桌面和应用程序一起使用</b>              | <b>95</b>  |
| USB 设备类型的相关限制                                | 96         |
| USB 重定向建议                                    | 97         |
| 设置 USB 重定向概述                                 | 97         |
| 配置指纹扫描仪重定向                                   | 98         |
| 配置读卡器重定向                                     | 98         |
| 网络流量和 USB 重定向                                | 99         |
| 启用通过会话增强 SDK 传输 USB 流量功能                     | 99         |
| 自动连接到 USB 设备                                 | 100        |
| 在安全的 Horizon 7 环境中部署 USB 设备                  | 100        |
| 对所有类型的设备禁用 USB 重定向                           | 101        |
| 对特定设备禁用 USB 重定向                              | 102        |
| 使用日志文件进行故障排除和确定 USB 设备 ID                    | 103        |
| 使用策略控制 USB 重定向                               | 103        |
| 为复合 USB 设备配置设备拆分策略设置                         | 104        |
| 为 USB 设备配置过滤策略设置                             | 106        |
| USB 设备系列                                     | 110        |
| Horizon Agent 配置 ADMX 模板中的 USB 设置            | 111        |
| 排除 USB 重定向故障                                 | 113        |
| <br>   |            |
| <b>5 配置桌面和应用程序池的策略</b>                       | <b>115</b> |
| 在 Horizon Administrator 中设置策略                | 116        |
| 配置全局策略设置                                     | 116        |
| 配置桌面池策略                                      | 116        |
| 配置用户策略                                       | 117        |
| Horizon 7 策略                                 | 117        |
| 使用 智能策略                                      | 118        |
| 智能策略的要求                                      | 118        |
| 安装 User Environment Manager                  | 118        |
| 配置 User Environment Manager                  | 118        |
| Horizon 智能策略设置                               | 119        |
| 带宽配置文件引用                                     | 120        |

|  |     |
|--|-----|
| 将条件添加到 Horizon 智能策略定义                                    | 120 |
| 在 User Environment Manager 中创建 Horizon 智能策略              | 122 |
| 使用 Active Directory 组策略                                  | 123 |
| 为远程桌面创建 OU   | 123 |
| 为远程桌面启用环回处理  | 123 |
| 使用 Horizon 7 组策略管理模板文件                                   | 124 |
| Horizon 7 ADMX 模板文件                                      | 124 |
| 将 ADMX 模板文件添加到 Active Directory                          | 126 |
| VMware View Agent 配置 ADMX 模板设置                           | 126 |
| 发送到远程桌面的客户端系统信息  | 132 |
| 在 Horizon 桌面上运行命令  | 136 |
| 会话协作策略设置   | 136 |
| 客户端驱动器重定向策略设置  | 137 |
| VMware HTML5 功能策略设置                                      | 138 |
| 适用于 Skype for Business 的 VMware Virtualization Pack 策略设置 | 140 |
| VMware Horizon 性能跟踪器策略设置                                 | 140 |
| VMware 集成打印策略设置  | 141 |
| PCoIP 策略设置   | 142 |
| PCoIP 常规设置   | 143 |
| PCoIP 剪贴板和拖放设置   | 148 |
| PCoIP 带宽设置   | 151 |
| PCoIP 键盘设置   | 153 |
| PCoIP 无损构建功能   | 154 |
| VMware Blast 策略设置  | 155 |
| 为 VMware Blast 启用无损压缩                                    | 160 |
| 使用远程桌面服务组策略  | 160 |
| RDS 应用程序兼容性设置  | 161 |
| RDS 连接设置   | 161 |
| RDS 设备和资源重定向设置   | 164 |
| RDS 许可设置   | 167 |
| RDS 打印机重定向设置   | 168 |
| RDS 配置文件设置   | 171 |
| RDS 连接服务器设置  | 172 |
| RDS 远程会话环境设置   | 175 |
| RDS 安全性设置  | 179 |
| RDS 会话时间限制   | 182 |
| RDS 临时文件夹设置  | 186 |
| 为虚拟打印筛选打印机   | 186 |
| 设置基于位置的打印  | 187 |
| 注册基于位置的打印组策略 DLL 文件                                      | 188 |
| 配置基于位置的打印组策略   | 189 |

|                              |     |
|------------------------------|-----|
| 基于位置的打印组策略设置语法               | 190 |
| 管理特殊的 Unity 窗口               | 191 |
| Active Directory 组策略示例       | 192 |
| 为 Horizon 7 计算机创建 OU         | 193 |
| 为 Horizon 7 组策略创建 GPO        | 193 |
| 将 Horizon 7 ADMX 模板文件添加到 GPO | 194 |
| 为远程桌面启用环回处理                  | 195 |

# 在 Horizon 7 中配置远程桌面功能

《在 Horizon 7 中配置远程桌面功能》介绍了如何在虚拟桌面上或 RDS 主机上配置随 Horizon Agent 一起安装的远程桌面功能。您还可以配置策略来控制桌面池和应用程序池、计算机以及用户的行为。

## 目标读者

此信息适用于任何要在虚拟桌面上或 RDS 主机上配置远程桌面功能或策略的人员。本文档中的信息专为已熟练掌握虚拟机技术和数据中心操作的 Windows 系统管理员所编写。



## 配置远程桌面功能

某些随 Horizon Agent 一起安装的远程桌面功能可以在 Horizon 7 版本中进行更新。您可以配置这些功能来增强最终用户的远程桌面体验。

这些功能包括 HTML Access、Unity Touch、Flash URL 重定向、HTML5 多媒体重定向、地理位置重定向、实时音频-视频、Windows Media 多媒体重定向 (Multimedia Redirection, MMR)、USB 重定向、扫描仪重定向、串行端口重定向、指纹扫描仪重定向、会话协作、Skype for Business 以及 URL 内容重定向。

有关 HTML Access 的信息，请参阅《VMware Horizon HTML Access 安装和设置指南》文档。有关 USB 重定向的信息，请参阅第 4 章 将 USB 设备与远程桌面和应用程序一起使用。有关 URL 内容重定向的信息，请参阅第 3 章 配置 URL 内容重定向。

本章讨论了以下主题：

- 配置 Unity Touch
- 为多播流或单播流配置 Flash URL 重定向
- 配置 Flash 重定向
- 配置 HTML5 多媒体重定向
- 配置地理位置重定向
- 使用实时音频-视频配置 Microsoft Teams
- 配置实时音频-视频
- 配置扫描仪重定向
- 配置串行端口重定向
- 管理对 Windows Media 多媒体重定向 (MMR) 功能的访问
- 管理对客户端驱动器重定向的访问
- 配置拖放功能
- 配置简单设备方向 (SDO) 传感器重定向
- 配置会话协作
- 配置适用于 Skype for Business 的 VMware Virtualization Pack
- 配置 VMware Integrated Printing 重定向
- 为 USB 重定向、Windows Media Player MMR 重定向或客户端驱动器重定向激活 BEAT 侧通道

## 配置 Unity Touch

通过 Unity Touch，平板电脑和智能手机用户无需使用“开始”菜单或任务栏，即可轻松浏览、搜索和打开 Windows 应用程序和文件，选择收藏的应用程序和文件，以及在正在运行的应用程序之间轻松切换。您可以配置默认在 Unity Touch 边栏显示的收藏应用程序列表。

安装 Horizon Agent 后，您可以通过在 Horizon Agent 配置 ADMX 模板文件 (vdm\_agent.admx) 中配置启用 Unity Touch 组策略设置来禁用或启用 Unity Touch 功能。

面向 iOS、Android 和 Chrome 操作系统设备的 VMware Horizon Client 文档针对 Unity Touch 提供的最终用户功能进行了详细介绍。请参阅 <https://docs.vmware.com/cn/VMware-Horizon-Client/index.html>。

## Unity Touch 的系统要求

安装 Horizon Client 的 Horizon Client 软件和移动设备必须满足特定版本要求，以支持 Unity Touch。

### 远程桌面

要支持 Unity Touch，最终用户将访问的虚拟机上必须安装下列软件：

- 您可以安装 View Agent 6.0 或更高版本或者 Horizon Agent 7.0 或更高版本，以安装 Unity Touch 功能。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“在虚拟机中安装 Horizon Agent”。
- 操作系统：Windows 7（32 位或 64 位）、Windows 8（32 位或 64 位）、Windows 8.1（32 位或 64 位）、Windows Server 2008 R2 或 Windows Server 2012 R2、Windows 10（32 位或 64 位）

### Horizon Client 软件

以下 Horizon Client 版本支持 Unity Touch：

- 适用于 iOS 的 Horizon Client
- 适用于 Android 的 Horizon Client
- 适用于 Chrome OS 的 Horizon Client

## 配置 Unity Touch 显示的收藏的应用程序

利用 Unity Touch 功能，平板电脑和智能手机用户可从 Unity Touch 边栏快速导航至远程桌面应用程序或文件。尽管最终用户可以指定显示在边栏中的收藏应用程序，但为便于使用，管理员可以配置收藏应用程序默认列表。

如果您使用浮动分配桌面池，除非您启用 Active Directory 中的漫游用户配置文件，否则断开桌面连接时最终用户指定的收藏应用程序和文件将会丢失。

当最终用户首次连接到启用 Unity Touch 的桌面时，收藏应用程序默认列表保持有效。但是，当用户配置了自己的收藏应用程序列表时，默认列表将被忽略。用户的收藏应用程序列表保存在用户的漫游配置文件中，在用户连接到浮动池或专用池中的不同计算机时可以使用。

如果您创建了收藏应用程序默认列表，但是列表中的一个或多个应用程序未在远程桌面操作系统中安装，或在“开始”菜单中找不到这些应用程序的路径，则这些应用程序将不会显示在收藏列表中。您可以利用此行为设置一个收藏应用程序的默认主列表，此列表可应用于安装了不同应用程序的多个虚拟机映像。

例如，如果 Microsoft Office 和 Microsoft Visio 安装在一个虚拟机上，Windows Powershell 和 VMware vSphere Client 安装在另一个虚拟机上，则您可以创建一个包含这四个应用程序的列表。仅已安装的应用程序在各个桌面中显示为默认收藏的应用程序。

您可以使用不同的方法指定收藏应用程序的默认列表：

- 向桌面池中虚拟机上的 Windows 注册表添加值
- 从 Horizon Agent 安装程序创建管理安装软件包，并将此软件包分发给虚拟机
- 从虚拟机上的命令行运行 Horizon Agent 安装程序

---

**注** Unity Touch 假定应用程序的快捷方式位于开始菜单的“程序”文件夹中。如果快捷方式不在“程序”文件夹内，请在快捷方式路径中添加前缀 **Programs**。例如，Windows Update.lnk 位于 ProgramData\Microsoft\Windows\Start Menu 文件夹中。要将此快捷方式公布为默认收藏的应用程序，请在快捷方式路径中添加前缀 **Programs**。例如：“Programs/Windows Update.lnk”。

---

### 前提条件

- 确认虚拟机上安装了 Horizon Agent。
- 确认您对虚拟机具有管理权限。在此过程中，您可能需要编辑注册表设置。
- 如果您拥有浮动分配桌面池，请使用 Active Directory 设置漫游用户配置文件。请遵循 Microsoft 的指示操作。

浮动分配桌面池用户将可以在每次登录时看到收藏的应用程序和文件列表。

### 步骤

- ◆ （可选）通过向 Windows 注册表中添加值创建收藏应用程序的默认列表。
  - a 打开 regedit，导航至 HKLM\Software\VMware, Inc.\VMware Unity 注册表设置。  
在 64 位虚拟机上，导航至 HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity 目录。
  - b 创建名为 FavAppList 的字符串值。
  - c 指定默认收藏的应用程序。

使用以下格式指定在开始菜单中使用的应用程序快捷方式路径。

```
path-to-app-1|path-to-app-2|path-to-app-3|...
```

例如：

```
Programs/Accessories/Accessibility/Speech Recognition.lnk|Programs/VMware/VMware vSphere Client.lnk|Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010 Language Preferences.lnk
```

- ◆ （可选） 通过从 Horizon Agent 安装程序创建管理安装软件包，创建收藏的应用程序的默认列表。

- a 通过命令行使用以下格式创建管理安装软件包。

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""a network share to store the admin install package"" UNITY_DEFAULT_APPS=""the list of default favorite apps that should be set in the registry""
```

例如：

```
VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""\\foo-installer-share \ViewFeaturePack\"" UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of Access.lnk|Programs/Accessories/System Tools/Character Map.lnk|Programs/Accessories/Windows PowerShell/Windows PowerShell.lnk|Programs/Internet Explorer (64-bit).lnk|Programs/Google Chrome/Google Chrome.lnk|Programs/iTunes/iTunes.lnk|Programs/Microsoft Office/Microsoft SharePoint Workspace 2010.lnk|Programs/PuTTY/PuTTY.lnk|Programs/Skype/Skype.lnk|Programs/WebEx/Productivity Tools/WebEx Settings.lnk|""
```

- b 使用贵组织所用的标准 Microsoft Windows Installer (MSI) 部署方法将管理安装软件包从网络共享分发到桌面虚拟机。

- ◆ （可选） 通过直接在虚拟机的命令行中运行 Horizon Agent 安装程序创建收藏的应用程序的默认列表。

使用以下格式：

```
VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /v"/qn UNITY_DEFAULT_APPS=""the list of default favorite apps that should be set in the registry""
```

**注** 以上命令包含了安装 Horizon Agent 和指定收藏的应用程序的默认列表这两项操作。因此，在运行此命令之前，您无需安装 Horizon Agent。

## 后续步骤

如果您直接在虚拟机上执行此任务（通过编辑 Windows 注册表或从命令行安装 Horizon Agent），则您必须部署新配置的虚拟机。您可以创建快照或制作模板，以及创建桌面池或重构现有池。您还可以创建 Active Directory 组策略来部署新配置。

## 为多播流或单播流配置 Flash URL 重定向

客户现在可以借助 Adobe Media Server 和多播或单播方式在虚拟桌面基础架构 (VDI) 环境中传送实时视频事件。要在 VDI 环境内传送多播或单播实时视频流，应绕过远程桌面，直接从媒体源向终端发送媒体流。Flash URL 重定向功能通过从远程桌面截获 ShockWave Flash (SWF) 文件并将它们重定向到客户端终端来支持上述功能。

然后使用客户端的本地 Flash 媒体播放器显示 Flash 内容。

将 Flash 内容直接从 Adobe Media Server 流式传输到客户端终端可以降低数据中心 ESXi 主机上的负载，无需通过数据中心进行路由，减少将 Flash 内容同时流式传输到多个客户端终端所需的带宽。

Flash URL 重定向功能使用由网页管理员嵌入到 HTML 网页中的 JavaScript。每当远程桌面用户在网页中单击指定的 URL 链接，JavaScript 便会从远程桌面会话中截获 SWF 文件并将其重定向到客户端终端。终端随后会在远程桌面会话外部打开本地 Flash Projector，开始在本地播放媒体流。

要配置 Flash URL 重定向，您必须设置 HTML 网页和客户端设备。

## 步骤

### 1 Flash URL 重定向的系统要求

要支持 Flash URL 重定向，Horizon 7 部署必须满足特定的软件和硬件要求。

### 2 验证是否安装了 Flash URL 重定向功能

在使用此功能前，请验证是否已安装 Flash URL 重定向功能，且在虚拟桌面中处于运行状态。

### 3 设置提供多播或单播流的网页

要允许进行 Flash URL 重定向，您必须在提供多播或单播流链接的 MIME HTML (MHTML) 网页中嵌入 JavaScript 命令。用户在其远程桌面的浏览器中显示这些网页以访问视频流。

### 4 为 Flash URL 重定向设置客户端设备

Flash URL 重定向功能可将 SWF 文件从远程桌面重定向到客户端设备。为使这些客户端设备能从多播或单播流播放 Flash 视频，必须验证客户端设备中是否安装了相应的 Adobe Flash Player。客户端还必须与媒体源具有 IP 连接。

### 5 禁用或启用 Flash URL 重定向

使用 VDM\_FLASH\_URL\_REDIRECTION=1 属性执行 Horizon Agent 的静默安装时，Flash URL 重定向功能将会处于启用状态。通过在这些虚拟机上的 Windows 注册表项上设置一个值，可以禁用或重新启用选定远程桌面上的 Flash URL 重定向功能。

## Flash URL 重定向的系统要求

要支持 Flash URL 重定向，Horizon 7 部署必须满足特定的软件和硬件要求。

### 远程桌面

- 您可以在静默安装 View Agent 6.0 或更高版本或者 Horizon Agent 7.0 或更高版本期间，通过在命令行中键入 VDM\_FLASH\_URL\_REDIRECTION 属性来安装 Flash URL 重定向功能。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“Horizon Agent 静默安装属性”。
- 桌面必须运行 64 位或 32 位 Windows 7 操作系统。
- 支持的桌面浏览器包括 Internet Explorer 8、9 和 10 和 Chrome 29.x，以及 Firefox 20.x。

### Flash 媒体播放器和 ShockWave Flash (SWF)

您必须将相应的 Flash 媒体播放器（例如 Strobe Media Playback）集成到网站上。要流式处理多播内容，您可以在网页中使用 `multicastplayer.swf` 或 `StrobeMediaPlayback.swf`。要流式处理实时单播内容，您必须使用 `StrobeMediaPlayback.swf`。还可以将 `StrobeMediaPlayback.swf` 用于支持的其他功能，例如 HTTP 动态流式处理。

## Horizon Client 软件

以下 Horizon Client 版本支持多播和单播：

- 适用于 Linux 的 Horizon Client 2.2 或更高版本
- 适用于 Windows 的 Horizon Client 2.2 或更高版本

以下 Horizon Client 版本仅支持多播（不支持单播）：

- 适用于 Linux 的 Horizon Client 2.0 或 2.1
- 适用于 Windows 的 Horizon Client 5.4

## Horizon Client 计算机或客户端访问设备

- 在 x86 瘦客户端设备上运行适用于 Linux 的 Horizon Client 的所有操作系统均支持 Flash URL 重定向。ARM 处理器不支持此功能。
- 运行适用于 Windows 的 Horizon Client 的所有操作系统均支持 Flash URL 重定向。有关更多信息，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。
- 在 Windows 客户端设备上，您必须为 Internet Explorer 安装 Adobe Flash Player 10.1 或更高版本。
- 在 Linux 瘦客户端设备上，您必须安装 libexpat.so.0 和 libflashplayer.so 文件。请参阅[Flash URL 重定向设置客户端设备](#)。

---

**注** 利用 Flash URL 重定向功能，多播或单播流可能被重定向到组织防火墙之外的客户端设备。客户端必须对托管 ShockWave Flash (SWF) 文件的 Adobe Web 服务器具有访问权限，SWF 文件可启动多播或单播流。根据需要配置防火墙，打开相应的端口，以允许客户端设备访问此服务器。

---

## 验证是否安装了 Flash URL 重定向功能

在使用此功能前，请验证是否已安装 Flash URL 重定向功能，且在虚拟桌面中处于运行状态。

需要支持多播或单播重定向的每个桌面都必须具备 Flash URL 重定向功能。有关 Horizon Agent 安装说明，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“Horizon Agent 静默安装属性”。

### 步骤

- 1 启动使用 PCoIP 的远程桌面会话。
- 2 打开任务管理器。
- 3 验证 ViewMPServer.exe 进程是否正在桌面上运行。

## 设置提供多播或单播流的网页

要允许进行 Flash URL 重定向，您必须在提供多播或单播流链接的 MIME HTML (MHTML) 网页中嵌入 JavaScript 命令。用户在其远程桌面的浏览器中显示这些网页以访问视频流。

此外，您可以自定义在 Flash URL 重定向出现问题时为最终用户显示的英文错误消息。如果您要向最终用户显示本地化错误消息，则执行此可选步骤。您必须在 MHTML 网页中嵌入 `var vmwareScriptErrorMessage` 配置和本地化文本字符串。

### 前提条件

验证 `swfobject.js` 资源库已被导入到 MHTML 网页。

### 步骤

- 1 将 `viewmp.js` JavaScript 命令嵌入到 MHTML 网页。

例如: `<script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>`

- 2 （可选） 自定义发送给最终用户的 Flash URL 重定向错误消息。

例如: `"var vmwareScriptErrorMessage=localized error message"`

- 3 确保在将 ShockWave Flash (SWF) 文件导入到 MHTML 网页前嵌入 `viewmp.js` JavaScript 命令，然后有选择性地自定义 Flash URL 重定向错误消息。

用户在远程桌面上显示网页时，`viewmp.js` JavaScript 命令将调用远程桌面上的 Flash URL 重定向功能，以将 SWF 文件从桌面重定向到托管客户端设备。

## 为 Flash URL 重定向设置客户端设备

Flash URL 重定向功能可将 SWF 文件从远程桌面重定向到客户端设备。为使这些客户端设备能从多播或单播流播放 Flash 视频，必须验证客户端设备中是否安装了相应的 Adobe Flash Player。客户端还必须与媒体源具有 IP 连接。

---

**注** 利用 Flash URL 重定向功能，多播或单播流可能被重定向到组织防火墙之外的客户端设备。客户端必须对托管 SWF 文件的 Adobe Web 服务器具有访问权限，SWF 文件可启动多播或单播流。根据需要配置防火墙，打开相应的端口，以允许客户端设备访问此服务器。

---



**步骤**

- ◆ 在客户端设备上安装 Adobe Flash Player。

| 操作系统    | 操作  |
|---------|---|
| Windows | 为 Internet Explorer 安装 Adobe Flash Player 10.1 或更高版本。   |
| Linux   | <p>a 安装 <code>libexpat.so.0</code> 文件，或确认已安装此文件。</p> <p>确保文件安装在 <code>/usr/lib</code> 或 <code>/usr/local/lib</code> 目录中。</p> <p>b 安装 <code>libflashplayer.so</code> 文件，或验证此文件已安装。</p> <p>确保文件安装在 Linux 操作系统的相应 Flash 插件目录中。</p> <p>c 安装 <code>wget</code> 程序，或验证此程序文件已安装。</p> |

**禁用或启用 Flash URL 重定向**

使用 `VDM_FLASH_URL_REDIRECTION=1` 属性执行 Horizon Agent 的静默安装时，Flash URL 重定向功能将会处于启用状态。通过在这些虚拟机上的 Windows 注册表项上设置一个值，可以禁用或重新启用选定远程桌面上的 Flash URL 重定向功能。

**步骤**

- 1 在虚拟机上启动 Windows 注册表编辑器。
- 2 导航至控制 Flash URL 重定向的 Windows 注册表项。

| 选项               | 说明   |
|------------------|--|
| Windows 7 (64 位) | <code>HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware ViewMP\enabled = value</code> |
| Windows 7 (32 位) | <code>HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware ViewMP\enabled = value</code>             |

- 3 设置值以禁用或启用 Flash URL 重定向。

| 选项  | 值 |
|-----|---|
| 已禁用 | 0 |
| 已启用 | 1 |

默认情况下，该值设置为 1。

**配置 Flash 重定向**

配置 Flash 重定向后，如果最终用户使用 Internet Explorer 9、10 或 11，则会将 Flash 内容发送到客户端系统，从而减少 ESXi 主机上的负载。客户端系统使用 Flash Player ActiveX 版本在 Flash 容器窗口中播放媒体内容。

尽管该功能的名称类似于名为“Flash URL 重定向”的功能，但它们之间存在显著的区别，如下表中所述。



**表 2-1. Flash 重定向功能与 Flash URL 重定向功能的比较**

| 区别项目                     | Flash 重定向  | Flash URL 重定向                               |
|--------------------------|--|---|
| 支持此功能的 Horizon Client 类型 | 仅 Windows 客户端  | Windows 客户端和 Linux 客户端                      |
| 显示协议                     | PCoIP 和 VMware Blast。  | PCoIP                                       |
| 浏览器                      | 适用于远程桌面的 Internet Explorer 9、10 或 11                           | 当前 Horizon Client 和 Horizon Agent 上支持的所有浏览器 |
| 配置机制                     | 使用 Horizon Agent 组策略设置指定使用 Flash 重定向的网站白名单或不使用 Flash 重定向的网站黑名单 | 要嵌入所需的 JavaScript，需修改网页上的源代码。               |

## 功能限制

Flash 重定向功能具有以下限制：

- 单击 Flash Player 窗口内的 URL 链接会在客户端而不是远程桌面（代理端）上打开浏览器。
- 一些网站不支持在某些浏览器版本中使用 Flash 重定向。例如，使用 Internet Explorer 11 时，vimeo.com 就不能使用该功能。
- Flash 和 Java 脚本可能无法按预期工作。
- Horizon Client 窗口在播放 Flash 内容时可能会冻结，不过您可以通过设置一个 Windows 注册表项来解决此问题。

在 32 位客户端上，将 HKLM\Software\VMware, Inc.\VMware VDM\Client\Enabled3DRenderer 值设置为“FALSE”，在 64 位客户端上，将 HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Enabled3DRenderer 设置为“FALSE”。

- YouTube 不再支持 Flash 媒体。
- Flash 重定向对 redbox.com 不起作用。
- 已禁用 Flash 上下文菜单（通过右键单击激活）。
- 如果 Horizon Client 4.1 使用 PCoIP 连接远程桌面，则 Flash 重定向会失败。结果或者是 Horizon Client 在远程桌面的本机播放器中播放 Flash 内容，或者是用户看到白屏。

## Flash 重定向的系统要求

Horizon Agent 和 Horizon Client 以及您安装代理和客户端软件的远程桌面和客户端系统必须满足特定要求才能支持 Flash 重定向功能。

### 远程桌面

- 必须在选定“Flash 重定向”自定义安装选项的情况下在虚拟桌面中安装 Horizon Agent 7.0 或更高版本。默认情况下，不会选择“Flash 重定向”自定义安装选项。请参阅《在 Horizon 7 中设置虚拟桌面》文档中有关安装 Horizon Agent 的主题。
- 必须配置相应的组策略设置。请参阅[安装并配置 Flash 重定向](#)。

- Windows 7、Windows 8、Windows 8.1 和 Windows 10 虚拟桌面支持 Flash 重定向。
- 必须在 Internet Explorer 9、10 或 11 中安装相应的 Flash ActiveX 插件。
- 安装相应插件后，必须在 Internet Explorer 中启用 VMware View FlashMMR Server 加载项。

#### Horizon Client 计算机或客户端访问设备

- 必须安装 Horizon Client 4.0 或更高版本。默认情况下，“Flash 重定向”选项处于启用状态。请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档中有关安装 Horizon Client 的主题。
- 在 Windows 7、Windows 8、Windows 8.1 和 Windows 10 上支持 Flash 重定向。
- 必须安装并启用 Flash ActiveX 插件

#### 用于远程会话的显示协议

- PCoIP
- VMware Blast（需要使用 Horizon Agent 7.0 或更高版本）

## 安装并配置 Flash 重定向

要将 Flash 内容从远程桌面重定向到本地客户端系统上的 Flash Player 窗口，需要在远程桌面和客户端系统上安装 Flash 重定向功能和 Internet Explorer，并指定使用此功能的网站。

要启用此功能并指定使用此功能的网站，您需要配置组策略设置。或者，也可以使用远程桌面上的 Windows 注册表设置来配置要用于 Flash 重定向的网站白名单。请参阅[使用 Windows 注册表设置配置 Flash 重定向](#)。

#### 前提条件

- 在客户端系统上安装 Horizon Client，在远程桌面上安装 Horizon Agent，并启用 Flash 重定向功能。有关所需的版本、安装选项和完整的系统要求，请参阅[Flash 重定向的系统要求](#)。
- 确认您能够以管理员域用户的身份登录到托管 Active Directory 服务器的计算机。
- 确认 MMC 和组策略对象编辑器插件在您的 Active Directory 服务器上可用。
- 将 Horizon Agent 配置 ADMX 模板文件 `vdm_agent.admx` 添加到远程桌面的 OU。有关安装说明，请参阅[将 ADMX 模板文件添加到 Active Directory](#)。
- 编译可以（白名单）或不能（黑名单）重定向 Flash 内容的网站列表。
- 确认 Flash ActiveX 已经安装，并且可以正常使用。要确认是否安装，请运行 Internet Explorer 并转到<https://helpx.adobe.com/flash-player.html>。

## 步骤

- 1 在客户端系统上，如有必要，请安装 Flash Player ActiveX 版本（而不是 NPAPI 版本）。

Internet Explorer 10 和 11 中默认已安装 Flash Player。对于 Internet Explorer 9，可能需要访问 <https://get.adobe.com/flashplayer/> 来下载并安装 Flash Player。

- 2 在远程桌面上，请执行以下安装步骤。

- a 安装 Internet Explorer 9、10 或 11。
- b 如有必要，安装 Flash Player ActiveX 版本（而不是 NPAPI 版本）。

Internet Explorer 10 和 11 中默认已安装 Flash Player。对于 Internet Explorer 9，可能需要访问 <https://get.adobe.com/flashplayer/> 来下载并安装 Flash Player。

- 3 在远程桌面上，从 Internet Explorer 的菜单栏中选择 **工具 > 管理加载项**，然后确认列出并启用了 **VMware View FlashMMR Server**。

- 4 在 Active Directory 服务器上，打开组策略管理编辑器，然后在 **计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > VMware FlashMMR** 文件夹中配置 Flash 重定向策略设置。

| 设置                    | 说明  |
|-----------------------|---|
| 启用 Flash 多媒体重定向       | 指定是否在远程桌面（代理端）上启用 Flash 重定向 (FlashMMR)。如果启用，该功能会通过 TCP 通道将 Flash 多媒体数据从指定 URL 转发到客户端，并调用客户端系统上的本地 Flash Player。该功能可大幅降低对代理端 CPU 和网络带宽的需求。               |
| 用于启用 FlashMMR 的最小矩形大小 | 为播放 Flash 内容的矩形指定最小宽度和高度（以像素为单位）。例如， <b>400,300</b> 指定宽度为 400 像素，高度为 300 像素。仅当 Flash 内容等于或大于此策略中指定的值时，才会使用 Flash 重定向。如果未配置此 GPO，则使用默认值 <b>320,200</b> 。 |

- 5 在 Active Directory 服务器上，打开组策略管理编辑器，然后在 **用户配置 > 策略 > 管理模板 > VMware View Agent 配置 > VMware FlashMMR** 文件夹中配置 Flash 重定向策略设置。

- a 要定义用于 Flash 重定向的主机 URL 列表，请打开 **FlashMMR URL 列表使用定义** 设置，并选择 **已启用**。
- b 在 **FlashMMR URL 列表使用定义** 下拉菜单中，选择 **启用白名单** 或 **启用黑名单**，然后单击 **确定**。  
默认情况下启用白名单。
- c 要添加使用或不使用 Flash 重定向的主机 URL 列表，请打开 **启用 FlashMMR 的主机 URL 列表** 设置，并选择 **已启用**。

- d 单击**显示**，然后在“值名称”列中输入您为白名单或黑名单编译的完整 URL。

请在 URL 中包含 `http://` 或 `https://` 前缀。您可以使用正则表达式。例如，可以指定 `https://*.google.com` 和 `http://www.cnn.com/*`。

在“值”列中，您可以选择指定 `requireIECompatibility=true` 或 `appMode=0`，或者同时指定两者。请使用逗号分隔两个字符串。

默认情况下，在 Flash 重定向运行时启用外部接口支持，而这可能会降低性能。在某些情况下，设置 `appMode=0` 可提高性能，并提供更出色的用户体验。

- e 单击**确定**以保存 URL 列表，然后再次单击**确定**以保存策略设置。

- 6 在远程桌面上，打开命令提示符，并导航到 `%Program Files%\Common Files\VMware\Remote Experience` 目录。

- 7 要向 Internet Explorer 添加白名单或黑名单，请运行 `cscript mergeflashmmrwhitelist.vbs` 命令。

- 8 重新启动 Internet Explorer。

设置了 `requireIECompatibility=true` 参数的站点会被添加到 Internet Explorer 的兼容性视图中。要验证兼容性视图中的站点，请从菜单栏中选择**工具 > 兼容性视图设置**。

这些站点还会被添加到 Internet Explorer 的受信任站点列表中。要验证受信任的站点，请从 Internet Explorer 菜单栏中选择**工具 > Internet 选项**，然后单击**安全选项卡**上的**站点**。

## 使用 Windows 注册表设置配置 Flash 重定向

如果您是在 Active Directory 服务器上没有管理员特权的域用户，则可以选择通过在远程桌面上设置 Windows 注册表项的相应值来配置 Flash 重定向。

您可以将此过程作为使用组策略设置配置 Flash 重定向的替代方法。

### 前提条件

- 要确保只有在列表中指定的 URL 可以重定向 Flash 内容，请编译网站白名单。您无法使用 Windows 注册表设置来启用黑名单。要启用黑名单，请使用 Flash 重定向的组策略设置。
- 确认远程桌面中安装了 Horizon Agent 7.0 或更高版本、Flash Player 以及 Internet Explorer 9、10 或 11。请参阅 [Flash 重定向的系统要求](#)。
- 确认客户端系统中安装了 Horizon Client 4.0 或更高版本以及 Flash Player ActiveX 版本。

### 步骤

- 1 使用 Horizon Client 访问远程桌面。
- 2 在远程桌面上打开 Windows 注册表编辑器 (`regedit.exe`)，导航到 `HKLM\Software\VMware, Inc.\VMware FlashMMR` 文件夹，然后将 **FlashRedirection** 设置为 **1**。

**注** 此设置将启用 Flash 重定向功能。如果在 `HKLM\Software\Policies\VMware, Inc.\VMware FlashMMR` 中禁用此设置（设置为 0），则会在域范围内禁用 Flash 重定向，在这种情况下，必须由域管理员才能进行启用。

- 3 导航到 `HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMware FlashMMR` 文件夹。

如果此文件夹不存在，请进行创建。

- 4 在 `VMware FlashMMR` 文件夹中，创建一个名为 `UrlWhiteList` 的子项。

- 5 右键单击 `UrlWhiteList` 项，选择**新建 > 字符串值**，然后输入使用 `Flash` 重定向的网站 URL 作为名称。

您可以使用正则表达式。例如，可以指定 `https://*.google.com`。将数据值留空。

- 6 （可选）在新注册表值的数据字段中，添加数据 `requireIECompatibility=true` 或 `appMode=0`，或者同时添加两者。

请使用逗号分隔两个字符串。默认情况下，在 `Flash` 重定向运行时会启用外部接口支持，而这可能会降低性能。在某些情况下，设置 `appMode=0` 可提高性能，设置 `appMode=1` 可提供更出色的用户体验。

- 7 要添加其他 URL，请重复上述步骤，然后关闭注册表编辑器。

- 8 在远程桌面上，打开命令提示符，并导航到 `%Program Files%\Common Files\VMware\Remote Experience` 目录。

- 9 要向 Internet Explorer 添加白名单，请运行 `cscript mergeflashmmrwhitelist.vbs` 命令。

- 10 重新启动 Internet Explorer。

设置了 `requireIECompatibility=true` 参数的站点会被添加到 Internet Explorer 的兼容性视图中。要验证兼容性视图中的站点，请从菜单栏中选择**工具 > 兼容性视图设置**。

这些站点还会被添加到 Internet Explorer 的受信任站点列表中。要验证受信任的站点，请从 Internet Explorer 菜单栏中选择**工具 > Internet 选项**，然后单击**安全选项卡**上的**站点**。

## 配置 HTML5 多媒体重定向

配置 HTML5 多媒体重定向后，如果最终用户使用 Google Chrome 或 Microsoft Edge 浏览器，会将 HTML5 多媒体内容发送到客户端系统，从而减少 ESXi 主机上的负载。客户端系统会播放多媒体内容，并且用户将获得更出色的音频和视频体验。

## HTML5 多媒体重定向的系统要求

Horizon Agent 和 Horizon Client 以及您安装代理和客户端软件的远程桌面和客户端系统必须满足特定要求才能支持 HTML5 多媒体重定向功能。

### 远程桌面

- 虚拟桌面必须在选定“HTML5 多媒体重定向”自定义安装选项的情况下安装 Horizon Agent 7.3.2 或更高版本（对于 Chrome）或 Horizon Agent 7.5 或更高版本（对于 Edge）。默认情况下，不会选择此选项。请参阅《在 Horizon 7 中设置虚拟桌面》文档中有关安装 Horizon Agent 的主题。

- 已发布桌面的 RDS 主机必须在选定“HTML5 多媒体重定向”自定义安装选项的情况下安装 Horizon Agent 7.3.2 或更高版本。默认情况下，不会选择此选项。请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档中有关安装 Horizon Agent 的主题。
- 必须在 Active Directory 服务器上配置 HTML5 多媒体重定向组策略设置。请参阅[安装和配置 HTML5 多媒体重定向](#)。
- 必须安装 Chrome 或 Edge 浏览器。
- 必须在 Chrome 或 Edge 浏览器中安装 VMware Horizon HTML5 多媒体重定向扩展。请参阅[安装适用于 Chrome 的 VMware Horizon HTML5 重定向扩展](#)或[安装适用于 Edge 的 VMware Horizon HTML5 重定向扩展](#)。

## 客户端系统

- 对于 Windows 客户端系统，必须在选定“HTML5 多媒体重定向支持”自定义安装选项的情况下安装 Horizon Client 4.6 或更高版本（对于 Chrome）或者 Horizon Client 4.8 或更高版本（对于 Edge）。默认情况下，此选项处于选定状态。请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档中有关安装 Horizon Client 的主题。
- 对于 Linux 客户端系统，必须在选定“HTML5 多媒体重定向支持”自定义安装选项的情况下安装 Horizon Client 5.1 或更高版本。默认情况下，此选项处于选定状态。请参阅《适用于 Linux 的 VMware Horizon Client 安装和设置指南》中有关安装 Horizon Client 的主题。
- HTML5 多媒体重定向不支持 Horizon Client 相对鼠标功能。

## 用于远程会话的显示协议

- PCoIP
- VMware Blast

## 安装和配置 HTML5 多媒体重定向

要将 HTML5 多媒体内容从远程桌面重定向到本地客户端系统，需要在远程桌面上安装 HTML5 多媒体重定向功能和 Chrome 或 Edge 浏览器，启用 HTML5 多媒体重定向功能，并指定使用此功能的网站。

要启用 HTML5 多媒体重定向并指定使用此功能的网站，您需要在 Active Directory 服务器上配置组策略设置。您必须编译可重定向 HTML5 多媒体内容的网站 URL 列表。应在 URL 中包含 `http://` 或 `https://` 前缀。您可以在 URL 中使用匹配模式。

例如，要重定向 YouTube 上的所有视频，可指定 `https://www.youtube.com/*`。要重定向 Vimeo 上的所有视频，可指定 `https://www.vimeo.com/*`。有关更多信息，请参阅[https://developer.chrome.com/extensions/match\\_patterns](https://developer.chrome.com/extensions/match_patterns)。

### 前提条件

- 在客户端系统上安装 Horizon Client，在远程桌面上安装 Horizon Agent，并启用 HTML5 多媒体重定向功能。有关所需的版本、安装选项和完整的系统要求，请参阅[HTML5 多媒体重定向的系统要求](#)。

- 确认您能够以管理员域用户的身份登录到托管 Active Directory 服务器的计算机。
- 确认 MMC 和组策略对象编辑器插件在您的 Active Directory 服务器上可用。
- 将 Horizon Agent 配置 ADMX 模板文件 `vdm_agent.admx` 添加到与虚拟桌面的 OU 或已发布桌面的 RDS 主机链接的 GPO。有关安装说明，请参阅[将 ADMX 模板文件添加到 Active Directory](#)。
- 编译可重定向 HTML5 多媒体内容的网站 URL 列表。

#### 步骤

- 1 在远程桌面上安装 Chrome 或 Edge 浏览器。
- 2 在 Active Directory 服务器上，打开组策略管理编辑器。
- 3 导航到**计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > VMware HTML5 功能**文件夹。
- 4 打开**启用 VMware HTML5 功能**设置，选择已启用，然后单击**确定**。
- 5 导航到**计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > VMware HTML5 功能 > VMware HTML5 多媒体重定向**文件夹。
- 6 打开**启用 VMware HTML5 多媒体重定向**设置，选择已启用，然后单击**确定**。
- 7 要使用 Chrome 浏览器，请执行以下步骤。
  - a 导航到**计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > VMware HTML5 功能 > VMware HTML5 多媒体重定向**文件夹。
  - b 打开为 **Chrome 浏览器启用 VMware HTML5 多媒体重定向**，选择已启用，然后单击**确定**。
- 8 要使用 Edge 浏览器，请执行以下步骤。
  - a 导航到**计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > VMware HTML5 功能 > VMware HTML5 多媒体重定向**文件夹。
  - b 打开为 **Edge 浏览器启用 VMware HTML5 多媒体重定向**设置，选择已启用，然后单击**确定**。
  - c 导航到**计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > VMware HTML5 功能**文件夹。
  - d 打开**禁止自动检测 Intranet**设置，选择已启用，然后单击**确定**。
- 9 指定哪些网站将使用 HTML5 多媒体重定向功能。
  - a 导航到**计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > VMware HTML5 功能 > VMware HTML5 多媒体重定向**文件夹。
  - b 打开**启用 VMware HTML5 多媒体重定向的 URL 列表**设置，并选择已启用。
  - c 单击**显示**，然后在“值名称”列中输入您编译的 URL。

只有您指定的 URL 才可以重定向 HTML5 多媒体内容。默认情况下，不会添加任何 URL。将“值”列留空。
  - d 单击**确定**以保存 URL 列表，然后再次单击**确定**以保存策略设置。



## 后续步骤

要使用 Chrome 浏览器，请在远程桌面上的 Chrome 浏览器中安装适用于 Chrome 的 VMware Horizon HTML5 重定向扩展。请参阅[安装适用于 Chrome 的 VMware Horizon HTML5 重定向扩展](#)。

要使用 Edge 浏览器，请在远程桌面上的 Edge 浏览器中安装适用于 Edge 的 VMware Horizon HTML5 重定向扩展。请参阅[安装适用于 Edge 的 VMware Horizon HTML5 重定向扩展](#)。

## 安装适用于 Chrome 的 VMware Horizon HTML5 重定向扩展

要在 Chrome 中使用 HTML5 多媒体重定向功能，您必须在远程桌面上强制安装 VMware Horizon HTML5 重定向扩展。通过在 Active Directory 服务器上配置 Google Chrome 组策略设置，可以强制安装该扩展。

要将 Chrome 组策略设置应用到远程桌面，您必须将 ADMX 模板文件添加到 Active Directory 服务器上的 GPO。对于虚拟桌面，必须将此 GPO 链接到包含该虚拟桌面的 OU。对于已发布的桌面，必须将此 GPO 链接到包含 RDS 主机的 OU。

### 前提条件

- 配置 HTML5 多媒体重定向功能。请参阅[安装和配置 HTML5 多媒体重定向](#)。
- 确认您能够以管理员域用户的身份登录到托管 Active Directory 服务器的计算机。
- 确认 MMC 和组策略对象编辑器插件在您的 Active Directory 服务器上可用。

### 步骤

- 1 从 [https://dl.google.com/dl/edgedl/chrome/policy/policy\\_templates.zip](https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip) 下载 Google Chrome policy\_templates.zip 文件。
- 2 解压缩 policy\_templates.zip 文件，并将 chrome.admx 和 chrome.adml 文件复制到 Active Directory 服务器。

在 policy\_templates.zip 文件中，chrome.admx 文件位于 \windows\admx 文件夹内，而 chrome.adml 文件则位于 \windows\admx\language 文件夹内。

- a 将 chrome.admx 文件复制到 Active Directory 服务器上的 %systemroot%\PolicyDefinitions 文件夹。
- b 将 chrome.adml 语言资源文件复制到 Active Directory 服务器上 %systemroot%\PolicyDefinitions 中的相应语言子文件夹。

例如，将 chrome.adml 文件的 en\_us 版本复制到 Active Directory 服务器上的 %systemroot%\PolicyDefinitions\en\_us 子文件夹。

- 3 在 Active Directory 服务器上，打开组策略管理编辑器，并导航到**计算机配置 > 策略 > 管理模板 > Google Chrome > 扩展**文件夹。
- 4 打开**配置强制安装的应用程序和扩展列表**策略设置，并单击**已启用**。
- 5 单击**显示**，并在“值”列中键入 `ljmaegmnepbjgkghdfkgegbckolmcok;https://clients2.google.com/service/update2/crx`。



- 6 单击**确定**以保存扩展 ID/更新 URL，然后再次单击**确定**以保存策略设置。
- 7 确认 HTML5 多媒体重定向扩展已安装在远程桌面上。
  - a 连接到远程桌面并启动 Chrome。
  - b 在 Chrome 地址栏中键入 **chrome://extensions**。

**VMware Horizon HTML5 重定向扩展**随即会显示在“扩展程序”列表中。

## 安装适用于 Edge 的 VMware Horizon HTML5 重定向扩展

要在 Edge 浏览器中使用 HTML5 多媒体重定向功能，您必须在远程桌面上安装适用于 Edge 的 VMware Horizon HTML5 重定向扩展，该扩展可从 Microsoft 应用商店获取。

### 前提条件

配置 HTML5 多媒体重定向功能。请参阅[安装和配置 HTML5 多媒体重定向](#)。

### 步骤

- 1 连接到远程桌面。
- 2 从 Microsoft 应用商店下载并安装 **适用于 Edge 的 VMware Horizon HTML5 重定向扩展**扩展。

安装该扩展后，Edge 浏览器窗口右上角将显示 **VMware HTML5 多媒体重定向**图标。HTML5 多媒体重定向功能工作正常时，该图标上会显示字母 REDR。

## 配置地理位置重定向

通过地理位置重定向功能，远程桌面和已发布的应用程序可以使用客户端设备的地理位置信息。

## 地理位置重定向的系统要求

Horizon Agent 和 Horizon Client 以及安装了代理和客户端软件的虚拟桌面或 RDS 主机和客户端计算机必须满足特定要求，才能支持地理位置重定向功能。

### 虚拟桌面或 RDS 主机

- **设置 > 隐私 > 位置**中的 Windows **位置服务**设置必须为开。
- 地理位置重定向功能支持以下远程桌面应用程序。

| 应用程序                                    | 平台                       |
|---|--------------------------|
| Google Chrome（最新版本）                     | 所有虚拟桌面或 RDS 主机           |
| Internet Explorer 11                    | 所有虚拟桌面或 RDS 主机           |
| Edge、Maps、Weather 以及其他 Win32 和 UWP 应用程序 | Windows 8.1 和 Windows 10 |

必须分别在每个受支持的浏览器中启用**位置**权限设置（如果有）。

- 必须在选择“地理位置重定向”自定义安装选项的情况下安装 Horizon Agent 7.6 或更高版本。默认情况下，不会选择此选项。请参阅《《在 Horizon 7 中设置虚拟桌面》》和《《在 Horizon 7 中设置已发布的桌面和应用程序》》文档中有关安装 Horizon Agent 的主题。
- 必须在 Active Directory 服务器上配置 VMware 地理位置重定向组策略设置。请参阅[安装和配置地理位置重定向](#)。
- 对于 Internet Explorer 11，必须为 Windows 7 虚拟桌面和 RDS 主机启用 VMware Horizon 地理位置重定向 IE 插件。请参阅[启用 VMware Horizon 地理位置重定向 IE 插件](#)。不需要为 Windows 8.1 和 Windows 10 虚拟桌面启用 VMware Horizon 地理位置重定向 IE 插件。装有 VMware 地理位置重定向驱动程序的 Windows 8.1 和 Windows 10 虚拟桌面支持 Internet Explorer。
- 对于 Chrome，必须启用 VMware Horizon 地理位置重定向 Chrome 插件。请参阅[启用 VMware Horizon 地理位置重定向 Chrome 插件](#)。

#### 客户端系统

- 对于 Windows 8.1 和 Windows 10 客户端系统，**设置 > 隐私 > 位置**中的 Windows **位置服务**设置必须为**开启**，Horizon 才能访问您的位置。
- 您必须在客户端系统上安装适用于 Windows 的 Horizon Client 4.9 或更高版本，并且必须在适用于 Windows 的 Horizon Client 中配置**地理位置**设置以共享客户端系统的位置信息。不支持非 Windows 客户端。有关信息，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。

#### 用于远程会话的显示协议

- PCoIP
- VMware Blast

## 安装和配置地理位置重定向

要将地理位置信息从客户端设备重定向到远程桌面或已发布的应用程序，需要在代理计算机上启用地理位置重定向功能，在 Active Directory 服务器上配置组策略设置，以及指定使用该功能的网站。

要启用地理位置重定向并指定使用该功能的网站，请在 Active Directory 服务器上配置组策略设置。您必须编译可使用重定向的地理位置信息的网站的 URL 列表。应在 URL 中包含 `http://` 或 `https://` 前缀。您可以在 URL 中使用匹配模式。

#### 前提条件

- 在客户端系统上安装 Horizon Client，并在启用了地理位置重定向功能的虚拟桌面或 RDS 主机上安装 Horizon Agent。有关所需的版本、安装选项和完整的系统要求，请参阅[地理位置重定向的系统要求](#)。
- 确认您能够以管理员域用户的身份登录到托管 Active Directory 服务器的计算机。
- 确认 MMC 和组策略对象编辑器插件在您的 Active Directory 服务器上可用。

- 将 Horizon Agent 配置 ADMX 模板文件 (vdm\_agent.admx) 添加到与虚拟桌面或 RDS 主机的 OU 链接的 GPO 中。有关安装说明，请参阅[将 ADMX 模板文件添加到 Active Directory](#)。
- 编译可使用重定向的地理位置信息的网站的 URL 列表。
- 在代理计算机上安装 Internet Explorer 11 或 Chrome。

### 步骤

- 1 在 Active Directory 服务器上，打开组策略管理编辑器。
- 2 导航到计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > VMware HTML5 功能文件夹。
- 3 打开禁止自动检测 Intranet 设置，选择已启用，然后单击确定。
- 4 打开启用 VMware HTML5 功能设置，选择已启用，然后单击确定。
- 5 导航到计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > VMware HTML5 功能 > VMware 地理位置重定向文件夹。
- 6 打开启用 VMware 地理位置重定向设置，选择已启用，然后单击确定。
- 7 指定可使用地理位置重定向功能的网站。

VMware Horizon 地理位置重定向 Chrome 插件会在所有 RDS 主机和虚拟桌面环境中使用此网站列表。VMware Horizon 地理位置重定向 IE 插件会在 RDS 主机和 Windows 7 虚拟桌面环境中使用此网站列表。

- a 打开启用 VMware 地理位置重定向的 URL 列表设置，然后选择已启用。
- b 单击显示，然后在“值名称”列中输入您编译的 URL。

仅指定的 URL 可以使用重定向的地理位置信息。默认情况下，不会添加任何 URL。将“值”列留空。

- c 单击确定以保存 URL 列表，然后再次单击确定以保存策略设置。

- 8 打开设置报告位置更新的最短距离设置，选择已启用，并指定客户端中位置更新和上一次报告给代理的更新（必须更新了新位置）之间的最短距离（以米为单位）。

默认情况下，最短距离为 75 米。

### 后续步骤

如果您在 Windows 7 虚拟桌面或 RDS 主机代理计算机上安装了 Internet Explorer，则还必须启用 VMware Horizon 地理位置重定向 IE 插件。有关信息，请参阅[启用 VMware Horizon 地理位置重定向 IE 插件](#)。

---

**注** 装有 VMware 地理位置重定向驱动程序的 Windows 8.1 和 Windows 10 虚拟桌面支持 Internet Explorer。不需要为 Windows 8.1 和 Windows 10 虚拟桌面启用 VMware Horizon 地理位置重定向 IE 插件。

---

如果您在代理计算机上安装了 Chrome，则还必须启用 VMware Horizon 地理位置重定向 Chrome 插件。有关信息，请参阅[启用 VMware Horizon 地理位置重定向 Chrome 插件](#)。

## 启用 VMware Horizon 地理位置重定向 IE 插件

要将 Windows 7 虚拟桌面或已发布的桌面上的 Internet Explorer 与地理位置重定向功能结合使用，您必须在虚拟桌面或 RDS 主机上启用 VMware Horizon 地理位置重定向 IE 插件。

装有 VMware 地理位置重定向驱动程序的 Windows 8.1 和 Windows 10 虚拟桌面支持 Internet Explorer。不需要为 Windows 8.1 和 Windows 10 虚拟桌面启用 VMware Horizon 地理位置重定向 IE 插件。

### 前提条件

- [安装和配置地理位置重定向。](#)
- 确认在 Internet Explorer 11 中禁用了**增强保护模式**。该插件不适用于该功能。
- 对于 Windows Server 操作系统，确认关闭了 **Internet Explorer 增强的安全配置**。该插件不适用于该功能。

### 步骤

- 1 在启用了地理位置重定向功能的虚拟桌面或 RDS 主机上，打开 Internet Explorer 11。
- 2 单击浏览器窗口右上角的工具图标，然后选择**管理加载项**。
- 3 向下滚动到 VMware, Inc. 部分，选择 **VMware Horizon 地理位置重定向 IE 插件**，然后单击**启用**。
- 4 重新启动 Internet Explorer 11。

## 启用 VMware Horizon 地理位置重定向 Chrome 插件

要将地理位置重定向功能与 Chrome 结合使用，您必须启用 VMware Horizon 地理位置重定向 Chrome 插件。

### 前提条件

[安装和配置地理位置重定向。](#)

### 步骤

- 1 在 Active Directory 服务器上，下载 [https://dl.google.com/dl/edgedl/chrome/policy/policy\\_templates.zip](https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip) 文件。
- 2 解压缩 chrome.admx 文件，然后将其复制到 Active Directory 服务器上的 %systemroot%\PolicyDefinitions 文件夹。
- 3 解压缩 chrome.adml 语言资源文件，然后将其复制到 Active Directory 服务器上 %systemroot%\PolicyDefinitions 文件夹中的相应语言子文件夹。  
  
例如，将 chrome.adml 文件的 en\_us 版本复制到 Active Directory 服务器上的 %systemroot%\PolicyDefinitions\en\_us 子文件夹。
- 4 在 Active Directory 服务器上，打开组策略管理编辑器，并导航到**计算机配置 > 策略 > 管理模板 > Google Chrome > 扩展**文件夹。
- 5 打开**配置强制安装的应用程序和扩展列表**组策略设置，并单击**已启用**。

- 6 单击**显示**，在**值**文本框中键入 `lndponbebpcehnoblfgdfeiegeaokcf;https://clients2.google.com/service/update2/crx`，然后单击**确定**。
- 7 要保存更改，请单击**确定**。
- 8 要验证远程桌面上是否已安装 VMware Horizon 地理位置重定向扩展，请执行以下步骤。
  - a 连接到远程桌面并启动 Chrome。
  - b 在 Chrome 地址栏中键入 `chrome://extensions`。
  - c 确认 VMware Horizon 地理位置重定向显示在“扩展程序”列表中。

## 使用实时音频-视频配置 Microsoft Teams

通过实时音频-视频，Horizon 7 用户可以在其远程会话中运行 Microsoft Teams。

在本地连接到客户端系统的网络摄像头和音频设备会被重定向到远程会话，并且使用的带宽显著低于使用 USB 重定向时的带宽。

在远程桌面中启动 Microsoft Teams 应用程序时，您需要从应用程序的菜单中选择 VMware 虚拟输入和输出设备。VMware 虚拟设备会重定向连接到客户机的音频-视频设备。

对于虚拟桌面，请选择“VMware Virtual Microphone”和“VMware Virtual Webcam”。

对于已发布的桌面和应用程序，请选择“远程音频设备”和“VMware Virtual Webcam”。

要将实时音频-视频与 Microsoft Teams 配合使用，您必须在 Horizon Client 系统上安装音频和网络摄像头设备驱动程序。

随 Horizon Agent 一起安装实时音频-视频后，无需任何进一步配置，即可在您的远程会话中使用 Microsoft Teams。请参阅[配置实时音频-视频](#)。

## 将 Microsoft Teams 与实时音频-视频配合使用的建议

要将 Microsoft Teams 与实时音频-视频配合使用，请遵循以下建议：

- Windows、Linux 和 Mac 客户端上的 Horizon Agent 版本 7.9 及更高版本支持将 Microsoft Teams 与实时音频-视频配合使用。
- 要将 Microsoft Teams 与实时音频-视频配合使用，需要至少 4 个 vCPU 和 4 GB 的配置，最大视频分辨率为 640 x 480 像素。更多 vCPU 和更高的内存配置可提供更卓越的体验。
- 用于实时音频-视频的默认视频分辨率为 320 x 240 像素。您可以通过在组策略管理编辑器的 **VMware View Agent 配置 > 查看 RTAV 配置** 文件夹中更改设置来更改分辨率。
- 在 Windows 客户机上，您可以通过选择外围设备（如耳机）作为默认设备，来使用该设备。在客户机上，右键单击**通知区域图标**中的扬声器图标，然后选择**录音设备**。或者，在“控制面板”中，选择**声音**。右键单击要使用的设备，然后选择**设置为默认设备**。确保在“播放”和“录制”选项卡中选择了该默认设备。

## 配置实时音频-视频

通过实时音频-视频功能，Horizon 7 用户可以在其远程会话中运行 Skype、Webex、Google Hangouts、Microsoft Teams 及其他在线会议应用程序。使用实时音频-视频功能，客户端系统本地连接的网络摄像头和音频设备将被重定向到远程会话。此功能在重定向视频和音频数据时所占用的带宽远小于 USB 重定向。

实时音频-视频功能可兼容标准的会议应用程序和基于浏览器的视频应用程序，支持标准网络摄像头、音频 USB 设备和模拟音频输入。

在远程桌面上设置诸如 Skype、Webex、Google Hangouts 或 Microsoft Teams 之类的应用程序期间，您可以从该应用程序的菜单中选择输入和输出设备。对于虚拟机桌面，您可以选择“VMware 虚拟麦克风”和“VMware Virtual Webcam”。对于已发布的桌面和应用程序，您可以选择“远程音频设备”和“VMware Virtual Webcam”。

VMware Virtual Webcam 使用内核模式的网络摄像头驱动程序，可增强与基于浏览器的视频应用程序和其他第三方会议软件的兼容性。

会议应用程序或视频应用程序启动后，会显示并使用这些 VMware 虚拟设备，由这些设备处理从客户端上的本地连接设备进行的音频-视频重定向。

您的 Horizon Client 系统必须安装音频设备和网络摄像头设备的驱动程序才能启用重定向功能。

## 实时音频-视频的配置选择

随 Horizon Agent 一起安装实时音频-视频后，无需任何进一步配置，此功能即可在您的远程会话中使用。建议大多数标准设备和应用程序使用网络摄像头帧速率和图像分辨率的默认值。

您可以通过配置组策略设置更改默认值来满足特定应用程序、网络摄像头或环境的要求。也可以通过设置策略来禁用或启用该功能。利用 ADMX 模板文件，您可以在 Active Directory 服务器上或单个桌面上安装实时音频-视频组策略设置。请参阅[配置实时音频-视频组策略设置](#)。

如果用户具有多个内置的或连接到其客户端计算机的网络摄像头和音频输入设备，您可以配置将被重定向的首选网络摄像头和音频输入设备。请参阅[选择首选网络摄像头和麦克风](#)。

---

**注** 您可以选择首选音频设备，但是除此之外没有其他可用的音频配置选项。

---

当网络摄像头图像和音频输入被重定向到远程会话时，您无法在本地计算机上访问网络摄像头和音频设备。反之，如果在本地计算机上使用这些设备，您将无法在远程会话上对它们进行访问。

有关支持的应用程序的信息，请参阅 VMware 知识库文章《在 Horizon View 桌面上通过第三方应用程序使用实时音频-视频的指南》，网址为：<http://kb.vmware.com/kb/2053754>。

## 实时音频-视频的系统要求

实时音频-视频适用于标准网络摄像头、USB 音频设备和模拟音频设备。此功能也适用于 Skype、WebEx、Google Hangouts 和 Microsoft Teams 等标准会议应用程序。要支持实时音频-视频，您的 Horizon 部署必须满足特定的软件和硬件要求。

### 虚拟桌面

在将 Microsoft Teams 与 RTAV 配合使用时，VMware 建议虚拟桌面至少具有 4 个 vCPU 和 4 GB RAM。

### Horizon Client 软件

- 适用于 Windows 的 Horizon Client 2.2 或更高版本
- 适用于 Linux 的 Horizon Client 2.2 或更高版本。对于适用于 Linux 的 Horizon Client 3.1 或更低版本，仅第三方供应商提供的适用于 Linux 的 Horizon Client 版本具有该功能。对于适用于 Linux 的 Horizon Client 3.2 或更高版本，VMware 提供的客户端版本也具有该功能。
- 适用于 Mac 的 Horizon Client 2.3 或更高版本
- 适用于 iOS 的 Horizon Client 4.0 或更高版本。
- 适用于 Android 的 Horizon Client 4.0 或更高版本。

### Horizon Client 计算机或客户端访问设备

- 运行适用于 Windows 的 Horizon Client 的所有操作系统。
- 在 x86 设备上运行适用于 Linux 的 Horizon Client 的所有操作系统。ARM 处理器不支持此功能。
- Mac OS X Mountain Lion (10.8) 和更高版本。该功能在所有早期版本的 Mac OS X 操作系统中处于禁用状态。
- 运行适用于 iOS 的 Horizon Client 的所有操作系统。
- 运行适用于 Android 的 Horizon Client 的所有操作系统。
- 有关支持的客户端操作系统的信息，请参阅适用于相应系统或设备的 Horizon Client 安装和设置文档。
- 必须安装网络摄像头和音频设备驱动程序，且网络摄像头和音频设备在客户端计算机中必须可操作。您不需要在安装了代理的计算机上安装设备驱动程序。

### 显示协议

- PCoIP
- VMware Blast（需要使用 Horizon Agent 7.0 或更高版本）

## 确保使用的是实时音频-视频而非 USB 重定向

实时音频-视频功能支持适用于会议应用程序的网络摄像头和音频输入重定向。可随 Horizon Agent 一起安装的 USB 重定向功能不支持网络摄像头重定向。如果您通过 USB 重定向功能重定向音频输入设备，那么在实时音频-视频会话期间音频流将无法与视频正确同步，同时也将失去减少网络带宽需求这种优势。您可以采取一些措施来确保网络摄像头和音频输入设备将通过实时音频-视频功能（而非 USB 重定向功能）重定向到您的桌面。



如果为您的桌面配置了 USB 重定向，最终用户可以在 Windows 客户端菜单栏中选择**连接 USB 设备**选项或者在 Mac 客户端中选择**桌面 > USB** 菜单以连接并显示本地连接的 USB 设备。Linux 客户端默认会阻止音频和视频设备的 USB 重定向，并且不向最终用户提供 USB 设备选项。

如果最终用户从**连接 USB 设备**或**桌面 > USB** 列表中选择一个 USB 设备，该设备将不可用于视频或音频会议。例如，如果用户进行 Skype 通话，可能无法显示视频图像，或者音频流质量可能下降。如果最终用户在会议会话期间选择设备，网络摄像头或音频重定向将会中断。

要向最终用户隐藏这些设备并防止可能出现的中断，您可以配置 USB 重定向组策略设置来禁止在 VMware Horizon Client 中显示网络摄像头和音频输入设备。

特别是，您可以为 Horizon Agent 创建 USB 重定向过滤规则，然后指定要禁用的 audio-in 和 video 设备系列名称。有关设置组策略和指定 USB 重定向过滤规则的信息，请参阅[使用策略控制 USB 重定向](#)。

---

**小心** 如果您未设置 USB 重定向过滤规则来禁用 USB 设备系列，请告知最终用户，他们不能从 VMware Horizon Client 菜单栏的**连接 USB 设备**或**桌面 > USB** 列表中选择网络摄像头或音频设备。

---

## 选择首选网络摄像头和麦克风

如果客户端计算机有多个网络摄像头和麦克风，您可以配置一个首选网络摄像头和默认麦克风，实时音频-视频可将其重定向到远程桌面或已发布的应用程序。这些设备可以是内置的，也可以是连接到本地客户端计算机的设备。

在安装有适用于 Windows 的 Horizon Client 4.2 或更高版本的 Windows 客户端计算机上，您可以通过在“Horizon Client 设置”对话框中配置“实时音频-视频”设置来选择首选的网络摄像头。对于较早的 Horizon Client 版本，可以通过修改注册表设置选择首选的网络摄像头，并使用 Windows 操作系统中的声音控制来选择默认麦克风。

在 Mac 客户端计算机上，您可以使用 Mac 默认系统指定首选的网络摄像头或麦克风。

在 Linux 客户端计算机上，可以通过编辑配置文件指定首选网络摄像头。要选择默认麦克风，您可以在客户端计算机的 Linux 操作系统中配置声音控制。

实时音频-视频可重定向首选网络摄像头（如有）。如果没有首选网络摄像头，实时音频-视频将使用系统枚举提供的第一个网络摄像头。

## 选择 Windows 客户端系统上的首选网络摄像头或麦克风

配置实时音频-视频功能后，如果有多个网络摄像头或麦克风连接到本地客户端系统，远程桌面或已发布应用程序只会使用其中的一个设备。要指定首选的网络摄像头或麦克风，您可以配置 Horizon Client 中的“实时音频-视频”设置。

如果有首选网络摄像头或麦克风，则远程桌面或已发布的应用程序将使用首选网络摄像头。如果没有首选网络摄像头或麦克风，则使用其他的网络摄像头或麦克风。

利用实时音频-视频功能，视频设备、音频输入设备和音频输出设备无需使用 USB 重定向即可运行，所需的网络带宽总量也大大降低。也支持模拟音频输入设备。

---

**注** 如果使用 USB 网络摄像头或麦克风，请不要从 Horizon Client 中的**连接 USB 设备**菜单中进行连接。这样做将会导致通过 USB 重定向路由设备，并且导致设备不能使用实时音频-视频功能。

---



### 前提条件

- 确认本地客户端系统中已安装并可正常使用 USB 网络摄像头或者 USB 麦克风或其他类型的麦克风。
- 确认您对远程桌面或已发布应用程序使用的是 VMware Blast 显示协议或 PCoIP 显示协议。
- 连接到一个服务器。

### 步骤

- 1 打开**设置**对话框，然后在左侧窗格中选择**实时音频-视频**。
  - 单击桌面和应用程序选择器窗口右上角的**设置**（齿轮）图标。
  - 右键单击桌面和应用程序选择器窗口中的远程桌面或已发布的应用程序，然后选择**设置**。
- 2 要选择首选网络摄像头，请从**首选网络摄像头**下拉菜单中选择网络摄像头。  
该菜单中会显示客户端系统上的可用网络摄像头。
- 3 要选择首选麦克风，请从**首选麦克风**下拉菜单中选择麦克风。  
该菜单中会显示客户端系统上的可用麦克风。
- 4 要保存更改，请单击**确定**或**应用**。

当您在下一次启动远程桌面或已发布的应用程序时，会将您选择的首选网络摄像头或麦克风重定向到远程会话。

## 在 Mac 客户端上选择默认麦克风

如果在 Mac 客户端上有多个麦克风，远程桌面仅使用一个麦克风。可以使用 Mac 客户端上的“系统偏好设置”在远程桌面中指定默认麦克风。

利用实时音频-视频功能、音频输入设备和音频输出设备无需使用 USB 重定向即可运行，所需的网络带宽量也大大降低。也支持模拟音频输入设备。

---

**重要事项** 使用 USB 麦克风时，请不要从 Horizon Client 中的**连接 > USB** 菜单中进行连接。这样做将会导致通过 USB 重定向路由设备，并且导致设备不能使用实时音频-视频功能。

---

### 前提条件

- 确认 Mac 客户端中已安装并可正常使用 USB 麦克风或其他类型的麦克风。
- 对远程桌面使用 VMware Blast 显示协议或 PCoIP 显示协议。

### 步骤

- 1 在 Mac 客户端上，选择 **Apple 菜单 > 系统偏好设置**，然后单击**声音**。
- 2 打开“声音偏好设置”的“输入”窗格。
- 3 选择要使用的麦克风。

下次连接远程桌面并发起通话时，远程桌面会使用您在 Mac 客户端上选择的默认麦克风。

## 在 Mac 客户端上配置实时音频-视频

您可以使用 Mac 默认系统在命令行中配置实时音频-视频设置。通过使用默认系统，您可以使用 Terminal (/Applications/Utilities/Terminal.app) 读取、写入和删除 Mac 用户默认设置。

Mac 默认系统属于域，域通常对应于各个应用程序。实时音频-视频功能的域为 `com.vmware.rtav`。

### 实时音频-视频的配置语法

可以使用以下命令来配置实时音频-视频功能。

**表 2-2. 实时音频-视频配置的命令语法**

| 命令   | 说明   |
|--|--|
| <code>defaults write com.vmware.rtav srcWCamId "webcam-userid"</code>          | 设置要在远程桌面上使用的首选网络摄像头。未设置此值时，由系统枚举自动选定网络摄像头。您可以指定连接到（内置到）客户端系统的任何网络摄像头。  |
| <code>defaults write com.vmware.rtav srcAudioInId "audio-device-userid"</code> | 设置要在远程桌面上使用的首选麦克风（音频输入设备）。未设置此值时，远程桌面使用客户端系统上设置的默认录音设备。您可以指定连接到（内置到）客户端系统的任何麦克风。   |
| <code>defaults write com.vmware.rtav srcWCamFrameWidth pixels</code>           | 设置图像宽度。值默认为硬编码值 320 像素。您可以将图像宽度更改为任意像素值。   |
| <code>defaults write com.vmware.rtav srcWCamFrameHeight pixels</code>          | 设置图像高度。值默认为硬编码值 240 像素。您可以将图像高度更改为任意像素值。   |
| <code>defaults write com.vmware.rtav srcWCamFrameRate fps</code>               | 设置帧速率。值默认为 15 fps。您可以将帧速率更改为任意值。   |
| <code>defaults write com.vmware.rtav LogLevel "level"</code>                   | 设置实时音频-视频日志文件 (~/.Library/Logs/VMware/vmware-RTAV- <i>pid</i> .log) 的日志级别。可以将日志级别设置为 <code>trace</code> 或 <code>debug</code> 。 |
| <code>defaults write com.vmware.rtav IsDisabled value</code>                   | 确定是启用还是禁用实时音频-视频。默认情况下启用实时音频-视频。（此值无效。）要禁用客户端上的实时音频-视频，将该值设置为 <code>true</code> 。  |
| <code>defaults read com.vmware.rtav</code>                                     | 显示实时音频-视频配置设置。   |
| <code>defaults delete com.vmware.rtav setting</code>                           | 删除实时音频-视频配置设置，例如： <code>defaults delete com.vmware.rtav srcWCamFrameWidth</code>   |

**注** 您可以将帧速率从 1 fps 最高调整为 25 fps，将分辨率最高调整为最大值 1920x1080。并非所有设备或所有环境都支持较快帧速下的高分辨率。

## 在 Mac 客户端上配置首选的网络摄像头或麦克风

如果在 Mac 客户端上具有多个网络摄像头或麦克风，则在具有实时音频-视频功能的远程桌面中只能使用一个网络摄像头和一个麦克风。您可以使用 Mac 默认系统在命令行中指定首选的网络摄像头和麦克风。

利用实时音频-视频功能，网络摄像头、音频输入设备和音频输出设备无需使用 USB 重定向即可运行，所需的网络带宽总量也有所降低。也支持模拟音频输入设备。

在大多数环境中，不需要配置首选麦克风或网络摄像头。如果您未设置首选麦克风，远程桌面会使用在客户端系统的“系统偏好设置”中设置的默认音频设备。请参阅[在 Mac 客户端上选择默认麦克风](#)。如果您未配置首选网络摄像头，远程桌面会按枚举选择网络摄像头。

### 前提条件

- 如果要配置首选 USB 网络摄像头，请确认客户端系统中已安装并可正常使用该网络摄像头。
- 如果要配置首选 USB 麦克风或其他类型的麦克风，请确认 Mac 客户端中已安装并可正常使用该麦克风。
- 对远程桌面使用 VMware Blast 显示协议或 PCoIP 显示协议。

### 步骤

- 1 在 Mac 客户端上，启动一个网络摄像头或麦克风应用程序以触发摄像头设备或音频设备枚举并记录到实时音频-视频日志文件中。
  - a 添加网络摄像头或音频设备。
  - b 在应用程序文件夹中，双击 **VMware Horizon Client** 启动 Horizon Client。
  - c 发起一次通话，然后停止。
- 2 在实时音频-视频日志文件中找到网络摄像头或麦克风的日志条目。

- a 在文本编辑器中，打开实时音频-视频日志文件。

实时音频-视频日志文件名为 `~/Library/Logs/VMware/vmware-RTAV-pid.log`，其中 *pid* 是当前会话的进程 ID。

- b 在实时音频-视频日志文件中搜索标识连接的网络摄像头或麦克风的条目。

以下示例介绍了在实时音频-视频日志文件中网络摄像头条目可能的显示形式：

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() - 1
Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=FaceTime HD Camera (Built-in)   UserId=FaceTime HD Camera (Built-in)#0xfa20000005ac8509
SystemId=0xfa20000005ac8509
```

以下示例介绍了在实时音频-视频日志文件中麦克风条目可能的显示形式：

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: int
AVCaptureEnumerateAudioDevices(MMDev::DeviceList&) -
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() - 2
Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() -
Index=255   Name=Built-in Microphone   UserId=Built-in
Microphone#AppleHDAEngineInput:1B,0,1,0:1   SystemId=AppleHDAEngineInput:1B,0,1,0:1
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() -
Index=255   Name=Built-in Input   UserId=Built-in Input#AppleHDAEngineInput:1B,0,1,1:2
SystemId=AppleHDAEngineInput:1B,0,1,1:2
```

- 3 在实时音频-视频日志文件中找到您首选的网络摄像头或麦克风，并记录其用户 ID。

在日志文件中用户 ID 显示在字符串 `UserId=` 的后面。例如，内部视频通话摄像头的用户 ID 为 **FaceTime HD Camera (Built-in)**，而内部麦克风的用户 ID 为 **Built-in Microphone**。

- 4 在“终端” (/Applications/Utilities/Terminal.app) 中，使用 `defaults write` 命令设置首选网络摄像头或麦克风。

| 选项        | 操作   |
|-----------|--|
| 设置首选网络摄像头 | 键入 <code>defaults write com.vmware.rtav srcWCamId "webcam-userid"</code> ，其中 <code>webcam-userid</code> 是首选网络摄像头的用户 ID，可从实时音频-视频日志文件中获取。例如：<br><pre>defaults write com.vmware.rtav srcWCamId "HD Webcam C525"</pre>                      |
| 设置首选麦克风   | 键入 <code>defaults write com.vmware.rtav srcAudioInId "audio-device-userid"</code> ，其中 <code>audio-device-userid</code> 是首选麦克风的用户 ID，可从实时音频-视频日志文件中获取。例如：<br><pre>defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"</pre> |

- 5 （可选）使用 `defaults read` 命令来验证对实时音频-视频功能所做的更改。

例如：`defaults read com.vmware.rtav`

此命令会列出所有实时音频-视频设置。

下次连接远程桌面并发起新的通话时，远程桌面会使用您配置的首选网络摄像头或麦克风（如果可用）。如果首选网络摄像头或麦克风不可用，则远程桌面可以使用其他可用的网络摄像头或麦克风。

## 选择 Linux 客户端系统上的默认麦克风

如果您的客户端系统中有多于一个麦克风，远程桌面只使用其中一个。要指定默认麦克风，您可以使用客户端系统上的声音控制。

利用实时音频-视频功能，音频输入设备和音频输出设备无需使用 USB 重定向即可运行，所需的网络带宽总量也大大降低。也支持模拟音频输入设备。

此过程介绍如何从客户端系统用户界面上选择默认麦克风。管理员也可以通过编辑配置文件配置首选麦克风。请参阅[选择 Linux 客户端系统上的首选网络摄像头或麦克风](#)。

### 前提条件

- 确认客户端系统中已安装 USB 麦克风或其他类型的麦克风，且可正常使用。
- 验证您是否在远程桌面中使用 VMware Blast 或 PCoIP 显示协议。

### 步骤

- 1 在 Ubuntu 图形用户界面中，选择 **系统 > 首选项 > 声音**。

您也可以单击屏幕顶部工具栏右侧的**声音**图标。

- 2 单击“声音首选项”对话框中的**输入**选项卡。
- 3 选择首选设备，然后单击**关闭**。

## 选择 Linux 客户端系统上的首选网络摄像头或麦克风

启用实时音频-视频功能后，如果客户端系统中具有多个网络摄像头和麦克风，在远程桌面中只能使用一个网络摄像头和一个麦克风。要指定首选网络摄像头和麦克风，您可以编辑配置文件。

如果有首选网络摄像头或麦克风，则远程桌面将使用首选网络摄像头；如果没有，则使用其他的网络摄像头或麦克风。

利用实时音频-视频功能，网络摄像头、音频输入设备和音频输出设备无需使用 USB 重定向即可运行，所需的网络带宽总量也大大降低。也支持模拟音频输入设备。

要在 `/etc/vmware/config` 文件中设置属性并指定首选设备，您必须确定特定字段的值。您可以在日志文件中搜索这些字段的值。

- 对于网络摄像头，应将 `rtav.srcWCamId` 属性设置为网络摄像头的 `UserId` 字段值，将 `rtav.srcWCamName` 属性设置为网络摄像头的 `Name` 字段值。

`rtav.srcWCamName` 属性的优先级高于 `rtav.srcWCamId` 属性。这两个属性都应指定同一个网络摄像头。如果这两个属性指定不同的网络摄像头，并且 `rtav.srcWCamName` 指定的网络摄像头确实存在，将使用该网络摄像头。如果该网络摄像头不存在，将使用 `rtav.srcWCamId` 指定的网络摄像头。如果这两个网络摄像头均找不到，则使用默认的网络摄像头。

- 对于音频设备，您将 `rtav.srcAudioInId` 属性设置为脉冲音频 `device.description` 字段的值。

### 前提条件

根据您要配置首选网络摄像头和/或首选麦克风，执行相应的必备任务：

- 确认客户端系统中已安装 USB 网络摄像头，且可正常使用。
- 确认客户端系统中已安装 USB 麦克风或其他类型的麦克风，且可正常使用。
- 验证您是否在远程桌面中使用 VMware Blast 或 PCoIP 显示协议。

### 步骤

- 1 启动客户端，打开网络摄像头或麦克风应用程序，以触发照相机设备或音频设备的枚举并记录到客户端日志中。
  - a 添加您要使用的网络摄像头或音频设备。
  - b 使用 `vmware-view` 命令启动 Horizon Client。
  - c 发起一次通话，然后停止。

此过程将会创建一个日志文件。

## 2 查找网络摄像头或麦克风的日志条目。

### a 使用文本编辑器打开调试日志文件。

包含实时音频-视频日志消息的日志文件位于 `/tmp/vmware-<username>/vmware-RTAV-<pid>.log` 中。客户端日志位于 `/tmp/vmware-<username>/vmware-view-<pid>.log` 中。

### b 搜索日志文件，查找引用连接的网络摄像头和麦克风的日志文件条目。

以下示例显示了选定网络摄像头的摘录内容：

```
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - 3 Device(s) found
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=UVC Camera (046d:0819)
UserId=UVC Camera (046d:0819)#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.5
SystemId=/dev/video1
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=gspca main driver
UserId=gspca main driver#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.7
SystemId=/dev/video2
main| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=Microsoft® LifeCam HD-6000 for Notebooks UserId=Microsoft® LifeCam HD-6000 for
Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6 SystemId=/dev/video0
main| W110: RTAV: static bool AudioCaptureLin::EnumCaptureDevices(MMDev::DeviceList&) -
enumeration data unavailable
```

以下示例显示了选定音频设备的摘录内容以及每个设备当前的音频等级：

```
vthread-18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() - Triggering enumeration
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=1 'alsa_output.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-stereo.monitor' 'Monitor of Logitech USB
Headset Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:1 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=2 'alsa_input.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-mono' 'Logitech USB Headset Analog Mono')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:98304
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=3 'alsa_output.usb-
Microsoft_Microsoft_LifeChat_LX-6000-00-LX6000.analog-stereo.monitor' 'Monitor of Microsoft
LifeChat LX-6000 Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:65536
```

如果选定设备的任何源音频级别均不符合脉冲音频标准、源未设置为 100% (0dB) 或选定源设备已静音，则会显示如下所示的警告：

```
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel volume: 0: 67%
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel is muted
```

- 3 复制设备的描述并使用它在 `/etc/vmware/config` 文件中设置相应的属性。

以网络摄像头为例，可通过复制 Microsoft® LifeCam HD-6000 for Notebooks 和 Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6 将 Microsoft 网络摄像头指定为首选的网络摄像头，并按如下方法设置属性：

```
rtav.srcWCamName = "Microsoft® LifeCam HD-6000 for Notebooks"
rtav.srcWCamId = "Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6"
```

在此例中，您也可以将 `rtav.srcWCamId` 属性设置为 "Microsoft"。`rtav.srcWCamId` 属性支持部分匹配和完全匹配。`rtav.srcWCamName` 属性仅支持完全匹配。

对于音频设备示例，复制 Logitech USB Headset Analog Mono，以将 Logitech 耳机指定为首选音频设备，并按照如下所示设置属性：

```
rtav.srcAudioInId="Logitech USB Headset Analog Mono"
```

- 4 保存所做的更改，并关闭 `/etc/vmware/config` 配置文件。

- 5 注销桌面会话并启动新会话。

## 配置实时音频-视频组策略设置

您可以在远程桌面上对控制实时音频-视频 (Real-Time Audio-Video, RTAV) 行为的组策略设置进行配置。这些设置确定了虚拟网络摄像头的最大帧速率和图像分辨率。通过这些设置，您可以管理任何用户所能使用的带宽上限。可通过其他设置禁用或启用 RTAV 功能。

您无需配置这些策略设置。实时音频-视频功能可使用客户端系统上为网络摄像头设置的帧速率和图像分辨率。建议为大部分网络摄像头和音频应用程序使用默认设置。

有关实时音频-视频过程中使用的带宽示例，请参阅[实时音频-视频带宽](#)。

这些策略设置将会影响您的远程桌面，而不会影响物理设备所连接的客户端系统。要在桌面上配置这些设置，请在 Active Directory 中添加 RTAV 组策略管理模板 (ADMX) 文件。

有关在客户端系统上配置设置的信息，请参阅 VMware 知识库文章《在 Horizon View Client 上为实时音频-视频设置帧速率和分辨率》，网址为 <http://kb.vmware.com/kb/2053644>。



## 将 RTAV ADMX 模板添加到 Active Directory 并配置设置

您可以将 RTAV ADMX 文件 (vdm\_agent\_rtav.admx) 中的策略设置添加到 Active Directory 中的组策略对象 (Group Policy Object, GPO)，并在组策略对象编辑器中配置设置。

### 前提条件

- 确认您的虚拟机桌面和 RDS 主机上安装了 RTAV 安装选项。默认情况下会安装该设置选项，但您可以在安装期间取消选择它。如果未安装 RTAV，则设置无效。请参阅您的设置文档以了解有关安装 Horizon Agent 的信息。
- 验证已经为 RTAV 组策略设置创建了 Active Directory GPO。这些 GPO 必须链接到包含虚拟机桌面或 RDS 主机的 OU。请参阅 [Active Directory 组策略示例](#)。
- 确认 Microsoft MMC 和组策略对象编辑器插件在您的 Active Directory 服务器上可用。
- 熟悉 RTAV 组策略设置。请参阅[实时音频-视频组策略设置](#)。

### 步骤

- 1 从 VMware 下载站点中下载 Horizon 7 GPO 捆绑包 .zip 文件，网址为 <https://my.vmware.com/web/vmware/downloads>。

在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 GPO 捆绑包。

该文件名为 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip，其中 x.x.x 是版本号，yyyyyyy 是内部版本号。为 Horizon 7 提供组策略设置的所有 ADMX 文件均在此文件中提供。

- 2 解压缩 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 文件，并将 ADMX 文件复制到 Active Directory 服务器。
  - a 将 vdm\_agent\_rtav.admx 文件和 en-US 文件夹复制到 Active Directory 服务器上的 C:\Windows\PolicyDefinitions 文件夹。
  - b （可选）将语言资源文件 (vdm\_agent\_rtav.adml) 复制到 Active Directory 服务器上 C:\Windows\PolicyDefinitions\ 中的相应子文件夹。
- 3 在 Active Directory 服务器上，打开组策略管理编辑器并在该编辑器中输入模板文件的路径。

设置位于 **计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > View RTAV 配置** 文件夹中。

### 后续步骤

配置组策略设置。

## 实时音频-视频组策略设置

实时音频-视频 (RTAV) 组策略设置控制虚拟网络摄像头的最大帧速和最大图像分辨率。可通过其他设置禁用或启用 RTAV 功能。这些策略设置影响远程桌面，而不影响连接物理设备的客户端系统。

如果您未配置 RTAV 组策略设置，RTAV 使用客户端系统上设置的值。在客户端系统上，默认的网络摄像头帧速是每秒 15 帧。默认的网络摄像头图像分辨率是 320x240 像素。



分辨率组策略设置确定可以使用的最大值。客户端系统上设置的帧速和分辨率是绝对值。例如，如果将 RTAV 设置的最大图像分辨率配置为 640x480 像素，网络摄像头会将客户端上设置的任何分辨率显示为最高 640x480 像素。如果将客户端上的图像分辨率设置为高于 640x480 像素的值，客户端分辨率将最高显示 640x480 像素。

不是所有配置都可以达到最大组策略设置 1920x1080 分辨率（25 帧/秒）。针对给定分辨率您的配置可以达到的最大帧速取决于所使用的网络摄像头、客户端系统硬件、Horizon Agent 虚拟硬件以及可用的带宽。

分辨率组策略设置确定在用户未设置分辨率值时使用的默认值。

| 组策略设置   | 说明  |
|---|---|
| Disable RTAV  | <p>启用此设置时，会禁用实时音频-视频功能。</p> <p>未配置或禁用此设置时，会启用实时音频-视频。</p> <p>该设置位于组策略管理编辑器的 <b>VMware View Agent 配置 &gt; View RTAV 配置</b> 文件夹中。</p>   |
| Max frames per second                                 | <p>确定网络摄像头可以捕捉帧的每秒最大速率。您可以使用此设置限制低带宽网络环境中的网络摄像头帧速。最小值是每秒 1 帧。最大值是每秒 25 帧。</p> <p>未配置或禁用此设置时，不会设置最大帧速。实时音频-视频使用为客户端系统上的网络摄像头选择的帧速。</p> <p>默认情况下，客户端网络摄像头的帧速为每秒 15 帧。如果客户端系统上未配置设置且未配置或禁用<b>每秒最大帧数</b>设置，则网络摄像头每秒捕捉 15 帧。</p> <p>该设置位于组策略管理编辑器的 <b>VMware View Agent 配置 &gt; View RTAV 配置 &gt; View RTAV 网络摄像头设置</b> 文件夹中。</p>                |
| Resolution – Max image width in pixels                | <p>确定网络摄像头捕捉的图像帧的最大像素宽度。通过设置较低的最大图像宽度，您可以降低捕捉的帧的分辨率，这样可以改善低带宽网络环境中的图像处理体验。</p> <p>未配置或禁用此设置时，不会设置最大图像宽度。RTAV 使用客户端系统上设置的图像宽度。客户端系统上网络摄像头图像的默认宽度为 320 像素。</p> <p>任何网络摄像头图像的最大限制是 1920x1080 像素。如果将此设置配置为高于 1920 像素的值，则有效最大图像宽度为 1920 像素。</p> <p>该设置位于组策略管理编辑器的 <b>VMware View Agent 配置 &gt; View RTAV 配置 &gt; View RTAV 网络摄像头设置</b> 文件夹中。</p> |
| Resolution – Max image height in pixels               | <p>确定网络摄像头捕捉的图像帧的最大像素高度。通过设置较低的最大图像高度，您可以降低捕捉的帧的分辨率，这样可以改善低带宽网络环境中的图像处理体验。</p> <p>未配置或禁用此设置时，不会设置最大图像高度。RTAV 使用客户端系统上设置的图像高度。客户端系统上网络摄像头图像的默认高度为 240 像素。</p> <p>任何网络摄像头图像的最大限制是 1920x1080 像素。如果将此设置配置为高于 1080 像素的值，则有效最大图像高度为 1080 像素。</p> <p>该设置位于组策略管理编辑器的 <b>VMware View Agent 配置 &gt; View RTAV 配置 &gt; View RTAV 网络摄像头设置</b> 文件夹中。</p> |
| Resolution – Default image resolution width in pixels | <p>确定网络摄像头捕捉的图像帧的默认分辨率像素宽度。用户未定义任何分辨率值时使用此设置。</p> <p>未配置或禁用此设置时，默认映像宽度为 320 像素。</p> <p>仅当使用 View Agent 6.0 或更高版本以及 Horizon Client 3.0 或更高版本时，此策略设置配置的值才生效。对于 View Agent 和 Horizon Client 的较旧版本，此策略设置没有影响，默认映像宽度为 320 像素。</p> <p>该设置位于组策略管理编辑器的 <b>VMware View Agent 配置 &gt; View RTAV 配置 &gt; View RTAV 网络摄像头设置</b> 文件夹中。</p>               |

| 组策略设置  | 说明  |
|--|---|
| Resolution – Default image resolution height in pixels | <p>确定网络摄像头捕捉的图像帧的默认分辨率像素高度。用户未定义任何分辨率值时使用此设置。</p> <p>未配置或禁用此设置时，默认映像高度为 240 像素。</p> <p>仅当使用 View Agent 6.0 或更高版本以及 Horizon Client 3.0 或更高版本时，此策略设置配置的值才生效。对于 View Agent 和 Horizon Client 的较旧版本，此策略设置没有影响，默认映像高度为 240 像素。</p> <p>该设置位于组策略管理编辑器的 <b>VMware View Agent 配置 &gt; View RTAV 配置 &gt; View RTAV 网络摄像头设置</b> 文件夹中。</p> |

## 实时音频-视频带宽

实时音频-视频带宽根据网络摄像头的图像分辨率和帧速，以及被捕获的图像和音频数据的不同而有所差异。

表 2-3. 从 Horizon Client 向 Horizon Agent 发送实时音频-视频数据的带宽结果示例中展示的测试示例评估了实时音频-视频在 Horizon 7 环境中使用标准网络摄像头和音频输入设备所需的带宽。这些测试评估了从 Horizon Client 向 Horizon Agent 发送视频和音频数据所需的带宽。通过 Horizon Client 运行桌面会话所需的带宽总量可能高于这些数据。在以上测试中，网络摄像头以每秒 15 帧的图像分辨率捕获图像。

**表 2-3. 从 Horizon Client 向 Horizon Agent 发送实时音频-视频数据的带宽结果示例**

| 图像分辨率 (宽 x 高) | 所用带宽 (Kbps) |
|---------------|-------------|
| 160 x 120     | 225         |
| 320 x 240     | 320         |
| 640 x 480     | 600         |

## 配置扫描仪重定向

使用扫描仪重定向功能，最终用户可以通过与客户端计算机本地连接的扫描和图像处理设备扫描其远程桌面和应用程序中的信息。

扫描仪重定向支持与 TWAIN 和 WIA 格式以及 Linux 客户端上的 SANE 兼容的标准扫描和图像处理设备。

使用扫描仪重定向安装选项安装 Horizon Agent 后，无需进一步配置，此功能即可在远程桌面和应用程序中使用。您不需要在远程桌面或应用程序中配置特定于扫描仪的驱动程序。

您可以通过配置组策略设置更改默认值来满足特定扫描和图像处理应用程序或环境的要求。也可以设置策略以禁用或启用该功能。利用 ADMX 模板文件，您可以在 Active Directory 服务器上或单个桌面上安装扫描仪重定向组策略设置。请参阅[配置扫描仪重定向组策略设置](#)。

当扫描数据重定向到远程桌面或应用程序时，您将无法访问本地计算机上的扫描或图像处理设备。与之相反，如果在本地计算机上使用此类设备，您将无法访问远程桌面或应用程序中的该设备。

## 扫描仪重定向的系统要求

要支持扫描仪重定向，Horizon 7 部署必须满足特定的软件和硬件要求。

|               |  |
|---------------|--|
| 远程桌面或已发布的应用程序 | RDS 主机上的已发布桌面和已发布应用程序以及部署在单用户虚拟机上的虚拟桌面支持此功能。 |
|---------------|--|

您必须在父虚拟机或模板虚拟机或 RDS 主机上安装 View Agent 6.0.2 或更高版本或者 Horizon Agent 7.0 或更高版本，并且必须选择扫描仪重定向安装选项。

在 Windows 桌面和 Windows Server 客户机操作系统上，默认将取消选中 Horizon Agent 扫描仪重定向安装选项。

以下客户机操作系统在单用户虚拟机和特别注明的 RDS 主机上受支持：

- 32 位或 64 位 Windows 7
- 32 位或 64 位 Windows 8.x
- 32 位或 64 位 Windows 10
- 配置为桌面或 RDS 主机的 Windows Server 2008 R2
- 配置为桌面或 RDS 主机的 Windows Server 2012 R2

---

**重要事项** Windows Server 客户机操作系统上必须安装桌面体验功能，无论将这些系统配置为桌面还是 RDS 主机。

---

无需在安装了 Horizon Agent 的桌面操作系统上安装扫描仪设备驱动程序。

#### Horizon Client 软件

适用于 Windows 的 Horizon Client 3.2 或更高版本

#### Horizon Client 计算机或 客户端访问设备

支持的操作系统：

- 32 位或 64 位 Windows 7
- 32 位或 64 位 Windows 8.x
- 32 位或 64 位 Windows 10

必须安装扫描仪设备驱动程序，且扫描仪在客户端计算机中必须可操作。

#### 扫描设备标准

TWAIN 或 WIA

#### 显示协议

PCoIP

VMware Blast（需要使用 Horizon Agent 7.0 或更高版本）

RDP 桌面会话不支持扫描仪重定向。

## 扫描仪重定向的用户操作

借助扫描仪重定向，用户可以操作作为虚拟设备连接到客户端计算机的物理扫描仪和图像处理设备，从而在远程桌面和应用程序中执行扫描操作。

用户操作虚拟扫描仪的方式与使用本地连接的客户端计算机上的扫描仪类似。

- 在随 Horizon Agent 一起安装“扫描仪重定向”选项后，桌面上会添加一个扫描仪工具托盘图标 (🖨️)。在已发布的应用程序上，工具托盘图标将重定向到本地客户端计算机。

您无需使用扫描仪工具托盘图标。扫描仪重定向无需更多配置即可正常运行。您可以使用此图标配置选项，例如，多个设备连接到客户端计算机时，可以更改要使用的设备。

- 单击扫描仪图标后，将显示“VMware Horizon 扫描仪重定向”菜单。如果客户端计算机连接了不兼容的扫描仪，菜单列表中不会显示任何扫描仪。
- 默认情况下，系统会自动选择扫描设备。TWAIN 和 WIA 扫描仪单独进行选择。可同时选择一台 TWAIN 扫描仪和一台 WIA 扫描仪。
- 如果配置了多台本地连接的扫描仪，可选择与默认选择不同的扫描仪。
- WIA 扫描仪显示在远程桌面的“设备管理器”菜单中**图像处理设备**下面。WIA 扫描仪的名称为**VMware 虚拟 WIA 扫描仪**。
- 在“VMware Horizon 扫描仪重定向”菜单中，可以单击**首选项**选项并选择选项，例如，隐藏扫描仪重定向菜单的网络摄像头和确定如何选择默认扫描仪。

您还可以通过配置 Active Directory 中的扫描仪重定向组策略设置来控制这些功能。请参阅[扫描仪重定向组策略设置](#)。

- 操作 TWAIN 扫描仪时，“VMware Horizon 的 TWAIN 扫描仪重定向”菜单会提供其他选项，用于选择图像区域、彩色扫描、黑白扫描或灰度模式和选择其他常用功能。
- 要显示默认不显示窗口的 TWAIN 扫描软件的 TWAIN 用户界面窗口，可以在“VMware Horizon 扫描仪重定向首选项”对话框中选择**始终显示扫描仪设置对话框**选项。

请注意，大多数 TWAIN 扫描软件默认显示 TWAIN 用户界面窗口。对于此软件，无论您选择或取消选择**始终显示扫描仪设置对话框**选项，系统将始终显示此窗口。

---

**注** 如果运行两个托管于不同场的已发布应用程序，客户端计算机上会显示两个扫描仪重定向工具托盘图标。通常，只有一台扫描仪连接到客户端计算机。在这种情况下，两个图标均操作同一设备，选择哪个图标都不会影响最终结果。在某些情况下，您可能连接了两台本地扫描仪，并且在不同场上运行两个已发布应用程序。在这种情况下，您必须打开每个图标，以查看每个扫描仪重定向菜单所控制的已发布应用程序。

---

有关操作重定向扫描仪的最终用户说明，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。

## 配置扫描仪重定向组策略设置

您可以对控制远程桌面和应用程序中扫描仪重定向行为的组策略设置进行配置。借助这些策略设置，您可以从 Active Directory 集中控制用户的桌面和应用程序上 VMware Horizon 扫描仪重定向“首选项”对话框中可用的选项。

您无需配置这些策略设置。扫描仪重定向使用为远程桌面和客户端系统上的扫描设备配置的默认设置。

这些策略设置影响远程桌面和应用程序，而不影响已连接物理扫描仪的客户端系统。要在桌面和应用程序上配置这些设置，请在 Active Directory 中添加扫描仪重定向组策略管理模板 (ADMX) 文件。

## 将扫描仪重定向 ADMX 模板添加到 Active Directory

您可以将扫描仪重定向 ADMX 模板文件 (vdm\_agent\_scanner.admx) 中的策略设置添加到 Active Directory 中的组策略对象 (Group Policy Object, GPO)，并在组策略对象编辑器中配置设置。

### 前提条件

- 确认您的虚拟机桌面或 RDS 主机上安装了扫描仪重定向安装选项。如果未安装扫描仪重定向，则组策略设置无效。请参阅您的设置文档以了解有关安装 Horizon Agent 的信息。
- 验证已经为扫描仪重定向组策略设置创建了 Active Directory GPO。这些 GPO 必须链接到包含虚拟桌面或 RDS 主机的 OU。请参阅 [Active Directory 组策略示例](#)。
- 确认 MMC 和组策略对象编辑器插件在您的 Active Directory 服务器上可用。
- 熟悉扫描仪重定向组策略设置。请参阅[扫描仪重定向组策略设置](#)。

### 步骤

- 1 从 VMware 下载站点中下载 Horizon 7 GPO 捆绑包 .zip 文件，网址为 <https://my.vmware.com/web/vmware/downloads>。

在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 GPO 捆绑包。

该文件名为 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip，其中 x.x.x 是版本号，yyyyyyy 是内部版本号。为 Horizon 7 提供组策略设置的所有 ADMX 文件均在此文件中提供。

- 2 解压缩 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 文件，并将 ADMX 文件复制到 Active Directory 服务器。

- a 将 vdm\_agent\_scanner.admx 文件和 en-US 文件夹复制到 Active Directory 服务器上的 C:\Windows\PolicyDefinitions 文件夹。

- b （可选）将语言资源文件 (vdm\_agent\_scanner.adml) 复制到 Active Directory 服务器上 C:\Windows\PolicyDefinitions\ 中的相应子文件夹。

- 3 在 Active Directory 服务器上，打开组策略管理编辑器并在该编辑器中输入模板文件的路径。

设置位于 **计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > 扫描仪重定向** 文件夹中。

大多数设置还会被添加到 **用户配置** 文件夹，这些设置位于 **用户配置 > 策略 > 管理模板 > VMware View Agent 配置 > 扫描仪重定向** 文件夹中。

### 后续步骤

配置组策略设置。

## 扫描仪重定向组策略设置

扫描仪重定向组策略设置控制用户桌面和应用程序上的“VMware Horizon 扫描仪重定向首选项”对话框中可用的选项。

扫描仪重定向 ADMX 模板文件同时包含计算机配置策略和用户配置策略。借助用户配置策略，您可以针对虚拟桌面、已发布桌面和已发布应用程序的用户设置不同的配置。即使用户的桌面会话和应用程序在相同的 RDS 主机上运行，不同的用户配置策略也能生效。所有设置位于组策略管理编辑器的 **VMware Horizon Agent 配置 > 扫描仪重定向** 文件夹中。

**表 2-4. 扫描仪重定向策略设置**

| 设置                    | 计算机 | 用户 | 说明   |
|-----------------------|-----|----|--|
| Default Color Mode    |     |    | 如果启用，您可以配置默认颜色模式：黑白、灰度或彩色。在 Windows XP Professional 或 Windows Server 2003 或更高版本上支持该设置。   |
| Default Duplex        |     |    | 如果启用，您可以配置默认扫描模式：单面或双面。在双面模式下，扫描应用程序必须支持双面扫描并从扫描仪中请求两个页面。在 Windows XP Professional 或 Windows Server 2003 或更高版本上支持该设置。  |
| Default Scanner       | X   | X  | <p>提供扫描仪自动选择的集中管理。</p> <p>可为 TWAIN 和 WIA 扫描仪分别选择扫描仪自动选择选项。您可以选择以下自动选择选项：</p> <ul style="list-style-type: none"> <li>■ <b>无。</b>不自动选择扫描仪。</li> <li>■ <b>自动选择：</b>自动选择本地连接的扫描仪。</li> <li>■ <b>上次使用的扫描仪：</b>自动选择上次使用的扫描仪。</li> <li>■ <b>指定扫描仪：</b>选择您在<b>指定扫描仪</b>文本框中键入的扫描仪名称。</li> </ul> <p>当您将该设置作为计算机配置策略启用时，该设置将为所有受影响计算机用户确定扫描仪自动选择模式。用户无法在“VMware Horizon 扫描仪重定向首选项”对话框中更改<b>默认扫描仪</b>选项。</p> <p>当您将该设置作为用户配置策略启用时，该设置将为所有受影响用户确定扫描仪自动选择模式。但是，用户可以在“VMware Horizon 扫描仪重定向首选项”对话框中更改<b>默认扫描仪</b>选项。</p> <p>当您同时在计算机配置和用户配置中启用该设置时，计算机配置中的扫描仪自动选择模式将覆盖所有受影响计算机用户的用户配置中的相应策略设置。</p> <p>当您在任一策略配置中禁用该设置或不对其进行配置时，扫描仪自动选择模式由相应的策略设置（用户配置或计算机配置）决定，或由用户在“VMware Horizon 扫描仪重定向首选项”对话框中选择的选项决定。</p> |
| Disable functionality | X   |    | <p>禁用扫描仪重定向功能。</p> <p>启用该设置后，扫描仪无法重定向，并且不会在用户桌面和应用程序的扫描仪菜单中显示。</p> <p>禁用该设置或不对其进行配置时，扫描仪重定向可正常使用，并且扫描仪会在扫描仪菜单中显示。</p>  |



| 设置          | 计算机 | 用户 | 说明   |
|-------------|-----|----|--|
| Hide Webcam | X   | X  | <p>防止网络摄像头在“VMware Horizon 扫描仪重定向首选项”对话框中的扫描仪选择菜单中显示。</p> <p>在默认情况下，网络摄像头可重新定向到桌面和应用程序。用户可以选择网络摄像头，并将其用作虚拟扫描仪来捕获图像。</p> <p>当您将该设置作为计算机配置策略启用时，网络摄像头将对所有受影响计算机用户隐藏。用户无法在“VMware Horizon 扫描仪重定向首选项”对话框中更改<b>隐藏网络摄像头</b>选项。</p> <p>当您将该设置作为用户配置策略启用时，网络摄像头将对所有受影响用户隐藏。但是，用户可以在“VMware Horizon 扫描仪重定向首选项”对话框中更改<b>隐藏网络摄像头</b>选项。</p> <p>当您同时在计算机配置和用户配置中启用该设置时，计算机配置中的<b>隐藏网络摄像头</b>设置将覆盖所有受影响计算机用户的用户配置中的相应策略设置。</p> <p>当您在任一策略配置中禁用该设置或不对其进行配置时，<b>隐藏网络摄像头</b>设置由相应的策略设置（用户配置或计算机配置）决定，或由用户在“VMware Horizon 扫描仪重定向首选项”对话框中选择的选项决定。</p> |
| Lock config | X   |    | <p>锁定扫描仪重定向用户界面，以防止用户更改其桌面和应用程序上的配置选项。</p> <p>启用该设置后，用户将无法配置其桌面和应用程序上托盘菜单中的可用选项。用户可显示“VMware Horizon 扫描仪重定向首选项”对话框，但其中的选项处于非活动状态，无法对其进行更改。</p> <p>禁用该设置或不对其进行配置时，用户可以配置“VMware Horizon 扫描仪重定向首选项”对话框中的选项。</p>  |

## 配置串行端口重定向

使用串行端口重定向，用户可以重定向本地连接的串行 (COM) 端口，例如内置 RS232 端口或 USB 到串口适配器。诸如打印机、条形码读取器之类的设备以及其他串行设备，可以连接到这些端口并用于远程桌面和已发布的应用程序。

在您安装 Horizon Agent 并设置串行端口重定向功能后，此功能即可用于远程桌面和已发布的应用程序，无需进一步配置。例如，本地客户端系统上的 COM1 将重定向为远程桌面上的 COM1，而 COM2 将重定向为 COM2，除非远程桌面上已存在某个 COM 端口。如果出现这种情况，将映射该 COM 端口以避免冲突。例如，如果远程桌面上已存在 COM1 和 COM2，那么默认情况下，客户端上的 COM1 将映射到 COM3。您不必在远程桌面上配置 COM 端口或安装设备驱动程序。

要激活重定向的 COM 端口，用户可以在桌面会话期间从串行端口工具托盘图标上的菜单中选择**连接**选项。用户还可以将 COM 端口设备设置为只要用户登录远程桌面或已发布的应用程序就自动连接。请参阅[串行端口重定向的用户操作](#)。

您可以配置用于更改默认配置的组策略设置。例如，您可以锁定这些设置，以使用户无法更改 COM 端口映射或属性。也可以设置策略以禁用或启用该功能。利用 ADMX 模板文件，您可以在 Active Directory 中或单个计算机上安装串行端口重定向组策略设置。请参阅[配置串行端口重定向组策略设置](#)。

如果重定向的 COM 端口处于打开状态，并且正在远程桌面或已发布的应用程序上使用，您将无法在本地计算机上访问该端口。相反，如果 COM 端口正在本地计算机上使用，则您无法在远程桌面或已发布的应用程序上访问该端口。

## 串行端口重定向的系统要求

通过使用串行端口重定向功能，最终用户可以将本地连接的串行 (COM) 端口（例如，内置 RS232 端口或 USB 到串口适配器）重定向到其远程桌面和发布的应用程序。要支持串行端口重定向，您的 Horizon 部署必须满足特定的软件和硬件要求。

### 虚拟桌面

虚拟桌面（单会话虚拟机）必须安装 View Agent 6.2.x 或更高版本或者 Horizon Agent 7.0 或更高版本，并且安装时必须选择“串行端口重定向”安装选项。默认情况下，此安装选项处于未选中状态。

在虚拟桌面上支持以下操作系统。

- 32 位或 64 位 Windows 7
- 32 位或 64 位 Windows 8.x
- 32 位或 64 位 Windows 10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

不需要在虚拟桌面上安装串行端口设备驱动程序。

### 已发布的桌面和已发布的应用程序

RDS 主机必须在选定“串行端口重定向”安装选项的情况下安装 Horizon Agent 7.6 或更高版本。默认情况下，此安装选项处于未选中状态。

发布的桌面和发布的应用程序支持以下操作系统。

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

不需要在 RDS 主机上安装串行端口设备驱动程序。

### Horizon Client 计算机或客户端访问设备

在 Windows 7、Windows 8.x 和 Windows 10 客户端系统上支持串行端口重定向。必须安装所需的所有串行端口设备驱动程序，并且能够对串行端口进行操作。适用于 Windows 的 Horizon Client 3.4 及更高版本中提供了串行端口重定向功能。

### 显示协议

- PCoIP
- VMware Blast（需要使用 Horizon Agent 7.0 或更高版本）

RDP 桌面会话中不支持串行端口重定向。



## 串行端口重定向的用户操作

用户可以对连接到其客户端计算机的物理 COM 端口设备进行操作，并使用串行端口虚拟化功能将这些设备连接到其远程桌面（其中的第三方应用程序可以访问这些设备）。

- 在随 Horizon Agent 一起安装“串行端口重定向”选项后，远程桌面上会添加一个串行端口工具托盘图标 (🔌)。对于已发布的应用程序，该图标会重定向到本地客户端计算机。

仅当您使用所需版本的 Horizon Agent 和 Horizon Client for Windows，并且通过 PCoIP 连接时，才会显示此图标。如果您从 Mac、Linux 或移动客户端连接到远程桌面，则不会显示此图标。

您可以使用此图标来配置用于对映射的 COM 端口进行连接、断开连接和自定义操作的选项。

- 单击串行端口图标后，将显示 **VMware Horizon 的串行 COM 重定向** 菜单。
- 默认情况下，本地连接的 COM 端口将映射到远程桌面上的对应 COM 端口。例如：**COM1 映射到 COM3**。默认情况下，映射的端口处于未连接状态。
- 要使用映射的 COM 端口，您必须手动在 **VMware Horizon 的串行 COM 重定向** 菜单中选择 **连接** 选项，或者，必须在先前的桌面会话期间或通过配置组策略设置来设置 **Autoconnect** 选项。**Autoconnect** 可将映射的端口配置为在远程桌面会话启动时自动连接。
- 选择 **连接** 选项后，重定向的端口将处于活动状态。在远程桌面上客户机操作系统中的设备管理器内，重定向的端口显示为 **Serial Port Redirector for VMware Horizon (COMn)**。

连接 COM 端口后，您可以在第三方应用程序中打开该端口，并通过第三方应用程序与连接到客户端计算机的 COM 端口设备交换数据。当某个端口在应用程序中打开时，您无法在 **VMware Horizon 的串行 COM 重定向** 菜单中将该端口断开连接。

将 COM 端口断开连接之前，您必须在应用程序中关闭该端口，或关闭应用程序。然后，您可以选择 **断开连接** 选项将端口断开连接，并使物理 COM 端口在客户端计算机可供使用。

- 在 **VMware Horizon 的串行 COM 重定向** 菜单中，您可以右键单击重定向端口以选择 **端口属性** 命令。

在“COM 属性”对话框中，您可以将端口配置为在远程桌面会话启动时自动连接，忽略数据集就绪 (Data Set Ready, DSR) 信号，使端口成为永久端口，并通过在 **自定义端口名称** 下拉菜单中选择端口将客户端上的本地端口映射到远程桌面上的其他 COM 端口。

远程桌面端口可能显示为已重叠。例如，您可能会看到 **COM1 (重叠)**。在此情况下，将使用 ESXi 主机上的虚拟硬件中的 COM 端口来配置虚拟机。甚至在重定向端口映射到虚拟机上重叠的端口时，您仍可以使用此重定向端口。虚拟机通过 ESXi 主机或客户端系统的端口来接收串行数据。

- 在客户机操作系统的设备管理器中，您可以使用 **属性 > 端口设置** 选项卡为重定向 COM 端口配置设置。例如，您可以设置默认的波特率和数据位。但是，如果应用程序指定了端口设置，则您在设备管理器中配置的设置将被忽略。

有关操作重定向串行 COM 端口的最终用户说明，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。

## 有关配置串行端口重定向的准则

通过组策略设置，您可以配置串行端口重定向并控制用户对重定向 COM 端口的自定义程度。您的选择取决于自己所在组织中的用户角色和第三方应用程序。

有关组策略设置的信息，请参阅[串行端口重定向组策略设置](#)。

- 如果您的用户运行相同的第三方应用程序和 COM 端口设备，请确保以相同的方式配置重定向端口。例如，在使用销售点设备的银行或零售店中，请确保所有 COM 端口设备连接到客户端端点上的相同端口，并且所有端口映射到远程桌面上相同的重定向 COM 端口。

设置 **PortSettings** 策略设置，以便将客户端端口映射到重定向端口。选择 **PortSettings** 中的 **Autoconnect** 项以确保在每次桌面会话启动时连接重定向端口。启用 **Lock Configuration** 策略设置以阻止用户更改端口映射或对端口配置进行自定义。在此方案中，用户不必手动连接或断开连接，也不会意外地使第三方应用程序无法访问重定向 COM 端口。

- 如果您的用户是使用各种第三方应用程序的知识工作者，并且还可能在客户端计算机上本地使用 COM 端口，请确保这些用户可以连接到重定向 COM 端口以及从其断开连接。

如果默认的端口映射不正确，您可以设置 **PortSettings** 策略设置。您可以根据自己用户的要求决定是否设置 **Autoconnect** 项。请勿启用 **Lock Configuration** 策略设置。

- 确保您的第三方应用程序会打开映射到远程桌面的 COM 端口。
- 确保用于设备的波特率与第三方应用程序将要尝试使用的波特率匹配。
- 您最多可以将五个 COM 端口从客户端系统重定向至远程桌面。

## 配置串行端口重定向组策略设置

您可以配置组策略设置，以便在远程会话中控制串行端口重定向行为。通过使用这些策略设置，您可以从 Active Directory 中集中控制在远程桌面上的 **VMware Horizon** 的串行 COM 重定向菜单中提供的选项。

您无需配置这些策略设置。串行端口重定向使用在远程会话和客户端系统中为重定向的 COM 端口配置的默认设置。

这些策略设置影响您的远程会话，不影响已连接物理 COM 端口设备的客户端系统。要为远程桌面和发布的应用程序配置这些设置，请在 Active Directory 中添加串行端口重定向组策略管理模板 (ADMX) 文件。

## 将串行端口重定向 ADMX 模板添加到 Active Directory

您可以将 Serial COM（串行端口重定向）ADMX 文件 (vdm\_agent\_serialport.admx) 中的策略设置添加到 Active Directory 中的组策略对象 (GPO)，并在组策略对象编辑器中配置设置。

### 前提条件

- 确认在虚拟桌面或 RDS 主机上安装时选择了“串行端口重定向”安装选项。如果未安装串行端口重定向，组策略设置将无效。有关安装 Horizon Agent 的信息，请参阅《在 Horizon 7 中设置虚拟桌面》或《在 Horizon 7 中设置已发布的桌面和应用程序》文档。
- 确认已经为串行端口重定向组策略设置创建了 Active Directory GPO。这些 GPO 必须链接到包含虚拟桌面或 RDS 主机的 OU。请参阅[Active Directory 组策略示例](#)。

- 确认 MMC 和组策略对象编辑器插件在您的 Active Directory 服务器上可用。
- 熟悉串行端口重定向组策略设置。请参阅[串行端口重定向组策略设置](#)。

## 步骤

- 1 从 VMware 下载站点中下载 Horizon 7 GPO 捆绑包 .zip 文件，网址为 <https://my.vmware.com/web/vmware/downloads>。

在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 GPO 捆绑包。

该文件名为 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`，其中 `x.x.x` 是版本号，`yyyyyyy` 是内部版本号。为 Horizon 7 提供组策略设置的所有 ADMX 文件均在此文件中提供。

- 2 解压缩 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` 文件，并将 ADMX 文件复制到 Active Directory 服务器。

- a 将 `vdm_agent_serialport.admx` 文件和 `en-US` 文件夹复制到 Active Directory 服务器上的 `C:\Windows\PolicyDefinitions` 文件夹。

- b （可选）将语言资源文件 (`vdm_agent_serialport.adml`) 复制到 Active Directory 服务器上 `C:\Windows\PolicyDefinitions\` 中的相应子文件夹。

- 3 在 Active Directory 服务器上，打开组策略管理编辑器并在该编辑器中输入模板文件的路径。

设置位于 **计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > Serial COM** 文件夹中。

大多数设置还会被添加到 **用户配置** 文件夹，这些设置位于 **用户配置 > 策略 > 管理模板 > VMware View Agent 配置 > Serial COM** 中。

## 后续步骤

配置组策略设置。

## 串行端口重定向组策略设置

串行端口重定向组策略设置控制重定向的 COM 端口配置，包括远程桌面上的 **VMware Horizon** 的 **串行 COM 重定向** 菜单中提供的选项。

串行端口重定向 ADMX 文件同时包含计算机配置策略和用户配置策略。用户配置策略允许您为远程桌面的指定用户设置不同的配置。在计算机配置中配置的策略设置优先于在用户配置中配置的相应设置。

表 2-5. 串行端口策略设置

| 设置  | 计算机 | 用户 | 说明  |
|---|-----|----|---|
| PortSettings1<br>PortSettings2<br>PortSettings3<br>PortSettings4<br>PortSettings5 | X   | X  | <p>端口设置确定客户端系统上的 COM 端口与远程桌面上的重定向的 COM 端口之间的映射，并确定影响重定向的 COM 端口的其他设置。您可以分别配置每个重定向 COM 端口。</p> <p>共有五个可用的端口设置策略设置，最多允许将五个 COM 端口从客户端映射到远程桌面。请为要配置的每个 COM 端口选择一个端口设置策略设置。在启用端口设置策略设置时，您可以配置影响重定向的 COM 端口的以下项：</p> <ul style="list-style-type: none"> <li>■ <b>Source port number</b> 设置用于指定连接到客户端系统的物理 COM 端口的编号。</li> <li>■ <b>Destination virtual port number</b> 设置用于指定远程桌面上重定向虚拟 COM 端口的编号。</li> <li>■ <b>Autoconnect</b> 设置用于在每次桌面会话启动时自动将 COM 端口连接到重定向 COM 端口。</li> <li>■ <b>IgnoreDSR</b> 设置用于使重定向 COM 端口设备忽略数据集就绪 (Data Set Ready, DSR) 信号。</li> <li>■ <b>Pause before close port (in milliseconds)</b> 设置用于指定在用户关闭重定向端口之后直到该端口实际关闭之前的等待时间（以毫秒为单位）。某些 USB 到串口适配器需要此延迟以确保传输的数据已被保存。此设置用于故障排除。</li> <li>■ <b>Serial2USBModeChangeEnabled</b> 设置用于解决适用于使用 Prolific 芯片组的 USB 到串口适配器（包括 GlobalSat BU353 GPS 适配器）的问题。如果您没有为 Prolific 芯片组适配器启用此设置，则连接的设备可以传输数据，但无法接收数据。</li> <li>■ <b>Disable errors in wait mask</b> 设置用于禁用 COM 端口掩码中的错误值。某些应用程序需要使用此故障排除设置。有关详细信息，请参阅关于 <code>WaitCommEvent</code> 函数的 Microsoft 文档，网址为 <a href="http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx">http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx</a>。</li> <li>■ <b>HandleBtDisappear</b> 设置支持蓝牙 COM 端口行为。此设置用于故障排除。</li> <li>■ <b>UsbToComTroubleShooting</b> 设置用于解决适用于 USB 到串口适配器的一些问题。此设置用于故障排除。</li> <li>■ <b>永久</b>设置用于保留远程会话中的重定向 COM 端口状态，即使客户端断开连接也是如此。</li> </ul> <p>在为特定的 COM 端口启用端口设置策略设置时，用户可以连接和断开连接重定向的端口，但用户无法在远程桌面上配置该端口的属性。例如，用户无法将此端口设置为在其登录到桌面时自动重定向，并且无法忽略 DSR 信号。这些属性由组策略设置进行控制。</p> <p><b>注</b> 仅当物理 COM 端口在本地连接到客户端系统时，重定向 COM 端口才会连接且处于活动状态。如果您映射的 COM 端口在客户端上并不存在，则重定向端口在远程桌面上的工具托盘菜单中显示为非活动且不可用的状态。</p> <p>如果禁用或未配置端口设置策略设置，则重定向的 COM 端口使用用户在远程桌面上配置的设置。<b>VMware Horizon 的串行 COM 重定向</b>菜单选项处于活动状态且可供用户使用。</p> <p>这些设置位于组策略管理编辑器的 <b>VMware View Agent 配置 &gt; 串行 COM &gt; 端口设置</b>文件夹中。</p> |
| Bandwidth limit   | X   |    | <p>对重定向串行端口与客户端系统之间的数据传输速度（千字节/秒）设置限制。</p> <p>如果启用此设置，则您可以在 <b>Bandwidth limit (in kilobytes per second)</b> 框中设置值，该值确定重定向串行端口与客户端之间的最快数据传输速度。值为 0 将禁用带宽限制。</p> <p>如果禁用此设置，则表示未设置任何带宽限制。</p> <p>如果未配置此设置，则远程桌面上的本地程序设置将确定是否设置带宽限制。</p> <p>该设置位于组策略管理编辑器的 <b>VMware View Agent 配置 &gt; 串行 COM</b> 文件夹中。</p>  |

| 设置                      | 计算机 | 用户 | 说明  |
|-------------------------|-----|----|---|
| Disable functionality   | X   |    | <p>禁用串行端口重定向功能。</p> <p>如果启用此设置，则 COM 端口不会重定向至远程桌面。在远程桌面上不会显示串行端口工具托盘图标。</p> <p>如果禁用此设置，则串行端口重定向将会生效，并会显示串行端口工具托盘图标，而且 COM 端口会显示在 <b>VMware Horizon 的串行 COM 重定向</b> 菜单中。</p> <p>如果未配置此设置，则远程桌面的本地设置将确定禁用还是启用串行端口重定向。该设置位于组策略管理编辑器的 <b>VMware View Agent 配置 &gt; 串行 COM</b> 文件夹中。</p>   |
| Local settings priority | X   | X  | <p>使在远程桌面上配置的设置获得优先权。</p> <p>如果启用此策略，则用户在远程桌面上配置的串行端口重定向设置将优先于组策略设置。仅当远程桌面上未配置设置时，组策略设置才会生效。</p> <p>如果禁用或未配置此设置，则组策略设置将优先于在远程桌面上配置的设置。该设置位于组策略管理编辑器的 <b>VMware View Agent 配置 &gt; 串行 COM</b> 文件夹中。</p>  |
| Lock configuration      | X   | X  | <p>锁定串行端口重定向用户界面并阻止用户更改远程桌面上的配置选项。</p> <p>如果启用此设置，则用户将无法配置其桌面上工具托盘菜单中的可用选项。用户可以显示 <b>VMware Horizon 的串行 COM 重定向</b> 菜单，但选项处于非活动状态并且无法进行更改。</p> <p>如果禁用此设置，则用户可以配置 <b>VMware Horizon 的串行 COM 重定向</b> 菜单中的选项。</p> <p>如果未配置此设置，则远程桌面上的本地程序设置将确定用户是否可以配置 COM 端口重定向设置。</p> <p>该设置位于组策略管理编辑器的 <b>VMware View Agent 配置 &gt; 串行 COM</b> 文件夹中。</p> |

## 配置 USB 到串口适配器

您可以对使用 Prolific 芯片组的 USB 到串口适配器进行配置，使其通过串行端口重定向功能重定向到远程会话。

要确保在 Prolific 芯片组适配器上正确传输数据，您可以在 **Active Directory** 中、在单个虚拟机桌面上或在 RDS 主机上启用串行端口重定向组策略设置。

如果您没有通过配置组策略设置来解决 Prolific 芯片组适配器的问题，则连接的设备可以传输数据，但无法接收数据。

您不必在客户端系统上配置策略设置或注册表项。

### 前提条件

- 确认您的虚拟机桌面或 RDS 主机上安装了串行端口重定向安装选项。如果未安装串行端口重定向，组策略设置将无效。有关安装 Horizon Agent 的信息，请参阅《在 Horizon 7 中设置虚拟桌面》或《在 Horizon 7 中设置已发布的桌面和应用程序》文档。
- 确认已在 **Active Directory** 中添加了串行端口重定向 ADMX 模板文件。
- 熟悉 **PortSettings** 组策略设置中的 **Serial2USBModeChangeEnabled** 项。请参阅[串行端口重定向组策略设置](#)。

## 步骤

- 1 在 Active Directory 服务器上，打开组策略管理对象编辑器。
- 2 导航到**计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > Serial COM** 文件夹。
- 3 选择 **PortSettings** 文件夹。
- 4 选择并启用 **PortSettings** 组策略设置。
- 5 指定用于映射 COM 端口的源和目标 COM 端口号。
- 6 选中 **Serial2USBModeChangeEnabled** 复选框。
- 7 根据需要配置 **PortSettings** 策略设置中的其他项。
- 8 单击**确定**，然后关闭组策略管理对象编辑器。

现在，USB 到串口适配器就可以重定向到远程会话，并且在用户启动其下一个会话时可以成功接收数据。

## 管理对 Windows Media 多媒体重定向 (MMR) 功能的访问

Horizon 7 为在单用户计算机上运行的虚拟桌面和 RDS 主机上的已发布桌面提供了 Windows Media MMR 功能。

MMR 可直接将多媒体流交付给客户端计算机。通过 MMR，多媒体流在客户端系统上进行解码处理。客户端系统播放媒体内容，从而降低了 ESXi 主机上的负载需求。

MMR 数据未经过基于应用程序的加密通过网络发送，其中可能包含敏感数据，具体取决于将重定向的内容。为确保无法在网络上监视此数据，请仅在安全网络中使用 MMR。

如果启用安全加密链路，客户端与 View 安全网关之间的 MMR 连接是安全的，但是从 View 安全网关到桌面计算机的连接未加密。如果禁用安全加密链路，从客户端到桌面计算机的 MMR 连接未加密。

## 启用 Horizon 7 中的多媒体重定向

您可以采取一些步骤确保 MMR 仅可供具有足够资源处理本地多媒体解码以及连接到安全网络上的 Horizon 7 的 Horizon Client 系统访问。

默认情况下，Horizon Administrator 中的全局策略**多媒体重定向 (MMR)** 设置为**拒绝**。

要使用 MMR，您必须明确将此值设置为**允许**。

要控制对 MMR 的访问权限，您可以针对单个桌面池或特定用户全局启用或禁用**多媒体重定向 (MMR)**策略。

有关在 Horizon Administrator 中设置全局策略的说明，请参阅 [Horizon 7 策略](#)。



## Windows Media MMR 的系统要求

要支持 Windows Media 多媒体重定向 (MMR)，Horizon 7 部署必须满足特定的软件和硬件要求。Horizon 6.0.2 及更高版本中提供了 Windows Media MMR。

### 远程桌面

- 在单用户虚拟机上部署的虚拟机桌面上和 RDS 主机上的已发布桌面上支持该功能。

要在已发布桌面上支持该功能，必须安装 View Agent 6.1.1 或更高版本，或者 Horizon Agent 7.0 或更高版本。

要在单用户计算机上支持该功能，必须安装 View Agent 6.0.2 或更高版本，或者 Horizon Agent 7.0 或更高版本。
- 要支持 Microsoft Media Server (MMS) 和实时流协议 (Real Time Streaming Protocol, RTSP)，必须安装 Horizon 7 7.9。
- 以下是支持的客户端操作系统：
  - 64 位或 32 位 Windows 10。支持 Windows Media Player。不支持默认的 TV & Movies 播放器。
  - Windows Server 2016 是一项技术预览版功能。支持 Windows Media Player。不支持默认的 TV & Movies 播放器。
  - 64 位或 32 位 Windows 7 SP1 企业版或旗舰版（单用户计算机）。不支持 Windows 7 专业版。
  - 64 位或 32 位 Windows 8/8.1 专业版或企业版（单用户计算机）
  - 配置为 RDS 主机的 Windows Server 2008 R2
  - 配置为 RDS 主机的 Windows Server 2012 和 2012 R2
- 可在桌面池上启用或禁用 3D 呈现。
- 用户必须使用 Windows Media Player 12（或更高版本）或者 Internet Explorer 8（或更高版本）播放视频。

### Horizon Client 软件

要在单用户计算机上支持 Windows Media MMR，必须安装 Horizon Client for Windows 3.2 或更高版本。

### Horizon Client 计算机或客户端访问设备

客户端必须运行 64 位或 32 位 Windows 7、Windows 8/8.1 或 Windows 10 操作系统。

### 支持的媒体格式

Windows Media Player 支持的媒体格式，例如：M4V；MOV；MP4；WMP；MPEG-4 Part 2；WMV 7、8 和 9；WMA；AVI；ACE；MP3；WAV。

Horizon 7 7.9 支持 MMS 和 RTSP。

---

**注** 将不通过 Windows Media MMR 重定向 DRM 保护的内容。

---

- Horizon 策略** 在 Horizon Administrator 中，将**多媒体重定向 (MMR)** 策略设置为**允许**。默认值为**拒绝**。
- 后端防火墙** 如果 Horizon 7 部署在基于 DMZ 的安装服务器与内部网络之间配置了后台防火墙，则验证该防火墙是否允许将流量传输到桌面上的端口 **9427**。

## 确定是否基于网络延迟使用 Windows Media MMR

默认情况下，Windows Media MMR 会适应单用户桌面（运行于 Windows 8 或更高版本上）和已发布桌面（运行于 Windows Server 2012、2012 R2 或更高版本上）上的网络条件。如果 Horizon Client 与远程桌面之间的网络延迟为 29 毫秒或更少，则将使用 Windows Media MMR 重定向视频。如果网络延迟为 30 毫秒或更多，则不会重定向视频。相反，会在 ESXi 主机上将其呈现出来，并会通过 PCoIP 将其发送到客户端。

此功能适用于 Windows 8 或更高版本的单用户桌面，以及 Windows Server 2012、2012 R2 或更高版本的已发布桌面。用户可以运行任何受支持的客户端系统（Windows 7 或 Windows 8/8.1）。

此功能不适用于 Windows 7 单用户桌面或 Windows Server 2008 R2 已发布的桌面。在这些客户机操作系统上，无论网络延迟为多少，Windows Media MMR 将始终执行多媒体重定向。

通过在桌面上配置 **RedirectionPolicy** 注册表设置，您可以覆盖此功能，从而强制 Windows Media MMR 执行多媒体重定向，而不管网络延迟为多少。

### 步骤

- 1 启动远程桌面上的 Windows 注册表编辑器。
- 2 导航至控制重定向策略的 Windows 注册表项。

您为远程桌面配置的注册表项取决于 Windows Media Player 的位版本。

| 选项                               | 说明   |
|----------------------------------|--|
| <b>64 位 Windows Media Player</b> | <ul style="list-style-type: none"> <li>■ 对于 64 位桌面，使用以下注册表项：HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr</li> </ul>  |
| <b>32 位 Windows Media Player</b> | <ul style="list-style-type: none"> <li>■ 对于 32 位桌面，使用以下注册表项：HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr</li> <li>■ 对于 64 位桌面，使用以下注册表项：HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware tsmmr</li> </ul> |

- 3 将 **RedirectionPolicy** 值设置为 **always**。

```
Value name = RedirectionPolicy
Value Type = REG_SZ
Value data = always
```

- 4 在桌面上重新启动 Windows Media Player，以使更新的值生效。



## 管理对客户端驱动器重定向的访问

在通过客户端驱动器重定向部署 Horizon Client 和 Horizon Agent 时，文件夹和文件会以加密的方式通过网络进行发送。

客户端和 View 安全网关之间的客户端驱动器重定向连接以及从 View 安全网关到桌面计算机的连接是安全的。如果启用了 VMware Blast，文件和文件夹会以加密的方式通过虚拟通道进行传输。

需要通过端口 9427 进行 TCP 连接来支持客户端驱动器重定向。如果 Horizon 7 部署在基于 DMZ 的安全服务器与内部网络之间配置了后端防火墙，该后端防火墙必须允许将流量传输到远程桌面上的端口 9427。如果启用了 VMware Blast，则无需打开 TCP 端口 9427，因为客户端驱动器重定向将通过虚拟通道传输数据。

默认情况下，Horizon Agent 安装程序中的**客户端驱动器重定向**自定义安装选项将处于选定状态。最佳做法是，仅在用户需要此功能的远程桌面中启用**客户端驱动器重定向**自定义安装选项。

在版本低于 3.5 的 Horizon Client 或版本低于 6.2 的 Horizon Agent 中，客户端驱动器重定向文件夹和文件会以未加密的方式通过网络进行发送，并且可能包含敏感数据，具体取决于重定向的内容。如果启用安全加密链路，Horizon Client 和 View 安全网关之间的客户端驱动器重定向连接是安全的，但是从 View 安全网关到桌面计算机的连接未加密。如果禁用安全加密链路，则不会对从 Horizon Client 到桌面计算机的客户端驱动器重定向连接进行加密。对于较低的客户端和代理版本，为确保此数据不会在网络上受到监视，请仅在安全的网络上使用客户端驱动器重定向。

在 Horizon Agent 7.7 或更高版本上启用客户端驱动器重定向后，您便可以在 Horizon Client 4.10 或更高版本与远程桌面及已发布的应用程序之间拖放文件和文件夹。请参阅[配置拖放功能](#)。

## 在 Unified Access Gateway 实施中使用客户端驱动器重定向

如果您的 Horizon 7 实施使用 Unified Access Gateway 设备而不使用安全服务器，用户将客户端驱动器重定向与 PCoIP 显示协议一起使用，并且 Horizon Client 和 Horizon Agent 计算机位于不同的网络上，则必须为 Unified Access Gateway 设备启用 UDP 隧道服务器。

要启用 UDP 隧道服务器，请在 Unified Access Gateway 管理 UI 中，将 **UDP 隧道服务器已启用** 设置设置为是。

如果不启用 UDP 隧道服务器，用户便无法将客户端驱动器重定向功能与 PCoIP 显示协议一起使用。无论是否启用 UDP 隧道服务器，客户端驱动器重定向都可以与 VMware Blast 显示协议一起使用。

有关更多信息，请参阅 Unified Access Gateway 文档。

## 使用组策略禁用客户端驱动器重定向

您可以通过在 Active Directory 服务器上为远程桌面配置组策略设置来禁用客户端驱动器重定向。

组策略设置会覆盖用于启用客户端驱动器重定向功能的本地注册表和智能策略设置。

### 前提条件

- 确认您能够以管理员域用户的身份登录到托管 Active Directory 服务器的计算机。
- 确认 MMC 和组策略对象编辑器插件在您的 Active Directory 服务器上可用。

- 将远程桌面服务 ADMX 模板文件 `vmware_rdsh_server.admx` 添加到与虚拟桌面的 OU 或已发布桌面的 RDS 主机链接的 GPO。有关安装说明，请参阅[将 ADMX 模板文件添加到 Active Directory](#)。

#### 步骤

- 1 在 Active Directory 服务器上，打开组策略管理编辑器，并导航到**计算机配置\策略\管理模板\Windows 组件\远程桌面服务\远程桌面会话主机\设备和资源重定向**。
- 2 打开**不允许驱动器重定向**组策略设置，选择**已启用**，然后单击**确定**。

## 使用组策略配置驱动器盘符行为

您可以使用代理组策略设置配置使用客户端驱动器重定向功能重定向的驱动器的驱动器盘符行为。

#### 前提条件

- 确认您能够以管理员域用户的身份登录到托管 Active Directory 服务器的计算机。
- 确认 MMC 和组策略对象编辑器插件在您的 Active Directory 服务器上可用。
- 将 VMware Horizon 客户端驱动器重定向 ADMX 模板文件 (`vdm_agent_cdr.admx`) 添加到与虚拟桌面的 OU 或发布的桌面的 RDS 主机链接的 GPO 中。有关安装说明，请参阅[将 ADMX 模板文件添加到 Active Directory](#)。

#### 步骤

- 1 在 Active Directory 服务器上，打开组策略管理编辑器，然后导航到**计算机配置 > 管理模板 > VMware View Agent 配置 > VMware Horizon Client 驱动器重定向**。
- 2 要配置是否显示已重定向的驱动器的驱动器盘符，请配置**显示带驱动器盘符的已重定向设备**组策略设置。

默认情况下启用该设置。

- 3 要指定 Windows 资源管理器初始化和显示重定向的驱动器的驱动器盘符的等待时间（以毫秒为单位），请配置**驱动器盘符配置超时**组策略设置。

如果禁用或未配置该设置，则默认值为 5000 毫秒。

## 使用注册表设置配置客户端驱动器重定向

您可以使用 Windows 注册表项设置来控制远程桌面上的客户端驱动器重定向行为。该功能需要使用 Horizon Agent 7.0 或更高版本以及 Horizon Client 4.0 或更高版本。

位于以下路径中的 Windows 注册表设置可控制远程桌面上的客户端驱动器重定向行为：

```
HKLM\Software\VMware, Inc.\VMware TSDR
```

您可以使用远程桌面上的 Windows 注册表编辑器来编辑本地注册表设置。

---

**注** 使用智能策略设置的客户端驱动器重定向策略优先于本地注册表设置。

---

## 禁用客户端驱动器重定向

要禁用客户端驱动器重定向，请新建一个名为 `disabled` 的字符串值，然后将其值设置为 `true`。

```
HKLM\Software\VMware, Inc.\VMware TSDR\disabled=true
```

该值默认为 `false`（已启用）。

## 禁止对共享文件夹的写入访问权限

要禁止对与远程桌面共享的所有文件夹的写入访问权限，请新建一个名为 `permissions` 的字符串值，然后将其值设置为 `rw` 之外以 `r` 开头的任何字符串。

```
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

该值默认为 `rw`（所有共享文件夹均可读取和写入）。

## 共享特定文件夹

要与远程桌面共享特定文件夹，请新建一个名为 `default shares` 的项，然后为要与远程桌面共享的每个文件夹新建一个子项。对于每个子项，再新建一个名为 `name` 的字符串值，然后将其值设置为要共享的文件夹路径。以下示例共享了文件夹 `C:\ebooks` 和 `C:\spreadsheets`。

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

如果将 `name` 设置为 `*all`，则会与远程桌面共享所有客户端驱动器。仅 Windows 客户端系统支持 `*all` 设置。

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\1st\name=*all
```

要禁止客户端共享其他文件夹（即，不是通过 `default shares` 项指定的文件夹），请创建一个名为 `ForcedByAdmin` 的字符串值，然后将其值设置为 `true`。

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
```

如果该值为 `true`，则当用户在 Horizon Client 中连接到远程桌面时，不会显示“共享”对话框。该值默认为 `false`（客户端可以共享其他文件夹）。

以下示例共享了文件夹 `C:\ebooks` 和 `C:\spreadsheets`，使这两个文件夹只能读取，并禁止客户端共享其他文件夹。

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

---

**注** 请勿将 `ForcedByAdmin` 功能作为一项安全功能或共享控件来使用。用户可以创建现有共享的链接以指向未通过 `default shares` 项指定的文件夹，从而绕过 `ForcedByAdmin=true` 设置。

---

## 配置拖放功能

用户可以在客户端系统与远程桌面和已发布的应用程序之间拖放数据。

### 拖放功能的客户端要求

- 仅支持 Windows 客户端和 Mac 客户端系统。不支持其他类型的客户端系统。
- 用户必须使用 VMware Blast 或 PCoIP 显示协议。
- 要拖放文件和文件夹，必须在适用于 Windows 的 Horizon Client 中启用客户端驱动器重定向功能。
- 要使用最新的拖放功能，用户必须具有适用于 Windows 的 Horizon Client 5.1 或更高版本或者适用于 Mac 的 Horizon Client 5.1 或更高版本。较低版本的客户端仅提供部分拖放功能。

有关在 Windows 客户端上使用拖放功能的信息，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。有关在 Mac 客户端上使用拖放功能的信息，请参阅《适用于 Mac 的 VMware Horizon Client 安装和设置指南》文档。

### 拖放功能的代理要求

要对文件和文件夹使用拖放功能，必须在安装 Horizon Agent 时启用客户端驱动器重定向选项。

### 使用组策略设置配置拖放功能

您可以通过编辑 VMware Blast 和 PCoIP 显示协议的组策略设置来配置拖放方向、允许的拖放格式以及拖放大小限制。请参阅 [VMware Blast 策略设置](#) 和 [PCoIP 剪贴板和拖放设置](#)。

### 使用 User Environment Manager 配置拖放功能

对于 User Environment Manager 9.8 或更高版本以及 Horizon Client 5.1 或更高版本，您可以使用智能策略配置拖放行为，包括完全禁用拖放功能。请参阅 [Horizon 智能策略设置](#)。

## 配置简单设备方向 (SDO) 传感器重定向

简单设备方向 (Simple Device Orientation, SDO) 传感器重定向功能可以感知客户端设备屏幕方向的变化，并相应地在设备上显示不同的视图。

SDO 传感器重定向功能与 Horizon Agent 上的软件应用程序相集成。如果您的应用程序使用 SimpleOrientationSensor 类 <https://docs.microsoft.com/zh-cn/uwp/api/windows.devices.sensors.simpleorientationsensor>，则应用程序可以根据客户端设备的当前象限方向显示内容。

### SDO 传感器重定向的系统要求

支持以下设备：

**表 2-6. 支持 SDO 传感器重定向的设备**

| 设备           | 客户端操作系统                        | Windows 操作系统服务器             | 协议          |
|--------------|--------------------------------|-----------------------------|-------------|
| Surface Book | Windows 10 1709                | Windows 10 1709 (64 位、32 位) | PCoIP、Blast |
| Surface Pro  | Windows 10 1709<br>Windows 8.1 | Windows 10 1709 (64 位、32 位) | PCoIP、Blast |

对于 Horizon Agent 操作系统，只支持 Windows 10 32 位和 64 位。

## 安装 SDO 传感器

SDO 传感器重定向是 Horizon Agent 安装程序中的一个自定义安装选项。默认情况下不选择该选项。您必须选择“SDO 传感器重定向”才会进行安装。有关 SDO 传感器重定向的静默安装属性，请参阅《在 Horizon 7 中设置虚拟桌面》文档。

必须启用本地系统上的传感器服务，SDO 驱动程序才能正常工作。必须在客户端设备上启用 SDO 传感器。

## 日志

SDO 传感器重定向的 Horizon Client 日志将记录在 rdeSvc 日志文件 %TEMP%\vmware-%USERNAME%\vmware-rdeSvc-x-xxxxx.log 中。

SDO 传感器重定向的 Horizon Agent 日志将记录在 rdeSvc 日志文件 C:\Windows\Temp\vmware-SYSTEM\*\vmware-rdeSvc-x-xxxx.log 中。

## 配置会话协作

通过使用会话协作功能，用户可以邀请其他用户加入现有的 Windows 远程桌面会话。要在 Linux 桌面上设置会话协作，请参阅《设置 Horizon 7 for Linux 桌面》文档。

## 会话协作的系统要求

要支持会话协作功能，您的 Horizon 部署必须满足特定要求。

**表 2-7. 会话协作的系统要求**

| 组件           | 要求   |
|--------------|--|
| 客户端系统        | 会话所有者和协作者必须已在客户端系统上安装了适用于 Windows、Mac 或 Linux 的 Horizon Client 4.7 或更高版本，否则，必须使用 HTML Access 4.7 或更高版本。  |
| Windows 远程桌面 | 虚拟桌面或已发布应用程序的 RDS 主机上必须安装 Horizon Agent 7.4 或更高版本。必须在桌面池或场级别启用会话协作功能。有关为桌面池启用会话协作功能的信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档。有关为场启用会话协作功能的信息，请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档。 |
| Linux 远程桌面   | 有关 Linux 远程桌面要求，请参阅《设置 Horizon 7 for Linux 桌面》文档。  |
| 连接服务器        | 连接服务器实例使用企业许可证。  |
| 显示协议         | VMware Blast   |

有关如何使用会话协作功能的信息，请参阅 [Horizon Client 文档](#)。

## 配置会话协作组策略设置

使用 VMware View Agent 配置 ADMX 模板文件 (vdm\_agent.admx) 中的“协作”组策略设置来配置会话协作。请参阅[会话协作策略设置](#)。

## 会话协作功能的限制

用户无法在协作会话中使用以下远程桌面功能。

- USB 重定向
- 实时音频-视频 (RTAV)
- 多媒体重定向
- 客户端驱动器重定向
- 智能卡重定向
- 虚拟打印
- Microsoft Lync 重定向
- 文件重定向和“在 Dock 中保留”功能
- 剪贴板重定向

用户无法在协作会话中更改远程桌面分辨率。

用户不能在同一台客户端计算机上进行多个协作会话。

## 配置适用于 Skype for Business 的 VMware Virtualization Pack

您可以使用 Skype for Business 在虚拟桌面中进行优化的音频和视频通话，而不会对虚拟基础架构造成不利影响，也不会导致网络过载。在 Skype 音频和视频通话期间，将在客户端计算机上进行所有媒体处理，而不是在虚拟桌面中进行。

## 适用于 Skype for Business 的 VMware Virtualization Pack 功能

适用于 Skype for Business 的 VMware Virtualization Pack 可提供以下功能：

- 使用 HTTPS 代理服务器提供通话和会议
- 响应组
- Microsoft Office 集成：可以从 Word、Outlook 和 SharePoint 等软件启动 Skype for Business 通话
- 用户体验质量允许 Skype for Business 客户端向 Skype for Business 服务器报告通话指标以生成报告
- 以代理的身份代表其他人管理通话
- 主动识别说话人

- 可通过家用电话号码和工作电话号码等拨号
- 可从远程桌面控制音量
- E911 调用
- 呼叫寄存和取回
- 匿名加入外部会议
- 将呼叫重定向到移动设备
- 呼叫统计信息
- 智能卡身份验证
- 点到点音频通话
- 点到点视频通话
- 通过拨号盘进行 PSTN 通话
- 呼叫转接、呼叫转移、通话静音、将通话置于保持状态和恢复通话
- HID 命令
- 通过中介服务器呼叫 PSTN
- 通过 Edge 服务器进行远程连接和呼叫
- 等待音乐
- 自定义铃声
- 语音信箱集成
- USB 电话
- 支持已发布的应用程序
- 音频和视频前向纠错 (Forward Error Correction, FEC)
- Skype for Business 联机会议
- 立即开会功能
- 白板和屏幕共享

## 适用于 Skype for Business 的 VMware Virtualization Pack 的系统要求

适用于 Skype for Business 的 VMware Virtualization Pack 支持以下配置。

**表 2-8. 适用于 Skype for Business 的 VMware Virtualization Pack 系统要求**

| 系统            | 要求  |
|---------------|---|
| Microsoft 服务器 | Lync Server 2013、Skype for Business Server 2015、Office365、Skype for Business Server 2019  |
| Microsoft 客户端 | <p>VMware 强烈建议使用最新的 Skype for Business 客户端更新。</p> <ul style="list-style-type: none"> <li>■ Skype for Business 2015 客户端：15.0.4933.100 或更高版本</li> <li>■ Skype for Business 2016 作为 Office 365 Plus 的一部分：16.0.7571.2072 或更高版本</li> <li>■ Skype for Business 2016 作为 Office 2016 的一部分：16.0.4561.1000 或更高版本</li> </ul> <p><b>注</b> 不支持 Skype for Business Basic 2015 或 2016 客户端。</p>   |
| 虚拟桌面操作系统      | <p>最低要求：2 个 vCPU</p> <ul style="list-style-type: none"> <li>■ Windows 7 SP1</li> <li>■ Windows 8.1</li> <li>■ Windows 10 永久和非永久桌面</li> <li>■ Windows 2008 R2 SP1 桌面</li> <li>■ Windows 2012 R2 桌面</li> <li>■ Windows 2008 R2 SP1 RDSH 桌面</li> <li>■ Windows 2012 R2 RDSH 桌面</li> <li>■ Windows Server 2016 RDSH 桌面</li> <li>■ 已发布的应用程序支持</li> </ul>   |
| 客户端计算机操作系统    | <p>最低硬件要求：2.4 GHz 双核</p> <ul style="list-style-type: none"> <li>■ Windows 7 SP1</li> <li>■ Windows 8.1</li> <li>■ Windows 10</li> <li>■ Windows Embedded Standard 7</li> <li>■ Windows 10 IoT</li> <li>■ Windows Thin PC</li> </ul> <p>适用于 Skype for Business 的 VMware Virtualization Pack 支持的 Linux 操作系统与适用于 Linux 的 Horizon Client 支持的系统相同。</p> <p>适用于 Skype for Business 的 VMware Virtualization Pack 支持的 Mac 操作系统与适用于 Mac 的 Horizon Client 支持的系统相同。</p> |
| 部署            | <ul style="list-style-type: none"> <li>■ VDI（内部部署和云部署）</li> <li>■ 永久和非永久桌面</li> <li>■ RDS 部署（已发布的桌面和应用程序）</li> </ul>  |
| 显示协议          | VMware Blast 和 PCoIP  |
| 网络端口          | 与本机 Skype for Business 客户端所用的端口相同。请参阅 <a href="https://technet.microsoft.com/en-us/library/gg398833.aspx">https://technet.microsoft.com/en-us/library/gg398833.aspx</a> 中的客户端端口。  |
| 麦克风和网络摄像头     | 可用于 Skype for Business 的相同设备。请参阅 <a href="https://technet.microsoft.com/en-us/office/dn947482.aspx">https://technet.microsoft.com/en-us/office/dn947482.aspx</a> 中列出的网络摄像头。   |
| 音频和视频编解码器     | 与本机 Skype for Business 客户端所用的音频和视频编解码器相同。请参阅 <a href="https://technet.microsoft.com/en-us/library/gg425841.aspx?f=255&amp;MSPPError=-2147217396">https://technet.microsoft.com/en-us/library/gg425841.aspx?f=255&amp;MSPPError=-2147217396</a> 。  |



| 系统                                  | 要求  |
|-------------------------------------|---|
| 兼容对等的 Skype for Business 客户端（非 VDI） | <ul style="list-style-type: none"> <li>■ 安装了最新更新的 Skype for Business 2016 客户端</li> <li>■ 安装了最新更新的 Skype for Business 2015 客户端</li> <li>■ 安装了最新更新的 Lync 2013 客户端</li> <li>■ Lync 2010 客户端（仅限音频通话）</li> </ul> |
| 媒体功能包                               | 必须安装在 Windows 10 N 和 KN 版本的远程桌面上。您可以从 <a href="https://www.microsoft.com/en-us/download/details.aspx?id=48231">https://www.microsoft.com/en-us/download/details.aspx?id=48231</a> 安装媒体功能。                   |

## 安装适用于 Skype for Business 的 VMware Virtualization Pack

要使用 Skype for Business，必须在客户机上安装适用于 Skype for Business 的 VMware Virtualization Pack。适用于 Skype for Business 的 VMware Virtualization Pack 软件会默认作为适用于 Windows 的 Horizon Client（4.6 及更高版本）、适用于 Linux 的 Horizon Client（4.6 及更高版本）以及适用于 Mac 的 Horizon Client（4.7 及更高版本）安装程序的一部分进行安装。有关 Horizon Client 的安装信息，请参阅相应 Horizon Client 版本的安装和设置指南。

Horizon 管理员必须在 Horizon Agent 安装期间，在虚拟桌面上安装适用于 Skype for Business 的 VMware Virtualization Pack。有关 Horizon Agent 安装信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档。

适用于 Skype for Business 的 VMware Virtualization Pack 包含以下软件模块：

- 安装在虚拟桌面中的 Horizon Media Proxy
- 安装在客户端端点中的 Horizon Media Provider。

要确认是否已在虚拟机上安装了适用于 Skype for Business 的 VMware Virtualization Pack，请查看以下注册表项：

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office\Lync\VdiMediaProvider - GUID(REG\_SZ)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\Lync\VdiMediaProvider - GUID(REG\_SZ)

## 会话的配对模式

Lync.exe 会在启动时加载适用于 Skype for Business 的 VMware Virtualization Pack 插件。此插件会检查是否存在有效的会话，并在注册表中写入配对模式状态。要查询配对模式，请在进程列表中确认 Lync.exe 正在运行，然后检查 HKEY\_CURRENT\_USER\Software\VMware, Inc.\VMWMMAPLugin - PairingMode(REG\_SZ)。

有效的配对模式包括：

- 已优化：有效会话
- 回退：没有有效的会话
- 已优化 (版本不匹配)
- 回退 (版本不匹配)
- 正在连接

- 已断开连接
- 未定义

Lync.exe 退出时，该插件将从注册表中删除配对模式值。

用户不需要管理员特权即可查看配对模式。登录远程桌面的多个用户可以在 HKCU 配置单元中查找每个用户的配对模式。

## 配置适用于 Skype for Business 的 VMware Virtualization Pack 组策略设置

您可以配置用于更改默认配置的组策略设置。请参阅[适用于 Skype for Business 的 VMware Virtualization Pack 策略设置](#)。

## 适用于 Skype for Business 的 VMware Virtualization Pack 限制

适用于 Skype for Business 的 VMware Virtualization Pack 存在以下限制：

- 不支持 Socks 和 http 代理服务器。
- 适用于 Skype for Business 的 VMware Virtualization Pack 解决方案不支持与第三方多方会议系统（例如，Pexip）进行互操作。
- 当前不支持库视图。
- 不能录制通话。
- 不支持媒体绕过。有关详细信息，请参阅 <https://kb.vmware.com/s/article/56977>。
- 不支持双跃点方案，例如随 Horizon Client 一起嵌套 Horizon Agent。
- 不支持在远程桌面上使用优化的 Skype for Business 客户端的同时，在客户端计算机上使用 Lync 或 Skype for Business 客户端。
- 将 Skype 2015 客户端连接到 Lync 2013 服务器时，不支持 Lync 2013 客户端 UI。管理员可以在服务器上配置 Skype 客户端 UI： <https://social.technet.microsoft.com/wiki/contents/articles/30282.switch-between-skype-for-business-and-lync-client-ui.aspx>
- 在视频预览窗口中，如果想要预览列出的摄像头之外的其他摄像头，请选择该设备，关闭对话框，然后重新将其打开以进行预览。如果您希望摄像头动态更新，请使用 Skype for Business 2016 即点即用安装程序版本 16.0.11001.20097 或更高版本。
- 如果您在远程桌面上安装 Skype for Business 时连接到专用网络，安装程序会为该网络配置文件添加入站和出站防火墙规则。从域网络登录到远程桌面，然后使用 Skype for Business 时，您会看到防火墙异常。要解决该问题，请在所有网络配置文件的防火墙规则中为 Skype for Business 客户端手动添加防火墙例外。

## 收集日志以排除 Skype for Business 故障

要排除 Skype for Business 故障，请从 Horizon Agent 和适用于 Windows 的 Horizon Client 中收集日志。

### 步骤

- 1 要从 Horizon Agent 中收集 Horizon 日志（包括 Media Proxy 日志），请登录安装了 Horizon Agent 的虚拟机。
- 2 打开命令提示符，并运行 `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat`。
- 3 要从 Horizon Client 中收集 Horizon 日志（包括 Media Provider 日志），请登录安装了 Horizon Client 的物理机或虚拟机。
- 4 打开命令提示符，并运行 `support.bat`。
  - 32 位: `C:\Program Files\VMware\VMware Horizon View Client\DCT\support.bat`
  - 64 位: `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT\support.bat`

将在桌面上显示一个包含压缩日志文件的名为 `vdm-sdct` 的文件夹，该文件夹中将包括以下目录，这些目录包含适用于 Skype for Business 的 VMware Horizon Virtualization Pack 的日志：

- 客户端设备: `%TEMP%\vmware-  
<username>\VMWMediaProvider`
- 虚拟桌面：
  - `%TEMP%\vmware-  
<username>\VMWMediaProviderProxy`
  - `%TEMP%\vmware-  
<username>\VMWMediaProviderProxyLocal`
  - `%TEMP%\vmware-  
<username>\MMAPlugin`

默认日志级别为 7，此时的日志级别大小和崩溃转储都较小。您可以将日志级别提高到 8，以收集最大日志和完整的崩溃转储。所有设置均为 DWORD：

- 客户端: `HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMWMediaProvider\DebugLogging/LoggingPriority = 8`
- 代理: `HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMWMediaProviderProxy/DebugLogging/LoggingPriority = 8`
- 代理: `HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMWMediaProviderProxyLocal/DebugLogging/LoggingPriority = 8`

## 配置 VMware Integrated Printing 重定向

通过 VMware Integrated Printing 功能，用户可以使用其 Windows、Mac 和 Linux 客户端计算机上可用的任何打印机进行打印。

VMware Integrated Printing 支持客户端打印机重定向、基于位置的打印以及持久打印设置。

## 客户端打印机重定向

通过客户端打印机重定向功能，用户可以从远程桌面打印到 Windows、Mac 或 Linux 客户端上安装的任何本地或网络打印机。对于从 Windows 客户端重定向到远程桌面的打印机，VMware Integrated Printing 在远程桌面上支持两种类型的打印机驱动程序：

- 本机打印机驱动程序 (Native Printer Driver, NPD)。您必须在远程桌面上安装与客户端打印机驱动程序相同的打印机驱动程序。NPD 仅支持 v3 打印机。
- 通用打印机驱动程序 (Universal Printer Driver, UPD)。您无需在远程桌面上安装任何驱动程序。

默认情况下，如果在 Horizon Agent 上安装本机驱动程序，则会使用 NPD。否则，将使用 UPD。您可以通过设置组策略来选择要在远程桌面上使用的打印机驱动程序类型。

要查看远程桌面中使用的打印机驱动程序类型，请转到**控制面板 > 硬件和声音 > 设备和打印机**，右键单击虚拟打印机，然后从上下文菜单中选择**打印机属性**。在**常规**选项卡上，如果**型号**为 VMware 通用 EMF 驱动程序，则会使用 UPD。否则，将使用 NPD。

## 基于位置的打印

基于位置的打印功能可将物理位置接近客户端系统的打印机映射到远程桌面，从而使用户能够从远程桌面打印到网络打印机。以下远程桌面和应用程序支持基于位置的打印：

- 在单用户计算机上部署的桌面，包括 Windows 桌面和 Windows Server 计算机
- 在 RDS 主机上部署的已发布桌面和已发布应用程序，其中 RDS 主机为虚拟机或物理机

要使用基于位置的打印，您必须在远程桌面上安装正确的打印机驱动程序，并在 LBP.xml 文件中为每个基于位置的打印机定义转换规则。这些规则确定打印机是否被映射到远程桌面以供特定客户端系统使用。当用户连接到远程桌面时，Horizon 7 会将客户端系统与转换规则进行比较。如果客户端系统符合所有转换规则，则 Horizon 7 会在用户会话期间将打印机映射到远程桌面。

您可以根据已登录到远程桌面的用户名称、客户端系统的 IP 地址、主机名以及 MAC 地址来定义转换规则。您可以为某个特定打印机指定一个转换规则或者若干转换规则的组合。如果在 LBP.xml 中将任何基于位置的打印机设置为默认打印机，则该打印机将成为远程桌面上的默认打印机，其优先级高于客户端系统上的默认打印机。

要使规则生效，需在远程桌面上将 LBP.xml 保存到 %ProgramData%\VMware，然后重新连接远程桌面或远程应用程序。

您可以在 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip 中找到 LBP.xml 的模板。请参阅 [Horizon 7 ADMX 模板文件](#)。

可以通过设置组策略来禁用基于位置的打印。

## 嵌套模式重定向

在嵌套模式设置中，您可以将第一层和第二层上安装的本地打印机重定向到第三层上的远程桌面或远程应用程序。根据 GPO 设置以及是否安装了本机打印驱动程序，第三层上的重定向的打印机可以使用 UPD 或 NPD。

## 静态打印机名称

重定向的打印机在会话之间保留其名称（名称带有后缀 **vd**i），以便用户在连接到其他会话时无需手动重新映射打印机。仅在单用户计算机上支持静态打印机名称，在采用 VDI 模式的 Windows Server 上不支持该名称。

## 持久打印设置

在用户从桌面注销或断开连接后，将会保留已重定向的客户端打印机（包括本机打印机驱动程序和通用打印机驱动程序）或基于位置的打印机的打印机设置。例如，用户可能将已重定向的客户端打印机或基于位置的打印机设置为使用黑白模式。在用户注销并重新登录到桌面后，之前的打印设置会持久保留。

可以通过设置组策略来禁用持久打印设置。

## 通用打印机驱动程序打印设置

VMware Integrated Printing 为从 Windows 客户机重定向的 UPD 打印机提供了以下打印设置。

- **方向：**选择纸张方向（纵向或横向）。
- **双面打印：**为具有双面打印功能的打印机选择双面打印。
- **每张纸打印多页：**如果要将多个文档页面打印到一个物理页面上，请选择要打印到一个物理页面上的页数，然后选择页面布局。
- **纸张：**选择纸张大小的类型，例如 **letter** 或 **legal**。
- **介质：**选择要打印到的介质类型。
- **颜色：**指定彩色打印机应进行彩色打印还是黑白打印。
- **DPI：**指定打印机分辨率。
- **打印和预览：**选择**直接打印**或**打印预览**：
  - 对于**直接打印**，您可以选择在**打开首选项对话框时**，这将在打印前打开客户端打印机首选项，以便您更改打印设置。
  - 对于**打印预览**，在**打开首选项对话框时**选项不可用。
- **份数：**指定打印份数。
- **打印为图像：**将每个页面打印为一个图像。
- **压缩：**指定如何压缩打印文档中的图像。

## 打印机装订选项

在将特定的硬件连接到打印机时，这些重定向的本机打印机支持装订选项：

**表 2-9. 打印机装订选项**

| 打印机                         | 装订选项    | 客户端本地打印机上的要求  |
|-----------------------------|---------|---|
| FX ApeosPort-IV C5575 PCL 6 | 钉书钉、小册子 | 确认装订硬件设备连接到打印机。<br>在打印机属性中使用双向通信更新打印机信息。<br>在打印机首选项中启用装订选项。 |
| Ricoh MP C5003              | 钉书钉     | 根据设备设置手动添加装订器以启用装订选项，将在打印机首选项中提供该选项。                        |

## 安装 VMware Integrated Printing 重定向

VMware Integrated Printing 是 Horizon Agent 安装程序中的一个自定义安装选项。默认情况下不选择该选项。您必须选择“VMware Integrated Printing”以安装该功能。要在虚拟机上安装此功能，请参阅《在 Horizon 7 中设置虚拟桌面》文档。要在 RDS 主机上安装此功能，请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档。这些文档发布在 <https://docs.vmware.com/cn/VMware-Horizon-7/index.html>。要在 Windows 客户端上设置打印首选项，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档中的为 VMware Integrated Printing 重定向功能设置打印首选项，网址为 <https://docs.vmware.com/cn/VMware-Horizon-Client-for-Windows/index.html>。

## 配置 VMware Integrated Printing 重定向组策略设置

可使用 VMware View Agent 配置 ADMX 模板文件 (printerRedirection.admx) 中的组策略设置来禁用基于位置的打印，禁用打印设置持久性，以及选择已重定向的客户端打印机的打印机驱动程序。请参阅 [VMware 集成打印策略设置](#)。

## 为 USB 重定向、Windows Media Player MMR 重定向或客户端驱动器重定向激活 BEAT 侧通道

采用 VMware Blast 显示协议时，您可以将 USB 重定向、Windows Media Player 多媒体重定向 (MMR) 和客户端驱动器重定向功能配置为通过 Blast 极高自适应传输 (Blast Extreme Adaptive Transport, BEAT) 连接发送侧通道流量，而不是通过 VMware 虚拟通道 (VMware Virtual Channel, VVC) 或 TCP 侧通道发送。

通过 BEAT 侧通道，您可以整合 USB 重定向、Windows Media Player MMR 重定向和客户端驱动器重定向的网络端口要求。如果您的网络允许 VMware Blast 会话流量，则您不需要打开任何其他 UDP 端口，因为 BEAT 侧通道与核心（鼠标、键盘和显示器）VMware Blast 会话流量共享一个 UDP 端口。相比之下，TCP 侧通道就需要您打开其他 TCP 端口，因为它不共享用于会话流量的 TCP 端口。

### 步骤

- 1 要为 USB 重定向功能激活 BEAT 侧通道，请执行以下步骤。
  - a 导航到 HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware UsbRedirection，并将 sideChannelType 注册表项设置为 beat。
  - b 导航到 HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration，并将 UsbVirtualChannelEnabled 注册表项设置为 true。

**2** 要为 Windows Media Player 多媒体重定向 (MMR) 功能激活 BEAT 侧通道，请执行以下步骤。

| 选项                      | 说明  |
|-------------------------|---|
| <b>x86 Windows 操作系统</b> | <ul style="list-style-type: none"><li>a 打开代理计算机上的 Windows 注册表编辑器 (regedit.exe)。</li><li>b 导航到 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware TSMMR，并将 sideChannelType 项设置为 beat。</li></ul>   |
| <b>x64 Windows 操作系统</b> | <ul style="list-style-type: none"><li>a 打开代理计算机上的 Windows 注册表编辑器 (regedit.exe)。</li><li>b 导航到 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware TSMMR，并将 sideChannelType 项设置为 beat。</li><li>c 导航到 HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\VMware, Inc.\VMware TSMMR，并将 sideChannelType 项设置为 beat。</li></ul> |

在适用于 Windows 的 Horizon Client 和适用于 Linux 的 Horizon Client 上支持该功能。

**3** 要为客户端驱动器重定向功能激活 BEAT 侧通道，请执行以下步骤。

- a 打开代理计算机上的 Windows 注册表编辑器 (regedit.exe)。
- b 导航到 HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware TSDR，并将 sideChannelType 注册表项设置为 beat。

## 配置 URL 内容重定向

通过 URL 内容重定向功能，您可以将特定 URL 配置为在客户端计算机上、在远程桌面上或在已发布的应用程序中打开。您可以重定向用户在 Internet Explorer 地址栏或应用程序中键入的 URL。

本章讨论了以下主题：

- 了解 URL 内容重定向
- URL 内容重定向要求
- 在 Cloud Pod 架构环境中使用 URL 内容重定向
- 安装具有 URL 内容重定向功能的 Horizon Agent
- 配置代理到客户端重定向
- 配置客户端到代理重定向
- URL 内容重定向限制
- 不支持的 URL 内容重定向功能
- 在 Windows 上安装并启用适用于 Chrome 的 URL 内容重定向帮助程序扩展
- 在 Mac 上启用适用于 Chrome 的 URL 内容重定向帮助程序

### 了解 URL 内容重定向

URL 内容重定向功能支持从远程桌面或已发布应用程序到客户端的重定向，以及从客户端到远程桌面或已发布应用程序的重定向。

从远程桌面或已发布应用程序到客户端的重定向称为代理到客户端重定向。从客户端到远程桌面或已发布应用程序的重定向称为客户端到代理重定向。

#### 代理到客户端重定向

利用代理到客户端重定向，Horizon Agent 可将 URL 发送到 Horizon Client，以便在客户端计算机上打开 URL 中协议的默认应用程序。

#### 客户端到代理重定向

利用客户端到代理重定向，Horizon Client 可打开您指定用来处理 URL 的远程桌面或已发布应用程序。如果将 URL 重定向到远程桌面，将在该桌面上使用协议的默认浏览器打开链接。如果将 URL 重定向到已发布的应用程序，将通过指定的已发布应用程序打开链接。最终用户必须有权访问桌面或应用程序池。



您可以将一些 URL 从远程桌面或已发布的应用程序重定向到客户端，而将其他一些 URL 从客户端重定向到远程桌面或已发布的应用程序。您可以重定向任意数量的协议，包括 HTTP、HTTPS、mailto 和 callto。Chrome 浏览器的重定向功能不支持 callto 协议。

## URL 内容重定向要求

要使用 URL 内容重定向功能，您的客户端计算机、远程桌面计算机和 RDS 主机必须满足特定要求。

### Web 浏览器

- Internet Explorer 9、10 和 11
  - Chrome 60.0.3112.101 或更高版本（官方内部版本），64 位或 32 位
- 要在 Chrome 浏览器中使用 URL 内容重定向，必须在 Chrome 中安装并启用 VMware Horizon URL 内容重定向帮助程序扩展。有关 Windows 安装说明，请参阅在 [Windows 上安装并启用适用于 Chrome 的 URL 内容重定向帮助程序扩展](#)。有关 Mac 安装说明，请参阅在 [Mac 上启用适用于 Chrome 的 URL 内容重定向帮助程序](#)。

### Windows 客户端

- 适用于 Windows 的 Horizon Client 4.0 或更高版本。
- 要在 Chrome 浏览器中使用 URL 内容重定向，您必须安装 Horizon Client 4.7 或更高版本。
- 要使用客户端到代理重定向，您必须在适用于 Windows 的 Horizon Client 安装过程中启用 URL 内容重定向功能。

---

**注** 要使用代理到客户端重定向，您无需在适用于 Windows 的 Horizon Client 中启用 URL 内容重定向功能。

---

### Mac 客户端

- 适用于 Mac 的 Horizon Client 4.2 或更高版本。

---

**注** 在适用于 Mac 的 Horizon Client 4.2 和 4.3 中，URL 内容重定向是一项技术预览版功能，仅支持代理到客户端重定向。在适用于 Mac 的 Horizon Client 4.4 及更高版本中，正式支持 URL 内容重定向，且该功能同时支持代理到客户端和客户端到代理重定向。

---

- 要在 Chrome 浏览器中使用 URL 内容重定向，您必须安装 Horizon Client 4.7 或更高版本。

### 桌面虚拟机和 RDS 主机

- Horizon Agent 7.0 或更高版本（在提供已发布桌面和已发布应用程序的远程桌面虚拟机和 RDS 主机中）。
- 要在 Chrome 浏览器中使用 URL 内容重定向，您必须安装 Horizon Agent 7.4 或更高版本。
- 您必须在 Horizon Agent 安装过程中启用 URL 内容重定向功能。

### 显示协议

- VMware Blast

## ■ PCoIP

# 在 Cloud Pod 架构环境中使用 URL 内容重定向

如果您具有 Cloud Pod 架构环境，则除了可配置本地 URL 内容重定向设置外，您还可以配置全局 URL 内容重定向设置。

与仅在本地容器中可见的本地 URL 内容重定向设置不同，全局 URL 内容重定向设置将在整个容器联合中可见。利用全局 URL 内容重定向设置，可以将客户端中的 URL 链接重定向到全局资源，例如全局桌面授权和全局应用程序授权。

用户使用 Horizon Client 登录到容器联合中的连接服务器实例时，该连接服务器实例会查找分配给此用户的所有本地和全局 URL 内容重定向设置。每当用户在客户端计算机上单击 URL 时，便会合并和使用本地与全局设置。

有关配置和管理 Cloud Pod 架构环境的完整信息，请参阅《在 Horizon 7 中管理 Cloud Pod 架构》文档。

## 安装具有 URL 内容重定向功能的 Horizon Agent

要使用从远程桌面或已发布应用程序到客户端（代理到客户端重定向）或者从客户端到远程桌面或应用程序（客户端到代理重定向）的 URL 内容重定向，必须在安装 Horizon Agent 时启用 URL 内容重定向功能。

在命令提示符窗口中运行以下命令（而不是双击安装程序文件）来开始安装 Horizon Agent：

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

按照提示完成安装。

要验证是否已安装 URL 内容重定向功能，请确保 `vmware-url-protocol-launch-helper.exe` 和 `vmware-url-filtering-plugin.dll` 文件均位于 `%PROGRAMFILES%\VMware\VMware View\Agent\bin\UrlRedirection` 目录中。如果要在 Internet Explorer 中使用 URL 内容重定向功能，则还需验证是否已启用“VMware Horizon View URL 筛选插件”这一 Internet Explorer 附加模块。

## 配置代理到客户端重定向

利用代理到客户端重定向，Horizon Agent 可将 URL 发送到 Horizon Client，以打开 URL 中协议的默认应用程序。

要启用代理到客户端重定向，请执行以下配置任务。

- 在 Horizon Agent 中启用 URL 内容重定向功能。请参阅[安装具有 URL 内容重定向功能的 Horizon Agent](#)。
- 将 URL 内容重定向组策略设置应用到远程桌面和已发布的应用程序。请参阅[将 URL 内容重定向 ADMX 模板添加到 GPO](#)。
- 配置组策略设置以指示对于每个协议，Horizon Agent 应如何重定向 URL。请参阅[URL 内容重定向组策略设置](#)。

- （可选）要在 Chrome 浏览器中使用 URL 内容重定向，请安装并启用 VMware Horizon URL 内容重定向帮助程序扩展。请参阅[在 Windows 上安装并启用适用于 Chrome 的 URL 内容重定向帮助程序扩展](#)。

## 将 URL 内容重定向 ADMX 模板添加到 GPO

URL 内容重定向 ADMX 模板文件（名为 `urlRedirection.admx`）中包含的设置允许您控制是在客户端（代理到客户端重定向）上还是在远程桌面或已发布的应用程序（客户端到代理重定向）中打开 URL 链接。

要将 URL 内容重定向组策略设置应用到远程桌面和已发布的应用程序，可将 ADMX 模板文件添加到 Active Directory 服务器上的 GPO。对于有关在远程桌面或已发布的应用程序中单击的 URL 链接的规则，必须将 GPO 链接到包含虚拟桌面和 RDS 主机的 OU。

您还可以将组策略设置应用于链接到的 OU 包含 Windows 客户端计算机的 GPO，但是配置客户端到代理重定向的首选方法是使用 `vdmutil` 命令行实用程序。由于 macOS 不支持 GPO，因此，在具有 Mac 客户端时，您必须使用 `vmdutil`。

### 前提条件

- 确认在您安装 Horizon Agent 时已包含 URL 内容重定向功能。请参阅[安装具有 URL 内容重定向功能的 Horizon Agent](#)。
- 确认为 URL 内容重定向组策略设置创建了 Active Directory GPO。
- 确认 MMC 和组策略管理编辑器插件在您的 Active Directory 服务器上可用。

### 步骤

- 1 从 VMware 下载站点中下载 Horizon 7 GPO 捆绑包 .zip 文件，网址为 <https://my.vmware.com/web/vmware/downloads>。

在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 GPO 捆绑包。

该文件名为 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`，其中 `x.x.x` 是版本号，`yyyyyyy` 是内部版本号。为 Horizon 7 提供组策略设置的所有 ADMX 文件均在此文件中提供。

- 2 解压缩 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` 文件，并将 URL 内容重定向 ADMX 文件复制到 Active Directory 服务器。

a 将 `urlRedirection.admx` 文件复制到 `C:\Windows\PolicyDefinitions` 文件夹。

b 将 `urlRedirection.adml` 语言资源文件复制到 `C:\Windows\PolicyDefinitions` 中的相应子文件夹。

例如，对于 EN 区域设置，将 `urlRedirection.adml` 文件复制到 `C:\Windows\PolicyDefinitions\en-US` 文件夹。

- 3 在 Active Directory 服务器上，打开组策略管理编辑器。

URL 内容重定向组策略设置安装在 **计算机配置 > 策略 > 管理模板 > VMware Horizon URL 重定向** 中。

## 后续步骤

配置组策略设置。请参阅 [URL 内容重定向组策略设置](#)。

## URL 内容重定向组策略设置

URL 内容重定向模板文件中包含的组策略设置允许您创建代理到客户端和客户端到代理重定向的规则。该模板文件同时包含计算机配置和用户配置策略。所有设置位于组策略管理编辑器的 **VMware Horizon URL 重定向** 文件夹中。

下表介绍了 URL 内容重定向模板文件中的组策略设置。

**表 3-1. URL 内容重定向组策略设置**

| 设置   | 计算机 | 用户 | 属性   |
|--|-----|----|--|
| IE Policy: Prevent users from changing URL Redirection plugin loading behavior | X   |    | 确定用户是否可以禁用 URL 内容重定向功能。<br>默认情况下不配置此设置。  |
| IE Policy: Automatically enable URL Redirection plugin                         | X   |    | 确定是否自动激活新安装的 Internet Explorer 插件。<br>默认情况下不配置此设置。                             |
| Url Redirection Enabled  | X   |    | 确定是否启用了 URL 内容重定向功能。即使已在客户端或代理中安装了 URL 内容重定向功能，您也可以使用此设置禁用该功能。<br>默认情况下不配置此设置。 |

| 设置                               | 计算机 | 用户 | 属性   |
|----------------------------------|-----|----|--|
| Url Redirection Protocol 'http'  | X   |    | <p>对于使用 HTTP 协议的所有 URL，请指定应重定向的 URL。此设置包含以下选项：</p> <ul style="list-style-type: none"> <li>■ <b>代理主机名</b> - 在将 URL 重定向到远程桌面或应用程序时使用的连接服务器主机的 IP 地址或完全限定名称。</li> <li>■ <b>远程项目</b> - 可以处理代理规则中指定的 URL 的远程桌面或应用程序池的显示名称。</li> <li>■ <b>客户端规则</b> - 应重定向到客户端的 URL。例如，如果将客户端规则设置为 <b>.*.mycompany.com</b>，则所有包含文本 mycompany.com 的 URL 均会被重定向到基于 Windows 的客户端，并在客户端上的默认浏览器中打开。</li> <li>■ <b>代理规则</b> - 应重定向到远程项目中指定的远程桌面或应用程序的 URL。例如，如果将代理规则设置为 <b>.*.mycompany.com</b>，则所有包含“mycompany.com”的 URL 均会被重定向到远程桌面或应用程序。</li> </ul> <p>您可以在<b>客户端规则</b>和<b>代理规则</b>中输入正则表达式。如果启用了 <b>Url Redirection IP Rules Enabled</b> 设置，您还可以输入特定的 IP 地址或 IP 地址范围。有关完整的语法信息，请参阅 <a href="#">URL 内容重定向规则的语法</a>。</p> <p>在创建代理规则时，您还必须使用<b>代理主机名</b>选项指定连接服务器主机的 IP 地址或完全限定域名，并使用<b>远程项目</b>选项指定桌面或应用程序池的显示名称。</p> <p>最佳做法是为 HTTP 和 HTTPS 协议配置相同的重定向设置。这样，如果用户在 Internet Explorer 中键入部分 URL（如 mycompany.com），并且该站点自动从 HTTP 重定向到 HTTPS，则 URL 内容重定向功能将按预期工作。在此示例中，如果为 HTTPS 设置一个规则，但没有为 HTTP 设置相同的重定向设置，则不会重定向用户键入的部分 URL。</p> <p>默认情况下启用该设置。</p> |
| Url Redirection Protocol 'https' | X   |    | <p>对于使用 HTTPS 协议的所有 URL，请指定应重定向的 URL。</p> <p>对于 Url Redirection Protocol 'http'，这些选项是相同的。</p> <p>默认情况下不配置此设置。</p>  |
| Url Redirection Protocol '[...]' | X   |    | <p>将此设置用于除 HTTP 和 HTTPS 以外的任何协议，例如 email 或 callto。</p> <p>对于 Url Redirection Protocol 'http' 和 Url Redirection Protocol 'https'，这些选项是相同的。</p> <p>如果您不需要配置其他协议，可以在将 URL 内容重定向模板文件添加到 Active Directory 之前删除或注释掉此条目。</p> <p>默认情况下不配置此设置。</p>  |

| 设置  | 计算机 | 用户 | 属性  |
|---|-----|----|---|
| Install the Chrome extension that is required in the URL content redirection feature. |     | X  | <p>如果启用此设置，将以静默方式自动安装 URL 内容重定向功能所需的 Chrome 扩展。此安装还包括授予必需的权限。取消此安装需要具备管理特权。</p> <p>如果禁用或未配置此设置，将不会安装 URL 内容重定向功能所需的 Chrome 扩展，并且 URL 内容重定向将无法在 Chrome 浏览器中使用，即使设置了重定向也是如此，除非从 Chrome 网上应用店中手动安装该扩展。</p> <p>默认情况下不配置此设置。</p> |
| Url Redirection IP Rules Enabled  | X   |    | <p>如果启用了该设置，您可以在<b>客户端规则</b>或<b>代理规则</b>中输入特定的 IP 地址或 IP 地址范围。有关更多信息，请参阅<a href="#">IP 地址</a>和<a href="#">IP 地址范围筛选</a>。</p> <p>默认情况下禁用该设置。</p> <p><b>注</b> 仅 Internet Explorer 和 IPv4 支持该功能。</p>                           |

对于客户端到代理重定向，如果您配置的协议没有默认处理程序，则在为此协议配置组策略设置后，您必须先启动 Horizon Client 一次，才能重定向指定此协议的 URL。

配置客户端到代理重定向的首选方法是使用 vdmutil 命令行实用程序，而不是组策略设置。

## URL 内容重定向规则的语法

在使用 URL 内容重定向组策略设置时，您必须指定在客户端（**客户端规则**选项）或者远程桌面或发布的应用程序（**代理规则**选项）中打开的 URL。

### URL

您可以在**客户端规则**和**代理规则**中输入 URL。可以使用通配符 (\*) 指定匹配多个 URL 的 URL 模式。您必须在句点前面添加转义符 (\) 以在规则条目中指定句点。例如，如果您指定 “.\*\ .net”，则会重定向 xxxx.net，而不会重定向 http://intranet。

下表显示包含 URL 的规则条目示例。

| 规则条目                               | 说明  |
|------------------------------------|---|
| .*                                 | 指定重定向所有 URL。<br>如果将该设置用于代理规则（ <b>代理规则</b> 选项），则在指定的远程桌面或发布的应用程序中打开所有 URL。如果将该设置用于客户端规则（ <b>客户端规则</b> 选项），则将所有 URL 重定向到客户端。        |
| .*\ .acme\ .com;.*\ .example\ .com | 指定重定向所有包含文本 .acme.com 或 example.com 的 URL。应使用分号分隔多个条目。不允许在条目之间使用空格。   |
| .*\ .acme\ .com/ software          | 指定重定向所有包含文本 .acme.com 和子目录 /software 的 URL。例如，http://www.acme.com/software 会被重定向。此外，http://www.acme.com/software/consumer 也会被重定向。 |
| [空格或保留空白]                          | 指定不重定向任何 URL。例如，如果将 <b>客户端规则</b> 选项保留空白，则指定不将任何 URL 重定向到客户端。  |

### 正则表达式

您可以在**客户端规则**和**代理规则**中输入正则表达式。有关语法信息，请参阅[URL 内容重定向支持的正则表达式规则](#)。

## IP 地址和 IP 地址范围筛选

如果启用“URL 重定向 IP 规则已启用”组策略设置，您可以在**客户端规则**和**代理规则**中输入特定的 IP 地址或 IP 地址范围。

例如，如果启用“URL 重定向 IP 规则已启用”并输入

“**\*\mycompany.com;22.22.22.22;10.10.1.2-10.10.12.20**”，则会重定向以下 URL 和 IP 地址。

- 所有包含 .mycompany.com 的 URL
- IP 地址 22.22.22.22
- 在 10.10.1.2 至 10.10.12.20 范围内的所有 IP 地址
- 解析为 IP 地址 22.22.22.22 的所有 URL
- 解析为 IP 地址范围 10.10.1.2 至 10.10.12.20 的所有 URL

如果同时输入 URL 以及 IP 地址或 IP 地址范围，则 URL 规则具有较高的优先级。如果与 URL 匹配，将直接使用 URL 进行重定向。如果与 URL 不匹配，Horizon 将执行 DNS 查询，然后进行 IP 地址或 IP 地址范围筛选。

仅 Internet Explorer 和 IPv4 支持该功能。默认情况下它被禁用。

## URL 内容重定向支持的正则表达式规则

您可以在**客户端规则**和**代理规则**中输入正则表达式。正则表达式是一个描述字符模式的对象。正则表达式对文本执行模式匹配以及搜索和替换功能。

URL 内容重定向支持以下正则表达式规则。

| 规则        | 详细信息                          |
|-----------|-------------------------------|
| 括号        | [ ]、[ ^ ]、( )、( ? : )、( ? = ) |
| \ 元字符或元字符 | “\w”、“\W”、“\d”、“\D”、“\b”、“\B” |
| 限定符       | +, *, ?, {x}, {x,y}, {x,}     |
| 替换符       |                               |

有关正则表达式的详细信息，请参阅 [https://en.wikipedia.org/wiki/Regular\\_expression](https://en.wikipedia.org/wiki/Regular_expression)。

下表包含 URL 内容重定向支持的正则表达式规则示例。

**注** 第二列中的粗体文本表示与左侧列中的正则表达式匹配的 URL 部分。

| 规则条目          | 匹配的 URL 和 IP 地址示例   |
|---------------|---|
| *\net         | www.hello. <b>net</b> 、www.inter. <b>net</b> 、train.word. <b>net</b> 、test.train. <b>net</b> 以及 train.chromeie. <b>net</b> .com.cn。 |
| *\sth\ctirial | example. <b>sth.ctirial</b> 、www.google. <b>sth.ctirial</b> 和 www.google.com/test. <b>sth.ctirial</b> /editpage.action。             |
| *administra   | www. <b>administra</b> .com、www.ask <b>administra</b> -tor.net 和 google.akmkda.eae/ <b>administra</b> .cn。                          |



| 规则条目  | 匹配的 URL 和 IP 地址示例   |
|---|---|
| .*a{4}custom\.com   | world.banada.cn/aaaacustom.com、www.aaaacustom.com 和 exple.aaaacustom.com.net/nodepad.action。                          |
| .*a{2,3}custom\.com   | world.banada.aacustom.com、www.aacustom.com 和 exple.aacustom.com.net/nodepad.action。                                   |
| .*train[abc]\.net   | hello.traina.net、hello.trainb.net、example.trainc.net.com 以及 www.testtraina.net.com/edit。                              |
| .*train[^abc]\.net  | hello.traind.net、hello.traine.net、example.train2.net.com 以及 www.testtrain3.net.com/edit。                              |
| .*a+c*tra\.net  | www.actra.net.com、aactra.net.cn、atra.net.www.train 以及 aaccetra.netword。   |
| .*example(test)?\.cn  | www.example.cn、www.exampletest.cn、example.cn/editpage 以及 exampletest.cn/editpage。                                     |
| sac(?:=sprt)  | helloworld.sacsprt.net、examplesacsprt.com/text 和 www.sacsprtexam.com。   |
| sac(?:!sprt)  | helloworld.sacspra.net、examplesacbprrt.com/text 和 www.sacexam.com。  |
| 10\.\.1\.\.1[0-5]   | 10.1.1.10 至 10.1.1.15。  |
| 10\.\.1\.(1 2)\.\.1[0-5]  | 10.1.1.10 至 10.1.1.15 以及 10.1.2.10 至 10.1.2.15。   |
| 10\.[2-4]\.\.19\.\.12   | 10.2.19.12、10.3.19.12 和 10.4.19.12。   |
| 10\[2-4]\.\.19\.\.12  | 10.6.19.12、10.1.19.12、10.5.19.12 和 10.7.19.12。  |
| a(\w)cd(\d)345a\.com  | www.abccd2345a.com.net 和 train.adc2cd1345a.com/edit.action。   |
| abc(\W)cd(\D)345a\.com  | google.abc+cda345a.com 和 test.train.net/abc&cda345a.com。  |
| ((25[0-5] 2[0-4][0-9] [01]?[0-9]?[0-9])\.){3}(25[0-5] 2[0-4][0-9] [01]?[0-9]?[0-9]) | 所有 IPv4 地址。   |
| .*example(test)?\.cn;10\.\.1\.\.1[0-5];a(\w)cd(\d)345a\.com                         | www.example.cn、example.cn/editpage、10.1.1.10 至 10.1.1.15、www.abccd2345a.com.net 以及 train.adc2cd1345a.com/edit.action。 |

## 代理到客户端重定向组策略示例

您可能希望使用代理到客户端重定向来节约资源或作为额外的安全层。例如，如果员工在远程桌面或已发布的应用程序中观看视频，可以将这些 URL 重定向到客户端计算机，以便不会在数据中心产生额外的负载。为了安全起见，对于在公司网络外部工作的员工，您可能希望在员工自己的客户端计算机上打开指向公司网络外部位置的所有 URL。

例如，您可以配置一些规则，将未指向公司网络的所有 URL 重定向在客户端计算机上打开。在此示例中，可以使用以下包含正则表达式的设置：

- 对于代理规则：.\*.mycompany.com

此规则可重定向任何包含文本 mycompany.com 的 URL，使其在指定的远程桌面或已发布的应用程序（代理）中打开。

- 对于客户端规则：.\*

此规则可将所有 URL 重定向到客户端，使其通过默认的客户端浏览器打开。

URL 内容重定向功能使用以下过程应用客户端和代理规则：

- 1 当用户在已发布的应用程序或远程桌面中单击链接时，将首先检查客户端规则。
- 2 如果 URL 与客户端规则匹配，则随后检查代理规则。
- 3 如果代理和客户端规则之间存在冲突，将在本地打开链接。在此示例中，将在代理计算机上打开 URL。
- 4 如果不存在冲突，URL 将被重定向到客户端。

在此示例中，客户端和代理规则发生冲突是因为包含 **mycompany.com** 的 URL 是所有 URL 的一个子集。由于发生该冲突，将在本地打开包含 **mycompany.com** 的 URL。如果在远程桌面中单击 URL 中包含 **mycompany.com** 的链接，将在该远程桌面上打开此 URL。如果从客户端系统中单击 URL 中包含 **mycompany.com** 的链接，将在客户端上打开该 URL。

## 配置客户端到代理重定向

利用客户端到代理重定向功能，Horizon Client 可打开远程桌面或已发布的应用程序来处理用户在客户端中单击的 URL 链接。如果打开远程桌面，URL 中协议的默认应用程序会处理该 URL。如果打开已发布的应用程序，此已发布的应用程序会处理该 URL。

要使用客户端到代理重定向，请执行以下配置任务。

- 在 Horizon Agent 中启用 URL 内容重定向功能。请参阅[安装具有 URL 内容重定向功能的 Horizon Agent](#)。
- （仅限 Windows 客户端）在适用于 Windows 的 Horizon Client 中启用 URL 内容重定向功能。请参阅[安装具有 URL 内容重定向功能的适用于 Windows 的 Horizon Client](#)。
- （可选）要在 Chrome 浏览器中使用 URL 内容重定向，请安装并启用 VMware Horizon URL 内容重定向帮助程序扩展。对于 Windows 客户端，请参阅[在 Windows 上安装并启用适用于 Chrome 的 URL 内容重定向帮助程序扩展](#)。对于 Mac 客户端，请参阅[在 Mac 上启用适用于 Chrome 的 URL 内容重定向帮助程序](#)。
- 使用 **vdmutl** 命令行实用程序创建 URL 内容重定向设置，以指示对于每个协议，Horizon Client 应如何重定向 URL。请参阅[创建本地 URL 内容重定向设置](#)或[创建全局 URL 内容重定向设置](#)。
- 使用 **vdmutl** 命令行实用程序将 URL 内容重定向设置分配给 Active Directory 用户或组。请参阅[将 URL 内容重定向设置分配给用户或组](#)。
- 验证 URL 内容重定向设置。请参阅[测试 URL 内容重定向设置](#)。

---

**重要事项** 您可以使用组策略设置来配置客户端到代理重定向规则，但使用 **vdmutl** 命令行实用程序是首选方法。有关使用组策略设置的信息，请参阅[使用组策略设置配置客户端到代理重定向](#)。对于 Mac 客户端，您必须使用 **vdmutl** 配置客户端到代理重定向。由于 macOS 不支持 GPO，因此，在具有 Mac 客户端时，您无法使用组策略设置来配置客户端到代理配置。

---

## 安装具有 URL 内容重定向功能的适用于 Windows 的 Horizon Client

要使用从 Windows 客户端到远程桌面或已发布应用程序的 URL 内容重定向（客户端到代理重定向），必须安装具有 URL 内容重定向功能的适用于 Windows 的 Horizon Client。

要启用 URL 内容重定向功能，必须通过命令行选项使用适用于 Windows 的 Horizon Client 安装程序。在命令提示符窗口中运行以下命令（而不是双击安装程序文件）来开始安装：

```
VMware-Horizon-Client-x86-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

要验证是否已安装 URL 内容重定向功能，请确保 `vmware-url-protocol-launch-helper.exe` 和 `vmware-url-filtering-plugin.dll` 文件均位于 `%PROGRAMFILES%\VMware\VMware Horizon View Client` 目录中。如果要在 Internet Explorer 中使用 URL 内容重定向功能，则还需验证是否已安装“VMware Horizon View URL 筛选插件”这一 Internet Explorer 附加模块。

---

**注** 适用于 Mac 的 Horizon Client 4.4 在默认情况下支持客户端到代理重定向。无需执行额外的安装步骤。适用于 Mac 的 Horizon Client 4.2 和 4.3 不支持客户端到代理重定向。

---

## 使用 vdmutil 命令行实用程序

您可以使用 `vdmutil` 命令行界面为客户端到代理重定向创建、分配和管理 URL 内容重定向设置。

---

**注** 您必须使用 `vdmutil` 命令来为 Mac 客户端配置客户端到代理重定向。由于 macOS 不支持 GPO，因此，在具有 Mac 客户端时，您无法使用 GPO 配置客户端到代理配置。

---

### 命令用法

`vdmutil` 命令的语法可从 Windows 命令提示符中控制其操作。

```
vdmutil command_option [additional_optionargument] ...
```

您可以使用的附加选项取决于命令选项。

默认情况下，`vdmutil` 命令可执行文件的路径为 `C:\Program Files\VMware\VMware View\Server\tools\bin`。为避免在命令行中输入此路径，可以将此路径添加到 `PATH` 环境变量中。

### 命令身份验证

必须以具有管理员角色的用户身份运行 `vdmutil` 命令。

可以使用 Horizon Administrator 将管理员角色分配给用户。有关更多信息，请参阅《Horizon 7 管理指南》文档。

`vdmutil` 命令包括用于指定进行身份验证时使用的用户名、域和密码的选项。必须将这些身份验证选项与除 `--help` 和 `--verbose` 之外的所有 `vdmutil` 命令选项结合使用。

**表 3-2. vdmutil 命令身份验证选项**

| 选项             | 说明   |
|----------------|--|
| --authAs       | 要向连接服务器实例进行身份验证的 Horizon 管理员用户的用户名。请勿使用域\用户名或用用户主体名称 (User Principal Name, UPN) 格式。      |
| --authDomain   | --authAs 选项中指定的 Horizon 管理员用户的完全限定域名。  |
| --authPassword | --authAs 选项中指定的 Horizon 管理员的密码。在命令行中键入 "*" 来代替密码会导致 vdmutil 命令提示输入密码，并且不会在命令历史记录中保留敏感密码。 |

例如，以下 vdmutil 命令将以用户 mydomain\johndoe 的身份登录。

```
vdmutil --listURLSetting --authAs johndoe --authDomain mydomain --authPassword secret
```

## 命令输出

操作成功时，vdmutil 命令将返回 0；操作失败时，将返回故障特定的非零代码。vdmutil 命令会将错误消息写入标准错误。当某个操作生成输出时，或通过使用 --verbose 选项启用了详细日志记录时，vdmutil 命令会使用美国英语将输出写入标准输出。

## 用于 URL 内容重定向的选项

您可以使用以下 vdmutil 命令选项创建、分配和管理 URL 内容重定向设置。所有选项的前面都有两个短划线 (--)。

**表 3-3. 用于 URL 内容重定向的 vdmutil 命令选项**

| 选项                      | 说明  |
|-------------------------|---|
| --addGroupURLSetting    | 将组分配给特定的 URL 内容重定向设置。                         |
| --addUserURLSetting     | 将用户分配给特定的 URL 内容重定向设置。                        |
| --createURLSetting      | 创建 URL 内容重定向设置。                               |
| --deleteURLSetting      | 删除 URL 内容重定向设置。                               |
| --disableURLSetting     | 禁用 URL 内容重定向设置。                               |
| --enableURLSetting      | 启用之前通过 --disableURLSetting 选项禁用的 URL 内容重定向设置。 |
| --listURLSetting        | 列出连接服务器实例中的所有 URL 内容重定向设置。                    |
| --readURLSetting        | 显示有关 URL 内容重定向设置的信息。                          |
| --removeGroupURLSetting | 从 URL 内容重定向设置中移除组分配。                          |
| --removeUserURLSetting  | 从 URL 内容重定向设置中移除用户分配。                         |
| --updateURLSetting      | 更新现有的 URL 内容重定向设置。                            |

通过键入 vdmutil --help，可以显示所有 vdmutil 选项的语法信息。要显示特定选项的详细语法信息，请键入 vdmutil --option --help。

## “--agentURLPattern” 选项的语法

当您使用 `vdmutl` 命令创建 URL 内容重定向设置时，需在 `--agentURLPattern` 选项中键入带双引号的字符串，用于指定应在远程桌面或已发布应用程序上打开的一个或多个 URL。

带双引号的字符串包含正则表达式，且必须包含协议前缀。可以使用通配符指定匹配多个 URL 的 URL 模式。

下表介绍了一些示例 URL 模式。

| 代理 URL 模式                  | 说明  |
|----------------------------|---|
| "*"                        | 所有客户端 URL 均会被重定向到远程桌面或已发布的应用程序。   |
| "http://google.*"          | 所有包含文本 <b>google</b> 的客户端 URL 均会被重定向到远程桌面或已发布的应用程序。   |
| "http://acme.com/software" | 所有包含文本 <b>acme.com</b> 和子目录 <b>/software</b> 的客户端 URL 均会被重定向到远程桌面或已发布的应用程序。例如， <code>http://www.acme.com/software</code> 会被重定向。此外， <code>http://www.acme.com/software/consumer</code> 也会被重定向。 |

## 创建本地 URL 内容重定向设置

您可以创建本地 URL 内容重定向设置，以重定向特定的 URL，使其在远程桌面或已发布的应用程序上打开。本地 URL 内容重定向设置仅在本地容器中可见。

您可以配置任意数量的协议，包括 HTTP、HTTPS、mailto 和 callto。Chrome 浏览器的重定向功能不支持 callto 协议。

最佳做法是为 HTTP 和 HTTPS 协议配置相同的重定向设置。这样，如果用户在 Internet Explorer 中键入部分 URL（如 `mycompany.com`），并且该站点自动从 HTTP 重定向到 HTTPS，则 URL 内容重定向功能将按预期工作。在此示例中，如果为 HTTPS 设置一个规则，但没有为 HTTP 设置相同的重定向设置，则不会重定向用户键入的部分 URL。

要创建在整个容器联合中可见的全局 URL 内容重定向设置，请参阅[创建全局 URL 内容重定向设置](#)。

### 前提条件

- 熟悉 `vdmutl` 命令行界面选项和要求，并确认有足够的特权来运行 `vdmutl` 命令。请参阅[使用 vdmutil 命令行实用程序](#)。
- 熟悉 URL 内容重定向设置中 URL 的语法。请参阅[“--agentURLPattern” 选项的语法](#)。

### 步骤

- 1 登录到连接服务器实例。

## 2 运行带有 `--createUrlSetting` 选项的 `vdmutil` 命令，以创建 URL 内容重定向设置。

```
vdmutil --createUrlSetting --urlSettingName value --urlRedirectionScope LOCAL
[--description value] [--urlScheme value] [--entitledApplication value | --entitledDesktop value]
[--agentURLPattern value]
```

| 选项                                 | 说明   |
|------------------------------------|--|
| <code>--urlSettingName</code>      | URL 内容重定向设置的唯一名称。名称可以包含 1 到 64 个字符。  |
| <code>--urlRedirectionScope</code> | URL 内容重定向设置的范围。指定“LOCAL”可使设置仅在本地容器中可见。   |
| <code>--description</code>         | URL 内容重定向设置的描述。描述包含的字符数可介于 1 到 1024 个字符之间。   |
| <code>--urlScheme</code>           | 将 URL 内容重定向设置应用到的协议，例如 <code>http</code> 、 <code>https</code> 、 <code>mailto</code> 或 <code>calto</code> 。 |
| <code>--entitledApplication</code> | 用来打开指定 URL 的本地应用程序池的显示名称，例如 <code>iexplore-2012</code> 。您还可以使用此选项指定本地 RDS 桌面池的显示名称。                        |
| <code>--entitledDesktop</code>     | 用来打开指定 URL 的本地桌面池的显示名称，例如 <code>Win10</code> 。对于 RDS 桌面池，请使用 <code>--entitledApplication</code> 选项。        |
| <code>--agentURLPattern</code>     | 一个带有引号的字符串，用于指定应在远程桌面或已发布的应用程序上打开的 URL。  |

## 3 （可选）运行带有 `--updateURLSetting` 选项的 `vdmutil` 命令，以将更多协议、URL 和本地资源添加到您创建的 URL 内容重定向设置。

```
vdmutil --updateURLSetting --urlSettingName value --urlRedirectionScope LOCAL
[--description value][--urlScheme value][--entitledApplication value | --entitledDesktop value]
[--agentURLPattern value]
```

这些选项与带有 `--createUrlSetting` 选项的 `vdmutil` 命令的选项相同。

### 示例：创建本地 URL 内容重定向设置

以下示例创建了一个名为 `url-filtering` 的本地 URL 内容重定向设置，该设置可将所有包含文本 `http://google.*` 的客户端 URL 重定向到名为 `iexplore2012` 的应用程序池。

```
VdmUtil --createUrlSetting --urlSettingName url-filtering --urlScheme http
--entitledApplication iexplore2012 --agentURLPattern "http://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

以下示例更新了 `url-filtering` 设置，以便也将所有包含文本 `https://google.*` 的客户端 URL 重定向到名为 `iexplore2012` 的应用程序池。

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme https
--entitledApplication iexplore2012 --agentURLPattern "https://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

以下示例更新了 `url-filtering` 设置，以便将所有包含文本 `mailto://.*.mycompany.com` 的客户端 URL 重定向到名为 Outlook2008 的应用程序池。

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme mailto
--entitledApplication Outlook2008 --agentURLPattern "mailto://.*.mycompany.com"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

### 后续步骤

将 URL 内容重定向设置分配给用户或组。请参阅[将 URL 内容重定向设置分配给用户或组](#)。

## 创建全局 URL 内容重定向设置

如果您具有 Cloud Pod 架构环境，可以创建全局 URL 内容重定向设置，以重定向特定的 URL，使其在容器联合的任何容器中的远程桌面或已发布的应用程序上打开。

全局 URL 内容重定向设置将在整个容器联合中可见。在创建全局 URL 内容重定向设置时，您可以将 URL 重定向到全局资源，例如全局桌面授权和全局应用程序授权。

您可以配置任意数量的协议，包括 HTTP、HTTPS、mailto 和 callto。Chrome 浏览器的重定向功能不支持 callto 协议。

最佳做法是为 HTTP 和 HTTPS 协议配置相同的重定向设置。这样，如果用户在 Internet Explorer 中键入部分 URL（如 `mycompany.com`），并且该站点自动从 HTTP 重定向到 HTTPS，则 URL 内容重定向功能将按预期工作。在此示例中，如果为 HTTPS 设置一个规则，但没有为 HTTP 设置相同的重定向设置，则不会重定向用户键入的部分 URL。

有关配置和管理 Cloud Pod 架构环境的完整信息，请参阅《在 Horizon 7 中管理 Cloud Pod 架构》文档。

要创建本地 URL 内容重定向设置，请参阅[创建本地 URL 内容重定向设置](#)。

### 前提条件

- 熟悉 `vdmutil` 命令行界面选项和要求，并确认您有足够的特权来运行 `vdmutil` 命令。请参阅[使用 vdmutil 命令行实用程序](#)。
- 熟悉 URL 内容重定向设置中 URL 的语法。请参阅“`--agentURLPattern`”选项的语法。

### 步骤

- 1 登录到容器联合中的任何连接服务器实例。
- 2 运行带有 `--createURLSetting` 选项的 `vdmutil` 命令，以创建 URL 内容重定向设置。

```
vdmutil --createURLSetting --urlSettingName value --urlRedirectionScope GLOBAL
[--description value] [--urlScheme value] [--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

| 选项                                 | 说明                                       |
|------------------------------------|--|
| <code>--urlSettingName</code>      | URL 内容重定向设置的唯一名称。名称可以包含 1 到 64 个字符。      |
| <code>--urlRedirectionScope</code> | URL 内容重定向设置的范围。指定“GLOBAL”可使设置在整个容器联合中可见。 |



| 选项                           | 说明   |
|------------------------------|--|
| <b>--description</b>         | URL 内容重定向设置的描述。描述包含的字符数可介于 1 到 1024 个字符之间。         |
| <b>--urlScheme</b>           | 将 URL 内容重定向设置应用到的协议，例如 http、https、mailto 或 callto。 |
| <b>--entitledApplication</b> | 用来打开指定 URL 的全局应用程序授权的显示名称。                         |
| <b>--entitledDesktop</b>     | 用于打开指定 URL 的全局桌面授权的显示名称，例如，GE-1。                   |
| <b>--agentURLPattern</b>     | 一个带有引号的字符串，用于指定应在远程桌面或已发布的应用程序上打开的 URL。            |

- 3 （可选）运行带有 **--updateURLSetting** 选项的 **vdmutl** 命令，以将更多协议、URL 和全局资源添加到您创建的 URL 内容重定向设置。

```
vdmutl --updateURLSetting --urlSettingName value --urlRedirectionScope GLOBAL
[--description value][--urlScheme value][--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

这些选项与带有 **--createURLSetting** 选项的 **vdmutl** 命令的选项相同。

## 示例：配置全局 URL 内容重定向设置

以下示例创建了一个名为 **Operations-Setting** 的全局 URL 内容重定向设置，该设置可将所有包含文本 **http://google.\*** 的客户端 URL 重定向到名为 **GAE1** 的全局应用程序授权。

```
vdmutl --createURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme http --entitledApplication GAE1 --agentURLPattern "http://google.*" --authAs johndoe
--authDomain mydomain --authPassword secret
```

以下示例更新了 **Operations-Setting** 设置，以便也将所有包含文本 **https://google.\*** 的 URL 重定向到名为 **GAE1** 的全局应用程序授权。

```
vdmutl --updateURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme https --entitledApplication GAE1 --agentURLPattern "https://google.*" --authAs johndoe
--authDomain mydomain --authPassword secret
```

以下示例更新了 **Operations-Setting** 设置，以便将所有包含文本 **"mailto://\*.mycompany.com"** 的 URL 重定向到名为 **GA2** 的全局应用程序授权。

```
vdmutl --updateURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme mailto --entitledApplication GAE2 --agentURLPattern "mailto://*.mycompany.com"
--authAs johndoe --authDomain mydomain --authPassword secret
```

## 后续步骤

将 URL 内容重定向设置分配给用户或组。请参阅[将 URL 内容重定向设置分配给用户或组](#)。

## 将 URL 内容重定向设置分配给用户或组

在创建 URL 内容重定向设置后，您可以将其分配给 Active Directory 用户或组。

### 前提条件

熟悉 vdmutil 命令行界面选项和要求，并确认您有足够的特权来运行 vdmutil 命令。请参阅[使用 vdmutil 命令行实用程序](#)。

### 步骤

- ◆ 要将 URL 内容重定向设置分配给用户，请运行带有 --addUserURLSetting 选项的 vdmutil 命令。

```
vdmutil --addUserURLSetting --urlSettingName value --userName value
```

| 选项               | 说明   |
|------------------|--|
| --urlSettingName | 要分配的 URL 内容重定向设置的名称。                         |
| --userName       | Active Directory 用户的名称，其格式为 domain\username。 |

- ◆ 要将 URL 内容重定向设置分配给组，请运行带有 --addGroupURLSetting 选项的 vdmutil 命令。

```
vdmutil --addGroupURLSetting --urlSettingName value --groupName value
```

| 选项               | 说明                                       |
|------------------|--|
| --urlSettingName | 要分配的 URL 内容重定向设置的名称。                     |
| --groupName      | Active Directory 组的名称，其格式为 domain\group。 |

### 示例：分配 URL 内容重定向设置

以下示例将名为 url-filtering 的 URL 内容重定向设置分配给名为 mydomain\janedoe 的用户。

```
vdmutil --addUserURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --userName mydomain\janedoe
```

以下示例将名为 url-filtering 的 URL 内容重定向设置分配给名为 mydomain\usergroup 的组。

```
vdmutil --addGoupURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --groupName mydomain\usergroup
```

### 后续步骤

验证您的 URL 内容重定向设置。请参阅[测试 URL 内容重定向设置](#)。

## 测试 URL 内容重定向设置

在创建并分配 URL 内容重定向设置后，需执行特定的步骤以验证该设置是否可正常工作。

### 前提条件

熟悉 `vdmutil` 命令行界面选项和要求，并确认有足够的特权来运行 `vdmutil` 命令。请参阅[使用 vdmutil 命令行实用程序](#)。

### 步骤

- 1 登录到连接服务器实例。
- 2 运行带有 `--readURLSetting` 选项的 `vdmutil` 命令。

例如：

```
vdmutil --readURLSetting --urlSettingName url-filtering --authAs johndoe
--authDomain mydomain --authPassword secret
```

该命令会显示有关 URL 内容重定向设置的详细信息。例如，以下有关 `url-filtering` 设置的命令输出显示了包含文本 `google.*` 的 HTTP 和 HTTPS URL 会从客户端重定向到名为 `iexplore2012` 的本地应用程序池。

```
URL Redirection setting url-filtering
Description                        : null
Enabled                            : true
Scope of URL Redirection Setting   : LOCAL
URL Scheme And Local Resource handler pairs
  URL Scheme                       : http
  Handler type                     : APPLICATION
  Handler Resource name             : iexplore2012
  URL Scheme                       : https
  Handler type                     : APPLICATION
  Handler Resource name             : iexplore2012
AgentPatterns
  https://google.*
  http://google.*
ClientPatterns
  No client patterns configured
```

- 3 在 Windows 客户端计算机上，打开 **Horizon Client**，连接到连接服务器实例，单击与设置中配置的 URL 模式相匹配的 URL，然后验证这些 URL 是否可按预期进行重定向。
- 4 在同一台 Windows 客户端计算机上，打开注册表编辑器 (`regedit`) 并检查路径 `\Computer\HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\URLRedirection\` 中的注册表项。

您应看到在设置中指定的每个协议都有一个对应的注册表项。您可以单击某个协议以查看与该协议关联的规则。例如，`agentRules` 显示重定向的 URL，`brokerHostName` 显示在重定向 URL 时使用的连接服务器实例的 IP 地址或完全限定主机名，`remoteItem` 显示处理重定向 URL 的桌面或应用程序池的显示名称。

## 管理 URL 内容重定向设置

您可以使用 `vdmutil` 命令管理 URL 内容重定向设置。

您必须指定用于所有命令的 `--authAs`、`--authDomain` 和 `--authPassword` 选项。有关更多信息，请参阅[使用 vdmutil 命令行实用程序](#)。

### 显示设置

运行带有 `--listURLSetting` 选项的 `vdmutil` 命令，可列出已配置的所有 URL 内容重定向设置的名称。

```
vdmutil --listURLSetting
```

运行带有 `--readURLSetting` 的 `vdmutil` 命令，可查看有关特定 URL 内容重定向设置的详细信息。

```
vdmutil --readURLSetting --urlSettingName value
```

### 删除设置

运行带有 `--deleteURLSetting` 选项的 `vdmutil` 命令，可删除 URL 内容重定向设置。

```
vdmutil --deleteURLSetting --urlSettingName value
```

### 禁用和启用设置

运行带有 `--disableURLSetting` 选项的 `vdmutil` 命令，可禁用 URL 内容重定向设置。

```
vdmutil --disableURLSetting --urlSettingName value
```

运行带有 `--enableURLSetting` 选项的 `vdmutil`，可启用已禁用的 URL 内容重定向设置。

```
vdmutil --enableURLSetting --urlSettingName value
```

### 从设置中移除用户或组

运行带有 `--removeUserURLSetting` 选项的 `vdmutil` 命令，可从 URL 内容重定向设置中移除用户。

```
vdmutil --removeUserURLSetting --urlSettingName value --userName value
```

运行带有 `--removeGroupURLSetting` 选项的 `vdmutil` 命令以从 URL 内容重定向设置中移除组。

```
vdmutil --removeGroupURLSetting --urlSettingName value --userGroup value
```

在指定用户或组名称时，请使用 `domain\username` 或 `domain\groupname` 格式。

## 使用组策略设置配置客户端到代理重定向

URL 内容重定向 ADMX 模板文件 (`urlRedirection.admx`) 中包含的组策略设置可用于创建将 URL 从客户端重定向到远程桌面或已发布应用程序（客户端到代理重定向）的规则。

---

**重要事项** 配置客户端到代理重定向的首选方法是使用 `vdmutil` 命令行界面。由于 macOS 不支持组策略，如果您具有 Mac 客户端，则无法使用组策略配置客户端到代理配置。

---

要创建客户端到代理重定向规则，请使用**远程项目**选项指定桌面或应用程序池的显示名称，并使用**代理规则**选项指定应重定向到远程桌面或发布的应用程序的 URL。您还必须使用**代理主机名**选项指定在将 URL 重定向到远程桌面或发布的应用程序时使用的连接服务器主机的 IP 地址或完全限定域名。

例如，为了安全起见，您可能希望在远程桌面或已发布应用程序中打开指向公司网络的所有 HTTP URL。在这种情况下，您可以将**代理规则**选项设置为 `*.mycompany.com`。

有关 URL 内容重定向模板文件安装说明、组策略设置说明以及**代理规则**选项语法，请参阅[配置代理到客户端重定向](#)。

## URL 内容重定向限制

URL 内容重定向功能的行为可能会出现某些意外结果。

- 如果 URL 根据区域设置打开一个特定于国家/地区的页面，则链接的来源决定打开的区域设置页面。例如，如果远程桌面（代理来源）位于日本的数据中心，用户计算机位于美国，并且 URL 将从代理重定向到客户端计算机，则在美国的客户端上打开的页面是日语页面。
- 如果用户从网页中创建收藏项，则收藏项在重定向后才会创建。例如，如果用户在客户端计算机上单击链接，并且 URL 将被重定向到远程桌面（代理），同时该用户又为此页面创建收藏项，则收藏项会在代理中创建。下次用户在客户端计算机上打开浏览器时，用户可能希望在客户端计算机上找到该收藏项，但该收藏项存储在远程桌面（代理来源）上。
- 用户下载的文件显示在用来打开 URL 的浏览器所在的计算机上，例如，当用户在客户端计算机上单击链接，并且 URL 将被重定向到远程桌面时。如果链接下载了文件，或者链接与用户下载文件的网页相对应，则文件将下载到远程桌面，而不是客户端计算机。
- 如果您在同一计算机上安装 Horizon Agent 和 Horizon Client，则可以在 Horizon Agent 或 Horizon Client 中启用 URL 内容重定向，但不能在两者中都启用该功能。您可以在这台计算机上设置客户端到代理的重定向或代理到客户端的重定向，但不能同时设置两者。

## 不支持的 URL 内容重定向功能

在某些情况下，URL 内容重定向功能无法正常工作。

### 缩短的 URL

缩短的 URL（如 `https://goo.gl/abc`）可以根据过滤规则进行重定向，但过滤机制不会检查原始的未缩短 URL。

例如，如果您的规则对包含 `acme.com` 的 URL（像 `http://www.acme.com/some-really-long-path` 之类的原始 URL，以及像 `https://goo.gl/xyz` 之类的原始 URL 的缩短 URL）进行重定向，则会重定向原始 URL，而不重定向缩短的 URL。

您可以解决此限制，办法是创建规则以阻止或重定向经常用于缩短 URL 的网站中的 URL。

## 嵌入的 HTML 页面

嵌入的 HTML 页面会绕过 URL 重定向，例如，当用户访问与 URL 重定向规则不匹配的 URL 时。如果某个页面包含嵌入的 HTML 页面（iFrame 或内嵌框架），并且该嵌入的 HTML 页面所包含的 URL 与某个重定向规则匹配，URL 重定向规则将不起作用。该规则仅适用于最上层的 URL。

## 禁用的 Internet Explorer 插件

URL 内容重定向功能在禁用了 Internet Explorer 插件的情况下无法使用，例如，当用户在 Internet Explorer 中切换到“**InPrivate** 浏览”时。人们使用隐私浏览，以便不会将网页和从网页下载的文件记录到其计算机上的浏览和下载历史记录中。出现此限制是因为，URL 重定向功能要求启用某些 Internet Explorer 插件，而隐私浏览会禁用这些插件。

您可以解决此限制，办法是使用 GPO 设置阻止用户禁用插件。这些设置包括“禁止用户启用或禁用加载项”和“自动启用新安装的加载项”。在组策略管理编辑器中，这些设置位于**计算机配置 > 管理模板 > Windows 组件 > Internet Explorer** 下面。

要解决这一特定于 Internet Explorer 的限制，请使用 GPO 设置禁用 InPrivate 模式。该设置称为“关闭 InPrivate 浏览”。在组策略管理编辑器中，这些设置位于**计算机配置 > 管理模板 > Windows 组件 > Internet Explorer > 隐私**下面。

这些解决办法是最佳做法，可以防止在除隐私浏览以外的其他情况下可能导致重定向问题。

## Windows 10 通用应用程序是协议的默认处理程序

如果 Windows 10 通用应用程序是在链接中指定的协议的默认处理程序，则 URL 重定向无法正常工作。通用应用程序在通用 Windows 平台上构建，以便可将其下载到个人计算机、平板电脑和手机上，这些应用程序包括 Microsoft Edge 浏览器、Mail、Maps、Photos、Grove Music，等等。

如果所单击链接的默认处理程序是其中一个应用程序，则不会重定向 URL。例如，如果用户在应用程序中单击一个电子邮件链接，并且默认电子邮件应用程序是 Mail 通用应用程序，则不会重定向链接中指定的 URL。

您可以解决此限制，办法是将其他应用程序设置为要重定向的 URL 协议的默认处理程序。例如，如果 Edge 是默认浏览器，则将 Internet Explorer 设置为默认浏览器。

## 在 Windows 上安装并启用适用于 Chrome 的 URL 内容重定向帮助程序扩展

要在 Windows 客户端或 Windows 代理计算机上一同使用 Chrome 浏览器和 URL 内容重定向功能，您必须安装并启用适用于 Chrome 的 VMware Horizon URL 内容重定向帮助程序扩展。

通过启用 URL 内容重定向组策略设置，可以安装并启用 VMware Horizon URL 内容重定向帮助程序扩展。

此过程介绍了如何在您的 **Active Directory** 服务器上将 **URL** 内容重定向组策略设置应用到 **GPO**。对于 **Windows** 客户端计算机，必须将 **GPO** 链接到包含您的 **Windows** 客户端计算机的 **OU**。对于远程桌面和应用程序，必须将 **GPO** 链接到包含您的虚拟桌面和 **RDS** 主机的 **OU**。

如果您不使用组策略来安装并启用 **VMware Horizon URL** 内容重定向帮助程序扩展，则必须从 **Chrome** 网上应用店中手动安装该扩展。

#### 前提条件

- 对于 **Windows** 客户端计算机，请安装 **Horizon Client 4.7** 或更高版本，并启用 **URL** 内容重定向功能。请参阅[安装具有 URL 内容重定向功能的适用于 Windows 的 Horizon Client](#)。
- 对于 **Windows** 代理计算机，请安装 **Horizon Agent 7.4** 或更高版本，并启用 **URL** 内容重定向功能。请参阅[安装具有 URL 内容重定向功能的 Horizon Agent](#)。
- 安装 **Chrome** 浏览器。有关支持的版本，请参阅[URL 内容重定向要求](#)。
- 确认您能够以管理员域用户的身份登录到托管 **Active Directory** 服务器的计算机。
- 确认 **MMC** 和组策略对象编辑器插件在您的 **Active Directory** 服务器上可用。
- 将 **URL** 内容重定向 **ADMX** 模板文件添加到您的 **Active Directory** 服务器。请参阅[将 URL 内容重定向 ADMX 模板添加到 GPO](#)。

#### 步骤

- 1 在 **Active Directory** 服务器上，打开组策略管理编辑器，并导航到**用户配置 > 策略 > 管理模板 > VMware Horizon URL 重定向**文件夹。
- 2 打开安装在 **URL** 内容重定向功能中所需的 **Chrome** 扩展设置，选择已启用，然后单击**确定**。
- 3 在 **Windows** 计算机上启动 **Chrome**。

**VMware Horizon URL** 内容重定向帮助程序扩展将会以静默方式进行安装。

- 4 要确认已安装该 **Chrome** 扩展，请在 **Chrome** 浏览器中键入 **chrome://extensions**。

**VMware Horizon URL** 内容重定向帮助程序将显示在“扩展程序”列表中，并且其已启用复选框处于选中状态。

#### 后续步骤

首次从客户端上的 **Chrome** 浏览器重定向 **URL** 时，系统会提示用户在 **Horizon Client** 中打开该 **URL**。用户必须单击**打开 URL:VMware Hori...lient 协议**，否则不会进行 **URL** 重定向。如果用户选中**记住我对 URL:VMware Hori...lient 协议链接的选择**复选框（推荐），则不会再次显示此提示。

## 在 Mac 上启用适用于 Chrome 的 URL 内容重定向帮助程序

要在 **Mac** 客户端上一同使用 **Chrome** 浏览器和 **URL** 内容重定向功能，您必须启用适用于 **Chrome** 的 **VMware Horizon URL** 内容重定向帮助程序扩展。

#### 前提条件

- 在 **Mac** 客户端上安装 **Chrome** 浏览器。有关支持的版本，请参阅[URL 内容重定向要求](#)。



- 在 Mac 上安装 Horizon Client 4.7 或更高版本。有关信息，请参阅《适用于 Mac 的 VMware Horizon Client 安装和设置指南》文档。

#### 步骤

- 1 在 Mac 上启动 Horizon Client，并连接到配置了 URL 内容重定向规则的连接服务器实例。  
VMware Horizon URL 内容重定向帮助程序扩展将会自动安装在 Mac 客户端上的 Chrome 浏览器中。
- 2 在 Mac 上重新启动 Chrome 浏览器。
- 3 当系统提示您启用 VMware Horizon URL 内容重定向帮助程序扩展时，单击**启用扩展**。  
您必须启用该扩展才能在 Chrome 浏览器中使用 URL 内容重定向。

---

**注** 如果移除该扩展，仍可以从 Chrome 网上应用店中手动安装它。

---

- 4 要确认已安装该 Chrome 扩展，请在 Chrome 浏览器中键入 **chrome://extensions**。  
**VMware Horizon URL 内容重定向帮助程序**将显示在“扩展程序”列表中，并且其**已启用**复选框处于选中状态。

#### 后续步骤

首次从 Mac 客户端上的 Chrome 浏览器重定向 URL 时，系统会提示用户在 Horizon Client 中打开该 URL。用户必须单击**打开 VMware Horizon Client**，否则不会进行 URL 重定向。如果用户选中**记住我对 VMware Horizon Client 链接的选择**复选框（推荐），则不会再次显示此提示。

# 将 USB 设备与远程桌面和应用程序一起使用

# 4

管理员可以配置从虚拟桌面使用各种 **USB** 设备的能力，如使用拇指闪存盘、摄像头、VoIP（IP 语音）设备和打印机。此功能称为 **USB 重定向**。虚拟桌面最多可容纳 128 个 **USB** 设备。

您还可以重定向某些本地连接的 **USB** 设备，以便在已发布的桌面和应用程序中使用。有关支持的特定设备类型的信息，请参阅 [USB 设备类型的相关限制](#)。

在已在单用户计算机上部署的桌面池中使用该功能时，已附加到本地客户端系统的大多数 **USB** 设备在远程桌面中变为可用。您甚至可以从远程桌面连接并管理 iPad。例如，可使 iPad 与安装在远程桌面中的 iTunes 同步。在某些客户端设备（如 Windows 和 Mac 计算机）上，将在 Horizon Client 菜单中列出 **USB** 设备。此菜单可用于连接设备和断开设备的连接。

在大多数情况下，无法同时在客户端系统和远程桌面中使用 **USB** 设备。只有几种类型的 **USB** 设备可以在远程桌面和本地计算机之间共享。这些设备包括智能卡读卡器和人机接口设备（如键盘和指针设备）。

管理员可指定最终用户可连接的 **USB** 设备类型。对于客户端系统上包含多种设备类型（例如，包含一个视频输入设备和一个存储设备）的复合设备，管理员可通过拆分设备，允许连接其中一个设备（如视频输入设备），而禁止连接另一个（如存储设备）。

**USB 重定向**功能仅适用于特定类型的客户端。要了解某个特定客户端是否支持该功能，请参阅针对该客户端的 Horizon Client 安装和设置文档中提供的功能支持表。

---

**重要事项** 部署 **USB 重定向**功能时，可以执行一些步骤来防止您的组织出现可能会影响 **USB** 设备的安全漏洞。请参阅[在安全的 Horizon 7 环境中部署 USB 设备](#)。

---

本章讨论了以下主题：

- [USB 设备类型的相关限制](#)
- [USB 重定向建议](#)
- [设置 USB 重定向概述](#)
- [配置指纹扫描仪重定向](#)
- [配置读卡器重定向](#)
- [网络流量和 USB 重定向](#)
- [自动连接到 USB 设备](#)
- [在安全的 Horizon 7 环境中部署 USB 设备](#)

- 使用日志文件进行故障排除和确定 USB 设备 ID
- 使用策略控制 USB 重定向
- 排除 USB 重定向故障

## USB 设备类型的相关限制

虽然 Horizon 7 没有明确阻止任何设备使用 USB 重定向功能，但受网络延迟和带宽等因素的影响，有些设备可能不如其他设备运行得那么顺畅。默认情况下，某些设备会被自动过滤或阻止，从而无法使用。

### USB 3.0 设备限制

自 Horizon 6 版本 6.0.1 和 Horizon Client 3.1 及更高版本开始，在客户端计算机上可以将 USB 3.0 设备插入到 USB 3.0 端口中。仅支持单个流通过 USB 3.0 设备。由于未实现多流支持，USB 设备性能未得到改善。由于网络延迟，一些需要持续高吞吐量才能正常运行的 USB 3.0 设备在远程会话中可能不起作用。

### 虚拟桌面的 USB 重定向限制

以下类型的 USB 设备可能不适合 USB 重定向至部署在单用户计算机上的远程桌面：

- 网络摄像头通常消耗 60 Mbps 以上的带宽，就因为这种带宽需求，网络摄像头不支持 USB 重定向。对于网络摄像头，您可以使用实时音频-视频功能。
- 音频 USB 设备的重定向不稳定，具体取决于网络状况。有些设备即使在闲置状态下也要求具备高数据吞吐量。如果具有实时音频-视频功能，音频输入和输出设备将可使用此功能正常运行，您无需为这些设备使用 USB 重定向。
- 不支持 USB CD/DVD 刻录。
- 某些 USB 设备的性能差异很大，具体取决于网络延迟情况和可靠性，尤其是通过 WAN 连接时。例如，单个 USB 存储设备读取请求需要在客户端和远程桌面之间往返三次。读取一个完整的文件可能需要多个 USB 读取操作，延迟越大，往返需要花费的时间也越长。

文件结构可能较大，具体取决于文件格式。较大的 USB 磁盘驱动器可能需要几分钟时间才能显示在桌面中。把 USB 设备处理为 NTFS 格式，而不使用 FAT 格式，有助于缩短首次连接时间。不可靠的网络链路接会导致重试，并且性能会进一步降低。

同样，USB CD/DVD 读取器和扫描仪无法在延迟网络上正常工作，例如，WAN。

- USB 扫描仪的重定向不稳定，具体取决于网络的状态，扫描花费的时间可能长于正常完成的时间。

### 已发布桌面和应用程序的 USB 重定向限制

在使用 View Agent 6.2.x 和更高版本或 Horizon Agent 7.0 和更高版本时，您可以重定向本地连接的 USB 拇指闪存盘和硬盘以用于已发布的桌面和应用程序。从 Horizon Agent 7.0.2 开始，发布的桌面和应用程序还可以支持更通用的 USB 设备，包括 TOPAZ 签名板、Olympus 语音听写脚踏板和 Wacom 签名板。发布的桌面和应用程序不支持其他类型的 USB 设备，包括安全存储驱动器和 USB CD-ROM 驱动器。

## USB 重定向建议

对于某些类型的 USB 设备，您可以使用建议的 USB 重定向解决方案。

请使用以下重定向功能来提供更好的性能和用户体验，而不要使用 USB 重定向：

- 对于扫描仪，请使用扫描仪重定向。请参阅[配置扫描仪重定向](#)。
- 对于打印机，请使用打印机重定向。请参阅[配置 VMware Integrated Printing 重定向](#)。
- 对于智能卡读卡器，请使用智能卡重定向。请参阅《Horizon 7 管理指南》文档。
- 对于串行端口设备，请使用串行端口重定向。请参阅[配置串行端口重定向](#)。
- 要进行文件共享，请使用客户端驱动器重定向，而不是 USB 重定向，USB 重定向适用于 USB 磁盘和大量存储设备。请参阅[管理对客户端驱动器重定向的访问](#)。

## 设置 USB 重定向概述

要设置部署以便最终用户可以连接可移除设备（如 USB 闪存驱动器、摄像头和耳机），您必须在远程桌面或 RDS 主机和客户端设备上安装某些组件，并且必须确认已在 Horizon Administrator 中启用了 USB 设备的全局设置。

此核对表包括在企业中设置 USB 重定向的必要任务和可选任务。

USB 重定向功能仅适用于某些类型的客户端。要了解某个特定类型的客户端是否支持该功能，请参阅针对该特定类型的客户端设备的安装和设置文档中提供的功能支持表。

---

**重要事项** 部署 USB 重定向功能时，可以执行一些步骤来防止您的组织出现可能会影响 USB 设备的安全漏洞。例如，您可以使用组策略设置对某些远程桌面和用户禁用 USB 重定向，或限制哪些类型的 USB 设备可以进行重定向。请参阅[在安全的 Horizon 7 环境中部署 USB 设备](#)。

---

- 1 在远程桌面源或 RDS 主机上运行 Horizon Agent 安装向导时，请务必包含 USB 重定向组件。

默认已取消选择此组件。必须选择此组件才会进行安装。

- 2 在客户端系统上运行 VMware Horizon Client 安装向导时，请包含 USB 重定向组件。

默认已包括此组件。

- 3 确认已在 Horizon Administrator 中启用了从远程桌面或应用程序访问 USB 设备的权限。

在 Horizon Administrator 中，转到**策略 > 全局策略**，确认 **USB 访问** 已设置为**允许**。

- 4 （可选）配置 Horizon Agent 组策略来指定允许重定向哪些类型的设备。

请参阅[使用策略控制 USB 重定向](#)。

- 5 （可选）在客户端设备上配置相似的设置。

您还可以配置当 Horizon Client 连接到远程桌面或应用程序或者最终用户插入 USB 设备时是否自动连接设备。在客户端设备上配置 USB 设置的方法取决于设备的类型。例如，对于 Windows 客户端，您可以配置组策略。对于 Mac 客户端，您可以使用命令行命令。有关更多信息，请参阅针对该特定类型客户端设备的安装和设置文档。

## 6 让最终用户连接到远程桌面或应用程序并将他们的 USB 设备插入本地客户端系统。

如果远程桌面或 RDS 主机中尚未安装 USB 设备的驱动程序，客户机操作系统会检测 USB 设备并搜索合适的驱动程序，就像在 Windows 物理机上一样。

## 配置指纹扫描仪重定向

可以将插入到 Windows 客户端系统上的 USB 端口的生物识别设备（尤其是指纹扫描仪）重定向到虚拟桌面。

要重定向这些指纹扫描仪，远程代理桌面至少需要 200 Mbps 网络带宽。

支持以下指纹扫描设备：

**表 4-1. 支持的指纹扫描仪**

| 设备                 | 客户端操作系统                               | Windows 操作系统服务器   | 协议          |
|--------------------|---------------------------------------|---|-------------|
| U.are.U 5160 指纹读取器 | Windows 10 1809 (64 位)                | Windows 10 1809 (64 位)  | PCoIP、Blast |
|                    | Windows 7 SP 1 Enterprise (32 位、64 位) | Windows 10 1903 (64 位)<br>Windows 7 SP 1 Enterprise (32 位、64 位) |             |
| U.are.U 5300 指纹读取器 | Windows 10 1809 (64 位)                | Windows 10 1809 (64 位)  | PCoIP、Blast |
|                    | Windows 7 SP 1 Enterprise (32 位、64 位) | Windows 10 1903 (64 位)<br>Windows 7 SP 1 Enterprise (32 位、64 位) |             |

## 配置读卡器重定向

可以将通过 PCoIP 虚拟通道插入到 Windows 客户端系统上的 USB 端口的读卡器重定向到虚拟桌面。

支持以下读卡器：

**表 4-2. 支持的读卡器**

| 设备                  | 客户端操作系统                               | Windows 操作系统服务器   | 协议    |
|---------------------|---------------------------------------|---|-------|
| Sony FeliCa RC-S320 | Windows 10 1809 (64 位)                | Windows 10 1809 (64 位)  | PCoIP |
|                     | Windows 7 SP 1 Enterprise (32 位、64 位) | Windows 10 1903 (64 位)<br>Windows 7 SP 1 Enterprise (32 位、64 位) |       |
| Sony PaSoRi RC-S380 | Windows 10 1809 (64 位)                | Windows 10 1809 (64 位)  | PCoIP |
|                     | Windows 7 SP 1 Enterprise (32 位、64 位) | Windows 10 1903 (64 位)<br>Windows 7 SP 1 Enterprise (32 位、64 位) |       |

## 配置通过 PCoIP 虚拟通道传输 USB 流量

要使用 UDP 端口 4172 配置通过 PCoIP 虚拟通道传输 USB 流量，请在 Horizon Agent 中修改相应的注册表项：

- 1 将注册表项 HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration\UsbVirtualChannelEnabled (REG\_SZ) 设置为 true。
- 2 将注册表项 HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware UsbRedirection\sideChannelType (REG\_SZ) 设置为 pcoip。
- 3 重新引导 Horizon Agent 虚拟机。

要检查配置是否已生效，请执行以下操作：

- 1 使用 PCoIP 协议连接 Horizon Agent 桌面。
- 2 从 “C:\用户\<用户名>\AppData\Local\Temp\vmware-<用户名>\vmware-UsbRedirectionClient-xxxx.log” 中查看 Horizon Client 日志。如果配置已生效，您可以在该文件中找到 “RPCManager::OnChannelDataObjectStateChanged(): Requesting virtual side channel”。

## 网络流量和 USB 重定向

客户端系统与远程桌面或应用程序之间的网络流量可以经各种路由传输，这取决于客户端系统是否位于企业网络内部以及管理员选择何种方式来设置安全性。

USB 重定向的工作方式不依赖于显示协议，并且 USB 流量通常使用 TCP 端口 32111。

如果客户端系统位于企业网络内部，从而能够在客户端与远程桌面或应用程序之间建立直接连接，则 USB 流量将使用 TCP 端口 32111。

如果客户端系统位于企业网络外部，则客户端可以通过 DMZ 中的 Unified Access Gateway 设备或安全服务器建立连接。DMZ 中的 Unified Access Gateway 设备和安全服务器在企业防火墙的保护下与连接服务器实例进行通信，并且能够保护连接服务器实例免受公共 Internet 的威胁，从而提供额外的安全保护层。

Unified Access Gateway 设备（首选方法）不需要在防火墙上为 USB 流量打开额外的端口。安全服务器需要在防火墙上为 USB 流量打开 TCP 端口 32111。有关完整的安全服务器端口要求，请参阅《Horizon 7 架构规划指南》文档中的“基于 DMZ 的安全服务器的防火墙规则”。

您可以配置通过会话增强 SDK 传输 USB 流量功能，以避免打开 TCP 端口 32111。请参阅[启用通过会话增强 SDK 传输 USB 流量功能](#)。

## 启用通过会话增强 SDK 传输 USB 流量功能

利用通过会话增强 SDK 传输 USB 流量功能，您无需为 USB 流量打开 TCP 端口 32111。RDS 主机上的虚拟桌面和已发布桌面均支持此功能。

要启用通过会话增强 SDK 传输 USB 流量功能，请在远程桌面上打开 Windows 注册表编辑器 (regedit.exe)，导航到 HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration，然后将 UsbVirtualChannelEnabled 项设置为 true。



启用此功能后，USB 流量可能使用显示协议所使用的 TCP 或 Blast 极高自适应传输 (BEAT) 连接，也可能使用专用的 TCP 或 BEAT 连接。USB 流量具体使用哪种连接取决于您的配置。

例如，采用 VMware Blast 显示协议时，USB 流量可能使用 VMware 虚拟通道 (VVC)、BEAT 侧通道或 TCP 侧通道。采用 PCoIP 显示协议时，USB 流量只使用 TCP 侧通道。

默认情况下，TCP 侧通道使用 TCP 端口 9427。VVC 和 BEAT 侧通道使用与 VMware Blast 显示协议相同的端口。

如果将 USB 流量配置为使用 VVC，则在 Windows 代理上使用 PerfMon 显示的 USB 计数器将有效。

有关采用 VMware Blast 时使用 BEAT 侧通道传输 USB 流量的信息，请参阅[USB 重定向](#)、[Windows Media Player MMR 重定向](#)或[客户端驱动器重定向](#)激活 BEAT 侧通道。

## 自动连接到 USB 设备

在某些客户端系统中，管理员和/或最终用户可以配置 USB 设备自动连接到远程桌面。可以选择在用户将 USB 设备插入客户端系统时或者客户端连接到远程桌面时进行自动连接。

在 Windows 客户端上，从 Horizon Client 4.7 开始，USB 自动连接功能（包括 URI 查询、命令行选项和组策略设置）除适用于远程桌面之外，还适用于已发布的应用程序。

某些设备（如智能手机和平板电脑）需要自动连接功能，因为它们在升级过程中会重新启动并因此断开连接。如果不将这些设备设置为自动重新连接，它们在升级期间重新启动后，将连接到本地客户端系统。

管理员在客户端上设置的或者最终用户使用 Horizon Client 菜单项设置的自动 USB 连接配置属性适用于所有 USB 设备，除非设备被配置为不包括在 USB 重定向之列。例如，在某些客户端版本中，网络摄像头和麦克风默认不包括在 USB 重定向之列，原因是这些设备通过实时音频-视频功能工作的效果更好。有时候可能默认不会将 USB 设备排除在重定向之外，而是需要管理员明确从重定向中排除设备。例如，以下类型的 USB 设备不适合 USB 重定向，不得自动连接到远程桌面或应用程序：

- **USB 以太网设备。**如果您重定向某个 USB 以太网设备，而该设备是客户端系统唯一的以太网设备，客户端可能会失去网络连接。
- **触摸屏设备。**如果您重定向触摸屏设备，远程桌面或应用程序将接收触摸输入而非键盘输入。

如果已将远程桌面或应用程序设置为自动连接 USB 设备，可以配置一条策略来排除特定设备，例如，触摸屏和网络设备。有关更多信息，请参阅[USB 设备配置过滤策略设置](#)。

在 Windows 客户端上，除了使用设置来自动连接除已排除设备之外的所有设备，您还可以在客户端上编辑配置文件，将 Horizon Client 设置为只重新连接特定的一个或多个设备，例如，智能手机和平板电脑。有关说明，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。

## 在安全的 Horizon 7 环境中部署 USB 设备

USB 设备容易受到一种称为 BadUSB 的安全威胁，这使某些 USB 设备上的固件可能受到劫持，并被恶意软件取而代之。例如，可以使设备重定向网络流量或模拟键盘并捕获按键。可以配置 USB 重定向功能以防止 Horizon 7 部署出现此安全漏洞。

通过禁用 USB 重定向，可以防止任何 USB 设备重定向到用户的远程桌面和应用程序。或者，也可以禁用特定 USB 设备的重定向，只允许用户访问其远程桌面和应用程序上的特定设备。



是否执行这些步骤取决于您组织中的安全要求。这些步骤并不是强制性的。您可以安装 USB 重定向，并保持对 Horizon 7 部署中的所有 USB 设备启用此功能。至少，要慎重考虑组织应尝试限制其暴露于此安全漏洞的程度。

## 对所有类型的设备禁用 USB 重定向

部分高度安全的环境要求您防止用户可能已连接到其客户端设备的所有 USB 设备重定向至其远程桌面和应用程序。您可以为所有桌面池、特定桌面池或桌面池中的特定用户禁用 USB 重定向。

选择以下适合您的情形的任何策略：

- 在桌面映像或 RDS 主机上安装 Horizon Agent 时，取消选中 **USB 重定向** 安装选项。（该选项默认为取消选中。）此方法可防止访问从桌面映像或 RDS 主机部署的所有远程桌面和应用程序上的 USB 设备。
- 在 Horizon Administrator 中，编辑特定池的 **USB 访问策略**，以拒绝或允许访问。通过此方法，不必更改桌面映像，且可以控制对特定桌面和应用程序池中 USB 设备的访问。

只有全局 **USB 访问策略** 可用于已发布的桌面池和应用程序池。无法为单个已发布的桌面池或应用程序池设置此策略。

- 在 Horizon Administrator 中，当您在桌面或应用程序池级别设置策略后，可以通过选择 **用户覆盖** 设置和选择用户覆盖池中特定用户的策略。
- 根据需要在 Horizon Agent 端或在客户端将 **Exclude All Devices** 策略设置为 **true**。
- 使用智能策略创建一个策略，以禁用 **USB 重定向** Horizon 策略设置。通过此方法，您可以在满足特定条件的情况下禁用特定远程桌面上的 USB 重定向。例如，您可以配置一个策略，以在用户从您的企业网络外部连接到远程桌面时禁用 USB 重定向。

如果将 **Exclude All Devices** 策略设置为 **true**，Horizon Client 会阻止重定向所有 USB 设备。您可以使用其他策略设置以允许重定向指定设备或设备系列。如果将策略设置为 **false**，Horizon Client 将允许重定向所有 USB 设备（其他策略设置阻止的设备除外）。在 Horizon Agent 和 Horizon Client 上均可以设置此策略。下表显示了如何组合可以为 Horizon Agent 和 Horizon Client 设置的 **Exclude All Devices** 策略，从而为客户端计算机生成有效的策略。默认情况下，所有 USB 设备都可以被重定向，除非设备被阻止。

**表 4-3. 结合使用排除所有设备策略的影响**

| 在 Horizon Agent 上排除所有设备策略      | 在 Horizon Client 上排除所有设备策略     | 结合使用有效的排除所有设备策略 |
|--------------------------------|--------------------------------|-----------------|
| <b>false</b> 或未定义（包含所有 USB 设备） | <b>false</b> 或未定义（包含所有 USB 设备） | 包含所有 USB 设备     |
| <b>false</b> （包含所有 USB 设备）     | <b>true</b> （排除所有 USB 设备）      | 排除所有 USB 设备     |
| <b>true</b> （排除所有 USB 设备）      | 任意或未定义                         | 排除所有 USB 设备     |

如果已将 **Disable Remote Configuration Download** 策略设置为 **true**，则 Horizon Agent 上 **Exclude All Devices** 的值不会传递给 Horizon Client，但 Horizon Agent 和 Horizon Client 会强制使用 **Exclude All Devices** 的本地值。

这些策略包含在 Horizon Agent 配置 ADMX 模板文件 (vdm\_agent.admx) 中。

## 对特定设备禁用 USB 重定向

一些用户可能必须重定向特定的本地连接的 USB 设备，以便他们可以在其远程桌面或应用程序上执行任务。例如，某医生可能必须使用录音机 USB 设备录制患者的医疗信息。在这些情况下，无法禁止访问所有 USB 设备。您可以使用组策略设置启用或禁用特定设备的 USB 重定向。

对特定设备启用 USB 重定向之前，确保您信任与您企业中客户端计算机连接的物理设备。确保您信任您的供应链。如果可能，请跟踪 USB 设备的监管链。

此外，教育员工以确保他们不会从未知源连接设备。如果可能，将环境中的设备限制为仅接受已签发的固件更新、已通过 FIPS 140-2 Level 3 认证且不支持任何种类的字段可更新固件的设备。这些类型的 USB 设备供货困难，且根据您的设备要求可能无法找到。这些选择可能不实用，但它们值得考虑。

每个 USB 设备都具有其自己的供应商及用于在计算机上进行标识的产品 ID。通过配置 Horizon Agent 配置组策略设置，可以为已知的设备类型设置包含策略。通过此方法，可以消除允许将未知设备插入环境中的风险。

例如，可以防止除已知设备供应商和产品 ID vid/pid=0123/abcd 以外的所有设备重定向至远程桌面或应用程序：

```
ExcludeAllDevices    Enabled

IncludeVidPid        o:vid-0123_pid-abcd
```

**注** 此示例中的配置提供了保护措施，但是受到威胁的设备可报告任何 vid/pid，因此仍可能会发生潜在攻击。

默认情况下，Horizon 7 会阻止特定设备系列重定向至远程桌面或应用程序。例如，阻止 HID（人机接口设备）和键盘出现在客户机中。某些已发布的 BadUSB 代码以 USB 键盘设备为目标。

您可以防止特定设备系列重定向至远程桌面或应用程序。例如，可以阻止所有视频、音频和大容量存储设备：

```
ExcludeDeviceFamily  o:video;audio;storage
```

相反，可以通过防止重定向所有设备但允许使用特定设备系列来创建白名单。例如，可以阻止除存储设备以外的所有设备：

```
ExcludeAllDevices    Enabled

IncludeDeviceFamily  o:storage
```

当远程用户登录到桌面或应用程序并使其感染时，可能会出现其他风险。您可以防止 USB 访问来自公司防火墙外部的任何 Horizon 7 连接。可以从内部（而非外部）使用 USB 设备。

请注意，如果您阻止 TCP 端口 32111 以禁止从外部访问 USB 设备，将无法进行时区同步，因为端口 32111 也用于时区同步。对于零客户端，USB 流量将嵌入到 UDP 端口 4172 上的虚拟通道中。由于端口 4172 用于显示协议以及 USB 重定向，因此无法阻止端口 4172。如果需要，可以在零客户端上禁用 USB 重定向。有关详细信息，请参见零客户端产品文献或联系零客户端供应商。

设置策略以阻止特定设备系列或特定设备，可帮助缓解被 BadUSB 恶意软件感染的风险。这些策略不会缓解所有风险，但它们是整体安全策略的有效组成部分。

## 使用日志文件进行故障排除和确定 USB 设备 ID

有用的 USB 日志文件位于客户端系统和远程桌面操作系统或 RDS 主机上。您可以利用这两个位置的日志文件进行故障排除。要找到特定设备的产品 ID，请使用客户端日志。

如果试图配置 USB 设备拆分或过滤，或者试图确定特定设备为什么未显示在 Horizon Client 菜单中，请查看客户端日志。客户端日志是针对 USB 仲裁程序和 Horizon View USB 服务生成的。Windows 和 Linux 客户端上的日志记录默认情况下处于启用状态。在 Mac 客户端上，将默认禁用日志记录。要在 Mac 客户端上启用日志记录，请参阅《适用于 Mac 的 VMware Horizon Client 安装和设置指南》文档。

配置与 USB 设备拆分和过滤相关的策略时，您设置的某些值会要求提供 USB 设备的 VID（供应商 ID）和 PID（产品 ID）。要查找 VID 和 PID，可在 Internet 上以产品名称与 vid 和 pid 的组合作为关键字进行搜索。或者，也可以在 Horizon Client 运行时将 USB 设备插入本地系统，然后在客户端日志文件中查找。下表显示了日志文件的默认位置。

**表 4-4. 日志文件位置**

| 客户端或代理        | 日志文件路径  |
|---------------|---|
| Windows 客户端   | %PROGRAMDATA%\VMware\VDM\logs\debug-*.txt<br>C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log                |
| Horizon Agent | %PROGRAMDATA%\VMware\VDM\logs\debug-*.txt   |
| Mac 客户端       | /var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log<br>/Library/Logs/VMware/vmware-usbarbitrator-xxxx.log |
| Linux 客户端     | （默认位置）/tmp/vmware-root/vmware-view-usbd-*.log   |

如果在将设备重定向到远程桌面或应用程序后设备出现问题，请检查客户端和代理端日志。

## 使用策略控制 USB 重定向

您可以为远程桌面或应用程序 (Horizon Agent) 以及 Horizon Client 配置 USB 策略。这些策略指定了客户端设备是否应将复合 USB 设备拆分为单独的组件进行重定向。您可以拆分设备来限制客户端可供重定向的 USB 设备类型，以及使 Horizon Agent 阻止从客户端计算机转发某些 USB 设备。

如果安装了较低版本的 Horizon Agent 或 Horizon Client，则并非 USB 重定向策略的所有功能都可用。此表说明了 Horizon 7 如何针对不同的 Horizon Agent 和 Horizon Client 组合应用策略。

**表 4-5. USB 策略设置的兼容性**

| Horizon Agent 版本 | Horizon Client 版本 | USB 策略设置对 USB 重定向的影响   |
|------------------|-------------------|--|
| 5.1 或更高版本        | 5.1 或更高版本         | <p>USB 策略设置同时适用于 Horizon Agent 和 Horizon Client。您可以使用 Horizon Agent USB 策略设置来阻止将 USB 设备转发到桌面。Horizon Agent 可以将设备拆分和过滤策略设置发送给 Horizon Client。您可以使用 Horizon Client USB 策略设置防止 USB 设备从客户端计算机重定向到桌面。</p> <p><b>注</b> 在 View Agent 6.1 或更高版本或 Horizon Agent 7.0 或更改版本以及 Horizon Client 3.3 或更高版本中，这些 USB 重定向策略设置适用于已发布桌面和应用程序以及在单用户计算机上运行的远程桌面。</p> |
| 5.1 或更高版本        | 5.0.x 或更低版本       | <p>USB 策略设置仅适用于 Horizon Agent。您可以使用 Horizon Agent USB 策略设置来阻止将 USB 设备转发到桌面。不可以使用 Horizon Client USB 策略设置来控制哪些设备可以从客户端计算机重定向到桌面。Horizon Client 无法从 Horizon Agent 接收设备拆分和过滤策略设置。Horizon Client 现有的 USB 重定向的注册表设置仍然有效。</p>  |
| 5.0.x 或更低版本      | 5.1 或更高版本         | <p>USB 策略设置仅适用于 Horizon Client。您可以使用 Horizon Client USB 策略设置防止 USB 设备从客户端计算机重定向到桌面。您无法使用 Horizon Agent USB 策略设置来阻止将 USB 设备转发到桌面。Horizon Agent 无法将设备拆分和过滤策略设置发送给 Horizon Client。</p>  |
| 5.0.x 或更低版本      | 5.0.x 或更低版本       | <p>USB 策略设置不适用。Horizon Client 现有的 USB 重定向的注册表设置仍然有效。</p>   |

如果您升级 Horizon Client，任何有关 USB 重定向的现有注册表设置（如 HardwareIdFilters）仍将保持有效，直到您为 Horizon Client 定义 USB 策略为止。

在不支持客户端 USB 策略的客户端设备上，可以使用适用于 Horizon Agent 的 USB 策略来控制允许将哪些 USB 设备从客户端转发到桌面或应用程序。

## 为复合 USB 设备配置设备拆分策略设置

复合 USB 设备包含两台或更多不同的设备，例如视频输入设备和存储设备或者麦克风和鼠标设备。如果您想允许一个或多个组件使用重定向功能，您可以将复合设备拆分为组件接口，禁止重定向特定接口，并允许重定向其他接口。

您可以设置一个自动拆分复合设备的策略。如果自动拆分设备功能对特定设备不起作用，或者如果自动拆分功能不生成应用程序所需的结果，您可以手动拆分复合设备。

### 自动设备拆分

如果启用了自动设备拆分功能，Horizon 7 将尝试根据生效的过滤器规则拆分复合设备中的功能或设备。例如，输入麦克风可能会自动拆分，以便鼠标设备仍作为设备的本地设备，其余的设备将转发至远程桌面。

下表介绍了 Allow Auto Device Splitting 设置的值如何确定 Horizon Client 是否尝试自动拆分复合 USB 设备。默认情况下禁用自动拆分。

**表 4-6. 结合使用禁用自动拆分策略的影响**

| 在 Horizon Agent 上允许自动设备拆分策略     | 在 Horizon Client 上允许自动设备拆分策略 | 结合使用有效的允许自动设备拆分策略 |
|---------------------------------|------------------------------|-------------------|
| Allow – Default Client Setting  | <b>false</b> （禁用自动拆分）        | 禁用自动拆分            |
| Allow – Default Client Setting  | <b>true</b> （启用自动拆分）         | 启用自动拆分            |
| Allow – Default Client Setting  | 未定义                          | 启用自动拆分            |
| Allow – Override Client Setting | 任意或未定义                       | 启用自动拆分            |
| 未定义                             | 未定义                          | 禁用自动拆分            |

**注** 这些策略包含在 Horizon Agent 配置 ADMX 模板文件中。ADMX 模板文件名为 (vdm\_agent.admx)。

默认情况下，Horizon 7 禁用自动拆分，并禁止重定向复合 USB 设备的任何音频输出设备、键盘、鼠标或智能卡组件。

Horizon 7 先应用设备拆分策略设置，然后再应用任何过滤策略设置。如果您已启用自动拆分并且没有通过指定供应商和产品 ID 来明确禁止拆分某一复合 USB 设备，Horizon 7 会检查复合 USB 设备的每个接口，并根据过滤策略设置确定应该排除或包含哪些接口。如果您已禁用自动设备拆分，并且没有明确指定要进行拆分的复合 USB 设备的供应商和产品 ID，则 Horizon 7 会将过滤策略应用到整个设备。

如果您启用了自动拆分，您可以使用 **Exclude Vid/Pid Device From Split** 策略来指定希望从拆分操作中排除的复合 USB 设备。

## 手动设备拆分

您可以使用 **Split Vid/Pid Device** 策略来指定希望拆分的复合 USB 设备的供应商和产品 ID。您还可以指定要从重定向操作中排除的复合 USB 设备组件的接口。Horizon 7 不会将任何过滤策略设置应用到您以此方式排除的组件中。

**重要事项** 如果您使用 **Split Vid/Pid Device** 策略，Horizon 7 不会自动包含您未明确排除的组件。您必须指定一个过滤策略（如 **Include Vid/Pid Device**）来包含这些组件。

**表 4-7. Horizon Agent 上设备拆分策略设置的拆分修改符**介绍了一些修改符，这些修改符可以指定当存在针对 Horizon Client 的等效设备拆分策略设置时，Horizon Client 将如何处理 Horizon Agent 设备拆分策略设置。这些修改符适用于所有设备拆分策略设置。

**表 4-7. Horizon Agent 上设备拆分策略设置的拆分修改符**

| 修改符           | 说明   |
|---------------|--|
| <b>m</b> （合并） | 除 Horizon Client 设备拆分策略设置外，Horizon Client 还会应用 Horizon Agent 设备拆分策略设置。 |
| <b>o</b> （覆盖） | Horizon Client 使用 Horizon Agent 设备拆分策略设置，而不使用 Horizon Client 设备拆分策略设置。 |

**表 4-8. 将拆分修改符应用到设备拆分策略设置的示例**举例说明了 Horizon Client 如何在您指定不同的拆分修改符时对 **Exclude Device From Split by Vendor/Product ID** 进行设置。

**表 4-8. 将拆分修改符应用到设备拆分策略设置的示例**

| 根据 Horizon Agent 上的供应商/产品 ID<br>将设备从拆分中排除 | 根据 Horizon Client 上的供应商/产品 ID<br>将设备从拆分中排除 | 根据 Horizon Client 所使用的供应商/产品<br>ID 策略设置有效地将设备从拆分中排除 |
|---|--|---|
| m:vid-XXXX_pid-XXXX                       | vid-YYYY_pid-YYYY                          | vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY                 |
| o:vid-XXXX_pid-XXXX                       | vid-YYYY_pid-YYYY                          | vid-XXXX_pid-XXXX                                   |
| m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY     | vid-YYYY_pid-YYYY                          | vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY                 |
| o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY     | vid-YYYY_pid-YYYY                          | vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY                 |

Horizon Agent 不在其所在端的连接上应用设备拆分策略设置。

Horizon Client 根据以下优先级顺序评估设备拆分策略设置。

- Exclude Vid/Pid Device From Split
- Split Vid/Pid Device

将设备从拆分操作中排除的设备拆分策略优先于任何拆分设备的策略设置。如果您将接口或设备定义为从拆分中排除，则 Horizon Client 将禁止重定向匹配的组件设备用。

## 设置策略以拆分复合 USB 设备的示例

为桌面设置拆分策略，禁止具有特定供应商和产品 ID 的设备自动拆分后进行重定向，并将这些策略传递到客户端计算机：

- 对于 Horizon Agent，请将 Allow Auto Device Splitting 策略设置为 Allow – Override Client Setting。
- 对于 Horizon Agent，请将 Exclude VidPid From Split 策略设置为 o:vid-xxx\_pid-yyyy，其中 xxx 和 yyyy 为适用的 ID。

允许桌面上的自动设备拆分功能，并在客户端计算机上为要拆分的特定设备指定策略：

- 对于 Horizon Agent，请将 Allow Auto Device Splitting 策略设置为 Allow – Override Client Setting。
- 对于客户端设备，请将 Include Vid/Pid Device 过滤策略设置为包括要拆分的特定设备，例如 vid-0781\_pid-554c。
- 对于客户端设备，请将 Split Vid/Pid Device 策略设置为 vid-0781\_pid-554c(exintf:00;exintf:01)（举例说明），以拆分指定的复合 USB 设备并禁止重定向接口 00 和接口 01。

## 为 USB 设备配置过滤策略设置

为 Horizon Agent 和 Horizon Client 配置的过滤策略设置将确定哪个 USB 设备可以从客户端计算机重定向到远程桌面或应用程序。公司通常使用 USB 设备过滤，以便禁止在远程桌面上使用大容量存储设备，或者阻止转发特定类型的设备，例如，把客户端设备连接到远程桌面的 USB 以太网适配器。



当您连接到桌面或应用程序后，Horizon Client 会下载 Horizon Agent USB 策略设置并将其与 Horizon Client USB 策略设置结合使用，以确定允许您从客户端计算机重定向哪些 USB 设备。

在应用过滤策略设置前，Horizon 7 可以应用任何设备拆分策略设置。如果您已拆分复合 USB 设备，Horizon 7 会根据过滤策略设置检查每个设备接口，以确定应排除或包含哪些接口。如果您没有拆分复合 USB 设备，Horizon 7 将对整个设备应用过滤策略设置。

设备拆分策略包含在 Horizon Agent 配置 ADMX 模板文件 (vdm\_agent.admx) 中。

## 代理强制执行的 USB 设置的交互

下表介绍了一些修改符，这些修改符可以指定当存在针对 Horizon Client 的等效过滤策略设置时，Horizon Client 将如何处理代理可强制执行的设置的 Horizon Agent 过滤策略设置。

**表 4-9. 用于代理可强制执行的设置的过滤修改符**

| 修改符           | 说明   |
|---------------|--|
| <b>m</b> (合并) | 除 Horizon Client 过滤策略设置外，Horizon Client 还会应用 Horizon Agent 过滤策略设置。对于布尔或 true/false 设置，如果未设置客户端策略，则将使用代理设置。如果设置了客户端策略，则将忽略代理设置，但 Exclude All Devices 设置除外。如果在代理端设置了 Exclude All Devices 策略，该策略将覆盖客户端设置。 |
| <b>o</b> (覆盖) | Horizon Client 使用 Horizon Agent 过滤策略设置，而不使用 Horizon Client 过滤策略设置。   |

例如，代理端上的以下策略将覆盖客户端上的任何包含规则，且仅设备 VID-0911\_PID-149a 将应用包含规则：

```
IncludeVidPid: o:VID-0911_PID-149a
```

您也可以使用星号作为通配符；例如：**o:vid-0911\_pid-\*\*\*\***

**重要事项** 如果配置代理端时不使用 **o** 或 **m** 修改符，则会将该配置规则视为无效，并将忽略它。

## 在客户端上解释的 USB 设置的交互

下表介绍了一些修改符，这些修改符可以指定 Horizon Client 将如何处理在客户端上解释的设置的 Horizon Agent 过滤策略设置。

**表 4-10. 用于在客户端上解释的设置的过滤修改符**

| 修改符                                 | 说明  |
|-------------------------------------|---|
| <b>Default</b> (注册表设置中为 <b>d</b> )  | 如果不存在 Horizon Client 过滤策略设置，Horizon Client 将使用 Horizon Agent 过滤策略设置。如果存在 Horizon Client 过滤策略设置，Horizon Client 将应用该策略设置并忽略 Horizon Agent 过滤策略设置。 |
| <b>Override</b> (注册表设置中为 <b>o</b> ) | Horizon Client 使用 Horizon Agent 过滤策略设置，而不使用任何等效的 Horizon Client 过滤策略设置。   |

Horizon Agent 在其所在端的连接上不会为在客户端上解释的设置应用过滤策略设置。

下表举例说明了在您指定不同过滤修改符时 Horizon Client 将如何处理 Allow Smart Cards 设置。



表 4-11. 将过滤修改符应用到在客户端上解释的设置的示例

| Horizon Agent 的允许智能卡设置   | Horizon Client 的允许智能卡设置 | Horizon Client 使用的有效允许智能卡策略设置 |
|--|-------------------------|-------------------------------|
| Disable – Default Client Setting<br>(注册表设置中为 <b>d:false</b> )  | <b>true</b> (允许)        | <b>true</b> (允许)              |
| Disable – Override Client Setting<br>(注册表设置中为 <b>o:false</b> ) | <b>true</b> (允许)        | <b>false</b> (禁用)             |

如果将 **Disable Remote Configuration Download** 策略设置为 **true**，Horizon Client 将忽略从 Horizon Agent 接收到的任何过滤策略设置。

Horizon Agent 始终在其所在端的连接上应用代理可强制执行的设置中的过滤策略设置，即使您将 Horizon Client 配置为使用不同的过滤策略设置或禁止 Horizon Client 从 Horizon Agent 下载过滤策略设置也是如此。Horizon Client 不报告 Horizon Agent 阻止设备被转发。

## 设置的优先级

Horizon Client 会根据优先级评估过滤策略设置。阻止匹配设备进行重定向的过滤策略设置优先于包含该设备的等效过滤策略设置。如果 Horizon Client 没有遇到排除设备的过滤策略设置，Horizon Client 将允许设备重定向，除非 **Exclude All Devices** 策略设置为了 **true**。然而，如果您已将 Horizon Agent 的过滤策略设置配置为排除设备，则桌面或应用程序将阻止向其重定向设备的所有尝试。

Horizon Client 按照优先级顺序评估过滤策略设置，并会考虑 Horizon Client 设置、Horizon Agent 设置，以及应用到 Horizon Agent 设置的修改符值。以下列表显示了优先级顺序，其中项 1 具有最高优先级。

- 1 Exclude Path
- 2 Include Path
- 3 Exclude Vid/Pid Device
- 4 Include Vid/Pid Device
- 5 Exclude Device Family
- 6 Include Device Family
- 7 Allow Audio Input Devices、Allow Audio Output Devices、Allow HIDBootable、Allow HID (Non Bootable and Not Mouse Keyboard)、Allow Keyboard and Mouse Devices、Allow Smart Cards 和 Allow Video Devices
- 8 评估结合使用的有效的 **Exclude All Devices** 策略以排除或包含所有 USB 设备

您只能为 Horizon Client 设置 **Exclude Path** 和 **Include Path** 过滤策略设置。引用单独设备系列的 **Allow** 过滤策略设置具有同等优先级。

如果配置策略设置根据供应商 ID 和产品 ID 来排除设备，那么 Horizon Client 将排除其供应商 ID 和产品 ID 与该策略设置匹配的设备，即使您可能为该设备所属的系列配置了 **Allow** 策略设置，也是如此。

策略设置的优先级顺序避免了策略设置之间的冲突。如果您将 **Allow Smart Cards** 配置为允许智能卡重定向，任何具有更高优先级的排除策略设置都将覆盖此策略。例如，您可能已将 **Exclude Vid/Pid Device** 策略设置配置为排除具有匹配路径或供应商 ID 和产品 ID 值的智能卡设备，或者也可能已配置排除整个 **Exclude Device Family** 设备系列的 **smart-card** 策略设置。

如果您配置了任何 **Horizon Agent** 过滤策略设置，**Horizon Agent** 将根据以下优先级顺序在远程桌面或应用程序上评估并强制执行过滤策略设置，其中第 1 项具有最高优先级。

- 1 **Exclude Vid/Pid Device**
- 2 **Include Vid/Pid Device**
- 3 **Exclude Device Family**
- 4 **Include Device Family**
- 5 将代理可强制执行的 **Exclude All Devices** 策略设置为排除或包含所有 USB 设备

**Horizon Agent** 将在其所在端的连接上执行过滤策略设置的此项限制设置。

通过为 **Horizon Agent** 定义过滤策略设置，您可以为非托管的客户端计算机创建过滤策略。借助该功能，还可以阻止设备从客户端计算机转发，即使 **Horizon Client** 的过滤策略设置允许该重定向，也是如此。

例如，您配置的一个策略可使 **Horizon Client** 允许某一设备重定向，如果您又配置了 **Horizon Agent** 策略来排除该设备，那么 **Horizon Agent** 将阻止该设备。

## 设置策略以过滤 USB 设备的示例

在这些示例中使用的供应商 ID 和产品 ID 只是示例。有关确定特定设备的供应商 ID 和产品 ID 的信息，请参阅[使用日志文件进行故障排除和确定 USB 设备 ID](#)。

- 在客户端上，禁止特定设备进行重定向：

```
Exclude Vid/Pid Device:    Vid-0341_Pid-1a11
```

- 阻止所有存储设备重定向到此桌面或应用程序池。使用代理端设置：

```
Exclude Device Family:    o:storage
```

- 对于桌面池中的所有用户，阻止音频和视频设备，以确保这些设备将始终可用于实时音频-视频功能。使用代理端设置：

```
Exclude Device Family:    o:video;audio
```

请注意，还有另一种策略，那就是按供应商 ID 和产品 ID 来排除特定设备。

- 在客户端上，阻止所有设备重定向，但一个特定设备除外：

```
Exclude All Devices:      true
Include Vid/Pid Device:    Vid-0123_Pid-abcd
```

- 排除由特定公司制造的所有设备，因为这些设备会给您的最终用户带来问题。使用代理端设置：

```
Exclude Vid/Pid Device:    o:Vid-0341_Pid-*
```

- 在客户端上，包括两个特定设备，但排除所有其他设备：

```
Exclude All Devices:      true
Include Vid/Pid Device:    Vid-0123_Pid-abcd;Vid-1abc_Pid-0001
```

## USB 设备系列

在为 Horizon Client、View Agent 或 Horizon Agent 创建 USB 筛选规则时，可以指定 USB 设备系列。

**注** 有些设备不报告设备系列。

**表 4-12. USB 设备系列**

| 设备系列名称       | 说明                        |
|--------------|---------------------------|
| audio        | 任一音频输入或音频输出设备。            |
| audio-in     | 音频输入设备，例如麦克风。             |
| audio-out    | 音频输出设备，例如扬声器和耳机。          |
| bluetooth    | 通过蓝牙连接的设备。                |
| comm         | 通信设备，例如调制解调器和有线网络适配器。     |
| hid          | 除键盘和指针设备之外的人机接口设备。        |
| hid-bootable | 启动时除键盘和指针设备之外的其他可用人机接口设备。 |
| imaging      | 图像处理设备，例如扫描仪。             |
| keyboard     | 键盘设备。                     |
| mouse        | 指针设备，例如鼠标。                |
| other        | 未指定设备系列。                  |
| pda          | 个人数字助理。                   |
| physical     | 力反馈设备，例如力反馈操纵杆。           |
| printer      | 打印设备。                     |
| security     | 安全设备，例如指纹识别器。             |
| smart-card   | 智能卡设备。                    |
| storage      | 大容量存储设备，例如闪存和外接硬盘。        |
| unknown      | 设备系列未知。                   |
| vendor       | 具备供应商专有功能的设备。             |
| video        | 视频输入设备。                   |
| wireless     | 无线网络适配器。                  |
| wusb         | 无线 USB 设备。                |

## Horizon Agent 配置 ADMX 模板中的 USB 设置

您可以为 Horizon Agent 和 Horizon Client 定义 USB 策略设置。连接后，Horizon Client 将从 Horizon Agent 下载 USB 策略设置，并将其与 Horizon Client USB 策略设置配合使用以确定允许哪些设备从客户端计算机进行重定向。

Horizon Agent 配置 ADMX 模板文件包含与 Horizon Agent 的身份验证和环境组件相关的策略设置，包括 USB 重定向。ADMX 模板文件名为 (vdm\_agent.admx)。该设置适用于计算机级别。Horizon Agent 优先从计算机级别的 GPO 中读取设置，其次从位于 HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\USB 的注册表中读取。

### 用于配置 USB 设备拆分的设置

下表介绍了 Horizon Agent 配置 ADMX 模板文件中拆分复合 USB 设备的各个策略设置。所有这些设置位于组策略管理编辑器的 **VMware Horizon Agent 配置 > View USB 配置 > 仅客户端可下载设置** 文件夹中。Horizon Agent 不会强制执行这些设置。Horizon Agent 会将这些设置传递到 Horizon Client，并根据您是指定合并 (m) 还是覆盖 (o) 修改符来解释和执行。Horizon Client 使用这些设置来确定是否将复合 USB 设备拆分为组件设备以及是否禁止组件设备用于重定向。有关 Horizon 如何应用策略以拆分复合 USB 设备的说明，请参阅[为复合 USB 设备配置设备拆分策略设置](#)。

**表 4-13. Horizon Agent 配置模板：设备拆分设置**

| 设置  | 属性   |
|---|--|
| Allow Auto Device Splitting<br>属性: AllowAutoDeviceSplitting | 允许复合 USB 设备的自动拆分。<br>未定义默认值，相当于 <b>false</b> 。   |
| Exclude Vid/Pid Device from Split<br>属性: SplitExcludeVidPid | 从拆分中排除供应商和产品 ID 指定的复合 USB 设备。设置的格式为 {m o}:vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...<br>您必须以十六进制格式指定 ID 号。可以使用通配符 (*) 代替 ID 中的单个数字。<br>例如: <b>o:vid-0781_pid-55**</b><br>未定义默认值。   |
| Split Vid/Pid Device<br>属性: SplitVidPid                     | 将供应商和产品 ID 指定的复合 USB 设备组件视为单独设备。设置的格式为 {m o}:vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww])<br>或<br>{m o}:vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww])<br>可以使用 exintf 关键字通过指定接口号禁止重定向组件。您必须以十六进制格式指定 ID 号，以十进制格式（包含前导零）指定接口号。可以使用通配符 (*) 代替 ID 中的单个数字。<br>例如: <b>o:vid-0781_pid-554c(exintf:01;exintf:02)</b><br><br><b>注</b> Horizon 7 不会自动包含您未明确排除的组件。您必须指定一个筛选策略（如 Include Vid/Pid Device）来包含这些组件。<br><br>未定义默认值。 |

## Horizon Agent 强制执行的 USB 设置

下表介绍了 Horizon Agent 配置 ADMX 模板文件中代理强制执行的各个 USB 策略设置。所有这些设置位于组策略管理编辑器的 **VMware Horizon Agent 配置 > View USB 配置** 文件夹中。Horizon Agent 使用这些设置来确定是否能够将 USB 设备转发至主机。Horizon Agent 还会将这些设置传递到 Horizon Client，并根据您是指定合并 (m) 还是覆盖 (o) 修改符来解释和执行。Horizon Client 使用这些设置来确定 USB 设备是否可以重定向。由于 Horizon Agent 始终执行您指定的代理强制执行的策略设置，其影响可能会抵消您为 Horizon Client 设置的策略。有关 Horizon 7 如何应用策略以筛选 USB 设备的说明，请参阅[USB 设备配置过滤策略设置](#)。

**表 4-14. Horizon Agent 配置模板：代理强制执行的设置**

| 设置   | 属性  |
|--|---|
| Exclude All Devices<br>属性: ExcludeAllDevices | 禁止转发所有 USB 设备。如果设置为 <b>true</b> ，您可以使用其他策略设置以允许特定设备或设备系列被转发。如果设置为 <b>false</b> ，您可以使用其他策略设置以防止特定设备或设备系列被转发。<br><br>如果设置为 <b>true</b> 并传递至 Horizon Client，该设置总是覆盖 Horizon Client 上的设置。您无法通过该设置使用合并 (m) 或覆盖 (o) 修改符。<br><br>未定义默认值，相当于 <b>false</b> 。 |
| Exclude Device Family<br>属性: ExcludeFamily   | 禁止设备系列被转发。设置的格式为 {m o}:family_name_1[;family_name_2]...<br>例如: <b>o:bluetooth;smart-card</b><br><br>如果您启用了自动设备拆分，则 Horizon 7 会检查复合 USB 设备每个接口的设备系列，确定应排除哪些接口。如果您禁用了自动设备拆分，则 Horizon 7 会检查整个复合 USB 设备的设备系列。<br><br>未定义默认值。                           |
| Exclude Vid/Pid Device<br>属性: ExcludeVidPid  | 禁止具有指定供应商和产品 ID 的设备被转发。设置的格式为 {m o}:vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...<br>您必须以十六进制格式指定 ID 号。可以使用通配符 (*) 代替 ID 中的单个数字。<br>例如: <b>m:vid-0781_pid-****;vid-0561_pid-554c</b><br><br>未定义默认值。  |
| Include Device Family<br>属性: IncludeFamily   | 包含可以被转发的设备系列。设置的格式为 {m o}:family_name_1[;family_name_2]...<br>例如: <b>m:storage</b><br><br>未定义默认值。   |
| Include Vid/Pid Device<br>属性: IncludeVidPid  | 包含可被转发的具有指定供应商和产品 ID 的设备。设置的格式为 {m o}:vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...<br>您必须以十六进制格式指定 ID 号。可以使用通配符 (*) 代替 ID 中的单个数字。<br>例如: <b>o:vid-0561_pid-554c</b><br><br>未定义默认值。  |

## 在客户端上解释的 USB 设置

下表介绍了 Horizon Agent 配置 ADMX 模板文件中在客户端上解释的各个策略设置。所有这些设置位于组策略管理编辑器的 **VMware Horizon Agent 配置 > View USB 配置 > 仅客户端可下载设置** 文件夹中。Horizon Agent 不会强制执行这些设置。Horizon Agent 会将这些设置传递到 Horizon Client 进行解释和执行。Horizon Client 使用这些设置来确定 USB 设备是否可以重定向。

**表 4-15. Horizon Agent 配置模板：在客户端上解释的设置**

| 设置   | 属性   |
|--|--|
| Allow Audio Input Devices<br>属性: AllowAudioIn              | 允许转发音频输入设备。<br>未定义默认值，相当于 <b>true</b> 。                                    |
| Allow Audio Output Devices<br>属性: AllowAudioOut            | 允许转发音频输出设备。<br>未定义默认值，相当于 <b>false</b> 。                                   |
| Allow HID-Bootable<br>属性: AllowHIDBootable                 | 允许转发引导时可用的输入设备（也称为可引导的 <b>hid</b> 设备），键盘或鼠标除外。<br>未定义默认值，相当于 <b>true</b> 。 |
| Allow Other Input Devices                                  | 允许转发输入设备（可引导的 <b>hid</b> 设备和具有集成指针设备的键盘）。<br>未定义默认值。                       |
| Allow Keyboard and Mouse Devices<br>属性: AllowKeyboardMouse | 允许转发具有集成指针设备（如鼠标、轨迹球或触摸板）的键盘。<br>未定义默认值，相当于 <b>false</b> 。                 |
| Allow Smart Cards<br>属性: AllowSmartcard                    | 允许转发智能卡设备。<br>未定义默认值，相当于 <b>false</b> 。                                    |
| Allow Video Devices<br>属性: AllowVideo                      | 允许转发视频设备。<br>未定义默认值，相当于 <b>true</b> 。                                      |

## 排除 USB 重定向故障

在 Horizon Client 中进行 USB 重定向时可能会出现各种问题。

### 问题

Horizon Client 中的 USB 重定向功能无法为远程桌面或应用程序启用本地设备，或是某些设备看上去无法用于 Horizon Client 重定向。

### 原因

USB 重定向可能会由于以下原因而无法正确或按预期运行。

- 该设备是复合 USB 设备且所包含的其中一个设备被默认阻止。例如，默认情况下，包含鼠标的语音输入设备由于鼠标设备被默认阻止而被阻止。要解决此问题，请参阅[为复合 USB 设备配置设备拆分策略设置](#)。
- 在部署已发布桌面和应用程序的 Windows Server 2008 RDS 主机上不支持 USB 重定向。
- 设备无法正常使用 USB 重定向，或已发布的桌面和应用程序不支持该功能。有关更多信息，请参阅[USB 设备类型的相关限制](#)。
- 网络摄像头不支持重定向。
- 音频 USB 设备的重定向不稳定，具体取决于网络状况。有些设备即使在闲置状态下也要求具备高数据吞吐量。

- 引导设备不支持 USB 重定向。如果在通过 USB 设备引导的 Windows 系统上运行 Horizon Client，而且将该设备重定向到远程桌面，本地操作系统就可能无法响应或不可用。请参阅 <http://kb.vmware.com/kb/1021409>。
- 默认情况下，Horizon Client for Windows 不允许您选择键盘、鼠标、智能卡和音频输出设备进行重定向。请参阅 <http://kb.vmware.com/kb/1011600>。
- RDP 不支持用于控制台会话的 USB HID 或智能卡读卡器的重定向。请参阅 <http://kb.vmware.com/kb/1011600>。
- Windows Mobile 设备中心可阻止 RDP 会话中的 USB 设备重定向。请参阅 <http://kb.vmware.com/kb/1019205>。
- 对于某些 USB HID，您必须配置虚拟机来更新鼠标指针的位置。请参阅 <http://kb.vmware.com/kb/1022076>。
- 某些音频设备可能需要对策略设置或注册表设置进行更改。请参阅 <http://kb.vmware.com/kb/1023868>。
- 网络延迟可能造成设备交互缓慢，或导致应用程序因与本地设备交互而表现为冻结。大型 USB 磁盘驱动器可能需要几分钟才会显示在 Windows 资源管理器中。
- 使用 FAT32 文件系统格式化的 USB 闪存卡加载速度很慢。请参阅 <http://kb.vmware.com/kb/1022836>。
- 在连接到远程桌面或应用程序之前，本地系统上的某个进程或服务已打开该设备。
- 如果重新连接到桌面或应用程序会话，则已重定向的 USB 设备将停止运行，即使桌面或应用程序显示该设备可用。
- 在 Horizon Administrator 中禁用了 USB 重定向。
- 客户机上缺少或禁用了 USB 重定向驱动程序。

## 解决方案

- ◆ 如果可能，请使用 VMware Blast 或 PCoIP 作为协议，而不使用 RDP。
- ◆ 如果临时断开连接后重定向的设备仍然不可用或停止工作，则需要拔出并重新插入该设备，然后重新尝试重定向。
- ◆ 在 Horizon Administrator 中，转到**策略 > 全局策略**，然后确认已将“View 策略”下的 USB 访问设置为允许。
- ◆ 检查客户机上的日志中的 ws\_vhub 类的条目，以及客户端上的日志中的 vmware-view-usbd 类的条目。  
如果用户不是管理员，或者 USB 重定向驱动程序未安装或不能正常运行，这些分类的条目将被写入日志中。有关这些日志文件的位置，请参阅[使用日志文件进行故障排除和确定 USB 设备 ID](#)。
- ◆ 打开客户机上的“设备管理器”，展开“通用串行总线控制器”，重新安装（如已丢失）或启用（如被禁用）VMware View 虚拟 USB 主机控制器和 VMware View 虚拟 USB 集线器驱动程序。



## 配置桌面和应用程序池的策略

您可以配置策略来控制桌面和应用程序池、计算机和用户的行为。使用 **Horizon Administrator** 可设置客户端会话策略。您可以使用 **Active Directory** 组策略设置来控制 **Horizon Agent**、适用于 Windows 的 **Horizon Client**，以及影响单个用户计算机、RDS 主机、PCoIP 或 VMware Blast 的功能的行为。

本章讨论了以下主题：

- 在 **Horizon Administrator** 中设置策略
- 使用 智能策略
- 使用 **Active Directory** 组策略
- 使用 **Horizon 7** 组策略管理模板文件
- **Horizon 7 ADMX** 模板文件
- 将 **ADMX** 模板文件添加到 **Active Directory**
- **VMware View Agent** 配置 **ADMX** 模板设置
- 会话协作策略设置
- 客户端驱动器重定向策略设置
- **VMware HTML5** 功能策略设置
- 适用于 **Skype for Business** 的 **VMware Virtualization Pack** 策略设置
- **VMware Horizon** 性能跟踪器策略设置
- **VMware** 集成打印策略设置
- **PCoIP** 策略设置
- **VMware Blast** 策略设置
- 使用远程桌面服务组策略
- 为虚拟打印筛选打印机
- 设置基于位置的打印
- 管理特殊的 **Unity** 窗口
- **Active Directory** 组策略示例

## 在 Horizon Administrator 中设置策略

您可以使用 Horizon Administrator 配置客户端会话策略。

您可以将这些策略设置为影响特定用户、特定桌面池或所有客户端会话用户。影响特定用户和桌面池的策略称为用户级别策略和桌面池级别策略。影响所有会话和用户的策略称为全局策略。

用户级别策略将从等效的桌面池级别策略设置继承设置。同样，桌面池级别策略将从等效的全局策略设置继承设置。桌面池级别策略设置优先于等效的全局策略设置。用户级别策略设置优先于等效的全局和池级别策略设置。

低级别策略设置可能比等效的高级别设置或多或少地要严格。例如，您可以将某个全局策略设置为**拒绝**，并将等效的桌面池级别策略设置为**允许**，反之亦然。

---

**注** 仅全局策略适用于已发布的桌面和应用程序池。无法为已发布的桌面和应用程序池设置用户级别的策略或池级别的策略。

---

### 配置全局策略设置

您可以配置全局策略以控制所有客户端会话用户的行为。

#### 前提条件

请熟悉策略描述。请参阅 [Horizon 7 策略](#)。

#### 步骤

- 1 在 Horizon Administrator 中，选择**策略 > 全局策略**。
- 2 单击**查看策略**窗格中的 **View 策略**。
- 3 单击**确定**保存更改。

### 配置桌面池策略

您可以配置桌面级策略以影响特定桌面池。桌面级策略设置优先于等效的全局策略设置。

#### 前提条件

请熟悉策略描述。请参阅 [Horizon 7 策略](#)。

#### 步骤

- 1 在 Horizon Administrator 中，选择**目录 > 桌面池**。
- 2 双击所需桌面池的 ID，然后单击**策略**选项卡。  
**策略**选项卡将显示当前的池策略设置。如果设置是从等效的全局策略继承而来，**桌面池策略**列中会显示**继承**。
- 3 单击**查看策略**窗格中的 **View 策略**。
- 4 单击**确定**保存更改。

## 配置用户策略

您可以配置用户级别策略以影响特定用户。用户级别策略设置始终优先于等效的全局和桌面池级别策略设置。

### 前提条件

请熟悉策略描述。请参阅 [Horizon 7 策略](#)。

### 步骤

1 在 Horizon Administrator 中，选择目录 > 桌面池。

2 双击所需桌面池的 ID，然后单击策略选项卡。

策略选项卡将显示当前的池策略设置。如果设置是从等效的全局策略继承而来，桌面池策略列中会显示继承。

3 单击用户覆盖，然后单击添加用户。

4 要查找用户，请单击添加，键入用户的名称和描述，然后单击查找。

5 从列表中选择一个或多个用户，单击确定，然后单击下一步。

屏幕上将显示“添加单个策略”对话框。

6 配置 Horizon 策略并单击完成保存更改。

## Horizon 7 策略

您可以将 Horizon 7 策略配置为影响所有客户端会话，或者只影响特定桌面池或用户。

下表介绍了每项 Horizon 7 策略设置。

表 5-1. Horizon 策略

| 策略           | 说明  |
|--------------|---|
| 多媒体重定向 (MMR) | <p>确定是否为客户端系统启用 MMR。</p> <p>MMR 是一种 Windows Media Foundation 过滤器，可直接通过 TCP 套接字将多媒体数据从远程桌面中的特定编解码器转发至客户端系统。随后，直接在播放数据的客户端系统中解码数据。</p> <p>默认值为拒绝。</p> <p>如果客户端系统没有足够的资源来处理本地多媒体解码，请将设置保留为拒绝。</p> <p>多媒体重定向 (MMR) 数据在不采用应用程序加密的情况下跨网络传输，其中可能包含敏感数据，具体取决于被重定向的内容。为确保无法在网络上监视此数据，请仅在安全网络中使用 MMR。</p> |
| USB 访问       | <p>确定远程桌面是否可以使用 USB 设备连接客户端系统。</p> <p>默认值为允许。如果出于安全因素阻止使用外部设备，请将设置更改为拒绝。</p>  |
| PCoIP 硬件加速   | <p>确定是否启用 PCoIP 显示协议的硬件加速，指定分配给 PCoIP 用户会话的加速优先级。</p> <p>仅在托管远程桌面的物理机中装有 PCoIP 硬件加速设备时，此设置才有效。</p> <p>默认值为允许，优先级为中。</p>   |

## 使用 智能策略

您可以使用智能策略创建一些策略，用来控制特定远程桌面上 USB 重定向、虚拟打印、剪贴板重定向、客户端驱动器重定向和 PCoIP 显示协议功能的行为。您还可以使用智能策略创建一些策略，用来控制已发布的应用程序的行为。

使用智能策略，可以创建仅在满足特定条件时才会生效的策略。例如，可以配置这样一个策略：当用户从企业网络外部连接到远程桌面时，禁用客户端驱动器重定向功能。

## 智能策略的要求

要使用智能策略，您的 Horizon 7 环境必须满足特定的要求。

- 必须在要通过智能策略进行管理的远程桌面上安装 Horizon Agent 7.0 或更高版本以及 VMware User Environment Manager 9.0 或更高版本。
- 用户必须使用 Horizon Client 4.0 或更高版本连接到要通过智能策略进行管理的远程桌面。

## 安装 User Environment Manager

要使用智能策略控制远程桌面上远程桌面功能的行为，您必须在远程桌面上安装 User Environment Manager 9.0 或更高版本。

您可以从 VMware 下载页面下载 User Environment Manager 安装程序。您必须在要通过 User Environment Manager 进行管理的每个远程桌面上安装 VMware UEM FlexEngine。您可以在要从中管理 User Environment Manager 环境的任何桌面上安装 User Environment Manager 管理控制台组件。

对于链接克隆池，可在用作链接克隆的基础映像的父虚拟机中安装 User Environment Manager。对于 RDS 桌面池，可在提供已发布桌面会话的 RDS 主机上安装 User Environment Manager。

有关 User Environment Manager 系统要求和完整的安装说明，请参阅《安装和配置 VMware User Environment Manager》文档。

## 配置 User Environment Manager

您必须先配置 User Environment Manager，才能使用它为远程桌面功能创建智能策略。

要配置 User Environment Manager，请按照《VMware User Environment Manager 管理指南》中的配置说明进行操作。以下配置步骤是对该文档中的信息所做的补充。

要配置 User Environment Manager，请按照《VMware User Environment Manager 管理指南》中的配置说明进行操作。

- 在远程桌面上配置 VMware UEM FlexEngine 客户端组件时，需创建 FlexEngine 登录和注销脚本。对于多个会话，例如，RDSH 桌面和 RDSH 应用程序，或者同一 RDSH 主机上同一用户的多个 RDSH 应用程序会话，请在登录脚本中使用 **-HorizonViewMultiSession -r** 参数。对于注销脚本，请使用 **-HorizonViewMultiSession -s** 参数。

---

**注** 请勿使用登录脚本在远程桌面上启动其他应用程序。额外的登录脚本可能会使远程桌面登录延迟长达 10 分钟。

---

- 在远程桌面上启用用户组策略设置同步运行登录脚本。此设置位于 `User Configuration\Policies\Administrative Templates\System\Scripts` 文件夹中。
- 在远程桌面上启用计算机组策略设置计算机启动和登录时总是等待网络。此设置位于 `Computer Configuration\Administrative Template\System\Logon` 文件夹中。
- 对于 Windows 8.1 远程桌面，禁用计算机组策略设置配置登录脚本延迟。此设置位于 `Computer Configuration\Administrative Templates\System\Group Policy` 文件夹中。
- 要确保在用户重新连接到桌面会话时刷新 Horizon 智能策略设置，需使用 User Environment Manager 管理控制台创建一个触发任务。可将触发器设置为**重新连接会话**，将操作设置为**用户环境刷新**，并为此刷新选择 **Horizon 智能策略**。

**注** 如果在创建触发任务时用户已登录到远程桌面，则该用户必须从桌面注销才能使触发任务生效。

## Horizon 智能策略设置

您可以通过创建 Horizon 智能策略来控制 User Environment Manager 中远程功能的行为。

表 5-2. Horizon 智能策略设置描述了在 User Environment Manager 中定义 Horizon 智能策略时可选择的设置。

**表 5-2. Horizon 智能策略设置**

| 设置        | 说明   |
|-----------|--|
| USB 重定向   | 确定是否在远程桌面上启用 USB 重定向。通过 USB 重定向功能，用户可以从远程桌面使用本地连接的 USB 设备，如闪存、照相机和打印机。如果使用智能策略配置 USB 重定向，您必须使用 User Environment Manager 9.5 或更高版本。   |
| 打印        | 确定是否在远程桌面上启用了虚拟打印功能或 VMware 虚拟打印。通过虚拟打印功能，用户可以从远程桌面打印到虚拟打印机或与客户端计算机连接的 USB 打印机。VMware 虚拟打印可将客户端打印机重定向到代理系统。  |
| 剪贴板       | <p>确定允许执行剪贴板重定向的方向。您可以选择以下值之一：</p> <ul style="list-style-type: none"> <li>■ <b>禁用</b>。双向禁用剪贴板重定向。</li> <li>■ <b>允许全部</b>。启用剪贴板重定向。用户可以在客户端系统和远程桌面之间来回复制并粘贴内容。</li> <li>■ <b>允许从客户端复制到代理</b>。用户只能从客户端系统向远程桌面复制并粘贴内容。</li> <li>■ <b>允许从代理复制到客户端</b>。用户只能从远程桌面向客户端系统复制并粘贴内容。</li> </ul>   |
| 客户端驱动器重定向 | <p>确定是否在远程桌面上启用客户端驱动器重定向，以及共享的驱动器和文件夹是否可写入。您可以选择以下值之一：</p> <ul style="list-style-type: none"> <li>■ <b>禁用</b>。在远程桌面上禁用客户端驱动器重定向。</li> <li>■ <b>允许全部</b>。客户端驱动器和文件夹与远程桌面共享，并且可以读取和写入。</li> <li>■ <b>只读</b>。客户端驱动器和文件夹与远程桌面共享，并且可以读取，但不可写入。</li> </ul> <p>如果未配置此设置，则共享的驱动器和文件夹是否可写入将取决于本地注册表设置。有关更多信息，请参阅<a href="#">使用注册表设置配置客户端驱动器重定向</a>。</p> |

| 设置               | 说明  |
|------------------|---|
| 拖放               | <p>确定是否可以在客户端系统与远程桌面或已发布的应用程序之间拖放支持的数据类型。您可以选择以下值之一：</p> <ul style="list-style-type: none"> <li>■ <b>禁用</b>。在远程桌面或已发布应用程序上禁用拖放功能。</li> <li>■ <b>允许全部</b>。可以从客户端系统拖放到远程桌面或已发布的应用程序，也可以从远程桌面或已发布的应用程序拖放到客户端系统。</li> <li>■ <b>允许从客户端拖放到代理</b>。只能从客户端系统拖放到远程桌面或已发布的应用程序。</li> <li>■ <b>允许从代理拖放到客户端</b>。只能从远程桌面或已发布的应用程序拖放到客户端系统。</li> </ul> |
| 带宽配置文件           | <p>配置远程桌面上 PCoIP 和 Blast 会话的带宽配置文件。您可以选择预定义的带宽配置文件，例如 <b>LAN</b>。如果选择预定义的带宽配置文件，则可阻止代理尝试以高于链路容量的速率传输数据。如果选择默认配置文件，则最大带宽为每秒 90000 千比特。</p> <p>有关更多信息，请参阅<a href="#">带宽配置文件引用</a>。</p>  |
| HTML Access 文件传输 | 确定如何在客户端与代理之间传输 HTML 文件。  |

总之，为 User Environment Manager 中的远程功能配置的 Horizon 智能策略设置会覆盖任何等效的注册表项和组策略设置。

## 带宽配置文件引用

通过智能策略，您可以使用带宽配置文件策略设置为远程桌面上的 PCoIP 或 Blast 会话配置带宽配置文件。

表 5-3. 带宽配置文件

| 带宽配置文件 | 最大会话 BW (Kbps) | 最小会话 BW (Kbps) | 启用无损构建 (BTL) | 最高初始图像质量 | 最低图像质量 | 最大 FPS | 最大音频 BW (Kbps) | 图像质量性能 |
|--------|----------------|----------------|--------------|----------|--------|--------|----------------|--------|
| 高速 LAN | 900000         | 64             | 是            | 100      | 50     | 60     | 1600           | 50     |
| LAN    | 900000         | 64             | 是            | 90       | 50     | 30     | 1600           | 50     |
| 专用 WAN | 900000         | 64             | 否            | 80       | 40     | 30     | 500            | 50     |
| 宽带 WAN | 5000           | 64             | 否            | 70       | 40     | 20     | 500            | 50     |
| 低速 WAN | 2000           | 64             | 否            | 70       | 30     | 15     | 200            | 25     |
| 超低速连接  | 1000           | 64             | 否            | 70       | 30     | 10     | 90             | 0      |

## 将条件添加到 Horizon 智能策略定义

在 User Environment Manager 中定义 Horizon 智能策略时，可以添加要使策略生效所必须满足的条件。例如，您可以添加一个条件，以便仅当用户从企业网络外部连接到远程桌面时，才禁用客户端驱动器重定向功能。

您可以为同一远程桌面功能添加多个条件。例如，您可以添加一个条件，以便当用户是 HR 组成员时启用本地打印，同时再添加另一个条件，以便当远程桌面位于 Win7 池时也启用本地打印。

有关在 User Environment Manager 管理控制台中添加和编辑条件的详细信息，请参阅《VMware User Environment Manager 管理指南》。

## 使用 Horizon Client 属性条件

当用户连接或重新连接到远程桌面时，Horizon Client 会收集有关客户端计算机的信息，然后连接服务器会将这些信息发送到远程桌面。您可以将 Horizon Client 属性条件添加到 Horizon 策略定义，以根据远程桌面收到的信息控制策略生效时间。

**注** 仅当用户通过 PCoIP 显示协议或 VMware Blast 显示协议启动远程桌面时，Horizon Client 属性条件才会生效。如果用户通过 RDP 显示协议启动远程桌面，则 Horizon Client 属性条件不会生效。

**表 5-4. Horizon Client 属性条件的预定义属性** 描述了在您使用 Horizon Client 属性条件时，可从属性下拉菜单中选择的预定义属性。每个预定义属性均对应一个 ViewClient\_ 注册表项。

**表 5-4. Horizon Client 属性条件的预定义属性**

| 属性    | 对应的注册表项                           | 说明   |
|-------|-----------------------------------|--|
| 客户端位置 | ViewClient_Broker_GatewayLocation | <p>指定用户客户端系统的位置。有效值如下：</p> <ul style="list-style-type: none"> <li>■ “内部” - 仅当用户从企业网络内部连接到远程桌面时，策略才会生效。</li> <li>■ “外部” - 仅当用户从企业网络外部连接到远程桌面时，策略才会生效。</li> </ul> <p>有关为连接服务器或安全服务器主机设置网关位置的信息，请参阅《Horizon 7 管理指南》文档。</p> <p>有关为 Access Point 设备设置网关位置的信息，请参阅《部署和配置 Unified Access Gateway》文档。</p> |
| 启动标记  | ViewClient_Launch_Matched_Tags    | <p>指定一个或多个标记。用逗号或分号分隔多个标记。仅当允许远程桌面或应用程序启动发生的标记与指定的某个标记相匹配时，策略才会生效。</p> <p>有关将标记分配给连接服务器实例和桌面池的信息，请参阅您的设置文档。</p>  |
| 池名称   | ViewClient_Launch_ID              | <p>指定桌面或应用程序池 ID。仅当用户在启动远程桌面或应用程序时选择的桌面或应用程序池 ID 与指定的桌面或应用程序池 ID 相匹配时，策略才会生效。例如，如果用户选择了 Win7 池，并且此属性也设置为 Win7，则策略便会生效。</p> <p><b>注</b> 如果在同一个 RDS 主机会话中启动了多个应用程序池，则值为从 Horizon Client 启动的第一个应用程序的 ID。</p>  |

属性下拉菜单也是一个文本框，您可以在该文本框中手动输入任何 ViewClient\_ 注册表项。在输入注册表项时，请勿包含 ViewClient\_ 前缀。例如，要指定 ViewClient\_Broker\_URL，只需输入 Broker\_URL 即可。

您可以在远程桌面上使用 Windows 注册表编辑器 (regedit.exe) 查看 ViewClient\_ 注册表项。Horizon Client 会将客户端计算机信息写入在单用户计算机上部署的远程桌面的系统注册表路径 HKEY\_CURRENT\_USER\Volatile Environment。对于在 RDS 会话中部署的远程桌面，Horizon Client 会将客户端计算机信息写入系统注册表路径 HKEY\_CURRENT\_USER\Volatile Environment\x，其中 x 是 RDS 主机上的会话 ID。



## 使用其他条件

User Environment Manager 管理控制台提供了许多条件。在为远程桌面功能创建策略时，以下条件可能会特别有用。

|        |   |
|--------|---|
| 组成员    | 您可以使用此条件配置策略，使其仅当用户是特定组的成员时才生效。                                     |
| 远程显示协议 | 您可以使用此条件配置策略，使其仅当用户选择特定显示协议时才生效。条件设置包括 RDP、PCoIP 和 Blast。           |
| IP 地址  | 您可以使用此条件配置策略，使其仅当用户从企业网络内部或外部连接时才生效。使用条件设置可指定内部 IP 地址范围或外部 IP 地址范围。 |

---

**注** 您还可以在 Horizon Client 属性条件中使用客户端位置属性。

---

有关所有可用条件的描述，请参阅《VMware User Environment Manager 管理指南》文档。

## 在 User Environment Manager 中创建 Horizon 智能策略

您可以使用 User Environment Manager 管理控制台在 User Environment Manager 中创建 Horizon 智能策略。在定义 Horizon 智能策略时，您可以添加要使智能策略生效所必须满足的条件。

### 前提条件

- 安装并配置 User Environment Manager。请参阅[安装 User Environment Manager](#)和[配置 User Environment Manager](#)。
- 熟悉 Horizon 智能策略设置。请参阅[Horizon 智能策略设置](#)。
- 熟悉可添加到 Horizon 智能策略定义的条件。请参阅[将条件添加到 Horizon 智能策略定义](#)。

有关使用 User Environment Manager 管理控制台的完整信息，请参阅《VMware User Environment Manager 管理指南》文档。

### 步骤

- 1 在 User Environment Manager 管理控制台中，选择**用户环境**选项卡，然后单击树视图中的 **Horizon 智能策略**。

现有的 Horizon 智能策略定义（如果有）会显示在“Horizon 智能策略”窗格中。

- 2 右键单击 **Horizon 智能策略**，并选择**创建 Horizon 智能策略定义**，以创建新的智能策略。

此时会显示“Horizon 智能策略”对话框。

- 3 选择**设置**选项卡，并定义智能策略设置。

- a 在“常规设置”部分的**名称**文本框中，输入智能策略的名称。

例如，如果智能策略会影响客户端驱动器重定向功能，可以将智能策略命名为 CDR。

- b 在“Horizon 智能策略设置”部分，选择要包含在智能策略中的远程桌面功能和设置。

您可以选择多个远程桌面功能。

- 4 （可选）要向智能策略中添加条件，请选择**条件**选项卡，单击**添加**，然后选择一个条件。

您可以向智能策略定义中添加多个条件。

- 5 单击**保存**以保存智能策略。

User Environment Manager 会在用户每次连接或重新连接到远程桌面时处理 Horizon 智能策略。

User Environment Manager 按照智能策略名称的字母顺序处理多个智能策略。Horizon 智能策略将按字母顺序显示在“Horizon 智能策略”窗格中。如果智能策略发生冲突，则最后处理的智能策略具有较高优先级。例如，如果您有一个名为 Sue 的智能策略对名为 Sue 的用户启用 USB 重定向，同时还有另一个名为 Pool 的智能策略对名为 Win7 的桌面池禁用 USB 重定向，则在 Sue 连接到 Win7 桌面池中的远程桌面时，将会启用 USB 重定向功能。

## 使用 Active Directory 组策略

您可以使用 Microsoft Windows 组策略来优化和保护远程桌面，控制 Horizon 7 组件的行为，以及配置基于位置的打印功能。

组策略是 Microsoft Windows 操作系统的一项功能，能够在 Active Directory 环境中对计算机和远程用户进行集中管理和配置。

组策略设置包含在称为组策略对象 (GPO) 的实体中。GPO 与 Active Directory 对象相关联。您可以将 GPO 应用于整个域内的 Horizon 7 组件，以控制 Horizon 7 环境的各个方面。应用后，GPO 设置将存储在指定组件的本地 Windows 注册表中。

您可以使用 Microsoft Windows 组策略对象编辑器来管理组策略设置。组策略对象编辑器是一个 Microsoft 管理控制台 (Microsoft Management Console, MMC) 插件。MMC 是 Microsoft 组策略管理控制台 (Microsoft Group Policy Management Console, GPMC) 的一部分。有关安装和使用 GPMC 的信息，请访问 Microsoft TechNet 网站。

## 为远程桌面创建 OU

在 Active Directory 中专为您的远程桌面创建一个组织单位 (Organizational Unit, OU)。

为防止组策略设置应用到远程桌面所在域中的其他 Windows 服务器或工作站，请为 Horizon 7 组策略创建一个 GPO，并将其链接到包含您的远程桌面的 OU。

有关创建组织单位和 GPO 的信息，请参阅 Microsoft TechNet 网站上的 Microsoft Active Directory 文档。

## 为远程桌面启用环回处理

默认情况下，用户的策略设置来自应用于 Active Directory 中的用户对象的 GPO 集。但是，在 Horizon 7 环境中，GPO 将基于用户登录的计算机应用于这些用户。

启用环回处理后，将对登录到特定计算机的所有用户应用一组一致的策略，无论他们在 Active Directory 中的位置如何。

有关启用环回处理的信息，请参阅 Microsoft Active Directory 文档。

---

**注** 环回处理只是在 Horizon 7 中处理 GPO 的一种方法。您可能还需要实施其他方法。

---

## 使用 Horizon 7 组策略管理模板文件

Horizon 7 提供了多个特定于组件的组策略管理 ADMX 模板文件。您可以将这些 ADMX 模板文件中的策略设置添加到 Active Directory 中的新 GPO 或现有 GPO，从而优化和保护远程桌面和应用程序。

为 Horizon 7 提供组策略设置的所有 ADMX 文件包含在 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 中，其中 x.x.x 是版本，yyyyyyy 是内部版本号。您可以从 VMware 下载站点中下载该文件，网址为 <https://my.vmware.com/web/vmware/downloads>。在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 ZIP 文件。

Horizon 7 ADMX 模板文件同时包含计算机配置组策略和用户配置组策略。

- 计算机配置策略将设置应用于所有远程桌面的策略（无论哪个用户连接到桌面）。
- 用户配置策略将设置应用于所有用户的策略（无论他们连接到哪个远程桌面或应用程序）。用户配置策略覆盖等效的计算机配置策略。

Microsoft Windows 在桌面启动时和用户登录时应用策略。

## Horizon 7 ADMX 模板文件

Horizon 7 ADMX 模板文件提供了组策略设置，让您可以控制和优化 Horizon 7 组件。

ADMX 文件包含在 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 中，您可以从 VMware 下载站点下载该文件，网址为 <https://my.vmware.com/web/vmware/downloads>。在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 ZIP 文件。

**表 5-5. Horizon ADMX 模板文件**

| 模板名称                     | 模板文件                | 说明  |
|--------------------------|---------------------|---|
| VMware View Agent 配置     | vdm_agent.admx      | 包含与 Horizon Agent 的身份验证和环境组件相关的策略设置。  |
| VMware Horizon Client 配置 | vdm_client.admx     | 包含与 Horizon Client for Windows 相关的策略设置。<br>从连接服务器主机域外部连接的客户端不受应用于 Horizon Client 的策略的影响。<br>请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。   |
| VMware Horizon URL 重定向   | urlRedirection.admx | 包含与 URL 内容重定向功能相关的策略设置。如果您将此模板添加到远程桌面池或应用程序池的 GPO，则在远程桌面或应用程序内单击的某些 URL 链接会被重定向到基于 Windows 的客户端，并在客户端浏览器中将其打开。<br>如果您将此模板添加到客户端 GPO，则当用户在基于 Windows 的客户端系统中单击某些 URL 链接时，会在远程桌面或应用程序中打开该 URL。<br>请参阅第 3 章 配置 URL 内容重定向以及《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。 |

| 模板名称                         | 模板文件                              | 说明   |
|------------------------------|-----------------------------------|--|
| VMware View Server 配置        | vdm_server.admx                   | 包含与连接服务器相关的策略设置。<br>请参阅《View 管理指南》文档。  |
| VMware View 公共配置             | vdm_common.admx                   | 包含所有 Horizon 组件中的常见策略设置。<br>请参阅《View 管理指南》文档。  |
| PCoIP 会话变量                   | pcoip.admx                        | 包含与 PCoIP 显示协议相关的策略设置。   |
| PCoIP 客户端会话变量                | pcoip.client.admx                 | 包含与影响 Horizon Client for Windows 的 PCoIP 显示协议相关的策略设置。<br>请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。 |
| 用户配置管理                       | ViewPM.admx                       | 包含与 Horizon Persona Management 相关的策略设置。<br>请参阅《在 Horizon 7 中设置虚拟桌面》文档。                                       |
| VMware 虚拟打印重定向               | printerRedirection.admx           | 包含执行以下操作的策略设置：禁用基于位置的打印、禁用打印设置持久性和为重定向的客户端打印机选择打印机驱动程序。  |
| 基于位置的打印                      | LBP.xml                           | 用于为每个基于位置的打印机定义 VMware 虚拟打印的转换规则的模板。   |
| 查看 RTAV 配置                   | vdm_agent_rtav.admx               | 包含与实时音频-视频功能配合使用的网络摄像头相关的策略设置。<br>请参阅 <a href="#">实时音频-视频组策略设置</a> 。   |
| 扫描仪重定向                       | vdm_agent_scanner.admx            | 包含与被重定向以用于已发布桌面和应用程序的扫描设备相关的策略设置。<br>请参阅 <a href="#">扫描仪重定向组策略设置</a> 。                                       |
| Serial COM                   | vdm_agent_serialport.admx         | 包含与被重定向以用于虚拟桌面的串行 (COM) 端口相关的策略设置。<br>请参阅 <a href="#">串行端口重定向组策略设置</a> 。                                     |
| VMware Horizon 打印机重定向        | vdm_agent_printing.admx           | 包含与筛选重定向的打印机相关的策略设置。<br>请参阅 <a href="#">为虚拟打印筛选打印机</a> 。   |
| View Agent Direct-Connection | view_agent_direct_connection.admx | 包含与 View Agent Direct-Connection 插件相关的策略设置。请参阅《View Agent Direct-Connection 插件管理指南》文档。                       |
| VMware Horizon 性能跟踪器         | perf_tracker.admx                 | 包含与 VMware Horizon 性能跟踪器功能相关的策略设置。<br>请参阅 <a href="#">VMware Horizon 性能跟踪器策略设置</a> 。                         |
| VMware Horizon Client 驱动器重定向 | vdm_agent_cdr.admx                | 包含与客户端驱动器重定向功能相关的策略设置。<br>请参阅 <a href="#">使用组策略配置驱动器盘符行为</a> 。   |

## 将 ADMX 模板文件添加到 Active Directory

您可以将 Horizon 7 ADMX 文件中特定远程桌面功能的策略设置添加到 Active Directory 中的组策略对象 (Group Policy Object, GPO)。

### 前提条件

- 确认您的虚拟机桌面和 RDS 主机上安装了要应用其策略的远程桌面功能的安装选项。如果未安装该远程桌面功能，则组策略设置将无效。请参阅您的设置文档以了解有关安装 Horizon Agent 的信息。
- 为要对其应用组策略设置的远程桌面功能创建 GPO，并将其链接到包含虚拟机桌面或 RDS 主机的 OU。
- 确认您要添加到 Active Directory 的 ADMX 模板文件的名称。请参阅 [Horizon 7 ADMX 模板文件](#)。
- 确认在 Active Directory 服务器上可以使用组策略管理功能。

### 步骤

- 1 从 VMware 下载站点中下载 Horizon 7 GPO 捆绑包 .zip 文件，网址为 <https://my.vmware.com/web/vmware/downloads>。

在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 GPO 捆绑包。

该文件名为 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip，其中 x.x.x 是版本号，yyyyyyy 是内部版本号。为 Horizon 7 提供组策略设置的所有 ADMX 文件均在此文件中提供。

- 2 解压缩 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 文件，并将 ADMX 文件复制到 Active Directory 服务器。
  - a 将 .admx 文件和 en-US 文件夹复制到 Active Directory 服务器上的 %systemroot%\PolicyDefinitions 文件夹。
  - b 将语言资源文件 (.adml) 复制到 Active Directory 服务器上 %systemroot%\PolicyDefinitions\ 中的相应子文件夹。
- 3 在 Active Directory 服务器上，打开组策略管理编辑器并在该编辑器中输入模板文件在安装后所在的路径。

### 后续步骤

配置组策略设置。

## VMware View Agent 配置 ADMX 模板设置

VMware View Agent 配置 ADMX 模板文件 (vdm\_agent.admx) 包含与 Horizon Agent 的身份验证和环境组件相关的策略设置。

ADMX 文件包含在 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 中，您可以从 VMware 下载站点下载该文件，网址为 <https://my.vmware.com/web/vmware/downloads>。在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 ZIP 文件。

下表介绍了 VMware View Agent 配置 ADMX 模板文件中的策略设置。该模板既包含“计算机配置”设置，也包含“用户配置”设置。“用户配置”设置优先于等效的“计算机配置”设置。

## 代理配置设置

代理配置设置位于组策略管理编辑器的 **VMware View Agent 配置 > 代理配置** 文件夹中。

**表 5-6. 代理配置策略设置**

| 设置                                | 计算机 | 用户 | 属性   |
|-----------------------------------|-----|----|--|
| AllowDirectRDP                    | X   |    | <p>决定除 Horizon Client 设备之外的客户端是否可以使用 RDP 直接连接到远程桌面。如果禁用此设置，代理将只允许通过 Horizon Client 建立受 Horizon 管理的连接。</p> <p>从适用于 Mac 的 Horizon Client 中连接到远程桌面时，不要禁用 AllowDirectRDP 设置。如果禁用此设置，连接会失败并返回访问被拒绝错误。</p> <p>默认情况下，用户登录到远程桌面会话后，您可以使用 RDP 连接虚拟机。RDP 连接会终止远程桌面会话，并且用户未保存的数据和设置可能会丢失。关闭外部 RDP 连接后，用户才能登录到桌面。为避免这种情况，请禁用 AllowDirectRDP 设置。</p> <p><b>重要事项</b> 必须在每个桌面的客户机操作系统上运行 Windows 远程桌面服务。您可以使用此设置防止用户通过 RDP 直接连接到其桌面。</p> <p>默认情况下启用该设置。</p> |
| AllowSingleSignon                 | X   |    | <p>确定是否通过单点登录 (SSO) 将用户连接到桌面和应用程序。启用该设置时，用户在登录到服务器时仅需要输入一次凭据。禁用该设置时，用户必须在进行远程连接时重新进行身份验证。</p> <p>默认情况下启用该设置。</p>   |
| CommandsToRunOnConnect            | X   |    | <p>指定在会话首次连接时运行的一组命令或命令脚本。</p> <p>请参阅在 <a href="#">Horizon 桌面上运行命令</a> 了解更多信息。</p>   |
| CommandsToRunOnDisconnect         | X   |    | <p>指定在会话断开连接时运行的一组命令或命令脚本。</p> <p>请参阅在 <a href="#">Horizon 桌面上运行命令</a> 了解更多信息。</p>   |
| CommandsToRunOnReconnect          | X   |    | <p>指定在会话断开后重新连接时运行的一组命令或命令脚本。</p> <p>请参阅在 <a href="#">Horizon 桌面上运行命令</a> 了解更多信息。</p>  |
| ConnectionTicketTimeout           | X   |    | <p>指定 Horizon 连接票证的有效时间（以秒为单位）。</p> <p>连接代理时，Horizon Client 设备使用连接票证进行验证和单点登录。出于安全性原因，连接票证仅在有限时间内有效。当用户连接到远程桌面时，必须在连接票证超时或会话超时之前进行身份验证。如果未配置该设置，则使用默认超时时限 900 秒。</p>   |
| CredentialFilterExceptions        | X   |    | <p>指定不允许加载代理 CredentialFilter 的可执行文件。文件名不得包含路径或后缀。使用分号分隔多个文件名。</p>   |
| Disable Time Zone Synchronization | X   | X  | <p>确定远程桌面的时区是否与连接的客户端的时区同步。仅当 Horizon Client 配置策略的禁用时区转发设置未设为禁用时，“已启用”设置才适用。</p> <p>默认情况下禁用该设置。</p>  |

| 设置                                 | 计算机 | 用户 | 属性  |
|------------------------------------|-----|----|---|
| DPI Synchronization                | X   | X  | <p>调整远程会话的系统范围 DPI 设置。如果启用或不配置此设置，则远程会话的系统范围 DPI 设置会被设置为与客户端操作系统上的对应 DPI 设置相匹配。如果禁用此设置，则远程会话的系统范围 DPI 设置始终不发生更改。</p> <p>有关支持的客户机操作系统列表，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档中的“使用 DPI 同步”主题。</p> <p>默认情况下启用该设置。</p>  |
| DPI Synchronization Per Connection | X   | X  | <p>确定在用户重新连接到远程会话时是否调整显示器 DPI 设置。如果启用，在用户重新连接到远程会话时，该设置将显示器 DPI 设置为与客户端系统上的相应 DPI 设置匹配。还必须启用 DPI Synchronization 设置。</p> <p>如果禁用或未配置，在用户重新连接到远程会话时，该设置不会更改显示器 DPI 设置。</p> <p>有关支持的客户机操作系统列表，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档中的“使用 DPI 同步”主题。</p> <p>默认情况下禁用该设置。</p> |
| Enable multi-media acceleration    | X   |    | <p>确定是否在远程桌面上启用多媒体重定向 (MMR)。</p> <p>MMR 是一种 Windows Media Foundation 过滤器，可直接通过 TCP 套接字将多媒体数据从远程系统上的特定编解码器转发到客户端。随后，直接在播放数据的客户端上对数据进行解码。如果客户端没有足够资源处理本地多媒体解码，您可以禁用 MMR。</p> <p>默认情况下启用该设置。</p>   |
| Enable Unauthenticated Access      | X   |    | <p>启用或禁用未验证访问功能。如果启用此设置，未验证访问用户无需提供 AD 凭据，即可从 Horizon Client 访问已发布的应用程序。如果禁用此设置，未验证访问用户将需要提供 AD 凭据，才能从 Horizon Client 访问已发布的应用程序。</p> <p>您必须重新引导 RDS 主机，才能使该设置生效。</p> <p>默认情况下启用该设置。</p>  |
| Force MMR to use software overlay  | X   |    | <p>MMR 尝试使用硬件覆盖播放视频以提高性能。在使用多个显示器时，硬件覆盖仅在其中的一个显示器上存在：主显示器或启动 WMP 的显示器。如果将 WMP 拖到另一个显示器，视频将显示为黑色矩形。可以使用该选项强制 MMR 使用适用于所有显示器的软件覆盖。</p> <p>默认情况下启用该设置。</p>   |
| ShowDiskActivityIcon               | X   |    | <p>此设置在此发行版中不受支持。</p>   |
| Single sign-on retry timeout       | X   |    | <p>指定在重试单点登录之前等待的时间（以毫秒为单位）。可以将该值设置为 0 以禁用单点登录重试。默认值为 5000 毫秒。</p> <p>默认情况下启用该设置。</p>   |
| Toggle Display Settings Control    | X   |    | <p>确定当客户端会话采用 PCoIP 显示协议时是否禁用 <b>Display（显示）</b> 控制面板上的 <b>Settings（设置）</b> 选项卡。</p> <p>默认情况下启用该设置。</p>   |



**注** Horizon 6 版本 6.1 中已移除 Connect using DNS Name 设置。您可以设置 Horizon 7 LDAP 属性 **pae-PreferDNS**，以告知连接服务器在将桌面计算机和 RDS 主机的地址发送到客户端和网关时优先考虑 DNS 名称。请参阅《Horizon 7 安装指南》文档中的“当 Horizon 连接服务器返回地址信息时优先考虑 DNS 名称”。

## 代理安全设置

代理安全设置位于组策略管理编辑器的 **VMware View Agent 配置 > 代理安全** 文件夹中。

**表 5-7. 代理安全策略设置**

| 设置                                     | 计算机 | 用户 | 属性  |
|--|-----|----|---|
| Accept SSL encrypted framework channel |     | X  | <p>启用 TLS 加密框架通道。可以使用以下选项：</p> <ul style="list-style-type: none"> <li>■ <b>禁用</b> - 禁用 TLS。</li> <li>■ <b>启用</b> - 启用 TLS。允许旧版客户端不通过 TLS 进行连接。</li> <li>■ <b>强制</b> - 启用 TLS。拒绝旧版客户端连接。</li> </ul> <p>默认情况下启用该设置。</p> |

## 会话协作设置

会话协作设置位于组策略管理编辑器的 **VMware View Agent 配置 > 协作** 文件夹中。请参阅[会话协作策略设置](#)。

## 用户配置管理设置

用户配置管理设置位于组策略管理编辑器的 **VMware View Agent 配置 > 用户配置管理** 文件夹中。请参阅《在 Horizon 7 中设置虚拟桌面》文档。

## 扫描仪重定向设置

扫描仪重定向设置位于组策略管理编辑器的 **VMware View Agent 配置 > 扫描仪重定向** 文件夹中。请参阅[扫描仪重定向组策略设置](#)。

## 串行 COM 设置

串行 COM 设置位于组策略管理编辑器的 **VMware View Agent 配置 > Serial COM** 文件夹中。请参阅[串行端口重定向组策略设置](#)。

## 智能卡重定向设置

智能卡重定向设置位于组策略管理编辑器的 **VMware View Agent 配置 > 智能卡重定向 > 本地读取器访问** 文件夹中。

表 5-8. 智能卡重定向策略设置

| 设置  | 计算机 | 用户 | 属性   |
|---|-----|----|--|
| Allow applications access to Local Smart Card readers | X   |    | <p>如果启用，即使安装了智能卡重定向功能，应用程序也能够访问所有本地智能卡读取器。如果启用，将监控桌面是否存在本地读取器，如果检测到本地读取器，智能卡重定向将关闭，以便允许访问本地读取器。在用户下次连接到会话前，重定向将保持关闭。在启用本地访问时，应用程序无法再访问客户端上存在的远程读取器。</p> <p>远程桌面服务角色启用后，此设置将不适用于 RDP 或 RDS 主机。</p> <p>默认情况下禁用该设置。</p> |
| Local Reader Name                                     | X   |    | <p>指定要监控的本地读取器的名称，以便启用本地访问。默认情况下，必须在读取器插入卡才能启用本地访问。您可以使用 <b>Require an inserted Smart Card</b> 设置来禁用此要求。</p> <p>默认情况下启用该设置。</p>  |
| Require an inserted Smart Card                        | X   |    | <p>如果启用，则在本地读取器中插入卡时启用本地读取器访问。如果禁用，只要检测到本地读取器，就会启用本地访问。</p> <p>默认情况下启用该设置。</p>   |

## True SSO 配置设置

True SSO 配置设置位于组策略管理编辑器的 **VMware View Agent 配置 > True SSO 配置** 文件夹中。请参阅《Horizon 7 管理指南》文档。

## Unity Touch 和托管应用程序设置

Unity Touch 和托管应用程序设置位于组策略管理编辑器的 **VMware View Agent 配置 > Unity Touch 和托管应用程序** 文件夹中。

表 5-9. Unity Touch 和托管应用程序策略设置

| 设置  | 计算机 | 用户 | 属性   |
|---|-----|----|--|
| Send updates for empty or offscreen windows       | X   |    | <p>指定客户端是否接收有关空窗口或屏幕外窗口的更新。如果禁用该设置，则不会将有关小于 2x2 像素的窗口或完全位于屏幕外部的窗口的信息发送到客户端。</p> <p>默认情况下禁用该设置。</p>   |
| Enable Unity Touch                                | X   |    | <p>确定是否在远程桌面上启用 <b>Unity Touch</b> 功能。<b>Unity Touch</b> 支持在 <b>Horizon Client</b> 中提供已发布的应用程序，并允许移动设备用户在 <b>Unity Touch</b> 边栏中访问应用程序。</p> <p>默认情况下启用该设置。</p> |
| Enable system tray redirection for Hosted Apps    | X   |    | <p>确定用户在运行已发布的应用程序时是否已启用系统托盘重定向。</p> <p>默认情况下启用该设置。</p>  |
| Enable user profile customization for Hosted Apps | X   | X  | <p>指定在使用已发布的应用程序时是否自定义用户配置文件。如果启用该设置，则会生成一个用户配置文件，自定义 <b>Windows</b> 主题并注册启动应用程序。</p> <p>默认情况下禁用该设置。</p>   |

| 设置  | 计算机 | 用户 | 属性  |
|---|-----|----|---|
| Only launch new instances of Hosted Apps if arguments are different | X   |    | 该策略控制当启动已发布的应用程序，但断开的协议会话中已有该应用程序的现有实例在运行时的行为。如果禁用，将激活应用程序的现有实例。如果启用，只有在命令行参数匹配时，才会激活应用程序的现有实例。<br>默认情况下禁用该设置。  |
| Limit usage of Windows hooks  | X   |    | 在使用已发布的应用程序或 <b>Unity Touch</b> 时禁用大多数挂钩。该设置适用于在设置操作系统级别挂钩时存在兼容性问题的应用程序。例如，如果启用该设置，将禁用大多数 <b>Windows</b> 活动辅助功能和进程内挂钩。<br>默认情况下，将禁用该设置，这意味着使用所有首选的挂钩。 |
| Unity Filter rule list  | X   |    | 指定在使用已发布的应用程序时用于 <b>Unity</b> 窗口的筛选器规则。 <b>Horizon Agent</b> 会使用这些规则来支持自定义应用程序。有关创建筛选器规则的信息，请参阅 <a href="#">管理特殊的 Unity 窗口</a> 。<br>默认情况下不配置此设置。      |

## Horizon Agent Direct-Connection 配置设置

Horizon Agent Direct-Connection 配置设置位于组策略管理编辑器的 **VMware View Agent 配置 > View Agent Direct-Connection** 配置文件夹中。请参阅《View Agent Direct-Connection 插件管理指南》文档。

## 实时音频-视频配置设置

RTAV 配置设置位于组策略管理编辑器的 **VMware View Agent 配置 > 查看 RTAV** 配置文件夹中。请参阅[实时音频-视频组策略设置](#)。

## Horizon Agent 的 USB 配置设置

请参阅 [Horizon Agent 配置 ADMX 模板中的 USB 设置](#)。

## VMware 客户端 IP 透明度设置

VMware 客户端 IP 透明度设置位于组策略管理编辑器的 **VMware View Agent 配置 > VMware 客户端 IP 透明度** 文件夹中。

表 5-10. VMware 客户端 IP 透明度策略设置

| 设置                        | 计算机 | 用户 | 属性  |
|---------------------------|-----|----|---|
| Default auto detect proxy | X   |    | 默认 Internet Explorer 连接设置。在“Internet 选项” > “局域网 (LAN) 设置”中启用 <a href="#">自动检测设置</a> 。<br>默认情况下不启用该设置。 |
| Default Proxy Server      | X   |    | 代理服务器的默认 Internet Explorer 连接设置。在“Internet 选项” > “局域网 (LAN) 设置”中指定要使用的代理服务器。<br>默认情况下不启用该设置。          |

| 设置                        | 计算机 | 用户 | 属性   |
|---------------------------|-----|----|--|
| Enable                    | X   |    | 启用 VMware 客户端 IP 透明度。到 Internet Explorer 的远程连接使用客户端的 IP 地址，而不是远程桌面计算机的 IP 地址。该设置在下次登录时生效。<br>如果在 Horizon Agent 安装程序中选择“VMware 客户端 IP 透明度”自定义设置选项，将默认启用该设置。   |
| Set proxy for Java applet | X   |    | 为 Java 小程序设置代理。可以使用以下选项： <ul style="list-style-type: none"> <li>■ 在 Java 代理中使用客户端 IP 透明度 - 指示远程连接使用客户端的 IP 地址，而不是 Java 小程序的远程桌面计算机的 IP 地址。</li> <li>■ 在 Java 代理中使用直接连接 - 使用直接连接绕过 Java 小程序的浏览器设置。</li> <li>■ 在 Java 代理中使用默认值 - 还原原始 Java 代理设置。</li> </ul> 默认情况下不启用该设置。 |

## Flash 重定向设置

Flash 重定向设置位于组策略管理编辑器的 **VMware View Agent 配置 > VMware FlashMMR** 文件夹中。

表 5-11. FlashMMR 策略设置

| 设置                                   | 计算机 | 用户 | 属性   |
|--------------------------------------|-----|----|--|
| Enable flash multi-media redirection | X   |    | 指定是否在代理上启用 Flash 重定向。                                |
| Minimum rect size to enable FlashMMR | X   |    | 指定最小矩形大小以启用 Flash 重定向。<br>默认宽度为 320 像素，默认高度为 200 像素。 |

## HTML5 多媒体重定向设置

HTML5 多媒体重定向设置位于组策略管理编辑器的 **VMware View Agent 配置 > VMware HTML5 多媒体重定向** 文件夹中。请参阅 [VMware HTML5 功能策略设置](#)。

## 适用于 Skype for Business 的 VMware Virtualization Pack 设置

HTML5 多媒体重定向设置位于组策略管理编辑器的 **VMware View Agent 配置 > 适用于 Skype for Business 的 VMware Virtualization Pack** 文件夹中。请参阅[适用于 Skype for Business 的 VMware Virtualization Pack 策略设置](#)。

## 发送到远程桌面的客户端系统信息

当用户连接或重新连接到远程桌面时，Horizon Client 会收集有关客户端系统的信息，然后连接服务器会将这些信息发送到远程桌面。

Horizon Agent 会将客户端计算机信息写入在单用户计算机上部署的远程桌面的系统注册表路径 HKCU\Volatile Environment。对于在 RDS 会话中部署的远程桌面，Horizon Agent 会将客户端计算机信息写入系统注册表路径 HKCU\Volatile Environment\x，其中 x 是 RDS 主机上的会话 ID。

如果 **Horizon Client** 在远程桌面会话内运行，它会将物理客户端信息发送到远程桌面，而非发送虚拟机信息。例如，如果用户从其客户端系统连接到远程桌面，在远程桌面中启动 **Horizon Client**，然后连接到其他远程桌面，则会将物理客户端系统的 IP 地址发送到第二个远程桌面。此功能称作嵌套模式或双跃点方案。**Horizon Client** 发送 **ViewClient\_Nested\_Passthrough**（设置为 1）以及客户端系统信息，以表明它发送的是嵌套模式信息。

**注** 对于 **Horizon Client 4.1**，会在初始协议连接时将客户端系统信息传递到第二个跃点桌面。对于 **Horizon Client 4.2** 和更高版本，如果第一个跃点协议连接断开并重新连接，也会更新客户端系统信息。

您可以向 **Horizon Agent**、**CommandsToRunOnConnect**、**CommandsToRunOnReconnect** 和 **CommandsToRunOnDisconnect** 组策略设置中添加命令，以便当用户连接和重新连接到桌面时，运行从系统注册表中读取此信息的命令或命令脚本。请参阅在 [Horizon 桌面上运行命令](#) 了解更多信息。

**表 5-12. 客户端系统信息** 介绍了包含客户端系统信息的注册表项，并列出了支持这些注册表项的桌面和客户端系统类型。如果 **支持嵌套模式** 列显示“是”，则表明将物理客户端信息（而非虚拟机信息）发送到第二个跃点桌面。

**表 5-12. 客户端系统信息**

| 注册表项                                  | 说明             | 支持嵌套模式 | 支持的桌面              | 支持的客户端系统  |
|---------------------------------------|----------------|--------|--------------------|---|
| <b>ViewClient_IP_Address</b>          | 客户端系统的 IP 地址。  | 是      | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac、Android、iOS、Windows 应用商店  |
| <b>ViewClient_MAC_Address</b>         | 客户端系统的 MAC 地址。 | 是      | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac、Android   |
| <b>ViewClient_Machine_Name</b>        | 客户端系统的计算机名。    | 是      | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac、Android、iOS、Windows 应用商店  |
| <b>ViewClient_Machine_Domain</b>      | 客户端系统的域。       | 是      | VDI（单用户计算机）<br>RDS | Windows、Windows 应用商店  |
| <b>ViewClient_LoggedOn_Username</b>   | 用于登录客户端系统的用户名。 |        | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac   |
| <b>ViewClient_LoggedOn_Domainname</b> | 用于登录客户端系统的域名。  |        | VDI（单用户计算机）<br>RDS | Windows、Windows 应用商店<br>对于 Linux 和 Mac 客户端，请参阅 <b>ViewClient_Machine_Domain</b> 。Linux 或 Mac 客户端没有提供 <b>.ViewClient_LoggedOn_Domainname</b> ，因为 Linux 和 Mac 帐户未绑定到 Windows 域。 |

| 注册表项                                | 说明  | 支持嵌套模式 | 支持的桌面              | 支持的客户端系统                                   |
|-------------------------------------|---|--------|--------------------|--|
| ViewClient_Type                     | 客户端系统的瘦客户端名或操作系统类型。   | 是      | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac、Android、iOS、Windows 应用商店 |
| ViewClient_Broker_DNS_Name          | View 连接服务器实例的 DNS 名称。   |        | VDI（单用户计算机）<br>RDS | 值直接从 View 连接服务器发出，而不由 Horizon Client 收集。   |
| ViewClient_Broker_URL               | View 连接服务器实例的 URL。  |        | VDI（单用户计算机）<br>RDS | 值直接从 View 连接服务器发出，而不由 Horizon Client 收集。   |
| ViewClient_Broker_Tunneled          | View 连接服务器安全加密链路连接的状态，可以是 true（启用）或 false（禁用）。                                    |        | VDI（单用户计算机）<br>RDS | 值直接从 View 连接服务器发出，而不由 Horizon Client 收集。   |
| ViewClient_Broker_Tunnel_URL        | View 连接服务器安全加密链路连接的 URL（如果启用了安全加密链路连接）。   |        | VDI（单用户计算机）<br>RDS | 值直接从 View 连接服务器发出，而不由 Horizon Client 收集。   |
| ViewClient_Broker_Remote_IP_Address | View 连接服务器实例所查看到的客户端系统的 IP 地址。  |        | VDI（单用户计算机）<br>RDS | 值直接从 View 连接服务器发出，而不由 Horizon Client 收集。   |
| ViewClient_TZID                     | Olson 时区 ID。<br>要禁用时区同步，请启用 Horizon AgentDisable Time Zone Synchronization 组策略设置。 |        | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac、Android、iOS              |
| ViewClient_Windows_Timezone         | GMT 标准时间。<br>要禁用时区同步，请启用 Horizon AgentDisable Time Zone Synchronization 组策略设置。    |        | VDI（单用户计算机）<br>RDS | Windows、Windows 应用商店                       |
| ViewClient_Broker_DomainName        | 用于向 View 连接服务器进行身份验证的域名。  |        | VDI（单用户计算机）<br>RDS | 值直接从 View 连接服务器发出，而不由 Horizon Client 收集。   |
| ViewClient_Broker_UserName          | 用于向 View 连接服务器进行身份验证的用户名。   |        | VDI（单用户计算机）<br>RDS | 值直接从 View 连接服务器发出，而不由 Horizon Client 收集。   |
| ViewClient_Client_ID                | 指定用作许可证密钥链接的 Unique Client HardwareId。  |        | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac、Android、iOS、Windows 应用商店 |
| ViewClient_Displays.Number          | 指定客户端上使用的监视器的数量。  |        | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac、Android、iOS、Windows 应用商店 |

| 注册表项                           | 说明                               | 支持嵌套模式 | 支持的桌面              | 支持的客户端系统                                   |
|--------------------------------|----------------------------------|--------|--------------------|--|
| ViewClient_Displays.Topology   | 指定客户端上显示器的排列方式、分辨率和尺寸。           |        | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac、Android、iOS、Windows 应用商店 |
| ViewClient_Keyboard.Type       | 指定客户端上正在使用的键盘的类型。例如：日语和韩语键盘。     |        | VDI（单用户计算机）<br>RDS | Windows                                    |
| ViewClient_Launch_SessionType  | 指定会话类型。该类型可以是桌面或应用程序。            |        | VDI（单用户计算机）<br>RDS | 值直接从 View 连接服务器发出，而不由 Horizon Client 收集。   |
| ViewClient_Mouse.Identifier    | 指定鼠标的类型。                         |        | VDI（单用户计算机）<br>RDS | Windows                                    |
| ViewClient_Mouse.NumButtons    | 指定鼠标支持的按键数量。                     |        | VDI（单用户计算机）<br>RDS | Windows                                    |
| ViewClient_Mouse.SampleRate    | 指定对 PS/2 鼠标的输入进行采样的速率（单位为每秒报告数）。 |        | VDI（单用户计算机）<br>RDS | Windows                                    |
| ViewClient_Protocol            | 指定正在使用的协议。                       |        | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac、Android、iOS、Windows 应用商店 |
| ViewClient_Language            | 指定操作系统的语言。                       |        | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac、Android、iOS、Windows 应用商店 |
| ViewClient_Launch_Matched_Tags | 指定一个或多个标记。                       |        | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac、Android、iOS、Windows 应用商店 |
| ViewClient_Launch_ID           | 指定桌面或应用程序池的唯一 ID。                |        | VDI（单用户计算机）<br>RDS | Windows、Linux、Mac、Android、iOS、Windows 应用商店 |
| ViewClient_Broker_Farm_ID      | 指定 RDS 主机上桌面或应用程序池的场 ID。         |        | RDS                | Windows、Linux、Mac、Android、iOS、Windows 应用商店 |

**注 表 5-12. 客户端系统信息** 中的 ViewClient\_LoggedOn\_Username 和

ViewClient\_LoggedOn\_Domainname 的定义适用于 Windows 版 Horizon Client 2.2 或更高版本。

对于 Windows 版 Horizon Client 5.4 或更早版本，ViewClient\_LoggedOn\_Username 发送在 Horizon Client 中输入的用户名，ViewClient\_LoggedOn\_Domainname 发送在 Horizon Client 中输入的域名。

适用于 Windows 的 Horizon Client 2.2 高于适用于 Windows 的 Horizon Client 5.4 的版本。从 Horizon Client 2.2 开始，Windows 的版本号与其他操作系统和设备上的 Horizon Client 版本保持一致。



## 在 Horizon 桌面上运行命令

您可以使用 Horizon Agent 的 `CommandsToRunOnConnect`、`CommandsToRunOnReconnect` 和 `CommandsToRunOnDisconnect` 组策略设置在用户连接、重新连接和断开连接时在 Horizon 桌面上运行命令和命令脚本。

要运行一个命令或命令脚本，请将命令名称或脚本文件路径添加到组策略设置的命令列表中。例如：

```
date
```

```
C:\Scripts\myscript.cmd
```

要运行需要访问控制台的脚本，请添加 `-C` 或 `-c` 前缀并附带一个空格。例如：

```
-c C:\Scripts\Cli_clip.cmd
```

```
-C e:\procexp.exe
```

支持的文件类型包括 `.CMD`、`.BAT` 和 `.EXE`。`.VBS` 文件无法运行，除非此类文件由 `cscript.exe` 或 `wscript.exe` 解析。例如：

```
-C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs
```

字符串总长度（包括 `-C` 或 `-c` 选项在内）不应超过 260 个字符。

## 会话协作策略设置

VMware View Agent 配置 ADMX 模板文件 (`vdm_agent.admx`) 包含与会话协作有关的策略设置。

这些设置位于组策略管理编辑器的 **计算机配置 > 管理模板 > VMware View Agent 配置 > 协作** 文件夹中。

**表 5-13. 会话协作策略设置**

| 设置  | 说明  |
|---|---|
| Allow control passing to collaborators                        | 如果启用，用户可以在协作期间将输入控制权转给其他协作者。如果禁用，则不会在协作窗口中显示切换开关。默认情况下启用该设置。  |
| Allow inviting collaborators by e-mail                        | 如果启用，您可以使用安装的电子邮件应用程序发送协作邀请。如果禁用，您无法使用电子邮件邀请协作者，即使安装了电子邮件应用程序也是如此。默认情况下启用该设置。   |
| Allow inviting collaborators by IM                            | 如果启用，您可以使用安装的即时消息 (Instant Message, IM) 应用程序发送协作邀请。如果禁用，您无法使用 IM 邀请协作者，即使安装了 IM 应用程序也是如此。默认情况下启用该设置。  |
| Separator used for multiple e-mail addresses in mailto: links | 配置用于分隔 <code>mailto:</code> 链接中多个电子邮件地址的分隔符，以便更好地与各种电子邮件客户端兼容。如果未配置，默认值为使用不带空格的分号来分隔电子邮件地址。<br>如果您的默认电子邮件客户端不允许使用分号作为分隔符，请尝试其他组合，例如逗号加一个空格或分号加一个空格。 |
| Server URLs to include in invitation message                  | 设置要包含在协作邀请中的服务器 URL。如果不配置，将使用默认的 URL，但除非是最简单的部署，这种做法可能不正确。  |

| 设置                                      | 说明   |
|---|--|
| Turn off collaboration                  | 如果启用，将完全关闭会话协作功能。如果禁用或未配置，您可以在场或桌面池级别控制该功能。在重新引导 Horizon Agent 计算机后，该设置才会生效。 |
| Maximum number of invited collaborators | 指定可邀请加入会话的协作者的最大数量。默认最大值为 5 个。该设置限制为 10 个。                                   |

## 客户端驱动器重定向策略设置

VMware Horizon 客户端驱动器重定向 ADMX 模板文件 (vdm\_agent\_cdr.admx) 包含与客户端驱动器重定向功能有关的策略设置。

客户端驱动器重定向设置位于组策略管理编辑器的 **VMware View Agent 配置 > VMware Horizon 客户端驱动器重定向** 文件夹中。

**表 5-14. 客户端驱动器重定向设置**

| 设置  | 计算机 | 用户 | 属性   |
|---|-----|----|--|
| Display redirected device with drive letter | X   |    | 确定是否显示使用客户端驱动器重定向功能重定向的驱动器的驱动器盘符。默认情况下启用该设置。   |
| Timeout for drive letter initialization     | X   |    | 指定 Windows 资源管理器初始化和显示使用客户端驱动器重定向功能重定向的驱动器的驱动器盘符的等待时间（以毫秒为单位）。如果禁用或未配置该设置，则默认值为 5000 毫秒。 |

## 用于筛选客户端设备的策略设置

用于客户端驱动器重定向的设备筛选设置位于组策略管理编辑器的 **VMware View Agent 配置 > VMware Horizon 客户端驱动器重定向 > 设备筛选** 文件夹中。

设备筛选功能只能在适用于 Windows、Mac 和 Linux 的 Horizon Client 版本 5.1 和更高版本中使用。设置这些设备筛选策略后，将对其他客户端（包括 Android、iOS 和 Chrome，以及 Horizon Client 版本 5.0 和更低版本）禁用客户端驱动器重定向。

表 5-15. 设备筛选设置

| 设置                     | 计算机 | 用户 | 属性  |
|------------------------|-----|----|---|
| Exclude Vid/Pid Device | X   |    | <p>排除具有指定供应商和产品 ID 的设备，从而禁止使用客户端驱动器重定向功能重定向这些设备。</p> <p>您必须以十六进制格式指定 ID 号。可以使用通配符 (*) 代替 ID 中的单个数字。使用分号分隔多个设备。例如：</p> <pre>vid-0781_pid-554c;vid-0781_pid-****</pre> <p>默认值为“未定义”（不排除任何设备）。</p> <p>此设置优先于<b>包含 Vid/Pid 设备</b>设置。</p> <p><b>注</b> 要对所有设备禁用客户端驱动器重定向，您可以指定 vid-****_pid-****。</p> |
| Include Vid/Pid Device | X   |    | <p>指定具有指定供应商和产品 ID 的设备，以便能够使用客户端驱动器重定向功能重定向这些设备。</p> <p>您必须以十六进制格式指定 ID 号。可以使用通配符 (*) 代替 ID 中的单个数字。使用分号分隔多个设备。例如：</p> <pre>vid-054C_pid-0099;vid-8888_pid-****</pre> <p>默认值为“未定义”（包括所有设备）。</p>  |

## VMware HTML5 功能策略设置

VMware View Agent 配置 ADMX 模板文件 (vdm\_agent.admx) 包含与 VMware HTML5 功能有关的策略设置。

### 常规 VMware HTML5 功能设置

常规 VMware HTML5 功能设置位于组策略管理编辑器的**计算机配置 > 管理模板 > VMware View Agent 配置 > VMware HTML5 功能**文件夹中。

表 5-16. 常规 VMware HTML5 功能设置

| 设置                                    | 说明   |
|---------------------------------------|--|
| Enable VMware HTML5 Features          | <p>启用 VMware HTML5 功能。您必须启用该设置才能使用 VMware HTML5 多媒体重定向或地理位置重定向功能。该设置在下次登录时生效。</p>  |
| Disable Automatically Detect Intranet | <p>如果启用该策略，则在下次登录时禁用 Intranet 设置“包括没有列在其他区域的所有本地(Intranet)站点”和“包括所有不使用代理服务器的站点”。</p> <p>如果禁用此策略，则不会对 IE 的“本地 Intranet”区域做出任何更改。</p> <p><b>重要事项</b> 如果为 Edge 浏览器启用 HTML5 多媒体重定向功能或启用地理位置重定向功能，则必须启用该设置。</p> |

## VMware HTML5 多媒体重定向功能设置

VMware HTML5 多媒体重定向功能设置位于组策略管理编辑器的**计算机配置 > 管理模板 > VMware View Agent 配置 > VMware HTML5 功能 > VMware HTML5 多媒体重定向**文件夹中。

**表 5-17. VMware HTML5 多媒体重定向策略设置**

| 设置  | 说明  |
|---|---|
| Enable VMware HTML5 Multimedia Redirection                    | 启用 VMware HTML5 多媒体重定向功能。该设置在下次登录时生效。   |
| Enable URL list for VMware HTML5 Multimedia Redirection       | <p>指定将使用 HTML5 多媒体重定向功能的网站。</p> <p>在“值名称”列中，输入可重定向 HTML5 多媒体内容的网站的 URL 列表。应在 URL 中包含 <b>http://</b> 或 <b>https://</b> 前缀。您可以在 URL 中使用匹配模式。</p> <p>例如，要重定向 YouTube 上的所有视频，请输入 <b>https://www.youtube.com/*</b>。要重定向 Vimeo 上的所有视频，请输入 <b>https://www.vimeo.com/*</b>。</p> <p>将“值”列留空。</p> |
| Enable Chrome Browser for VMware HTML5 Multimedia Redirection | 只有在已启用 VMware HTML5 多媒体重定向功能时，才会使用此策略。如果未配置此策略，则默认值与“启用 VMware HTML5 多媒体重定向”设置的值相同。   |
| Enable Edge Browser for VMware HTML5 Multimedia Redirection   | 只有在已启用 VMware HTML5 多媒体重定向功能时，才会使用此策略。如果未配置此策略，则默认值与“启用 VMware HTML5 多媒体重定向”设置的值相同。   |

## VMware 地理位置重定向功能设置

VMware 地理位置重定向功能设置位于组策略管理编辑器的**计算机配置 > 管理模板 > VMware View Agent 配置 > VMware HTML5 功能 > VMware 地理位置重定向**文件夹中。

**表 5-18. VMware 地理位置重定向设置**

| 设置  | 说明   |
|---|--|
| Enable VMware Geolocation Redirection                         | 启用 VMware 地理位置重定向功能。该设置在下次登录时生效。   |
| Enable URL list for VMware Geolocation Redirection            | <p>指定使用地理位置重定向功能的网站。</p> <p>在“值名称”列中，输入可重定向地理位置信息的网站的 URL 列表。应在 URL 中包含 <b>http://</b> 或 <b>https://</b> 前缀。您可以在 URL 中使用匹配模式。</p> <p>例如，要指定所有 YouTube 视频，请输入 <b>https://www.youtube.com/*</b>。要指定所有 Vimeo 视频，请输入 <b>https://www.vimeo.com/*</b>。</p> <p>将“值”列留空。</p> |
| Set the minimum distance for which to report location updates | <p>指定客户端中位置更新和上一次报告给代理的更新（必须将新位置报告给代理）之间的最短距离（以米为单位）。</p> <p>默认情况下，所使用的最短距离为 <b>75 米</b>。</p>  |

## 适用于 Skype for Business 的 VMware Virtualization Pack 策略设置

VMware View Agent 配置 ADMX 模板文件 (vdm\_agent.admx) 包含与适用于 Skype for Business 的 VMware Virtualization Pack 相关的策略设置。

这些设置位于组策略管理编辑器的 **计算机配置 > 管理模板 > VMware View Agent 配置 > 适用于 Skype for Business 的 VMware Virtualization Pack** 文件夹中。

**表 5-19. 适用于 Skype for Business 的 Virtualization Pack 策略设置**

| 设置  | 说明   |
|---|--|
| Disable extended filter for acoustic echo cancellation in VMware Virtualization Pack for Skype for Business | 默认情况下，将启用于消除声音回音的扩展筛选器，该筛选器可以更好地消除回音和反馈，当 Horizon Client 系统的麦克风和扬声器彼此靠近时，该筛选器尤为有效。如果您不希望适用于 Skype for Business 的 VMware Virtualization Pack 使用此筛选器，请启用该策略。   |
| EnableDetectProxySettings   | 在 Horizon Client 系统需要使用代理服务器时，可以启用该策略以降低延迟。如果启用，适用于 Skype for Business 的 Virtualization Pack 检查 Horizon Client 系统上的代理设置，并在媒体流量中使用这些设置。如果在 Horizon Client 系统上没有代理设置，则适用于 Skype for Business 的 Virtualization Pack 使用直接连接。   |
| Force Skype for Business in non-optimized mode  | <p>对于 Horizon Client 连接，您可以在安装了 Horizon Agent 的计算机上设置连接时提供的环境变量名称，以强制 Skype for Business 在非优化模式下运行。如果设置该变量名称，适用于 Skype for Business 的 Virtualization Pack 将恢复到回退模式。</p> <p>例如，在 Horizon Client 计算机使用 F5 负载均衡器从网络外部进行连接时，如果在远程桌面代理计算机上设置 ViewClient_F5_APM 环境变量，并且您希望强制使用非优化模式，请将该值设置为 ViewClient_F5_APM。默认情况下不配置此策略。</p> |
| Show Icon   | 显示适用于 Skype for Business 的 Virtualization Pack 图标。默认情况下，将启用该策略。如果禁用了适用于 Skype for Business 的 Virtualization Pack 的“显示图标”策略，则不会显示图标。如果禁用该策略，您将无法查看通话统计信息或消息。  |
| Show Messages   | 显示适用于 Skype for Business 的 Virtualization Pack 消息。默认情况下，将启用该策略。如果禁用了适用于 Skype for Business 的 Virtualization Pack 的“显示图标”或“显示消息”策略，则不会显示消息。   |
| Suppress minor version mismatch warning   | 如果适用于 Skype for Business 的 Virtualization Pack 在 Horizon Client 系统和 Horizon 桌面上具有不同的次要 API 版本，通知区域将显示警告。如果启用该策略，将禁止显示该警告。请注意，如果次要 API 版本不匹配，虽然 Skype for Business 通话会得到优化，但 Virtualization Pack 可能不具有最新的功能。  |

## VMware Horizon 性能跟踪器策略设置

Horizon 性能跟踪器 ADMX 模板文件 (perf\_tracker.admx) 包含与 VMware Horizon 性能跟踪器功能有关的策略设置。

有关配置和使用 Horizon 性能跟踪器功能的信息，请参阅《Horizon 7 管理指南》文档。

**表 5-20. Horizon 性能跟踪器策略设置**

| 设置                             | 说明  |
|--------------------------------|---|
| Horizon 性能跟踪器基本设置              | 如果启用，您可以设置 Horizon 性能跟踪器收集数据的频率（秒）。                                     |
| 在远程桌面连接中启用 Horizon 性能跟踪器自动启动   | 如果启用，在用户登录到远程桌面连接时，将自动启动 Horizon 性能跟踪器。要清除该首选项 GPO 设置，请选择 <b>禁用</b> 。   |
| 在远程应用程序连接中启用 Horizon 性能跟踪器自动启动 | 如果启用，在用户登录到远程应用程序连接时，将自动启动 Horizon 性能跟踪器。要清除该首选项 GPO 设置，请选择 <b>禁用</b> 。 |

## VMware 集成打印策略设置

VMware View Agent 配置 ADMX 模板文件 (printerRedirection.admx) 包含与 VMware 集成打印有关的策略设置。

这些设置位于组策略管理编辑器的**计算机配置 > 管理模板 > VMware 集成打印**文件夹中。

**表 5-21. VMware 集成打印策略设置**

| 设置                                   | 说明  |
|--------------------------------------|---|
| Disable LBP                          | 指定是否启用基于位置的打印。如果启用此设置，基于位置的打印将会禁用。如果禁用或未配置此设置，基于位置的打印将会启用。  |
| Disable Printer Property Persistence | 指定是否启用打印机属性持久性。如果启用此设置，打印机属性将不会在客户端本地打印机和重定向的打印机之间持久保留。如果禁用或未配置此设置，打印机属性将会在客户端本地打印机和重定向的打印机之间持久保留。  |
| Print Preview Setting                | <p><b>禁用打印选项</b> 确定是否启用打印目标。默认情况下，不配置该设置。如果选中，则用户无法选择打印目标。如果未选中或未配置，则用户可以选择打印目标。</p> <ul style="list-style-type: none"> <li>■ <b>直接打印</b>：打印 UI 中的默认打印选项是直接打印。</li> <li>■ <b>打印预览</b>：打印 UI 中的默认打印选项是打印预览。</li> </ul> |

| 设置  | 说明  |
|---|---|
| Printer Driver Selection                        | <p>指定用于重定向的客户端打印机的打印机驱动程序：通用打印机驱动程序 (UPD) 或本机打印机驱动程序 (NPD)。如果启用此设置，相关选项包括：</p> <ul style="list-style-type: none"> <li>■ <b>始终使用 NPD：</b>将本机打印机驱动程序用于重定向的打印机。</li> <li>■ <b>始终使用 UPD：</b>将通用打印机驱动程序用于重定向的打印机。</li> <li>■ <b>先使用 NPD，再使用 UPD：</b>首先使用本机打印机驱动程序，如果不存在该驱动程序，然后再使用通用打印机驱动程序。</li> <li>■ <b>先使用 UPD，再使用 NPD：</b>首先使用通用打印机驱动程序，如果不存在该驱动程序，然后再使用本机打印机驱动程序。</li> </ul> <p>如果禁用或未配置此设置，则默认值为<b>先使用 NPD，再使用 UPD</b>。</p>   |
| Specify a filter in redirecting client printers | <p>如果启用，请在<b>注册表值名称：PrinterFilterString</b> 文本框中键入筛选规则。筛选规则是一个正则表达式，用于指定不应重定向的打印机（黑名单）。与筛选规则中的打印机不匹配的任何打印机均会被重定向。默认情况下，筛选规则为空，这意味着将重定向所有客户端打印机。</p> <ul style="list-style-type: none"> <li>■ 属性：DriverName、VendorName 和 PrinterName</li> <li>■ 运算符：AND、OR 和 NOT</li> <li>■ 通配符：* 和 ?</li> </ul> <p>筛选规则示例：</p> <pre>(DriverName="DrName1" OR VendorName="VeName1") AND NOT PrinterName="PrNa.?e"  PrinterName=".*HP.*" OR PrinterName=".*EPSON.*" AND DriverName="PDF"  PrinterName!=".*PDFCreator.*"</pre> |

## PCoIP 策略设置

PCoIP ADMX 模板文件 (pcoip.admx) 包含与 PCoIP 显示协议有关的策略设置。您可以将设置配置为可被管理员覆盖的默认值，或配置为不可覆盖的值。

ADMX 文件包含在 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 中，您可以从 VMware 下载站点下载该文件，网址为 <https://my.vmware.com/web/vmware/downloads>。在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 ZIP 文件。

PCoIP 会话变量 ADMX 模板文件包含两个子类别：

|            |  |
|------------|--|
| 管理员可覆盖的默认值 | <p>指定 PCoIP 策略设置默认值。这些设置可被管理员覆盖。这些设置将注册表项值写入 HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults 中。所有这些设置位于组策略管理编辑器的<b>计算机配置 &gt; 策略 &gt; 管理模板 &gt; PCoIP 会话变量 &gt; 管理员可覆盖的默认值</b>文件夹中。</p> |
| 管理员不可覆盖的设置 | <p>包含与“管理员可覆盖的默认值”相同的设置，但这些设置不能被管理员覆盖。这些设置将注册表项值写入 HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin 中。所有这些设置位于组策略管理编辑器的<b>用户配置 &gt; 策略 &gt; 管理模板 &gt; PCoIP 会话变量 &gt; 管理员不可覆盖的设置</b>文件夹中。</p>     |



该模板既包含“计算机配置”设置，也包含“用户配置”设置。

## 非策略注册表项

如果需要应用本地计算机设置且不能将其放置在 HKLM\Software\Policies\Teradici 下，可将本地计算机设置放置在 HKLM\Software\Teradici 的注册表项中。可将相同的注册表项放置在 HKLM\Software\Teradici 中，就像放置在 HKLM\Software\Policies\Teradici 中一样。如果两个位置均存在相同的注册表项，HKLM\Software\Policies\Teradici 中的设置将覆盖本地计算机值。

## PCoIP 常规设置

PCoIP ADMX 模板文件包含用于配置 PCoIP 图像质量、USB 设备和网络端口等常规设置的组策略设置。

所有这些设置位于组策略管理编辑器的**计算机配置 > 策略 > 管理模板 > PCoIP 会话变量 > 管理员可覆盖的默认值**文件夹中。

所有这些设置还位于组策略管理编辑器的**用户配置 > 策略 > 管理模板 > PCoIP 会话变量 > 管理员不可覆盖的设置**文件夹中。

**表 5-22. PCoIP 常规策略设置**

| 设置  | 说明   |
|---|--|
| Configure PCoIP event log cleanup by size in MB   | <p>启用 PCoIP 事件日志清理大小 (MB) 配置。</p> <p>配置此策略后，该设置可以控制日志文件变为多大时会被清理。设置为非零值 <i>m</i> 时，超过 <i>m</i> MB 的日志文件会被自动静默删除。设置为 0 表示不会按大小清理任何文件。</p> <p>禁用或未配置此策略时，默认的事件日志清理大小为 100 MB。</p> <p>将在会话启动时执行一次日志文件清理。对该设置所做的更改只有到下一个会话时才会生效。</p> |
| Configure PCoIP event log cleanup by time in days | <p>启用 PCoIP 事件日志清理时间 (天) 配置。</p> <p>配置此策略后，该设置可以控制日志文件保留多少天后会被清理。设置为非零值 <i>n</i> 时，早于 <i>n</i> 天的日志文件会被自动静默删除。设置为 0 表示不会按时间清理任何文件。</p> <p>禁用或未配置此策略时，默认的事件日志清理时间为 7 天。</p> <p>将在会话启动时执行一次日志文件清理。对该设置所做的更改只有到下一个会话时才会生效。</p>      |
| Configure PCoIP event log verbosity               | <p>设置 PCoIP 事件日志详细级别。值范围为 0（最不详细）至 3（最详细）。</p> <p>启用设置后，您可以将详细级别设置为 0 至 3。未配置或者禁用设置时，默认的事件日志详细级别为 2。</p> <p>如果在活动的 PCoIP 会话期间修改该设置，则新的设置立即生效。</p>  |

| 设置   | 说明  |
|--|---|
| Configure PCoIP image quality levels             | <p>控制在网络拥挤期间 PCoIP 如何呈现图像。<b>最低图像质量</b>、<b>最高初始图像质量</b>和<b>最高帧速率</b>值交互作用，从而精密控制网络带宽受限环境。</p> <p>使用<b>最低图像质量</b>值可平衡带宽受限情况下的图像质量和帧速率。可指定 30 至 100 之间的值。默认值为 40。较低的值支持较高帧速率，但是可能会导致显示质量降低。较高的值支持较高的图像质量，但在网络带宽受限时可能会导致帧速率降低。当网络带宽不受限时，无论值设置如何，PCoIP 均保持最高质量。</p> <p>通过使用<b>最高初始图像质量</b>值限制显示图像更改区域的初始质量，可降低 PCoIP 所要求的网络带宽峰值。可指定 30 至 100 之间的值。默认值为 80。较低的值会降低变化内容的图像质量和峰值带宽要求。较高的值会提高变化内容的图像质量和峰值带宽要求。无论值设置如何，无变化的图像区域会逐渐以无损（完美）质量呈现。设置为 80 或更低的值可充分地利用可用带宽。</p> <p><b>最低图像质量</b>值不能超过 <b>最高初始图像质量</b>值。</p> <p>使用<b>最高帧速率</b>值来限制每秒屏幕更新的次数，从而可以管理每位用户占用的平均带宽。可指定每秒 1 帧至每秒 120 帧之间的值。默认值为 30。较高的值会占用更多的带宽，但更稳定，支持更顺畅地传输变化图像，例如视频。较低的值占用的带宽较低，但稳定性较差。</p> <p>这些图像质量值仅适用于软主机，对软客户端不起作用。</p> <p>禁用或未配置此设置时，使用默认值。</p> <p>如果在活动的 PCoIP 会话期间修改该设置，则新的设置立即生效。</p> |
| Configure frame rate vs image quality preference | <p>将帧速率和图像质量首选项配置为从 0（最高帧速率）到 100（最高图像质量）之间的值。如果禁用或未配置此策略，则默认设置为 50。</p> <p>较高值（最大：100）表示即使帧速率不连贯，您也希望获得较高的图像质量。较低值（最小：0）表示您希望在降低图像质量的情况下获得流畅体验。</p> <p>此设置可用于 Configure PCoIP image quality levels GPO，以便确定最高初始图像质量级别和最低图像质量级别。尽管 Frame rate and image quality preference 可以调整每个帧的图像质量级别，但它不能超过 Configure PCoIP image quality levels GPO 配置的最大/最小质量级别阈值。</p> <p>在运行时更改此策略后，所做的更改可以立即生效。</p>  |
| Configure PCoIP session encryption algorithms    | <p>控制会话协商期间 PCoIP 终端播发的加密算法。</p> <p>勾选其中一个复选框将禁用相关加密算法。必须启用至少一个算法。</p> <p>此设置适用于代理和客户端。各端点协商实际所用的会话加密算法。如果启用了 FIPS140-2 许可模式，通常会覆盖<b>禁用 AES-128-GCM 加密</b>值，从而启用 AES-128-GCM 加密。</p> <p>受支持的加密算法按优先顺序排列为：<b>SALSA20/12-256</b>、<b>AES-GCM-128</b> 和 <b>AES-GCM-256</b>。默认情况下，所有受支持的加密算法均可供此终端协商使用。</p> <p>如果将两个终端都配置为支持所有三个算法，且连接不使用安全网关 (SG)，则将协商使用 SALSA20 算法。但如果连接使用 SG，则会自动禁用 SALSA20，并将协商使用 AES128。如果一个终端或 SG 禁用 SALSA20，且一个终端禁用 AES128，则将协商使用 AES256。</p>   |

| 设置   | 说明   |             |  |                     |   |        |  |        |   |
|--|--|-------------|--|---------------------|---|--------|--|--------|---|
| Configure PCoIP USB allowed and unallowed device rules | <p>对于使用运行 Teradici 固件的零客户端的 PCoIP 会话，指定有权进行和无权进行此种会话的 USB 设备。PCoIP 会话中使用的 USB 设备必须显示在 USB 授权表中。USB 取消授权表中显示的 USB 设备不能在 PCoIP 会话中使用。</p> <p>最多可定义 10 条 USB 授权规则和 10 条 USB 取消授权规则。使用竖线 ( ) 字符来分隔不同的规则。</p> <p>每条规则可以包含供应商 ID (VID) 和产品 ID (PID)，或者也可以描述一个 USB 设备类。类规则可允许或禁用整个设备类、单个子类或子类中的协议。</p> <p>VID/PID 组合规则的格式为 <b>1xxxxyyyy</b>，其中 <b>xxxx</b> 是十六进制格式的 VID，<b>yyyy</b> 为十六进制格式的 PID。例如，授权或阻止某个 VID 为 <b>0x1a2b</b>、PID 为 <b>0x3c4d</b> 的设备的规则为 <b>11a2b3c4d</b>。</p> <p>对于类规则，请使用以下格式之一：</p> <table> <tr> <td>允许所有 USB 设备</td><td>格式： <b>23XXXXXX</b><br/>示例： <b>23XXXXXX</b></td></tr> <tr> <td>允许具有特定类 ID 的 USB 设备</td><td>格式： <b>22classXXXX</b><br/>示例： <b>22aaXXXX</b></td></tr> <tr> <td>允许特定子类</td><td>格式： <b>21class-subclassXX</b><br/>示例： <b>21aabbXX</b></td></tr> <tr> <td>允许特定协议</td><td>格式： <b>20class-subclass-protocol</b><br/>示例： <b>20aabbcc</b></td></tr> </table> <p>例如，允许 USB HID（鼠标和键盘）设备（类 ID 0x03）和网络摄像头（类 ID 0x0e）的 USB 授权字符串为 <b>2203XXXX 220eXXXX</b>。禁用 USB 大容量存储设备（类 ID 0x08）的 USB 取消授权字符串为 <b>2208XXXX</b>。</p> <p>空的 USB 授权字符串表示不授权任何 USB 设备。空的 USB 取消授权字符串表示不禁用任何 USB 设备。</p> <p>此设置仅适用于 Horizon Agent，且仅在远程桌面与运行 Teradici 固件的零客户端会话时应用。各个终端会相互协商来确定使用哪些设备。</p> <p>默认情况下，允许使用所有设备，不禁用任何设备。</p> | 允许所有 USB 设备 | 格式： <b>23XXXXXX</b><br>示例： <b>23XXXXXX</b> | 允许具有特定类 ID 的 USB 设备 | 格式： <b>22classXXXX</b><br>示例： <b>22aaXXXX</b> | 允许特定子类 | 格式： <b>21class-subclassXX</b><br>示例： <b>21aabbXX</b> | 允许特定协议 | 格式： <b>20class-subclass-protocol</b><br>示例： <b>20aabbcc</b> |
| 允许所有 USB 设备  | 格式： <b>23XXXXXX</b><br>示例： <b>23XXXXXX</b>   |             |  |                     |   |        |  |        |   |
| 允许具有特定类 ID 的 USB 设备                                    | 格式： <b>22classXXXX</b><br>示例： <b>22aaXXXX</b>  |             |  |                     |   |        |  |        |   |
| 允许特定子类   | 格式： <b>21class-subclassXX</b><br>示例： <b>21aabbXX</b>   |             |  |                     |   |        |  |        |   |
| 允许特定协议   | 格式： <b>20class-subclass-protocol</b><br>示例： <b>20aabbcc</b>  |             |  |                     |   |        |  |        |   |
| Configure PCoIP virtual channels                       | <p>指定能够以及不能通过 PCoIP 会话操作的虚拟通道。此设置还决定是否禁用 PCoIP 主机上的剪贴板处理功能。</p> <p>PCoIP 会话中使用的虚拟通道必须显示在虚拟通道授权列表中。未授权虚拟通道列表中显示的虚拟通道不能在 PCoIP 会话中使用。</p> <p>最多可指定 15 个虚拟通道，以在 PCoIP 会话中使用。</p> <p>使用竖线 ( ) 字符来分隔不同的通道名称。例如，允许 mksvchan 和 vdp_rdpvcbridge 虚拟通道的虚拟通道授权字符串为 <b>mksvchan vdp_vdpvcbridge</b>。</p> <p>如果通道名称包含竖线或反斜线 (\) 字符，请在这两个字符的前面插入一个反斜线字符。例如，通道名称 <b>awk\ward\channel</b> 应输入为 <b>awk\ ward\channel</b>。</p> <p>授权虚拟通道列表为空时表示禁用所有虚拟通道。未授权虚拟通道列表为空时表示允许使用所有虚拟通道。</p> <p>此虚拟通道设置适用于代理和客户端。必须在代理和客户端上均启用虚拟通道才能使用虚拟通道。</p> <p>虚拟通道设置中有一个单独的复选框，可供您禁用 PCoIP 主机上的远程剪贴板处理功能。此值仅适用于代理。</p> <p>默认情况下，启用所有虚拟通道，包括剪贴板处理功能。</p>  |             |  |                     |   |        |  |        |   |

| 设置   | 说明  |
|--|---|
| Configure the PCoIP transport header                             | <p>配置 PCoIP 传输标头，并设置传输会话优先级。</p> <p>PCoIP 传输标头为添加至所有 PCoIP UDP 数据包的 32 位标头（仅当双方启用并支持传输标头时）。PCoIP 传输标头能够使网络设备在网络拥挤时，做出更好的优先级/服务质量决策。默认情况下传输标头处于启用状态。</p> <p>传输会话的优先级决定了 PCoIP 传输标头所报告的 PCoIP 会话优先级。网络设备基于指定的传输会话优先级做出更好的优先级/服务质量决策。</p> <p>启用 <b>Configure the PCoIP transport header</b> 设置时，以下传输会话优先级可供使用：</p> <ul style="list-style-type: none"> <li>■ 高</li> <li>■ 中（默认值）</li> <li>■ 低</li> <li>■ 未定义</li> </ul> <p>PCoIP 代理和客户端进行协商来确定传输会话的优先级值。如果 PCoIP 代理指定了传输会话的优先级值，则会话将使用 PCoIP 代理所指定的会话优先级。如果仅仅是客户端指定了传输会话优先级，则会话将使用客户端所指定的会话优先级。如果代理或客户端均未指定传输会话优先级，也未指定<b>未定义的优先级</b>，则会话将使用默认值，即<b>中</b>优先级。</p>   |
| Configure the TCP port to which the PCoIP host binds and listens | <p>指定软件 PCoIP 主机绑定的 TCP 代理端口。</p> <p>TCP 端口值指定代理尝试绑定的基本 TCP 端口。TCP 端口范围值确定当基本端口不可用时尝试其他端口的个数。端口范围必须在 1 和 10 之间。</p> <p>此范围从基本端口跨越至基本端口与端口范围之和。例如，如果基本端口为 4172，端口范围为 10，则其范围为 4172 至 4182。</p> <p>不要将重试端口范围的大小设为 0。将该值设为 0 会导致用户使用 PCoIP 显示协议登录桌面时出现连接失败。Horizon Client 会返回错误消息：此桌面的显示协议当前不可用。请联系您的系统管理员（The Display protocol for this desktop is currently not available. Please contact your system administrator）。</p> <p>此设置仅适用于 Horizon Agent。</p> <p>在单用户计算机上，对于 View 4.5 及更高版本，默认的基本 TCP 端口为 4172。对于 View 4.0.x 及更低版本，默认的基本端口为 50002。默认情况下，端口范围为 1。</p> <p>在 RDS 主机上，默认的基本 TCP 端口为 4173。将 PCoIP 与 RDS 主机结合使用时，将为每个用户连接使用单独的 PCoIP 端口。由远程桌面服务设置的默认端口范围的大小足够容纳预期的最多并发用户连接。</p> <p><b>重要事项</b> 作为最佳实践，不要使用此策略设置更改 RDS 主机上的默认端口范围，或者更改 TCP 端口的默认值 4173。最重要的是，不要将 TCP 端口值设置为 4172。将此值重置为 4172 将会对 RDS 会话中的 PCoIP 性能产生负面影响。</p> |

| 设置  | 说明  |
|---|---|
| Configure the UDP port to which the PCoIP host binds and listens      | <p>指定软件 PCoIP 主机绑定的 UDP 代理端口。</p> <p>UDP 端口值指定代理尝试绑定的基本 UDP 端口。UDP 端口范围值确定当基本端口不可用时尝试其他端口的个数。端口范围必须在 1 和 10 之间。</p> <p>不要将重试端口范围的大小设为 0。将该值设为 0 会导致用户使用 PCoIP 显示协议登录桌面时出现连接失败。Horizon Client 会返回错误消息：此桌面的显示协议当前不可用。请联系您的系统管理员（The Display protocol for this desktop is currently not available. Please contact your system administrator）。</p> <p>此范围从基本端口跨越至基本端口与端口范围之和。例如，如果基本端口为 4172，端口范围为 10，则其范围为 4172 至 4182。</p> <p>此设置仅适用于 Horizon Agent。</p> <p>在单用户计算机上，对于 View 4.5 及更高版本，默认的基本 UDP 端口为 4172；对于 View 4.0.x 及更低版本，默认的基本 UDP 端口为 50002。默认情况下，端口范围为 10。</p> <p>在 RDS 主机上，默认的基本 UDP 端口为 4173。将 PCoIP 与 RDS 主机结合使用时，将为每个用户连接使用单独的 PCoIP 端口。由远程桌面服务设置的默认端口范围的大小足够容纳预期的最多并发用户连接。</p> <p><b>重要事项</b> 作为最佳实践，不要使用此策略设置更改 RDS 主机上的默认端口范围，或者更改 UDP 端口的默认值 4173。最重要的是，不要将 UDP 端口值设置为 4172。将此值重置为 4172 将会对 RDS 会话中的 PCoIP 性能产生负面影响。</p> |
| Enable access to a PCoIP session from a vSphere console               | <p>确定是否允许 vSphere Client 控制台显示活动 PCoIP 会话以及将输入发送到桌面。</p> <p>默认情况下，如果客户端通过 PCoIP 连接，vSphere Client 控制台屏幕为空白且控制台无法发送输入。此默认设置可确保当 PCoIP 远程会话处于活动状态时，恶意用户无法查看用户桌面或从本地向主机进行输入。</p> <p>此设置仅适用于 Horizon Agent。</p> <p>禁用或未配置此设置时，不允许进行控制台访问。启用此设置后，控制台将显示 PCoIP 会话并允许控制台输入。</p> <p>启用此设置后，控制台仅在 Windows 7 虚拟机硬件版本为 v8 时显示 Windows 7 系统中运行的 PCoIP 会话。硬件 v8 仅在 ESXi 5.0 及更高版本中可用。与此相反，无论虚拟机硬件版本为何，都允许从控制台向 Windows 7 系统进行输入。</p>   |
| Enable/disable audio in the PCoIP session                             | <p>确定是否在 PCoIP 会话中启用音频。两个终端必须都启用音频。启用此设置时，允许使用 PCoIP 音频。禁用此设置时，禁用 PCoIP 音频。未配置此设置时，默认启用音频。</p>  |
| Enable/disable microphone noise and DC offset filter in PCoIP session | <p>确定是否在 PCoIP 会话期间启用麦克风输入的麦克风噪声和 DC 偏移过滤器。此设置仅适用于 Horizon Agent 和 Teradici 音频驱动程序。</p> <p>如未配置该设置，Teradici 音频驱动程序默认使用麦克风噪声和 DC 偏移过滤器。</p>  |
| Turn on PCoIP user default input language synchronization             | <p>确定 PCoIP 会话中用户的默认输入语言是否与 PCoIP 客户端终端的默认输入语言同步。启用此设置时，允许同步。禁用或未配置此设置时，禁止同步。</p> <p>此设置仅适用于 Horizon Agent。</p>   |

| 设置  | 说明   |
|---|--|
| Configure SSL Connections to satisfy Security Tools | <p>指定如何建立 SSL 会话协商连接。</p> <p>要满足端口扫描程序要求，请启用“配置 SSL 连接”设置并在 Horizon Agent 上完成以下任务：</p> <ol style="list-style-type: none"> <li>1 在 Microsoft 管理控制台中，将一个正确命名并签名的证书存储到本地计算机的计算机帐户的个人存储中，并将其标记为可导出。</li> <li>2 将对该证书进行签名的颁发机构的证书存储在受信任的根证书存储中。</li> <li>3 禁用到 VMware View 5.1 和更低版本的连接。</li> <li>4 配置 Horizon Agent 以仅从证书存储中加载证书。如果使用本地计算机的个人存储，请将证书存储名称保留为“MY”和“ROOT”（不带引号），除非在步骤 1 和 2 中使用不同的存储位置。</li> </ol> <p>生成的 PCoIP Server 将满足端口扫描程序等安全工具的要求。</p> |
| Configure SSL Protocols                             | <p>在建立加密的 SSL 连接之前，配置 OpenSSL 协议以限制使用某些协议。协议列表包含一个或多个以冒号分隔的 OpenSSL 协议字符串。请注意，所有密码字符串不区分大小写。</p> <p>默认值为“TLS1.1:TLS1.2”。</p> <p>这表示启用了 TLS v1.1 和 TLS v1.2（禁用了 SSL v2.0、SSLv3.0 和 TLS v1.0）。</p> <p>该设置适用于 Horizon Agent 和 Horizon Client。</p> <p>如果在两端设置了该设置，将遵循 OpenSSL 协议协商规则。</p>  |
| Configure SSL cipher list                           | <p>在建立加密的 SSL 连接之前，配置 SSL 密码列表以限制使用密码套件。该列表由一个或多个以冒号分隔的密码套件字符串组成。所有密码套件字符串均不区分大小写。</p> <p>默认值为 ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH。</p> <p>如果配置了此设置，将忽略配置 SSL 连接以满足安全工具要求设置中的强制实施 AES-256 或更强的密码进行 SSL 连接协商复选框。</p> <p>此设置必须同时应用于 PCoIP 服务器和 PCoIP 客户端。</p>  |

## PCoIP 剪贴板和拖放设置

Horizon PCoIP ADMX 模板文件包含用于为复制和粘贴及拖放操作配置剪贴板设置的组策略设置。

所有这些设置位于组策略管理编辑器的计算机配置 > 策略 > 管理模板 > PCoIP 会话变量 > 管理员可覆盖的默认值文件夹中。

所有这些设置还位于组策略管理编辑器的用户配置 > 策略 > 管理模板 > PCoIP 会话变量 > 管理员不可覆盖的设置文件夹中。

表 5-23. PCoIP 剪贴板策略设置

| 设置  | 说明   |
|---|--|
| Configure clipboard audit                 | <p>指定是否在代理计算机上启用剪贴板审核功能。如果启用此设置，相关选项包括：</p> <ul style="list-style-type: none"> <li>■ <b>双向禁用</b> - 不记录有关剪贴板数据的信息。</li> <li>■ <b>仅启用客户端到服务器</b> - 在代理计算机上的事件日志中记录有关从客户端计算机复制到代理计算机的剪贴板数据的信息。</li> <li>■ <b>双向启用</b> - 在代理计算机上的事件日志中记录有关从客户端计算机复制到代理计算机以及从代理计算机复制到客户端计算机的剪贴板数据的信息。</li> <li>■ <b>仅启用服务器到客户端</b> - 在代理计算机上的事件日志中记录有关从代理计算机复制到客户端计算机的剪贴板数据的信息。</li> </ul> <p>如果禁用或未配置此设置，默认值为<b>双向禁用</b>。</p> <p>您可以在代理计算机上使用 <b>Windows</b> 事件查看器来查看事件日志。日志名称为 <b>VMware Horizon RX Audit</b>。要在一个集中位置查看事件日志，您可以配置 <b>VMware Log Insight</b> 或 <b>Windows</b> 事件收集器。</p> <p>对于 <b>Windows</b> 客户端，<b>Horizon Client 4.9</b> 及更高版本支持代理计算机到客户端计算机剪贴板审核。对于所有客户端，<b>Horizon Client 4.10</b> 及更高版本均支持客户端计算机到代理计算机剪贴板审核。</p> <p><b>注</b> 仅 <b>Windows</b> 客户端支持代理计算机到客户端计算机剪贴板审核。</p> |
| Configure clipboard memory size on server | <p>以字节或千字节为单位指定服务器上的剪贴板内存大小值，依选择而定。如果未配置，则内存大小以千字节为单位。</p> <p>客户端也具有剪贴板内存大小值，此值始终以千字节为单位。在建立会话后，服务器会将其剪贴板内存大小值发送到客户端。有效的剪贴板内存大小值为客户端和服务器的剪贴板内存大小值中的较小者。</p> <p>此设置只适用于安装了 <b>Horizon Client 4.1</b> 或更高版本的 <b>Windows</b>、<b>Linux</b> 和 <b>Mac</b> 客户端，以及安装了 <b>Horizon Client 4.7</b> 或更高版本的 <b>iOS</b> 客户端。在较低版本中，剪贴板内存大小设置为 <b>1 MB</b> 且无法进行配置。</p> <p><b>注</b> 较大的剪贴板内存大小可能会对性能产生负面影响，具体取决于您的网络。<b>VMware</b> 建议您不要将剪贴板内存大小设置为大于 <b>16 MB</b> 的值。</p>  |
| Configure clipboard redirection           | <p>确定允许执行剪贴板重定向的方向。您可以选择以下值之一：</p> <ul style="list-style-type: none"> <li>■ <b>仅启用客户端到代理</b></li> <li>■ <b>双向禁用</b></li> <li>■ <b>双向启用</b></li> <li>■ <b>仅启用代理到客户端</b></li> </ul> <p>剪贴板重定向作为虚拟通道实施。如果禁用了虚拟通道，则无法实施剪贴板重定向。</p> <p>此设置仅适用于 <b>Horizon Agent</b>。</p> <p>如果此设置已禁用或未配置，默认值为<b>仅启用客户端到代理</b>。</p>  |
| Configure drag and drop direction         | <p>指定允许拖放的方向。如果启用，相关选项包括：</p> <ul style="list-style-type: none"> <li>■ <b>双向禁用</b></li> <li>■ <b>仅启用客户端到代理</b>。仅允许从客户端系统拖放到代理。</li> <li>■ <b>仅启用代理到客户端</b>。仅允许从代理拖放到客户端系统。</li> <li>■ <b>双向启用</b></li> </ul> <p>如果此设置已禁用或未配置，默认值为<b>仅启用客户端到代理</b>。</p> <p>该设置仅适用于代理。</p>   |



| 设置   | 说明  |
|--|---|
| Configure drag and drop formats  | <p>确定每种数据格式所允许的拖放方向（双向禁用、仅启用代理到客户端、仅启用客户端到代理或双向启用）。如果启用此设置，相关选项包括：</p> <ul style="list-style-type: none"> <li>■ 用于文件格式的选项</li> <li>■ 用于文本格式的选项</li> <li>■ 用于富文本格式的选项</li> <li>■ 用于图像格式的选项</li> <li>■ 用于 HTML 格式的文件</li> <li>■ 用于文件内容格式的选项</li> </ul> <p>如果此设置已禁用或未配置，则所有格式的默认值都将为双向启用。</p> <p>该设置仅适用于代理。</p>  |
| Configure drag and drop size threshold                                       | <p>为拖动除文件和文件夹以外的常用数据类型确定大小限制。</p> <p>如果启用此设置，请从<b>选择拖放大小的单位</b>下拉菜单中选择拖动数据大小的单位。您可以选择<b>字节</b>、<b>千字节</b>或<b>兆字节</b>。在<b>拖放大小阈值</b>文本框中选择或输入拖动数据大小。每个单位的有效数据范围如下所示：</p> <ul style="list-style-type: none"> <li>■ <b>字节</b>：1 到 1023</li> <li>■ <b>千字节</b>：1 到 1023</li> <li>■ <b>兆字节</b>：1 到 16（可拖放的最大数据大小为 16 兆字节）</li> </ul> <p>如果此设置已禁用或未配置，则会设置 1 兆字节的默认阈值。</p> <p>该设置仅适用于代理。</p> |
| Filter text out of the incoming clipboard data                               | 指定是否从由客户端发送到代理的剪贴板数据中过滤掉文本数据。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。  |
| Filter Rich Text Format data out of the incoming clipboard data              | 指定是否从由客户端发送到代理的剪贴板数据中过滤掉富文本格式数据。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。   |
| Filter images out of the incoming clipboard data                             | 指定是否从由客户端发送到代理的剪贴板数据中过滤掉图像数据。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。  |
| Filter Microsoft Office text data out of the incoming clipboard data         | 指定是否从由客户端发送到代理的剪贴板数据中过滤掉 Microsoft Office 文本格式数据（BIFF12 格式）。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。   |
| Filter Microsoft Chart and Smart Art data out of the incoming clipboard data | 指定是否从由客户端发送到代理的剪贴板数据中过滤掉 Microsoft Office 图表和 Smart Art 数据 (Art::GVML ClipFormat)。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。   |
| Filter Microsoft Text Effects data out of the incoming clipboard data        | 指定是否从由客户端发送到代理的剪贴板数据中过滤掉 Microsoft Office 文字效果数据（HTML 格式）。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。   |
| Filter text out of the outgoing clipboard data                               | 指定是否从由代理发送到客户端的剪贴板数据中过滤掉文本数据。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。  |
| Filter Rich Text Format data out of the outgoing clipboard data              | 指定是否从由代理发送到客户端的剪贴板数据中过滤掉富文本格式数据。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。   |

| 设置   | 说明   |
|--|--|
| Filter images out of the outgoing clipboard data                                     | 指定是否从由代理发送到客户端的剪贴板数据中过滤掉图像数据。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。   |
| Filter Microsoft Office text data out of the outgoing clipboard data                 | 指定是否从由代理发送到客户端的剪贴板数据中过滤掉 Microsoft Office 文本格式数据（BIFF12 格式）。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。  |
| Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data         | 指定是否从由代理发送到客户端的剪贴板数据中过滤掉 Microsoft Office 图表和 Smart Art 数据 (Art::GVML ClipFormat)。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。  |
| Filter Microsoft Text Effects data out of the outgoing clipboard data                | 指定是否从由代理发送到客户端的剪贴板数据中过滤掉 Microsoft Office 文字效果数据（HTML 格式）。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。  |
| Whether block clipboard redirection to client side when client doesn't support audit | <p>指定是否阻止将剪贴板重定向到不支持剪贴板审核功能的客户端。</p> <p>如果启用该设置，您必须选择以下值之一。</p> <ul style="list-style-type: none"> <li>■ <b>阻止</b> - 如果代理计算机支持剪贴板审核功能，但客户端计算机不支持该功能，则阻止代理到客户端剪贴板重定向。</li> <li>■ <b>直通</b> - 如果代理计算机支持剪贴板审核功能，但客户端计算机不支持该功能，则允许代理到客户端剪贴板重定向。</li> </ul> <p>如果禁用或未配置此设置，默认值为<b>阻止</b>。</p> <p>您必须启用 <b>Configure clipboard audit</b> 组策略设置以使该设置生效。</p> |

## PCoIP 带宽设置

Horizon PCoIP ADMX 模板文件包含用于配置 PCoIP 带宽特征的组策略设置。

所有这些设置位于组策略管理编辑器的**计算机配置 > 策略 > 管理模板 > PCoIP 会话变量 > 管理员可覆盖的默认值**文件夹中。

所有这些设置还位于组策略管理编辑器的**用户配置 > 策略 > 管理模板 > PCoIP 会话变量 > 管理员不可覆盖的设置**文件夹中。

表 5-24. Horizon PCoIP 会话带宽变量

| 设置  | 说明   |
|---|--|
| Configure the maximum PCoIP session bandwidth | <p>指定 PCoIP 会话中的最大带宽（单位为 kbps）。此带宽包括所有图像处理、音频、虚拟通道、USB 以及控制 PCoIP 流量。</p> <p>将此值设为终端所连链路的总容量，考虑所需的并发 PCoIP 会话数。例如，对于采用 4Mbps Internet 连接的单用户 VDI 配置（单一 PCoIP 会话），应将此值设为 4Mb 或其 90%，为其他网络流量保留一些容限。希望多个并发 PCoIP 会话共享一个链路（该链路由多个 VDI 用户或一个 RDS 配置组成）时，您可能需要相应地调整设置。但是，降低此值的大小将限制每个活动会话的最大带宽。</p> <p>设置此值可防止代理尝试以超过链路容量的速率进行传输，从而避免出现丢失数据包或用户体验下降现象。此值是对称的。该设置强制客户端和代理使用两者上所设置的两个值中较小的一个。例如，设置 4Mbps 的最大带宽将强制代理以低于此值的速率传输数据，即便在客户端上配置了此设置也是如此。</p> <p>在终端上禁用或未配置此设置时，终端不实施带宽限制。配置此设置后，该设置会被用作终端的最大带宽限制（以 kbps 为单位）。</p> <p>未配置此设置时的默认值为 900000 kbps。</p> <p>此设置适用于 Horizon Agent 和客户端。如果两个终端的设置不同，将使用较低的值。</p> |
| Configure the PCoIP session bandwidth floor   | <p>指定 PCoIP 会话预留的带宽下限（单位为 Kbps）。</p> <p>此设置配置终端的最低预期带宽传输速率。使用此设置来为终端预留带宽时，用户无需等待带宽变得可用，从而提高了会话的响应能力。</p> <p>确保不要为所有终端过度预定总体预留带宽。确保配置的所有连接带宽下限之和不超过网络流量。</p> <p>默认值为 0，表示不预留最小带宽。禁用或未配置此设置时，不预留最小带宽。</p> <p>此设置适用于 Horizon Agent 和客户端，但只影响配置了该设置的端点。</p> <p>如果在活动的 PCoIP 会话期间修改此设置，则更改立即生效。</p>   |
| Configure the PCoIP session MTU               | <p>指定 PCoIP 会话的 UDP 数据包的最大传输单元 (MTU) 大小。</p> <p>此 MTU 大小包括 IP 和 UDP 数据包标头。TCP 使用标准 MTU 发现机制来设置 MTU，且不受此设置影响。</p> <p>最大 MTU 大小为 1500 字节。最小 MTU 大小为 500 字节。默认值为 1300 字节。</p> <p>通常情况下，无需更改 MTU 大小。如果存在会造成 PCoIP 数据包出现碎片的异常网络设置，请更改此值。</p> <p>此设置适用于 Horizon Agent 和客户端。如果两个终端的 MTU 大小设置不同，将使用最低的值。</p> <p>如果禁用或未配置此设置，则客户端在与 Horizon Agent 进行协商时将使用默认值。</p>  |

| 设置  | 说明  |
|---|---|
| Configure the PCoIP session audio bandwidth limit | <p>指定 PCoIP 会话中音频（声音播放）可用的最大带宽。</p> <p>音频处理进程监视音频使用的带宽。此处理进程根据当前带宽利用率来选择可提供最佳音频的音频压缩算法。如果设置了带宽限制，处理进程会通过更改所选的压缩算法来降低音质，直到达到带宽限制为止。如果在指定的带宽限制下无法提供最低音质，音频将被禁用。</p> <p>要允许传输未压缩的高品质立体声音频，请将此设置设为大于 1600 kbps 的值。设为 450 kbps 及更高值可支持压缩的高品质立体声音频。设为 50 kbps 至 450 kbps 之间的值可支持 FM 广播与电话品质之间的音频。设为低于 50 kbps 的值将无法播放音频。</p> <p>此设置仅适用于 Horizon Agent。必须在两个终端上启用音频，此设置方可生效。</p> <p>此外，此设置对 USB 音频不起作用。</p> <p>如果禁用或未配置此设置，将采用 500 kbps 的默认音频带宽限制配置，以限制所选音频压缩算法。如果配置了此设置，则值的单位为 kbps，且默认音频带宽限制为 500 kbps。</p> <p>此设置适用于 View 4.6 及更高版本。它对较早版本的 View 不起作用。</p> <p>如果在活动的 PCoIP 会话期间修改此设置，则更改立即生效。</p> |
| Turn off Build-to-Lossless feature                | <p>指定禁用或启用 PCoIP 协议的无损构建功能。该功能在默认情况下处于禁用状态。</p> <p>如果启用或未配置此设置，则将关闭无损构建功能，而且永远无法构建无损状态的映像和其他桌面及应用程序内容。在带宽受限的网络环境中，关闭无损构建功能可以节省带宽。</p> <p>如果禁用此设置，则将开启无损构建功能。建议在需要构建无损状态的图像和其他桌面及应用程序内容的环境中开启该功能。</p> <p>如果在活动的 PCoIP 会话期间修改此设置，则更改立即生效。</p> <p>关于 PCoIP 无损构建功能的更多信息，请参阅 <a href="#">PCoIP 无损构建功能</a>。</p>   |

## PCoIP 键盘设置

View PCoIP ADMX 模板文件包含用于配置影响键盘使用的 PCoIP 设置的组策略设置。

所有这些设置位于组策略管理编辑器的计算机配置 > 策略 > 管理模板 > PCoIP 会话变量 > 管理员可覆盖的默认值文件夹中。

所有这些设置还位于组策略管理编辑器的用户配置 > 策略 > 管理模板 > PCoIP 会话变量 > 管理员不可覆盖的设置文件夹中。

表 5-25. 针对键盘的 Horizon PCoIP 会话变量

| 设置  | 说明   |
|---|--|
| Disable sending CAD when users press Ctrl+Alt+Del       | <p>启用此策略后，如果要在 PCoIP 会话期间将安全注意序列 (SAS) 发送到远程桌面，用户必须按 <b>Ctrl+Alt+Insert</b> 而不是 <b>Ctrl+Alt+Del</b>。</p> <p>当用户按 <b>Ctrl+Alt+Del</b> 锁定客户端终端时，如果一个 SAS 被发送到主机和客户端，他们一定会感到困惑。这种情况下，您可能希望启用此设置。</p> <p>此设置仅适用于 <b>Horizon Agent</b>，对客户端不起作用。</p> <p>未配置或禁用此策略时，用户可按 <b>Ctrl+Alt+Del</b> 或 <b>Ctrl+Alt+Insert</b> 将 SAS 发送至远程桌面。</p>   |
| Use alternate key for sending Secure Attention Sequence | <p>指定一个用于发送安全注意序列 (SAS) 的备用键，而不是指定 <b>Insert</b>（插入）键。</p> <p>您可以使用此设置保留在 PCoIP 会话期间从远程桌面启动的虚拟机中的 <b>Ctrl+Alt+Ins</b> 按键序列。</p> <p>例如，用户可从 PCoIP 桌面启动 <b>vSphere Client</b>，并打开 <b>vCenter Server</b> 中虚拟机的控制台。如果在 <b>vCenter Server</b> 虚拟机的客户机操作系统中使用了 <b>Ctrl+Alt+Ins</b> 序列，则会将 <b>Ctrl+Alt+Del</b> SAS 发送至虚拟机。此设置允许通过 <b>Ctrl+Alt+备用键</b> 序列将 <b>Ctrl+Alt+Del</b> SAS 发送至 PCoIP 桌面。</p> <p>启用此设置后，必须从下拉菜单中选择一个备用键。不能启用此设置但不指定任何值。</p> <p>禁用或未配置此设置时，<b>Ctrl+Alt+Ins</b> 按键序列用作 SAS。</p> <p>此设置仅适用于 <b>Horizon Agent</b>，对客户端不起作用。</p> |

## PCoIP 无损构建功能

您可以将 PCoIP 显示协议配置为使用称为渐进构建或无损构建的编码方法，该方法即便是在受限的网络条件下也能够提供最佳的总体用户体验。该功能在默认情况下处于禁用状态。

无损构建功能首先提供一个高度压缩的初始图像（称为有损图像），然后逐渐将其构建为完全无损状态。无损状态意味着该图像将以预期的完全保真状态显示。

在 LAN 上，PCoIP 始终采用无损压缩显示文本。如果开启了无损构建功能，当每个会话的可用带宽降至 **1Mbps** 以下时，PCoIP 会首先显示有损的文本图像，然后迅速构建该图像至无损状态。这种方法可以让桌面在不同的网络条件下保持响应能力，并尽可能显示最佳图像效果，进而为用户提供最佳体验。

无损构建功能具有以下特点：

- 动态调整图像质量
- 在网络阻塞时降低图像质量
- 通过减少屏幕更新延迟保持响应能力
- 在网络不阻塞时恢复最高图像质量

可以通过禁用 **Turn off Build-to-Lossless feature** 组策略设置来启用无损构建功能。请参阅 [PCoIP 带宽设置](#)。

## VMware Blast 策略设置

VMware Blast ADMX 模板文件 (vdm\_blast.admx) 包含用于 VMware Blast 显示协议的策略设置。应用该策略后，这些设置将存储在注册表项 HKLM\Software\Policies\VMware, Inc.\VMware Blast \config 中。

这些设置适用于 HTML Access 和所有 Horizon Client 平台。

**表 5-26. VMware Blast 策略设置**

| 设置                                | 说明   |
|-----------------------------------|--|
| Audio playback                    | 指定是否为远程桌面启用音频播放。此设置用于启用音频播放。   |
| Clipboard memory size on server   | <p>以字节或千字节为单位指定服务器上的剪贴板内存大小值，依选择而定。如果未配置，则内存大小以千字节为单位。</p> <p>客户端也具有剪贴板内存大小值，此值始终以千字节为单位。在建立会话后，服务器会将其剪贴板内存大小值发送到客户端。有效的剪贴板内存大小值为客户端和服务器的剪贴板内存大小值中的较小者。</p> <p>对于 Windows 客户端，Horizon Client 4.9 及更高版本支持代理计算机到客户端计算机剪贴板审核。对于所有客户端，Horizon Client 4.10 及更高版本均支持客户端计算机到代理计算机剪贴板审核。</p> <p><b>注</b> 仅 Windows 客户端支持代理计算机到客户端计算机剪贴板审核。</p>   |
| Configure clipboard audit         | <p>指定是否在代理计算机上启用剪贴板审核功能。如果启用此设置，相关选项包括：</p> <ul style="list-style-type: none"> <li>■ <b>双向禁用</b> - 不记录有关剪贴板数据的信息。</li> <li>■ <b>仅启用客户端到服务器</b> - 在代理计算机上的事件日志中记录有关从客户端计算机复制到代理计算机的剪贴板数据的信息。</li> <li>■ <b>双向启用</b> - 在代理计算机上的事件日志中记录有关从客户端计算机复制到代理计算机以及从代理计算机复制到客户端计算机的剪贴板数据的信息。</li> <li>■ <b>仅启用服务器到客户端</b> - 在代理计算机上的事件日志中记录有关从代理计算机复制到客户端计算机的剪贴板数据的信息。</li> </ul> <p>如果禁用或未配置此设置，默认值为<b>双向禁用</b>。</p> <p><b>注</b> 仅 Windows 客户端支持代理计算机到客户端计算机剪贴板审核。所有其他客户端仅支持客户端计算机到代理计算机剪贴板审核。</p> <p>您可以在代理计算机上使用 Windows 事件查看器来查看事件日志。日志名称为 <b>VMware Horizon RX Audit</b>。要在一个集中位置查看事件日志，您可以配置 <b>VMware Log Insight</b> 或 <b>Windows 事件收集器</b>。</p> |
| Configure clipboard redirection   | <p>指定剪贴板重定向的许可行为。相关选项包括：</p> <ul style="list-style-type: none"> <li>■ <b>双向启用</b></li> <li>■ <b>双向禁用</b></li> <li>■ <b>仅启用客户端到服务器</b></li> <li>■ <b>仅启用服务器到客户端</b></li> </ul> <p>默认值为<b>仅启用客户端到服务器</b>。</p>  |
| Configure drag and drop direction | <p>指定允许拖放的方向。如果启用此设置，相关选项包括：</p> <ul style="list-style-type: none"> <li>■ <b>双向禁用</b></li> <li>■ <b>仅启用客户端到代理</b>。仅允许从客户端系统拖放到代理。</li> <li>■ <b>仅启用代理到客户端</b>。仅允许从代理拖放到客户端系统。</li> <li>■ <b>双向启用</b></li> </ul> <p>如果此设置已禁用或未配置，默认值为<b>仅启用客户端到代理</b>。</p> <p>该设置仅适用于代理。</p>  |

| 设置                                     | 说明   |
|--|--|
| Configure drag and drop formats        | <p>确定每种数据格式所允许的拖放方向（双向禁用、仅启用代理到客户端、仅启用客户端到代理或双向启用）。如果启用此设置，相关选项包括：</p> <ul style="list-style-type: none"> <li>■ 用于文件格式的选项</li> <li>■ 用于文本格式的选项</li> <li>■ 用于富文本格式的选项</li> <li>■ 用于图像格式的选项</li> <li>■ 用于 HTML 格式的文件</li> <li>■ 用于文件内容格式的选项</li> </ul> <p>如果已禁用或未配置此设置，则所有格式的默认值都将为双向启用。</p> <p>该设置仅适用于代理。</p>   |
| Configure drag and drop size threshold | <p>为拖动除文件和文件夹以外的常用数据类型确定大小限制。</p> <p>如果启用此设置，请从<b>选择拖放大小的单位</b>下拉菜单中选择拖动数据大小的单位。您可以选择<b>字节</b>、<b>千字节</b>或<b>兆字节</b>。在<b>拖放大小阈值</b>文本框中选择或输入拖动数据大小。每个单位的有效数据范围如下所示：</p> <ul style="list-style-type: none"> <li>■ 字节：1 到 1023</li> <li>■ 千字节：1 到 1023</li> <li>■ 兆字节：1 到 16（可拖放的最大数据大小为 16 兆字节）</li> </ul> <p>如果此设置已禁用或未配置，则会设置 1 兆字节的默认阈值。</p> <p>该设置仅适用于代理。</p> |
| Configure file transfer                | <p>为远程桌面与 HTML Access 客户端之间的文件传输指定许可的行为。可选择以下值之一：</p> <ul style="list-style-type: none"> <li>■ 禁用上载和下载</li> <li>■ 启用上载和下载</li> <li>■ 仅启用文件上载（用户只能将文件从客户端系统上载到远程桌面。）</li> <li>■ 仅启用文件下载（用户只能将文件从远程桌面下载到客户端系统。）</li> </ul> <p>默认为<b>仅启用文件上载</b>。</p> <p>此设置仅适用于 HTML Access 4.1 和更高版本。</p>   |
| Cookie Cleanup Interval                | <p>确定删除与不活动会话相关联的 Cookie 的频率（以毫秒为单位）。默认值为 100 毫秒。</p>  |



| 设置   | 说明   |
|--|--|
| DSCP Marking   | <p>如果启用或未配置，该设置允许在出站 <b>Blast</b> 网络流量中设置差分服务代码点 (Differentiated Services Code Point, DSCP) 值，由每个网络跃点的各种单独设置指定。如果禁用，则不会在 <b>Blast</b> 网络流量中设置 DSCP 值。</p> <p>如果启用，您可以为以下网络连接设置 0-63 范围内的数值：</p> <ul style="list-style-type: none"> <li>■ DSCP from Agent, TCP/IPv4</li> <li>■ DSCP from Agent, TCP/IPv6</li> <li>■ DSCP from Agent, UDP/IPv4</li> <li>■ DSCP from Agent, UDP/IPv6</li> <li>■ DSCP from BSG to Client, TCP/IPv4</li> <li>■ DSCP from BSG to Client, TCP/IPv6</li> <li>■ DSCP from BSG to Client, UDP/IPv4</li> <li>■ DSCP from BSG to Client, UDP/IPv6</li> <li>■ DSCP from BSG to Agent, TCP/IPv4</li> <li>■ DSCP from BSG to Agent, TCP/IPv6</li> <li>■ DSCP from BSG to Agent, UDP/IPv4</li> <li>■ DSCP from BSG to Agent, UDP/IPv6</li> <li>■ DSCP from Client, TCP/IPv4</li> <li>■ DSCP from Client, TCP/IPv6</li> <li>■ DSCP from Client, UDP/IPv4</li> <li>■ DSCP from Client, UDP/IPv6</li> </ul> |
| Filter images out of the incoming clipboard data                             | 指定是否从由客户端发送到代理的剪贴板数据中过滤掉图像数据。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。   |
| Filter images out of the outgoing clipboard data                             | 指定是否从由代理发送到客户端的剪贴板数据中过滤掉图像数据。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。   |
| Filter Microsoft Chart and Smart Art data out of the incoming clipboard data | 指定是否从由客户端发送到代理的剪贴板数据中过滤掉 <b>Microsoft Office</b> 图表和 <b>Smart Art</b> 数据 (Art::GVML ClipFormat)。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。  |
| Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data | 指定是否从由代理发送到客户端的剪贴板数据中过滤掉 <b>Microsoft Office</b> 图表和 <b>Smart Art</b> 数据 (Art::GVML ClipFormat)。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。  |
| Filter Microsoft Office text data out of the incoming clipboard data         | 指定是否从由客户端发送到代理的剪贴板数据中过滤掉 <b>Microsoft Office</b> 文本格式数据 (BIFF12 格式)。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。  |
| Filter Microsoft Office text data out of the outgoing clipboard data         | 指定是否从由代理发送到客户端的剪贴板数据中过滤掉 <b>Microsoft Office</b> 文本格式数据 (BIFF12 格式)。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。  |

| 设置  | 说明  |
|---|---|
| Filter Microsoft Text Effects data out of the incoming clipboard data | 指定是否从由客户端发送到代理的剪贴板数据中过滤掉 Microsoft Office 文字效果数据（HTML 格式）。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。   |
| Filter Microsoft Text Effects data out of the outgoing clipboard data | 指定是否从由代理发送到客户端的剪贴板数据中过滤掉 Microsoft Office 文字效果数据（HTML 格式）。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。   |
| Filter Rich Text Format data out of the incoming clipboard data       | 指定是否从由客户端发送到代理的剪贴板数据中过滤掉富文本格式数据。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。   |
| Filter Rich Text Format data out of the outgoing clipboard data       | 指定是否从由代理发送到客户端的剪贴板数据中过滤掉富文本格式数据。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。   |
| Filter text out of the incoming clipboard data                        | 指定是否从由客户端发送到代理的剪贴板数据中过滤掉文本数据。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。  |
| Filter text out of the outgoing clipboard data                        | 指定是否从由代理发送到客户端的剪贴板数据中过滤掉文本数据。启用此设置，并选中相应复选框时，将过滤掉此类数据。禁用或不配置此设置时，将允许复制和粘贴此类数据。  |
| H264  | 指定使用 H.264 编码还是 JPEG/PNG 编码。默认使用 H.264 编码。  |
| H264 High Color Accuracy  | 使用 H.264 编码时，将使用 YUV 4:4:4 颜色空间而不是 4:2:0 来提高色彩精度。<br>在使用非常高的分辨率或多个显示器时，此设置可能会导致性能下降。  |
| H.264 Quality   | <p>针对配置为使用 H.264 编码的远程显示指定图像质量。您可以指定最小量化值和最大量化值，以确定在多大程度上控制图像的无损压缩。您可以指定最佳图像质量的最小量化值。您可以指定最低图像质量的最大量化值。您可以指定以下设置：</p> <ul style="list-style-type: none"> <li>■ <b>H264maxQP</b>（可用值范围：0-51，默认值：36）</li> <li>■ <b>H264minQP</b>（可用值范围：0-51，默认值：10）</li> </ul> <p>要获得最佳图像质量，请将量化参数（QP）值范围设置为可用的值范围 +5 或 -5。这些参数确定丢弃的数据量，因此，较低的值导致较高的图像质量。</p> |
| HTTP Service  | 指定用于在安全服务器或 Access Point 设备与桌面之间进行安全通信（HTTPS）的端口。必须配置防火墙，使其打开此端口。默认值为 22443。  |
| Image Quality   | <p>指定远程显示的图像质量。您可以指定两个低质量设置、两个高质量设置和一个中等质量设置。低质量设置用于经常变化的屏幕区域，例如，发生滚动时。高质量设置用于较为静态的屏幕区域，从而产生更好的图像质量。您可以指定以下设置：</p> <ul style="list-style-type: none"> <li>■ <b>低 JPEG 质量</b>（可用值范围：10 - 100，默认值：25）</li> <li>■ <b>中等 JPEG 质量</b>（可用值范围：10 - 100，默认值：35）</li> <li>■ <b>高 JPEG 质量</b>（可用值范围：10 - 100，默认值：90）</li> </ul>                       |
| Keyboard locale synchronization                                       | <p>指定是否将客户端的键盘区域设置列表和默认的键盘区域设置同步到远程桌面或应用程序。如果启用此设置，则会发生同步。此设置仅适用于 Horizon Agent。</p> <p><b>注</b> 仅适用于 Windows 的 Horizon Client 支持该功能。</p>   |
| Max Frame Rate  | 指定屏幕更新的最大速率。使用此设置可管理用户占用的平均带宽。默认值为每秒更新 30 次。  |

| 设置   | 说明  |
|--|---|
| Max Session Bandwidth  | 指定 VMware Blast 会话的最大带宽，以千比特/秒 (kbps) 为单位。此带宽包括所有图像处理、音频、虚拟通道、USB 以及 VMware Blast 控制流量。默认值为 1 Gbps。   |
| Max Session Bandwidth kbit/s Megapixel Slope   | 指定为 VMware Blast 会话保留的最大带宽坡度，以千比特/秒 (kbps) 为单位。最小值为 100。最大值为 100000。默认值为 6200。  |
| Min Session Bandwidth  | 指定为 VMware Blast 会话保留的最小带宽，以千比特/秒 (kbps) 为单位。默认值为 256 kbps。   |
| PNG  | 如果您启用或不配置此设置，PNG 编码可用于远程会话。如果禁用此设置，则在 JPEG/PNG 模式下仅使用 JPEG 编码进行编码。当 H.264 编码器处于活动状态时，不应用此策略。默认情况下不配置此设置。  |
| Screen Blanking  | 指定当桌面有活动会话时，使桌面虚拟机的控制台显示用户看到的实际桌面，还是显示空白屏幕。默认显示空白屏幕。  |
| UDP Protocol   | 指定使用 UDP 协议还是 TCP 协议。默认使用 UDP 协议。该设置要求重新引导注册表项所在的 Horizon Agent 计算机。此设置不适用于 HTML Access，HTML Access 始终使用 TCP 协议。  |
| Whether block clipboard redirection to client side when client doesn't support audit | <p>确定是否阻止将剪贴板重定向到不支持剪贴板审核功能的客户端计算机。</p> <p>如果启用该设置，您必须选择以下值之一。</p> <ul style="list-style-type: none"> <li>■ <b>阻止</b> - 如果代理计算机支持剪贴板审核功能，但客户端计算机不支持该功能，则阻止代理到客户端剪贴板重定向。</li> <li>■ <b>直通</b> - 如果代理计算机支持剪贴板审核功能，但客户端计算机不支持该功能，则允许代理到客户端剪贴板重定向。</li> </ul> <p>如果禁用或未配置此设置，默认值为<b>阻止</b>。</p> <p>您必须启用 <code>Configure clipboard audit</code> 组策略设置以使该设置生效。</p> |

## 应用 VMware Blast 策略设置

如果以下 VMware Blast 策略在客户端会话期间发生更改，则 Horizon Client 可检测到该更改并立即应用新设置。

- H264
- Audio Playback
- Max Session Bandwidth
- Min Session Bandwidth
- Max Frame Rate
- Image Quality

对于所有其他 VMware Blast 策略，需遵循 Microsoft GPO 更新规则。可以采用手动方式或通过重新启动 Horizon Agent 计算机来更新 GPO。有关详细信息，请参阅 Microsoft 文档。

## 为 VMware Blast 启用无损压缩

您可以启用 **VMware Blast** 显示协议，以使用称为渐进构建或无损构建的编码方法。此功能首先提供一个高度压缩的初始图像（称为有损图像），然后逐渐将其构建为完全无损状态。无损状态意味着该图像将以预期的完全保真状态显示。

要为 **VMware Blast** 启用无损压缩，请在代理计算机上的 **Windows** 注册表中，将 **HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config** 文件夹中的 **EncoderBuildToPNG** 项设置为 **1**。默认值为 **0**（禁用），即编解码器不构建为 **PNG** 无损格式。

对 **EncoderBuildToPNG** 项所做的配置更改会立即生效。

---

**注** 为 **VMware Blast** 启用无损压缩会增加带宽和 **CPU** 使用率。如果需要无损压缩，**VMware** 建议使用 **PCoIP** 显示协议代替 **VMware Blast**。有关为 **PCoIP** 配置无损压缩的信息，请参阅 [PCoIP 无损构建功能](#)。

---

## 使用远程桌面服务组策略

您可以使用远程桌面服务组策略控制 **RDS** 主机以及已发布桌面和应用程序会话的配置和性能。**Horizon 7** 提供了包含在 **Horizon 7** 中支持的 **Microsoft RDS** 组策略的 **ADMX** 文件。

作为最佳做法，请配置在 **Horizon 7 ADMX** 文件中提供的组策略，而不是相应的 **Microsoft** 组策略。**Horizon 7** 组策略已通过认证，支持您的 **Horizon 7** 部署。

## RDS 应用程序兼容性设置

RDS 应用程序兼容性组策略设置控制 Windows Installer 兼容性、远程桌面 IP 虚拟化、网络适配器选择以及 RDS 主机 IP 地址的使用。

**表 5-27. RDS 应用程序兼容性组策略设置**

| 设置  | 说明  |
|---|---|
| Turn off Windows Installer RDS Compatibility  | <p>该策略设置指定对于完全安装的应用程序，Windows Installer RDS 兼容性是否在每个用户的基础上运行。Windows Installer 允许一次运行 <code>msiexec</code> 进程的一个实例。默认情况下，Windows Installer RDS 兼容性为启用状态。</p> <p>如果启用该策略设置，Windows Installer RDS 兼容性将关闭，一次只能有一个 <code>msiexec</code> 进程的实例运行。</p> <p>如果禁用或未配置该策略设置，Windows Installer RDS 兼容性将开启，多个按用户应用程序安装请求将按照这些请求的接收顺序由 <code>msiexec</code> 进程排队和处理。</p> |
| Turn on Remote Desktop IP Virtualization  | <p>该策略设置指定是否开启远程桌面 IP 虚拟化。</p> <p>默认情况下，远程桌面 IP 虚拟化处于关闭状态。</p> <p>如果启用该策略设置，远程桌面 IP 虚拟化将开启。可以选择应用该设置的模式。如果使用“按程序”模式，必须输入使用虚拟 IP 地址的程序的列表。将每个程序在单独行中列出（程序之间不输入任何空行）。例如：</p> <pre>explorer.exe mstsc.exe</pre> <p>如果禁用或未配置该策略设置，远程桌面 IP 虚拟化将关闭。</p>   |
| Select the network adapter to be used for Remote Desktop IP Virtualization                        | <p>该策略设置指定与用于虚拟 IP 地址的网络适配器对应的 IP 地址和网络掩码。IP 地址和网络掩码应以“无类别域间路由”表示法输入。例如：192.0.2.96/24。</p> <p>如果启用该策略设置，则使用指定的 IP 地址和网络掩码选择用于虚拟 IP 地址的网络适配器。</p> <p>如果禁用或未配置该策略设置，远程桌面 IP 虚拟化将关闭。必须配置网络适配器才能使远程桌面 IP 虚拟化正常工作。</p>   |
| Do not use Remote Desktop Session Host server IP address when virtual IP address is not available | <p>该策略设置指定在虚拟 IP 地址不可用时会话是否使用 RDS 主机的 IP 地址。</p> <p>如果启用该策略设置，则在虚拟 IP 不可用时不使用 RDS 主机的 IP 地址。会话将没有网络连接。</p> <p>如果禁用或未配置该策略设置，则在虚拟 IP 不可用时使用 RDS 主机的 IP 地址。</p>   |

## RDS 连接设置

通过使用 RDS 连接组策略设置，用户可以为到 RDS 主机上的会话的连接设置策略。

Horizon 7 RDS 组策略设置安装在 **计算机配置 > 策略 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 连接文件夹** 中。

Horizon 7 RDS 组策略设置还安装在**用户配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 连接**文件夹中。

**表 5-28. RDS 连接组策略设置**

| 设置   | 说明  |
|--|---|
| Automatic reconnection   | <p>指定在远程桌面连接客户端的网络链路暂时中断时是否允许自动重新连接到 RDS 主机上的会话。默认情况下，在 5 秒的时间间隔内最多进行 20 次重新连接尝试。</p> <p>如果启用该策略设置，在所有运行远程桌面连接的客户端的网络连接中断时，将自动尝试重新连接。</p> <p>如果禁用该策略设置，则会禁止客户端自动重新连接。</p> <p>如果未配置该策略设置，则不会在组策略级别指定自动重新连接。不过，用户可以在远程桌面连接中使用<b>体验</b>选项卡上的<b>如果连接中断，则重新连接</b>复选框配置自动重新连接。</p>  |
| Allow users to connect remotely using Remote Desktop Services    | <p>该策略设置使用远程桌面服务配置对计算机的远程访问。</p> <p>如果启用该策略设置，作为目标计算机上的“远程桌面用户”组成员的用户可以使用远程桌面服务远程连接到目标计算机。</p> <p>如果禁用该策略设置，则用户无法使用远程桌面服务远程连接到目标计算机。目标计算机将保持任何当前连接，但不接受任何新的传入连接。</p> <p>如果未配置该策略设置，则远程桌面服务使用目标计算机上的远程桌面设置确定是否允许建立远程连接。可以在<b>系统属性</b>中的<b>远程</b>选项卡上找到该设置。默认情况下，不允许建立远程连接。</p> <p><b>注</b> 您可以配置位于<b>计算机配置 &gt; 管理模板 &gt; Windows 组件 &gt; 远程桌面服务 &gt; 远程桌面会话主机 &gt; 安全</b>文件夹中的“要求使用网络级别的身份验证对远程连接的用户进行身份验证”策略设置以限制哪些客户端可以使用远程桌面服务进行远程连接。您可以通过以下方法限制可同时连接的用户数：在远程桌面会话主机配置工具中的<b>网络适配器</b>选项卡上配置“最大连接数”选项，或者配置位于<b>计算机配置 &gt; 管理模板 &gt; Windows 组件 &gt; 远程桌面服务 &gt; 远程桌面会话主机 &gt; 连接</b>文件夹中的“限制连接的数量”策略设置。</p> |
| Deny logoff of an administrator logged in to the console session | <p>该策略设置确定尝试远程连接到服务器控制台的管理员是否可以注销当前登录到控制台的管理员。</p> <p>在当前连接的管理员不希望被其他管理员注销时，该策略是非常有用的。如果注销连接的管理员，以前未保存的任何数据将会丢失。</p> <p>如果启用该策略设置，则不允许注销连接的管理员。</p> <p>如果禁用或未配置该策略设置，则允许注销连接的管理员。</p> <p><b>注</b> 控制台会话也称为“会话 0”。可以在远程桌面连接的计算机字段名称或命令行中使用 <b>/console</b> 开关以获取控制台访问。</p>   |

| 设置  | 说明  |
|---|---|
| Configure keep-alive connection interval                              | <p>通过使用该策略设置，您可以输入保持活动状态时间间隔以确保 RDS 主机上的会话状态与客户端状态一致。</p> <p>在客户端与 RDS 主机断开连接后，RDS 主机上的会话可能会保持活动状态，而不是更改为断开连接状态，即使实际将客户端与 RDS 主机断开连接。如果客户端再次登录到同一个 RDS 主机，可能会建立新的会话（如果将 RDS 主机配置为允许多个会话），并且原来的会话可能仍处于活动状态。</p> <p>如果启用该策略设置，您必须输入保持活动状态时间间隔。保持活动状态时间间隔确定服务器检查会话状态的频率（以分钟为单位）。可以输入的值范围是 1 到 999,999。</p> <p>如果禁用或未配置该策略设置，则不设置保持活动状态时间间隔，并且服务器不检查会话状态。</p>   |
| Limit number of connections   | <p>指定远程桌面服务是否限制到服务器的同时连接数。</p> <p>可以使用该设置限制可在服务器上处于活动状态的远程桌面服务会话数。如果超过该数量，尝试连接的其他用户将收到错误消息，指出服务器繁忙，需要稍后再试。限制会话数可以提高性能，因为请求系统资源的会话较少。默认情况下，RDS 主机允许使用不受限制的远程桌面服务会话数，并且用于管理的远程桌面允许使用两个远程桌面服务会话。</p> <p>要使用该设置，请输入希望为服务器指定的最大连接数。要指定不受限制的连接数，请键入 999999。</p> <p>如果启用该策略设置，则将最大连接数限制为与服务器上运行的 Windows 版本和远程桌面服务模式一致的指定数量。</p> <p>如果禁用或未配置该策略设置，则不会在组策略级别强制限制连接数。</p> <p><b>注</b> 该设置设计用于 RDS 主机，这些主机是运行 Windows 操作系统并安装了远程桌面会话主机角色服务的服务器。</p> |
| Set rules for remote control of Remote Desktop Services user sessions | <p>可以使用该策略设置指定在远程桌面服务会话中允许的远程控制级别。</p> <p>您可以使用该策略设置选择以下两种远程控制级别之一：“查看会话”或“完全控制”。“查看会话”允许远程控制用户查看会话。“完全控制”允许管理员与会话进行交互。可以在具有或没有用户权限的情况下建立远程控制。</p> <p>如果启用该策略设置，则管理员可以根据指定的规则与用户的远程桌面服务会话进行远程交互。要设置这些规则，请在“选项”列表中选择所需的控制和权限级别。要禁用远程控制，请选择“不允许远程控制”。</p> <p>如果禁用或未配置该策略设置，则远程控制规则由远程桌面会话主机配置工具中的 <b>远程控制</b> 选项卡上的设置确定。默认情况下，远程控制用户在具有用户权限的情况下完全控制会话。</p> <p><b>注</b> 该策略设置显示在“计算机配置”和“用户配置”中。如果配置了两个策略设置，则优先使用“计算机配置”策略设置。</p>            |



| 设置   | 说明  |
|--|---|
| Restrict Remote Desktop Services users to a single Remote Desktop Services session | <p>可以使用该策略设置将用户限制为单个远程桌面服务会话。</p> <p>如果启用该策略设置，则将使用远程桌面服务远程登录的用户限制为该服务器上的单个会话（活动或断开连接）。如果用户将会话保持断开连接状态，则用户在下次登录时自动重新连接到该会话。</p> <p>如果禁用该策略设置，则允许用户使用远程桌面服务建立不限数量的同时远程连接。</p> <p>如果未配置该策略设置，则远程桌面会话主机配置工具中的“限制每个用户使用一个会话”设置确定是否将用户限制为单个远程桌面服务会话。</p>   |
| Allow remote start of unlisted programs  | <p>可以使用该策略设置指定在远程用户启动远程桌面服务会话时是可以启动 RDS 主机上的任何程序，还是只能启动 RemoteApp 程序列表中列出的程序。</p> <p>您可以使用 RemoteApp 管理器工具创建 RemoteApp 程序列表以控制可远程启动 RDS 主机上的哪些程序。默认情况下，在用户启动远程桌面服务会话时，只能启动 RemoteApp 程序列表中的程序。</p> <p>如果启用该策略设置，在远程用户启动远程桌面服务会话时，他们可以启动 RDS 主机上的任何程序。例如，远程用户可以在连接时使用远程桌面连接客户端指定任何程序的可执行文件路径以启动该程序。</p> <p>如果禁用或未配置该策略设置，在远程用户启动远程桌面服务会话时，他们只能启动在 RemoteApp 管理器的 RemoteApp 程序列表中列出的程序。</p> |
| Turn off Fair Share CPU Scheduling   | <p>公平份额 CPU 调度根据会话数以及每个会话中的处理器时间需求，为相同 RDS 主机上的所有远程桌面服务会话动态分配处理器时间。</p> <p>如果启用此策略设置，Fair Share CPU Scheduling 将关闭。</p> <p>如果禁用或未配置此策略设置，将开启 Fair Share CPU Scheduling。</p>   |

## RDS 设备和资源重定向设置

RDS 设备和资源重定向组策略设置控制对远程桌面服务会话中客户端计算机上的设备和资源的访问权限。

Horizon 7 RDS 组策略设置安装在 **计算机配置 > 策略 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 设备和资源重定向** 文件夹中。

Horizon 7 RDS 组策略设置还安装在 **用户配置 > 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** 文件夹中。

**表 5-29. RDS 设备和资源重定向组策略设置**

| 设置   | 说明   |
|--|--|
| Allow audio and video playback redirection | <p>可以使用该策略设置指定用户是否可以在远程桌面服务会话中重定向远程计算机的音频和视频输出。</p> <p>用户可以在远程桌面连接 (RDC) 的“本地资源”选项卡上配置远程音频设置以指定播放远程计算机的音频输出的位置。用户可以选择在远程计算机或本地计算机上播放远程音频。用户也可以选择不播放音频。可以使用远程桌面协议 (.rdp) 文件中的 <b>videoplayback</b> 设置配置视频播放。默认情况下，将启用视频播放。</p> <p>默认情况下，在连接到运行 Windows Server 2008 R2、Windows Server 2008 或 Windows Server 2003 的计算机时，不允许进行音频和视频播放重定向。在连接到运行 Windows 7、Windows Vista 或 Windows XP Professional 的计算机时，默认允许进行音频和视频播放重定向。</p> <p>如果启用该策略设置，则允许进行音频和视频播放重定向。</p> <p>如果禁用该策略设置，则不允许进行音频和视频播放重定向，即使在 RDC 中指定了音频播放重定向或在 .rdp 文件中指定了视频播放。</p> <p>如果未配置该策略设置，则远程桌面会话主机配置工具中的“客户端设置”选项卡上的音频和视频播放设置确定是否允许进行音频和视频播放重定向。</p> |
| Allow audio recording redirection          | <p>可以使用该策略设置指定用户是否可以在远程桌面服务会话中将音频录制到远程计算机。</p> <p>用户可以在远程桌面连接 (RDC) 的“本地资源”选项卡上配置远程音频设置以指定是否将音频录制到远程计算机。用户可以使用本地计算机上的音频输入设备（如内置麦克风）录制音频。</p> <p>默认情况下，在连接到运行 Windows Server 2008 R2 的计算机时，不允许进行音频录制重定向。默认情况下，在连接到运行 Windows 7 的计算机时，允许进行音频录制重定向。</p> <p>如果启用该策略设置，则允许进行音频录制重定向。</p> <p>如果禁用该策略设置，则不允许进行音频录制重定向，即使在 RDC 中指定了音频录制重定向。</p> <p>如果未配置该策略设置，则远程桌面会话主机配置工具中的“客户端设置”选项卡上的音频录制设置确定是否允许进行音频录制重定向。</p>  |
| Limit audio playback quality               | <p>可以使用该策略设置限制远程桌面服务会话的音频播放质量。限制音频播放质量可以提高连接性能，尤其是通过慢速链路。</p> <p>如果启用该策略设置，您必须选择以下选项之一：“高”、“中”或“动态”。如果选择“高”，则不进行任何压缩并以最小延迟发送音频。这需要使用大量带宽。如果选择“中”，则进行一定压缩并以最小延迟（由使用的编解码器确定）发送音频。如果选择“动态”，则由远程连接的带宽确定发送音频时的压缩级别。</p> <p>使用该策略设置在远程计算机上指定的音频播放质量是远程桌面服务会话可使用的最高质量，而与在客户端计算机上配置的音频播放质量无关。例如，如果在客户端计算机上配置的音频播放质量高于在远程计算机上配置的音频播放质量，则使用较低级别的音频播放质量。</p> <p>可以在客户端计算机上使用远程桌面协议 (.rdp) 文件中的 <b>audioqualitymode</b> 设置配置音频播放质量。默认情况下，音频播放质量设置为“动态”。</p>  |

| 设置                                 | 说明   |
|------------------------------------|--|
| Do not allow clipboard redirection | <p>指定是否在远程桌面服务会话期间禁止在远程计算机和客户端计算机之间共享剪贴板内容（剪贴板重定向）。</p> <p>您可以使用该设置禁止用户在远程计算机和本地计算机之间重定向剪贴板数据。默认情况下，远程桌面服务允许剪贴板重定向。</p> <p>如果启用该设置，则用户无法重定向剪贴板数据。</p> <p>如果禁用该策略设置，则远程桌面服务始终允许剪贴板重定向。</p> <p>如果未配置该策略设置，则不会在组策略级别指定剪贴板重定向。不过，管理员仍然可以使用远程桌面会话主机配置工具禁用剪贴板重定向。</p>  |
| Do not allow COM port redirection  | <p>指定是否在远程桌面服务会话中禁止将数据从远程计算机重定向到客户端 <b>COM</b> 端口。</p> <p>您可以使用该设置禁止用户在登录到远程桌面服务会话时将数据重定向到 <b>COM</b> 端口外设或映射本地 <b>COM</b> 端口。默认情况下，远程桌面服务允许该 <b>COM</b> 端口重定向。</p> <p>如果启用该设置，则用户无法将服务器数据重定向到本地 <b>COM</b> 端口。</p> <p>如果禁用该策略设置，则远程桌面服务始终允许 <b>COM</b> 端口重定向。</p> <p>如果未配置该策略设置，则不会在组策略级别指定 <b>COM</b> 端口重定向。不过，管理员仍然可以使用远程桌面会话主机配置工具禁用 <b>COM</b> 端口重定向。</p> |
| Do not allow drive redirection     | <p>指定是否禁止在远程桌面服务会话中映射客户端驱动器（驱动器重定向）。</p> <p>默认情况下，<b>RD</b> 会话主机服务器在连接时自动映射客户端驱动器。映射的驱动器以 &lt;计算机名&gt; 上的 &lt;驱动器号&gt; 格式显示在 <b>Windows</b> 资源管理器或“我的电脑”的会话文件夹树中。您可以使用该设置覆盖该行为。</p> <p>如果启用该设置，则在远程桌面服务会话中不允许进行客户端驱动器重定向。</p> <p>如果禁用该设置，则始终允许进行客户端驱动器重定向。</p> <p>如果未配置该策略设置，则不会在组策略级别指定客户端驱动器重定向。不过，管理员仍然可以使用远程桌面会话主机配置工具禁用客户端驱动器重定向。</p>                     |
| Do not allow LPT Port redirection  | <p>指定在远程桌面服务会话期间是否禁止将数据重定向到客户端 <b>LPT</b> 端口。</p> <p>您可以使用该设置禁止用户映射本地 <b>LPT</b> 端口以及将数据从远程计算机重定向到本地 <b>LPT</b> 端口外设。默认情况下，远程桌面服务允许该 <b>LPT</b> 端口重定向。</p> <p>如果启用该设置，则远程桌面服务会话中的用户无法将服务器数据重定向到本地 <b>LPT</b> 端口。</p> <p>如果禁用该设置，则始终允许进行 <b>LPT</b> 端口重定向。</p> <p>如果未配置该策略设置，则不会在组策略级别指定 <b>LPT</b> 端口重定向。不过，管理员仍然可以使用远程桌面会话主机配置工具禁用本地 <b>LPT</b> 端口重定向。</p>    |

| 设置  | 说明   |
|---|--|
| Do not allow supported Plug and Play device redirection | <p>可以使用该策略设置控制在远程桌面服务会话中将支持的即插即用设备（如 Windows 便携设备）重定向到远程计算机。</p> <p>默认情况下，远程桌面服务允许重定向支持的即插即用设备。用户可以使用远程桌面连接的“本地资源”选项卡上的“更多”选项选择支持的即插即用设备以重定向到远程计算机。</p> <p>如果启用该策略设置，则用户无法将支持的即插即用设备重定向到远程计算机。</p> <p>如果禁用或未配置该策略设置，则用户可以将支持的即插即用设备重定向到远程计算机。</p> <p><b>注</b> 也可以在远程桌面会话主机配置工具中的“客户端设置”选项卡上禁止重定向支持的即插即用设备。您可以使用<b>计算机配置 &gt; 管理模板 &gt; 系统 &gt; 设备安装 &gt; 设备安装限制</b>文件夹中的策略设置禁止重定向支持的特定类型的即插即用设备。</p> |
| Do not allow smart card device redirection              | <p>可以使用该策略设置在远程桌面服务会话中控制智能卡设备重定向。</p> <p>如果启用该策略设置，则远程桌面服务用户无法使用智能卡登录到远程桌面服务会话。</p> <p>如果禁用或未配置该策略设置，则允许进行智能卡设备重定向。默认情况下，远程桌面服务在连接时自动重定向智能卡设备。</p> <p><b>注</b> 客户端计算机必须至少运行 Microsoft Windows 2000 Server 或 Microsoft Windows XP Professional，并且必须将目标服务器加入域。</p>   |
| Allow time zone redirection                             | <p>该策略设置确定客户端计算机是否将其时区设置重定向至远程桌面服务会话。</p> <p>如果启用此策略设置，能够进行时区重定向的客户端将其时区信息发送给服务器。然后，服务器基本时间将用于计算当前会话时间（当前会话时间 = 服务器基本时间 + 客户额时区）。</p> <p>如果禁用或未配置此策略设置，客户端计算机不会重定向其时区信息，会话时区与服务器时区相同。</p>  |

## RDS 许可设置

RDS 许可组策略设置控制 RDS 许可证服务器的查找顺序、是否显示问题通知以及 RDS 客户端访问许可证 (CAL) 是用户模式许可还是设备模式许可。

Horizon 7 RDS 组策略设置安装在**计算机配置 > 策略 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 许可**文件夹中。

表 5-30. RDS 许可组策略设置

| 设置  | 说明  |
|---|---|
| Use the specified Remote Desktop license servers                                      | <p>通过使用该策略设置，您可以指定 RDS 主机服务器尝试查找远程桌面许可证服务器的顺序。</p> <p>如果启用该策略设置，则 RDS 主机服务器先尝试查找指定的许可证服务器。如果找不到指定的许可证服务器，则 RDS 主机服务器尝试自动查找许可证服务器。</p> <p>在自动查找许可证服务器过程中，基于 Windows Server 的域中的 RDS 主机服务器尝试按照以下顺序联系许可证服务器：</p> <ol style="list-style-type: none"> <li>1 在远程桌面会话主机配置工具中指定的许可证服务器。</li> <li>2 在 Active Directory 域服务中发布的许可证服务器。</li> <li>3 在与 RDS 主机相同的域中的域控制器上安装的许可证服务器。</li> </ol> <p>如果禁用或未配置该策略设置，则 RDS 主机使用在远程桌面会话主机配置工具中指定的许可证服务器查找模式。</p> |
| Hide notifications about RD Licensing problems that affect the RD Session Host server | <p>该策略设置确定在出现的 RD 许可问题影响 RDS 主机时是否在 RDS 主机上显示通知。</p> <p>默认情况下，如果出现的 RD 许可问题影响 RDS 主机，在以本地管理员身份登录后，将在 RDS 主机上显示通知。如果适用，还会显示通知以说明 RDS 主机许可宽限期到期天数。</p> <p>如果启用该策略设置，则不会在 RDS 主机上显示这些通知。</p> <p>如果禁用或未配置该策略设置，在以本地管理员身份登录后，将在 RDS 主机上显示这些通知。</p>   |
| Set the Remote Desktop licensing mode   | <p>通过使用该策略设置，您可以指定连接到该 RDS 主机所需的远程桌面服务客户端访问许可证 (RDS CAL) 类型。</p> <p>您可以使用该策略设置选择以下两种许可模式之一：“每用户”或“每设备”。</p> <p>“每用户”许可模式要求连接到该 RDS 主机的每个用户帐户具有一个 RDS 每用户 CAL。</p> <p>“每设备”许可模式要求连接到该 RDS 主机的每个设备具有一个 RDS 每设备 CAL。</p> <p>如果启用此策略设置，您指定的许可模式将优先于在安装远程桌面会话主机期间所指定的或在远程桌面会话主机配置工具中指定的许可模式。</p> <p>如果禁用或未配置此策略设置，则使用在安装远程桌面会话主机角色服务期间所指定的或在远程桌面会话主机配置工具中指定的许可模式。</p>  |

## RDS 打印机重定向设置

通过使用 RDS 打印机重定向组策略设置，用户可以配置打印机重定向策略。

Horizon 7 RDS 组策略设置安装在**计算机配置 > 策略 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 打印机重定向**文件夹中。

Horizon 7 RDS 组策略设置还安装在**用户配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 打印机重定向**文件夹中。

表 5-31. RDS 打印机重定向组策略设置

| 设置   | 说明   |
|--|--|
| Do not set default client printer to be default printer in a session | <p>可以使用该策略设置指定是否将客户端默认打印机自动设置为 RDS 主机上的会话中的默认打印机。</p> <p>默认情况下，远程桌面服务自动将客户端默认打印机指定为 RDS 主机上的会话中的默认打印机。您可以使用该策略设置覆盖该行为。</p> <p>如果启用该策略设置，则默认打印机为在远程计算机上指定的打印机。</p> <p>如果禁用该策略设置，则 RDS 主机自动映射客户端默认打印机并在连接时将其设置为默认打印机。</p> <p>如果未配置该策略设置，则不会在组策略级别指定默认打印机。不过，管理员可以使用远程桌面会话主机配置工具为客户端会话配置默认打印机。</p>  |
| Do not allow client printer redirection                              | <p>可以使用该策略设置指定是否禁止在远程桌面服务会话中映射客户端打印机。</p> <p>您可以使用该策略设置禁止用户将打印作业从远程计算机重定向到其本地（客户端）计算机连接的打印机。默认情况下，远程桌面服务允许该客户端打印机映射。</p> <p>如果启用该策略设置，则用户无法在远程桌面服务会话中将打印作业从远程计算机重定向到本地客户端打印机。</p> <p>如果禁用该策略设置，则用户可以通过客户端打印机映射重定向打印作业。</p> <p>如果未配置该策略设置，则不会在组策略级别指定客户端打印机映射。不过，管理员仍然可以使用远程桌面会话主机配置工具禁用客户端打印机映射。</p>   |
| Use Remote Desktop Easy Print printer driver first                   | <p>可以使用该策略设置指定是否先使用远程桌面轻松打印打印机驱动程序安装所有客户端打印机。</p> <p>如果启用或未配置该策略设置，则 RDS 主机先尝试使用远程桌面轻松打印打印机驱动程序安装所有客户端打印机。如果由于任何原因无法使用远程桌面轻松打印打印机驱动程序，则使用 RDS 主机上与客户端打印机匹配的打印机驱动程序。如果 RDS 主机没有与客户端打印机匹配的打印机驱动程序，则远程桌面会话无法使用客户端打印机。</p> <p>如果禁用该策略设置，则 RDS 主机尝试查找合适的打印机驱动程序以安装客户端打印机。如果 RDS 主机没有与客户端打印机匹配的打印机驱动程序，RDS 主机将尝试使用远程桌面轻松打印驱动程序安装客户端打印机。如果由于任何原因无法使用远程桌面轻松打印打印机驱动程序，则远程桌面服务会话无法使用客户端打印机。</p> <p><b>注</b> 如果启用了“不允许客户端打印机重定向”策略设置，则会忽略“首先使用远程桌面轻松打印打印机驱动程序”策略设置。</p> |

| 设置  | 说明   |
|---|--|
| Specify RD Session Host Server fallback printer driver behavior | <p>可以使用该策略设置指定 RDS 主机回退打印机驱动程序行为。</p> <p>默认情况下，将禁用 RDS 主机回退打印机驱动程序。如果 RDS 主机没有与客户端的打印机匹配的打印机驱动程序，则远程桌面服务会话无法使用打印机。</p> <p>如果启用该策略设置，则会启用回退打印机驱动程序，并且默认行为是 RDS 主机查找合适的打印机驱动程序。如果找不到打印机驱动程序，则无法使用客户端的打印机。您可以选择更改该默认行为。可用的选项包括：</p> <ul style="list-style-type: none"> <li>■ <b>Do nothing if one is not found。</b>如果打印机驱动程序不匹配，RDS 主机将尝试查找合适的驱动程序。如果找不到打印机驱动程序，则无法使用客户端的打印机。这是默认行为。</li> <li>■ <b>Default to PCL if one is not found。</b>如果找不到合适的打印机驱动程序，则默认为打印机控制语言 (Printer Control Language, PCL) 回退打印机驱动程序。</li> <li>■ <b>Default to PS if one is not found。</b>如果找不到合适的打印机驱动程序，则默认为 PostScript (PS) 回退打印机驱动程序。</li> <li>■ <b>Show both PCL and PS if one is not found。</b>如果找不到合适的驱动程序，则显示基于 PS 和 PCL 的回退打印机驱动程序。</li> </ul> <p>如果禁用该策略设置，则会禁用 RDS 主机回退驱动程序，并且 RDS 主机不会尝试使用回退打印机驱动程序。</p> <p>如果未配置该策略设置，则回退打印机驱动程序行为是默认禁用。</p> <p><b>注</b> 如果启用了“不允许客户端打印机重定向”设置，则会忽略该策略设置并禁用回退打印机驱动程序。</p> |
| Redirect only the default client printer                        | <p>可以使用该策略设置指定默认客户端打印机是否为在远程桌面服务会话中重定向的唯一打印机。</p> <p>如果启用该策略设置，则仅在远程桌面服务会话中重定向默认客户端打印机。</p> <p>如果禁用或未配置该策略设置，则在远程桌面服务会话中重定向所有客户端打印机。</p>   |



## RDS 配置文件设置

RDS 配置文件组策略设置控制远程桌面服务会话的漫游配置文件和主目录设置。

**表 5-32. RDS 配置文件组策略设置**

| 设置  | 说明  |
|---|---|
| Limit the size of the entire roaming user profile cache | <p>此策略设置可限制本地驱动器上整个漫游用户配置文件缓存的大小。此策略设置仅适用于安装了远程桌面会话主机角色服务的计算机。</p> <p><b>注</b> 如果您要限制单个用户配置文件的大小，请使用位于<b>用户配置策略\管理模板\系统\用户配置文件</b>中的 Limit profile size 策略设置。</p> <p>如果您启用此策略设置，必须指定监视间隔（单位为分钟）和整个漫游用户配置文件缓存的最大大小（单位为千兆字节）。监视间隔决定检查整个漫游用户配置文件缓存大小的频率。当整个漫游用户配置文件缓存的大小超过指定的最大大小时，将删除最旧（最近使用最少）的漫游用户配置文件，直到整个漫游用户配置文件缓存的大小低于指定的最大大小。</p> <p>如果您禁用或未配置此策略设置，将不会限制本地驱动器上整个漫游用户配置文件缓存的大小。</p> <p>注意：如果启用了位于<b>计算机配置\策略\管理模板\系统\用户配置文件</b>中的 Prevent Roaming Profile changes from propagating to the server 策略设置，则会忽略该策略设置。</p> |
| Set Remote Desktop Services User Home Directory         | <p>指定远程桌面服务是使用指定的网络共享还是本地目录路径作为远程桌面服务会话的用户主目录的根路径。</p> <p>要使用此设置，请从“位置”下拉列表中选择主目录的位置（网络或本地）。如果您选择将目录放在网络共享中，请以 \\Computersname\Sharename 格式键入主目录根路径，然后选择要将网络共享映射到的驱动器盘符。</p> <p>如果您选择将主目录保留在本地计算机上，请以 Drive:\Path 格式键入主目录根路径，不要包含环境变量或省略号。不要为用户别名指定占位符，因为远程桌面服务会在用户登录时自动添加此内容。</p> <p><b>注</b> 如果您选择指定本地路径，将忽略“驱动器盘符”字段。如果您选择指定本地路径，但是在“主目录根路径”中键入了网络共享的名称，远程桌面服务会将用户主目录放在网络位置。</p> <p>如果状态设置为“已启用”，远程桌面服务将在本地计算机或网络上指定的位置创建用户主目录。每个用户的主目录路径是指定的主目录根路径加上用户别名。</p> <p>如果状态设置为“已禁用”或“未配置”，用户的主目录将为服务器指定的路径。</p>             |

| 设置  | 说明  |
|---|---|
| Use mandatory profiles on the RD Session Host server      | <p>通过使用该策略设置，您可以指定远程桌面服务是否针对远程连接到 RDS 主机的所有用户使用强制配置文件。</p> <p>如果您启用此策略设置，远程桌面服务将使用 <b>Set path for Remote Desktop Services Roaming User Profile</b> 策略设置中指定的路径作为强制用户配置文件的根文件夹。远程连接到 RDS 主机的所有用户使用相同的用户配置文件。</p> <p>如果禁用或未配置该策略设置，则远程连接到 RDS 主机的用户不使用强制用户配置文件。</p> <p><b>注</b> 要使此策略设置生效，您还必须启用并配置 <b>Set path for Remote Desktop Services Roaming User Profile</b> 策略设置。</p>  |
| Set path for Remote Desktop Services Roaming User Profile | <p>此策略设置可指定远程桌面服务使用的漫游用户配置文件的网络路径。</p> <p>默认情况下，远程桌面服务在 RDS 主机本地存储所有用户配置文件。您可以使用该策略设置指定一个可集中存储用户配置文件的网络共享，这样，对于配置为使用该网络共享存储用户配置文件的所有 RDS 主机上的会话，用户可以访问相同的配置文件。</p> <p>如果您启用此策略设置，远程桌面服务将使用指定的路径作为所有用户配置文件的根目录。配置文件将包含在以每个用户的帐户名命名的子文件夹中。</p> <p>要配置此策略设置，请以 <code>\\Computersname\Sharename</code> 格式键入网络共享的路径。不要为用户帐户名指定占位符，因为远程桌面服务会在用户登录并创建配置文件时自动添加此内容。如果指定的网络共享不存在，远程桌面服务将在 RDS 主机上显示错误消息，并在 RDS 主机本地存储用户配置文件。</p> <p>如果禁用或未配置该策略设置，则在 RDS 主机本地存储用户配置文件。您可以在用户的帐户“属性”对话框上的“远程桌面服务配置文件”选项卡上配置用户的配置文件路径。</p> <p>说明：</p> <ol style="list-style-type: none"> <li>1 通过该策略设置启用的漫游用户配置文件仅适用于远程桌面服务连接。用户可能还配置了 Windows 漫游用户配置文件。远程桌面服务的漫游用户配置文件在远程桌面服务会话中始终优先。</li> <li>2 要为远程连接到 RDS 主机的所有用户配置强制远程桌面服务漫游用户配置文件，请将该策略设置与位于 <b>计算机配置\管理模板\Windows 组件\远程桌面服务\RD 会话主机\配置文件</b> 中的 <b>Use mandatory profiles on the RD Session Host server</b> 策略设置一起使用。<b>Set path for Remote Desktop Services Roaming User Profile</b> 策略设置中设定的路径应包含强制配置文件。</li> </ol> |

## RDS 连接服务器设置

通过使用 RDS 连接服务器组策略设置，用户可以为连接服务器设置策略。

Horizon 7 RDS 组策略设置安装在 **计算机配置 > 策略 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > RD 连接代理** 文件夹中。

表 5-33. RDS 连接服务器组策略设置

| 设置                                       | 说明  |
|--|---|
| Join RD Connection Broker                | <p>可以使用该策略设置指定 RDS 主机是否应加入在 RDS 主机上安装的连接服务器中的场。RDS 主机上的连接服务器跟踪用户会话，并允许用户重新连接到负载均衡 RDS 场中的现有会话。要加入 RDS 主机上的连接服务器，必须在 RDS 主机上安装远程桌面会话主机角色服务。</p> <p>如果已启用该策略设置，RDS 主机将加入在“配置 RD 连接代理场名称”设置中指定的场。该场位于“配置 RD 连接代理服务器名称”策略设置中指定的连接服务器上。</p> <p>如果禁用该策略设置，则 RDS 主机不会加入连接服务器中的场，并且不会执行用户会话跟踪。如果已禁用该设置，则无法使用远程桌面会话主机配置工具或终端服务 WMI 提供程序将 RDS 主机加入连接服务器。</p> <p>如果未配置该策略设置，则不会在组策略级别指定该设置。在这种情况下，您可以使用远程桌面会话主机配置工具或终端服务 WMI 提供程序配置 RDS 主机以加入 RDS 主机上的连接服务器。</p> <p><b>注</b></p> <ol style="list-style-type: none"> <li>如果启用该设置，还必须启用“配置 RD 连接代理场名称”和“配置 RD 连接代理服务器名称”策略设置，或者使用远程桌面会话主机配置工具或终端服务 WMI 提供程序配置这些设置。</li> <li>对于 Windows Server 2008，至少在 Windows Server 2008 Standard 上支持该策略设置。</li> </ol> |
| Configure RD Connection Broker farm name | <p>可以使用该策略设置指定要在 RDS 主机的连接服务器中加入的场的名称。连接服务器使用场名称确定哪些 RDS 主机位于同一 RDS 场中。因此，同一负载均衡场中的所有 RDS 主机必须使用相同的场名称。场名称不必与 Active Directory 域服务中的名称相对应。</p> <p>如果指定新的场名称，则会在 RDS 主机的连接服务器中创建新的场。如果指定现有的场名称，RDS 主机将加入 RDS 主机上的连接服务器中的该场。</p> <p>如果启用该策略设置，您必须指定 RDS 主机的连接服务器中的某个场的名称。</p> <p>如果禁用或未配置该策略设置，则组策略不会指定场名称。在这种情况下，您可以使用远程桌面会话主机配置工具或终端服务 WMI 提供程序调整场名称。</p> <p><b>注</b> 对于 Windows Server 2008，至少在 Windows Server 2008 Standard 上支持该策略设置。除非使用组策略、远程桌面会话主机配置工具或终端服务 WMI 提供程序启用并配置“加入 RD 连接代理”和“配置 RD 连接代理服务器名称”设置，否则，该设置无效。</p>  |

| 设置                         | 说明   |
|----------------------------|--|
| Use IP Address Redirection | <p>可以使用该策略设置指定在客户端设备重新连接到负载均衡 RDS 场中的现有远程桌面服务会话时使用的重定向方法。该设置适用于配置为使用 RDS 主机上的连接服务器的 RDS 主机，而不适用于配置为使用远程桌面上的连接服务器的 RDS 主机。</p> <p>如果启用该策略设置，远程桌面服务客户端将查询 RDS 主机上的连接服务器，并使用现有会话所在的 RDS 主机的 IP 地址重定向到该会话。要使用该重定向方法，客户端计算机必须能够通过 IP 地址直接连接到场中的 RDS 主机。</p> <p>如果禁用该策略设置，则不会将 RDS 主机的 IP 地址发送到客户端，而是在令牌中嵌入该 IP 地址。在客户端重新连接到负载均衡器时，将使用路由令牌将客户端重定向到场中的相应 RDS 主机上的现有会话。只有在网络负载均衡解决方案支持使用 RDS 主机连接服务器路由令牌并且不希望客户端通过 IP 地址直接连接到负载均衡场中的 RDS 主机时，才应禁用该设置。</p> <p>如果未配置该策略设置，则使用远程桌面会话主机配置工具中的“使用 IP 地址重定向”设置。默认情况下，将启用远程桌面会话主机配置工具中的该设置。</p> <p><b>注</b> 对于 Windows Server 2008，至少在 Windows Server 2008 Standard 上支持该策略设置。</p> |

| 设置   | 说明  |
|--|---|
| Configure RD Connection Broker Server name | <p>可以使用该策略设置指定 RDS 主机用于跟踪和重定向负载均衡 RDS 场的用户会话的连接服务器。指定的 RDS 主机必须运行连接服务器服务。负载均衡场中的所有 RDS 主机应使用相同的连接服务器。</p> <p>如果启用该策略设置，您必须使用主机名、IP 地址或完全限定域名指定 RDS 主机的连接服务器。如果为连接服务器指定的名称或 IP 地址无效，则会在 RDS 主机上的事件查看器中记录一条错误消息。</p> <p>如果禁用或未配置该策略设置，您可以使用远程桌面会话主机配置工具或终端服务 WMI 提供程序调整 RDS 主机连接服务器名称或 IP 地址。</p> <p><b>注</b></p> <ul style="list-style-type: none"> <li>■ 对于 Windows Server 2008，在 Windows Server 2008 Standard 上支持该策略设置。</li> <li>■ 除非启用“加入 RD 连接代理”策略设置，或使用远程桌面会话主机配置工具或终端服务 WMI 提供程序将 RDS 主机配置为加入 RDS 主机上的连接服务器，否则，该策略设置无效。</li> <li>■ 要成为 RDS 场上启用连接服务器的会话的活动成员，该场中的每个 RDS 主机的计算机帐户必须是 RDS 主机的连接服务器上的“会话目录计算机”本地组的成员。</li> </ul> |
| Use RD Connection Broker load balancing    | <p>可以使用该策略设置指定是否在 RDS 主机上的连接服务器中使用负载均衡功能在 RDS 场中的服务器之间平衡负载。</p> <p>如果启用该策略设置，则 RDS 主机上的连接服务器将没有现有会话的用户重定向到场中具有最少会话的 RDS 主机。不会影响具有现有会话的用户的重定向行为。如果将服务器配置为使用 RDS 主机上的连接服务器，具有现有会话的用户将重定向到其会话所在的 RDS 主机。</p> <p>如果禁用该策略设置，则没有现有会话的用户登录到他们连接到第一个 RDS 主机。</p> <p>如果未配置该策略设置，您可以使用远程桌面会话主机配置工具或终端服务 WMI 提供程序配置 RDS 主机以参与 RDS 主机的连接服务器负载均衡。</p> <p><b>注</b> 如果启用该策略设置，您还必须启用“加入 RD 连接代理”、“配置 RD 连接代理场名称”和“配置 RD 连接代理服务名称”策略设置。</p>   |

## RDS 远程会话环境设置

RDS 远程会话环境组策略设置控制远程桌面服务会话中的用户界面配置。

Horizon 7 RDS 组策略设置安装在 **计算机配置 > 策略 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 远程会话环境** 文件夹中。

Horizon 7 RDS 组策略设置还安装在 **用户配置 > 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** 文件夹中。

表 5-34. RDS 远程会话环境组策略设置

| 设置  | 说明   |
|---|--|
| Limit maximum color depth                   | <p>可以使用该策略设置指定远程桌面服务连接的最大颜色分辨率（颜色深度）。</p> <p>您可以使用该策略设置为使用 RDP 的任何连接的颜色深度设置限制。限制颜色深度可以提高连接性能（尤其是通过慢速链路）和降低服务器负载。</p> <p>如果启用该策略设置，则指定的颜色深度是通过 RDP 的用户连接允许的最大颜色深度。连接的实际颜色深度是由客户端计算机上提供的颜色支持确定的。如果选择“客户端兼容”，则使用客户端支持的最大颜色深度。</p> <p><b>注</b> 仅在 Windows XP Professional 和 Windows Server 2003 上支持 24 位颜色深度。</p> <p>如果禁用或未配置该策略设置，则连接的颜色深度是由远程桌面会话主机配置工具中的“客户端设置”选项卡上的“限制最大颜色深度”设置确定的，除非用户在连接时指定了更低级别。</p>  |
| Enforce Removal of Remote Desktop Wallpaper | <p>指定是否向通过远程桌面服务连接的远程客户端显示桌面墙纸。</p> <p>您可以使用该设置在远程桌面服务会话期间强制移除墙纸。默认情况下，Windows XP Professional 向通过远程桌面连接的远程客户端显示墙纸，具体取决于客户端配置。有关详细信息，请参阅远程桌面连接选项中的“体验”选项卡。默认情况下，运行 Windows Server 2003 的服务器在远程桌面服务会话中不显示墙纸。</p> <p>如果启用该设置，则从不在远程桌面服务会话中显示墙纸。</p> <p>如果禁用该设置，则可以在远程桌面服务会话中显示墙纸，具体取决于客户端配置。</p> <p>如果未配置该设置，则默认行为适用。</p>  |
| Configure RemoteFX                          | <p>可以使用该策略设置控制 RemoteFX 在远程桌面虚拟化主机（RD 虚拟化主机）和 RDS 主机上是否可用。</p> <p>如果部署在 RD 虚拟化主机上，RemoteFX 使用图形处理单元 (GPU) 或硬件在服务器上呈现内容以提供丰富的用户体验。默认情况下，适用于 RD 虚拟化主机的 RemoteFX 使用服务器端 GPU 或硬件通过 LAN 连接和 RDP 7.1 提供丰富的用户体验。</p> <p>如果部署在 RDS 主机上，RemoteFX 使用硬件加速的压缩模式提供丰富的用户体验。</p> <p>如果启用该策略设置，将使用 RemoteFX 通过 LAN 连接和 RDP 7.1 提供丰富的用户体验。</p> <p>如果禁用该策略设置，则会禁用 RemoteFX。</p> <p>如果未配置该策略设置，则使用默认行为。默认情况下，将启用适用于 RD 虚拟化主机的 RemoteFX，并禁用适用于 RDS 主机的 RemoteFX。</p> |
| Limit maximum display resolution            | <p>可以使用该策略设置指定用于显示远程桌面服务会话的每个显示器可使用的最大显示分辨率。限制用于显示远程会话的分辨率可以提高连接性能（尤其是通过慢速链路）和降低服务器负载。</p> <p>如果启用该策略设置，您必须指定分辨率宽度和高度。指定的分辨率是用于显示远程桌面服务会话的每个显示器可使用的最大分辨率。</p> <p>如果禁用或未配置该策略设置，则用于显示远程桌面服务会话的每个显示器可使用的最大分辨率是由远程桌面会话主机配置工具中的“显示设置”选项卡上指定的值确定的。</p>  |

| 设置   | 说明   |
|--|--|
| Limit maximum number of monitors                 | <p>可以使用该策略设置限制用户可用于显示远程桌面服务会话的显示器数。限制用于显示远程桌面服务会话的显示器数可以提高连接性能（尤其是通过慢速链路）和降低服务器负载。</p> <p>如果启用该策略设置，您可以指定可用于显示远程桌面服务会话的显示器数。您可以指定 1 到 10 之间的数字。</p> <p>如果禁用或未配置该策略设置，可用于显示远程桌面服务会话的显示器数是由远程桌面会话主机配置工具中的“显示设置”选项卡上的“每个会话的最大监视器数目”框中指定的值确定的。</p>   |
| Remove "Disconnect" option from Shut Down dialog | <p>可以使用该策略设置在远程桌面服务会话中移除“关闭 Windows”对话框中的“断开连接”选项。</p> <p>您可以使用该策略设置禁止用户使用这种熟悉的方法将其客户端与 RDS 主机断开连接。</p> <p>如果启用该策略设置，则“关闭 Windows”对话框的下拉列表中不会显示“断开连接”选项。</p> <p>如果禁用或未配置该策略设置，则不会从“关闭 Windows”对话框的列表中移除“断开连接”。</p> <p><b>注</b> 该策略设置仅影响“关闭 Windows”对话框。它不会禁止用户使用其他方法与远程桌面服务会话断开连接。该策略设置也不会禁止服务器上断开连接的会话。您可以在<b>计算机配置 &gt; 管理模板 &gt; Windows 组件 &gt; 远程桌面服务 &gt; RD 会话主机 &gt; 会话时间限制</b>文件夹中配置“设置已中断会话的时间限制”策略设置以控制断开连接的会话在服务器上保持活动状态的时间。</p> |
| Optimize visual experience when using RemoteFX   | <p>可以使用该策略设置指定远程用户在使用 RemoteFX 的远程桌面连接 (RDC) 连接中获得的视觉体验。您可以使用该策略在使用的网络带宽与提供的图形体验类型之间获得平衡。</p> <p>根据用户的要求，您可以降低屏幕捕获速率以减少使用的网络带宽。也可以降低图像质量（增加执行的图像压缩量）以减少使用的网络带宽。</p> <p>如果网络带宽高于平均值，您可以选择最高的屏幕捕获速率设置和最高的图像质量设置以最大限度利用带宽。</p> <p>默认情况下，将优化使用 RemoteFX 的远程桌面连接会话以在 LAN 条件下获得均衡的体验。如果禁用或未配置该策略设置，则使用 RemoteFX 的远程桌面连接会话是相同的，就好像选择了中等屏幕捕获速率和中等图像压缩设置（默认行为）一样。</p>   |
| Set compression algorithm for RDP data           | <p>可以使用该策略设置指定要使用的远程桌面协议 (RDP) 压缩算法。</p> <p>默认情况下，服务器使用基于服务器的硬件配置的 RDP 压缩算法。</p> <p>如果启用该策略设置，您可以指定要使用的 RDP 压缩算法。如果选择优化以使用较少内存的算法，该选项使用较少的内存，但使用更多的网络带宽。如果选择优化以使用较少网络带宽的算法，该选项使用较少的网络带宽，但使用更多的内存。此外，还可以使用平衡使用的内存和网络带宽的第三个选项。</p> <p>也可以选择不使用 RDP 压缩算法。选择不使用 RDP 压缩算法将使用更多的网络带宽；只有在使用旨在优化网络流量的硬件设备时，才建议这样做。即使选择不使用 RDP 压缩算法，仍会压缩某些图形数据。</p> <p>如果禁用或未配置该策略设置，则使用默认 RDP 压缩算法。</p>  |



| 设置  | 说明  |
|---|---|
| Optimize visual experience for Remote Desktop Services sessions | <p>可以使用该策略设置指定远程用户在远程桌面服务会话中获得的视觉体验。然后，对远程计算机上的远程会话进行优化以支持该视觉体验。</p> <p>默认情况下，将针对丰富的多媒体优化远程桌面服务会话，例如，使用 <b>Silverlight</b> 或 <b>Windows Presentation Foundation</b> 的应用程序。</p> <p>如果启用该策略设置，您必须选择要优化远程桌面服务会话的视觉体验。您可以选择“丰富的多媒体”或“文本”。</p> <p>如果禁用或未配置该策略设置，则会为丰富的多媒体优化远程桌面服务会话。</p>   |
| Start a program on connection                                   | <p>配置远程桌面服务以在连接时自动运行指定的程序。</p> <p>您可以使用该设置指定在用户登录到远程计算机时自动运行的程序。</p> <p>默认情况下，远程桌面服务会话提供对整个 <b>Windows</b> 桌面的访问，除非服务器管理员或用户在配置客户端连接时指定了不同的设置。启用该设置将覆盖服务器管理员或用户设置的“启动程序”设置。不会显示“开始”菜单和 <b>Windows</b> 桌面；在用户退出程序时，将自动注销会话。</p> <p>要使用该设置，请在“程序路径和文件名”中键入在用户登录时运行的可执行文件的完全限定路径和文件名。如果需要，请在“工作目录”中键入指向程序启动目录的完全限定路径。如果将“工作目录”保留空白，则使用默认工作目录运行程序。如果指定的程序路径、文件名或工作目录不是有效的目录名称，<b>RDS</b> 主机连接将失败并显示错误消息。</p> <p>如果将状态设置为“已启用”，则远程桌面服务会话自动运行指定的程序并将指定的工作目录或程序默认目录（如果未指定工作目录）作为程序工作目录。</p> <p>如果将状态设置为“已禁用”或“未配置”，则远程桌面服务会话以完整桌面启动，除非服务器管理员或用户指定了不同的设置。有关详细信息，请参阅<b>计算机配置 &gt; 管理模板 &gt; 系统 &gt; 登录</b>文件夹中的“在用户登录时运行这些程序”策略设置。</p> <p><b>注</b> 该设置显示在“计算机配置”和“用户配置”中。如果配置了两个设置，则“计算机配置”设置覆盖“用户配置”设置。</p> |
| Always show desktop on connection                               | <p>该策略设置确定在客户端连接到远程计算机后是始终显示桌面，还是可以运行初始程序。可以使用该设置要求在客户端连接到远程计算机后显示桌面，即使已在默认用户配置文件、远程桌面连接、远程桌面服务客户端中或通过组策略指定了初始程序。</p> <p>如果启用该策略设置，在客户端连接到远程计算机时，将始终显示桌面。该策略设置覆盖任何初始程序策略设置。</p> <p>如果禁用或未配置该策略设置，则可以指定在客户端连接到远程计算机后在远程计算机上运行的初始程序。如果未指定初始程序，则在客户端连接到远程计算机后始终在远程计算机上显示桌面。</p> <p><b>注</b> 如果启用该策略设置，则忽略“连接时启动程序”策略设置。</p>  |

| 设置  | 说明  |
|---|---|
| Allow desktop composition for remote desktop sessions | <p>可以使用该策略设置指定是否允许远程桌面会话使用桌面拼合。该策略设置不适用于 <b>RemoteApp</b> 会话。</p> <p>桌面拼合为远程桌面会话提供 <b>Windows Aero</b> 用户界面元素，例如，半透明窗口。由于 <b>Windows Aero</b> 需要使用额外的系统和带宽资源，允许远程桌面会话使用桌面拼合可能会降低连接性能（尤其是通过慢速链路）和增加远程计算机负载。</p> <p>如果启用该策略设置，则允许远程桌面会话使用桌面拼合。在客户端计算机上，您可以在远程桌面连接 (RDC) 中的“体验”选项卡上配置桌面拼合，或者使用远程桌面协议 (.rdp) 文件中的“允许桌面拼合”设置进行配置。此外，客户端计算机还必须具有所需的硬件以支持 <b>Windows Aero</b> 功能。</p> <p><b>注</b> 可能需要在远程计算机上进行额外的配置以使远程桌面会话能够使用 <b>Windows Aero</b> 功能。例如，必须在远程计算机上安装桌面体验功能，并且必须将远程计算机上的最大颜色深度设置为每像素 32 位。此外，还必须在远程计算机上启动主题服务。</p> <p>如果禁用或未配置该策略设置，则不允许远程桌面会话使用桌面拼合，即使在 RDC 或 .rdp 文件中启用了桌面拼合。</p> |
| Do not allow font smoothing                           | <p>可以使用该策略设置指定是否允许远程连接使用字体平滑。</p> <p>字体平滑为远程连接提供 <b>ClearType</b> 功能。<b>ClearType</b> 是一种显示计算机字体的技术，以使字体更清晰平滑，尤其是在使用 LCD 显示器时。由于字体平滑需要使用额外的带宽资源，禁止远程连接使用字体平滑可以提高连接性能，尤其是通过慢速链路。</p> <p>默认情况下，允许远程连接使用字体平滑。您可以在远程桌面连接 (RDC) 中的“体验”选项卡上配置字体平滑，或者使用远程桌面协议 (.rdp) 文件中的“允许字体平滑”设置进行配置。</p> <p>如果启用该策略设置，则不允许远程连接使用字体平滑，即使在 RDC 或 .rdp 文件中启用了字体平滑。</p> <p>如果禁用或未配置该策略设置，则允许远程连接使用字体平滑。</p>  |
| Remove Windows Security item from Start menu          | <p>指定是否从远程桌面客户端的“设置”菜单中移除“<b>Windows 安全</b>”项。您可以使用此设置防止经验不足的用户无意中从远程桌面服务注销。</p> <p>如果状态设置为“已启用”，“开始”菜单上的“设置”中将不显示“<b>Windows 安全</b>”。这样，用户必须键入诸如 <b>CTRL+ALT+END</b> 的安全注意序列才能在客户端计算机上打开“<b>Windows 安全</b>”对话框。</p> <p>如果状态设置为“已禁用”或“未配置”，“<b>Windows 安全</b>”将保留在“设置”菜单中。</p>  |

## RDS 安全性设置

RDS 安全组策略设置控制是否允许本地管理员自定义权限。

Horizon 7 RDS 组策略设置安装在 **计算机配置 > 策略 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 安全性** 文件夹中。

表 5-35. RDS 安全组策略设置

| 设置   | 说明   |
|--|--|
| Server Authentication Certificate Template | <p>可以使用该策略设置指定确定自动选择哪个证书以对 RDS 主机进行身份验证的证书模板名称。</p> <p>在 RDP 连接期间使用 SSL (TLS 1.0) 保护客户端和 RDS 主机之间的通信安全时，需要使用证书以对 RDS 主机进行身份验证。</p> <p>如果启用该策略设置，您需要指定证书模板名称。在自动选择用于对 RDS 主机进行身份验证的证书时，仅考虑使用指定的证书模板创建的证书。只有在未选择特定的证书时，才会自动选择证书。</p> <p>如果找不到使用指定的证书模板创建的证书，RDS 主机将发出证书注册请求并在完成请求之前使用当前证书。如果找到多个使用指定的证书模板创建的证书，将选择最晚到期并与当前 RDS 主机名称匹配的证书。</p> <p>如果禁用或未配置该策略设置，则默认使用自签名证书对 RDS 主机进行身份验证。您可以在远程桌面会话主机配置工具的“常规”选项卡上选择用于对 RDS 主机进行身份验证的特定证书。</p> <p><b>注</b> 如果选择特定证书以用于对 RDS 主机进行身份验证，该证书将优先于该策略设置。</p>  |
| Set client connection encryption level     | <p>指定在远程桌面协议 (RDP) 连接期间是否需要使用特定加密级别保护客户端和 RDS 主机之间的通信安全。</p> <p>如果启用该设置，则在远程连接期间客户端和 RDS 主机之间的所有通信必须使用该设置中指定的加密方法。默认情况下，加密级别设置为“高”。可以使用以下加密方法：</p> <ul style="list-style-type: none"> <li>■ <b>High</b>。“高”设置使用 128 位强加密对在客户端和服务端之间发送的数据进行加密。可以在仅包含 128 位客户端（例如，运行远程桌面连接的客户端）的环境中使用该加密级别。不支持该加密级别的客户端无法连接到 RDS 主机服务器。</li> <li>■ <b>Client Compatible</b>。“客户端兼容”设置使用客户端支持的最大密钥强度对在客户端和服务端之间发送的数据进行加密。可以在包含不支持 128 位加密的客户端的环境中使用该加密级别。</li> <li>■ <b>Low</b>。“低”设置仅使用 56 位加密对从客户端发送到服务器的数据进行加密。</li> </ul> <p>如果禁用或未配置该设置，则不会通过组策略强制使用用于到 RDS 主机的远程连接的加密级别。不过，您可以使用远程桌面会话主机配置工具为这些连接配置所需的加密级别。</p> <p><b>重要事项</b> 可以通过<b>计算机配置 &gt; Windows 设置 &gt; 安全设置 &gt; 本地策略 &gt; 安全选项</b>文件夹中的“系统加密: 将 FIPS 兼容算法用于加密、哈希和签名”策略设置或远程桌面会话主机配置中的“FIPS 兼容”设置配置 FIPS 兼容。“FIPS 兼容”设置使用 Microsoft 加密模块和联邦信息处理标准 (FIPS) 140-1 加密算法加密和解密在客户端和服务端之间发送的数据。在客户端和 RDS 主机之间的通信需要使用最高的加密级别时，请使用该加密级别。如果已通过“系统加密: 将 FIPS 兼容算法用于加密、哈希和签名”组策略设置启用了 FIPS 兼容，该设置将覆盖在该组策略设置或远程桌面会话主机配置工具中指定的加密级别。</p> |

| 设置  | 说明   |
|---|--|
| Always prompt for password upon connection                          | <p>指定远程桌面服务是否始终在连接时提示客户端输入密码。</p> <p>您可以使用该设置强制提示登录到远程桌面服务的用户输入密码，即使他们已在远程桌面连接客户端中提供了密码。</p> <p>默认情况下，远程桌面服务允许用户在远程桌面连接客户端中输入密码以自动登录。</p> <p>如果启用该设置，则用户无法在远程桌面连接客户端中提供其密码以自动登录到远程桌面服务。将提示他们输入密码以进行登录。</p> <p>如果禁用该设置，则用户始终可以在远程桌面连接客户端中提供其密码以自动登录到远程桌面服务。</p> <p>如果未配置该设置，则不会在组策略级别指定自动登录。不过，管理员仍然可以使用远程桌面会话主机配置工具强制提示输入密码。</p>   |
| Require secure RPC communication                                    | <p>指定 RDS 主机是要求所有客户端进行安全的 RPC 通信，还是允许进行不安全的通信。</p> <p>您可以使用该设置仅允许经过身份验证并加密的请求以增强与客户端的 RPC 通信的安全性。</p> <p>如果启用该设置，则远程桌面服务接受来自支持安全请求的 RPC 客户端的请求，并且不允许与不受信任的客户端进行不安全的通信。</p> <p>如果禁用该设置，则远程桌面服务始终要求保护所有 RPC 流量的安全。不过，未响应该请求的 RPC 客户端允许进行不安全的通信。</p> <p>如果未配置该设置，则允许进行不安全的通信。</p> <p><b>注</b> RPC 接口用于管理和配置远程桌面服务。</p>  |
| Require use of specific security layer for remote (RDP) connections | <p>指定在远程桌面协议 (RDP) 连接期间是否需要使用特定安全层保护客户端和 RDS 主机之间的通信安全。</p> <p>如果启用该设置，则在远程连接期间客户端和 RDS 主机之间的所有通信必须使用该设置中指定的安全方法。可以使用以下安全方法：</p> <ul style="list-style-type: none"> <li>■ <b>Negotiate</b>。“协商”方法强制使用客户端支持的最安全方法。如果支持传输层安全 (TLS) 1.0 版，则使用该版本对 RDS 主机进行身份验证。如果不支持 TLS，则使用本地远程桌面协议 (RDP) 加密保护通信安全，但不会对 RDS 主机进行身份验证。</li> <li>■ <b>RDP</b>。RDP 方法使用本地 RDP 加密保护客户端和 RDS 主机之间的通信安全。如果选择该设置，则不会对 RDS 主机进行身份验证。</li> <li>■ <b>SSL (TLS 1.0)</b>。SSL 方法要求使用 TLS 1.0 对 RDS 主机进行身份验证。如果不支持 TLS，连接将失败。</li> </ul> <p>如果禁用或未配置该设置，则不会通过组策略强制使用用于到 RDS 主机的远程连接的安全方法。不过，您可以使用远程桌面会话主机配置工具为这些连接配置所需的安全方法。</p> |

| 设置  | 说明  |
|---|---|
| Require user authentication for remote connections by using Network | <p>可以使用该策略设置指定是否要求使用网络级别身份验证对远程连接到 RDS 主机的用户进行身份验证。该策略设置要求在远程连接过程早期对用户进行身份验证以增强安全性。</p> <p>如果启用该策略设置，仅支持网络级别身份验证的客户端计算机可以连接到 RDS 主机。</p> <p>要确定客户端计算机是否支持网络级别身份验证，请在客户端计算机上启动远程桌面连接，单击“远程桌面连接”对话框左上角的图标，然后单击“关于”。在“关于远程桌面连接”对话框中，查找词语“支持网络级别的身份验证”。</p> <p>如果禁用或未配置该策略设置，在允许远程连接到 RDS 主机之前，不要求使用网络级别身份验证对用户进行身份验证。</p> <p>您可以使用远程桌面会话主机配置工具或“系统属性”中的“远程”选项卡指定需要使用网络级别身份验证对用户进行身份验证。</p> <hr/> <p><b>重要事项</b> 如果禁用或未配置该策略设置，则具有较低的安全性，因为用户身份验证是在远程连接过程后期进行的。</p> |
| Do not allow local administrators to customize permissions          | <p>指定是否在远程桌面会话主机配置工具中禁用管理员自定义安全权限的权利。</p> <p>您可以使用此设置阻止管理员对远程桌面会话主机配置工具中“权限”选项卡上的用户组进行更改。默认情况下，管理员能够进行此类更改。</p> <p>如果状态设置为“已启用”，远程桌面会话主机配置工具中的“权限”选项卡无法用于自定义每连接安全描述符或更改现有组的默认安全描述符。所有安全描述符均为只读。</p> <p>如果状态设置为“已禁用”或“未配置”，则服务器管理员对远程桌面会话主机配置工具中“权限”选项卡上的用户安全描述符具有完整读/写特权。</p> <hr/> <p><b>注</b> 首选的用户访问权限管理方法是将用户添加到远程桌面用户组。</p>  |

## RDS 会话时间限制

通过使用 RDS 会话时间限制组策略设置，用户可以为 RDS 主机上的会话设置时间限制策略。

Horizon 7 RDS 组策略设置安装在**计算机配置 > 策略 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 会话时间限制**文件夹中。

Horizon 7 RDS 组策略设置还安装在**用户配置 > 管理模板 > Windows 组件 > 远程桌面服务 > 远程桌面会话主机 > 会话时间限制**文件夹中。

表 5-36. RDS 会话时间限制组策略设置

| 设置  | 说明  |
|---|---|
| Set time limit for disconnected sessions                            | <p>可以使用该策略设置为断开连接的远程桌面服务会话配置时间限制。</p> <p>您可以使用该策略设置指定断开连接的会话在服务器上保持活动状态的最长时间。默认情况下，远程桌面服务允许用户从远程桌面服务会话中断开连接，而无需注销并结束会话。</p> <p>在会话处于断开连接状态时，运行的程序将保持活动状态，即使用户当前不再处于连接状态。默认情况下，这些断开连接的会话在服务器上保留无限长的时间。</p> <p>如果启用该策略设置，则在指定的时间后从服务器中删除断开连接的会话。要强制使用默认行为以将断开连接的会话保留无限长的时间，请选择“从不”。如果具有控制台会话，则断开连接的会话时间限制不适用。</p> <p>如果禁用或未配置该策略设置，则将断开连接的会话保留无限长的时间。您可以在远程桌面会话主机配置工具中的“会话”选项卡上指定断开连接的会话的时间限制。</p> <p><b>注</b> 该策略设置显示在“计算机配置”和“用户配置”中。如果配置了两个策略设置，则优先使用“计算机配置”策略设置。</p>  |
| Set time limit for active but idle Remote Desktop Services sessions | <p>可以使用该策略设置指定活动远程桌面服务会话在自动断开连接之前处于空闲状态（无用户输入）的最长时间。</p> <p>如果启用该策略设置，您必须在“空闲会话限制”下拉列表中选择所需的时间限制。在超过指定的时间后，远程桌面服务自动断开连接活动但空闲的会话。用户在会话断开连接之前两分钟收到警告，以使用户可以按下键或移动鼠标以将会话保持活动状态。如果具有控制台会话，则空闲会话时间限制不适用。</p> <p>如果禁用或未配置该策略设置，则远程桌面服务允许将会话保持活动但空闲状态无限长的时间。您可以在远程桌面会话主机配置工具中的“会话”选项卡上指定活动但空闲的会话的时间限制。</p> <p>如果在到达时间限制时希望远程桌面服务终止而不是断开连接会话，您可以在<b>计算机配置 &gt; 管理模板 &gt; Windows 组件 &gt; 远程桌面服务 &gt; 远程桌面会话主机 &gt; 会话时间限制</b>文件夹中配置“达到时间限制时终止会话”策略设置。</p> <p><b>注</b> 该策略设置显示在“计算机配置”和“用户配置”中。如果配置了两个策略设置，则优先使用“计算机配置”策略设置。</p> |

| 设置  | 说明  |
|---|---|
| <p>Set time limit for active Remote Desktop Services sessions</p> | <p>可以使用该策略设置指定远程桌面服务会话在自动断开连接之前处于活动状态的最长时间。</p> <p>如果启用该策略设置，您必须在“活动会话限制”下拉列表中选择所需的时间限制。在超过指定的时间后，远程桌面服务自动断开连接活动会话。用户在远程桌面服务会话断开连接之前两分钟收到警告，以使用户可以保存打开的文件并关闭程序。如果具有控制台会话，则活动会话时间限制不适用。</p> <p>如果禁用或未配置该策略设置，则远程桌面服务允许将会话保持活动状态无限长的时间。您可以在远程桌面会话主机配置工具中的“会话”选项卡上指定活动会话的时间限制。</p> <p>如果在到达时间限制时希望远程桌面服务终止而不是断开连接会话，您可以在<b>计算机配置 &gt; 管理模板 &gt; Windows 组件 &gt; 远程桌面服务 &gt; 远程桌面会话主机 &gt; 会话时间限制</b>文件夹中配置“达到时间限制时终止会话”策略设置。</p> <p><b>注</b> 该策略设置显示在“计算机配置”和“用户配置”中。如果配置了两个策略设置，则优先使用“计算机配置”策略设置。</p> |



| 设置   | 说明  |
|--|---|
| <p>Terminate session when time limits are reached</p>  | <p>指定是否终止超时的远程桌面服务会话，而不是将其断开连接。您可以使用该设置指示远程桌面服务在达到活动或空闲会话的时间限制后终止该会话（即，注销用户并从服务器中删除该会话）。默认情况下，远程桌面服务断开连接达到时间限制的会话。</p> <p>时间限制是由服务器管理员在本地或组策略中设置的。请参阅“设置活动的远程桌面服务会话的时间限制”和“设置活动但空闲的远程桌面服务会话的时间限制”设置。</p> <p>如果启用该设置，则远程桌面服务终止达到超时限制的任何会话。</p> <p>如果禁用该设置，则远程桌面服务始终断开连接超时的会话，即使服务器管理员指定了不同的设置。</p> <p>如果未配置该设置，则远程桌面服务断开连接超时的会话，除非在本地设置中指定了不同的设置。</p> <p><b>注</b> 该设置仅适用于在远程桌面会话主机配置工具或组策略管理控制台有意设置的超时限制，而不适用于由于连接或网络状况而发生的超时事件。还要注意，该设置显示在“计算机配置”和“用户配置”中。如果配置了两个设置，则“计算机配置”设置优先。</p> |
| <p>Set time limit for logoff of RemoteApp sessions</p> | <p>可以使用该策略设置指定从 RDS 主机中注销用户的远程应用程序会话之前将该会话保持断开连接状态的时间。</p> <p>默认情况下，如果用户关闭远程应用程序，则将会话与 RDS 主机断开连接。</p> <p>如果启用该策略设置，在用户关闭远程应用程序时，远程应用程序会话将保持断开连接状态，直到达到指定的时间限制。在达到指定的时间限制时，将从 RDS 主机中注销远程应用程序会话。如果用户在达到时间限制之前启动远程应用程序，用户将重新连接到 RDS 主机上断开连接的会话。</p> <p>如果禁用或未配置该策略设置，在用户关闭远程应用程序时，会话将与 RDS 主机断开连接。</p> <p><b>注</b> 该策略设置显示在“计算机配置”和“用户配置”中。如果配置了两个策略设置，则优先使用“计算机配置”策略设置。</p>   |

## RDS 临时文件夹设置

RDS 连接组策略设置控制远程桌面服务会话的临时文件夹创建和删除操作。

**表 5-37. RDS 临时文件夹组策略设置**

| 设置                                       | 描述  |
|--|---|
| Do not delete temp folder upon exit      | <p>指定远程桌面服务在注销时是否保留用户的每会话临时文件夹。</p> <p>您可以使用该设置保留远程计算机上的用户会话特定临时文件夹，即使用户从会话注销也是如此。默认情况下，当用户注销时远程桌面服务会删除用户的临时文件夹。</p> <p>如果状态设置为“已启用”，当用户从会话注销时会保留用户的每会话临时文件夹。</p> <p>如果状态设置为“已禁用”，则当用户注销时会删除临时文件夹，即使管理员在远程桌面会话主机配置工具中另行指定也是如此。</p> <p>如果状态设置为“未配置”，远程桌面服务会在注销时从远程计算机删除临时文件夹，除非服务器管理员另行指定。</p> <p><b>注</b> 仅当每会话临时文件夹在服务器中正在使用时，此设置才生效。即，如果您启用“请勿使用每会话临时文件夹”设置，则此设置无效。</p>                                 |
| Do not use temporary folders per session | <p>此策略设置允许您阻止远程桌面服务创建会话特定临时文件夹。</p> <p>您可以使用此策略设置禁用远程计算机上为每个会话创建单独的临时文件夹。默认情况下，远程桌面服务为用户在远程计算机上保留的每个活动会话创建单独的临时文件夹。这些临时文件夹在远程计算机上 <b>Temp</b> 文件夹中的用户配置文件文件夹下创建，并使用 <b>sessionid</b> 命名。</p> <p>如果启用此策略设置，则不会创建每会话临时文件夹。相反，远程计算机上用户针对所有会话的临时文件夹存储在远程计算机上用户配置文件文件夹下的通用 <b>Temp</b> 文件夹中。</p> <p>如果禁用此策略设置，会始终创建每会话临时文件夹，即使在远程桌面会话主机配置工具中另行指定也是如此。</p> <p>如果未配置此策略设置，将会创建每会话临时文件夹，除非在远程桌面会话主机配置工具中另行指定。</p> |

## 为虚拟打印筛选打印机

启用虚拟打印功能后，用户可以从远程桌面和应用程序打印到客户端系统上的任何可用打印机。您可以使用**指定在重定向客户端打印机时使用的筛选器**代理组策略设置，防止虚拟打印功能将特定客户端打印机重定向到远程桌面和应用程序。

**指定在重定向客户端打印机时使用的筛选器**组策略设置在 VMware Horizon 打印机重定向 ADMX 模板文件 (vdm\_agent\_printing.admx) 中提供，该文件捆绑在 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip 文件中。有关安装说明，请参阅[将 ADMX 模板文件添加到 Active Directory](#)。

启用**指定在重定向客户端打印机时使用的筛选器**组策略设置时，您必须在**注册表值名称**：

**PrinterFilterString** 文本框中键入筛选规则。筛选规则是一个正则表达式，用于指定不应重定向的打印机（黑名单）。与筛选规则中的打印机不匹配的任何打印机均会被重定向。默认情况下，筛选规则为空，这意味着将重定向所有客户端打印机。

下表列出了您在筛选规则中可以使用的属性、运算符和通配符。

**表 5-38. 筛选规则支持的属性、运算符和通配符**

| 属性                                  | 运算符          | 通配符   |
|-------------------------------------|--------------|-------|
| DriverName、VendorName 和 PrinterName | AND、OR 和 NOT | * 和 ? |

下面列举了筛选规则的几个示例。

```
(DriverName="DrName1" OR VendorName="VeName1") AND NOT PrinterName="PrNa.?e"

PrinterName=".*HP.*" OR PrinterName=".*EPSON.*" AND DriverName="PDF"

PrinterName!=".*PDFCreator.*"
```

在虚拟桌面或 RDS 主机上安装 Horizon Agent 时，您可以启用虚拟打印功能。有关安装说明，请参阅《在 Horizon 7 中设置虚拟桌面》和《在 Horizon 7 中设置已发布的桌面和应用程序》文档。

## 设置基于位置的打印

基于位置的打印功能可将物理位置接近客户端系统的打印机映射到远程桌面，从而使用户能够从远程桌面打印到本地打印机和网络打印机。

IT 组织可以通过基于位置的打印将远程桌面映射到与终端客户端设备最近的打印机。以医生为例，无论他在医院的哪个房间打印文档，其打印作业都会发送到最近的一台打印机。

基于位置的打印功能适用于 Windows、Mac、Linux 和移动客户端设备。此功能还适用于基于浏览器的客户端。

**注** 如果您使用 HTML Access 连接到远程桌面和已发布的应用程序，则将不支持使用 MAC 地址或客户端名称的基于位置的打印策略。

以下远程桌面和应用程序支持基于位置的打印：

- 在单用户计算机上部署的桌面，包括 Windows 桌面和 Windows Server 计算机
- 在 RDS 主机上部署的已发布桌面和已发布应用程序，其中 RDS 主机为虚拟机或物理机
- 从远程桌面内的 Horizon Client 启动的已发布应用程序

要使用基于位置的打印功能，必须随 Horizon Agent 一起安装“虚拟打印”安装选项，并在桌面上安装正确的打印机驱动程序。

通过配置 Active Directory 组策略设置 AutoConnect Map Additional Printers for VMware View，您可以设置基于位置的打印功能，该设置位于 Microsoft 组策略对象编辑器计算机配置下的软件设置文件夹中。

**注** AutoConnect Map Additional Printers for VMware View 是一个针对计算机的策略。无论哪个用户连接到桌面，针对计算机的策略都会应用于所有远程桌面。

**AutoConnect Map Additional Printers for VMware View** 作为一个名称转换表实施。您可以使用表中的每一行识别一个特定的打印机，并为该打印机定义一组转换规则。转换规则确定打印机是否被映射到远程桌面以供某个特定客户端系统使用。

当用户连接到远程桌面时，**Horizon 7** 会将客户端系统与表中每个打印机所关联的转换规则进行比较。如果客户端系统符合为某个打印机设置的所有转换规则，或者某个打印机没有关联的转换规则，则 **Horizon 7** 会在用户会话过程中将该打印机映射到远程桌面。

您可以根据客户端系统的 IP 地址、名称和 MAC 地址，以及用户的名称和所在的组来定义转换规则。可以为某个特定打印机指定一个转换规则或者若干转换规则的组合。

用于将打印机映射到远程桌面的信息存储在远程桌面上的一个注册表项中，其位置为：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect。

## 基于位置的打印的打印机设置

用户从桌面注销或断开连接后，基于位置的打印机的打印机设置仍会保留。例如，用户可将基于位置的打印机设置为黑白模式。用户注销并重新登录到桌面后，基于位置的打印机将继续使用黑白模式。

要在已发布应用程序中的会话之间保存打印机设置，用户必须在应用程序的打印对话框中选择基于位置的打印机，右键单击所选打印机，然后选择**打印首选项**。如果用户在应用程序的打印对话框中选择打印机并单击**首选项**按钮，则不会保存打印机设置。

如果打印机设置保存在打印机驱动程序的专用空间中，而不是 **Microsoft** 建议的打印机驱动程序的 **DEVMODE** 扩展部分，则不支持基于位置的打印机的永久设置。要支持永久设置，请部署设置保存在打印机驱动程序的 **DEVMODE** 部分中的打印机。

## 注册基于位置的打印组策略 DLL 文件

您必须注册 DLL 文件 **TPVMGPoACmap.dll**，才能为基于位置的打印配置组策略设置。

32 位和 64 位版本的 **TPVMGPoACmap.dll** 在名为 **VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip** 的 .zip 文件中提供，其中，**x.x.x** 是版本，**yyyyyyy** 是内部版本号。您可以从 **VMware** 下载站点中下载该文件，网址为 <http://www.vmware.com/go/downloadview>。

### 步骤

- 1 将适当版本的 **TPVMGPoACmap.dll** 文件复制到您的 **Active Directory** 服务器或者您用来配置组策略的域计算机中。
- 2 用 **regsvr32** 实用程序注册 **TPVMGPoACmap.dll** 文件。

例如：**regsvr32 "C:\TPVMGPoACmap.dll"**

### 后续步骤

为基于位置的打印配置组策略设置。

## 配置基于位置的打印组策略

要设置基于位置的打印，您需要配置 AutoConnect Map Additional Printers for VMware View 组策略设置。该组策略设置是一个将打印机映射到 Horizon 桌面的名称转换表。

### 前提条件

- 确认您的 Active Directory 服务器上或者您用来配置组策略的域计算机上具有可用的 Microsoft MMC 和组策略对象编辑器插件。
- 在您的 Active Directory 服务器上或者您用来配置组策略的域计算机上注册 DLL 文件 TPVMGPoACmap.dll。请参阅[注册基于位置的打印组策略 DLL 文件](#)。
- 熟悉 AutoConnect Map Additional Printers for VMware View 组策略设置的语法。请参阅[基于位置的打印组策略设置语法](#)。
- 为基于位置的组策略设置创建 GPO，并将其链接到包含您的 Horizon 桌面的 OU。有关如何为 Horizon 组策略创建 GPO 的示例，请参阅[为 Horizon 7 组策略创建 GPO](#)。
- 确认在桌面中随 Horizon Agent 安装了虚拟打印安装选项。要对此进行验证，请检查 TP 自动连接服务和 TP VC 网关服务是否安装在桌面操作系统中。
- 由于打印作业直接从 Horizon 桌面发送到打印机，因此请确认桌面上安装了必需的打印机驱动程序。

### 步骤

- 1 在 Active Directory 服务器中，编辑 GPO。

| AD 版本        | 导航路径  |
|--------------|---|
| Windows 2003 | <ol style="list-style-type: none"> <li>a 选择开始 &gt; 所有程序 &gt; 管理工具 &gt; Active Directory 用户和计算机。</li> <li>b 右键单击包含您的 Horizon 桌面的 OU，然后选择属性。</li> <li>c 在组策略选项卡上，单击打开以打开组策略管理插件。</li> <li>d 在右侧窗格中，右键单击您为基于位置的打印组策略设置创建的 GPO，然后选择编辑。</li> </ol> |
| Windows 2008 | <ol style="list-style-type: none"> <li>a 选择开始 &gt; 管理工具 &gt; 组策略管理。</li> <li>b 展开您的域，右键单击为基于位置的打印组策略设置创建的 GPO 并选择编辑。</li> </ol>   |

屏幕上将显示组策略对象编辑器窗口。

- 2 展开计算机配置，打开软件设置文件夹，并选择为 VMware View 自动连接映射其他打印机。
- 3 在“策略”窗格中，双击配置自动连接映射其他打印机。

屏幕上将显示为 VMware View 自动连接映射其他打印机窗口。

- 4 选择已启用以启用组策略设置。

组策略窗口中将显示转换表标题和按钮。

---

**重要事项** 单击已禁用将删除所有表条目。作为预防措施，您可以保存配置以便将来进行导入。

---

- 5 添加您希望映射到 Horizon 桌面的打印机，并定义其关联的转换规则。
- 6 单击确定保存更改。

## 基于位置的打印组策略设置语法

您使用 AutoConnect Map Additional Printers for VMware View 组策略设置将打印机映射到远程桌面。

AutoConnect Map Additional Printers for VMware View 是一个名称转换表，用于标识打印机和定义关联的转换规则。表 5-39. 转换表的列和值 介绍了该转换表的语法。

基于位置的打印将本地打印机映射到远程桌面，但不支持映射使用 UNC 路径配置的网络打印机。

**表 5-39. 转换表的列和值**

| 列            | 说明  |
|--------------|---|
| IP Range     | <p>指定客户端系统 IP 地址范围的转换规则。</p> <p>要指定特定范围的 IP 地址，请使用以下表示法：<br/><b><i>ip_address -ip_address</i></b></p> <p>例如： <b>10.112.116.0-10.112.119.255</b></p> <p>要指定特定子网中的所有 IP 地址，请使用以下表示法：<br/><b><i>IP 地址/子网掩码位</i></b></p> <p>例如： <b>10.112.4.0/22</b></p> <p>此表示法指定了从 10.112.4.1 到 10.112.7.254 的可用 IPv4 地址。</p> <p>键入星号可匹配任意 IP 地址。</p> <hr/> <p><b>重要事项</b> 在 IPv6 混合模式环境中，为一个打印机添加两个 IP 地址范围（一个范围用于 IPv4 地址，另一个范围用于 IPv6 地址），以确保该打印机显示在远程会话中，而无论 Horizon Client 使用哪种协议进行连接。</p> |
| Client Name  | <p>指定计算机名的转换规则。</p> <p>例如： <b>Mary's Computer</b></p> <p>键入星号可匹配任意计算机名。</p>   |
| Mac Address  | <p>指定 MAC 地址的转换规则。在 GPO 编辑器中，所使用的格式必须与客户端系统所用格式保持一致。例如：</p> <ul style="list-style-type: none"> <li>■ Windows 客户端使用连字符： <b>01-23-45-67-89-ab</b></li> <li>■ Linux 客户端使用冒号： <b>01:23:45:67:89:ab</b></li> </ul> <p>键入星号可匹配任意 MAC 地址。</p>  |
| User/Group   | <p>指定用户名或组名的转换规则。</p> <p>要指定特定的用户或组，请使用以下表示法：<br/><b><i>\\domain\user_or_group</i></b></p> <p>例如： <b>\\\\mydomain\\Mary</b></p> <p>完全限定域名 (FQDN) 不是受支持的域名表示法。键入星号可匹配任意用户名或组名。</p>   |
| Printer Name | <p>打印机映射到远程桌面时的名称。</p> <p>例如： <b>PRINTER-2-CLR</b></p> <p>映射的名称不必与客户端系统上的打印机名称一致。</p> <p>打印机必须位于客户端设备本地。不支持映射 UNC 路径中的网络打印机。</p>  |

| 列                      | 说明   |
|------------------------|--|
| Printer Driver         | 打印机使用的驱动程序名称。<br>例如: <b>HP Color LaserJet 4700 PS</b><br><br><b>重要事项</b> 由于打印作业直接从远程桌面发送到打印机, 因此, 必须在远程桌面上安装打印机驱动程序。                               |
| IP Port/ThinPrint Port | 对于网络打印机, 其 IP 地址带有 <b>IP_</b> 前缀。<br>例如: <b>IP_10.114.24.1</b><br>默认端口为 <b>9100</b> 。您可以通过将端口号附加到 IP 地址来指定非默认端口。<br>例如: <b>IP_10.114.24.1:9104</b> |
| Default                | 指明打印机是否为默认打印机。   |

您可以使用栏标题上方显示的按钮来添加、删除和移动行, 以及保存和导入表条目。每个按钮都有一个等效的键盘快捷键。将鼠标停放在每个按钮上可以看到该按钮的说明和等效的键盘快捷键。例如, 要在表末尾插入一行, 可单击第一个表按钮, 或者按 **Alt+A** 键。单击最后两个按钮可导入和保存表条目。

表 5-40. 基于位置的打印组策略设置示例 显示了包含两行的转换表示例。

**表 5-40. 基于位置的打印组策略设置示例**

| IP Range (IP 范围)              | Client Name (客户名称) | Mac Address (Mac 地址) | User/ User/ Group (用户/组) | Printer Name (打印机名称) | Printer Driver (打印机驱动程序)  | IP Port/ThinPrint Port (IP 端口/ThinPrint 端口) | 默认 |
|-------------------------------|--------------------|----------------------|--------------------------|----------------------|---------------------------|---|----|
| *                             | *                  | *                    | *                        | PRINTER-1-CLR        | HP Color LaserJet 4700 PS | IP_10.114.24.1                              |    |
| 10.112.116.140-10.112.116.145 | *                  | *                    | *                        | PRINTER-2-CLR        | HP Color LaserJet 4700 PS | IP_10.114.24.2                              | X  |

对于任何客户端系统, 第一行中指定的网络打印机都将映射到远程桌面, 因为所有转换规则栏中都显示有星号。只有当客户端系统具有 10.112.116.140 到 10.112.116.145 范围之间的 IP 地址时, 第二行中指定的网络打印机才会映射到远程桌面。

## 管理特殊的 Unity 窗口

在使用已发布的应用程序时, 您可以使用 **Unity 筛选器规则列表** 代理组策略设置来筛选 Unity 窗口, 或将 Unity 窗口映射到特定类型。如果您遇到窗口显示问题 (例如窗口中出现黑色背景, 或下拉窗口的大小不正确), 则此功能非常有用。

**Unity 筛选器规则列表** 组策略设置在 VMware View Agent 配置 ADMX 模板文件 (vdm\_agent.admx) 中提供, 该文件捆绑在 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip 文件中。有关安装说明, 请参阅 [将 ADMX 模板文件添加到 Active Directory](#)。



启用 **Unity 筛选器规则列表** 组策略设置时，需单击**显示**，并在**值**文本框中键入一个筛选规则。筛选规则由特性和操作组成。如果指定 **map** 操作，则还必须包含类型。下表列出了可在筛选规则中使用的特性、操作和类型。

**表 5-41. Unity 筛选器规则的特性、操作和类型**

| 特性   | 操作        | 类型   |
|--|-----------|--|
| classname、company、product、major、minor、build、revision | block、map | normal、panel、dialog、tooltip、splash、toolbar、dock、desktop、widget、combobox、startscreen、sidepanel、taskbar、metrofullscreen、metro docked |

窗口类名通常是首选的特性，例如 `classname = CustomClassName`。如果您必须将规则限制到特定产品，则可以提供 **company**、**product**、**major**、**minor**、**build** 和 **revision** 特性。您可以在可执行文件的**属性**窗口中找到这些特性的值。这些特性的值必须精确匹配大小写，包括任何特殊字符。如果提供多个特性，则所有值都必须匹配，才能将规则应用到窗口。

要指定某个操作，需键入 `action=value`，例如 `action=block`。**block** 操作告知 Horizon Agent 不要在客户端上显示窗口。当客户端上的窗口显示过大或干扰正常的窗口焦点行为时，请使用 **block** 操作。

**map** 操作（例如 `action=map`）告知 Horizon Agent 将窗口视为某种经过硬编码的类型。要指定类型，您必须在规则中包含 `type=value`，例如 `type=normal`。由于很难确定窗口是否映射到错误的类型，因此，只有在 VMware 技术支持团队指示您将窗口映射到某个类型时，您才需要这样做。

## 筛选规则示例

以下筛选规则会阻止所有类名为“MyClassName”的窗口。

```
classname=MyClassName;action=block
```

以下筛选规则会阻止名为“MyProduct”的产品中的所有窗口。

```
product=MyProduct;action=block
```

以下筛选规则会将自定义类映射到组合框类型。

```
classname=MyClassName;action=map;type=combobox
```

**注** 与在 RDS 主机上的 %ProgramData%\VMware\RdeServer\Unity Filters 目录内的文件中指定的筛选规则相比，**Unity 筛选器规则列表** 组策略设置具有较低优先级。

## Active Directory 组策略示例

在 Horizon 7 中实施 Active Directory 组策略的一种方法是提供远程桌面会话的计算机创建一个 OU，然后将一个或多个 GPO 链接到该 OU。您可以使用这些 GPO 将组策略设置应用于 Horizon 7 计算机。

如果策略设置适用于域中的所有计算机，您可以直接将 GPO 链接到域。但是作为一种最佳做法，大多数部署应将 GPO 链接到单个 OU，以免在域中的所有计算机上处理策略。

您可以在 **Active Directory** 服务器或域中的任意计算机上配置策略。本示例显示了如何直接在 **Active Directory** 服务器上配置策略。

---

**注** 由于每个 Horizon 7 环境各有不同，因此您可能需要执行不同的步骤来满足组织的特定需求。

---

## 为 Horizon 7 计算机创建 OU

要将组策略应用于提供远程桌面会话的计算机且不影响同一 **Active Directory** 域中的其他 Windows 计算机，可以专门为 Horizon 7 计算机创建一个 OU。您可以为整个 Horizon 7 部署创建一个 OU，也可以分别为虚拟桌面计算机和 RDS 主机创建不同的 OU。

### 步骤

- 1 在 **Active Directory** 服务器上，选择**开始 > 所有程序 > 管理工具 > Active Directory 用户和计算机**。
- 2 右键单击包含您的 Horizon 7 计算机的域，然后选择**新建 > 组织单位**。
- 3 为组织单位键入一个名称，然后单击**确定**。

新组织单位将显示在左侧窗格中。

- 4 将 Horizon 7 计算机添加到新 OU。

- a 单击左侧窗格中的**计算机**。

域中的所有计算机对象都将显示在右侧窗格中。

- b 在右侧面板中右键单击代表 Horizon 7 计算机的计算机对象的名称，然后选择**移动**。
- c 选择组织单位，然后单击**确定**。

选择 OU 时，Horizon 7 计算机将显示在右侧窗格中。

### 后续步骤

为 Horizon 7 组策略创建 GPO。

## 为 Horizon 7 组策略创建 GPO

创建 GPO 以包含针对 Horizon 7 组件和基于位置的打印功能的组策略，然后将它们链接到您的 Horizon 7 计算机的组织单位 (OU)。

### 前提条件

- 为您的 Horizon 7 计算机创建一个 OU。
- 确认您能够以管理员域用户的身份登录到托管 **Active Directory** 服务器的计算机。
- 确认 MMC 和组策略管理插件在您的 **Active Directory** 服务器上可用。

### 步骤

- 1 在 **Active Directory** 服务器上，打开组策略管理控制台。
- 2 展开您的域，右键单击包含您的 Horizon 7 计算机的 OU，然后选择**在这个域中创建 GPO 并在此处链接**。

- 3 为 GPO 键入名称，并单击**确定**。

新 GPO 将显示在左侧窗格中该组织单位的下方。

- 4 (可选) 将 GPO 应用于 OU 中的特定 Horizon 7 计算机。
  - a 从左侧窗格中选择所需的 GPO。
  - b 选择**安全过滤 > 添加**。
  - c 键入 Horizon 7 计算机的计算机名，然后单击**确定**。

Horizon 7 计算机将显示在“安全过滤”窗格中。GPO 中的设置将仅应用于这些计算机。

#### 后续步骤

将 Horizon ADMX 模板添加到 GPO。

## 将 Horizon 7 ADMX 模板文件添加到 GPO

要将 Horizon 7 组件组策略设置应用到您的桌面和应用程序，可将其 ADMX 模板文件添加到 GPO。

#### 前提条件

- 为 Horizon 7 组件组策略设置创建 GPO，并将其链接到包含您的 Horizon 7 虚拟机的组织单位。
- 确认您能够以管理员域用户的身份登录到托管 Active Directory 服务器的计算机。
- 确认 MMC 和组策略管理插件在您的 Active Directory 服务器上可用。

#### 步骤

- 1 从 VMware 下载站点中下载 Horizon 7 GPO 捆绑包 .zip 文件，网址为 <https://my.vmware.com/web/vmware/downloads>。

在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 GPO 捆绑包。

该文件名为 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip，其中 x.x.x 是版本号，yyyyyyy 是内部版本号。为 Horizon 7 提供组策略设置的所有 ADMX 文件均在此文件中提供。

- 2 解压缩 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 文件，并将 ADMX 文件复制到 Active Directory 服务器。
  - a 将 .admx 文件和 en-US 文件夹复制到 Active Directory 服务器上的 %systemroot%\PolicyDefinitions 文件夹。
  - b 将语言资源文件 (.adml) 复制到 Active Directory 服务器上 %systemroot%\PolicyDefinitions\ 中的相应子文件夹。
- 3 在 Active Directory 服务器上，打开组策略管理编辑器并在该编辑器中输入模板文件在安装后所在的路径。

#### 后续步骤

为您的 Horizon 7 计算机配置组策略设置并启用环回处理。

## 为远程桌面启用环回处理

要将通常应用于某个计算机的“用户配置”设置应用于登录该计算机的所有用户，请启用环回处理。

### 前提条件

- 为 Horizon 7 组件组策略设置创建 GPO，并将其链接到包含您的 Horizon 7 虚拟机的组织单位。
- 确认您能够以管理员域用户的身份登录到托管 Active Directory 服务器的计算机。
- 确认 MMC 和组策略管理插件在您的 Active Directory 服务器上可用。

### 步骤

- 1 在 Active Directory 服务器上，打开组策略管理控制台。
- 2 展开您的域，右键单击为组策略设置创建的 GPO 并选择**编辑**。
- 3 在组策略管理编辑器中，导航到**计算机配置 > 策略 > 管理模板: 策略定义 > 系统 > 组策略**。
- 4 在右侧窗格中，双击**用户组策略环回处理模式**。
- 5 选择**已启用**，然后从**模式**下拉菜单中选择一个环回处理模式。

| 选项                 | 操作  |
|--------------------|---|
| <b>Merge（合并）</b>   | 应用的用户策略设置结合了计算机 GPO 与用户 GPO 中包含的设置。如果发生冲突，则优先选用计算机 GPO。 |
| <b>Replace（替换）</b> | 用户策略完全由与计算机关联的 GPO 定义。任何与用户关联的 GPO 都将被忽略。               |

- 6 单击**确定**保存更改。