

在 View 中设置桌面和应用 程序池

VMware Horizon 7 7.0



vmware®

在 **View** 中设置桌面和应用程序池

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

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
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

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

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

版权所有 © 2019 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

目录

在 **View** 中设置桌面和应用程序池 12

1 桌面和应用程序池简介 13

场、**RDS** 主机以及桌面和应用程序池 13

桌面池的优势 14

特定类型员工的桌面池 15

任务型员工池 15

知识型员工和超级用户池 16

Kiosk 用户池 17

应用程序池的优点 18

2 准备未受管的计算机 19

为远程桌面部署准备未受管计算机 19

在未受管计算机上安装 **Horizon Agent** 20

适用于未管理的计算机的 **Horizon Agent** 自定义安装选项 21

3 为克隆创建并准备父虚拟机 23

为克隆创建虚拟机 23

在 **vSphere** 中创建虚拟机 24

安装客户机操作系统 26

为远程桌面部署准备客户机操作系统 26

准备 **Windows Server** 操作系统供桌面使用 28

在 **Windows Server 2008 R2** 上安装桌面体验 29

在 **Windows Server 2012** 或 **2012 R2** 上安装桌面体验 29

将 **Windows** 防火墙服务配置为在出现故障后重新启动 30

在虚拟机上安装 **Horizon Agent** 30

Horizon Agent 自定义安装选项 32

静默安装 **Horizon Agent** 34

Microsoft Windows Installer 命令行选项 35

Horizon Agent 的静默安装属性 37

为 **Horizon Agent** 配置具有多个网卡的虚拟机 40

优化客户机操作系统性能 41

禁用 **Windows** 客户体验改善计划 42

为即时克隆和 **View Composer** 链接克隆虚拟机优化 **Windows** 43

禁用 **Windows** 服务和任务所带来的优势 43

引起即时克隆和链接克隆中磁盘增长的 **Windows** 服务和任务 43

在 **Windows** 父虚拟机中禁用计划的磁盘碎片整理 45

- 禁用 Windows Update 46
- 在 Windows 虚拟机上禁用诊断策略服务 46
- 在 Windows 虚拟机上禁用预取和超级获取功能 47
- 在 Windows 虚拟机上禁用 Windows 注册表备份 47
- 在 Windows 虚拟机上禁用系统还原 48
- 在 Windows 虚拟机上禁用 Windows Defender 48
- 禁用 Windows 虚拟机中的 Microsoft Feeds Synchronization 48
- 准备父虚拟机 49
 - 配置父虚拟机 49
 - 激活即时克隆和 View Composer 链接克隆上的 Windows 51
 - 在父虚拟机中禁用 Windows 休眠功能 52
 - 为 View Composer 链接克隆配置本地存储 52
 - 记录 View Composer 父虚拟机的页面文件大小 52
 - 延长 ClonePrep 和 QuickPrep 自定义脚本的超时限制 53
- 创建虚拟机模板 54
- 创建自定义规范 54
- 4 创建包含完整虚拟机的自动桌面池 55**
 - 包含完整虚拟机的自动池 55
 - 用于创建包含完整虚拟机的自动池的工作表 55
 - 创建包含完整虚拟机的自动池 58
 - 克隆自动桌面池 59
 - 包含完整虚拟机的自动池的桌面设置 60
- 5 创建链接克隆桌面池 62**
 - 链接克隆桌面池 62
 - 用于创建链接克隆桌面池的工作表 62
 - 创建链接克隆桌面池 70
 - 克隆自动桌面池 71
 - 链接克隆桌面池的桌面池设置 72
 - View Composer 对链接克隆 SID 和第三方应用程序的支持 73
 - 选择 QuickPrep 或 Sysprep 来自定义链接克隆计算机 74
 - 在 View Composer 操作期间将链接克隆计算机保持已置备状态以在远程桌面会话中使用 78
 - 针对链接克隆使用现有的 Active Directory 计算机帐户 78
- 6 创建即时克隆桌面池 80**
 - 即时克隆桌面池 80
 - 映像发布和重新平衡即时克隆桌面池 82
 - 添加即时克隆域管理员 82
 - 用于创建即时克隆桌面池的工作表 83
 - 创建即时克隆桌面池 85

[ClonePrep 客户机自定义](#) 86

[即时克隆维护实用程序](#) 87

7 创建手动桌面池 90

[手动桌面池](#) 90

[用于创建手动桌面池的工作表](#) 90

[创建手动桌面池](#) 92

[创建包含一个虚拟机的手动池](#) 93

[手动池的桌面池设置](#) 94

8 设置远程桌面服务主机 96

[远程桌面服务主机](#) 96

[在 Windows Server 2008 R2 上安装远程桌面服务](#) 98

[在 Windows Server 2012 或 2012 R2 上安装远程桌面服务](#) 98

[在 Windows Server 2008 R2 上安装桌面体验](#) 99

[在 Windows Server 2012 或 2012 R2 上安装桌面体验](#) 99

[限制用户只能进行单个会话](#) 100

[在远程桌面服务主机上安装 Horizon Agent](#) 100

[适用于 RDS 主机的 Horizon Agent 自定义安装选项](#) 101

[从嵌套会话内启动的远程应用程序打印](#) 103

[为 RDS 桌面和应用程序会话启用时区重定向](#) 103

[为应用程序启用基本的 Windows 主题](#) 104

[配置组策略以启动 Runonce.exe](#) 105

[RDS 主机性能选项](#) 105

[为 RDS 主机配置 3D 图形](#) 106

9 创建场 108

[场](#) 108

[为自动场准备父虚拟机](#) 109

[准备 RDS 主机父虚拟机](#) 109

[在链接克隆 RDS 主机上激活 Windows](#) 111

[在父虚拟机中禁用 Windows 休眠功能](#) 111

[用于创建手动场的工作表](#) 112

[用于创建自动场的工作表](#) 113

[创建手动场](#) 116

[创建自动场](#) 117

10 创建应用程序池 118

[应用程序池](#) 118

[用于手动创建应用程序池的工作表](#) 118

[创建应用程序池](#) 119

11 创建 RDS 桌面池 121

了解 RDS 桌面池 121

创建 RDS 桌面池 122

适用于 RDS 桌面池的桌面池设置 122

为 RDS 桌面池配置 Internet Explorer 中的 Adobe Flash 调节 123

12 置备桌面池 124

桌面池中的用户分配 124

手动命名计算机或提供命名模式 125

指定计算机名称列表 126

为自动桌面池使用命名模式 127

计算机命名示例 128

将计算机添加到通过名称列表置备的自动池中 129

手动自定义计算机 131

在维护模式下自定义计算机 131

自定义单个计算机 131

适用于所有桌面池类型的桌面池设置 132

Adobe Flash 质量和调节 135

为桌面池设置电源策略 136

桌面池的电源策略 136

将专用计算机配置为在用户断开连接后挂起 138

电源策略如何影响自动桌面池 138

具有浮动分配的自动池电源策略示例 139

具有专用分配的自动池电源策略示例 140

防止 View 电源策略冲突 140

为桌面配置 3D 呈现 140

3D 呈现器选项 144

配置 3D 呈现的最佳实践 146

准备 vDGA 功能 147

准备 NVIDIA GRID vGPU 功能 148

准备使用采用 vDGA 的 AMD 多用户 GPU 功能 149

配置采用 vDGA 的 AMD 多用户 GPU 149

检查 ESXi 主机上的 GPU 资源 151

阻止通过 RDP 访问 View 桌面 151

部署大型桌面池 152

在包含超过 8 个主机的群集上配置桌面池 152

向桌面池分配多个网络标签 153

13 授权用户和组 154

为桌面池或应用程序池添加授权 154

- 移除对桌面池或应用程序池的授权 155
- 查看桌面或应用程序池授权 155
- 限制远程桌面访问 155
 - 受限制的授权示例 156
 - 标签匹配 157
 - 与受限制的授权相关的考虑因素及限制因素 158
 - 为 View 连接服务器实例分配标签 158
 - 为桌面池分配标签 158
- 限制网络外部的远程桌面访问 159
 - 限制网络外部的用户 159

14 配置远程桌面功能 161

- 配置 Unity Touch 161
 - Unity Touch 的系统要求 162
 - 配置 Unity Touch 显示的收藏的应用程序 162
- 为多播流或单播流配置 Flash URL 重定向 164
 - Flash URL 重定向的系统要求 165
 - 验证是否安装了 Flash URL 重定向功能 166
 - 设置提供多播或单播流的网页 167
 - 为 Flash URL 重定向设置客户端设备 167
 - 禁用或启用 Flash URL 重定向 168
- 配置 Flash 重定向 168
 - Flash 重定向的要求 170
 - 安装并配置 Flash 重定向 170
 - 使用 Windows 注册表设置配置 Flash 重定向 173
- 配置 URL 内容重定向 174
 - URL 内容重定向的要求和限制 175
 - 安装具有 URL 内容重定向功能的 Horizon Client 176
 - 安装具有 URL 内容重定向功能的 Horizon Agent 176
 - 在 Active Directory 中添加 URL 内容重定向 ADM 模板 177
 - VMware Horizon URL 内容重定向模板设置 178
- 配置实时音频-视频 180
 - 实时音频-视频的配置选择 181
 - 实时音频-视频的系统要求 181
 - 确保使用的是实时音频-视频而非 USB 重定向 182
 - 选择首选网络摄像头和麦克风 183
 - 配置实时音频-视频组策略设置 190
 - 实时音频-视频带宽 193
- 配置扫描仪重定向 193
 - 扫描仪重定向的系统要求 193
 - 扫描仪重定向的用户操作 194

配置扫描仪重定向组策略设置	195
配置串行端口重定向	197
串行端口重定向的要求	198
串行端口重定向的用户操作	199
有关配置串行端口重定向的准则	200
配置串行端口重定向组策略设置	200
配置 USB 到串口适配器	203
管理对 Windows Media 多媒体重定向 (MMR) 功能的访问	204
启用 View 中的多媒体重定向	204
Windows Media MMR 的系统要求	204
确定是否基于网络延迟使用 Windows Media MMR	205
管理对客户驱动器重定向的访问	206
使用组策略禁用客户驱动器重定向	207
使用注册表设置配置客户驱动器重定向	207
限制复制和粘贴操作的剪贴板格式	208
15 将 USB 设备与远程桌面和应用程序一起使用	210
USB 设备类型的相关限制	211
设置 USB 重定向概述	212
网络流量和 USB 重定向	213
自动连接到 USB 设备	213
在安全 View 环境中部署 USB 设备	214
对所有类型的设备禁用 USB 重定向	214
对特定设备禁用 USB 重定向	215
使用日志文件进行故障排除和确定 USB 设备 ID	216
使用策略控制 USB 重定向	217
为复合 USB 设备配置设备拆分策略设置	218
为 USB 设备配置过滤策略设置	220
USB 设备系列	223
Horizon Agent 配置 ADM 模板中的 USB 设置	224
排除 USB 重定向故障	227
16 降低并管理存储要求	229
使用 vSphere 管理存储	229
使用 Virtual SAN 实现高性能存储和基于策略的管理	231
Virtual SAN 数据存储的默认存储策略配置文件	232
使用虚拟卷实现以虚拟机为中心的存储和基于策略的管理	233
使用即时克隆减少存储需求	234
使用 View Composer 降低存储要求	235
确定即时克隆和 View Composer 链接克隆桌面池的存储大小	236
即时克隆和链接克隆池的大小调整原则	237

- 即时克隆和链接克隆池的大小计算公式 239
- 编辑池或在单独的数据存储中存储副本时创建克隆的大小计算公式 240
- View Composer 链接克隆虚拟机的存储过载 241
 - 设置链接克隆虚拟机的存储过载级别 241
- View Composer 链接克隆数据磁盘 242
- 在本地数据存储上存储 View Composer 链接克隆 243
- 将即时克隆和 View Composer 链接克隆的副本和克隆存储在不同的数据存储中 244
 - 将副本存储在单独数据存储中的可用性注意事项 245
- 为 View Composer 链接克隆配置 View Storage Accelerator 245
- 在 View Composer 链接克隆上回收磁盘空间 247
- 将 VAAI 存储用于 View Composer 链接克隆 248
- 为 View Composer 链接克隆设置 Storage Accelerator 和空间回收中断时间 249

17 配置桌面和应用程序池的策略 251

- 在 View Administrator 中设置策略 251
 - 配置全局策略设置 252
 - 配置桌面池策略 252
 - 配置用户策略 252
 - View 策略 253
- 使用 智能策略 253
 - 智能策略的要求 253
 - 安装 User Environment Manager 254
 - 配置 User Environment Manager 254
 - Horizon 智能策略设置 254
 - 带宽配置文件引用 255
 - 将条件添加到 Horizon 智能策略定义 256
 - 在 User Environment Manager 中创建 Horizon 智能策略 257
- 使用 Active Directory 组策略 258
 - 为远程桌面创建 OU 258
 - 为远程桌面启用环回处理 259
- 使用 View 组策略管理模板文件 259
- View ADM 和 ADMX 模板文件 259
- Horizon Agent 配置 ADM 模板设置 261
 - 发送到远程桌面的客户端系统信息 263
 - 在 View 桌面上运行命令 266
- PCoIP 策略设置 267
 - PCoIP 常规设置 268
 - PCoIP 剪贴板设置 273
 - PCoIP 带宽设置 275
 - PCoIP 键盘设置 277
 - PCoIP 无损构建功能 277

- VMware Blast 策略设置 278
 - 为 VMware Blast 启用无损压缩 281
- 使用远程桌面服务组策略 281
 - 配置 RDS 每设备 CAL 存储 281
 - 将远程桌面服务 ADMX 文件添加到 Active Directory 282
 - RDS 应用程序兼容性设置 283
 - RDS 连接设置 284
 - RDS 设备和资源重定向设置 284
 - RDS 许可设置 285
 - RDS 配置文件设置 286
 - RDS 远程会话环境设置 288
 - RDS 安全性设置 288
 - RDS 临时文件夹设置 289
- 设置基于位置的打印 289
 - 注册基于位置的打印组策略 DLL 文件 290
 - 配置基于位置的打印组策略 291
 - 基于位置的打印组策略设置语法 292
- Active Directory 组策略示例 294
 - 为 View 计算机创建 OU 294
 - 为 View 组策略创建 GPO 295
 - 将 View ADM 模板添加到 GPO 中 296
 - 为远程桌面启用环回处理 296

18 使用 View Persona Management 配置用户配置文件 298

- 在 View 中提供用户配置 298
- 将 View Persona Management 用于独立系统 299
- 使用 View Persona Management 迁移用户配置文件 300
- 用户配置管理和 Windows 漫游配置文件 302
- 配置 View Persona Management 部署 303
 - 设置 View Persona Management 部署概述 303
 - 配置用户配置文件存储库 304
 - 使用 View Persona Management 选项安装 Horizon Agent 306
 - 安装独立的 View Persona Management 306
 - 添加 View Persona Management ADM 或 ADMX 模板文件 307
 - 配置 View Persona Management 策略 310
 - 创建使用用户配置管理的桌面池 312
- 配置 View Persona Management 部署的最佳实践 313
 - 将用户配置文件配置为包含 ThinApp 沙箱文件夹 315
 - 使用 View Persona Management 配置 View Composer 永久磁盘 315
 - 管理独立笔记本电脑上的用户配置文件 316
- View Persona Management 组策略设置 316

- 漫游和同步组策略设置 318
- 文件夹重定向组策略设置 320
- 桌面 UI 组策略设置 323
- 日志组策略设置 323

19 排除计算机和桌面池的问题 325

- 显示出现问题的计算机 325
- 向桌面用户发送消息 326
- 桌面池置备或重新创建问题 327
 - 即时克隆置备或推送映像故障 327
 - 即时克隆映像发布失败 327
 - 在即时克隆置备期间无休止地进行错误恢复 327
 - 无法删除孤立的即时克隆 328
 - 如果找不到自定义规范，创建池操作将失败 328
 - 因权限问题导致池创建操作失败 328
 - 因配置问题导致池置备失败 329
 - 由于 View 连接服务器实例无法连接 vCenter 导致池置备失败 330
 - 因数据存储问题导致池置备失败 330
 - vCenter Server 过载导致池置备失败 331
 - 虚拟机长时间处于“置备”状态 331
 - 虚拟机长时间处于“正在自定义”状态 332
 - 移除孤立的或已删除的链接克隆 332
 - 重复删除和重新创建的计算机故障排除 333
 - 排除 QuickPrep 自定义问题 334
 - 查找并取消保护未使用的 View Composer 副本 335
 - View Composer 置备错误 336
- 排除网络连接问题 338
 - 计算机与 View 连接服务器实例之间的连接问题 338
 - Horizon Client 与 PCoIP 安全网关之间的连接问题 339
 - 计算机与 View 连接服务器实例之间的连接问题 341
 - 由于将 IP 地址错误地分配给克隆计算机而导致的连接问题 342
- 排除 USB 重定向故障 342
- 管理未授权用户的计算机和策略 344
- 使用 ViewDbChk 命令解决数据库不一致问题 344
- 更多故障排除信息 347

在 View 中设置桌面和应用程序池

《在 View 中设置桌面和应用程序池》介绍了如何创建和置备在 Microsoft 远程桌面服务 (RDS) 主机上运行的计算机池和远程应用程序池。其中包含使用 View Persona Management 准备计算机、配置策略、授权用户和组、配置远程桌面功能以及配置用户配置文件。

目标读者

此信息适用于任何要创建和置备桌面池和应用程序池的用户。本文档中的信息专门为已熟练掌握虚拟机技术和数据中心操作、并具有丰富经验的 Windows 系统管理员编写。

桌面和应用程序池简介

借助 Horizon 7，您可以创建包含成千上万个虚拟桌面的桌面池。您可以部署在虚拟机 (Virtual Machine, VM)、物理机和 Windows 远程桌面服务 (Remote Desktop Services, RDS) 主机上运行的桌面。创建一个虚拟机作为基础映像后，Horizon 7 便可通过该映像生成大量虚拟桌面。还可以创建应用程序池，为用户提供这些应用程序的远程访问权限。

本章讨论了以下主题：

- 场、RDS 主机以及桌面和应用程序池
- 桌面池的优势
- 特定类型员工的桌面池
- 应用程序池的优点

场、RDS 主机以及桌面和应用程序池

您可以创建桌面和应用程序池，以便授予用户远程访问基于虚拟机的桌面、基于会话的桌面、物理机和应用程序的权限。您还可以选择 Microsoft 远程桌面服务 (Remote Desktop Services, RDS)、VMware PC-over-IP (PCoIP) 或 VMware Blast，以便向用户提供远程访问权限。

RDS 主机

RDS 主机是安装了 Windows 远程桌面服务和 Horizon Agent 的服务器计算机。这些服务器用于托管用户可以远程访问的应用程序和桌面会话。要访问 RDS 桌面池或应用程序，必须安装 Horizon Client 3.0 或更高版本。

桌面池

主要有三种类型的桌面池：自动、手动和 RDS。自动桌面池使用 vCenter Server 虚拟机模板或快照创建相同虚拟机的池。手动桌面池是现有 vCenter Server 虚拟机、物理计算机或第三方虚拟机的集合。在自动池或手动池中，每个计算机一次可供一位用户进行远程访问。RDS 桌面池不是计算机的集合，而是在 RDS 主机上为用户提供桌面会话。多个用户可以同时在一个 RDS 主机上拥有桌面会话。

应用程序池

应用程序池可用来将应用程序传送给多个用户。应用程序池中的应用程序在 RDS 主机的一个场中运行。

场

场是 RDS 主机的集合，可简化这些主机的管理。场所拥有的 RDS 主机数量可以变化，为用户提供应用程序或 RDS 桌面的公用集合。创建 RDS 桌面池或应用程序池时，必须指定场。场中的 RDS 主机为用户提供桌面和应用程序会话。

桌面池的优势

借助 Horizon 7，您可以创建桌面池，并将桌面池置备为集中管理的基础。

您可以通过以下来源创建远程桌面池：

- 物理桌面 PC 或 RDS 主机等物理系统
- 位于 ESXi 主机上并由 vCenter Server 管理的虚拟机
- 在虚拟化平台上运行的虚拟机，而非支持 Horizon Agent 的 vCenter Server。

如果将 vSphere 虚拟机作为桌面源使用，您可以按需要自动生成任意数量的相同虚拟桌面。您可以设置为池生成的虚拟桌面数量的最大值和最小值。设置这些参数可确保您始终能够获得足够的远程桌面来使用，同时又不会生成过多的桌面浪费可用资源。

使用池来管理桌面，您可以对池中的所有远程桌面应用设置或部署应用程序。以下示例介绍了一些可用设置：

- 指定远程桌面默认使用的远程显示协议，以及是否允许最终用户覆盖默认值。
- 对于 View Composer 链接克隆虚拟机或完整克隆虚拟机，指定在不使用时是否关闭虚拟机以及是否将其完全删除。将始终启动即时克隆虚拟机。
- 对于 View Composer 链接克隆虚拟机，您可以指定是使用 Microsoft Sysprep 自定义规范还是 VMware 的 QuickPrep。Sysprep 为池中的每个虚拟机生成唯一的 SID 和 GUID。即时克隆需要使用 VMware 提供的不同自定义规范（称为 ClonePrep）。

也可以指定如何为用户分配池中的桌面。

专用分配池

每个用户都被分配了一个特定的远程桌面，并在每次登录时返回同一个桌面。专用的分配池需要具有一对一的桌面到用户关系。例如，一个具有 100 个用户的组需要使用一个具有 100 个桌面的池。

浮动分配池

在每次使用远程桌面后可选择性地删除并重新创建远程桌面，从而形成高度可控的环境。

利用浮动分配池，您还可以创建可供轮班制用户使用的桌面池。例如，包含 100 个桌面的池可供 300 名轮班制用户（每班 100 个用户）使用。

特定类型员工的桌面池

View 提供多种功能来帮助您节约存储空间和降低各种应用情况下所需的处理能力。其中很多功能都是通过池设置来实现。

最基本的问题是衡量特定类型的用户，判定用户需要有状态桌面映像还是无状态桌面映像。需要有状态桌面映像的用户将其数据存放于必须保留、维护和备份的操作系统映像本身中。例如，这些用户会安装一些个人应用程序，或者拥有不能保存在虚拟机本身以外位置（如在文件服务器上或应用程序数据库中）的数据。

无状态桌面映像

无状态体系结构（也称为非持久桌面）具有许多优势，如易于支持和存储成本较低。此外，该体系结构还能限制虚拟机的备份需求，并提供更加简化、廉价的灾难恢复和业务连续性选项。

有状态桌面映像

这些映像（也称为持久桌面）可能需要使用传统映像管理方法。有状态映像与特定存储系统技术一起使用时，可降低存储成本。规划备份、灾难恢复和业务连续性策略时，VMware Consolidated Backup 和 VMware Site Recovery Manager 等备份和恢复技术都是重要的考量因素。

可以通过两种方法在 View 中创建无状态桌面映像：

- 您可以创建即时克隆虚拟机的浮动分配池。可以选择使用文件夹重定向和漫游配置文件存储用户数据。
- 您可以使用 View Composer 创建链接克隆虚拟机的浮动分配池。可以选择使用文件夹重定向和漫游配置文件存储用户数据。

可以通过几种方法在 View 中创建有状态桌面映像：

- 您可以创建即时克隆虚拟机的浮动分配池，并使用 App Volumes 连接用户数据和用户安装的应用程序。可以选择使用文件夹重定向和漫游配置文件存储用户数据。
- 您可以使用 View Composer 创建链接克隆虚拟机的专用分配池。您可以配置 View Composer 永久磁盘。
- 您可以创建完整克隆或完整虚拟机。一些存储供应商具有经济高效的完整克隆存储解决方案。这些供应商通常拥有自己的最佳实践和置备实用程序。如果使用其中某家供应商的技术，可能需要创建专用的分配池。

使用无状态桌面还是有状态桌面取决于具体的员工类型。

任务型员工池

您可以为任务型员工提供标准化无状态桌面映像，让映像随时保有易懂、易于支持的配置，因此员工可以登录到任意可用桌面。

由于任务型员工需要用一套为数不多的应用程序来执行重复性任务，因此您可以为其创建无状态桌面映像来节省存储空间并降低处理要求。使用以下池设置：

- 创建一个自动池，以便在创建池时创建桌面，或是根据池的利用率来按需生成桌面。
- 对于即时克隆池，要优化资源利用率，请使用按需置备以根据使用情况扩大或缩小池。请务必指定足够的备用桌面以满足登录速率要求。

- 使用浮动分配，以便用户能登录到任意可用桌面。如果所有用户都不需要在同一时间登录，该设置就可以减少所需的桌面数量。
- 创建即时克隆或 **View Composer** 链接克隆桌面，以使桌面共享相同的基础映像，并减少在数据中心内使用的存储空间（相对于完整虚拟机）。
- 对于 **View Composer** 桌面池，请确定在用户注销时执行的操作（如果有）。磁盘容量会不断增长。为节省磁盘空间，您可以在用户注销时将桌面刷新到原始状态。也可以设置计划来定期刷新桌面。例如，安排桌面每天、每周或每月刷新一次。
- 对于即时克隆桌面池，每次用户注销时，**View** 将自动删除即时克隆。将创建新的即时克隆并做好准备以供下一个用户登录时使用，从而在每次注销时有效地刷新桌面。
- 如果适用并且使用 **View Composer** 链接克隆池，请考虑在本地 **ESXi** 数据存储上存储桌面。这一策略的优势包括：使用价格低廉的硬件、快速置备虚拟机、实现高效的开关机以及简化管理等。有关限制信息，请参阅[在本地数据存储上存储 View Composer 链接克隆](#)。在本地数据存储上不支持即时克隆池。

注 有关其他类型的存储选项的信息，请参见第 16 章 [降低并管理存储要求](#)。

- 使用 **Persona Management** 功能，以便用户始终应用首选的桌面外观和应用程序设置，就像使用 **Windows** 用户配置文件一样。如果您未将桌面设置为在注销时刷新或删除，您可以配置在注销时移除用户配置。

重要事项 **View Persona Management** 为希望在会话期间保留设置的用户实施浮动分配池提供了便利。之前，浮动分配桌面的一个限制是：当最终用户注销时，他们会丢失其所有配置设置和存储在远程桌面中的所有数据。

每当最终用户登录时，其桌面背景即设置为默认壁纸，他们必须重新配置每个应用程序的首选项。使用 **View Persona Management**，浮动分配桌面的最终用户无法区分自身会话与专用分配桌面会话之间的差异。

知识型员工和超级用户池

知识型员工必须能够创建复杂的文档并将其保留在桌面上。超级用户则必须能够安装并保留其个人应用程序。根据所保留的个人数据的性质和数量，可以采用有状态或无状态类型的桌面。

对于不需要使用用户安装的应用程序（临时应用除外）的知识型员工，您可以创建无状态桌面映像，并将其所有个人数据保存在虚拟机以外的位置，如文件服务器或应用程序数据库中。对于其他知识型员工和超级用户，您可以为其创建有状态桌面映像。使用以下池设置：

- 一些超级用户和知识型员工（如会计、销售经理、市场营销研究分析师）可能需要每次登录到相同的桌面。请为他们创建专用的分配池。
- 使用 **Persona Management** 功能，以便用户始终应用首选的桌面外观和应用程序设置，就像使用 **Windows** 用户配置文件一样。
- 使用 **vStorage Thin Provisioning**，以便每一个桌面在最初都能仅使用磁盘在初始操作时所需的存储空间。

- 对于必须安装其个人应用程序（从而在操作系统磁盘中添加数据）的超级用户和知识型员工来说，共有两种选择。一种选择是创建完整虚拟机桌面，并使用 **Mirage** 部署和更新应用程序而不覆盖用户安装的应用程序。

另一种选择是创建链接克隆或即时克隆池，并使用 **App Volumes** 在登录之间永久保存用户安装的应用程序和用户数据。

- 如果知识型员工不需要使用用户安装的应用程序（临时使用除外），您可以创建 **View Composer** 链接克隆桌面或即时克隆桌面。桌面映像可以共享同一个基础映像，所需的存储空间也低于完整虚拟机。
- 如果您将 **View Composer** 与 **vSphere 5.1** 或更高版本的虚拟桌面共用，请为 **vCenter Server** 和桌面池启用空间回收功能。凭借空间回收功能，客户机操作系统中过期或已删除的数据将通过擦除和压缩流程自动回收。
- 如果您使用 **View Composer** 链接克隆桌面，需要实施 **View Persona Management**、漫游配置文件或其他配置文件管理解决方案。您也可以配置永久磁盘，以便刷新和重构链接克隆操作系统磁盘，并将用户配置文件的副本保存在永久磁盘上。
- 如果您使用即时克隆桌面，请实施漫游配置文件或其他配置文件管理解决方案。您不需要配置永久磁盘。您可以使用 **App Volumes** 保留用户数据和配置文件的副本。

Kiosk 用户池

Kiosk 用户包括机场登记处的乘客、教室或图书馆内的学生、医疗数据录入工作站的医护人员或自助服务点的顾客。由于用户无需登录即可使用客户端设备或远程桌面，因此与客户端设备（而非用户）关联的帐户才有权使用这些桌面池。但仍可要求用户提供身份验证凭据来访问某些应用程序。

由于用户数据无需保留在操作系统磁盘中，因此设置为在 **Kiosk** 模式中运行的虚拟机桌面使用无状态桌面映像。**Kiosk** 模式桌面用于在瘦客户端设备或锁定的 **PC** 中使用。您必须确保：桌面应用程序可通过身份验证机制保证交易安全、物理网络不会被篡改和偷窃，以及连接到网络的所有设备都是受信任的。

最佳实践是使用专用的 **View** 连接服务器实例处理 **Kiosk** 模式的客户端，并在 **Active Directory** 中为这些客户端的帐户创建专用的组织单位和组。这样不仅能防止这些系统遭受意外入侵，还会使客户端的配置和管理变得更加容易。

要设置 **kiosk** 模式，您必须使用 **vdadmin** 命令行界面并按照《**View** 管理指南》文档中有关 **kiosk** 模式的主题中所述内容来执行若干个操作步骤。在此设置过程中，您可以使用以下池设置。

- 创建一个自动池，以便在创建池时创建桌面，或是根据池的利用率来按需生成桌面。
- 使用浮动分配，使用户能够访问池中的任何可用桌面。
- 创建即时克隆或 **View Composer** 链接克隆桌面，以使桌面共享相同的基础映像，并减少在数据中心内使用的存储空间（相对于完整虚拟机）。
- 如果使用 **View Composer** 链接克隆桌面，请设置一个刷新策略以经常刷新桌面，例如，每次用户注销时。
- 如果使用即时克隆桌面池，每次用户注销时，**View** 将自动删除即时克隆。将创建新的即时克隆并做好准备以供下一个用户登录时使用，从而在每次注销时有效地刷新桌面。

- 如果适用，请考虑将桌面存储在本地 ESXi 存储中。这一策略的优势包括：使用价格低廉的硬件、快速置备虚拟机、实现高效的开关机以及简化管理等。有关限制信息，请参阅[在本地数据存储上存储 View Composer 链接克隆](#)。在本地数据存储上不支持即时克隆池。

注 有关其他类型的存储选项的信息，请参见 [第 16 章 降低并管理存储要求](#)。

- 使用 **Active Directory GPO**（组策略对象）配置基于位置的打印，以便桌面能够使用位置最近的打印机。有关可通过组策略管理 (ADM) 模板获得的设置的完整列表和描述，请参阅[第 17 章 配置桌面和应用程序池的策略](#)。
- 使用 **GPO** 或智能策略控制在启动桌面或将本地 **USB** 设备插入客户端计算机时是否将 **USB** 设备连接到桌面。

应用程序池的优点

利用应用程序池，您可以授权用户访问在数据中心内的服务器上（而不是在用户的个人计算机或设备上）运行的应用程序。

应用程序池具有多个显著优势：

- **可访问性**

用户可以从网络上的任何位置访问应用程序。您还可以配置安全网络访问。

- **设备独立性**

借助应用程序池，您可以支持多种客户端设备，如智能电话、平板电脑、笔记本电脑、瘦客户端和个人计算机。客户端设备可以运行各种操作系统，如 **Windows**、**iOS**、**Mac OS** 或 **Android**。

- **访问控制**

您可以轻松、快速地为一个人或一组用户授予或撤销访问应用程序的权限。

- **加速部署**

使用应用程序池时，由于您仅在数据中心内的服务器上部署应用程序，并且一台服务器可以支持多个用户，因此可以加快应用程序部署。

- **可管理性**

管理部署在客户端计算机和设备上的软件通常需要大量资源。管理任务包括部署、配置、维护、支持和升级。使用应用程序池时，由于软件在数据中心内的服务器上运行，需要的安装副本较少，因此您可以简化企业内的管理。

- **安全性和法规遵从性**

使用应用程序池时，由于应用程序及其关联的数据集中存在于数据中心内，因此可以提高安全性。数据集中可以解决安全性和法规遵从性问题。

- **降低成本**

根据软件许可协议，在数据中心托管应用程序更节省成本。其他因素（包括加快部署速度和提高可管理性）也可以降低企业内的软件成本。

准备未受管的计算机

用户可以访问由未受 vCenter Server 管理的计算机提供的远程桌面。这些未受管的计算机可包括物理机和除 vCenter Server 以外的虚拟化平台上运行的虚拟机。您必须对未受管的计算机进行适当准备才能提供远程桌面访问。

有关为用作远程桌面服务 (RDS) 主机的计算机进行准备的信息，请参阅[第 8 章 设置远程桌面服务主机](#)。

有关为远程桌面部署准备 Linux 虚拟机的信息，请参阅《《设置 Horizon 7 for Linux 桌面》》指南。

本章讨论了以下主题：

- [为远程桌面部署准备未受管计算机](#)
- [在未受管计算机上安装 Horizon Agent](#)

为远程桌面部署准备未受管计算机

必须执行一些特定任务，以便为部署远程桌面准备未受管计算机。

前提条件

- 确认对未受管计算机具有管理权限。
- 为确保远程桌面用户添加到未受管计算机的本地远程桌面用户组中，应在 Active Directory 中创建受限的远程桌面用户组。有关更多信息，请参阅《View 安装指南》文档。

步骤

- 1 打开未受管计算机的电源，并确认其可由 View 连接服务器实例访问。
- 2 将未受管计算机加入到远程桌面的 Active Directory 域中。
- 3 将 Windows 防火墙配置为允许远程桌面连接到未受管计算机。

后续步骤

在未受管计算机上安装 Horizon Agent。请参阅[在未受管计算机上安装 Horizon Agent](#)。

在未受管计算机上安装 Horizon Agent

您必须在所有未受管计算机上安装 Horizon Agent。如果不安装 Horizon Agent，View 将无法管理未受管计算机。

要在多个 Windows 物理机上安装 Horizon Agent，而无需响应向导提示，您可以静默安装 Horizon Agent。请参阅[静默安装 Horizon Agent](#)。

前提条件

- 确认对未受管计算机具有管理权限。
- 要使用未受管的 Windows Server 计算机作为远程桌面（而不是作为 RDS 主机），请执行[准备 Windows Server 操作系统供桌面使用](#)中所述的步骤。
- 熟悉适用于未受管计算机的 Horizon Agent 自定义安装选项。请参阅[适用于未管理的计算机的 Horizon Agent 自定义安装选项](#)。
- 熟悉 Horizon Agent 安装程序在防火墙上打开的 TCP 端口。有关更多信息，请参阅《View 体系结构规划指南》文档。
- 如果计算机安装了 Microsoft Visual C++ Redistributable 软件包，请确认软件包的版本为 2005 SP1 或更高版本。如果软件包的版本为 2005 或更低版本，可以升级或卸载该软件包。
- 从 VMware 产品页面 <http://www.vmware.com/go/downloadview> 下载 Horizon Agent 安装程序文件。

步骤

- 1 要启动 Horizon Agent 安装程序，请双击安装程序文件。

安装程序的文件名为 VMware-viewagent-y.y.y-xxxxxx.exe 或 VMware-viewagent-x86_64-y.y.y-xxxxxx.exe，其中 y.y.y 是版本号，xxxxxx 是内部版本号。

- 2 接受 VMware 许可条款。
- 3 选择 Internet 协议 (IP) 版本 (IPv4 或 IPv6)。

必须使用同一 IP 版本安装所有 View 组件。

- 4 选择启用还是禁用 FIPS 模式。

仅当在 Windows 中启用 FIPS 模式时，此选项才可用。

- 5 选择自定义安装选项。

- 6 接受或更改目标文件夹。

- 7 在**服务器**文本框中，键入 View 连接服务器主机的主机名或 IP 地址。

在安装过程中，安装程序会向此 View 连接服务器实例注册未受管的计算机。注册之后，指定的 View 连接服务器实例以及同一 View 连接服务器组中的其他任何实例，都可以与该未受管的计算机通信。

8 选择一个身份验证方法以便向 View 连接服务器实例注册未受管的计算机。

选项	操作
Authenticate as the currently logged in user （作为当前登录的用户进行身份验证）	用户名和密码文本框将被禁用，您将通过当前用户名和密码登录到 View 连接服务器实例。
指定管理员凭据	您必须在用户名和密码文本框中提供 View 连接服务器管理员的用户名和密码。

使用以下格式提供用户名：**Domain\User**。

用户帐户必须是有权访问 View 连接服务器实例上 View LDAP 的域用户。本地用户不适用。

9 按照 Horizon Agent 安装程序中的提示完成安装。

10 如果您选择了 USB 重定向选项，请重新启动未受管计算机来启用 USB 支持。

此外，**发现新硬件**向导也可能启动。在重新启动未受管计算机之前，请先按照向导中的提示配置硬件。

VMware Horizon Horizon Agent 服务将在未受管计算机上启动。

后续步骤

使用未受管的计算机创建远程桌面。请参阅[手动桌面池](#)。

适用于未管理的计算机的 Horizon Agent 自定义安装选项

在未管理的计算机上安装 Horizon Agent 时，您可以选择或取消选择特定的自定义安装选项。此外，Horizon Agent 还会在支持某些功能的所有客户机操作系统上自动安装这些功能。这些功能并非可选。

要在安装最新的 Horizon Agent 版本后更改自定义安装选项，您必须卸载并重新安装 Horizon Agent。对于修补程序和升级，您可以运行新的 Horizon Agent 安装程序并选择一组新的选项，而无需卸载以前的版本。

表 2-1. IPv4 环境中适用于未管理的计算机的 Horizon Agent 自定义安装选项（可选）

选项	说明
USB 重定向	<p>允许用户访问其桌面上本地连接的 USB 设备。</p> <p>在单用户计算机上部署的远程桌面上支持 USB 重定向。此外，RDS 桌面和应用程序上支持 USB 闪存驱动器和硬盘的重定向。</p> <p>默认情况下，不会选择该安装选项。必须选择此选项才会进行安装。</p> <p>有关安全地使用 USB 重定向的指导，请参阅《View 安全指南》指南。例如，可以使用组策略设置针对特定用户禁用 USB 重定向。</p>
客户端驱动器重定向	<p>允许 Horizon Client 用户与其远程桌面共享本地驱动器。</p> <p>安装此安装选项之后，无需在远程桌面上进行进一步配置。</p> <p>在受管的单用户虚拟机上运行的 VDI 桌面中以及在 RDS 桌面和应用程序中也支持客户端驱动器重定向。</p>
View Persona Management	<p>将本地桌面上的用户配置文件与远程配置文件存储库同步，确保用户无论在何时登录桌面，均可访问配置文件。</p>

选项	说明
智能卡重定向	允许用户在使用 PCoIP 或 Blast Extreme 显示协议时使用智能卡进行身份验证。 在单用户计算机上部署的远程桌面上支持智能卡重定向，但在基于 RDS 主机的远程桌面上不支持该功能。
虚拟音频驱动程序	在远程桌面上提供虚拟音频驱动程序。

在 IPv6 环境中，唯一的可选功能是智能卡重定向。

表 2-2. IPv4 环境中在未管理的计算机上自动安装的 Horizon Agent 功能（不可选）

功能	说明
PCoIP 代理	允许用户使用 PCoIP 显示协议连接至远程桌面。 使用 Teradici TERA 主机卡配置的物理机支持 PCoIP 代理功能。
Lync	在远程桌面上提供对 Microsoft Lync 2013 客户端的支持。
Unity Touch	允许平板电脑和智能手机用户与运行于远程桌面上的 Windows 应用程序轻松进行交互。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。

在 IPv6 环境中，唯一自动安装的功能是 PCoIP 代理。

为克隆创建并准备父虚拟机

您可以通过克隆 vCenter Server 虚拟机 (Virtual Machine, VM) 来创建桌面计算机池。在创建桌面池之前，您需要准备并配置此虚拟机，此虚拟机将作为克隆的父虚拟机。

有关为用作远程桌面服务 (RDS) 主机的计算机进行准备的信息，请参阅[第 8 章 设置远程桌面服务主机](#)。

有关准备 Linux 虚拟机以进行远程桌面部署的信息，请参阅《设置 Horizon 7 for Linux 桌面》指南。

注

- 从版本 7.0 开始，View Agent 更名为 Horizon Agent，View Administrator 更名为 Horizon Administrator。
 - 从 Horizon 7.0 起可以使用的显示协议 VMware Blast 也称为 VMware Blast Extreme。
-

本章讨论了以下主题：

- [为克隆创建虚拟机](#)
- [在虚拟机上安装 Horizon Agent](#)
- [静默安装 Horizon Agent](#)
- [为 Horizon Agent 配置具有多个网卡的虚拟机](#)
- [优化客户机操作系统性能](#)
- [禁用 Windows 客户体验改善计划](#)
- [为即时克隆和 View Composer 链接克隆虚拟机优化 Windows](#)
- [准备父虚拟机](#)
- [创建虚拟机模板](#)
- [创建自定义规范](#)

为克隆创建虚拟机

在部署克隆桌面池的过程中，第一步是在 vSphere 中创建虚拟机，然后安装并配置操作系统。

步骤

1 [在 vSphere 中创建虚拟机](#)

您可以在 vSphere 中从头创建虚拟机，或通过克隆现有虚拟机进行创建。此过程说明了如何从头创建虚拟机。

2 安装客户机操作系统

创建虚拟机后，必须安装客户机操作系统。

3 为远程桌面部署准备客户机操作系统

您必须执行某些特定操作来为远程桌面部署准备客户机操作系统。

4 准备 Windows Server 操作系统供桌面使用

要将 Windows Server 2008 R2 或 Windows Server 2012 R2 虚拟机用作单一会话 View 桌面（而不是用作 RDS 主机），必须在虚拟机中安装 Horizon Agent 之前执行某些步骤。还必须配置 View Administrator 以将 Windows Server 视为供 View 桌面使用的受支持操作系统。

5 在 Windows Server 2008 R2 上安装桌面体验

对于 RDS 桌面和应用程序以及在运行 Windows Server 的单用户虚拟机上部署的 VDI 桌面，扫描仪重定向需要您在 RDS 主机和单用户虚拟机中安装桌面体验功能。

6 在 Windows Server 2012 或 2012 R2 上安装桌面体验

对于 RDS 桌面和应用程序以及在运行 Windows Server 的单用户虚拟机上部署的 VDI 桌面，扫描仪重定向需要您在 RDS 主机和单用户虚拟机中安装桌面体验功能。

7 将 Windows 防火墙服务配置为在出现故障后重新启动

在进行置备后，部署为单一会话桌面的某些 Windows Server 2012 R2、Windows 8.1 和 Windows 10 计算机不会立即变得可用。如果 Windows 防火墙服务在其超时期限到期后未重新启动，则会出现此问题。您可以在父虚拟机或模板虚拟机上配置 Windows 防火墙服务，以确保桌面池中的所有计算机都变得可用。

在 vSphere 中创建虚拟机

您可以在 vSphere 中从头创建虚拟机，或通过克隆现有虚拟机进行创建。此过程说明了如何从头创建虚拟机。

前提条件

- 熟悉虚拟机自定义配置参数。请参阅[虚拟机自定义配置参数](#)。

步骤

- 1 登录到 vSphere Client。
- 2 选择文件 > 新建 > 虚拟机以启动新建虚拟机向导。
- 3 选择自定义，配置自定义配置参数。
- 4 选择在完成之前编辑虚拟机设置，然后单击继续配置硬件设置。
 - a 添加一个 CD/DVD 驱动器，将媒体类型设置为使用 ISO 映像文件，选择相应操作系统的 ISO 映像文件，然后选择打开电源时连接。
 - b 将开机引导延迟设置为 10,000 毫秒。
- 5 单击完成以创建虚拟机。

后续步骤

安装操作系统。

虚拟机自定义配置参数

为远程桌面部署创建虚拟机时，您可以使用虚拟机自定义配置参数作为基准设置。

使用 View Administrator 从虚拟机部署桌面池时，您可以更改某些设置。

表 3-1. 自定义配置参数

参数	描述和建议
Name and Location	虚拟机的名称和位置。 如果打算将该虚拟机用作模板，应当指定一个通用名称。位置可以是数据中心清单内的任意文件夹。
Host/Cluster	将运行该虚拟机的 ESXi Server 或服务器群集资源。 如果打算使用该虚拟机作为模板，则初始虚拟机的位置不必指定以后由模板创建的虚拟机将驻留的位置。
Resource Pool	如果物理 ESXi Server 资源分为若干资源池，您可以将它们分配给虚拟机。
Datastore	与虚拟机关联的文件的位置。
Hardware Machine Version	可用的硬件计算机版本取决于正在运行的 ESXi 版本。最佳实践是选择提供最强虚拟机功能的最新可用硬件计算机版本。某些 View 功能需要最低的硬件计算机版本。
Guest Operating System	在虚拟机中安装的操作系统的类型。
CPUs	虚拟机中虚拟处理器的数目。 对于大多数客户机操作系统来说，一个处理器已经足够。
Memory	分配给虚拟机的内存容量。 在多数情况下，512 MB 已经足够。
Network	虚拟机中虚拟网络适配器 (NIC) 的数目。 通常情况下，一个 NIC 已经足够。虚拟基础架构的网络名称应当一致。如果模板中的网络名称错误，将导致实例自定义阶段失败。 在具有多个网卡的虚拟机上安装 Horizon Agent 时，必须配置 Horizon Agent 使用的子网。请参阅 为 Horizon Agent 配置具有多个网卡的虚拟机 以了解详细信息。 重要事项 对于 Windows 7、Windows 8.*、Windows 10、Windows Server 2008 R2 和 Windows Server 2012 R2 操作系统，必须选择 VMXNET 3 网络适配器。使用默认的 E1000 适配器可能会导致虚拟机上出现自定义超时错误。要使用 VMXNET 3 适配器，必须安装 Microsoft 修补程序： 对于 Windows 7 SP1，请安装以下修补程序： <ul style="list-style-type: none">■ http://support.microsoft.com/kb/2550978 在安装 Horizon Agent 之前先安装修补程序。安装修补程序时，如果遇到 Windows Update 错误 0x80070424，请参阅 https://support.microsoft.com/en-us/kb/968002。■ https://support.microsoft.com/en-au/kb/2578159■ https://support.microsoft.com/en-au/kb/2661332 有关安装修补程序的详细信息，请参阅 https://ikb.vmware.com/kb/2073945。

参数	描述和建议
SCSI Controller	<p>在虚拟机中使用的 SCSI 适配器类型。</p> <p>在 Windows 8/8.1 和 Windows 7 客户机操作系统中，您应该指定 LSI Logic 适配器。LSI Logic 适配器性能更佳，与通用 SCSI 设备协作效果更好。</p> <p>LSI Logic SAS 仅在硬件版本为 7 和更高版本的虚拟机中可用。</p>
Select a Disk	<p>要在虚拟机中使用的磁盘。</p> <p>根据您的决定分配给每个用户的本地存储容量，创建一个新的虚拟磁盘。应为操作系统安装程序、修补程序以及本地安装的应用程序提供足够的存储空间。</p> <p>为降低磁盘空间和本地数据管理需求，您应当将用户的信息、配置文件和文档存储在网络共享位置，而不是本地磁盘。</p>

安装客户机操作系统

创建虚拟机后，必须安装客户机操作系统。

前提条件

- 确认 ESXi Server 上的数据存储中有客户机操作系统的 ISO 映像文件。
- 确认虚拟机中的 CD/DVD 驱动器指向客户机操作系统的 ISO 映像文件，并且配置为在开机时连接。

步骤

- 1 在 vSphere Client 中，登录到虚拟机所在的 vCenter Server 系统。
- 2 右键单击虚拟机，选择**电源**，然后选择**打开电源**启动虚拟机。

由于已将 CD/DVD 驱动器配置为指向客户机操作系统 ISO 映像并在开机时连接，因此客户机操作系统安装进程将自动开始。

- 3 单击**控制台**选项卡，按照操作系统供应商提供的安装说明操作。
- 4 激活 Windows。

后续步骤

为 View 桌面部署准备客户机操作系统。

为远程桌面部署准备客户机操作系统

您必须执行某些特定操作来为远程桌面部署准备客户机操作系统。

前提条件

- 创建虚拟机并安装客户机操作系统。
- 为远程桌面配置 Active Directory 域控制器。有关更多信息，请参阅《View 安装指南》文档。
- 为确保桌面用户添加到虚拟机的本地“远程桌面用户”组，在 Active Directory 中创建一个受限的“远程桌面用户”组。有关更多信息，请参阅《View 安装指南》文档。

- 验证是否已在虚拟机上启动了远程桌面服务。Horizon Agent 安装、SSO 和其他 View 操作都需要使用远程桌面服务。您可以通过配置桌面池设置和组策略设置来禁止通过 RDP 访问 View 桌面。请参阅[阻止通过 RDP 访问 View 桌面](#)。
- 确认您具有客户机操作系统的管理权限。
- 在 Windows Server 操作系统上，准备操作系统以供桌面使用。请参阅[准备 Windows Server 操作系统供桌面使用](#)。
- 如果您想要为您的桌面池配置 3D 图形呈现功能，请熟悉虚拟机的[启用 3D 支持](#)设置。

该设置适用于 Windows 7 及更高版本的操作系统。ESXi 5.1 及更高版本的主机也提供一些选项，可确定 ESXi 主机如何管理 3D 呈现器。有关详细信息，请参阅《vSphere 虚拟机管理指南》文档。

步骤

- 1 在 vSphere Client 中，登录到虚拟机所在的 vCenter Server 系统。
- 2 右键单击虚拟机，选择**电源**，然后选择**打开电源**启动虚拟机。
- 3 右键单击虚拟机，选择**客户机**，然后选择**安装/升级 VMware Tools**，以安装最新版本的 VMware Tools。

注 虚拟打印功能只有在通过 Horizon Agent 进行安装的情况下才受支持。如果使用 VMware Tools 进行安装，则不支持虚拟打印。

- 4 使用 VMware Tools 时间同步功能确保虚拟机与 ESXi 同步。

ESXi 必须与外部 NTP 源（例如与 Active Directory 相同的源）同步。

禁用其他时间同步机制，如 Windows 时间服务等。

VMware Tools 联机帮助提供了配置客户机和主机时间同步的信息。

- 5 安装服务包和更新。
- 6 安装防病毒软件。
- 7 安装其他应用程序和软件，如智能卡驱动程序（如果使用智能卡身份验证功能）。

如果计划使用 VMware Identity Manager 提供包含 ThinApp 应用程序的目录，您必须安装适用于 Windows 的 VMware Identity Manager。

重要事项 如果要安装 Microsoft .NET Framework，您必须在安装 Horizon Agent 后再安装此服务。

- 8 如果 Horizon Client 设备将通过 PCoIP 显示协议连接到虚拟机，请将电源选项**关闭显示器**设置为**从不**。

如果您不禁用此设置，当节能模式启动时，显示器会冻结在其最后的状态。

- 9 如果 Horizon Client 设备将通过 PCoIP 显示协议连接到虚拟机，请转至**控制面板 > 系统 > 高级系统设置 > 性能设置**，将**视觉效果**设置更改为**调整为最佳性能**。

如果您改用**调整为最佳外观**设置，或者选择让 **Windows 选择计算机的最佳设置**而 Windows 选择外观而非性能，则性能将受到负面影响。

- 10 如果您的网络环境中使用了代理服务器，请配置网络代理设置。
- 11 配置网络连接属性。
 - a 分配一个静态 IP 地址或指定一个由 DHCP 服务器分配的 IP 地址。
View 不支持 View 桌面的链接克隆 (169.254.x.x) 地址。
 - b 将首选及备用 DNS 服务器地址设置为您的 Active Directory 服务器地址。
- 12 （可选）将虚拟机加入远程桌面的 Active Directory 域。
用于创建即时克隆或 View Composer 链接克隆的父虚拟机必须属于桌面计算机将加入的同一 Active Directory 域，或是工作组的成员。
- 13 将 Windows 防火墙配置为允许远程桌面连接到虚拟机。
- 14 （可选）禁用热插拔 PCI 设备。
此步骤可以防止用户意外断开虚拟网络设备 (vNIC) 与虚拟机的连接。
- 15 （可选）配置用户自定义脚本。

准备 Windows Server 操作系统供桌面使用

要将 Windows Server 2008 R2 或 Windows Server 2012 R2 虚拟机用作单一会话 View 桌面（而不是用作 RDS 主机），必须在虚拟机中安装 Horizon Agent 之前执行某些步骤。还必须配置 View Administrator 以将 Windows Server 视为供 View 桌面使用的受支持操作系统。

前提条件

- 熟悉在 Windows Server 2008 R2 或 Windows Server 2012 R2 上安装桌面体验功能的步骤。请参阅[在 Windows Server 2008 R2 上安装桌面体验](#)或在[Windows Server 2012 或 2012 R2 上安装桌面体验](#)
- 在 Windows Server 2012 R2 计算机上，熟悉将 Windows 防火墙服务配置为在出现故障后重新启动的步骤。请参阅[将 Windows 防火墙服务配置为在出现故障后重新启动](#)。

步骤

- 1 验证是否已安装远程桌面服务角色。
当不存在远程桌面服务角色时，Horizon Agent 安装程序会提示您确认是否要在桌面模式中安装 Horizon Agent。如果存在远程桌面服务角色，Horizon Agent 安装程序不会显示此提示，而是会将 Windows Server 计算机视为 RDS 主机而非单一会话 View 桌面。
- 2 安装 Windows Server 2008 R2 Service Pack 1 (SP1) 或 Windows Server 2012 R2。
如果不随 Windows Server 2008 R2 一起安装 SP1，则安装 Horizon Agent 时会发生错误。
- 3 （可选）如果想要使用以下功能，请安装桌面体验功能。
 - HTML Access
 - 扫描仪重定向
 - Windows Aero

- 4 （可选）要在 Windows Server 桌面上使用 Windows Aero，请启动 Themes 服务。

创建或编辑桌面池时，您可以为您的桌面配置 3D 图形呈现。“3D 呈现器”设置提供了软件选项，使用户可以在池中的桌面上运行 Windows Aero。

- 5 在 Windows Server 2012 R2 计算机上，将 Windows 防火墙服务配置为在出现故障后重新启动。
- 6 配置 View Administrator 以将 Windows Server 视为受支持的桌面操作系统。

如果未执行该步骤，则无法选择 Windows Server 计算机供 View Administrator 之中的桌面使用。

- a 在 View Administrator 中，选择 **View 配置 > 全局设置**。
- b 在“常规”窗格中，单击**编辑**。
- c 选中**启用 Windows Server 桌面**复选框，并单击**确定**。

在 View Administrator 中启用 Windows Server 桌面时，View Administrator 会显示所有可用 Windows Server 计算机（包括安装 View 连接服务器的计算机）作为供桌面使用的潜在计算机。无法在安装其他 View 软件组件的计算机上安装 Horizon Agent。

在 Windows Server 2008 R2 上安装桌面体验

对于 RDS 桌面和应用程序以及在运行 Windows Server 的单用户虚拟机上部署的 VDI 桌面，扫描仪重定向需要您在 RDS 主机和单用户虚拟机中安装桌面体验功能。

步骤

- 1 以管理员身份登录。
- 2 启动服务器管理器。
- 3 单击**功能**。
- 4 单击**添加功能**。
- 5 在“选择功能”页面上，选中**桌面体验**复选框。
- 6 查看有关桌面体验功能所需的其他功能的信息，然后单击**添加必需的功能**。
- 7 按照提示完成安装。

在 Windows Server 2012 或 2012 R2 上安装桌面体验

对于 RDS 桌面和应用程序以及在运行 Windows Server 的单用户虚拟机上部署的 VDI 桌面，扫描仪重定向需要您在 RDS 主机和单用户虚拟机中安装桌面体验功能。

在用作 RDS 主机的计算机上支持 Windows Server 2012 和 Windows Server 2012 R2。在单用户虚拟机上支持 Windows Server 2012 R2。

步骤

- 1 以管理员身份登录。
- 2 启动服务器管理器。
- 3 选择**添加角色和功能**。

- 4 在“选择安装类型”页面上，选择**基于角色或基于功能的安装**。
- 5 在“选择目标服务器”页面上，选择一个服务器。
- 6 在“选择服务器角色”页面上，接受默认选择并单击**下一步**。
- 7 在“选择功能”页面上的**用户界面和基础架构**下，选择**桌面体验**。
- 8 按照提示完成安装。

将 Windows 防火墙服务配置为在出现故障后重新启动

在进行置备后，部署为单一会话桌面的某些 Windows Server 2012 R2、Windows 8.1 和 Windows 10 计算机不会立即变得可用。如果 Windows 防火墙服务在其超时期限到期后未重新启动，则会出现此问题。您可以在父虚拟机或模板虚拟机上配置 Windows 防火墙服务，以确保桌面池中的所有计算机都变得可用。

如果您在置备期间遇到此问题，Windows 事件日志将会显示以下错误：Windows 防火墙服务由于以下服务特定错误终止：由于超时期限到期，此操作返回 (The Windows Firewall service terminated with the following service-specific error: This operation returned because the timeout period expired)。

在 Windows Server 2012 R2、Windows 8.1 和 Windows 10 计算机上，将会出现该问题。其他客户机操作系统将不受影响。

步骤

- 1 在从中部署桌面池的 Windows Server 2012 R2、Windows 8.1 或 Windows 10 父虚拟机或模板虚拟机上，选择**控制面板 > 管理工具 > 服务**。
- 2 在**服务**对话框中，右键单击 **Windows 防火墙** 服务并选择**属性**。
- 3 在 **Windows 防火墙属性** 对话框中，单击**恢复**选项卡。
- 4 选择恢复设置以在出现故障后重新启动此服务。

设置	下拉菜单选项
第一次故障:	重新启动服务
第二次故障:	重新启动服务
后续故障:	重新启动服务

- 5 选中**启用发生错误时停止的操作**复选框，然后单击**确定**。
- 6 从父虚拟机或模板虚拟机中部署或重新部署桌面池。

在虚拟机上安装 Horizon Agent

您必须在由 vCenter Server 管理的虚拟机上安装 Horizon Agent，连接服务器才能与这些虚拟机通信。可在您用作完整克隆桌面池的模板、链接克隆桌面池的父项、即时克隆桌面池的父项以及手动桌面池中的计算机的所有虚拟机上安装 Horizon Agent。

要在多个 Windows 虚拟机上安装 Horizon Agent，而无需响应向导提示，您可以静默安装 Horizon Agent。请参阅[静默安装 Horizon Agent](#)。

Horizon Agent 软件无法与其他 Horizon 软件组件共存于同一个虚拟机或物理机上，这些组件包括安全服务器、连接服务器和 View Composer。该软件可以与 Horizon Client 共存。

前提条件

- 准备客户机操作系统以进行远程桌面部署。请参阅[为远程桌面部署准备客户机操作系统](#)。
- 要使用 Windows Server 虚拟机作为远程桌面（而不是作为 RDS 主机），请执行[准备 Windows Server 操作系统供桌面使用](#)中所述的步骤。
- 如果计算机安装了 Microsoft Visual C++ Redistributable 软件包，请确认软件包的版本为 2005 SP1 或更高版本。如果软件包的版本为 2005 或更低版本，可以升级或卸载该软件包。
- 从 VMware 产品页面 <http://www.vmware.com/go/downloadview> 下载 Horizon Agent 安装程序文件。
- 确认您对虚拟机具有管理权限。
- 熟悉 Horizon Agent 自定义安装选项。请参阅[Horizon Agent 自定义安装选项](#)。
- 熟悉 Horizon Agent 安装程序在防火墙上打开的 TCP 端口。有关更多信息，请参阅《View 架构规划指南》文档。

步骤

- 1 要启动 Horizon Agent 安装程序，请双击安装程序文件。

安装程序的文件名为 VMware-viewagent-y.y.y-xxxxxx.exe 或 VMware-viewagent-x86_64-y.y.y-xxxxxx.exe，其中 y.y.y 是版本号，xxxxxx 是内部版本号。

- 2 接受 VMware 许可条款。
- 3 如果在未安装远程桌面服务 (Remote Desktop Services, RDS) 角色的 Windows Server 计算机上安装 Horizon Agent，则选择在“桌面模式”下安装 **VMware Horizon Agent**。

选择此选项可配置 Windows Server 计算机作为单用户 View 桌面而非作为 RDS 主机。如果您想要将该计算机作为 RDS 主机运行，则取消 Horizon Agent 安装，在该计算机上安装 RDS 角色，然后重新启动 Horizon Agent 安装。

- 4 选择 Internet 协议 (IP) 版本 (IPv4 或 IPv6)。

必须使用同一 IP 版本安装所有 View 组件。

- 5 选择启用还是禁用 FIPS 模式。

仅当在 Windows 中启用 FIPS 模式时，此选项才可用。

- 6 选择自定义安装选项。

要部署 View Composer 链接克隆桌面，请选择 **VMware Horizon View Composer Agent** 选项。要部署即时克隆桌面，请选择 **VMware Horizon Instant Clone Agent** 选项。您不能同时选择这两个选项。

- 7 接受或更改目标文件夹。

8 按照 Horizon Agent 安装程序中的提示完成安装。

注 如果您在准备客户机操作系统的过程中没有启用远程桌面支持，Horizon Agent 安装程序会提示您启用此功能。如果您在 Horizon Agent 安装过程中没有启用远程桌面支持，安装完成后您必须手动启用此功能。

9 如果您选择了“USB 重定向”选项，需要重新启动虚拟机以启用 USB 支持。

此外，发现新硬件向导也可能启动。在重新启动虚拟机之前，请先按照向导中的提示配置硬件。

后续步骤

如果虚拟机具有多个网卡，则需要配置 Horizon Agent 使用的子网。请参阅[为 Horizon Agent 配置具有多个网卡的虚拟机](#)。

Horizon Agent 自定义安装选项

在虚拟机上安装 Horizon Agent 时，您可以选择或取消选择自定义安装选项。此外，Horizon Agent 还会在支持某些功能的所有客户机操作系统上自动安装这些功能。这些功能并非可选。

要了解哪些客户机操作系统上支持哪些功能，请参阅《View 架构规划指南》文档中的“Horizon Agent 功能支持表”。

要在安装最新的 Horizon Agent 版本后更改自定义安装选项，您必须卸载并重新安装 Horizon Agent。对于修补程序和升级，您可以运行新的 Horizon Agent 安装程序并选择一组新的选项，而无需卸载以前的版本。

默认情况下，除串行端口重定向、扫描仪重定向、USB 重定向、Flash 重定向、智能卡重定向和 VMware Horizon Instant Clone Agent 之外的其他所有自定义安装选项都会被选中。

表 3-2. IPv4 环境中的 Horizon Agent 自定义安装选项

选项	说明
核心	安装核心功能。
串行端口重定向	重定向连接到客户端系统的串行 COM 端口，以便在远程桌面上使用这些端口。 默认情况下，不会选择此选项。必须选择此选项才会进行安装。 在单用户计算机上部署的远程桌面上支持串行端口重定向。 Horizon 6 版本 6.1.1 及更高版本中提供了串行端口重定向功能。
扫描仪重定向	重定向连接至客户端系统的扫描和图像处理设备，以便在远程桌面或应用程序上使用。 默认情况下，不会选择此选项。必须选择此选项才会进行安装。 Horizon 6.0.2 及更高版本中提供了扫描仪重定向功能。
USB 重定向	允许用户访问其桌面上本地连接的 USB 设备。 在单用户计算机上部署的远程桌面上支持 USB 重定向。此外，RDS 桌面和应用程序上支持 USB 闪存驱动器和硬盘的重定向。 默认情况下，不会选择此选项。必须选择此选项才会进行安装。 有关安全地使用 USB 重定向的指导，请参见《View 安全指南》指南。例如，可以使用组策略设置针对特定用户禁用 USB 重定向。
VMware Horizon View Composer Agent	让此虚拟机作为 View Composer 链接克隆桌面池的父虚拟机。如果选择此选项，您将无法选择 VMware Horizon Instant Clone Agent 选项。

选项	说明
VMware Horizon Instant Clone Agent	让此虚拟机作为即时克隆桌面池的父虚拟机。默认情况下，不会选择此选项。如果选择此选项，您将无法选择 VMware Horizon View Composer Agent 选项。
实时音频-视频	重定向到客户端系统连接的网络摄像头和音频设备，以便用于远程桌面。
客户端驱动器重定向	<p>允许 Horizon Client 用户与其远程桌面共享本地驱动器。</p> <p>安装此选项之后，无需在远程桌面上执行进一步的配置。</p> <p>在 RDS 桌面和应用程序上以及在未受管计算机上运行的 VDI 桌面上也支持客户端驱动器重定向。</p>
虚拟打印	<p>允许用户通过其客户端计算机上可用的任意打印机进行打印。用户不需要在其桌面上另外安装驱动程序。</p> <p>以下远程桌面和应用程序支持虚拟打印：</p> <ul style="list-style-type: none"> ■ 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 主机上部署的桌面，其中 RDS 主机为虚拟机。 ■ 远程应用程序。 ■ 从远程桌面内的 Horizon Client 启动的远程应用程序（嵌套会话）。 <p>虚拟打印功能只有在通过 Horizon Agent 进行安装的情况下才受支持。使用 VMware Tools 进行安装则不受支持。</p>
vRealize Operations Desktop Agent	提供允许适用于 View 的 vRealize Operations 监控 View 桌面的信息。
View Persona Management	将本地桌面上的用户配置文件与远程配置文件存储库同步，确保用户无论在何时登录桌面，均可访问配置文件。
智能卡重定向	<p>允许用户在使用 PCoIP 或 Blast Extreme 显示协议时使用智能卡进行身份验证。默认情况下，不会选择此选项。</p> <p>在单用户计算机中部署的远程桌面上支持智能卡重定向。</p>
VMware 音频	在远程桌面上提供虚拟音频驱动程序。
Flash 重定向	将 Internet Explorer 9、10 或 11 浏览器中的 Flash 多媒体内容重定向到客户端，以优化性能。在 Horizon 7.0 中，这是一项技术预览功能。在 Horizon 7.0.1 中，此功能受到完全支持。

在 IPv6 环境中，可选功能仅包括 **VMware Horizon View Composer Agent**、**VMware Horizon Instant Clone Agent** 和 **VMware 音频**。

表 3-3. 自动安装的 Horizon Agent 功能（不可选）

功能	说明
PCoIP 代理	<p>允许用户使用 PCoIP 显示协议连接到 View 桌面。</p> <p>如果安装 PCoIP 代理功能，将禁用 Windows 桌面的睡眠模式。当用户导航至“电源选项”或“关机”菜单时，睡眠模式或待机模式是无效的。经过一段默认的非活动时间后，桌面不会进入睡眠或待机模式。桌面将一直处于活动模式。</p>
Windows Media 多媒体重定向 (MMR)	<p>将多媒体重定向扩展到 Windows 7 及更高版本的桌面和客户端。</p> <p>通过此功能将多媒体流直接传输到客户端计算机，从而在客户端硬件而非远程 ESXi 主机上处理多媒体流。</p>

功能	说明
Unity Touch	允许平板电脑和智能手机用户与运行于远程桌面上的 Windows 应用程序轻松进行交互。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。
虚拟视频驱动程序	在远程桌面上提供虚拟视频驱动程序。

在 IPv6 环境中，唯一自动安装的功能是 PCoIP 代理。

静默安装 Horizon Agent

您可以使用 Microsoft Windows Installer (MSI) 的静默安装功能，在若干 Windows 虚拟机或物理机上安装 Horizon Agent。在静默安装中，您需要使用命令行，无需响应向导的提示。

通过静默安装，您可以在大型企业中高效部署 View 组件。

如果您不希望安装自动或默认安装的所有功能，则可以使用 ADDLOCAL MSI 属性有选择地安装各个安装选项和功能。有关 ADDLOCAL 属性的详细信息，请参阅 [表 3-5. MSI 命令行选项和 MSI 属性](#)。

前提条件

- 为桌面部署准备客户机操作系统。请参阅[为远程桌面部署准备客户机操作系统](#)。
- 要使用 Windows Server 作为单一会话远程桌面（而不是作为 RDS 主机），请执行[准备 Windows Server 操作系统供桌面使用](#)中所述的步骤。
- 如果计算机安装了 Microsoft Visual C++ Redistributable 软件包，请确认软件包的版本为 2005 SP1 或更高版本。如果软件包的版本为 2005 或更低版本，可以升级或卸载该软件包。
- 从 VMware 产品页面 <http://www.vmware.com/go/downloadview> 下载 Horizon Agent 安装程序文件。
安装程序的文件名为 VMware-viewagent-y.y.y-xxxxxx.exe 或 VMware-viewagent-x86_64-y.y.y-xxxxxx.exe，其中 y.y.y 是版本号，xxxxxx 是内部版本号。
- 确认您具有虚拟机或物理机的管理权限。
- 熟悉 Horizon Agent 自定义安装选项。请参阅 [Horizon Agent 自定义安装选项](#)。
- 熟悉 MSI 安装程序命令行选项。请参阅 [Microsoft Windows Installer 命令行选项](#)。
- 熟悉 Horizon Agent 可用的静默安装属性。请参阅 [Horizon Agent 的静默安装属性](#)。
- 熟悉 Horizon Agent 安装程序在防火墙上打开的 TCP 端口。有关更多信息，请参阅《View 架构规划指南》文档。
- 确认在计划静默安装 Horizon Agent 的客户机操作系统上安装了最新的 Windows Update 修补程序。在某些情况下，可能需要管理员进行交互式安装，以执行等待处理的 Windows Update 修补程序。确认所有操作系统操作和后续重新引导均已完成。

步骤

- 1 在虚拟机或物理机上打开一个 Windows 命令提示符。

2 在一行中键入安装命令。

以下示例将安装 Horizon Agent 以及 Core、VMware Blast、PCoIP、Unity Touch、VmVideo、PSG、View Composer Agent、虚拟打印、USB 重定向和实时音频-视频组件。

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1  
ADDLOCAL=Core,SVIAgent,ThinPrint,USB,RTAV"
```

以下示例将在未受管的计算机上安装 Horizon Agent，并通过指定的 View 连接服务器 cs1.companydomain.com 来注册桌面。此外，安装程序还会安装 Core、VMware Blast、PCoIP、Unity Touch、VmVideo、PSG、虚拟打印和 USB 重定向组件。

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=0  
VDM_SERVER_NAME=cs1.companydomain.com VDM_SERVER_USERNAME=admin.companydomain.com  
VDM_SERVER_PASSWORD=secret ADDLOCAL=Core,ThinPrint,USB"
```

如果在 Windows Server 计算机上安装 Horizon Agent，并想要配置该计算机作为单用户 View 桌面而非作为 RDS 主机，则必须在安装命令中包含 VDM_FORCE_DESKTOP_AGENT=1 属性。此要求适用于受 vCenter Server 管理的计算机和未受管的计算机。

后续步骤

如果虚拟机具有多个网卡，则需要配置 Horizon Agent 使用的子网。请参阅[为 Horizon Agent 配置具有多个网卡的虚拟机](#)。

Microsoft Windows Installer 命令行选项

要以静默方式安装 View 组件，您必须使用 Microsoft Windows Installer (MSI) 命令行选项和属性。View 组件安装程序是 MSI 程序，使用标准的 MSI 功能。

有关 MSI 的详细信息，请参阅 Microsoft 网站。关于 MSI 命令行选项，请访问 Microsoft Developer Network (MSDN) 资源库网站，搜索 MSI 命令行选项。要了解 MSI 命令行的用法，可以在安装了 View 组件的计算机中打开一个命令提示符，并键入 `msiexec /?`。

要以静默方式运行 View 组件安装程序，应当首先静默引导程序，因为该程序会将安装程序提取到一个临时目录中并启动交互式安装。

在命令行中，您必须输入控制安装程序的引导程序的命令行选项。

表 3-4. View 组件引导程序的命令行选项

选项	说明
/s	禁用引导程序初始屏幕和提取对话框，可阻止显示交互式对话框。 例如：VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s 运行静默安装需要 /s 选项。
/v" MSI 命令行选项"	指示安装程序将您在命令行中输入的双引号括住的字符串作为一组选项进行传递，供 MSI 解析。您必须用双引号括住命令行条目。在 /v 之后和命令行末尾之间添加双引号。 例如：VMware-viewagent-y.y.y-xxxxxx.exe /s /v"command_line_options" 要指示 MSI 安装程序解释一个包含空格的字符串，应当将该字符串括在两组双引号中。例如，您可能需要将 View 组件安装在名称中包含空格的安装路径下。 例如：VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder"" 在此示例中，MSI 安装程序会传递安装目录的路径，而不会试图将该字符串解释为两个命令行选项。请注意，最后一个双引号的作用是将整个命令行括住。 运行静默安装需要 /v"命令行选项" 选项。

您通过将命令行选项和 MSI 属性值传递到 MSI 安装程序 `msiexec.exe` 来控制静默安装的剩余部分。MSI 安装程序中包含 View 组件的安装代码。安装程序使用您在命令行中输入的值和选项来解释特定于 View 组件的安装选择和设置选项。

表 3-5. MSI 命令行选项和 MSI 属性

MSI 选项或属性	说明
/qn	指示 MSI 安装程序不显示安装程序向导页面。 例如，您可能希望只采用默认的安装选项和功能，以静默方式安装 Horizon Agent： VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn" 或者，您可以使用 /qb 选项在非交互式自动安装过程中显示向导页面。在安装过程中，向导页面将会出现，但是您无法响应。 运行静默安装需要 /qn 或 /qb 选项。
INSTALLDIR	指定 View 组件的可选安装路径。 采用 <code>安装目录=路径</code> 格式来指定安装路径。如果您要将 View 组件安装在默认路径下，则可以忽略此 MSI 属性。 此 MSI 属性是可选的。

MSI 选项或属性	说明
ADDLOCAL	<p>确定要安装的特定于组件的选项。</p> <p>在交互式安装中，View 安装程序会显示您可以选择或取消选择的自定义安装选项。在静默安装中，通过在命令行上指定选项，您可以使用 ADDLOCAL 属性选择性地安装各个安装选项。您没有明确指定的选项则不安装。</p> <p>在交互式安装和静默安装中，View 安装程序都将自动安装特定功能。无法使用 ADDLOCAL 控制是否安装这些非可选功能。</p> <p>键入 ADDLOCAL=ALL 以安装在交互式安装期间可安装的所有自定义安装选项，包括默认安装的选项以及必须选择安装的选项，但 NGVC 除外。NGVC 和 SVIAgent 是相互排斥的。要安装 NGVC，您必须明确指定该选项。</p> <p>以下示例将安装 Core、BlastProtocol、PCoIP、UnityTouch、VmVideo、PSG 以及在客户机操作系统上受支持的所有功能：VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</p> <p>如果您没有使用 ADDLOCAL 属性，将安装默认安装的自定义安装选项以及自动安装的功能。不会安装默认关闭（未选中）的自定义安装选项。</p> <p>以下示例将安装 Core、BlastProtocol、PCoIP、UnityTouch、VmVideo、PSG 以及在客户机操作系统上受支持且默认开启的自定义安装选项：VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"</p> <p>要单独指定各个安装选项，可键入以逗号分隔的安装选项名称列表。名称之间不要使用空格。采用以下格式：ADDLOCAL=值,值,值...。</p> <p>使用 ADDLOCAL=value,value,value... 属性时，您必须包含 Core。</p> <p>以下示例将安装 Horizon Agent 以及 Core、BlastProtocol、PCoIP、UnityTouch、VmVideo、PSG、Instant Clone Agent 和虚拟打印功能： VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,NGVC,ThinPrint"</p> <p>前一示例未安装其他组件，甚至未安装以交互方式默认安装的组件。</p> <p>ADDLOCAL MSI 属性为可选项。</p>
REBOOT	<p>您可以使用 REBOOT=ReallySuppress 选项，以允许在系统重新引导前完成系统配置任务。</p> <p>此 MSI 属性是可选的。</p>
/l*v log_file	<p>使用详细输出模式将日志记录信息写入指定的日志文件。</p> <p>例如：/l*v ""%TEMP%\vmmsi.log""</p> <p>本示例生成了详细的日志文件，与交互式安装过程中生成的日志类似。</p> <p>您可以使用该选项记录您安装的专有的自定义功能。您可以使用记录的信息指定在以后的静默安装中需要安装的功能。</p> <p>/l*v 选项是可选的。</p>

Horizon Agent 的静默安装属性

从命令行静默安装 **Horizon Agent** 时，可以包含特定属性。您必须使用 **PROPERTY=value** 的格式，以便 Microsoft Windows Installer (MSI) 理解各属性和值。

表 3-6. 静默安装 **Horizon Agent** 的 MSI 属性显示了您可以在命令行中使用的 **Horizon Agent** 静默安装属性。

表 3-6. 静默安装 Horizon Agent 的 MSI 属性

MSI 属性	说明	默认值
INSTALLDIR	<p>Horizon Agent 软件的安装路径和文件夹。</p> <p>例如: <code>INSTALLDIR=""D:\abc\my folder""</code></p> <p>括住路径的两组双引号可允许 MSI 安装程序忽略路径中的空格。</p> <p>此 MSI 属性是可选的。</p>	%ProgramFiles%\VMware\VMware View Agent
RDP_CHOICE	<p>确定是否在桌面上启用远程桌面协议 (RDP)。</p> <p>值为 1 时启用 RDP。值为 0 时禁用 RDP 设置。</p> <p>此 MSI 属性是可选的。</p>	1
UNITY_DEFAULT_APPS	<p>指定在移动设备的 Unity Touch 边栏中显示的默认收藏应用程序的默认列表。此属性的创建旨在为 Unity Touch 组件提供支持。它不是常规 MSI 属性。</p> <p>有关配置收藏应用程序的默认列表以及此属性所用语法和格式的信息, 请参阅配置 Unity Touch 显示的收藏的应用程序。</p> <p>此 MSI 属性是可选的。</p>	
URL_FILTERING_ENABLED	<p>指定是否安装了 URL 内容重定向功能。值为 1 时安装该功能。然后, 您必须使用组策略设置配置要重定向的 URL。请参阅配置 URL 内容重定向。</p> <p>此 MSI 属性是可选的。</p>	0
VDM_VC_MANAGED_AGENT	<p>确定 vCenter Server 是否管理安装了 Horizon Agent 的虚拟机。</p> <p>值为 1 时将桌面配置为受 vCenter Server 管理的虚拟机。</p> <p>值为 0 时将桌面配置为不受 vCenter Server 管理。</p> <p>此 MSI 属性是必要属性。</p>	无
VDM_SERVER_NAME	<p>Horizon Agent 安装程序在其中注册未受管桌面的 View 连接服务器计算机的主机名或 IP 地址。此属性适用于未受管的桌面。</p> <p>例如: <code>VDM_SERVER_NAME=10.123.01.01</code></p> <p>此 MSI 属性是未受管桌面的必要属性。</p> <p>不要将此 MSI 属性用于受 vCenter Server 管理的虚拟机桌面。</p>	无
VDM_SERVER_USERNAME	<p>View 连接服务器计算机上的管理员用户名。此 MSI 属性适用于未受管的桌面。</p> <p>例如: <code>VDM_SERVER_USERNAME=domain\username</code></p> <p>此 MSI 属性是未受管桌面的必要属性。</p> <p>不要将此 MSI 属性用于受 vCenter Server 管理的虚拟机桌面。</p>	无
VDM_SERVER_PASSWORD	<p>View 连接服务器管理员用户密码。</p> <p>例如: <code>VDM_SERVER_PASSWORD=secret</code></p> <p>此 MSI 属性是未受管桌面的必要属性。</p> <p>不要将此 MSI 属性用于受 vCenter Server 管理的虚拟机桌面。</p>	无
VDM_IP_PROTOCOL_USAGE	<p>指定 Horizon Agent 使用的 IP 版本。可能的值为 IPv4 和 IPv6。</p>	IPv4

MSI 属性	说明	默认值
VDM_FIPS_ENABLED	指定启用还是禁用 FIPS 模式。值为 1 将启用 FIPS 模式。值为 0 将禁用 FIPS 模式。如果此属性设置为 1 并且 Windows 未处于 FIPS 模式中，则安装程序将中止。	0
VDM_FLASH_URL_REDIRECTION	确定 Horizon Agent 是否可以安装 Flash URL 重定向功能。指定 1 允许安装，指定 0 禁止安装。 此 MSI 属性是可选的。	0

在静默安装命令中，您可以使用 MSI 属性 ADDLOCAL= 指定 Horizon Agent 安装程序配置的选项。

表 3-7. Horizon Agent 静默安装选项和交互式自定义安装选项 显示了您可以在命令行中键入的 Horizon Agent 选项。这些选项具有对应的安装选项，可以在交互式安装过程中取消选择或选择这些对应的安装选项。有关自定义安装选项的详细信息，请参阅 [Horizon Agent 自定义安装选项](#)。

当您没有在命令行中使用 ADDLOCAL 属性时，Horizon Agent 将安装在交互式安装过程中默认安装的所有选项（如果客户机操作系统上支持这些选项）。当您使用 ADDLOCAL=ALL 时，Horizon Agent 将安装除 NGVC 之外的以下所有选项，包括默认开启和默认关闭的选项（如果客户机操作系统上支持这些选项）。NGVC 和 SVIAgent 是相互排斥的。要安装 NGVC，您必须明确指定该选项。有关详细信息，请参阅 [Microsoft Windows Installer 命令行选项](#) 中的 ADDLOCAL 表单条目。

表 3-7. Horizon Agent 静默安装选项和交互式自定义安装选项

静默安装选项	交互式安装中的自定义安装选项	以交互方式默认安装或在未使用 ADDLOCAL 时默认安装
Core	Core	是
USB	USB 重定向	否
SVIAgent	View Composer Agent	是
NGVC	Instant Clone Agent	否
RTAV	实时音频-视频	是
ClientDriveRedirection	客户端驱动器重定向	是
SerialPortRedirection	串行端口重定向	否
ScannerRedirection	扫描仪重定向	否
FlashURLRedirection	Flash URL 重定向 除非您在命令行中使用 VDM_FLASH_URL_REDIRECTION=1 属性，否则会隐藏 此功能。	否
ThinPrint	虚拟打印	是
V4V	vRealize Operations Desktop Agent	是
VPA	View Persona Management	是
SmartCard	PCoIP 智能卡。默认情况下，在交互式安装中不 安装此功能。	否
VmwareAudio	VMware 音频（虚拟音频驱动程序）	是

静默安装选项	交互式安装中的自定义安装选项	以交互方式默认安装或在未使用 ADDLOCAL 时默认安装
TSMRR	Windows Media 多媒体重定向 (MMR)	是
RDP	在 View Administrator 中创建或编辑桌面池时，如果在命令行中使用 RDP_CHOICE=1 属性或将 RDP 选择为默认显示协议，则此功能将在注册表中启用 RDP。 此功能在交互式安装过程中处于隐藏状态。	是

如果您使用 ADDLOCAL 单独指定功能，即，不指定 ADDLOCAL=ALL，则必须始终指定 Core。

表 3-8. 自动安装的 Horizon Agent 静默安装功能

静默安装功能	说明
Core	Horizon Agent 核心功能。 如果您指定 ADDLOCAL=ALL，将安装核心功能。
BlastProtocol	VMware Blast
PCoIP	PCoIP 协议代理
VmVideo	虚拟视频驱动程序
UnityTouch	Unity Touch
PSG	此功能可以设置一个注册表项，使连接服务器知道 Horizon Agent 使用的是 IPv4 还是 IPv6。

可通过在静默安装中使用 VDM_FLASH_URL_REDIRECT=1 属性来安装 Flash URL 重定向功能。在交互式安装过程中或在静默安装中使用 ADDLOCAL=ALL 时未安装此功能。

例如: VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1
VDM_FLASH_URL_REDIRECT=1
ADDLOCAL=Core,SVIAgent,ThinPrint,USB,FlashURLRedirection,RTAV"

为 Horizon Agent 配置具有多个网卡的虚拟机

在具有多个网卡的虚拟机上安装 Horizon Agent 时，必须配置 Horizon Agent 使用的子网。子网确定 Horizon Agent 提供给连接服务器实例以进行客户端协议连接的网络地址。

步骤

- ◆ 在安装了 Horizon Agent 的虚拟机上，打开一个命令提示符，键入 **regedit.exe**，然后创建一个注册表项以配置子网。

例如，在 IPv4 网络中：

HKLM\Software\VMware, Inc.\VMware VDM\IpPrefix = n.n.n.n/m (REG_SZ)

在此示例中， $n.n.n.n$ 为 TCP/IP 子网， m 为子网掩码中的位数。

注 在 Horizon 6 版本 6.1 之前的版本中，此注册表路径为

HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = $n.n.n.n/m$ (REG_SZ)。

旧注册表设置不用于 View Agent 6.1 或更高版本。如果将 View Agent 从更早版本升级到 6.1 或更高版本，请确保使用当前的注册表设置。

优化客户机操作系统性能

您可以执行某些特定步骤来为远程桌面部署优化客户机操作系统性能。所有步骤都是可选操作。

这些建议包括关闭屏幕保护程序，以及不指定睡眠计时器。您的组织可能需要使用屏幕保护程序。例如，您可能拥有一个由 GPO 管理的安全策略，该策略将在屏幕保护程序运行一定时间后锁定桌面。在这种情况下，请使用空白的屏幕保护程序。

前提条件

- 为远程桌面部署准备客户机操作系统。
- 熟悉禁用 Windows 客户体验改善计划的步骤。请参阅[禁用 Windows 客户体验改善计划](#)。

步骤

- ◆ 禁用任何未使用的端口，如 COM1、COM2 和 LPT。
- ◆ 调整显示属性。
 - a 选择一个基本主题。
 - b 将背景设置为某一单色。
 - c 将屏幕保护程序设置为无。
 - d 确认已启用硬件加速。
- ◆ 选择一个高性能电源选项，并且不指定睡眠计时器。
- ◆ 禁用索引服务组件。

注 索引功能通过将文件分类来改进搜索性能。对于经常使用搜索功能的用户，不应禁用此功能。

- ◆ 将系统还原点移除或降至最少。
- ◆ 关闭 C:\ 上的系统保护。
- ◆ 禁用任何不必要的服务。
- ◆ 将声音方案设置为无声。
- ◆ 将视觉效果设置为调整为最佳性能。
- ◆ 打开 Windows Media Player 并使用默认设置。
- ◆ 关闭计算机自动维护。
- ◆ 将性能设置调整为最佳性能。

- ◆ 删除 C:\Windows 中任何隐藏的卸载文件夹，如 \$NtUninstallKB893756\$。
- ◆ 删除所有事件日志。
- ◆ 运行磁盘清理程序以便移除临时文件、清空回收站并移除系统文件和其他不再需要的内容。
- ◆ 运行磁盘碎片整理程序以重新整理碎片数据。
- ◆ 卸载 Tablet PC 组件，除非需要此功能。
- ◆ 禁用 IPv6，除非需要此功能。
- ◆ 使用文件系统实用程序 (fsutil) 命令禁用持续跟踪文件最后访问时间的设置。

例如: `fsutil behavior set disablelastaccess 1`

- ◆ 启动注册表编辑器 (regedit.exe) 并将 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Disk** 下的 TimeoutValue REG_DWORD 更改为 **0x000000be(190)**。
- ◆ 关闭 Windows 客户体验改善计划，禁用任务计划程序中的相关任务。
- ◆ 完成上述更改后重新启动 Windows。

后续步骤

请参阅[为即时克隆和 View Composer 链接克隆虚拟机优化 Windows](#)，了解有关禁用某些 Windows 服务和任务，以减缓即时克隆和 View Composer 链接克隆的增长速度的信息。禁用某些特定服务和任务也可为完整虚拟机带来性能优势。

禁用 Windows 客户体验改善计划

通过禁用 Windows 客户体验改善计划和控制该计划的相关任务计划程序任务，可以改善大型桌面池中的 Windows 7、Windows 8/8.1 和 Windows 10 的系统性能。

以下步骤适用于 Windows 7 和 Windows 8。这些步骤可能会因 Windows 操作系统而异。

步骤

- 1 在 Windows 7 或 Windows 8 客户机操作系统中，启动控制面板，然后单击**操作中心 > 更改操作中心设置**。
- 2 单击**客户体验改进计划设置**。
- 3 选择**否，我不想加入该计划**并单击**保存更改**。
- 4 启动控制面板，单击**管理工具 > 任务计划程序**。
- 5 在“任务计划程序”对话框的“任务计划程序 (本地)”窗格中，展开**任务计划程序库 > Microsoft > Windows** 节点，然后打开**应用程序体验**文件夹。
- 6 禁用 **AITAgent**、**ProgramDataUpdater** 以及 **Microsoft Compatibility Appraiser**（如果适用）任务。
- 7 在**任务计划程序库 > Microsoft > Windows** 节点中，打开**客户体验改进计划**文件夹。
- 8 禁用 **Consolidator**、**KernelCEIPTask** 和 **UsbCEIP** 任务。

9 在任务计划程序库 > Microsoft > Windows 节点中，打开 **Autochk** 文件夹。

10 禁用 **Proxy** 任务。

后续步骤

执行其他 Windows 优化任务。请参阅[优化客户机操作系统性能](#)。

为即时克隆和 View Composer 链接克隆虚拟机优化 Windows

通过禁用 Windows 7、Windows 8/8.1 和 Windows 10 的某些服务和任务，您可以减缓即时克隆和 View Composer 链接克隆的磁盘使用增长速度。禁用某些特定服务和任务也可为完整虚拟机带来性能优势。

禁用 Windows 服务和任务所带来的优势

Windows 7、Windows 8/8.1 和 Windows 10 计划的服务和任务可能会导致即时克隆和 View Composer 链接克隆增长，即使在计算机空闲时也不例外。操作系统磁盘的逐渐增长会消耗您在最初创建克隆时节省的存储空间。您可以通过禁用这些 Windows 服务来减缓磁盘大小的增长速度。

Windows 客户机操作系统计划默认运行一些服务，如磁盘碎片整理。如果您不禁用这些服务，它们会在后台运行。

影响操作系统磁盘增长的服务也会产生输入/输出操作。禁用这些服务可以降低 IOPS（每秒输入/输出操作数量），并提高任何类型桌面计算机的性能。

这些优化 Windows 的最佳做法适用于大多数用户环境。然而，您必须评估禁用各项服务对您的用户、应用程序和桌面的影响。您可能需要保留特定服务。

例如，禁用 Windows Update 服务将对即时克隆很有用，因为每当用户注销时都会刷新操作系统；如果您定期刷新或重构 View Composer 链接克隆，禁用这项服务也会对这些克隆很有用。

引起即时克隆和链接克隆中磁盘增长的 Windows 服务和任务

Windows 7、Windows 8/8.1 和 Windows 10 中的某些服务和任务可能会引起即时克隆或 View Composer 链接克隆的操作系统磁盘逐渐增长，即使在计算机空闲时也不例外。如果禁用这些服务和任务，您可以控制操作系统磁盘的增长速度。

影响操作系统磁盘增长的服务也会产生 I/O 操作。您也可以评估为完整克隆禁用这些服务的好处。

在禁用[表 3-9. Windows 服务和任务对操作系统磁盘增长和 IOPS 的影响](#)中说明的 Windows 服务之前，验证是否执行了[优化客户机操作系统性能](#)中的优化步骤。

表 3-9. Windows 服务和任务对操作系统磁盘增长和 IOPS 的影响

服务或任务	说明	默认出现或启动时间	对操作系统磁盘的影响	对 IOPS 的影响	是否关闭此服务或任务?
Windows 休眠	在电脑关机前将打开的文件和程序存储在一个文件夹中，从而提供一种省电状态。电脑重启时，文件夹将会被重新载入内存，恢复到启动休眠时的状态。	默认电源计划设置会禁用休眠功能。	高。 默认情况下，休眠文件 hiberfil.sys 的大小同虚拟机上安装的 RAM 相同。此功能会影响所有客户机操作系统。	高。 触发休眠功能后，系统会生成一个与安装的 RAM 同样大小的 hiberfil.sys 文件。	是 休眠功能在虚拟环境中没有任何用途。有关详细说明，请参阅 在父虚拟机中禁用 Windows 休眠功能 。
Windows 计划的磁盘碎片整理	磁盘碎片整理为计划的后台进程。	一周一次	高。 重复的碎片整理操作会将操作系统磁盘增大若干 GB，但这不会提高对磁盘的访问效率。	高	是
Windows Update 服务	检测、下载及安装 Windows 和其他程序的更新。	自动启动	中到高。 因为经常执行更新检查，所以会频繁写入操作系统磁盘。具体影响取决于所下载的更新。	中到高	是（对于即时克隆和您定期刷新或重构的 View Composer 链接克隆）。
Windows 诊断策略服务	检测、故障排除以及解决 Windows 组件中的问题。如果您停止此服务，诊断功能将不再可用。	自动启动	中到高。 此服务按需触发。根据需要程度，写入频率会有所不同。	低到中	是（如果您不需要诊断工具在桌面运行）。
预取/超级获取	存储您运行的应用程序的特定信息，帮助应用程序更快启动。	只要不被禁用即始终开启。	中 导致其布局、数据库信息和单个预取文件（按需生成）的周期性更新。	中	是（如果您禁用此功能后应用程序启动时所用的时间在可接受的范围内）。
Windows 注册表备份 (RegIdleBackup)	系统空闲时自动备份 Windows 注册表。	每 10 天的中午 12:00 点	中。 此任务每次运行时都会生成注册表备份文件。	中。	是。即时克隆和 View Composer 链接克隆都允许您恢复到快照，并实现还原注册表的目标。
系统还原	将 Windows 系统恢复至先前的某个正常运行状态。	Windows 启动时进行，之后每天一次。	低到中。 当系统检测到有需要时，捕捉系统还原点。	无重大影响。	是。即时克隆和 View Composer 链接克隆都允许您恢复到正常运行状态。

服务或任务	说明	默认出现或启动时间	对操作系统磁盘的影响	对 IOPS 的影响	是否关闭此服务或任务?
Windows Defender	提供反间谍软件功能。	Windows 启动时。每天快速扫描一次。每次扫描前均检查更新。	中到高。 执行定义更新、计划扫描以及按需启动的扫描。	中到高。	是（如果安装了其他反间谍软件）。
Microsoft Feeds Synchronization 任务 (msfeedssync.exe)	定期更新 Windows Internet Explorer Web 浏览器中的 RSS 源。此任务可更新启用了自动 RSS 源同步功能的 RSS 源。只有当 Internet Explorer 运行时，此进程才会显示在 Windows 任务管理器中。	一天一次。	中。 如果未配置永久磁盘，将会影响操作系统磁盘的增长。 如果配置了永久磁盘，将会影响永久磁盘。	中	是（如果您的用户不要求在其桌面中自动更新 RSS 源）。

在 Windows 父虚拟机中禁用计划的磁盘碎片整理

为即时克隆或 View Composer 链接克隆准备父虚拟机时，建议禁用计划的碎片整理。默认情况下，Windows 会计划每周执行一次磁盘碎片整理。碎片整理可显著增加克隆的虚拟磁盘的大小，但这不会提高即时克隆或 View Composer 链接克隆对磁盘的访问效率。

虽然这些克隆共享父虚拟机的操作系统磁盘，但每个克隆都会在其自己的虚拟磁盘中保留对文件系统的更改。包括碎片整理在内的任何活动都将增加每个克隆各自虚拟磁盘的大小，从而增加所占用的存储空间。最佳做法是，在拍摄快照及创建池之前先对父虚拟机进行碎片整理。

以下步骤适用于 Windows 7 和 Windows 8。这些步骤可能会因 Windows 操作系统而异。

步骤

- 1 在 vSphere Client 中，选择父虚拟机，然后选择**打开控制台**。
- 2 以管理员身份登录。
- 3 单击**开始**并在**查找程序和文件框**中键入 **defrag**。
- 4 在“程序”窗格中，单击**磁盘碎片整理程序**。
- 5 在**磁盘碎片整理程序**对话框中，单击**整理磁盘碎片**。
磁盘碎片整理程序会在虚拟机硬盘上整合整理过的文件。
- 6 在**磁盘碎片整理程序**对话框中，单击**配置计划**。
- 7 取消选择**按计划运行（推荐）**，然后单击**确定**。

禁用 Windows Update

禁用 Windows Update 功能可避免对文件系统执行某些 I/O 操作，从而可以减缓即时克隆或 View Composer 链接克隆虚拟磁盘的增长速度。

在禁用 Windows Update 之前，请先评估您环境的需求。如果您禁用此功能，可以手动将更新下载到父虚拟机，然后对即时克隆使用推送映像操作，或者对 View Composer 链接克隆进行重构，以便将更新应用到所有克隆。

以下步骤适用于 Windows 7 和 Windows 8。这些步骤可能会因 Windows 操作系统而异。

步骤

- 1 在 vSphere Client 中，选择父虚拟机，然后选择**打开控制台**。
- 2 以管理员身份登录。
- 3 单击**开始 > 控制面板 > 系统 and 安全性 > 启用或禁用自动更新**。
- 4 在“重要更新”菜单中，选择**从不检查更新**。
- 5 取消选择**以接收重要更新的相同方式为我提供推荐的更新**。
- 6 取消选择**允许所有用户在此计算机上安装更新**，然后单击**确定**。

在 Windows 虚拟机上禁用诊断策略服务

禁用 Windows 诊断策略服务可避免对文件系统执行某些 I/O 操作，从而可以减缓即时克隆或 View Composer 链接克隆虚拟磁盘的增长速度。

如果您的用户需要在桌面上使用诊断工具，请勿禁用 Windows 诊断策略服务。

以下步骤适用于 Windows 7 和 Windows 8。这些步骤可能会因 Windows 操作系统而异。

步骤

- 1 在 vSphere Client 中，选择父虚拟机，然后选择**打开控制台**。
- 2 以管理员身份登录。
- 3 单击**开始 > 控制面板 > 系统 and 安全性 > 管理工具**。
- 4 选择**服务**，然后单击**打开**。
- 5 双击**诊断策略服务**。
- 6 在“诊断策略服务属性 (本地计算机)”对话框中，单击**停止**。
- 7 在“启动类型”菜单中，选择**已禁用**。
- 8 单击**确定**。

在 Windows 虚拟机上禁用预取和超级获取功能

禁用预取和超级获取功能可避免对文件系统执行某些 I/O 操作，从而可以减缓即时克隆或 View Composer 链接克隆虚拟磁盘的增长速度。

要禁用预取和超级获取功能，您必须编辑一个 Windows 注册表项并在虚拟机中禁用预取服务。

以下步骤适用于 Windows 7 和 Windows 8。这些步骤可能会因 Windows 操作系统而异。

前提条件

有关如何使用 Windows 注册表编辑器的信息，请访问 [Microsoft TechNet 网站](#)。

步骤

- 1 在本地 Windows 虚拟机上启动 Windows 注册表编辑器。
- 2 导航至名为 **PrefetchParameters** 的注册表项。
该注册表项位于以下路径中：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters。
- 3 将 **EnablePrefetcher** 和 **EnableSuperfetch** 的值设置为 0。
- 4 单击开始 > 控制面板 > 系统 and 安全性 > 管理工具。
- 5 选择服务，然后单击打开。
- 6 双击 **Superfetch** 服务。
- 7 在“Superfetch 的属性 (本地计算机)”对话框中，单击停止。
- 8 在“启动类型”菜单中，选择已禁用。
- 9 单击确定。

在 Windows 虚拟机上禁用 Windows 注册表备份

禁用 Windows 注册表备份功能 (RegIdleBackup) 可避免对文件系统执行某些 I/O 操作，从而可以减缓即时克隆或 View Composer 链接克隆虚拟磁盘的增长速度。

以下步骤适用于 Windows 7 和 Windows 8。这些步骤可能会因 Windows 操作系统而异。

步骤

- 1 在 vSphere Client 中，选择父虚拟机，然后选择打开控制台。
- 2 以管理员身份登录。
- 3 单击开始 > 控制面板 > 系统 and 安全性 > 管理工具。
- 4 选择任务计划程序，然后单击打开。
- 5 在左侧窗格中，展开任务计划程序库、Microsoft、Windows。
- 6 双击注册表并选择 **RegIdleBackup**。
- 7 在“操作”窗格中，单击禁用。

在 Windows 虚拟机上禁用系统还原

禁用 Windows 系统还原功能可避免对文件系统执行某些 I/O 操作，从而可以减缓即时克隆或 View Composer 链接克隆虚拟磁盘的增长速度。

通过系统还原功能，您可以将计算机的状态恢复到以前的某个时间点。您可以通过对即时克隆执行推送映像操作，对 View Composer 链接克隆执行重构或刷新操作来实现相同的效果。此外，对于即时克隆，当用户注销时，会重新创建计算机，从而不必还原系统。

以下步骤适用于 Windows 7 和 Windows 8。这些步骤可能会因 Windows 操作系统而异。

步骤

- 1 在 vSphere Client 中，选择父虚拟机，然后选择**打开控制台**。
- 2 以管理员身份登录。
- 3 单击**开始 > 控制面板 > 系统 and 安全性 > 管理工具**。
- 4 选择**任务计划程序**，然后单击**打开**。
- 5 在左侧窗格中，展开**任务计划程序库、Microsoft、Windows**。
- 6 双击 **SystemRestore** 并选择 **SR**。
- 7 在“操作”窗格中，单击**禁用**。

在 Windows 虚拟机上禁用 Windows Defender

禁用 Windows Defender 可避免对文件系统执行某些 I/O 操作，从而可以减缓即时克隆或 View Composer 链接克隆虚拟磁盘的增长速度。

如果虚拟机上只安装了 Windows Defender 一个反间谍软件，您最好在您环境中的桌面上保留 Windows Defender。

以下步骤适用于 Windows 7 和 Windows 8。这些步骤可能会因 Windows 操作系统而异。

步骤

- 1 在 vSphere Client 中，选择父虚拟机，然后选择**打开控制台**。
- 2 以管理员身份登录。
- 3 单击**开始**并在“查找程序和文件”框中键入 **Windows Defender**。
- 4 单击**工具 > 选项 > 管理员**。
- 5 取消选择**使用此程序**并单击**保存**。

禁用 Windows 虚拟机中的 Microsoft Feeds Synchronization

Windows Internet Explorer 使用 Microsoft Feeds Synchronization 任务更新用户 Web 浏览器中的 RSS 源。禁用此任务可避免对文件系统执行某些 I/O 操作，从而可以减缓即时克隆或 View Composer 链接克隆虚拟磁盘的增长速度。

步骤

- 1 在 vSphere Client 中，选择父虚拟机，然后选择**打开控制台**。
- 2 以管理员身份登录。
- 3 单击**开始 > 控制面板 > 网络和 Internet > Internet** 选项。
- 4 单击**内容**选项卡。
- 5 在“源和网页快讯”下，单击**设置**。
- 6 取消选择**自动检查源和网页快讯的更新**并单击**确定**。
- 7 在“Internet 属性”对话框中，单击**确定**。

准备父虚拟机

要部署即时克隆或 View Composer 链接克隆桌面池，必须先准备父虚拟机。

■ 配置父虚拟机

创建计划用作父项的虚拟机后，需要配置 Windows 环境。

■ 激活即时克隆和 View Composer 链接克隆上的 Windows

要确保在创建 Windows 7、Windows 8/8.1、Windows 10 和 Windows Server 克隆后将其正确激活，必须在父虚拟机上使用 Microsoft 批量激活功能。批量激活技术需要使用批量许可证密钥。

■ 在父虚拟机中禁用 Windows 休眠功能

Windows 休眠功能可创建隐藏的系统文件 `Hiberfil.sys`，并使用此文件来存储混合睡眠所需的信息。禁用休眠功能可减小即时克隆或 View Composer 链接克隆虚拟磁盘的大小。

■ 为 View Composer 链接克隆配置本地存储

对于 View Composer 链接克隆桌面池，您可以将父虚拟机配置为在本地数据存储中存储虚拟机交换文件。链接克隆的交换文件将保留在本地存储中。此功能不适用于即时克隆。

■ 记录 View Composer 父虚拟机的页面文件大小

创建 View Composer 链接克隆桌面池后，您可以将克隆的页面文件和临时文件重定向到一个单独的磁盘。您必须将此磁盘配置为大于父虚拟机上页面文件的大小。

■ 延长 ClonePrep 和 QuickPrep 自定义脚本的超时限制

ClonePrep 和 QuickPrep 同步后或关机脚本的超时限制为 20 秒。通过更改父虚拟机上的 `ExecScriptTimeout` Windows 注册表值，您可以延长此限制。

配置父虚拟机

创建计划用作父项的虚拟机后，需要配置 Windows 环境。

前提条件

- 确认您为部署远程桌面准备了一个虚拟机。请参阅[为克隆创建虚拟机](#)。

父虚拟机可以属于桌面计算机将加入的同一 Active Directory 域，也可以是工作组的成员。

- 确认虚拟机不是从即时克隆或 View Composer 链接克隆转换的虚拟机。

重要事项 您也无法将即时克隆或 View Composer 链接克隆用作父虚拟机。

- 在父虚拟机上安装 Horizon Agent 时，请为即时克隆选择 **VMware Horizon Instant Clone Agent** 选项，或选择 **VMware Horizon View Composer Agent** 选项。请参阅[在虚拟机上安装 Horizon Agent](#)。

要在大型环境中更新 Horizon Agent，您可以使用标准的 Windows 更新机制，例如 Altiris、SMS、LanDesk、BMC 或其他系统管理软件。您还可以使用推送映像或重构操作来更新 Horizon Agent。

注 对于 View Composer 链接克隆，请勿在父虚拟机中更改 VMware View Composer Guest Agent Server 服务的登录帐户。默认情况下，该帐户为 Local System 帐户。如果更改此帐户，通过此父虚拟机创建的链接克隆将无法启动。

- 要部署 Windows 计算机，请配置批量许可证密钥，并使用批量激活功能激活父虚拟机的操作系统。请参阅[激活即时克隆和 View Composer 链接克隆上的 Windows](#)。
- 确认您遵循了优化操作系统的最佳做法。请参阅[为即时克隆和 View Composer 链接克隆虚拟机优化 Windows](#)。
- 熟悉禁用在 Windows Update 中搜索设备驱动程序的过程。参阅 [http://technet.microsoft.com/en-us/library/cc730606\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx) 上的“禁用在 Windows Update 中搜索设备驱动程序”Microsoft Technet 文章。

步骤

- ◆ 移除父虚拟机上的 DHCP 租期，以避免将租借的 IP 地址复制到池中的链接克隆。

a 在父虚拟机上打开一个命令提示符。

b 键入 **ipconfig /release** 命令。

- ◆ 确认系统磁盘包含一个卷。

无法通过包含多个卷的父虚拟机来部署链接克隆。但支持多个虚拟磁盘。

注 对于 View Composer 链接克隆，如果父虚拟机中包含多个虚拟磁盘，则在创建桌面池时，为 View Composer 永久磁盘或一次性数据磁盘选择的驱动器盘符不能是已存在于父虚拟机上的驱动器盘符，也不能与网络上挂载的驱动器所用的驱动器盘符冲突。

- ◆ 确认虚拟机不包含独立磁盘。

为虚拟机拍快照时将排除独立磁盘。克隆是基于快照创建的，因此将不包含独立磁盘。

- ◆ 对于 View Composer 链接克隆，如果您在创建链接克隆计算机时计划配置一次性数据磁盘，请从父虚拟机中移除默认用户 TEMP 和 TMP 变量。

您也可以移除 **pagefile.sys** 文件，避免将文件复制到所有链接克隆上。如果将 **pagefile.sys** 文件保留在父虚拟机中，链接克隆将沿用该文件的只读版本，而一次性数据磁盘则使用另外一个文件版本。

- ◆ 禁用休眠选项可减少每个克隆的虚拟磁盘的大小。

- ◆ 在拍摄父虚拟机快照前，请禁用在 Windows Update 中搜索设备驱动程序。

该 Windows 功能可能会干扰自定义过程。自定义每个克隆时，Windows 可能会在 Internet 上搜索适用于该克隆的最佳驱动程序，从而导致延迟。

- ◆ 在 vSphere Client 中，禁用父虚拟机上的 vApp 选项设置。
- ◆ 在 Windows 8.1、Windows Server 2008 R2 和 Windows Server 2012 R2 计算机上，禁用通过移除未使用的功能来恢复磁盘空间的计划维护任务。

例如: `Schtasks.exe /change /disable /tn "\Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup"`

例如，对于 View Composer 链接克隆，该维护任务会在创建链接克隆之后移除 Sysprep 自定义脚本，从而导致后续重构操作失败并出现自定义操作超时错误。有关详细信息，请参阅 <http://support.microsoft.com/kb/2928948> 上提供的 Microsoft 知识库文章。

后续步骤

使用 vSphere Client 或 vSphere Web Client 为处于关机状态的父虚拟机拍摄快照。此快照提供了克隆的基础映像。

重要事项 在拍摄快照之前，请先关闭父虚拟机。

激活即时克隆和 View Composer 链接克隆上的 Windows

要确保在创建 Windows 7、Windows 8/8.1、Windows 10 和 Windows Server 克隆后将其正确激活，必须在父虚拟机上使用 Microsoft 批量激活功能。批量激活技术需要使用批量许可证密钥。

要使用批量激活功能激活 Windows，您需要使用密钥管理服务 (Key Management Service, KMS)，密钥管理服务需要使用 KMS 许可证密钥。请咨询您的 Microsoft 经销商，获取批量许可证密钥并配置批量激活功能。

注 不支持多激活密钥 (Multiple Activation Key, MAK) 许可。

在创建即时克隆或 View Composer 链接克隆桌面池之前，必须在父虚拟机上使用批量激活功能来激活 Windows。

以下步骤说明了如何进行激活：

- 1 调用相应脚本以移除现有许可证。
- 2 重新启动 Windows。
- 3 调用使用 KMS 许可的脚本以激活 Windows。

KMS 将每个激活的克隆视为具有新颁发许可证的计算机。

在父虚拟机中禁用 Windows 休眠功能

Windows 休眠功能可创建隐藏的系统文件 `Hiberfil.sys`，并使用此文件来存储混合睡眠所需的信息。禁用休眠功能可减小即时克隆或 View Composer 链接克隆虚拟磁盘的大小。

小心 休眠功能不可用时，混合睡眠无法正常工作。如果发生断电，用户可能会丢失数据。

步骤

- 1 在 vSphere Client 中，选择父虚拟机，然后选择**打开控制台**。
- 2 以管理员身份登录。
- 3 禁用休眠选项。
 - a 单击**开始**，然后在**开始搜索**框中键入 `cmd`。
 - b 在搜索结果列表中，右键单击**命令提示符**然后单击**以管理员身份运行**。
 - c 在**用户帐户控制**提示中单击**继续**。
 - d 在命令提示符下，键入 `powercfg.exe /hibernate off`，然后按 Enter 键。
 - e 键入 `exit`，然后按 Enter 键。

为 View Composer 链接克隆配置本地存储

对于 View Composer 链接克隆桌面池，您可以将父虚拟机配置为在本地数据存储中存储虚拟机交换文件。链接克隆的交换文件将保留在本地存储中。此功能不适用于即时克隆。

在此过程中，您需要配置用于虚拟机交换文件（而不是客户机操作系统中的页面文件和临时文件）的本地存储。创建链接克隆池后，您还可以将客户机操作系统的页面文件和临时文件重定向到一个单独的磁盘。请参阅[用于创建链接克隆桌面池的工作表](#)。

步骤

- 1 在将要部署链接克隆池的 ESXi 主机或群集上配置交换文件数据存储。
- 2 当您在 vCenter Server 中创建父虚拟机时，请将虚拟机交换文件存储在本地 ESXi 主机或群集上的交换文件数据存储中：
 - a 在 vSphere Client 中，选择父虚拟机。
 - b 单击**编辑设置**，然后单击**选项**选项卡。
 - c 单击**交换文件位置**，然后单击**存储在主机的交换文件数据存储中**。有关详细说明，请参阅 VMware vSphere 文档。

记录 View Composer 父虚拟机的页面文件大小

创建 View Composer 链接克隆桌面池后，您可以将克隆的页面文件和临时文件重定向到一个单独的磁盘。您必须将此磁盘配置为大于父虚拟机上页面文件的大小。

当配置了单独的一次性文件磁盘的链接克隆关闭电源后，会重新创建该磁盘。此功能可减缓链接克隆大小的增长速度。但是，只有当您配置的一次性文件磁盘容量足以容纳克隆的页面文件时，才能使用此功能。

您必须先记录父虚拟机中的最大页面文件大小，才能配置一次性文件磁盘。链接克隆与父虚拟机具有相同的页面文件大小。

最佳做法是，在拍摄快照前将 `pagefile.sys` 文件从父虚拟机中移除，以避免将该文件复制到所有链接克隆上。请参阅[配置父虚拟机](#)。

注 此功能不同于为虚拟机交换文件配置本地存储。请参阅[View Composer 链接克隆配置本地存储](#)。

步骤

- 1 在 vSphere Client 中，右键单击父虚拟机，然后单击**打开控制台**。
- 2 选择**开始 > 设置 > 控制面板 > 系统**。
- 3 单击**高级选项卡**。
- 4 在“性能”窗格中，单击**设置**。
- 5 单击**高级选项卡**。
- 6 在“虚拟内存”窗格中，单击**更改**。
屏幕上将显示“虚拟内存”页面。
- 7 将页面文件的大小设置为大于分配给虚拟机的内存大小的值。

重要事项 如果**最大大小 (MB)** 设置小于虚拟机内存大小，请输入一个大于内存大小的值并保存新值。

- 8 记录在“所选驱动器的页面文件大小”窗格中配置的**最大大小 (MB)** 设置。

后续步骤

通过该父虚拟机配置链接克隆池后，需要配置一个容量大于页面文件的一次性文件磁盘。

延长 ClonePrep 和 QuickPrep 自定义脚本的超时限制

ClonePrep 和 QuickPrep 同步后或关机脚本的超时限制为 20 秒。通过更改父虚拟机上的 `ExecScriptTimeout` Windows 注册表值，您可以延长此限制。

除了延长超时限制之外，您还可以使用自定义脚本来启动其他执行长时间运行任务的脚本或流程。

注 多数 QuickPrep 自定义脚本可以在 20 秒的限制内完成运行。在延长限制之前，请对脚本进行测试。

步骤

- 1 在父虚拟机上启动 Windows 注册表编辑器。
 - a 选择**开始 > 命令提示符**。
 - b 通过命令提示符键入 **regedit**。
- 2 在 Windows 注册表中，找到 `vmware-viewcomposer-ga` 注册表项。
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vmware-viewcomposer-ga`

3 单击**编辑**，并修改注册表值。

```
Value Name: ExecScriptTimeout
Value Type: REG_DWORD
Value unit: milliseconds
```

默认值为 20000 毫秒。

创建虚拟机模板

您必须先创建虚拟机模板，才能创建包含完整虚拟机的自动池。

虚拟机模板是虚拟机的主要副本，可用于创建和置备新的虚拟机。通常情况下，模板中包括已安装的客户机操作系统和一组应用程序。

您可以在 **vSphere Client** 中创建虚拟机模板。您可以通过先前配置的虚拟机创建虚拟机模板，也可以将先前配置的虚拟机转换为虚拟机模板。

有关使用 **vSphere Client** 创建虚拟机模板的信息，请参阅《**vSphere Basic System Administration**》（**vSphere 基本系统管理**）指南。请参阅[包含完整虚拟机的自动池](#)，了解有关创建自动池的信息。

注 虚拟机模板不用于创建即时克隆或 **View Composer** 链接克隆桌面池。

创建自定义规范

使用 **Sysprep** 自定义克隆时，您需要提供自定义规范。

Sysprep 可用于 **View Composer** 链接克隆桌面池和自动完整克隆桌面池，但不适用于即时克隆桌面池。您可在 **vSphere** 中使用“自定义规范”向导创建自定义规范。有关使用“自定义规范”向导的信息，请参阅《**vSphere Virtual Machine Administration**》（**vSphere 虚拟机管理**）文档。

建议您先在 **vSphere** 中测试自定义规范，然后再使用该规范创建桌面池。在使用 **Sysprep** 自定义规范将 **Windows** 桌面加入一个域中时，您必须使用 **Active Directory** 域的完全限定域名 (Fully Qualified Domain Name, FQDN)。您不能使用 **NetBIOS** 名称。

创建包含完整虚拟机的自动桌面池

利用包含完整虚拟机的自动桌面池，可以创建虚拟机模板，View 使用该模板为每个桌面创建虚拟机。还可以选择性创建自定义规范，以加快自动池的部署。

本章讨论了以下主题：

- 包含完整虚拟机的自动池
- 用于创建包含完整虚拟机的自动池的工作表
- 创建包含完整虚拟机的自动池
- 克隆自动桌面池
- 包含完整虚拟机的自动池的桌面设置

包含完整虚拟机的自动池

为创建自动桌面池，View 会根据您应用于该池的设置动态置备计算机。View 使用虚拟机模板作为池的基础。通过模板，View 在 vCenter Server 中为每个桌面创建新虚拟机。

用于创建包含完整虚拟机的自动池的工作表

当您创建自动桌面池时，View Administrator 的添加桌面池向导会提示您配置特定选项。您可以使用此工作表在创建池之前准备配置选项。

您可以打印此工作表，并记下您要在运行添加桌面池向导时指定的值。

表 4-1. 工作表：用于创建包含完整虚拟机的自动池的配置选项

选项	说明	在此填写您要指定的值
用户分配	<p>选择用户分配类型：</p> <ul style="list-style-type: none"> ■ 在专用分配池中，每个用户会分配给一台计算机。用户每次登录到该池时都会收到相同的计算机。 ■ 在浮动分配池中，用户每次登录时都会接收到不同的计算机。 <p>有关详细信息，请参阅桌面池中的用户分配。</p>	
启用自动分配	<p>在专用分配池中，计算机在用户首次登录池时分配给该用户。还可以将计算机明确分配给用户。</p> <p>如果不启用自动分配，必须明确为每个用户分配计算机。</p> <p>即使在启用自动分配时，您也可以手动分配计算机。</p>	

选项	说明	在此填写您要指定的值
vCenter Server	选择用于管理池中虚拟机的 vCenter Server。	
桌面池 ID	<p>用于在 View Administrator 中标识池的唯一名称。</p> <p>如果您的环境中正在运行多个 vCenter Server，应确保其他 vCenter Server 没有使用同一个池 ID。</p> <p>View 连接服务器配置可以是独立的 View 连接服务器实例，或者是共享通用 View LDAP 配置的副本实例的容器。</p>	
显示名称	用户从客户端设备登录时所看到的池名称。如果不指定显示名称，系统将向用户显示池 ID。	
访问组	<p>选择用来存放池的访问组，或者将池留在默认的根访问组中。</p> <p>如果使用访问组，则可以将池的管理委托给某个具有特定角色的管理员。有关详细信息，请参阅《View 管理指南》文档中基于角色的委托管理章节。</p> <p>注 访问组不同于用来存储桌面虚拟机的 vCenter Server 文件夹。稍后，您需要在向导中选择存储其他 vCenter Server 设置的 vCenter Server 文件夹。</p>	
注销后删除计算机	<p>如果您选择浮动用户分配，需要选择是否在用户注销后删除计算机。</p> <p>注 可以在“桌面池设置”页面设置该选项。</p>	
桌面池设置	<p>这些设置用于确定桌面状态、虚拟机处于未使用状态时的电源状态、显示协议、Adobe Flash 质量等。</p> <p>有关说明，请参阅适用于所有桌面池类型的桌面池设置。</p> <p>有关适用于自动池的设置列表，请参阅包含完整虚拟机的自动池的桌面设置。</p> <p>有关电源策略和自动池的更多信息，请参阅为桌面池设置电源策略。</p>	
出现错误时停止置备	您可以指示 View 在置备虚拟机期间出现错误后停止置备或继续置备桌面池中的虚拟机。如果选择该设置，可以防止置备错误在多个虚拟机上重现。	
虚拟机命名	<p>选择置备计算机的方式是手动指定计算机名称列表，还是提供命名模式和计算机总数。</p> <p>有关详细信息，请参阅手动命名计算机或提供命名模式。</p>	
手动指定名称	如果手动指定名称，请准备计算机名称列表，以及关联的用户名（可选）。	
命名模式	<p>如果要采用这种命名方式，则需要提供命名模式。</p> <p>指定的模式用作所有计算机名称的前缀，后接一个唯一的编号，以标识每个计算机。</p> <p>有关详细信息，请参阅为自动桌面池使用命名模式。</p>	
计算机的最大数量	<p>如果您使用命名模式，需要指定池中的计算机总数。</p> <p>您还可以指定在首次创建池时要置备的最小计算机数。</p>	

选项	说明	在此填写您要指定的值
备用 (已打开电源) 计算机数量	<p>如果手动指定名称或者使用命名模式，需要指定可供新用户使用并且已打开电源的计算机的数量。有关详细信息，请参阅手动命名计算机或提供命名模式。</p> <p>手动指定名称时，该选项称为保持打开电源状态的未分配计算机的数量。</p>	
计算机的最小数量	<p>如果您使用命名模式并根据需要置备计算机，则需要指定池中的最小计算机总数。</p> <p>创建池时会创建最小数量的计算机。</p> <p>如果您按需置备计算机，则在用户首次连接到池或在您将计算机分配给用户时创建其他计算机。</p>	
使用 vSphere Virtual SAN	<p>指定是否使用 Virtual SAN（如果可用）。Virtual SAN 是一个软件定义的存储层，可以虚拟化在 ESXi 主机的群集上可用的本地物理存储磁盘。有关更多信息，请参阅使用 Virtual SAN 实现高性能存储和基于策略的管理。</p>	
模板	选择要用于创建池的虚拟机模板。	
vCenter Server 文件夹	选择要在其中驻留桌面池的 vCenter Server 文件夹。	
主机或群集	<p>选择要在其中运行虚拟机的 ESXi 主机或群集。</p> <p>在 vSphere 5.1 或更高版本中，您可以选择最多包含 32 台 ESXi 主机的群集。</p>	
资源池	选择要在其中驻留桌面池的 vCenter Server 资源池。	
数据存储	<p>选择一个或多个要在其中存储桌面池的数据存储区。</p> <p>对于群集，您可以使用共享或本地数据存储。</p> <p>注 如果使用 Virtual SAN，则只选择一个数据存储。</p>	
使用 View Storage Accelerator	<p>确定 ESXi 主机是否缓存常用虚拟机磁盘数据。View Storage Accelerator 可以提高性能并减少用于管理引导风暴和防病毒扫描 I/O 风暴的额外存储 I/O 带宽需求。</p> <p>vSphere 5.0 及更高版本支持此功能。</p> <p>该功能在默认情况下为启用状态。</p> <p>有关详细信息，请参阅View Composer 链接克隆配置 View Storage Accelerator。</p>	

选项	说明	在此填写您要指定的值
透明页面共享范围	<p>选择允许透明页面共享 (TPS) 的级别。选项包括：虚拟机（默认）、池、容器或全局。如果在池、容器或全局级别为所有计算机打开 TPS，ESXi 主机将消除因这些计算机使用同一客户机操作系统或应用程序而产生的内存冗余副本。</p> <p>页面共享发生在 ESXi 主机上。例如，如果在池级别启用 TPS，但池分散到多个 ESXi 主机，则只有同一主机和同一池中的虚拟机将共享页面。在全局级别，同一 ESXi 主机上所有受 View 管理的计算机都可以共享内存页，而不管这些计算机驻留在哪个池中。</p> <p>注 默认设置是不在计算机之间共享内存页，因为 TPS 可能会带来安全风险。调查表明可能会在非常有限的配置场景下滥用 TPS 来获取对数据的未授权访问。</p>	
客户机自定义	<p>从列表中选择一种自定义规范 (SYSPREP)，以配置许可、域附属、DHCP 设置以及计算机上的其他属性。</p> <p>或者，您也可以在创建计算机后手动自定义计算机。</p>	

创建包含完整虚拟机的自动池

您可以根据所选择的虚拟机模板来创建自动桌面池。View 会动态地部署桌面，在 vCenter Server 中为每个桌面创建一个新虚拟机。

前提条件

- 为 View 准备创建计算机时要使用的虚拟机模板。必须在模板上安装 Horizon Agent。请参阅[第 3 章 为克隆创建并准备父虚拟机](#)。
- 如果您希望使用自定义规范，请确保规范的准确性。在 vSphere Client 中，使用自定义规范按照您的模板部署和自定义虚拟机。全面测试生成的虚拟机，包括 DHCP 和身份验证。
- 确认用于虚拟机（用作远程桌面）的 ESXi 虚拟交换机上的端口数量充足。如果要创建大型桌面池，默认值可能不足以满足要求。ESXi 主机上的虚拟交换机端口的数量必须大于或等于虚拟机数量与每个虚拟机的虚拟网卡的数量的乘积。
- 收集您在创建池时必须提供的配置信息。请参阅[用于创建包含完整虚拟机的自动池的工作表](#)。
- 确定如何配置电源设置、显示协议、Adobe Flash 质量及其他设置。请参阅[适用于所有桌面池类型的桌面池设置](#)。
- 如果您想要通过 VMware Identity Manager 提供桌面和应用程序访问，请确认您作为拥有 View Administrator 根访问组的管理员角色的用户来创建桌面和应用程序池。如果您在其他访问组而非根访问组上向用户提供管理员角色，VMware Identity Manager 将不会识别您在 View 中配置的 SAML 身份验证器，您将无法在 VMware Identity Manager 中配置池。

步骤

- 1 在 View Administrator 中，选择目录 > 桌面池。

- 2 单击**添加**。
- 3 选择**自动桌面池**。
- 4 从 **vCenter Server** 页面上选择**完整虚拟机**。
- 5 按照向导中的提示创建池。

使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，您可以直接返回至已完成的任意向导页面。

在 View Administrator 中，可以在将计算机添加到池时查看这些计算机，方法是选择**目录 > 桌面池**。

后续步骤

授予用户访问池的权限。请参阅[为桌面池或应用程序池添加授权](#)。

克隆自动桌面池

您可以通过现有的池克隆自动桌面池。在克隆池时，现有桌面池的设置将复制到**添加桌面池**向导中，以便创建新的池而无需手动填写每个设置。

通过使用该功能，您可以简化创建池的过程，因为您不必在**添加桌面池**向导中键入每个选项。您可以确保使用向导中的预填充值标准化桌面池属性。

您可以克隆包含完整虚拟机或 **View Composer** 链接克隆的自动桌面池。您无法克隆包含即时克隆的自动桌面池、手动桌面池或 **RDS** 桌面池。

在克隆桌面池时，您无法更改某些设置：

- 桌面池类型
- 克隆类型（链接克隆或完整虚拟机）
- 用户分配（专用或浮动）
- vCenter Server 实例

前提条件

- 确认创建原始桌面池的前提条件仍然有效。

例如，对于包含完整虚拟机的池，确认准备了虚拟机模板。

对于链接克隆池，确认准备了父虚拟机并在关闭虚拟机后拍摄了快照。

在克隆池时，您可以使用相同的虚拟机模板或父虚拟机，也可以选择其他虚拟机模板或父虚拟机。

- 有关克隆自动完整克隆池的前提条件，请参阅[创建包含完整虚拟机的自动池](#)。
- 有关克隆链接克隆池的前提条件，请参阅[创建链接克隆桌面池](#)。

步骤

- 1 在 View Administrator 中，选择**目录 > 桌面池**。

- 2 选择要克隆的桌面池，然后单击**克隆**。

将显示**添加桌面池**向导。

- 3 在**添加桌面池**页上，键入唯一的池 ID。

- 4 在**置备设置**页上，为虚拟机提供唯一的名称。

选项	说明
使用一种命名模式	键入一种虚拟机命名模式。
手动指定名称	为虚拟机提供唯一的名称列表。

- 5 按照向导中的其他提示创建池。

根据需要，更改桌面池设置和值。

在 View Administrator 中，可以在将计算机添加到池时查看这些计算机，方法是选择**目录 > 桌面池**。

后续步骤

授予用户访问池的权限。请参阅[为桌面池或应用程序池添加授权](#)。

包含完整虚拟机的自动池的桌面设置

配置包含完整虚拟机的自动池时，您必须指定桌面池设置。适用于专用用户分配池和浮动用户分配池的设置有所不同。

[表 4-2. 包含完整虚拟机的自动池设置](#) 列出了适用于专用分配自动池和浮动分配自动池的设置。

有关每种桌面池设置的描述，请参阅[适用于所有桌面池类型的桌面池设置](#)。

表 4-2. 包含完整虚拟机的自动池设置

设置	专用分配自动池	浮动分配自动池
状态	是	是
连接服务器限制	是	是
远程计算机电源策略	是	是
断开连接后自动注销	是	是
允许用户重置其计算机	是	是
允许用户从不同的客户端设备启动单独的会话		是
注销后删除计算机		是
默认显示协议	是	是
允许用户选择协议	是	是
3D 呈现器	是	是
显示器最大数量	是	是
任意一台显示器的最大分辨率	是	是

在 **View** 中设置桌面和应用程序池

设置	专用分配自动池	浮动分配自动池
Adobe Flash 质量	是	是
Adobe Flash 调节	是	是
覆盖全局 Mirage 设置	是	是
Mirage 服务器配置	是	是

创建链接克隆桌面池

对于链接克隆桌面池，View 会基于您选择的父虚拟机创建桌面池。View Composer 服务可在 vCenter Server 中为每个桌面动态创建新的链接克隆虚拟机。

本章讨论了以下主题：

- [链接克隆桌面池](#)
- [用于创建链接克隆桌面池的工作表](#)
- [创建链接克隆桌面池](#)
- [克隆自动桌面池](#)
- [链接克隆桌面池的桌面池设置](#)
- [View Composer 对链接克隆 SID 和第三方应用程序的支持](#)
- [在 View Composer 操作期间将链接克隆计算机保持已置备状态以在远程桌面会话中使用](#)
- [针对链接克隆使用现有的 Active Directory 计算机帐户](#)

链接克隆桌面池

为创建链接克隆桌面池，View Composer 会从一个父虚拟机的某个快照生成链接克隆虚拟机。View 会根据您应用于池的设置动态地置备链接克隆桌面池。

由于链接克隆桌面会共享一个基础系统磁盘映像，因此它们使用的存储空间比完整虚拟机要少。

用于创建链接克隆桌面池的工作表

当您创建链接克隆桌面池时，View Administrator 的[添加桌面池](#)向导会提示您配置特定选项。您可以使用此工作表在创建池之前准备配置选项。

您可以打印此工作表，并记下您要在运行[添加桌面池](#)向导时指定的值。

在创建链接克隆池之前，您必须使用 vCenter Server 为准备用作池的父虚拟机拍摄快照。为父虚拟机拍摄快照之前必须将其关闭。View Composer 将使用该快照作为基础映像来创建克隆。

注 您不能从虚拟机模板来创建链接克隆池。

表 5-1. 工作表：用于创建链接克隆桌面池的配置选项

选项	说明	在此填写您要指定的值
用户分配	<p>选择用户分配类型：</p> <ul style="list-style-type: none"> ■ 在专用分配池中，每个用户会分配给一台计算机。用户每次登录时接收到的都是同一台计算机。 ■ 在浮动分配池中，用户每次登录时都会接收到不同的计算机。 <p>有关详细信息，请参阅桌面池中的用户分配。</p>	
启用自动分配	<p>在专用分配池中，计算机在用户首次登录池时分配给该用户。还可以将计算机明确分配给用户。</p> <p>如果不启用自动分配，必须明确为每个用户分配计算机。</p>	
vCenter Server	选择用于管理池中虚拟机的 vCenter Server。	
桌面池 ID	<p>用于在 View Administrator 中标识池的唯一名称。</p> <p>如果您的环境中运行了多个 View 连接服务器配置，应确保其他 View 连接服务器配置未使用同一个池 ID。</p> <p>View 连接服务器配置可以是独立的 View 连接服务器实例，或者是共享通用 View LDAP 配置的副本实例的容器。</p>	
显示名称	用户从客户端设备登录时所看到的池名称。如果不指定显示名称，系统将向用户显示池 ID。	
访问组	<p>选择用来存放池的访问组，或者将池留在默认的根访问组中。</p> <p>如果使用访问组，则可以将池的管理委托给某个具有特定角色的管理员。有关详细信息，请参阅《View 管理指南》文档中基于角色的委托管理章节。</p> <p>注 访问组不同于存储用作桌面的虚拟机的 vCenter Server 文件夹。稍后，您需要在向导中选择存储其他 vCenter Server 设置的 vCenter Server 文件夹。</p>	
注销时删除或刷新计算机	<p>如果选择浮动用户分配，需要选择在用户注销后刷新计算机、删除计算机还是不执行任何操作。</p> <p>注 可以在“桌面池设置”页面设置该选项。</p>	
桌面池设置	<p>这些设置用于确定计算机状态、虚拟机处于未使用状态时的电源状态、显示协议、Adobe Flash 质量等。</p> <p>有关说明，请参阅适用于所有桌面池类型的桌面池设置。</p> <p>有关适用于链接克隆池的设置列表，请参阅链接克隆桌面池的桌面池设置。</p> <p>有关电源策略和自动池的更多信息，请参阅为桌面池设置电源策略。</p>	
出现错误时停止置备	您可以指示 View 在置备虚拟机期间出现错误后停止置备或继续置备桌面池中的虚拟机。如果选择该设置，可以防止置备错误在多个虚拟机上重现。	
虚拟机命名	<p>选择置备计算机的方式是手动指定计算机名称列表，还是提供命名模式和计算机总数。</p> <p>有关详细信息，请参阅手动命名计算机或提供命名模式。</p>	

选项	说明	在此填写您要指定的值
手动指定名称	如果手动指定名称，请准备计算机名称列表，以及关联的用户名（可选）。	
命名模式	如果要采用这种命名方式，则需要提供命名模式。 指定的模式用作所有计算机名称的前缀，后接一个唯一的编号，以标识每个计算机。 有关详细信息，请参阅 为自动桌面池使用命名模式 。	
计算机的最大数量	如果您使用命名模式，需要指定池中的计算机总数。 您还可以指定在首次创建池时要置备的最小计算机数。	
备用 (已打开电源的) 计算机数量	如果手动指定名称或者使用命名模式，需要指定可供新用户使用并且已打开电源的计算机的数量。有关详细信息，请参阅 手动命名计算机或提供命名模式 。 手动指定名称时，该选项称为 保持打开电源状态的未分配计算机的数量 。	
View Composer 维护操作期间就绪 (已置备) 计算机的最小数量	如果手动指定名称或使用命名模式，请指定在执行 View Composer 维护操作时处于已置备状态以在远程桌面会话中使用的最小计算机数量。 通过使用该设置，用户可以在 View Composer 刷新、重构或重新平衡池中的计算机时保持现有的连接或发送新的连接请求。该设置不区别准备接受新连接的备用计算机和已在现有桌面会话中连接的计算机。 该值必须小于 计算机的最大数量 ，这是在按需置备计算机时指定的。 请参阅在 View Composer 操作期间将链接克隆计算机保持已置备状态以在远程桌面会话中使用 。	
按需置备计算机 或 预先置备所有计算机	如果使用命名模式，请选择是在创建池时置备所有计算机还是按需置备计算机。 <ul style="list-style-type: none"> ■ 预先置备所有计算机。创建池时，系统置备的计算机数量为您在计算机的最大数量中指定的数量。 ■ 按需置备计算机。创建池时，系统创建的计算机数量为您在计算机的最小数量中指定的数量。其他计算机在用户首次连接池或您为用户分配计算机时创建。 	
计算机的最小数量	如果您使用命名模式，并根据需要置备桌面，则需要指定池中计算机的最小数量。 系统会在您创建池时创建最小数量的计算机。即使其他设置（如 注销时删除或刷新计算机 ）导致计算机被删除，也会保持这一数量。	

选项	说明	在此填写您要指定的值
将 Windows 配置文件重定向到永久磁盘	<p>如果您选择专用用户分配，需要选择将 Windows 用户配置文件数据存储在一个单独的 View Composer 永久磁盘上，还是与操作系统数据存储在同一磁盘上。</p> <p>您可以使用单独的永久磁盘保留用户数据和设置。View Composer 刷新、重构和重新平衡操作不会影响永久磁盘。您可以将永久磁盘从链接克隆分离，并通过分离的磁盘重新创建链接克隆虚拟机。例如，删除计算机或池时，您可以分离永久磁盘并重新创建桌面，从而保留原始用户数据和设置。</p> <p>如果将 Windows 配置文件存储在操作系统磁盘中，则在刷新、重构和重新平衡操作过程中，用户数据和设置将被移除。</p>	
Disk size and drive letter for persistent disk（永久磁盘的磁盘大小和驱动器盘符）	<p>如果将用户配置文件数据存储在一个单独的 View Composer 永久磁盘中，则需要提供磁盘大小（以 MB 为单位）和驱动器盘符。</p> <p>注 不要选择父虚拟机上已经存在的驱动器盘符，或者与网络上装载的驱动器所用的驱动器盘符冲突的驱动器盘符。</p>	
一次性文件重定向	<p>选择是否将客户机操作系统的页面文件和临时文件重定向到一个单独的非永久磁盘。如果选择这样做，则需要指定磁盘大小（以 MB 为单位）。</p> <p>使用该配置时，当链接克隆关闭电源后，一次性文件磁盘被替换为使用链接克隆池创建的原始磁盘的副本。链接克隆的大小在用户与其桌面交互过程中会增长。一次性文件重定向可以减缓链接克隆的增长速度，从而节省存储空间。</p>	
一次性文件磁盘的磁盘大小和驱动器盘符	<p>如果将一次性文件重定向到一个非永久磁盘，请提供以兆字节为单位的磁盘大小和驱动器盘符。</p> <p>磁盘大小应大于客户机操作系统的页面文件大小。要确定页面文件的大小，请参阅记录 View Composer 父虚拟机的页面文件大小。</p> <p>配置一次性文件磁盘大小时，需注意格式化磁盘分区的实际大小比您在 View Administrator 中提供的值略小。</p> <p>您可以为一次性文件磁盘选择一个驱动器盘符。默认值为自动，可引导 View 分配驱动器盘符。</p> <p>注 不要选择父虚拟机上已经存在的驱动器盘符，或者与网络上装载的驱动器所用的驱动器盘符冲突的驱动器盘符。</p>	
使用 vSphere Virtual SAN	<p>指定是否使用 VMware Virtual SAN（如果可用）。Virtual SAN 是一个软件定义的存储层，可以虚拟化在 ESXi 主机的群集上可用的本地物理存储磁盘。有关更多信息，请参阅使用 Virtual SAN 实现高性能存储和基于策略的管理。</p>	
为永久磁盘和操作系统磁盘选择单独的数据存储	<p>（仅在不使用 Virtual SAN 时有效）如果将用户配置文件重定向到单独的永久磁盘，则可以将永久磁盘和操作系统磁盘存储在不同的数据存储中。</p>	

选项	说明	在此填写您要指定的值
为副本磁盘和操作系统磁盘选择单独的数据存储	<p>（仅在不使用 Virtual SAN 或虚拟卷时有效）可以将副本（主）虚拟机磁盘存储在高性能数据存储中，将链接克隆存储在单独的数据存储中。</p> <p>有关详细信息，请参阅将即时克隆和 View Composer 链接克隆的副本和克隆存储在不同的数据存储中。</p> <p>如果您将副本磁盘和操作系统磁盘存储在单独的数据存储中，则本地 NFS 快照无法使用。NAS 设备上的本地克隆仅在副本磁盘和操作系统磁盘存储在相同的数据存储中时发生。</p>	
父虚拟机	为池选择父虚拟机。	
快照 (默认映像)	<p>选择要用作池的基础映像的父虚拟机快照。</p> <p>不要删除 vCenter Server 中的快照和父虚拟机，除非池中的链接克隆均不使用此默认映像，且不会根据此默认映像创建链接克隆。系统需要使用父虚拟机和快照根据池策略在池中置备新的链接克隆。View Composer 维护操作也需要父虚拟机和快照。</p>	
虚拟机文件夹位置	选择要在其中驻留桌面池的 vCenter Server 文件夹。	
主机或群集	<p>选择要用来运行桌面虚拟机的 ESXi 主机或群集。</p> <p>使用 Virtual SAN 数据存储（vSphere 5.5 Update 1 的一项功能），可以选择最多包含 20 个 ESXi 主机的群集。使用虚拟卷数据存储（vSphere 6.0 的一项功能），可以选择最多包含 32 个 ESXi 主机的群集。</p> <p>在 vSphere 5.1 或更高版本中，如果副本存储在 VMFS5 或更高版本的数据存储中或 NFS 数据存储中，您就可选择最多含有 32 个 ESXi 主机的群集。如果您将副本磁盘存储在 VMFS5 之前的版本中，群集最多可包含 8 台主机。</p> <p>在 vSphere 5.0 中，如果副本存储于 NFS 数据存储中，则可选择包含八台以上 ESXi 主机的群集。如果您在 VMFS 数据存储中存储副本，则一个群集最多包含八台主机。请参阅在包含超过 8 个主机的群集上配置桌面池。</p>	
资源池	选择要在其中驻留桌面池的 vCenter Server 资源池。	

选项	说明	在此填写您要指定的值
数据存储	<p>选择一个或多个要在其中存储桌面池的数据存储区。</p> <p>“添加桌面池”向导中选择链接克隆数据存储页面上的一个表提供了估算池的存储要求的高级指导原则。这些信息能帮助您确定哪个数据存储有足够空间存储链接克隆磁盘。有关详细信息，请参阅确定即时克隆和 View Composer 链接克隆桌面池的存储大小。</p> <p>您可将共享数据存储或本地数据存储用于单个的 ESXi 主机或 ESXi 群集。如果您在 ESXi 群集中使用本地数据存储，则您必须考虑桌面部署的 vSphere 基础架构限制。请参阅在本地数据存储上存储 View Composer 链接克隆。</p> <p>使用 Virtual SAN 数据存储（vSphere 5.5 Update 1 的一项功能），可以选择最多包含 20 个 ESXi 主机的群集。使用虚拟卷数据存储（vSphere 6.0 的一项功能），可以选择最多包含 32 个 ESXi 主机的群集。</p> <p>在 vSphere 5.1 或更高版本中，如果副本存储在 VMFS5（或更高版本）或 NFS 数据存储中，则群集可包含 8 台以上的 ESXi 主机。在 vSphere 5.0 中，副本只有存储在 NFS 数据存储中时，群集才能包含 8 台以上的 ESXi 主机。请参阅在包含超过 8 个主机的群集上配置桌面池。</p> <p>有关为链接克隆创建的磁盘的更多信息，请参阅 View Composer 链接克隆数据磁盘。</p> <p>注 如果使用 Virtual SAN，则只选择一个数据存储。</p>	
存储过载	<p>确定在每个数据存储上创建链接克隆时的存储过载级别。</p> <p>随着级别的增加，数据存储上装载的链接克隆会越来越多，而为单个克隆的增长所保留的空间则越来越少。如果设置较高的存储过载级别，您创建的链接克隆的总逻辑大小就可以大于数据存储的物理存储限制。有关详细信息，请参阅设置链接克隆虚拟机的存储过载级别。</p> <p>注 如果使用 Virtual SAN，则该设置无效。</p>	
使用 View Storage Accelerator	<p>确定是否使用 View Storage Accelerator，View Storage Accelerator 可允许 ESXi 主机缓存常用虚拟机磁盘数据。View Storage Accelerator 可以提高性能并减少用于管理引导风暴和防病毒扫描 I/O 风暴的额外存储 I/O 带宽需求。</p> <p>vSphere 5.0 及更高版本支持此功能。</p> <p>该功能在默认情况下为启用状态。</p> <p>有关详细信息，请参阅View Composer 链接克隆配置 View Storage Accelerator。</p>	

选项	说明	在此填写您要指定的值
使用本地 NFS 快照 (VAAI)	<p>（仅在不使用 Virtual SAN 时有效）如果部署中包含支持 vStorage APIs for Array Integration (VAAI) 的 NAS 设备，则可以使用本地快照技术克隆虚拟机。</p> <p>仅当您选择了位于通过 VAAI 支持本地克隆操作的 NAS 设备上的数据存储时，才可以使用此功能。</p> <p>如果您将副本磁盘和操作系统磁盘存储在单独的数据存储中，则无法使用这些功能。无法在包含能节省空间的磁盘的虚拟机上使用此功能。</p> <p>vSphere 5.0 及更高版本支持此功能。</p> <p>有关详细信息，请参阅将 VAAI 存储用于 View Composer 链接克隆。</p>	
回收虚拟机磁盘空间	<p>（仅在不使用 Virtual SAN 或虚拟卷时有效）确定是否允许 ESXi 主机回收以节省空间的磁盘格式创建的链接克隆上的未用磁盘空间。空间回收功能减少了链接克隆桌面所需的总存储空间。</p> <p>vSphere 5.1 及更高版本支持此功能。链接克隆虚拟机必须是虚拟硬件版本 9 或更高版本。</p> <p>有关详细信息，请参阅在 View Composer 链接克隆上回收磁盘空间。</p>	
在虚拟机上的未使用空间超出以下值时启动回收：	<p>（仅在不使用 Virtual SAN 或虚拟卷时有效）键入为触发空间回收而必须在链接克隆操作系统磁盘上累积的未用磁盘空间的最小数量（千兆字节）。当未使用的磁盘空间超过此阈值时，View 将启动操作，指示 ESXi 主机回收操作系统磁盘上的空间。</p> <p>此值根据虚拟机而测得。在 View 开始对单个虚拟机进行空间回收过程之前，未使用的磁盘空间必须超过相应虚拟机上指定的阈值。</p> <p>例如：2 GB。</p> <p>默认值为 1 GB。</p>	
中断时间	<p>配置中断天数和时间，在此期间不进行 View Storage Accelerator 重新生成和虚拟机磁盘空间回收操作。</p> <p>为了确保必要时 ESXi 资源专供前台任务使用，您可以在指定日期的指定时段内禁止 ESXi 主机执行这些操作。</p> <p>有关详细信息，请参阅View Composer 链接克隆设置 Storage Accelerator 和空间回收中断时间。</p>	
透明页面共享范围	<p>选择允许透明页面共享 (TPS) 的级别。选项包括：虚拟机（默认）、池、容器或全局。如果在池、容器或全局级别为所有计算机打开 TPS，ESXi 主机将消除因这些计算机使用同一客户机操作系统或应用程序而产生的内存冗余副本。</p> <p>页面共享发生在 ESXi 主机上。例如，如果在池级别启用 TPS，但池分散到多个 ESXi 主机，则只有同一主机和同一池中的虚拟机将共享页面。在全局级别，同一 ESXi 主机上所有受 View 管理的计算机都可以共享内存页，而不管这些计算机驻留在哪个池中。</p> <p>注 默认设置是不在计算机之间共享内存页，因为 TPS 可能会带来安全风险。调查表明可能会在非常有限的配置场景下滥用 TPS 来获取对数据的未授权访问。</p>	

选项	说明	在此填写您要指定的值
域	<p>选择 Active Directory 域和用户名。</p> <p>View Composer 要求使用特定用户特权来创建链接克隆池。QuickPrep 或 Sysprep 使用域和用户帐户来自定义链接克隆计算机。</p> <p>当您为 vCenter Server 配置 View Composer 设置时，应指定此用户。配置 View Composer 设置时，可以指定多个域和用户。使用添加桌面池向导创建池时，必须从列表选择一个域和用户。</p> <p>有关配置 View Composer 的信息，请参阅《View 管理指南》文档。</p>	
AD 容器	<p>提供 Active Directory 容器的相对专有名称。</p> <p>例如: CN=Computers</p> <p>当您运行添加桌面池向导时，可以浏览 Active Directory 树以找到所需容器。</p>	
允许重新使用已存在的计算机帐户	<p>选择此选项可将 Active Directory 中现有的计算机帐户用于 View Composer 置备的链接克隆。此选项允许您控制在 Active Directory 中创建的计算机帐户。</p> <p>置备链接克隆后，如果现有 AD 计算机帐户名与链接克隆计算机名匹配，则 View Composer 会使用现有的计算机帐户。否则，需创建新的计算机帐户。</p> <p>现有的计算机帐户必须位于您通过 Active Directory 容器 设置而指定的 Active Directory 容器中。</p> <p>如果禁用此选项，View Composer 置备链接克隆时将创建新的 AD 计算机帐户。默认情况下禁用此选项。</p> <p>有关详细信息，请参阅针对链接克隆使用现有的 Active Directory 计算机帐户。</p>	
Use QuickPrep or a customization specification (Sysprep) (使用 QuickPrep 或自定义规范 (Sysprep))	<p>选择使用 QuickPrep 还是选择自定义规范 (Sysprep) 来配置许可、域附属、DHCP 设置和其他计算机属性。</p> <p>仅 vSphere 4.1 或更高版本软件支持 Sysprep 用于链接克隆。</p> <p>使用 QuickPrep 或 Sysprep 创建池后，无法在以后创建或重构池中的计算机时转换为其他自定义方法。</p> <p>有关详细信息，请参阅选择 QuickPrep 或 Sysprep 来自定义链接克隆计算机。</p>	
关机脚本	<p>QuickPrep 可以在链接克隆计算机的电源关闭之前在这些计算机上运行自定义脚本。</p> <p>提供父虚拟机上的脚本的路径以及脚本参数。</p>	
同步后脚本	<p>QuickPrep 可以在创建、重构和刷新克隆计算机后在这些计算机上运行自定义脚本。</p> <p>提供父虚拟机上的脚本的路径以及脚本参数。</p>	

创建链接克隆桌面池

您可以根据所选择的父虚拟机来创建自动链接克隆桌面池。View Composer 服务可在 vCenter Server 中为每个桌面动态创建新的链接克隆虚拟机。

要创建包含完整虚拟机的自动池，请参阅[包含完整虚拟机的自动池](#)。

前提条件

- 确认在与 vCenter Server 相同的主机或其他主机上安装了 View Composer 服务，并且配置了 View Composer 数据库。请参阅《View 安装指南》文档。
- 确认在 View Administrator 中配置了适用于 vCenter Server 的 View Composer 设置。请参阅《View 管理指南》文档。
- 确认用于虚拟机（用作远程桌面）的 ESXi 虚拟交换机上的端口数量充足。如果要创建大型桌面池，默认值可能不足以满足要求。ESXi 主机上的虚拟交换机端口的数量必须大于或等于虚拟机数量与每个虚拟机的虚拟网卡的数量的乘积。
- 确认已准备好父虚拟机。必须在该父虚拟机上安装 Horizon Agent。请参阅[第 3 章 为克隆创建并准备父虚拟机](#)。
- 在 vCenter Server 中为父虚拟机拍摄一个快照。为父虚拟机拍摄快照之前必须将其关闭。View Composer 将使用该快照作为基础映像来创建克隆。

注 您不能从虚拟机模板来创建链接克隆池。

- 收集您在创建池时必须提供的配置信息。请参阅[用于创建链接克隆桌面池的工作表](#)。
- 确定如何配置电源设置、显示协议、Adobe Flash 质量及其他设置。请参阅[适用于所有桌面池类型的桌面池设置](#)。
- 如果您想要通过 VMware Identity Manager 提供桌面和应用程序访问，请确认您作为拥有 View Administrator 根访问组的管理员角色的用户来创建桌面和应用程序池。如果您在其他访问组而非根访问组上向用户提供管理员角色，VMware Identity Manager 将不会识别您在 View 中配置的 SAML 身份验证器，您将无法在 VMware Identity Manager 中配置池。

重要事项 创建链接克隆池时，不要在 vCenter Server 中修改父虚拟机。例如，不要将父虚拟机转换为模板。View Composer 服务要求父虚拟机在池创建过程中保持静止不变的状态。

步骤

- 1 在 View Administrator 中，选择目录 > 桌面池。
- 2 单击添加。
- 3 选择自动桌面池。
- 4 从 vCenter Server 页面上选择 View Composer 链接克隆。

5 按照向导中的提示创建池。

使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，您可以直接返回至已完成的任意向导页面。

在 **vCenter 设置** 页面，您必须单击 **浏览** 并按顺序选择 **vCenter Server** 设置。您不能跳过任何 **vCenter Server** 设置：

- a 父虚拟机
- b 快照
- c 虚拟机文件夹位置
- d 主机或群集
- e 资源池
- f 数据存储

在 **View Administrator** 中，可以在将计算机添加到池时查看这些计算机，方法是选择 **目录 > 桌面池**。

链接克隆在置备期间可能会重新启动一次或多次。如果链接克隆处于错误状态，**View** 自动恢复机制将试图开启或关闭并重新启动链接克隆。如果多次恢复尝试失败，则此链接克隆将被删除。

View Composer 还会创建一个用作主映像的副本虚拟机，以供置备链接克隆。为减少占用的空间，该副本将被创建为一个精简磁盘。如果重构或删除了所有虚拟机，且没有任何克隆链接到副本，则系统将把副本虚拟机从 **vCenter Server** 中删除。

如果您未将副本存储在单独的数据存储中，**View Composer** 会在创建链接克隆的每个数据存储中创建一个副本。

如果您将副本存储在单独的数据存储中，则 **View Composer** 将为整个池创建一个副本，即使链接克隆是在多个数据存储上创建的。

后续步骤

授予用户访问池的权限。请参阅[为桌面池或应用程序池添加授权](#)。

克隆自动桌面池

您可以通过现有的池克隆自动桌面池。在克隆池时，现有桌面池的设置将复制到**添加桌面池**向导中，以便创建新的池而无需手动填写每个设置。

通过使用该功能，您可以简化创建池的过程，因为您不必在**添加桌面池**向导中键入每个选项。您可以确保使用向导中的预填充值标准化桌面池属性。

您可以克隆包含完整虚拟机或 **View Composer** 链接克隆的自动桌面池。您无法克隆包含即时克隆的自动桌面池、手动桌面池或 **RDS** 桌面池。

在克隆桌面池时，您无法更改某些设置：

- 桌面池类型
- 克隆类型（链接克隆或完整虚拟机）

- 用户分配（专用或浮动）
- vCenter Server 实例

前提条件

- 确认创建原始桌面池的前提条件仍然有效。
例如，对于包含完整虚拟机的池，确认准备了虚拟机模板。
对于链接克隆池，确认准备了父虚拟机并在关闭虚拟机后拍摄了快照。
在克隆池时，您可以使用相同的虚拟机模板或父虚拟机，也可以选择其他虚拟机模板或父虚拟机。
- 有关克隆自动完整克隆池的前提条件，请参阅[创建包含完整虚拟机的自动池](#)。
- 有关克隆链接克隆池的前提条件，请参阅[创建链接克隆桌面池](#)。

步骤

- 1 在 View Administrator 中，选择目录 > 桌面池。
- 2 选择要克隆的桌面池，然后单击**克隆**。
将显示**添加桌面池**向导。
- 3 在**添加桌面池**页上，键入唯一的池 ID。
- 4 在**置备设置**页上，为虚拟机提供唯一的名称。

选项	说明
使用一种命名模式	键入一种虚拟机命名模式。
手动指定名称	为虚拟机提供唯一的名称列表。

- 5 按照向导中的其他提示创建池。
根据需要，更改桌面池设置和值。

在 View Administrator 中，可以在将计算机添加到池时查看这些计算机，方法是选择目录 > 桌面池。

后续步骤

授予用户访问池的权限。请参阅[为桌面池或应用程序池添加授权](#)。

链接克隆桌面池的桌面池设置

配置包含由 View Composer 创建的链接克隆的自动池时，您必须指定计算机和桌面池设置。适用于专用用户分配池和浮动用户分配池的设置有所不同。

[表 5-2. 链接克隆桌面自动池的设置](#) 列出了适用于专用分配和浮动分配链接克隆池的设置。

有关每项设置的说明，请参阅[适用于所有桌面池类型的桌面池设置](#)。

表 5-2. 链接克隆桌面自动池的设置

设置	专用分配链接克隆池	浮动分配链接克隆池
状态	是	是
连接服务器限制	是	是
远程计算机电源策略	是	是
断开连接后自动注销	是	是
允许用户重置其计算机	是	是
允许用户从不同的客户端设备启动单独的会话		是
注销时删除或刷新计算机		是
注销后刷新操作系统磁盘	是	
默认显示协议	是	是
允许用户选择协议	是	是
3D 呈现器	是	是
显示器最大数量	是	是
任意一台显示器的最大分辨率	是	是
Adobe Flash 质量	是	是
Adobe Flash 调节	是	是
覆盖全局 Mirage 设置	是	是
Mirage 服务器配置	是	是

View Composer 对链接克隆 SID 和第三方应用程序的支持

在某些情形下，View Composer 可以为链接克隆虚拟机生成并保留本地计算机安全标识符 (SID)。View Composer 可保留第三方应用程序的全局唯一标识符 (GUID)，具体情况根据应用程序生成 GUID 的方式而定。

要了解 View Composer 操作如何影响 SID 和应用程序的 GUID，您应该了解如何创建和置备链接克隆计算机：

- 1 View Composer 通过以下操作创建链接克隆：
 - a 通过克隆父虚拟机快照创建副本。
 - b 创建可以将副本作为其父磁盘引用的链接克隆。
- 2 View Composer 和 View 使用 QuickPrep 或 Sysprep 自定义规范（具体取决于您在创建池时选择的自定义工具）对链接克隆进行自定义。
 - 如果您使用 Sysprep，系统将为每个克隆生成一个唯一 SID。
 - 如果您使用 QuickPrep，将不生成新的 SID。父虚拟机的 SID 将被复制到池中所有已置备的链接克隆计算机上。

- 某些应用程序会在自定义期间生成 GUID。

3 View 会为链接克隆创建快照。

该快照包含由 Sysprep 生成的唯一 SID，或者由 QuickPrep 生成的通用 SID。

4 View 会按照您在创建池时选择的设置打开计算机电源。

某些应用程序会在首次打开计算机电源时生成 GUID。

有关 QuickPrep 与 Sysprep 自定义的比较，请参阅[选择 QuickPrep 或 Sysprep 来自定义链接克隆计算机](#)。

当您刷新链接克隆时，View Composer 会使用快照将克隆还原到其初始状态。其 SID 会被保留。

如果您使用的是 QuickPrep，当重构链接克隆时，父虚拟机的 SID 将保留在链接克隆上（只要您为重构操作选择同一父虚拟机）。如果为重构操作选择不同的父虚拟机，新父虚拟机的 SID 将被复制到克隆上。

如果您使用的是 Sysprep，将始终在克隆上生成新的 SID。有关详细信息，请参阅[重构使用 Sysprep 自定义的链接克隆](#)。

表 5-3. View Composer 操作、链接克隆 SID，以及应用程序 GUID 显示了 View Composer 操作对链接克隆 SID 和第三方应用程序 GUID 的影响。

表 5-3. View Composer 操作、链接克隆 SID，以及应用程序 GUID

对 SID 或 GUID 的支持	克隆创建	刷新	重构
Sysprep: 为链接克隆生成唯一 SID	使用 Sysprep 自定义时，会为链接克隆生成唯一 SID。	保留唯一 SID。	不保留唯一 SID。
QuickPrep: 为链接克隆生成通用 SID	利用 QuickPrep 自定义，可为池中的所有克隆生成一个通用 SID。	保留通用 SID。	保留通用 SID。
第三方应用程序 GUID	每个应用程序都具有不同的行为。 注 Sysprep 和 QuickPrep 对 GUID 保留产生的影响相同。	如果应用程序在拍摄初始快照之前生成 GUID，将会保留 GUID。 如果应用程序在拍摄初始快照之后生成 GUID，则不会保留 GUID。	重构操作不会保留应用程序 GUID，除非应用程序将 GUID 写入被指定为 View Composer 永久磁盘的驱动器上。

选择 QuickPrep 或 Sysprep 来自定义链接克隆计算机

QuickPrep 和 Microsoft Sysprep 为自定义链接克隆计算机提供了不同的方式。QuickPrep 专为与 View Composer 协同高效工作而设计。Microsoft Sysprep 可提供标准的自定义工具。

创建链接克隆计算机时，您必须修改每个虚拟机，使其在网络中使用时具有唯一性。View 和 View Composer 提供两种对链接克隆计算机进行个性化设置的方法。

表 5-4. 比较 QuickPrep 和 Microsoft Sysprep 将 QuickPrep 和使用 Microsoft Sysprep 创建的自定义规范进行了比较。

表 5-4. 比较 QuickPrep 和 Microsoft Sysprep

QuickPrep	自定义规范 (Sysprep)
专为与 View Composer 配合使用而设计。 有关详细信息，请参阅 使用 QuickPrep 自定义链接克隆计算机 。	可以通过标准的 Microsoft Sysprep 工具创建。
为池中所有的链接克隆使用相同的本地计算机安全标识符 (Security Identifier, SID)。	为池中的每个链接克隆生成唯一的本地计算机 SID。
可以在关闭链接克隆之前，以及创建、刷新或重构链接克隆之后运行其他自定义脚本。	可以在用户首次登录时运行其他脚本。
将链接克隆计算机加入 Active Directory 域。	将链接克隆计算机加入 Active Directory 域。 不使用 Sysprep 自定义规范中的域和管理员信息。创建池时使用在 View Administrator 中输入的客户机自定义信息将虚拟机加入到域。
对于每个链接克隆，都要向 Active Directory 域帐户添加一个唯一 ID。	对于每个链接克隆，都要向 Active Directory 域帐户添加一个唯一 ID。
刷新链接克隆后不会生成新的 SID。通用 SID 将被保留。	自定义每个链接克隆时，均会生成一个新的 SID。在刷新操作过程中会保留唯一 SID，但在重构或重新平衡操作过程中不会保留。
重构链接克隆后不生成新的 SID。通用 SID 将被保留。	重构链接克隆后再次运行克隆，为虚拟机生成新的 SID。 有关详细信息，请参阅 重构使用 Sysprep 自定义的链接克隆 。
运行速度快于 Sysprep。	花费时间长于 QuickPrep。

使用 QuickPrep 或 Sysprep 自定义链接克隆池后，在池中创建或重构计算机时，无法切换到另一自定义方法。

使用 QuickPrep 自定义链接克隆计算机

您可以使用 QuickPrep 系统工具对通过父虚拟机创建的链接克隆计算机进行个性化设置。创建或重构链接克隆计算机时，View Composer 将执行 QuickPrep。

QuickPrep 通过以下几种方式自定义链接克隆计算机：

- 在您创建链接克隆池时为计算机指定一个名称。
- 在 Active Directory 中创建一个计算机帐户，将计算机添加到合适的域。
- 装载 View Composer 永久磁盘。Windows 用户配置文件将重定向到该磁盘。
- 将临时文件和页面文件重新定向到一个单独的磁盘。

这些步骤可能需要将链接克隆重新启动一次或多次。

QuickPrep 使用 KMS 批量许可证密钥激活 Windows 链接克隆计算机。有关详细信息，请参阅《View 管理指南》文档。

您可以自行创建脚本以进一步自定义链接克隆。QuickPrep 可以在预定义的时间运行两种类型的脚本：

- 在创建或重构链接克隆后
- 关闭链接克隆前

有关使用 QuickPrep 自定义脚本的指导原则和规则，请参阅[运行 QuickPrep 自定义脚本](#)。

注 View Composer 需要使用域用户凭据才能将链接克隆计算机加入 Active Directory 域。有关详细信息，请参阅《View 管理指南》文档。

运行 QuickPrep 自定义脚本

利用 QuickPrep 工具，可以创建用来自定义池中的链接克隆计算机的脚本。您可以将 QuickPrep 配置为在两个预定义的时间运行自定义脚本。

QuickPrep 脚本何时运行

同步后脚本会在创建、重构或重新平衡链接克隆后，且克隆的状态为**就绪**时运行。关机脚本在链接克隆关闭之前运行。这些脚本在链接克隆的客户机操作系统中运行。

QuickPrep 如何执行脚本

QuickPrep 进程使用 Windows CreateProcess API 调用来执行脚本。您的脚本可以调用任何 CreateProcess API 能够创建的进程。例如，cmd、vbscript、exe，以及可以和 API 协作的批文件进程。

特别是，QuickPrep 将为脚本指定的路径作为第二个参数传递到 CreateProcess API，并将第一个参数设置为 NULL。

例如，如果脚本路径为 c:\myscript.cmd，其在 View Composer 日志文件的函数中显示为第二个参数：CreateProcess(NULL,c:\myscript.cmd,...)。

提供 QuickPrep 脚本的路径

当您创建链接克隆计算机池或编辑池的客户机自定义设置时，需要提供 QuickPrep 自定义脚本的路径。这些脚本必须位于父虚拟机中。您不能使用指向网络共享位置的 UNC 路径。

如果您使用需要解释程序才能执行脚本的脚本语言，则脚本路径必须以解释程序二进制文件的路径为开头。

例如，如果您指定 C:\script\myvb.vbs 作为 QuickPrep 自定义脚本的路径，View Composer Agent 将无法执行该脚本。您必须指定一个以解释程序二进制文件路径开始的路径：

```
C:\windows\system32\cscript.exe c:\script\myvb.vbs
```

重要事项 防止普通用户访问 QuickPrep 自定义脚本。将脚本放在安全的文件夹中。

QuickPrep 脚本超时限制

View Composer 会终止运行时间超过 20 秒的同步后脚本或关机脚本。如果脚本运行时间会超过 20 秒，您可以延长超时限制。有关详细信息，请参阅[延长 ClonePrep 和 QuickPrep 自定义脚本的超时限制](#)。

或者，也可以使用您的脚本来启动其他执行长时间运行任务的脚本或进程。

QuickPrep 脚本帐户

QuickPrep 在配置运行 VMware View Composer 客户机代理服务器服务的帐户下运行脚本。默认情况下，此帐户为 Local System。

请勿更改这个登录帐户。如果您更改登录帐户，链接克隆将不会启动。

QuickPrep 进程特权

出于安全原因考虑，从调用 QuickPrep 自定义脚本的 View Composer Guest Agent 进程中删除了某些 Windows 操作系统特权。

QuickPrep 自定义脚本无法执行需要具有从 View Composer Guest Agent 进程中删除的特权才能执行的操作。

从调用 QuickPrep 脚本的进程中删除了以下特权：

```
SeCreateTokenPrivilege
SeTakeOwnershipPrivilege
SeSecurityPrivilege
SeSystemEnvironmentPrivilege
SeLoadDriverPrivilege
SeSystemtimePrivilege
SeUndockPrivilege
SeManageVolumePrivilege
SeLockMemoryPrivilege
SeIncreaseBasePriorityPrivilege
SeCreatePermanentPrivilege
SeDebugPrivilege
SeAuditPrivilege
```

QuickPrep 脚本日志

View Composer 日志中包含有关 QuickPrep 脚本的执行信息。日志中记录了执行的开始和结束时间以及输出或错误消息。日志位于 Windows temp 目录中：

C:\Windows\Temp\vmware-viewcomposer-ga-new.log

重构使用 Sysprep 自定义的链接克隆

如果要重构使用 Sysprep 自定义的链接克隆虚拟机，View 会在重构操作系统磁盘后再次运行 Sysprep 自定义规范。此操作将为链接克隆虚拟机生成一个新的 SID。

如果生成新的 SID，则重构的链接克隆将像网络中的新计算机一样运行。某些软件程序（如系统管理工具）会根据 SID 识别受其管理的计算机。这些程序可能无法识别或定位链接克隆虚拟机。

此外，如果系统磁盘上安装了第三方软件，那么在重构完成后，自定义规范可能会为该软件重新生成 GUID。

首次运行自定义规范之前，重构操作会将链接克隆恢复为其初始状态。在这种状态下，链接克隆不具有本地计算机 SID 或任何安装在系统驱动器中的第三方软件的 GUID。重构链接克隆后，View 必须运行 Sysprep 自定义规范。

在 View Composer 操作期间将链接克隆计算机保持已置备状态以在远程桌面会话中使用

如果用户必须能够随时访问远程桌面，则必须保持一定数量的已置备计算机以在远程桌面会话中使用，甚至在执行 View Composer 维护操作时也是如此。您可以设置在 View Composer 刷新、重构或重新平衡池中的链接克隆虚拟机时未处于维护模式的最小计算机数量。

在设置 **View Composer 维护操作期间就绪 (已置备) 计算机的最小数量** 时，View 确保在 View Composer 执行维护操作时将指定数量的计算机保持已置备状态，而不是置于维护模式。

通过使用该设置，用户可以在 View Composer 维护操作期间保持现有的连接或发送新的连接请求。该设置不区别准备接受新连接的备用计算机和已在现有桌面会话中连接的计算机。

在创建或编辑链接克隆池时，您可以指定该设置。

以下指导原则适用于该设置：

- 要允许多个用户保持现有的桌面连接并保留可接受新连接请求的最小数量的备用（已打开电源）计算机，请将 **View Composer 维护操作期间就绪 (已置备) 计算机的最小数量** 设置为足够大的值以包括两组计算机。
- 如果使用命名模式并按需置备计算机，请将 View Composer 操作期间的已置备计算机数设置为小于指定的 **计算机的最大数量** 值。如果超过最大值，则池中的总计算机数可能比要在 View Composer 操作期间保持已置备状态的最小计算机数量少。否则，View Composer 维护操作将无法进行。
- 如果手动指定一组计算机名称以置备计算机，请不要将池中的总计算机数缩减（通过移除计算机名称）为低于最小已置备计算机数量。否则，View Composer 维护操作将无法进行。
- 如果将最小已置备计算机数量设置为较大的值（相对于池大小），View Composer 维护操作可能需要更长的时间才能完成。虽然 View 在维护操作期间保留最小数量的已置备计算机，该操作可能不会达到 **最大并发 View Composer 维护操作数量** 设置中指定的并发限制。

例如，如果池包含 20 个计算机，已置备计算机的最小数量为 15 个，则 View Composer 每次最多可以在 5 个计算机上运行。如果 View Composer 维护操作的并发限制为 12，则将永远都达不到此并发限制。

- 在该设置中，术语“就绪”适用于链接克隆虚拟机的状态，而不适用于 View Administrator 中显示的计算机状态。当虚拟机已置备并且做好开启准备时，该虚拟机即处于就绪状态。计算机状态反映了计算机的 View 管理情况。例如，计算机可能具有已连接、已断开、无法访问代理、正在删除等状态，但仍将其视为“就绪”。

针对链接克隆使用现有的 Active Directory 计算机帐户

在创建或编辑桌面池或自动场时，您可以将 View Composer 配置为针对新置备的链接克隆使用 Active Directory 中的现有计算机帐户。

默认情况下，View Composer 将针对其置备的每一个链接克隆生成新的 Active Directory 计算机帐户。允许重新使用已存在的计算机帐户选项可通过确保 View Composer 使用现有的 AD 计算机帐户来允许您控制在 Active Directory 中创建的计算机帐户。

如果启用了该选项，在链接克隆置备完成后，View Composer 将检查现有的 AD 计算机帐户名称与链接克隆计算机名称是否匹配。如果匹配，View Composer 将使用现有的 AD 计算机帐户。如果 View Composer 未找到匹配的 AD 计算机帐户名称，View Composer 将为链接克隆生成新的 AD 计算机帐户。

在创建或编辑桌面池或自动场时，您可以设置**允许重新使用已存在的计算机帐户**选项。如果编辑池或场并设置了该选项，该设置将影响以后置备的链接克隆计算机。已置备的链接克隆不会受到影响。

在设置**允许重新使用已存在的计算机帐户**选项时，您可以限制分配给生成桌面池或场的 View Composer 用户帐户的 Active Directory 权限。仅需要以下 Active Directory 权限：

- 列出内容
- 读取全部属性
- 读取权限
- 重置密码

只有确定您想要置备的所有计算机在 Active Directory 中都已分配了现有计算机帐户，您才能限制 Active Directory 权限。如果没有发现匹配名称，View Composer 会生成一个新的 AD 计算机帐户。如果要创建新的计算机帐户，还必须具备其他权限（例如创建计算机对象）。有关创建 View Composer 用户帐户所需的完整权限列表，请参阅《View 管理指南》文档。

如果 View Composer 当前正在使用至少一个现有的 AD 计算机帐户，则该选项无法禁用。

以下过程适用于链接克隆桌面池。对于自动场，这些步骤是类似的。

前提条件

确认现有的计算机帐户位于您通过 **Active Directory 容器** 设置指定的 Active Directory 容器中。如果现有帐户位于其他容器中，则具备这些帐户名称的链接克隆的置备将会失败，并且显示错误消息，指出 Active Directory 中已经存在现有计算机帐户。

例如，如果您选择**允许重新使用已存在的计算机帐户**选项，并且指定 **Active Directory 容器** 为默认值，**CN=Computers**，并且现有计算机帐户位于 **OU=mydesktops**，则这些帐户的部署将会失败。

步骤

- 1 在 Active Directory 中，创建用于链接克隆计算机的计算机帐户。

例如，machine1、machine2、machine3。

计算机帐户名称必须使用连续整数，这样才能与 View 中在计算机置备过程中生成的名称相匹配。

- 2 在 View Administrator 中，使用“添加桌面池”向导创建池，或在“编辑”对话框中编辑池。
- 3 在“置备设置”页面或选项卡上，选择**使用命名模式**。
- 4 在**命名模式**文本框中，键入与 Active Directory 计算机帐户名称相匹配的计算机名称。

例如，machine。

View 向这些模式添加唯一的编号，从而为每个计算机提供唯一的名称。

例如，machine1、machine2、machine3。

- 5 在“客户机自定义”页面或选项卡上，选择**允许重新使用已存在的计算机帐户**选项。

创建即时克隆桌面池

要为用户提供对即时克隆桌面的访问权限，必须创建一个即时克隆桌面池。

本章讨论了以下主题：

- [即时克隆桌面池](#)
- [映像发布和重新平衡即时克隆桌面池](#)
- [添加即时克隆域管理员](#)
- [用于创建即时克隆桌面池的工作表](#)
- [创建即时克隆桌面池](#)
- [ClonePrep 客户机自定义](#)
- [即时克隆维护实用程序](#)

即时克隆桌面池

即时克隆桌面池是一个自动桌面池。vCenter Server 会根据您在创建池时指定的设置创建桌面虚拟机。

与 View Composer 链接克隆类似，即时克隆也会共享父虚拟机的虚拟磁盘，因此所占用的存储空间要比完整虚拟机少。此外，即时克隆还会共享父虚拟机的内存。即时克隆是使用 vmFork 技术创建的。即时克隆桌面池具有以下关键特征：

- 即时克隆的置备要比 View Composer 链接克隆快得多。
- 即时克隆在创建后始终处于电源打开状态，以方便用户连接。客户机自定义和 Active Directory 域加入操作会在初次打开电源工作流中完成。
- 用户注销后，桌面虚拟机会被删除。可以根据需要或预先按照置备策略创建新克隆。
- 通过推送映像操作，您可以从任何父虚拟机的任何快照重新创建池。您可以使用推送映像推出操作系统和应用程序修补程序。
- 创建克隆时，View 会选择一个可在数据存储之间实现克隆的最佳分配的数据存储。不需要手动重新平衡。
- View Storage Accelerator 会自动启用。
- 透明页面共享功能会自动启用。

由于 View 可以快速创建即时克隆，因此您无需预先置备桌面，也无需具有大量就绪桌面。与 View Composer 链接克隆相比，即时克隆可以简化管理大量桌面池的任务，同时还能减少所需的硬件资源数量。

即时克隆具有以下兼容性要求：

- vSphere 6.0 Update 1 或更高版本。
- 虚拟机硬件版本 11 或更高版本。

最佳做法是在 vSphere 环境中配置分布式虚拟交换机。

在 Horizon 7.0 中，即时克隆具有以下限制：

- 仅支持单用户桌面。不支持 RDS 主机。
- 仅支持浮动用户分配。用户会被随机分配池中的桌面。
- 即时克隆桌面不能具有永久磁盘。用户可以使用 VMware App Volumes 来存储永久数据。有关 App Volumes 的更多信息，请访问 <https://www.vmware.com/products/appvolumes>。
- 不支持虚拟卷和 VAAI (vStorage APIs for Array Integration) 本地 NFS 快照。
- Sysprep 不可用于桌面自定义。
- 支持 Windows 7 和 Windows 10，但不支持 Windows 8 或 Windows 8.1。
- 不支持 PowerCLI。
- 不支持本地数据存储。
- 不支持 IPv6。
- 即时克隆不能重用 Active Directory 中的现有计算机帐户。
- 无法使用用户配置管理。
- 无法使用 3D 呈现。
- 不能指定即时克隆维护操作期间就绪（已置备）计算机的最小数量。不需要此功能，因为快速创建即时克隆意味着即使在维护操作期间，某些桌面也始终可以使用。

不需要为 View Composer 链接克隆提供的磁盘空间回收功能，因为即时克隆会在用户注销时重新创建。对于即时克隆，回收虚拟机中未使用的磁盘空间不会对存储空间的占用产生显著影响。

映像发布和重新平衡即时克隆桌面池

即时克隆桌面池中的克隆均基于同一个映像。创建即时克隆时，系统会自动在数据存储之间重新平衡桌面池。

映像是父虚拟机的快照。创建即时克隆桌面池涉及以下几项操作：

- 1 **View** 发布您选择的映像。在 vCenter Server 中，如果 ClonePrepInternalTemplateFolder、ClonePrepParentVmFolder、ClonePrepReplicaVmFolder 和 ClonePrepResyncVmFolder 这四个文件夹不存在，将创建它们，并且还会创建克隆所需的一些内部虚拟机。在 View Administrator 中，您可以在桌面池的摘要选项卡上查看这项操作的进度。在发布过程中，“等待处理的映像”窗格将显示映像的名称和状态。

注 请不要篡改这四个文件夹或其中包含的内部虚拟机。否则，可能会出现错误。内部虚拟机在不再需要时会被移除。通常情况下，虚拟机会在删除池或推送映像操作后的 5 分钟内被移除。但是，有时移除操作可能需要长达 30 分钟。

- 2 创建克隆。此过程非常快速。通常情况下，不到 2 秒钟即可创建一个克隆。在此过程中，View Administrator 中的“当前映像”窗格将显示映像的名称和状态。

创建池后，您可以通过推送映像操作更改映像。请参阅《View 管理指南》文档中的“更改即时克隆桌面池的映像”。与创建池一样，将会首先发布新映像，然后再重新创建克隆。

如果编辑池以添加或移除数据存储，则在创建新克隆时，将自动重新平衡虚拟机。如果要提高重新平衡速度，请采取以下措施：

- 如果移除一个数据存储，请手动移除该数据存储上的桌面，以便在其余数据存储上创建新桌面。
- 如果添加一个数据存储，请从原来的数据存储中手动移除一些桌面，以便在新数据存储上创建新桌面。您也可以移除所有桌面或只是使用同一映像执行推送映像操作，以便当重新创建克隆时，这些克隆能够均匀地分布到数据存储中。

添加即时克隆域管理员

必须先向 View 中添加即时克隆域管理员，然后才能创建即时克隆桌面池。

即时克隆域管理员必须具有一定的 Active Directory 域特权。有关更多信息，请参阅《View 安装指南》文档中的“为即时克隆操作创建用户帐户”。

步骤

- 1 在 View Administrator 中，选择 **View 配置 > 即时克隆域管理员**。
- 2 单击**添加**。
- 3 输入即时克隆域管理员的登录名和密码。

用于创建即时克隆桌面池的工作表

创建即时克隆桌面池时，**添加桌面池**向导会提示您配置某些选项。您可以使用此工作表在创建池之前记录您的配置选项。

在创建即时克隆桌面池之前，需为父虚拟机拍摄快照。在拍摄快照之前必须关闭父虚拟机。此快照是克隆的基础映像。

注 您无法通过虚拟机模板创建即时克隆桌面池。

表 6-1. 工作表：用于创建即时克隆桌面池的配置选项

选项	说明	在此填写您要指定的值
用户分配	选择 浮动 。用户会被随机分配池中的桌面。	
vCenter Server	选择 即时克隆 ，然后选择管理即时克隆虚拟机的 vCenter Server。	
桌面池 ID	用于在 View Administrator 中标识池的唯一名称。 如果您有多个连接服务器配置，请确保不同的连接服务器配置不会使用相同的池 ID。连接服务器配置既可包含单个连接服务器，也可包含多个连接服务器	
显示名称	用户从客户端登录时所看到的池名称。如果您未指定名称，则使用池 ID。	
访问组	为池选择访问组，或者将池留在默认的根访问组中。 如果使用访问组，则可以将池的管理委托给某个具有特定角色的管理员。有关详细信息，请参阅《 View 管理指南 》文档中基于角色的委托管理章节。 注 访问组不同于存储桌面虚拟机的 vCenter Server 文件夹。您稍后会在向导中选择 vCenter Server 文件夹。	
状态	如果设置为 已启用 ，则表示池已经准备就绪，在置备后便可以使用。如果设置为 已禁用 ，则用户无法使用池。在置备期间，如果禁用池，置备会停止。	
连接服务器限制	您可以限制只有特定连接服务器才能访问池，方法是：单击 浏览 ，然后选择一个或多个连接服务器。 如果您想通过 VMware Identity Manager 提供桌面访问，并且配置了连接服务器限制，则当桌面实际受到限制时， VMware Identity Manager 应用程序可能会向用户显示这些桌面。 VMware Identity Manager 用户将无法启动这些桌面。	
断开连接后自动注销	<ul style="list-style-type: none"> ■ 立即。用户在断开连接时会被注销。 ■ 从不。永不注销用户。 ■ 之后。用户断开连接的时间超过此设置后即注销。键入持续时间（以分钟为单位）。 <p>注销时间适用于以后断开的连接。如果在设置注销时间时桌面会话已经断开，则该用户的注销持续时间以设置注销时间的时刻为起点，而不是会话最初断开的时刻。例如，如果您将此值设置为 5 分钟，而会话在 10 分钟前断开，View 将会在您设置完该值的 5 分钟后注销本次会话。</p>	
允许用户从不同的客户端设备启动单独的会话	选择该选项时，从不同的客户端设备连接到同一桌面池的用户将获取不同的桌面会话。用户只能从相同的客户端设备重新连接到现有会话。如果未选择该设置，则无论使用哪个客户端设备，用户都将始终重新连接到他们的现有会话。	
默认显示协议	选择默认显示协议。选项包括 Microsoft RDP 、 PCoIP 和 VMware Blast 。	
允许用户选择协议	指定用户能否选择除默认显示协议之外的其他显示协议。	

选项	说明	在此填写您要指定的值
HTML Access	<p>选择已启用以允许用户从 Web 浏览器连接到远程桌面。有关此功能的更多信息，请参阅《使用 HTML Access》（可从 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html 获得）。</p> <p>要将 HTML Access 与 VMware Identity Manager 配合使用，必须将连接服务器与 SAML 身份验证服务器进行配对，如《View 管理指南》文档中所述。必须安装并配置 VMware Identity Manager，才能与连接服务器一起使用。</p>	
Adobe Flash 质量	<p>选择网页上 Adobe Flash 内容的质量。</p> <ul style="list-style-type: none"> ■ 不进行控制：网页设置决定质量。 ■ 低。此设置占用最少的带宽量。如果未指定质量级别，则默认会使用此级别。 ■ 中。此设置占用中等的带宽量。 ■ 高。此设置占用最多的带宽量。 <p>有关更多信息，请参阅 Adobe Flash 质量和调节。</p>	
Adobe Flash 调节	<p>选择 Adobe Flash 影片的帧速率。如果启用此设置，您可以通过选择调节级别减少或增加每秒显示的帧数。</p> <ul style="list-style-type: none"> ■ 已禁用。不执行调节。 ■ 保守。计时器间隔为 100 毫秒。此设置可以使丢帧数达到最小。 ■ 适中。计时器间隔为 500 毫秒。 ■ 激进。计时器间隔为 2500 毫秒。此设置可以使丢帧数达到最大。 <p>有关更多信息，请参阅 Adobe Flash 质量和调节。</p>	
出现错误时停止置备	指定在出现错误时 View 是否停止置备桌面虚拟机，以及是否阻止错误影响多个虚拟机。	
命名模式	<p>指定 View 在所有桌面虚拟机名称中用作前缀的模式，其后跟有一个唯一编号。</p> <p>有关更多信息，请参阅自动桌面池使用命名模式。</p>	
计算机的最大数量	指定池中桌面虚拟机的总数。	
备用 (已打开电源) 计算机数量	指定保持用户可用的桌面虚拟机数量。有关详细信息，请参阅 手动命名计算机或提供命名模式 。	
按需置备计算机	指定在创建池时置备所有桌面虚拟机，还是根据需要置备虚拟机。	
计算机的最小数量	<ul style="list-style-type: none"> ■ 预先置备所有计算机。创建池时，View 会根据您在计算机的最大数量中指定的值，创建相应数量的虚拟机。 ■ 按需置备计算机。创建池时，View 会根据计算机的最小数量值或备用 (已打开电源) 计算机数量值（以较大者为准），创建相应数量的虚拟机。系统会额外创建一些虚拟机，以便在用户连接到桌面时保持有此最小数量的可用虚拟机。 	
预先置备所有计算机		
为副本磁盘和操作系统磁盘选择单独的数据存储	<p>指定是否在不同于即时克隆所在的数据存储上存储副本磁盘和操作系统磁盘。</p> <p>有关更多信息，请参阅将即时克隆和 View Composer 链接克隆的副本和克隆存储在不同的数据存储中。</p>	
父虚拟机	为池选择父虚拟机。	
快照 (默认映像)	选择要用作池的基础映像的父虚拟机快照。	
虚拟机文件夹位置	为桌面虚拟机选择 vCenter Server 中的文件夹。	
群集	为桌面虚拟机选择 vCenter Server 群集。	
资源池	为桌面虚拟机选择 vCenter Server 资源池。	

选项	说明	在此填写您要指定的值
数据存储	为桌面虚拟机选择一个或多个数据存储。 选择即时克隆数据存储 窗口提供了估算池的存储要求的高级指导原则。这些指导原则可帮助您确定哪些数据存储有足够大的空间来存储克隆。“存储过载”值始终设置为“无限制”，且无法进行配置。	
域	选择一个 Active Directory 域。下拉列表显示了您在配置即时克隆域管理员时指定的域。请参阅 添加即时克隆域管理员	
AD 容器	指定 Active Directory 容器的相对标识名。 例如: CN=Computers 在 添加桌面池 窗口中，您可以浏览容器的 Active Directory 树。	
关机脚本	指定在桌面虚拟机关闭前要在这些虚拟机上运行的脚本的路径名称以及脚本参数。	
同步后脚本	指定在创建桌面虚拟机后要在这些虚拟机上运行的脚本的路径名称以及脚本参数。	

创建即时克隆桌面池

添加桌面池向导可指导您完成创建即时克隆桌面池的步骤。

前提条件

- 确认即时克隆虚拟机连接的虚拟交换机具有足够的端口来支持预期的虚拟机数量。虚拟机上的每个网卡需要一个端口。
- 确认已准备好父虚拟机。有关更多信息，请参阅[第 3 章 为克隆创建并准备父虚拟机](#)。
- 收集池的配置信息。请参阅[用于创建即时克隆桌面池的工作表](#)。
- 确认已在 **View Administrator** 中添加即时克隆域管理员。请参阅[添加即时克隆域管理员](#)。

步骤

- 1 在 **View Administrator** 中，选择**目录 > 桌面池**。
- 2 单击**添加**。
- 3 选择**自动桌面池**。
- 4 在 **vCenter Server** 页面上，选择**即时克隆**。
- 5 按照提示创建池。

使用您在工作表中收集的配置信息。您可以通过在导航窗格中单击页面名称，直接返回至任意向导页面。

在 **View Administrator** 中，可以在将桌面虚拟机添加到池时查看这些桌面虚拟机，方法是选择**目录 > 桌面池**。

创建池后，只要该池存在，就不要删除父虚拟机或将其从 **vCenter Server** 清单中移除。如果您由于误操作将虚拟机从 **vCenter Server** 清单中移除，必须将其添加回去，然后使用当前映像执行一次推送映像操作。

后续步骤

授予用户访问池的权限。请参阅[为桌面池或应用程序池添加授权](#)。

ClonePrep 客户机自定义

ClonePrep 可在创建过程中对即时克隆进行自定义。

ClonePrep 可确保所有即时克隆全部加入 Active Directory 域。这些克隆具有与父虚拟机相同的计算机安全标识符 (Security Identifier, SID)。ClonePrep 还会保留应用程序的全局唯一标识符 (Globally Unique Identifier, GUID)，不过某些应用程序可能会在自定义期间生成一个新的 GUID。

添加即时克隆桌面池时，您可以指定一个在创建克隆后立即运行的脚本，以及另外一个在克隆关闭电源之前运行的脚本。

ClonePrep 如何运行脚本

ClonePrep 使用 Windows CreateProcess API 来运行脚本。您的脚本可以调用任何可通过 CreateProcess API 创建的进程。例如，cmd、vbscript、exe 和批处理文件进程可与此 API 配合使用。

特别是，ClonePrep 会将脚本的路径作为第二个参数传递到 CreateProcess API，并将第一个参数设置为 NULL。例如，如果脚本路径为 c:\myscript.cmd，则对 CreateProcess 的调用为 CreateProcess(NULL, c:\myscript.cmd, ...)。

提供 ClonePrep 脚本的路径

在创建或编辑桌面池时，您可以指定脚本。这些脚本必须位于父虚拟机中。您不能使用指向网络共享位置的 UNC 路径。

如果您使用需要解释程序才能运行脚本的脚本语言，则脚本路径必须以解释程序的可执行文件开头。例如，必须指定 C:\windows\system32\cmd.exe c:\script\myvb.vbs，而不是指定 C:\script\myvb.vbs。

重要事项 请将 ClonePrep 自定义脚本放置在安全的文件夹中，以防止进行未授权的访问。

ClonePrep 脚本超时限制

默认情况下，如果脚本执行时间超过 20 秒，ClonePrep 便会终止脚本。您可以增加此超时限制。有关详细信息，请参阅[延长 ClonePrep 和 QuickPrep 自定义脚本的超时限制](#)。

或者，您也可以指定一个脚本来运行其他运行时间较长的脚本或进程。

ClonePrep 脚本帐户

ClonePrep 用来运行脚本的帐户与 VMware Horizon Instant Clone Agent 服务所使用的帐户相同。默认情况下，此帐户为 Local System。请勿更改这个登录帐户。否则，克隆将无法启动。

ClonePrep 进程特权

出于安全原因考虑，从运行 ClonePrep 自定义脚本的 VMware Horizon Instant Clone Agent 进程中移除了某些 Windows 操作系统特权。脚本将无法执行需要这些特权的操作。

运行 ClonePrep 脚本的进程没有以下特权：

- SeCreateTokenPrivilege
- SeTakeOwnershipPrivilege
- SeSecurityPrivilege
- SeSystemEnvironmentPrivilege
- SeLoadDriverPrivilege
- SeSystemtimePrivilege
- SeUndockPrivilege
- SeManageVolumePrivilege
- SeLockMemoryPrivilege
- SeIncreaseBasePriorityPrivilege
- SeCreatePermanentPrivilege
- SeDebugPrivilege
- SeAuditPrivilege

ClonePrep 脚本日志

ClonePrep 会将消息写入日志文件。该日志文件为 C:\Windows\Temp\vmware-viewcomposer-ga-new.log。

即时克隆维护实用程序

连接服务器上有两个实用程序可用于维护 vCenter Server 中的即时克隆虚拟机以及这些虚拟机所在的群集。

这些实用程序为 IcMaint.cmd 和 IcUnprotect.cmd，位于 C:\Program Files\VMware\VMware View\Server\tools\bin 下。

IcMaint.cmd

此命令可删除父虚拟机，并且可以选择将主机置于维护模式。执行维护后，您可以运行以下命令，使主机退出维护模式。

语法：

```
IcMaint.cmd  
-vc
```

```
hostname_or_IP_address
-uid
user_ID
-password
password
-hostName
ESXi_hostname
-maintenance
ON|OFF
```

参数:

- *-vc host name or IP address of vCenter Server*
- *-uid vCenter Server user ID*
- *-password vCenter Server user password*
- *-hostname ESXi host name*
- *-maintenance ON|OFF*

此参数指定在删除父虚拟机后，是否进入维护模式。如果主机已经处于维护模式，*-maintenanceOFF* 可使主机退出维护模式。

所有参数均是必需参数。

IcUnprotect.cmd

此实用程序可对 ClonePrep 创建的文件夹和虚拟机取消保护。ClonePrep 是可在创建过程中对即时克隆进行自定义的机制。

语法:

```
IcUnprotect.cmd
-vc
hostname_or_IP_address
-uid
user_ID
-password
password [-clusterIdcluster_ID] [-includeFolders]
```

参数:

- *-vc host name or IP address of vCenter Server*
- *-uid vCenter Server user ID*
- *-password vCenter Server user password*
- *-clusterId cluster ID*
- *-includeFolders*

此参数可在对虚拟机取消保护的同时，也对文件夹取消保护。

除 **clusterId** 和 **includeFolders** 之外，其他所有参数都是必需参数。如果未指定 **clusterId**，则会对所有数据中心内的全部 **ClonePrep** 虚拟机取消保护。

创建手动桌面池

在手动桌面池中，最终用户访问的每个远程桌面都是一个单独的计算机。创建手动桌面池时，需要选择现有的计算机。您可以通过创建手动桌面池并选择一个计算机来创建包含单一桌面的池。

本章讨论了以下主题：

- [手动桌面池](#)
- [用于创建手动桌面池的工作表](#)
- [创建手动桌面池](#)
- [创建包含一个虚拟机的手动池](#)
- [手动池的桌面池设置](#)

手动桌面池

为了创建手动桌面池，View 会使用现有计算机置备桌面。您要为池中的每个桌面选择一个单独的计算机。

View 可以在手动池中使用几种类型的计算机：

- vCenter Server 管理的虚拟机
- 在不同于 vCenter Server 的虚拟化平台上运行的虚拟机
- 物理机

有关创建使用 Linux 虚拟机的手动桌面池的信息，请参阅《《设置 Horizon 7 for Linux 桌面》》指南。

用于创建手动桌面池的工作表

当您创建手动桌面池时，View Administrator 的**添加桌面池**向导会提示您配置特定选项。您可以使用此工作表在创建池之前准备配置选项。

您可以打印此工作表，并记下您要在运行**添加桌面池**向导时指定的值。

注 在手动池中，您必须对每台计算机完成准备工作，才能实现远程桌面访问。必须在每台计算机上安装并运行 Horizon Agent。

表 7-1. 工作表：用于创建手动桌面池的配置选项

选项	说明	在此填写您要指定的值
用户分配	<p>选择用户分配类型：</p> <ul style="list-style-type: none"> ■ 在专用分配池中，每个用户会分配给一台计算机。用户每次登录时接收到的都是同一台计算机。 ■ 在浮动分配池中，用户每次登录时都会接收到不同的计算机。 <p>有关详细信息，请参阅桌面池中的用户分配。</p>	
vCenter Server	<p>用来管理计算机的 vCenter Server。</p> <p>仅当计算机是受 vCenter Server 管理的虚拟机时，才会显示此选项。</p>	
计算机源	<p>要包含在桌面池中的虚拟机或物理机。</p> <ol style="list-style-type: none"> 1 确定要使用的计算机类型。可以使用受 vCenter Server 管理的虚拟机，也可以使用未受管的虚拟机和物理机。 2 准备好要包含在桌面池中的 vCenter Server 虚拟机或未受管虚拟机和物理机的列表。 3 在要包含在桌面池中的每台计算机上安装 Horizon Agent。 <p>要在未受管的虚拟机或物理机上使用 PCoIP，必须使用 Teradici 硬件。</p> <p>注 在 View Administrator 中启用 Windows Server 桌面后，View Administrator 会显示作为潜在计算机源的所有可用的 Windows Server 计算机，包括安装了 View 连接服务器和其他 View 服务器的计算机。</p> <p>如果计算机上已安装 View Server 软件，则无法为桌面池选择计算机。Horizon Agent 不能与任何其他 View 软件组件（包括 View 连接服务器、安全服务器、View Composer 或 Horizon Client）共存于同一台虚拟机或物理机上。</p>	
桌面池 ID	<p>用户登录时看到的池名称，用于在 View Administrator 中标识池。</p> <p>如果您的环境中正在运行多个 vCenter Server，应确保其他 vCenter Server 没有使用同一个池 ID。</p>	

选项	说明	在此填写您要指定的值
桌面池设置	<p>这些设置用于确定计算机状态、虚拟机处于未使用状态时的电源状态、显示协议、Adobe Flash 质量等。</p> <p>有关详细信息，请参阅适用于所有桌面池类型的桌面池设置。</p> <p>有关适用于手动池的设置列表，请参阅手动池的桌面池设置。</p>	
透明页面共享范围	<p>选择允许透明页面共享 (TPS) 的级别。选项包括：虚拟机（默认）、池、容器或全局。如果在池、容器或全局级别为所有计算机打开 TPS，ESXi 主机将消除因这些计算机使用同一客户机操作系统或应用程序而产生的内存冗余副本。</p> <p>页面共享发生在 ESXi 主机上。例如，如果在池级别启用 TPS，但池分散到多个 ESXi 主机，则只有同一主机和同一池中的虚拟机将共享页面。在全局级别，同一 ESXi 主机上所有受 View 管理的计算机都可以共享内存页，而不管这些计算机驻留在哪个池中。</p> <p>注 默认设置是不在计算机之间共享内存页，因为 TPS 可能会带来安全风险。调查表明可能会在非常有限的配置场景下滥用 TPS 来获取对数据的未授权访问。</p>	

创建手动桌面池

可以创建从现有虚拟机或物理计算机置备桌面的手动桌面池。必须选择要包含在桌面池中的计算机。

对于包含由 vCenter Server 管理的虚拟机的手动池，View 应确保有一个备用计算机已打开电源，以使用户能够与其连接。无论哪个电源策略有效，备用计算机都会打开电源。

前提条件

- 准备用于进行远程桌面访问的计算机。在手动池中，必须单独准备每台计算机。必须在每台计算机上安装并运行 Horizon Agent。
 - 要准备受 vCenter Server 管理的虚拟机，请参阅[第 3 章 为克隆创建并准备父虚拟机](#)。
 - 要准备未受管虚拟机和物理计算机，请参阅[第 2 章 准备未受管的计算机](#)。
- 收集您在创建池时必须提供的配置信息。请参阅[用于创建手动桌面池的工作表](#)。
- 确定如何配置电源设置、显示协议、**Adobe Flash** 质量及其他设置。请参阅[适用于所有桌面池类型的桌面池设置](#)。

步骤

- 1 在 View Administrator 中，选择目录 > 桌面池。
- 2 单击添加。
- 3 选择手动桌面池。

4 按照向导中的提示创建池。

使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，您可以直接返回至已完成的任意向导页面。

在 View Administrator 中，可以在将计算机添加到池时查看这些计算机，方法是选择目录 > 桌面池。

后续步骤

授予用户访问池的权限。请参阅[为桌面池或应用程序池添加授权](#)。

创建包含一个虚拟机的手动池

当用户需要一个唯一的专用桌面，或者多个用户需要在不同时间访问某个使用单一主机许可证的高成本应用程序时，您可以创建一个包含单个虚拟机的池。

通过创建手动桌面池并选择单个虚拟机，您可以将单个虚拟机置备在其专有的池中。

要模拟可由多个用户共享的物理机，可为具有池访问授权的用户指定浮动分配。

无论您使用专用分配还是浮动分配来配置单个虚拟机池，电源操作均由会话管理启动。虚拟机在用户请求桌面时开机，并在用户注销时关机或挂起。

如果您配置**确保计算机始终打开电源**策略，虚拟机将保持打开电源状态。如果用户关闭虚拟机，它将立即重新启动。

前提条件

- 准备虚拟机以交付远程桌面访问。必须在该虚拟机上安装并运行 Horizon Agent。
要准备由 vCenter Server 管理的虚拟机，请参阅[第 3 章 为克隆创建并准备父虚拟机](#)。
要准备未受管的虚拟机或物理机，请参阅[第 2 章 准备未受管的计算机](#)。
- 收集您在创建手动池时必须提供的配置信息。请参阅[用于创建手动桌面池的工作表](#)。
- 确定如何配置电源设置、显示协议、Adobe Flash 质量及其他设置。请参阅[适用于所有桌面池类型的桌面池设置](#)。

步骤

- 1 在 View Administrator 中，选择目录 > 桌面池。
- 2 单击添加。
- 3 选择手动桌面池。
- 4 选择用户分配类型。

选项	说明
专用	虚拟机分配给一个用户。只有该用户才可以登录此桌面。
浮动	虚拟机由具有池授权的所有用户共享。只要没有用户正在使用，任何得到授权的用户均可以登录此桌面。

- 5 在“虚拟机源”页面上，选择要包含在桌面池中的虚拟机。
- 6 按照向导中的提示创建池。

使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，您可以直接返回至已完成的任意向导页面。

在 View Administrator 中，您可以通过选择**目录 > 桌面池**查看要添加到池中的虚拟机。

后续步骤

授予用户访问池的权限。请参阅[为桌面池或应用程序池添加授权](#)。

手动池的桌面池设置

配置手动桌面池时，您必须指定计算机和池的设置。并非所有设置都适用于所有类型的手动池。

[表 7-2. 手动桌面池的设置](#) 列出了适用于通过以下属性配置的手动桌面池的设置：

- 专用用户分配
- 浮动用户分配
- 受管的计算机（vCenter Server 虚拟机）
- 未受管的计算机

这些设置也适用于包含单个计算机的手动池。

有关每种桌面池设置的描述，请参阅[适用于所有桌面池类型的桌面池设置](#)。

表 7-2. 手动桌面池的设置

设置	受管的专用分配 手动池	受管的浮动分配手动池	未受管的专用分配手动池	未受管的浮动分配手动池
状态	是	是	是	是
连接服务器限制	是	是	是	是
远程计算机电源策略	是	是		
断开连接后自动注销	是	是	是	是
允许用户重置其计算机	是	是		
允许用户从不同的客户端设备启动单独的会话		是		是
默认显示协议	是	是	是 要在不受 vCenter Server 管理的计算机中使用 PCoIP，您必须在该计算机上安装 Teradici 硬件。	是 要在不受 vCenter Server 管理的计算机中使用 PCoIP，您必须在该计算机上安装 Teradici 硬件。
允许用户选择协议	是	是	是	是

设置	受管的专用分配 手动池	受管的浮动分配手动池	未受管的专用分配手动池	未受管的浮动分配手动池
3D 呈现器	是	是		
显示器最大数量	是	是		
任意一台显示器的 最大分辨率	是	是		
Adobe Flash 质量	是	是	是	是
Adobe Flash 调节	是	是	是	是
覆盖全局 Mirage 设置	是	是	是	是
Mirage 服务器配置	是	是	是	是

设置远程桌面服务主机

Microsoft 远程桌面服务 (RDS) 主机提供了桌面会话和应用程序，用户可以从客户端设备进行访问。如果您打算创建 RDS 桌面池或应用程序池，必须先设置 RDS 主机。

本章讨论了以下主题：

- 远程桌面服务主机
- 在 Windows Server 2008 R2 上安装远程桌面服务
- 在 Windows Server 2012 或 2012 R2 上安装远程桌面服务
- 在 Windows Server 2008 R2 上安装桌面体验
- 在 Windows Server 2012 或 2012 R2 上安装桌面体验
- 限制用户只能进行单个会话
- 在远程桌面服务主机上安装 Horizon Agent
- 从嵌套会话内启动的远程应用程序打印
- 为 RDS 桌面和应用程序会话启用时区重定向
- 为应用程序启用基本的 Windows 主题
- 配置组策略以启动 Runonce.exe
- RDS 主机性能选项
- 为 RDS 主机配置 3D 图形

远程桌面服务主机

RDS 主机是托管应用程序和桌面会话以供远程访问的服务器计算机。RDS 主机可以是虚拟机或物理服务器。

RDS 主机已经安装了 Microsoft 远程桌面服务角色、Microsoft 远程桌面会话主机服务和 Horizon Agent。远程桌面服务以前称为终端服务。远程桌面会话主机服务允许服务器托管应用程序和远程桌面会话。在 RDS 主机上安装 Horizon Agent 后，用户可以使用 PCoIP 或 Blast Extreme 显示协议连接到应用程序和桌面会话。这两种协议都能提供远程内容（包括图像、音频和视频）交付的最佳用户体验。

RDS 主机的性能取决于多个因素。有关如何调整不同 Windows Server 版本的性能的信息，请参阅 <http://msdn.microsoft.com/library/windows/hardware/gg463392.aspx>。

Horizon 7 支持每个用户在 RDS 主机上最多进行一个桌面会话和一个应用程序会话。

用户同时从位于同一 RDS 主机上的 RDS 桌面或应用程序中提交打印作业时，RDS 主机上的 ThinPrint 服务器将串行处理打印请求，而不是并行处理。这会导致某些用户提交的打印作业发生延迟。请注意，打印服务器不会等待打印作业完成后才处理下一个打印作业。已发送至不同打印机的打印作业将并行打印。

如果用户同时启动应用程序和 RDS 桌面，并且两者都位于同一 RDS 主机上，则它们会共享相同的用户配置文件。如果用户从桌面启动一个应用程序，可能会在两个应用程序都尝试访问或修改用户配置文件的相同部分时出现冲突，且其中一个应用程序可能会无法正常运行。

设置应用程序或 RDS 桌面以进行远程访问的过程涉及以下任务：

- 1 设置 RDS 主机。
- 2 创建场。请参阅第 9 章 创建场。
- 3 创建应用程序池或 RDS 桌面池。请参阅第 10 章 创建应用程序池或第 11 章 创建 RDS 桌面池。
- 4 授权用户和组。请参阅第 13 章 授权用户和组。
- 5 （可选）为 RDS 桌面和应用程序会话启用时区重定向。请参阅为 RDS 桌面和应用程序会话启用时区重定向。

注 如果启用智能卡身份验证，请确保在 RDS 主机上禁用智能卡服务。否则，身份验证可能失败。此服务默认处于禁用状态。

小心 用户启动某个应用程序（例如，Web 浏览器）时，可能会获得对托管该应用程序的 RDS 主机上的本地驱动器的访问权限。如果应用程序提供的功能可使 Windows 资源管理器运行，则会发生此情况。要防止对 RDS 主机的此种类型访问，请遵循 <http://support.microsoft.com/kb/179221> 中所述的过程，以防止应用程序运行 Windows 资源管理器。

由于 <http://support.microsoft.com/kb/179221> 中介绍的过程影响桌面和应用程序会话，因此，当您计划遵循 Microsoft 知识库文章中的过程时，不建议创建 RDS 桌面池和应用程序池，以便不影响桌面会话。

安装应用程序

如果您计划创建应用程序池，则必须在 RDS 主机上安装应用程序。如果您希望 Horizon 7 自动显示已安装应用程序的列表，则必须安装应用程序，以使其可供所有用户在开始菜单中使用。创建应用程序池之前，您可以随时安装应用程序。如果您计划手动指定应用程序，则可以随时安装应用程序，创建应用程序池之前或之后均可。

重要事项 安装应用程序时，必须将其安装在场内的所有 RDS 主机上，而且安装在每个 RDS 主机的同一位置中。如果您未这样做，View Administrator 控制板将显示运行状况警告。在此类情况下，如果您创建应用程序池，用户在试图运行应用程序时则可能遇到错误。

当您创建应用程序池时，Horizon 7 会自动显示可供所有用户（而非个别用户）在场内所有 RDS 主机上的开始菜单中使用的应用程序。您可以从该列表选择任何应用程序。此外，您还可以手动指定不可供所有用户在开始菜单中使用的应用程序。可以安装在 RDS 主机上的应用程序无数量限制。

在 Windows Server 2008 R2 上安装远程桌面服务

远程桌面服务 (RDS) 是 Windows Server 可以具有的角色之一。您必须安装此角色才能设置运行 Windows Server 2008 R2 的 RDS 主机。

前提条件

- 确认 RDS 主机正在运行 Windows Server 2008 R2 Service Pack 1 (SP1)。
- 确认 RDS 主机是 Horizon 7 部署的 Active Directory 域的一部分。
- 安装 <http://support.microsoft.com/kb/2775511> 中记录的 Microsoft 修补程序汇总。
- 安装 Microsoft 更新 <https://support.microsoft.com/en-us/kb/2973201>。

步骤

- 1 以管理员身份登录 RDS 主机。
- 2 启动服务器管理器。
- 3 在导航树中选择角色。
- 4 单击添加角色启动添加角色向导。
- 5 选择远程桌面服务角色。
- 6 在“选择角色服务”页面上，选择远程桌面会话主机。
- 7 在“指定身份验证方法”页面上，选择需要网络级别身份验证或不需要网络级别身份验证（以适当者为准）。
- 8 在“配置客户端体验”页面上，选择要提供给用户的功能。
- 9 按照提示完成安装。

后续步骤

如果计划使用 HTML Access 或扫描仪重定向，则安装桌面体验功能。在 Windows Server 2008 R2 和 Windows Server 2012 或 2012 R2 上安装桌面体验的步骤有所不同。

将用户限制到单个桌面会话。请参阅[限制用户只能进行单个会话](#)。

在 Windows Server 2012 或 2012 R2 上安装远程桌面服务

“远程桌面服务”是 Windows Server 2012 或 2012 R2 可以具有的角色之一。您必须安装此角色才能设置 RDS 主机。

前提条件

- 确认 RDS 主机正在运行 Windows Server 2012 或 Windows Server 2012 R2。
- 确认 RDS 主机是 Horizon 7 部署的 Active Directory 域的一部分。

步骤

- 1 以管理员身份登录 RDS 主机。
- 2 启动服务器管理器。
- 3 选择**添加角色和功能**。
- 4 在“选择安装类型”页面上，选择**基于角色或基于功能的安装**。
- 5 在“选择目标服务器”页面上，选择一个服务器。
- 6 在“选择服务器角色”页面上，选择**远程桌面服务**。
- 7 在“选择功能”页面上，接受默认值。
- 8 在“选择角色服务”页面上，选择**远程桌面会话主机**。
- 9 按照提示完成安装。

后续步骤

如果计划使用 HTML Access 或扫描仪重定向，则安装桌面体验功能。在 Windows Server 2008 R2 和 Windows Server 2012 或 2012 R2 上安装桌面体验的步骤有所不同。

将用户限制到单个桌面会话。请参阅[限制用户只能进行单个会话](#)。

在 Windows Server 2008 R2 上安装桌面体验

对于 RDS 桌面和应用程序以及在运行 Windows Server 的单用户虚拟机上部署的 VDI 桌面，扫描仪重定向需要您在 RDS 主机和单用户虚拟机中安装桌面体验功能。

步骤

- 1 以管理员身份登录。
- 2 启动服务器管理器。
- 3 单击**功能**。
- 4 单击**添加功能**。
- 5 在“选择功能”页面上，选中**桌面体验**复选框。
- 6 查看有关桌面体验功能所需的其他功能的信息，然后单击**添加必需的功能**。
- 7 按照提示完成安装。

在 Windows Server 2012 或 2012 R2 上安装桌面体验

对于 RDS 桌面和应用程序以及在运行 Windows Server 的单用户虚拟机上部署的 VDI 桌面，扫描仪重定向需要您在 RDS 主机和单用户虚拟机中安装桌面体验功能。

在用作 RDS 主机的计算机上支持 Windows Server 2012 和 Windows Server 2012 R2。在单用户虚拟机上支持 Windows Server 2012 R2。

步骤

- 1 以管理员身份登录。
- 2 启动服务器管理器。
- 3 选择**添加角色和功能**。
- 4 在“选择安装类型”页面上，选择**基于角色或基于功能的安装**。
- 5 在“选择目标服务器”页面上，选择一个服务器。
- 6 在“选择服务器角色”页面上，接受默认选择并单击**下一步**。
- 7 在“选择功能”页面上的**用户界面和基础架构**下，选择**桌面体验**。
- 8 按照提示完成安装。

限制用户只能进行单个会话

Horizon 7 支持每个用户在 RDS 主机上最多进行一个桌面会话和一个应用程序会话。您必须配置 RDS 主机来限制用户只能进行单个会话。对于 Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2，您可以通过启用组策略设置

`Restrict Remote Desktop Services users to a single Remote Desktop Services session` 限制用户只能进行单个会话。此设置位于文件夹 `Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections` 中。对于 Windows Server 2008 R2，您还可以使用以下步骤限制用户只能进行单个会话。

前提条件

- 按照在 [Windows Server 2008 R2 上安装远程桌面服务](#) 中所述安装远程桌面服务角色。

步骤

- 1 单击 **开始 > 管理工具 > 远程桌面服务 > 远程桌面会话主机配置**。
- 2 在“编辑设置”窗格的“常规”下，双击**限制每个用户只能进行一个会话**。
- 3 在“属性”对话框的“常规”选项卡上，选择**限制每个用户只能进行一个会话**，然后单击**确定**。

后续步骤

在 RDS 主机上安装 Horizon Agent。请参阅在[远程桌面服务主机上安装 Horizon Agent](#)。

在远程桌面服务主机上安装 Horizon Agent

Horizon Agent 可与连接服务器通信，并支持 PCoIP 和 Blast Extreme 显示协议。您必须在 RDS 主机上安装 Horizon Agent。

前提条件

- 按照在 [Windows Server 2008 R2 上安装远程桌面服务](#) 或在 [Windows Server 2012 或 2012 R2 上安装远程桌面服务](#) 中所述安装远程桌面服务角色。

- 将用户限制到单个桌面会话。请参阅[限制用户只能进行单个会话](#)。
- 熟悉 Horizon Agent 自定义安装选项。请参阅[适用于 RDS 主机的 Horizon Agent 自定义安装选项](#)。
- 如果计算机安装了 Microsoft Visual C++ Redistributable 软件包，请确认软件包的版本为 2005 SP1 或更高版本。如果软件包的版本为 2005 或更低版本，可以升级或卸载该软件包。
- 从 VMware 产品页面 <http://www.vmware.com/go/downloadview> 下载 Horizon Agent 安装程序文件。

步骤

- 1 以管理员身份登录。

- 2 要启动 Horizon Agent 安装程序，请双击安装程序文件。

安装程序文件名为 `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`，其中 `y.y.y` 为版本号，`xxxxxx` 为内部版本号。

- 3 选择 Internet 协议 (IP) 版本 (IPv4 或 IPv6)。

必须使用同一 IP 版本安装所有 View 组件。

- 4 选择自定义安装选项。

如果在将位于手动场中的 RDS 主机上安装 Horizon Agent，请不要选择 View Composer Agent 选项。

- 5 在**服务器**文本框中，键入连接服务器主机的主机名或 IP 地址。

在安装过程中，安装程序会在该连接服务器实例上注册 RDS 主机。注册后，指定的连接服务器实例以及同一连接服务器组中的任何其他实例，都可以与该 RDS 主机进行通信。

- 6 选择一个身份验证方法以便在连接服务器实例上注册 RDS 主机。

选项	说明
Authenticate as the currently logged in user (作为当前登录的用户进行身份验证)	用户名和密码文本框会被禁用，您将通过当前用户名和密码登录到连接服务器实例。
指定管理员凭据	您必须在 用户名 和 密码 文本框中提供连接服务器管理员的用户名和密码。

用户帐户必须是有权访问 View 连接服务器实例上 View LDAP 的域用户。本地用户不适用。

- 7 按照提示完成安装。

后续步骤

创建场。请参阅[第 9 章 创建场](#)。

适用于 RDS 主机的 Horizon Agent 自定义安装选项

在 RDS 主机上安装 Horizon Agent 时，您可以选择自定义安装选项。此外，Horizon Agent 还会在支持某些功能的所有客户机操作系统上自动安装这些功能。这些功能并非可选。

要在安装最新的 Horizon Agent 版本后更改自定义安装选项，您必须卸载并重新安装 Horizon Agent。对于修补程序和升级，您可以运行新的 Horizon Agent 安装程序并选择一组新的选项，而无需卸载以前的版本。

表 8-1. IPv4 环境中适用于 RDS 主机的 Horizon Agent 自定义安装选项

选项	说明
USB 重定向	<p>授予用户访问本地连接的 USB 存储设备的权限。</p> <p>具体来说，RDS 桌面和应用程序中支持 USB 闪存驱动器和硬盘的重定向。RDS 桌面和应用程序中不支持其他类型的 USB 设备及其他类型的 USB 存储设备（如安全存储驱动器和 USB CD-ROM）的重定向。</p> <p>默认情况下，不会选择该安装选项。必须选择此选项才会进行安装。该选项在运行 Windows Server 2012 或 2012 R2 的 RDS 主机上可用，但在运行 Windows Server 2008 R2 的主机上不可用。</p> <p>有关安全地使用 USB 重定向的指导，请参阅《View 安全指南》指南。例如，可以使用组策略设置针对特定用户禁用 USB 重定向。</p>
HTML Access	<p>允许用户使用 HTML Access 连接到 RDS 桌面和应用程序。选择此安装选项时，将安装 HTML Access Agent。必须在 RDS 主机上安装此代理才能允许用户与 HTML Access 建立连接。</p>
3D RDSH	<p>为在该 RDS 主机上运行的应用程序提供 3D 图形支持。</p>
View Composer Agent	<p>如果该计算机是用于创建自动场的父虚拟机，请选择该选项。如果该计算机是手动场中的 RDS 主机，请不要选择该选项。</p>
客户端驱动器重定向	<p>允许 Horizon Client 用户与其 RDS 桌面和应用程序共享本地驱动器。</p> <p>安装此安装选项之后，无需在 RDS 主机上进行进一步配置。</p> <p>在单用户虚拟机和非受管计算机中运行的 VDI 桌面上也支持客户端驱动器重定向。</p>
虚拟打印	<p>允许用户通过其客户端计算机上可用的任意打印机进行打印。用户不需要在其桌面上另外安装驱动程序。</p> <p>以下远程桌面和应用程序支持虚拟打印：</p> <ul style="list-style-type: none"> ■ 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 主机上部署的桌面，其中 RDS 主机为虚拟机。 ■ 远程应用程序。 ■ 从远程桌面内的 Horizon Client 启动的远程应用程序（嵌套会话）。 <p>虚拟打印功能只有在通过 Horizon Agent 进行安装的情况下才受支持。使用 VMware Tools 进行安装则不受支持。</p>
vRealize Operations Desktop Agent	<p>允许 vRealize Operations Manager 与 vRealize Operations Manager for Horizon 配合使用。</p>
扫描仪重定向	<p>重定向连接到客户端系统的扫描设备，以便能在 RDS 桌面或应用程序上使用。</p> <p>必须在 RDS 主机上的 Windows Server 操作系统中安装桌面体验功能，才能在 Horizon Agent 安装程序中提供该选项。</p> <p>在 Windows Server 客户机操作系统上，默认不安装此安装选项。必须选择此选项才会进行安装。</p> <p>Horizon 6.0.2 和更高版本中提供了扫描仪重定向功能。</p>
VMware 客户端 IP 透明度	<p>启用到 Internet Explorer 的远程连接以使用客户端的 IP 地址，而不是远程桌面计算机的 IP 地址。</p> <p>默认情况下，不会选择该安装选项。必须选择此选项才会进行安装。</p>

在 IPv6 环境中，没有可选功能。

表 8-2. 在 RDS 主机上自动安装的 Horizon Agent 功能

选项	说明
PCoIP 代理	允许用户使用 PCoIP 显示协议连接到应用程序和 RDS 桌面。 如果您计划创建应用程序池，必须安装此组件，因为用户只能使用 PCoIP 连接到应用程序。
Windows Media 多媒体重定向 (MMR)	为 RDS 桌面提供多媒体重定向功能。通过该功能将多媒体流直接传输到客户端计算机，从而在客户端硬件而非远程 ESXi 主机上处理多媒体流。
Unity Touch	允许平板电脑和智能手机用户与远程桌面上运行的 Windows 应用程序进行交互。用户可以浏览、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切换，而无需使用“开始”菜单或任务栏。
PSG 代理	在 RDS 主机上安装 PCoIP 安全网关，以便为 RDS 主机上运行的桌面和应用程序会话实施 PCoIP 显示协议。
VMwareRDS	提供远程桌面服务功能的 VMware 实现。

在 IPv6 环境中，自动安装的功能有 PCoIP 代理、PSG 代理和 VMwareRDS。

有关 RDS 主机上支持的其他功能，请参阅《View 架构规划指南》文档中的“Horizon Agent 功能支持表”。

从嵌套会话内启动的远程应用程序打印

如果在安装 Horizon Agent 时启用了“虚拟打印”选项，用户将可以从通过远程桌面（嵌套会话）内 Horizon Client 启动的远程应用程序，打印到其本地客户端计算机上的打印机。

自 Horizon 7 版本 7.0.2 开始，用户可以从嵌套会话内启动的远程应用程序打印到与远程桌面计算机相连的打印机，而不是打印到与其本地客户端计算机相连的打印机。要启用此功能，请在 HKEY_LOCAL_MACHINE\SOFTWARE\ThinPrint\TPCLnRDP 中将 SiSActive 的值更改为 0，以更改远程桌面计算机上的 Thinprint 会话中会话模式。

注 在远程桌面计算机上将 SiSActive 设置为 0 以后，用户将无法再从在嵌套会话中启动的远程应用程序打印到与其本地客户端计算机相连的打印机。要重新启用默认的 ThinPrint 会话中会话模式，请在远程桌面计算机上的 HKEY_LOCAL_MACHINE\SOFTWARE\ThinPrint\TPCLnRDP 中，将 SiSActive 的值更改为 1。

有关在安装 Horizon Agent 期间启用虚拟打印选项的信息，请参阅[适用于 RDS 主机的 Horizon Agent 自定义安装选项](#)。

为 RDS 桌面和应用程序会话启用时区重定向

如果 RDS 主机在一个时区，而用户在另一个时区，则默认情况下，当用户连接 RDS 桌面时，桌面会显示 RDS 主机所在时区的时间。可以启用“时区重定向”组策略设置，以使 RDS 桌面显示本地时区的时间。该策略设置也适用于应用程序会话。

前提条件

- 确认在 Active Directory 服务器上可以使用组策略管理功能。

打开“组策略管理控制台”的步骤在 Windows 2012、Windows 2008 和 Windows 2003 Active Directory 版本中不同。请参阅[View 组策略创建 GPO](#)。

- 确认已将 Horizon 7 RDS ADMX 文件添加到 Active Directory 中。请参阅[将远程桌面服务 ADMX 文件添加到 Active Directory](#)。
- 熟悉组策略设置。请参阅[RDS 设备和资源重定向设置](#)。

步骤

- 1 在 Active Directory 服务器上，打开组策略管理控制台。
- 2 展开域和组策略对象。
- 3 右键单击为组策略设置创建的 GPO，然后选择**编辑**。
- 4 在“组策略管理编辑器”中，导航到**计算机配置 > 策略 > 管理模板 > Windows 组件 > Horizon View RDSH 服务 > 远程桌面会话主机 > 设备和资源重定向**。
- 5 启用允许时区重定向设置。

为应用程序启用基本的 Windows 主题

如果用户从未连接过 RDS 主机上的桌面，当用户启动某个在 RDS 主机上托管的应用程序时，将不会为该应用程序应用基本的 Windows 主题，即使已配置了 GPO 设置来加载 Aero 样式主题。Horizon 7 不支持 Aero 样式主题，但支持基本的 Windows 主题。要使基本的 Windows 主题应用于该应用程序，您必须再配置一项 GPO 设置。

前提条件

- 确认在 Active Directory 服务器上可以使用组策略管理功能。
- 打开“组策略管理控制台”的步骤在 Windows 2012、Windows 2008 和 Windows 2003 Active Directory 版本中不同。请参阅[View 组策略创建 GPO](#)。

步骤

- 1 在 Active Directory 服务器上，打开组策略管理控制台。
- 2 展开域和组策略对象。
- 3 右键单击为组策略设置创建的 GPO，然后选择**编辑**。
- 4 在组策略管理编辑器中，导航到**用户配置 > 策略 > 管理模板 > 控制面板 > 个性化**。
- 5 启用**强制使用特定的视觉样式文件或强制使用 Windows 经典设置**，并将“视觉样式的路径”设置为 `%windir%\resources\Themes\Aero\ aero.msstyles`。

配置组策略以启动 Runonce.exe

默认情况下，某些依赖 `Explorer.exe` 文件的应用程序可能无法在应用程序会话中运行。为避免这种问题，您必须配置组策略对象 (GPO) 设置来启动 `runonce.exe`。

前提条件

- 确认在 Active Directory 服务器上可以使用组策略管理功能。
打开“组策略管理控制台”的步骤在 Windows 2012、Windows 2008 和 Windows 2003 Active Directory 版本中不同。请参阅[View 组策略创建 GPO](#)。

步骤

- 1 在 Active Directory 服务器上，打开组策略管理控制台。
- 2 展开域和组策略对象。
- 3 右键单击为组策略设置创建的 GPO，然后选择**编辑**。
- 4 在组策略管理编辑器中，导航到**用户配置 > 策略 > Windows 设置 > 脚本 (登录/注销)**。
- 5 双击**登录**，然后单击**添加**。
- 6 在“脚本名”框中，键入 `runonce.exe`。
- 7 在“脚本参数”框中，键入 `/AlternateShellStartup`。

RDS 主机性能选项

您可以通过设置性能选项来针对前台程序或后台服务优化 Windows。默认情况下，Horizon 7 对所有支持的 Windows Server 版本均禁用某些 RDS 主机性能选项。

下表显示了 Horizon 7 所禁用的性能选项。

表 8-3. Horizon 7 所禁用的性能选项

Horizon 7 所禁用的性能选项
最小化和最大化时以动画显示窗口
在鼠标指针下显示阴影
在窗口下显示阴影
对桌面上的图标标签使用阴影
拖动时显示窗口内容

Horizon 7 所禁用的五个性能选项与注册表中的四个 Horizon 7 设置相对应。下表显示了 Horizon 7 设置及其默认注册表值。这些注册表值位于注册表子项 `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration` 中。您可以通过将一个或多个 Horizon 7 注册表值设置为 `false` 来重新启用性能选项。

表 8-4. 与 Windows 性能选项相关的 Horizon 7 设置

Horizon 7 设置	注册表值
禁用光标阴影	DisableMouseShadows
禁用全窗口拖动	DisableFullWindowDrag
禁用 ListView 阴影	DisableListViewShadow
禁用窗口动画	DisableWindowAnimation

为 RDS 主机配置 3D 图形

如果为 RDS 主机配置了 3D 图形，应用程序池中的应用程序以及在 RDS 桌面上运行的应用程序都可以显示 3D 图形。

可以使用以下 3D 图形选项：

NVIDIA GRID vGPU（共享 GPU 硬件加速）	在多个虚拟机之间共享 ESXi 主机上的物理 GPU。需要使用 ESXi 6.0 或更高版本。
采用 vDGA 的 AMD 多用户 GPU	在多个虚拟机之间共享 ESXi 主机上的物理 GPU。需要使用 ESXi 6.0 或更高版本。
虚拟专用图形加速 (vDGA)	ESXi 主机上的物理 GPU 专用于单个虚拟机。需要使用 ESXi 5.5 或更高版本。

注 某些 Intel vDGA 卡需要特定的 vSphere 6 版本。请参阅位于 <http://www.vmware.com/resources/compatibility/search.php> 的《VMware 硬件兼容性列表》。此外，对于 Intel vDGA，使用的是 Intel 集成的 GPU 而不是分离式 GPU，其他供应商的情况也是如此。

通过使用 vDGA，您可以将整个 GPU 分配给一台计算机，以获取最佳性能。RDS 主机必须位于手动场中。

通过使用采用 vDGA 的 AMD 多用户 GPU，您可以使一个 AMD GPU 显示为多个 PCI 直通设备，从而在多个 RDS 主机之间共享此 AMD GPU。RDS 主机必须位于手动场中。

通过使用 NVIDIA GRID vGPU，每个显卡可以支持多个 RDS 主机，并且 RDS 主机必须位于手动场中。如果 ESXi 主机具有多个物理 GPU，您还可以配置 ESXi 主机为 GPU 分配虚拟机的方式。默认情况下，ESXi 主机会将虚拟机分配给所分配到的虚拟机最少的物理 GPU。这称为“性能模式”。您也可以选择整合模式，在该模式下，ESXi 主机将虚拟机分配给同一物理 GPU，直到达到最大虚拟机数，然后再将虚拟机放到下一物理 GPU 上。要配置整合模式，请在 ESXi 主机上编辑 `/etc/vmware/config` 文件并添加以下内容：

```
vGPU.consolidation = "true"
```

只有在使用 PCoIP 或 VMware Blast 协议时，才支持 3D 图形。因此，场必须将 PCoIP 或 VMware Blast 用作默认协议，并且不得允许用户选择协议。

配置 3D 图形的步骤概述

本概述内容介绍了在 vSphere 和 Horizon 7 中配置 3D 图形时必须执行的任务。有关设置 NVIDIA GRID vGPU 的详细信息，请参阅《[适用于 VMware Horizon 6.1 的 NVIDIA GRID vGPU 部署指南](#)》文档。有关设置 vDGA 的详细信息，请参阅《[View 虚拟桌面中的图形加速](#)》文档。有关设置采用 vDGA 的 AMD 多用户 GPU 的详细信息，请参阅[准备使用采用 vDGA 的 AMD 多用户 GPU 功能](#)。

- 1 设置 RDS 主机虚拟机。有关更多信息，请参阅[第 8 章 设置远程桌面服务主机](#)。
- 2 将图形 PCI 设备添加到虚拟机中。请参阅《vSphere 虚拟机管理》文档的“配置虚拟机硬件”一章中的“其他虚拟机设备配置”。在添加设备时，请务必单击**预留所有内存**。
- 3 在虚拟机上，安装显卡的设备驱动程序。
- 4 将 RDS 主机添加到手动场中，创建 RDS 桌面池，使用 PCoIP 连接到桌面，然后激活显示适配器。

您不需要在 View Administrator 中为 RDS 主机配置 3D 图形。在安装 Horizon Agent 时选择 **3D RDSH** 选项就足够了。默认情况下，不会选择该选项并禁用 3D 图形。

创建场

场是一种为用户提供常见应用程序或 RDS 桌面的 RDS 主机组。

本章讨论了以下主题：

- 场
- 为自动场准备父虚拟机
- 用于创建手动场的工作表
- 用于创建自动场的工作表
- 创建手动场
- 创建自动场

场

场可以简化在企业中管理 RDS 主机、RDS 桌面和应用程序的任务。您可以创建手动或自动场，以便为不同规模或具有不同桌面或应用程序要求的用户群提供服务。

手动场包含已存在的 RDS 主机。RDS 主机可以是物理机，也可以是虚拟机。在创建场时，您可以手动添加 RDS 主机。

自动场包含作为 vCenter Server 中的链接克隆虚拟机的 RDS 主机。View Composer 根据在创建场时指定的参数创建虚拟机。这些虚拟机是从单个父虚拟机中克隆的，并通过某种机制与父虚拟机相关联，从而减少了虚拟机所需的存储量。

在创建应用程序池或 RDS 桌面池时，您必须指定一个（且只能指定一个）场。场中的 RDS 主机可以托管 RDS 桌面、应用程序或二者皆有。一个场最多可以支持一个 RDS 桌面池，但可以支持多个应用程序池。一个场可同时支持这两种类型的池。

场可以提供以下便利：

- 负载平衡

默认情况下，Horizon 7 会平衡场中所有 RDS 主机的 RDS 桌面会话和应用程序会话的负载。您可以编写和配置负载平衡脚本以控制新应用程序会话的位置。有关详细信息，请参阅《View 管理指南》文档中的“为 RDS 主机配置负载平衡”。

- 冗余性

如果场中的一个 RDS 主机脱机，该场中的其他 RDS 主机可继续为用户提供应用程序和桌面。

- 可扩展性

一个场可以拥有数量不定的 RDS 主机。您可以创建拥有不同数量 RDS 主机的场，以便为不同规模的用户群提供服务。

场具有以下属性：

- 一个 Horizon 7 容器最多可拥有 200 个场。
- 一个场最多可拥有 200 个 RDS 主机。
- 一个场中的 RDS 主机可以运行任何支持的 Windows Server 版本。请参阅《View 安装指南》文档中的“客户机操作系统的系统要求”。
- 自动场支持 View Composer 重构操作，但不支持刷新或重新平衡操作。您可以重构自动场，但不能重构场中的一部分 RDS 主机。

重要事项 Microsoft 建议您为每个场的用户单独配置漫游配置文件。场或用户的物理桌面之间不应共享配置文件，因为如果用户同时登录两个加载同一配置文件的计算机，可能会发生配置文件损坏和数据丢失的情况。

为自动场准备父虚拟机

要创建自动场，必须先准备父虚拟机。View Composer 使用该父虚拟机创建链接克隆虚拟机，这些虚拟机是场中的 RDS 主机。

- **准备 RDS 主机父虚拟机**

View Composer 服务需要通过父虚拟机来生成基础映像以创建链接克隆。

- **在链接克隆 RDS 主机上激活 Windows**

要确保 View Composer 在链接克隆 RDS 主机上正确激活 Windows Server 操作系统，您必须使用父虚拟机上的 Microsoft 批量激活功能。批量激活技术需要使用批量许可证密钥。

- **在父虚拟机中禁用 Windows 休眠功能**

Windows 休眠功能可创建隐藏的系统文件 Hiberfil.sys，并使用此文件来存储混合睡眠所需的信息。禁用休眠功能可减小即时克隆或 View Composer 链接克隆虚拟磁盘的大小。

准备 RDS 主机父虚拟机

View Composer 服务需要通过父虚拟机来生成基础映像以创建链接克隆。

前提条件

- 确认设置了 RDS 主机虚拟机。请参阅第 8 章 [设置远程桌面服务主机](#)。要设置 RDS 主机，请确保不要使用以前在 View 连接服务器中注册的虚拟机。

用于 View Composer 的父虚拟机必须属于链接克隆计算机将要加入的 Active Directory 域或是本地 WORKGROUP 的成员。

- 确认虚拟机不是从 **View Composer** 链接克隆转换的虚拟机。从链接克隆转换的虚拟机带有克隆的内部磁盘和状态信息。父虚拟机不能有状态信息。

重要事项 链接克隆以及由链接克隆转换的虚拟机不能作为父虚拟机。

- 在父虚拟机上安装 **Horizon Agent** 时，应选择 **View Composer Agent** 选项。请参阅[在远程桌面服务主机上安装 Horizon Agent](#)。

要在大型环境中更新 **Horizon Agent**，您可以使用标准的 **Windows** 更新机制，例如 **Altiris**、**SMS**、**LanDesk**、**BMC** 或其他系统管理软件。您还可以使用重构操作来更新 **Horizon Agent**。

注 请不要在父虚拟机中更改 **VMware View Composer Guest Agent Server** 服务的登录帐户。默认情况下，该帐户为 **Local System** 帐户。如果更改此帐户，通过此父虚拟机创建的链接克隆便不会启动。

- 要部署 **Windows** 计算机，请配置批量许可证密钥，并使用批量激活功能激活父虚拟机的操作系统。请参阅[激活即时克隆](#)和 [View Composer 链接克隆上的 Windows](#)。
- 熟悉禁用在 **Windows Update** 中搜索设备驱动程序的过程。参阅 [http://technet.microsoft.com/en-us/library/cc730606\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx) 上的“禁用在 **Windows Update** 中搜索设备驱动程序” **Microsoft Technet** 文章。
- 要实施 **RDS** 主机负载平衡功能，请按照《**View** 管理指南》文档的“为 **RDS** 主机配置负载平衡”中所述修改 **RDS** 主机父虚拟机。

步骤

- ◆ 移除父虚拟机上的 **DHCP** 租约，以避免将租借的 **IP** 地址复制到场中的链接克隆。
 - a 在父虚拟机上打开一个命令提示符。
 - b 键入 **ipconfig /release** 命令。
- ◆ 确认系统磁盘包含一个卷。

无法通过包含多个卷的父虚拟机来部署链接克隆。**View Composer** 服务不支持多个磁盘分区，但支持多个虚拟磁盘。
- ◆ 确认虚拟机不包含独立磁盘。

为虚拟机拍快照时将排除独立磁盘。从虚拟机中创建或重构的链接克隆将不包含独立磁盘。
- ◆ 禁用休眠选项以减少从父虚拟机创建的链接克隆操作系统磁盘的大小。
- ◆ 在拍摄父虚拟机快照前，请禁用在 **Windows Update** 中搜索设备驱动程序。

该 **Windows** 功能可能会干扰链接克隆计算机的自定义。自定义每个链接克隆时，**Windows** 可能会在 **Internet** 上搜索适用于该克隆的最佳驱动程序，从而导致重复搜索和自定义延迟。
- ◆ 在 **vSphere Client** 中，禁用父虚拟机上的 **vApp** 选项设置。
- ◆ 在 **Windows Server 2008 R2** 和 **Windows Server 2012 R2** 计算机上，移除未使用的功能以禁用恢复磁盘空间的计划维护任务。

例如: `Schtasks.exe /change /disable /tn "\Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup"`

如果保留启用状态，该维护任务会在创建链接克隆之后移除 Sysprep 自定义脚本，从而导致后续重构操作失败并出现自定义操作超时错误。有关详细信息，请参阅 <http://support.microsoft.com/kb/2928948> 上提供的 Microsoft 知识库文章。

- ◆ 在 Windows Server 2012 计算机上，应用 <https://support.microsoft.com/en-us/kb/3020396> 中提供的 Microsoft 修补程序。

通过使用该修补程序，Sysprep 可以自定义启用了 RDS 角色的 Windows Server 2012 虚拟机。如果未使用该修补程序，在自动场中部署的 Windows Server 2012 链接克隆计算机上的 Sysprep 自定义将失败。

后续步骤

使用 vSphere Client 或 vSphere Web Client 为处于关机状态的父虚拟机拍摄快照。该快照将用作第一组绑定到父虚拟机的链接克隆计算机的基准配置。

重要事项 拍摄快照前，请使用客户机操作系统中的关机命令彻底关闭父虚拟机。

在链接克隆 RDS 主机上激活 Windows

要确保 View Composer 在链接克隆 RDS 主机上正确激活 Windows Server 操作系统，您必须使用父虚拟机上的 Microsoft 批量激活功能。批量激活技术需要使用批量许可证密钥。

要使用批量激活功能激活 Windows，您需要使用密钥管理服务 (Key Management Service, KMS)，密钥管理服务需要使用 KMS 许可证密钥。请咨询您的 Microsoft 经销商，获取批量许可证密钥并配置批量激活功能。

注 View Composer 不支持多激活密钥 (Multiple Activation Key, MAK) 许可。

使用 View Composer 创建链接克隆计算机之前，必须使用批量激活功能激活父虚拟机上的操作系统。

链接克隆计算机创建完毕后，每次重构链接克隆时，View Composer Agent 均会使用父虚拟机的 KMS 服务器来激活链接克隆上的操作系统。

对于 KMS 许可，View Composer 将使用为激活父虚拟机配置的 KMS 服务器。KMS 服务器将激活的链接克隆视为具有新颁发许可证的计算机。

在父虚拟机中禁用 Windows 休眠功能

Windows 休眠功能可创建隐藏的系统文件 Hiberfil.sys，并使用此文件来存储混合睡眠所需的信息。禁用休眠功能可减小即时克隆或 View Composer 链接克隆虚拟磁盘的大小。

小心 休眠功能不可用时，混合睡眠无法正常工作。如果发生断电，用户可能会丢失数据。

步骤

- 1 在 vSphere Client 中，选择父虚拟机，然后选择**打开控制台**。
- 2 以管理员身份登录。

3 禁用休眠选项。

- a 单击**开始**，然后在**开始搜索**框中键入 **cmd**。
- b 在搜索结果列表中，右键单击**命令提示符**然后单击**以管理员身份运行**。
- c 在**用户帐户控制**提示中单击**继续**。
- d 在命令提示符下，键入 **powercfg.exe /hibernate off**，然后按 Enter 键。
- e 键入 **exit**，然后按 Enter 键。

用于创建手动场的工作表

在创建手动场时，**添加场**向导将提示您配置特定设置。

您可以打印此工作表，并记下您要在运行**添加场**向导时指定的值。

表 9-1. 工作表：用于创建手动场的配置设置

设置	说明	在此填写您要指定的值
ID	用于在 View Administrator 中标识场的唯一名称。	
说明	此场的描述。	
访问组	要在其中放置此场中所有池的访问组。 有关访问组的详细信息，请参阅《View 管理指南》文档中的基于角色的委托管理一章。	
默认显示协议	选择 VMware Blast 、 PCoIP 或 RDP 。RDP 仅适用于桌面池。应用程序池的显示协议始终为 VMware Blast 或 PCoIP 。如果选择 RDP 并计划使用该场来托管应用程序池，则必须将 允许用户选择协议 设置为 是 。默认设置为 PCoIP 。	
允许用户选择协议	选择 是 或 否 。该设置仅适用于 RDS 桌面池。如果选择 是 ，则用户可以在从 Horizon Client 中连接到 RDS 桌面时选择显示协议。默认值为 是 。	
空会话超时 (仅限应用程序)	确定空应用程序会话保持打开的时间。如果应用程序会话中运行的所有应用程序都已关闭，此会话便为空。当会话为打开状态时，用户可更快地打开应用程序。如果将空应用程序会话断开连接或注销，可以节省系统资源。选择 从不 ，或者设置超时分钟数。默认值为 在 1 分钟后 。	
发生超时	确定在达到 空会话超时 限制后将空应用程序会话断开连接还是注销。选择 断开连接 或 注销 。会话注销可以释放资源，但打开应用程序将花费更长的时间。默认值为 断开连接 。	
注销断开的会话	确定何时注销断开连接的会话。此设置同时应用于桌面会话和应用程序会话。选择 从不 、 立即 或 …分钟之后 。选择 立即 或 …分钟之后 ，请慎重考虑。注销断开连接的会话时，该会话将丢失。默认值为 从不 。	
允许 HTML Access 访问此场上的桌面和应用程序	确定是否允许 HTML Access 访问 RDS 桌面和应用程序。选中 已启用 复选框将允许 HTML Access 访问 RDS 桌面和应用程序。在创建场后编辑该设置时，新值将应用于现有的和新的桌面以及应用程序。	

注 与自动场不同，手动场没有**每个 RDS 服务器的最大会话数**设置，因为手动场可能具有不同的 RDS 主机。对于手动场中的 RDS 主机，您可以编辑各个 RDS 主机并更改等效的设置**连接数量**。

用于创建自动场的工作表

在创建自动场时，**添加场**向导将提示您配置特定设置。

您可以打印此工作表，并记下您要在运行**添加场**向导时指定的值。

表 9-2. 工作表：用于创建自动场的配置设置

设置	说明	在此填写您要指定的值
ID	用于在 View Administrator 中标识场的唯一名称。	
说明	此场的描述。	
访问组	要在其中放置此场中所有池的访问组。 有关访问组的详细信息，请参阅《View 管理指南》文档中的基于角色的委托管理一章。	
默认显示协议	选择 VMware Blast 、 PCoIP 或 RDP 。RDP 仅适用于桌面池。用于应用程序池的显示协议始终为 VMware Blast 或 PCoIP 。如果选择 RDP 并计划使用该场来托管应用程序池，则必须将 允许用户选择协议 设置为 是 。默认设置为 PCoIP 。	
允许用户选择协议	选择 是 或 否 。该设置仅适用于 RDS 桌面池。如果选择 是 ，则用户可以在从 Horizon Client 中连接到 RDS 桌面时选择显示协议。默认值为 是 。	
空会话超时 (仅限应用程序)	确定空应用程序会话保持打开的时间。如果应用程序会话中运行的所有应用程序都已关闭，此会话便为空。当会话为打开状态时，用户可更快地打开应用程序。如果将空应用程序会话断开连接或注销，可以节省系统资源。选择 从不 ，或者设置超时分钟数。默认值为 在 1 分钟后 。	
发生超时后	确定在达到 空会话超时 限制后将空应用程序会话断开连接还是注销。选择 断开连接 或 注销 。会话注销可以释放资源，但打开应用程序将花费更长的时间。默认值为 断开连接 。	
注销断开的会话	确定何时注销断开连接的会话。此设置同时应用于桌面会话和应用程序会话。选择 从不 、 立即 或 ...分钟之后 。选择 立即 或 ...分钟之后 ，请慎重考虑。注销断开连接的会话时，该会话将丢失。默认值为 从不 。	
允许 HTML Access 访问此场上的桌面和应用程序	确定是否允许 HTML Access 访问 RDS 桌面和应用程序。选中 已启用 复选框将允许 HTML Access 访问 RDS 桌面和应用程序。在创建场后编辑该设置时，新值将应用于现有的和新的桌面以及应用程序。	
每个 RDS 服务器的最大会话数	确定 RDS 主机可以支持的最大会话数。选择 不受限制 或 不超过... 。默认值是 不受限制 。	
启用置备	选中该复选框以在完成此向导后启用置备。默认情况下，将选中该框。	
出现错误时停止置备	选中该复选框以在出现置备错误时停止置备。默认情况下，将选中该框。	
命名模式	指定前缀或名称格式。View 将附加或插入自动生成的编号以组成计算机名称，从 1 开始。如果要将编号放在末尾，则只需指定前缀。否则，在字符串中的任意位置指定 {n}，{n} 将替换为编号。您还可以指定 {n:fixed=<number of digits>}，其中 fixed=<number of digits> 指示编号使用的位数。例如，指定 vm-{n:fixed=3}-sales，则计算机名称是 vm-001-sales、vm-002-sales，依此类推。 注 每个计算机名称（包括自动生成的编号）具有 15 个字符限制。	
计算机的最大数量	要置备的计算机数。	

设置	说明	在此填写您要指定的值
View Composer 维护操作期间就绪 (已置备) 计算机的最小数量	通过使用该设置，在 View Composer 重构场中的计算机时，您可以保留指定数量的计算机以接受连接请求。	
使用 vSphere Virtual SAN	指定是否使用 VMware Virtual SAN（如果可用）。Virtual SAN 是一个软件定义的存储层，可以虚拟化在 ESXi 主机的群集上可用的本地物理存储磁盘。有关详细信息，请参阅 使用 Virtual SAN 实现高性能存储和基于策略的管理 。	
为副本磁盘和操作系统磁盘选择单独的数据存储	（仅在不使用 Virtual SAN 时有效）出于性能或其他原因，您可以将副本和操作系统磁盘放在不同的数据存储中。	
父虚拟机	从列表中选择一个父虚拟机。请注意，该列表包括未安装 View Composer Agent 的虚拟机。您不能选择其中的任何虚拟机，因为需要使用 View Composer Agent。最佳做法是使用指示虚拟机是否安装了 View Composer Agent 的命名约定。	
快照	选择要用作场的基础映像的父虚拟机快照。 不要删除 vCenter Server 中的快照和父虚拟机，除非场中的链接克隆不使用该默认映像，并且不会根据该默认映像创建链接克隆。系统需要使用父虚拟机和快照根据场策略在场中置备新的链接克隆。View Composer 维护操作也需要父虚拟机和快照。	
虚拟机文件夹位置	选择场所在的 vCenter Server 文件夹。	
主机或群集	选择要用来运行桌面虚拟机的 ESXi 主机或群集。 使用 Virtual SAN 数据存储（vSphere 5.5 Update 1 的一项功能），可以选择最多包含 20 个 ESXi 主机的群集。使用虚拟卷数据存储（vSphere 6.0 的一项功能），可以选择最多包含 32 个 ESXi 主机的群集。 在 vSphere 5.1 或更高版本中，如果副本存储在 VMFS5 或更高版本的数据存储中或 NFS 数据存储中，您就可选择最多含有 32 个 ESXi 主机的群集。如果您将副本磁盘存储在 VMFS5 之前的版本中，群集最多可包含 8 台主机。 在 vSphere 5.0 中，如果副本存储于 NFS 数据存储中，则可选择包含八台以上 ESXi 主机的群集。如果您在 VMFS 数据存储中存储副本，则一个群集最多包含八台主机。	
资源池	选择场所在的 vCenter Server 资源池。	
数据存储	<p>选择一个或多个要在其中存储场的数据存储。</p> <p>“添加场”向导中的选择链接克隆数据存储页上的一个表简要说明了估算场的存储要求的准则。这些信息能帮助您确定哪个数据存储有足够空间存储链接克隆磁盘。有关详细信息，请参阅确定即时克隆和View Composer 链接克隆桌面池的存储大小。</p> <p>您可将共享数据存储或本地数据存储用于单个的 ESXi 主机或 ESXi 群集。如果您在 ESXi 群集中使用本地数据存储，则您必须考虑桌面部署的 vSphere 基础架构限制。请参阅在本地数据存储上存储 View Composer 链接克隆。</p> <p>注 如果使用 Virtual SAN，则只选择一个数据存储。</p>	
存储过载	<p>确定在每个数据存储上创建链接克隆时的存储过载级别。</p> <p>随着级别的增加，数据存储上装载的链接克隆会越来越多，而为单个克隆的增长所保留的空间则越来越少。如果设置较高的存储过载级别，您创建的链接克隆的总逻辑大小就可以大于数据存储的物理存储限制。有关详细信息，请参阅View Composer 链接克隆虚拟机的存储过载。</p> <p>注 如果使用 Virtual SAN，则该设置无效。</p>	

设置	说明	在此填写您要指定的值
使用本地 NFS 快照 (VAAI)	<p>（仅在不使用 Virtual SAN 时有效）如果部署中包含支持 vStorage APIs for Array Integration (VAAI) 的 NAS 设备，则可以使用本地快照技术克隆虚拟机。</p> <p>仅当您选择了位于通过 VAAI 支持本地克隆操作的 NAS 设备上的数据存储时，才可以使用此功能。</p> <p>如果您将副本磁盘和操作系统磁盘存储在单独的数据存储中，则无法使用这些功能。无法在包含能节省空间的磁盘的虚拟机上使用此功能。</p> <p>vSphere 5.0 及更高版本支持此功能。</p> <p>有关详细信息，请参阅将 VAAI 存储用于 View Composer 链接克隆。</p>	
回收虚拟机磁盘空间	<p>（仅在不使用 Virtual SAN 或虚拟卷时有效）确定是否允许 ESXi 主机回收以节省空间的磁盘格式创建的链接克隆上的未用磁盘空间。空间回收功能减少了链接克隆桌面所需的总存储空间。</p> <p>vSphere 5.1 及更高版本支持此功能。链接克隆虚拟机必须是虚拟硬件版本 9 或更高版本。</p> <p>有关详细信息，请参阅在 View Composer 链接克隆上回收磁盘空间。</p>	
在虚拟机上的未使用空间超出以下值时启动回收：	<p>（仅在不使用 Virtual SAN 或虚拟卷时有效）键入为触发空间回收而必须在链接克隆操作系统磁盘上累积的未用磁盘空间的最小数量（千兆字节）。当未使用的磁盘空间超过此阈值时，View 将启动操作，指示 ESXi 主机回收操作系统磁盘上的空间。</p> <p>此值根据虚拟机而测得。在 View 开始对单个虚拟机进行空间回收过程之前，未使用的磁盘空间必须超过相应虚拟机上指定的阈值。</p> <p>例如：2 GB。</p> <p>默认值为 1 GB。</p>	
中断时间	<p>配置不进行虚拟机磁盘空间回收操作的日期和时间。</p> <p>为了确保必要时 ESXi 资源专供前台任务使用，您可以在指定日期的指定时段内禁止 ESXi 主机执行这些操作。</p> <p>有关详细信息，请参阅View Composer 链接克隆设置 Storage Accelerator 和空间回收中断时间。</p>	
透明页面共享范围	<p>选择允许透明页面共享 (TPS) 的级别。选项包括：虚拟机（默认）、场、容器或全局。如果在场、容器或全局级别为所有计算机启用 TPS，ESXi 主机消除因这些计算机使用同一客户机操作系统或应用程序而产生的内存页冗余副本。</p> <p>页面共享发生在 ESXi 主机上。例如，如果在场级别启用 TPS，但场分散到多个 ESXi 主机，则仅相同主机和相同场中的虚拟机共享页面。在全球级别，View 在相同 ESXi 主机上管理的所有计算机可以共享内存页，而不管这些计算机位于哪个场中。</p> <p>注 默认设置是不在计算机之间共享内存页，因为 TPS 可能会带来安全风险。调查表明可能会在非常有限的配置场景下滥用 TPS 来获取对数据的未授权访问。</p>	
域	<p>选择 Active Directory 域和用户名。</p> <p>View Composer 需要具有场的特定用户权限。Sysprep 使用域和用户帐户来自定义链接克隆计算机。</p> <p>当您为 vCenter Server 配置 View Composer 设置时，应指定此用户。配置 View Composer 设置时，可以指定多个域和用户。在使用添加场向导创建场时，必须从列表中选择一个域和用户。</p> <p>有关配置 View Composer 的信息，请参阅《View 管理指南》文档。</p>	

设置	说明	在此填写您要指定的值
AD 容器	<p>提供 Active Directory 容器的相对专有名称。</p> <p>例如: CN=Computers</p> <p>在运行添加场向导时, 可以浏览 Active Directory 树以找到所需的容器。</p>	
允许重新使用已存在的计算机帐户	<p>选择该设置以将 Active Directory 中的现有计算机帐户用于 View Composer 置备的链接克隆。该设置允许您控制在 Active Directory 中创建的计算机帐户。</p> <p>置备链接克隆后, 如果现有 AD 计算机帐户名与链接克隆计算机名匹配, 则 View Composer 会使用现有的计算机帐户。否则, 需创建新的计算机帐户。</p> <p>现有的计算机帐户必须位于您通过 Active Directory 容器 设置而指定的 Active Directory 容器中。</p> <p>如果禁用该设置, 在 View Composer 置备链接克隆时, 将创建新的 AD 计算机帐户。默认情况下禁用此设置。</p> <p>有关详细信息, 请参阅针对链接克隆使用现有的 Active Directory 计算机帐户。</p>	
使用自定义规范 (Sysprep)	提供 Sysprep 自定义规范以自定义虚拟机。	

创建手动场

在授权用户访问应用程序或 RDS 桌面的过程中, 您可以创建手动场。

前提条件

- 设置属于场的 RDS 主机。请参阅[第 8 章 设置远程桌面服务主机](#)。
- 确认所有 RDS 主机均为“可用”状态。在 View Administrator 中, 选择 **View 配置 > 已注册的计算机**, 并在“RDS 主机”选项卡上检查每个 RDS 主机的状态。
- 收集创建场时必须提供的配置信息。请参阅[用于创建手动场的工作表](#)。

步骤

- 1 在 View Administrator 中, 单击**资源 > 场**。
- 2 单击**添加**输入在工作表中收集的配置信息。
- 3 选择**手动场**。
- 4 按照向导中的提示创建场。

使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称, 您可以直接返回至已完成的任意向导页面。

- 5 选择要添加到场的 RDS 主机, 然后单击**下一步**。
- 6 单击**完成**。

此时, 您可以在 View Administrator 中单击**资源 > 场**以查看该场。

后续步骤

创建应用程序池或 RDS 桌面池。请参阅[第 10 章 创建应用程序池](#)或[第 11 章 创建 RDS 桌面池](#)。

创建自动场

在授权用户访问应用程序或 RDS 桌面的过程中，您可以创建自动场。

前提条件

- 确认安装了 View Composer 服务。请参阅《View 安装指南》文档。
- 确认在 View Administrator 中配置了适用于 vCenter Server 的 View Composer 设置。请参阅《View 管理指南》文档。
- 确认用于虚拟机（用作远程桌面）的 ESXi 虚拟交换机上的端口数量充足。如果要创建大型桌面池，默认值可能不足以满足要求。ESXi 主机上的虚拟交换机端口的数量必须大于或等于虚拟机数量与每个虚拟机的虚拟网卡的数量的乘积。
- 确认已准备好父虚拟机。必须在该父虚拟机上安装 Horizon Agent 和 View Composer Agent。请参阅[为自动场准备父虚拟机](#)。
- 在 vCenter Server 中为父虚拟机拍摄一个快照。为父虚拟机拍摄快照之前必须将其关闭。View Composer 将使用该快照作为基础映像来创建克隆。

注 您不能从虚拟机模板来创建链接克隆池。

- 收集创建场时必须提供的配置信息。请参阅[用于创建自动场的工作表](#)。

步骤

- 1 在 View Administrator 中，单击**资源 > 场**。
- 2 单击**添加**输入在工作表中收集的配置信息。
- 3 选择**自动场**。
- 4 按照向导中的提示创建场。

使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，您可以直接返回至已完成的任意向导页面。

此时，您可以在 View Administrator 中单击**资源 > 场**以查看该场。

后续步骤

创建应用程序池或 RDS 桌面池。请参阅[第 10 章 创建应用程序池](#)或[第 11 章 创建 RDS 桌面池](#)。

创建应用程序池

为用户提供应用程序的远程访问权限所需执行的一个任务是创建应用程序池。有权访问应用程序池的用户可以从各种客户端设备远程访问该应用程序。

本章讨论了以下主题：

- 应用程序池
- 用于手动创建应用程序池的工作表
- 创建应用程序池

应用程序池

通过应用程序池，您可以将一个应用程序提供给很多用户。该应用程序将在 **RDS** 主机场上运行。

创建应用程序池时，您在用户从任意网络位置均可访问的数据中心内部署应用程序。有关应用程序池的简介，请参阅[场、RDS 主机以及桌面和应用程序池](#)。

一个应用程序池只有一个应用程序，并且只与一个场相关联。为了避免出现错误，您必须在场中的所有 **RDS** 主机上安装该应用程序。

当您创建应用程序池时，**View** 会自动显示场中所有 **RDS** 主机的**开始**菜单中可供所有用户（而非个别用户）使用的应用程序。您可以从列表中选择一个或多个应用程序。如果您从列表中选择多个应用程序，则会为每个应用程序创建一个单独的应用程序池。您也可以手动指定列表中没有的应用程序。如果要手动指定的应用程序尚未安装，**View** 会显示警告消息。

创建应用程序池时，您无法指定用于放置池的访问组。对于应用程序池和 **RDS** 桌面池，在创建场时指定访问组。

应用程序支持 **PCoIP** 和 **VMware Blast** 显示协议。要启用 **HTML Access**，请参阅《使用 **HTML Access**》文档中“设置和安装”一章的“为 **HTML Access** 准备桌面、池和场”，您可以从以下网址获取此文档：
https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html。

用于手动创建应用程序池的工作表

当您创建应用程序池并手动指定应用程序时，**添加应用程序池**向导会提示您输入有关应用程序的信息。并不需要应用程序已安装在任何 **RDS** 主机上。

您可以打印此工作表，并在手动指定应用程序时记下应用程序的属性。

表 10-1. 工作表：用于手动创建应用程序池的应用程序属性

属性	描述	在此填写您要指定的值
ID	用于在 View Administrator 中标识池的唯一名称。 此字段为必填字段。	
显示名称	用户登录到 Horizon Client 时看到的池名称。如果不指定显示名称，该名称将与 ID 相同。	
版本	应用程序的版本。	
发布者	应用程序的发布者。	
路径	应用程序的完整路径名。例如，C:\Program Files\app1.exe。此字段为必填字段。	
开始文件夹	应用程序的开始目录的完整路径名。	
参数	应用程序启动时传递给应用程序的参数。例如，您可以指定 <code>-username user1 -loglevel 3</code> 。	
描述	对此应用程序池的描述。	

创建应用程序池

为用户授予访问在 RDS 主机上运行的应用程序的权限的过程中，会创建一个应用程序池。

前提条件

- 设置 RDS 主机。请参阅[第 8 章 设置远程桌面服务主机](#)。
- 创建包含 RDS 主机的场。请参阅[第 9 章 创建场](#)。
- 如果要手动添加应用程序池，应收集有关该应用程序的信息。请参阅[用于手动创建应用程序池的工作表](#)。

步骤

- 1 在 View Administrator 中，单击 **目录 > 应用程序池**。
- 2 单击 **添加**。
- 3 按照向导中的提示创建池。

如果选择手动添加应用程序池，可使用工作表中收集的配置信息。如果从 View Administrator 显示的列表中选择应用程序，则可以选择多个应用程序。会为每个应用程序创建一个单独的池。

在 View Administrator 中，您现在可以单击 **目录 > 应用程序池** 以查看应用程序池。

后续步骤

授予用户访问池的权限。请参阅[第 13 章 授权用户和组](#)。

确保最终用户可以访问 Horizon Client 3.0 或更高版本的软件，以支持 RDS 应用程序。

如果您需要确保 **View** 连接服务器仅在具有足够资源以运行应用程序的 **RDS** 主机上启动应用程序，请为应用程序池配置一个反关联性规则。有关详细信息，请参阅《**View** 管理指南》文档中的“为应用程序池配置反关联性规则”。

创建 RDS 桌面池

为授予用户远程访问基于会话的桌面的权限，您需执行的任务之一是创建远程桌面服务 (RDS) 桌面池。RDS 桌面池所具备的属性能够满足远程桌面部署的一些特定需求。

本章讨论了以下主题：

- 了解 RDS 桌面池
- 创建 RDS 桌面池
- 适用于 RDS 桌面池的桌面池设置
- 为 RDS 桌面池配置 Internet Explorer 中的 Adobe Flash 调节

了解 RDS 桌面池

RDS 桌面池是您可以创建的三种桌面池之一。这种类型的桌面池在以前的 View 版本中称为 Microsoft 终端服务池。

RDS 桌面池和 RDS 桌面具有以下特点：

- RDS 桌面池与场关联，而场是一组 RDS 主机。每个 RDS 主机是一个 Windows 服务器，可以托管多个 RDS 桌面。
- RDS 桌面基于连接到 RDS 主机的会话。与此不同，自动桌面池中的桌面基于虚拟机，手动桌面池中的桌面基于虚拟机或物理机。
- RDS 桌面支持 RDP、PCoIP 和 VMware Blast 显示协议。要启用 HTML Access，请参阅《使用 HTML Access》文档中“设置和安装”一章的“为 HTML Access 准备桌面、池和场”，您可以从以下网址获取此文档：https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html。
- 只有支持 RDS 角色且受 View 支持的 Windows Server 操作系统上才支持 RDS 桌面池。请参阅《View 安装指南》文档中的“客户机操作系统的系统要求”。
- View 通过将连接请求定向到活动会话数最少的 RDS 主机，为场中的 RDS 主机提供负载平衡。
- 由于 RDS 桌面池提供基于会话的桌面，因此它不支持链接克隆桌面池特有的操作，如刷新、重构和重新平衡。
- 如果 RDS 主机是由 vCenter Server 管理的虚拟机，您可以使用快照作为基础映像。您可以使用 vCenter Server 管理快照。在 RDS 主机虚拟机上使用快照对于 View 来说是透明的。
- RDS 桌面不支持 View Persona Management。

- 默认情况下，HTML Access 中禁用复制和粘贴功能。要启用此功能，请参阅《使用 HTML Access》文档中“为最终用户配置 HTML Access”章节中的“HTML Access 组策略设置”，网址为 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html。

创建 RDS 桌面池

可在为用户授予对 RDS 桌面的访问权限的过程中创建 RDS 桌面。

前提条件

- 设置 RDS 主机。请参阅第 8 章 设置远程桌面服务主机。
- 创建包含 RDS 主机的场。请参阅第 9 章 创建场。
- 确定如何配置池设置。请参阅适用于 RDS 桌面池的桌面池设置。

步骤

- 1 在 View Administrator 中，选择目录 > 桌面池。
- 2 单击添加。
- 3 选择 RDS 桌面池。
- 4 提供池 ID、显示名称和描述。

池 ID 是用于在 View Administrator 中标识池的唯一名称。显示名称是用户登录到 Horizon Client 时看到的 RDS 桌面池的名称。如果您未指定显示名称，该名称将与池 ID 相同。

- 5 选择池设置。
- 6 为该池选择或创建一个场。

在 View Administrator 中，您现在可以通过选择目录 > 桌面池来查看 RDS 桌面池。

后续步骤

授予用户访问池的权限。请参阅为桌面池或应用程序池添加授权。

请确保最终用户有权访问 Horizon Client 3.0 或更高版本软件，对 RDS 桌面池提供支持需要这些软件。

适用于 RDS 桌面池的桌面池设置

您可以在创建 RDS 桌面池时指定特定的池设置。并非所有池设置都适用于所有类型的桌面池。

有关所有池设置的描述，请参阅适用于所有桌面池类型的桌面池设置。以下池设置适用于 RDS 桌面池。

表 11-1. 适用于 RDS 桌面池的设置

设置	默认值
状态	已启用
连接服务器限制	无

设置	默认值
Adobe Flash 质量	不进行控制
Adobe Flash 调节	已禁用

为 RDS 桌面池配置 Internet Explorer 中的 Adobe Flash 调节

为确保在 RDS 桌面中 Adobe Flash 调节可以与 Internet Explorer 共用，用户必须启用第三方浏览器扩展。

步骤

- 1 启动 Horizon Client 并登录到一个用户的桌面。
- 2 在 Internet Explorer 中，单击**工具 > Internet 选项**。
- 3 单击**高级**选项卡，选择**启用第三方浏览器扩展**，单击**确定**。
- 4 重新启动 Internet Explorer。

置备桌面池

创建桌面池时，您需要选择配置选项，从而确定池的管理方式，以及用户与桌面的交互方式。

这些置备任务适用于在单用户计算机上置备的桌面池，不适用于 RDS 桌面池。但是，Adobe Flash 质量和调节设置适用于所有桌面池类型，包括 RDS。

本章讨论了以下主题：

- 桌面池中的用户分配
- 手动命名计算机或提供命名模式
- 手动自定义计算机
- 适用于所有桌面池类型的桌面池设置
- Adobe Flash 质量和调节
- 为桌面池设置电源策略
- 为桌面配置 3D 呈现
- 阻止通过 RDP 访问 View 桌面
- 部署大型桌面池

桌面池中的用户分配

对于完整虚拟机或 View Composer 链接克隆的手动桌面池和自动桌面池，您可以为桌面选择浮动或专用用户分配。对于即时克隆桌面池，您只能选择浮动用户分配。

通过专用分配，可以将每个桌面分配给特定用户。首次登录的用户会获得一个未分配给其他用户的桌面。之后在登录后，该用户将始终获得此桌面，并且任何其他用户都不能使用此桌面。

通过浮动分配，用户会在每次登录时获得一个随机桌面。用户注销时，该桌面会返回到池。

对于即时克隆，用户注销时桌面会始终被删除，并从当前映像重新进行创建。对于 View Composer 链接克隆，您可以配置在用户注销时要删除的浮动分配计算机。通过自动删除，可以每次只保留您需要的虚拟机数量。

使用浮动分配，您也许能够降低软件许可成本。

手动命名计算机或提供命名模式

对于完整虚拟机或 View Composer 链接克隆的自动桌面池，您可以为桌面计算机指定一系列名称或提供命名模式。对于即时克隆桌面池，您只能在置备池时指定命名模式。

如果通过指定列表来命名计算机，您可以使用公司的命名方案，并且可以将每个计算机名称与一个用户相关联。

如果您提供了命名模式，View 可以根据用户的需要动态创建和分配计算机。

[表 12-1. 手动命名计算机或提供计算机命名模式](#) 对两种命名方法进行了比较，显示了两种方法对桌面池的创建和管理方式的影响。

表 12-1. 手动命名计算机或提供计算机命名模式

功能	使用计算机命名模式	手动命名计算机
计算机名称	<p>通过将一个数字附加到命名模式后面来生成计算机名称。</p> <p>有关详细信息，请参阅自动桌面池使用命名模式。</p>	<p>您要指定一个计算机名称列表。</p> <p>在专用分配池中，您可以通过列出用户名和计算机名称将用户与计算机配对。</p> <p>有关详细信息，请参阅指定计算机名称列表。</p>
池大小	您要指定计算机的最大数量。	您指定的计算机名称列表决定计算机的数量。
向池中添加计算机	您可以增加池大小的上限。	<p>您可以向列表中添加计算机名称。</p> <p>有关详细信息，请参阅将计算机添加到通过名称列表置备的自动池中。</p>
按需置备	<p>可用。</p> <p>在用户首次登录时或者当您计算机分配给用户时，View 会动态创建和置备指定的最小数量与备用数量的计算机。</p> <p>View 还可以在您创建池时创建和置备所有计算机。</p>	<p>不可用。</p> <p>View 创建和置备您在创建池时在列表中指定的所有计算机。</p>
初始自定义	<p>可用。</p> <p>置备计算机后，View 可以运行您选择的自定义规范。</p>	<p>可用。</p> <p>置备计算机后，View 可以运行您选择的自定义规范。</p>
手动自定义专用计算机	<p>不可用于即时克隆。</p> <p>要自定义计算机并将桌面访问权限返回给用户，您必须移除并重新分配每个计算机的所有权。根据是否在首次登录时分配计算机，您可能需要将这些步骤执行两次。您不能在维护模式下启动计算机。创建池后，您可以手动将计算机置于维护模式。</p>	<p>您可以在不重新分配所有权的情况下对计算机进行自定义和测试。</p> <p>创建池时，您可以在维护模式下启动所有计算机，以阻止用户访问。您可以自定义这些计算机，然后退出维护模式，将访问权返回给用户。</p> <p>有关详细信息，请参阅手动自定义计算机。</p>

功能	使用计算机命名模式	手动命名计算机
动态或固定的池大小	<p>动态。</p> <p>如果从专用分配池中的某个计算机移除用户分配，该计算机将被返回到可用计算机池。</p> <p>如果您在浮动分配池中选择注销后删除计算机，那么根据活动用户会话的数量，池大小可能会增大或缩小。</p> <p>注 即时克隆池只能为浮动分配池。计算机始终会在注销时被删除。</p>	<p>固定。</p> <p>池中包含的计算机数量取决于您在计算机名称列表中提供的信息。</p> <p>如果您手动命名计算机，则不能选择注销后删除计算机设置。</p>
备用计算机	<p>您可以指定一些备用计算机，View 会使这些计算机保持开机状态，以供新用户使用。</p> <p>View 会创建新的计算机以维持指定的数量。池的大小达到上限后，View 将停止创建备用计算机。</p> <p>View 将使备用计算机保持开机状态，即便池的电源策略为关闭或挂起，或者您并未设置电源策略，也都是如此。</p> <p>注 即时克隆池没有电源策略。</p>	<p>您可以指定一些备用计算机，View 会使这些计算机保持开机状态，以供新用户使用。</p> <p>View 不会创建新的备用计算机来维持指定的数量。</p> <p>View 将使备用计算机保持开机状态，即便池的电源策略为关闭或挂起，或者您并未设置电源策略，也都是如此。</p>
用户分配	<p>您可以为专用分配池和浮动分配池使用命名模式。</p> <p>注 即时克隆池只能为浮动分配池。</p>	<p>您可以为专用分配池和浮动分配池指定计算机名称。</p> <p>注 在浮动分配池中，您不能将用户名与计算机名称相关联。计算机不会专供关联的用户使用。在浮动分配池中，当前未处于使用状态的所有计算机均可供登录的用户访问。</p>

指定计算机名称列表

您可以通过手动指定计算机名称列表来置备自动桌面池。此命名方法允许您使用自己公司的命名约定来标识池中的计算机。

如果您明确指定计算机名称，那么用户登录其远程桌面时将看到基于其所在公司组织的熟悉名称。

按照以下指南手动指定计算机名称：

- 每个计算机名称都输入到单独的一行中。
- 计算机名称最多可以包含 15 个字母数字字符。
- 可以在每个计算机条目中添加一个用户名。使用逗号将用户名与计算机名称隔开。

在此示例中指定了两个计算机。第二个计算机与某个用户关联：

```
Desktop-001
Desktop-002,abccorp.com\jdoe
```

注 在浮动分配池中，您不能将用户名与计算机名称相关联。计算机不会专供关联的用户使用。在浮动分配池中，当前未处于使用状态的所有计算机均可供登录的用户访问。

前提条件

确保每个计算机名称都是唯一的。不能使用 vCenter Server 中现有虚拟机的名称。

步骤

- 1 创建一个包含计算机名称列表的文本文件。

如果要创建仅包含几个计算机的桌面池，您可以直接在**添加桌面池**向导中键入计算机名称。而不必创建单独的文本文件。

- 2 在 View Administrator 中，启动**添加桌面池**向导，开始创建自动桌面池。

- 3 在“置备设置”页面上，选择**手动指定名称**，然后单击**输入名称**。

- 4 复制**输入计算机名称**页面中的计算机名称列表，然后单击**下一步**。

输入计算机名称向导将显示桌面列表，并用红色的！来表明验证错误。

- 5 更正无效的计算机名称。

- a 将鼠标放置在无效名称上方，页面底部会显示相关的错误消息。

- b 单击**返回**。

- c 编辑该错误名称，然后单击**下一步**。

- 6 单击**完成**。

- 7 （可选）选择**在维护模式下启动计算机**。

利用此选项，您可以先自定义计算机，然后再允许用户登录和使用计算机。

- 8 按照向导中的提示完成桌面池的创建。

View 会为列表中的每个名称创建一个计算机。对于包含计算机和用户名的条目，View 会将该计算机分配给条目中的用户。

创建桌面池之后，您可以导入另一个包含其他计算机名称和用户的列表文件，从而添加更多计算机。请参阅《View 管理指南》文档中的“将计算机添加到通过名称列表置备的自动池中”。

为自动桌面池使用命名模式

您可以置备池中的计算机，方法是提供命名模式以及池中所需的计算机总数。默认情况下，View 将提供的模式用作所有计算机名称的前缀，并附加一个唯一的编号，以标识每个计算机。

计算机名称中命名模式的长度

计算机名称限制为 15 个字符，其中包括命名模式和自动生成的编号。

表 12-2. 计算机名称中命名模式的最大长度

设置的池中计算机数	最大前缀长度如下
1-99	13 个字符
100-999	12 个字符
1,000 或更多	11 个字符

包含固定长度令牌的名称具有不同的长度限制。请参阅[使用固定长度令牌时的命名模式长度](#)。

在计算机名称中使用令牌

通过使用令牌，您可以将自动生成的编号放置在名称中的任何位置。当您键入池名称时，需要在大括号中键入 **n** 来指定令牌。

例如：**amber-{n}-desktop**

创建计算机时，View 会将 **{n}** 替换为一个唯一编号。

您可以通过键入 **{n:fixed=位数}** 来生成一个固定长度的令牌。

View 将令牌替换为包含指定位数的编号。

例如，如果您键入 **amber-{n:fixed=3}**，View 会将 **{n:fixed=3}** 替换为一个三位编号，并创建以下计算机名称：**amber-001**、**amber-002** 和 **amber-003** 等等。

使用固定长度令牌时的命名模式长度

包括命名模式和令牌位数在内，包含固定长度令牌的名称的长度不能超过 15 个字符。

表 12-3. 使用固定长度令牌时的命名模式最大长度

固定长度的令牌	命名模式的最大长度
{n:fixed=1}	14 个字符
{n:fixed=2}	13 个字符
{n:fixed=3}	12 个字符

计算机命名示例

此示例显示了如何创建两个使用相同计算机名称，但各有一组不同编号的自动桌面池。此示例中使用的策略实现了具体的用户目标并展示了计算机命名方法的灵活性。

我们的目标是创建两个具有相同命名约定的池，如 **VDIABC-XX**，其中 **XX** 代表编号。每个池具有一组不同的顺序编号。例如，第一个池包含的计算机可能是 **VDIABC-01** 到 **VDIABC-10**，第二个池包含的计算机可能是 **VDIABC-11** 到 **VDIABC-20**。

您可以使用任意一种计算机命名方法来实现此目标。

- 要一次创建多组固定的计算机，请手动指定计算机名称。
- 要在用户首次登录时动态创建计算机，请提供一种命名模式，并使用令牌指定顺序编号。

手动指定名称

- 1 为第一个池（包含从 VDIABC-01 到 VDIABC-10 的计算机名称列表）准备一个文本文件。
- 2 在 View Administrator 中，创建池并手动指定计算机名称。
- 3 单击**输入名称**并将您的列表复制到**输入计算机名称**列表框中。
- 4 对第二个池（使用桌面名称 VDIABC-11 到 VDIABC-20）重复这些步骤。

有关详细说明，请参阅[指定计算机名称列表](#)。

您可以在创建每个池后向其中添加计算机。例如，您可以将计算机 VDIABC-21 到 VDIABC-30 添加到第一个池中，将 VDIABC-31 到 VDIABC-40 添加到第二个池中。请参阅[将计算机添加到通过名称列表置备的自动池中](#)。

使用令牌提供命名模式

- 1 在 View Administrator 中，创建第一个池，并使用命名模式置备计算机名称。
- 2 在命名模式文本框中键入 **VDIABC-0{n}**。
- 3 将池的最大大小限定为 9。
- 4 对第二个池重复这些步骤，但在命名模式文本框中键入 **VDIABC-1{n}**。

第一个池将包含计算机 VDIABC-01 到 VDIABC-09，第二个池将包含计算机 VDIABC-11 到 VDIABC-19。

也可以通过使用 2 位数的固定长度令牌，将每个池配置为最多包含 99 个计算机：

- 对于第一个池，键入 **VDIABC-0{n:fixed=2}**。
- 对于第二个池，键入 **VDIABC-1{n:fixed=2}**。

将每个池的最大大小限定为 99。此配置生成的计算机将具有 3 位数的顺序命名模式。

第一个池：

```
VDIABC-001  
VDIABC-002  
VDIABC-003
```

第二个池：

```
VDIABC-101  
VDIABC-102  
VDIABC-103
```

有关命名模式和令牌的详细信息，请参阅[为自动桌面池使用命名模式](#)。

将计算机添加到通过名称列表置备的自动池中

要将计算机添加到通过手动指定计算机名称置备的自动桌面池，应另外提供一个新计算机名称的列表。利用此功能，您可以扩展桌面池并继续使用您公司的命名约定。

在 Horizon 7.0 中，即时克隆不支持此功能。

手动添加计算机名称时请遵循以下准则：

- 每个计算机名称都输入到单独的一行中。
- 计算机名称最多可以包含 15 个字母数字字符。
- 可以在每个计算机条目中添加一个用户名。使用逗号将用户名与计算机名称隔开。

在本例中，添加了两个计算机。第二个计算机与某个用户关联：

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

注 在浮动分配池中，您不能将用户名与计算机名称相关联。计算机不会专供关联的用户使用。在浮动分配池中，当前未处于使用状态的所有计算机均可供登录的用户访问。

前提条件

验证是否通过手动指定计算机名称创建了桌面池。如果通过提供命名模式创建了池，则无法通过提供新计算机名称添加计算机。

步骤

- 1 创建一个文本文件，其中包含附加计算机名称的列表。

如果只打算添加几个计算机，可以直接在**添加桌面池**向导中键入计算机名称。而不必创建单独的文本文件。

- 2 在 View Administrator 中，选择**目录 > 桌面池**。

- 3 选择要扩展的桌面池。

- 4 单击**编辑**。

- 5 单击**置备设置**选项卡。

- 6 单击**添加计算机**。

- 7 复制**输入计算机名称**页面中的计算机名称列表，然后单击**下一步**。

输入计算机名称向导显示计算机列表，并用一个红色的 **X** 指示验证错误。

- 8 更正无效的计算机名称。

a 将鼠标放置在无效名称上方，页面底部会显示相关的错误消息。

b 单击**返回**。

c 编辑该错误名称，然后单击**下一步**。

- 9 单击**完成**。

- 10 单击**确定**。

在 vCenter Server 中，您可以监视新虚拟机的创建操作。

在 View Administrator 中，您可以在将计算机添加到桌面池时查看这些计算机，通过选择**目录 > 桌面池**便可实现此操作。

手动自定义计算机

创建自动池后，您可以自定义特定的计算机而无需重新分配所有权。通过在维护模式下启动计算机，您可以在将计算机发布给用户之前对计算机进行修改和测试。

注 此功能不可用于即时克隆桌面池。

在维护模式下自定义计算机

维护模式阻止用户访问桌面。如果您在维护模式下启动计算机，View 会在创建计算机后将每个计算机置于维护模式下。

在专用分配池中，您可以使用维护模式登录计算机，而无需为自己的管理员帐户重新分配所有权。完成自定义后，不必将所有权交还给为计算机分配的用户。

在浮动分配池中，您可以先在维护模式下测试计算机，然后再让用户登录。

要对自动池中的所有计算机进行同样的自定义，可以先对准备作为模板或父虚拟机的虚拟机进行自定义。View 会将您的自定义内容部署到所有计算机。创建池时，您也可以使用 Sysprep 自定义规范为所有计算机配置许可、域附属、DHCP 设置以及其他计算机属性。

注 当您为池手动指定计算机名称，而不是通过提供命名模式来命名计算机时，可以在维护模式下启动计算机。

自定义单个计算机

创建池之后，您可以通过在维护模式下启动计算机来自定义各个计算机。

步骤

- 1 在 View Administrator 中，启动**添加桌面池**向导开始创建自动桌面池。
- 2 在“置备设置”页面上，选择**手动指定名称**。
- 3 选择在**维护模式下启动计算机**。
- 4 完成**添加桌面池**向导以完成创建桌面池。
- 5 在 vCenter Server 中，登录、自定义并测试各个虚拟机。

您可以手动自定义计算机，也可以使用标准的 Windows 系统管理软件（如 Altiris、SMS、LanDesk 或 BMC）来进行自定义。

- 6 在 View Administrator 中，选择所需的桌面池。
- 7 使用过滤工具选择要发布给用户的特定计算机。
- 8 单击**更多命令 > 退出维护模式**。

后续步骤

通知用户他们可以登录桌面。

适用于所有桌面池类型的桌面池设置

在配置包含完整虚拟机的自动池、链接克隆桌面池、手动桌面池、即时克隆桌面池和 RDS 桌面池时，必须指定计算机和桌面池设置。并非所有设置都适用于所有类型的桌面池。

表 12-4. 桌面池设置描述

设置	选项
状态	<ul style="list-style-type: none"> ■ 已启用。桌面池创建后将自动启用，并可以立即投入使用。 ■ 已禁用。桌面池在创建完成后将被禁用且无法使用，池的置备也将停止。如果要执行部署后的活动，如测试或其他形式的基准维护，则该设置很适用。 <p>当此状态生效时，远程桌面不可用。</p>
连接服务器限制	<ul style="list-style-type: none"> ■ 无。任何连接服务器实例均可以访问桌面池。 ■ 带有标记。选择一个或多个连接服务器标签，可仅允许带有这些标签的连接服务器实例访问桌面池。您可以使用复选框选择多个标签。 <p>如果您想通过 VMware Identity Manager 提供桌面访问，并且配置了连接服务器限制，则当桌面实际受到限制时，VMware Identity Manager 应用程序可能会向用户显示这些桌面。VMware Identity Manager 用户将无法启动这些桌面。</p>
远程计算机电源策略	<p>确定用户从关联的桌面注销后该虚拟机的行为方式。</p> <p>有关电源策略选项的描述，请参阅桌面池的电源策略。</p> <p>有关电源策略对自动池的影响的更多信息，请参阅为桌面池设置电源策略。</p> <p>不适用于即时克隆桌面池。即时克隆始终处于电源打开状态。</p>
断开连接后自动注销	<ul style="list-style-type: none"> ■ 立即。用户在断开连接后立即注销。 ■ 从不。永不注销用户。 ■ 之后。用户断开连接的时间超过此设置后即注销。键入持续时间（以分钟为单位）。 <p>注销时间适用于以后断开的连接。如果在设置注销时间时桌面会话已经断开，则该用户的注销持续时间以设置注销时间的时刻为起点，而不是会话断开的时刻。例如，如果您将此值设置为五分钟，而会话在 10 分钟前断开，View 将会在您设置完该值的五分钟后注销本次会话。</p>
允许用户重置其计算机	<p>允许用户重置其自己的桌面。</p> <p>不适用于即时克隆桌面池。</p>
允许用户从不同的客户端设备启动单独的会话	<p>选择该设置时，从不同的客户端设备连接到同一桌面池的用户将获取不同的桌面会话。用户只能从启动该会话的客户端设备重新连接到现有的会话。未选择该设置时，用户可以使用任意客户端设备重新连接到其现有的会话。</p>
注销后删除计算机	<p>选择是否删除浮动分配的完整虚拟机。</p> <ul style="list-style-type: none"> ■ 否。用户注销后，虚拟机保留在桌面池中。 ■ 是。用户注销后立即关闭并删除虚拟机。 <p>对于即时克隆桌面，注销后始终会删除并重新创建计算机。</p>
注销时删除或刷新计算机	<p>选择将浮动分配链接克隆虚拟机删除、刷新还是保持不变。</p> <ul style="list-style-type: none"> ■ 从不。用户注销后，虚拟机保留在池中而不进行刷新。 ■ 立即删除。用户注销后立即关闭并删除虚拟机。用户注销时，虚拟机会立即进入正在删除状态。 ■ 立即刷新。用户注销后立即刷新虚拟机。用户注销时，虚拟机会立即进入维护模式，以防止其他用户在刷新操作开始时登录。 <p>对于即时克隆桌面，注销后始终会删除并重新创建计算机。</p>

设置	选项						
注销后刷新操作系统磁盘	<p>选择是否以及何时刷新专用分配链接克隆虚拟机的操作系统磁盘。</p> <ul style="list-style-type: none"> ■ 从不。从不刷新操作系统磁盘。 ■ 始终。用户每次注销时均刷新操作系统磁盘。 ■ 间隔时间。操作系统磁盘在指定的时间间隔（以天为单位）定期刷新。键入天数。 <p>天数将从最后一次刷新开始计算，如未进行过刷新，则从最初置备开始计算。例如，如果指定的值为 3 天，而且从上次刷新开始算起已超过 3 天，那么计算机将在用户注销后刷新。</p> <ul style="list-style-type: none"> ■ 特定量。当操作系统磁盘当前的容量达到其允许的最大容量的指定百分比时，刷新该操作系统磁盘。链接克隆操作系统磁盘的最大容量就是副本操作系统磁盘的容量。键入启动刷新操作的百分比。 <p>使用 特定量 选项时，数据存储中的链接克隆操作系统的大小将与允许的最大容量进行对比。磁盘利用率百分比不能反映您在计算机客户机操作系统中看到的磁盘使用情况。</p> <p>刷新专用分配链接克隆池中的操作系统磁盘时，View Composer 永久磁盘不受影响。</p> <p>对于即时克隆桌面，注销后始终会删除并重新创建计算机。</p>						
默认显示协议	<p>选择您希望连接服务器与客户端进行通信时使用的显示协议。</p> <table> <tr> <td>VMware Blast</td><td>VMware Blast Extreme 协议构建于 H.264 协议之上，支持任何网络中最广泛的客户端设备，包括智能手机、平板电脑、超低成本 PC 和 Mac。此协议具有最低的 CPU 资源消耗率，因此能够延长移动设备上的电池寿命。</td></tr> <tr> <td>PCoIP</td><td>受支持情况下的默认选项。PCoIP 可作为具有 Teradici 硬件的虚拟机和物理机的显示协议。PCoIP 为 LAN 或 WAN 中的广大用户提供了交付的图像、音频和视频内容方面的最佳 PC 体验。</td></tr> <tr> <td>Microsoft RDP</td><td>Microsoft 远程桌面连接 (RDC) 使用 RDP 来传输数据。RDP 是一种允许用户远程连接计算机的多通道协议。</td></tr> </table>	VMware Blast	VMware Blast Extreme 协议构建于 H.264 协议之上，支持任何网络中最广泛的客户端设备，包括智能手机、平板电脑、超低成本 PC 和 Mac。此协议具有最低的 CPU 资源消耗率，因此能够延长移动设备上的电池寿命。	PCoIP	受支持情况下的默认选项。PCoIP 可作为具有 Teradici 硬件的虚拟机和物理机的显示协议。PCoIP 为 LAN 或 WAN 中的广大用户提供了交付的图像、音频和视频内容方面的最佳 PC 体验。	Microsoft RDP	Microsoft 远程桌面连接 (RDC) 使用 RDP 来传输数据。RDP 是一种允许用户远程连接计算机的多通道协议。
VMware Blast	VMware Blast Extreme 协议构建于 H.264 协议之上，支持任何网络中最广泛的客户端设备，包括智能手机、平板电脑、超低成本 PC 和 Mac。此协议具有最低的 CPU 资源消耗率，因此能够延长移动设备上的电池寿命。						
PCoIP	受支持情况下的默认选项。PCoIP 可作为具有 Teradici 硬件的虚拟机和物理机的显示协议。PCoIP 为 LAN 或 WAN 中的广大用户提供了交付的图像、音频和视频内容方面的最佳 PC 体验。						
Microsoft RDP	Microsoft 远程桌面连接 (RDC) 使用 RDP 来传输数据。RDP 是一种允许用户远程连接计算机的多通道协议。						
允许用户选择协议	允许用户使用 Horizon Client 覆盖其桌面的默认显示协议。						
3D 呈现器	<p>如果池包含 Windows 7 或更高版本桌面，则您可以选择是否启用 3D 图形呈现。根据安装在 ESXi 5.1 或更高版本主机上的物理 GPU 显卡，您可配置 3D 呈现器 使用软件呈现或硬件呈现。</p> <p>要启用此功能，您必须选择 PCoIP 或 VMware Blast 作为协议，并禁用 允许用户选择协议 设置（选择否）。使用基于硬件的 3D 呈现器 选项，用户可利用图形应用程序执行设计、建模和多媒体操作。使用软件 3D 呈现器 选项，用户可以利用诸如 AERO、Microsoft Office 和 Google Earth 之类的要求相对低一些的应用程序中的图形增强功能。有关系统要求，请参阅为桌面配置 3D 呈现。</p> <p>如果您的 View 部署不是运行在 vSphere 5.0 或更高版本中，此设置会不可用，且在 View Administrator 中会处于非活动状态。</p> <p>在选择该功能时，如果选择自动、软件或硬件选项，则可以配置为池中的计算机分配的 VRAM 量。最大显示器数为 2 个，最大分辨率为 1920 x 1200。</p> <p>如果选择使用 vSphere Client 管理或 NVIDIA GRID vGPU，则必须在 vCenter Server 中配置 3D 内存量和显示器数。您可以为用作远程桌面的计算机选择最多四个显示器，具体取决于显示器分辨率。</p> <p>注 在配置或编辑此设置后，必须关闭现有虚拟机的电源，确认在 vCenter Server 中重新配置了这些计算机，然后打开其电源以使新设置生效。重新启动虚拟机不会使新设置生效。</p> <p>有关详细信息，请参阅为桌面配置 3D 呈现、3D 呈现器选项和配置 3D 呈现的最佳实践。</p> <p>不适用于即时克隆桌面池。</p>						

设置	选项
显示器最大数量	<p>如果选择 PCoIP 或 VMware Blast 作为显示协议，您可以选择用户用于显示桌面的显示器最大数量。您最多可以选择四个显示器。</p> <p>如果未选择 3D 呈现器 设置，显示器最大数量 设置将影响分配到池中计算机的 VRAM 大小。当您增加显示器数量时，相关联的 ESXi 主机将会消耗更多的内存。</p> <p>如果未选择 3D 呈现器 设置，禁用了 Aero 的 Windows 7 客户机操作系统在 3840x2160 分辨率下最多支持三个显示器。对于其他操作系统或启用了 Aero 的 Windows 7，在 3840x2160 分辨率下支持一个显示器。</p> <p>如果选择了 3D 呈现器 设置，在 3840x2160 分辨率下支持一个显示器。在较低的分辨率下，可以较好地支持多个显示器。如果选择较高的分辨率，请选择较少的显示器。</p> <p>注 您必须关闭并重新启动现有的虚拟机，才能使该设置生效。重新启动虚拟机不会使设置生效。</p> <p>不适用于即时克隆桌面池。在 Horizon 7.0 中，可用于即时克隆的最大显示器数量为 2 台。</p>
任意一台显示器的最大分辨率	<p>如果选择 PCoIP 或 VMware Blast 作为显示协议，您应该指定任意一台显示器的最大分辨率。默认情况下，任意一台显示器的最大分辨率 设置为 1920x1200 像素，但您可以配置该值。</p> <p>如果未选择 3D 呈现器 设置，任意一台显示器的最大分辨率 设置将影响分配给池中的计算机的 VRAM 大小。当您分辨率调大后，相关联的 ESXi 主机将会消耗更多的内存。</p> <p>如果未选择 3D 呈现器 设置，禁用了 Aero 的 Windows 7 客户机操作系统在 3840x2160 分辨率下最多支持三个显示器。对于其他操作系统或启用了 Aero 的 Windows 7，在 3840x2160 分辨率下支持一个显示器。</p> <p>如果选择了 3D 呈现器 设置，在 3840x2160 分辨率下支持一个显示器。在较低的分辨率下，可以较好地支持多个显示器。如果选择较高的分辨率，请选择较少的显示器。</p> <p>注 您必须关闭并重新启动现有的虚拟机，才能使该设置生效。重新启动虚拟机不会使设置生效。</p> <p>不适用于即时克隆桌面池。在 Horizon 7.0 中，任意显示器的最大分辨率均为 2560x1600。</p>
HTML Access	<p>选择已启用以允许用户从其 Web 浏览器连接到远程桌面。</p> <p>当用户通过 VMware Horizon Web 门户页面或 VMware Identity Manager 应用程序登录并选择远程桌面时，HTML Access 代理允许用户通过 HTTPS 连接到该桌面。桌面显示在用户的浏览器中。其他的显示协议如 PCoIP 或 RDP 不被使用。无需在客户端设备上安装 Horizon Client 软件。</p> <p>要使用 HTML Access，必须在 View 部署中安装 HTML Access。有关详细信息，请参阅《使用 HTML Access》（可从 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html 获得）。</p> <p>要将 HTML Access 与 VMware Identity Manager 配合使用，必须将连接服务器与 SAML 身份验证服务器进行配对，如《View 管理指南》文档中所述。必须安装并配置 VMware Identity Manager，才能与连接服务器一起使用。</p>
Adobe Flash 质量	<p>确定网页中显示的 Adobe Flash 内容的质量。</p> <ul style="list-style-type: none"> ■ 不进行控制：质量是由网页设置确定的。 ■ 低：此设置节省的带宽最多。如果未指定质量级别，系统会默认选用“低”。 ■ 中：此设置节省的带宽适中。 ■ 高：此设置节省的带宽最少。 <p>有关更多信息，请参阅 Adobe Flash 质量和调节。</p>
Adobe Flash 调节	<p>确定 Adobe Flash 影片的帧速率。如果启用此设置，您可以通过选择激进级别减少或增加每秒显示的帧数。</p> <ul style="list-style-type: none"> ■ 已禁用：不执行调节。不修改计时器间隔。 ■ 保守：计时器间隔为 100 毫秒。此设置可以使丢帧数达到最小。 ■ 适中：计时器间隔为 500 毫秒。 ■ 激进：计时器间隔为 2500 毫秒。此设置可以使丢帧数达到最大。 <p>有关更多信息，请参阅 Adobe Flash 质量和调节。</p>

设置	选项
覆盖全局 Mirage 设置	要为所有桌面池指定同一 Mirage 服务器，请使用全局 View 配置设置，而不要使用这个特定于池的设置。不适用于即时克隆桌面池。
Mirage 服务器配置	<p>允许您使用 <code>mirage://server-name:port</code> 或 <code>mirages://server-name:port</code> 格式指定 Mirage 服务器的 URL。其中的 <i>服务器名称</i> 是完全限定域名。如果不指定端口号，则将使用默认端口号 8000。</p> <p>还可以在 View Administrator 中指定 Mirage 服务器来代替在安装 Mirage 客户端时指定 Mirage 服务器。为确定哪些 Mirage 版本支持在 View Administrator 中指定该服务器，请参阅 Mirage 文档（位于 https://www.vmware.com/support/pubs/mirage_pubs.html）。</p> <p>不适用于即时克隆桌面池。</p>

Adobe Flash 质量和调节

您可以为 Adobe Flash 内容指定可重写网页设置的允许的最高质量级别。如果某个网页的 Adobe Flash 质量高于允许的最高级别，则其质量将会降低到指定的最高级别。较低的质量级别可以节省更多的带宽。

要利用减少 Adobe Flash 带宽的设置，不要在全屏幕模式下运行 Adobe Flash。

表 12-5. Adobe Flash 质量设置 显示了可用的 Adobe Flash 渲染质量设置。

表 12-5. Adobe Flash 质量设置

质量设置	描述
不进行控制	质量是由网页设置确定的。
低	此设置节省的带宽最多。
中	此设置节省的带宽适中。
高	此设置节省的带宽最少。

如果未指定最高质量级别，则系统默认值为低。

Adobe Flash 使用计时器服务更新任意给定时间在屏幕上显示的内容。典型的 Adobe Flash 计时器间隔值为 4 到 50 毫秒之间。通过调节或延长此间隔，您可以减少帧速率，从而减少带宽。

表 12-6. Adobe Flash 调节设置 显示了可用的 Adobe Flash 调节设置。

表 12-6. Adobe Flash 调节设置

调节设置	描述
已禁用	不执行调节。不修改计时器间隔。
保守	计时器间隔为 100 毫秒。此设置可以使丢帧数达到最小。
适中	计时器间隔为 500 毫秒。
激进	计时器间隔为 2500 毫秒。此设置可以使丢帧数达到最大。

无论选择哪种调节设置，音频速度都保持恒定不变。

为桌面池设置电源策略

您可以为桌面池中由 vCenter Server 管理的虚拟机（即时克隆除外）配置电源策略。即时克隆始终处于电源打开状态。

电源策略可控制虚拟机在与其关联的桌面未处于使用中时的行为方式。在用户登录之前，以及用户断开连接或注销之后，桌面会被认为未处于使用中。电源策略还可以控制虚拟机在管理任务（如刷新、重构和重新平衡）完成之后的行为方式。

您可以在 View Administrator 中创建或编辑桌面池时配置电源策略。

注 您无法为拥有未受管计算机的桌面池配置电源策略。

桌面池的电源策略

电源策略控制虚拟机在关联的远程桌面处于未使用状态时的行为。

您在创建或编辑桌面池时设置电源策略。表 12-7. 电源策略介绍了可用的电源策略。

表 12-7. 电源策略

电源策略	说明
不执行任何电源操作	<p>View 在用户注销后不强制执行任何电源策略。此设置有两个结果。</p> <ul style="list-style-type: none">■ View 在用户注销后不更改虚拟机的电源状态。 <p>例如，如果用户关闭虚拟机，则虚拟机将保持关机状态。如果用户注销而没有关机，则虚拟机将保持开机状态。当用户重新连接到桌面时，如果虚拟机已关闭，将重新启动虚拟机。</p> <ul style="list-style-type: none">■ View 在管理任务完成后不强制实现任何电源状态。 <p>例如，用户注销而没有关机，虚拟机将保持开机状态。执行计划的重构时，虚拟机将关闭。重构完成后，View 不会执行任何操作来更改虚拟机的电源状态。虚拟机将保持关机状态。</p>
确保计算机始终打开电源	<p>虚拟机将保持开机状态，即使在未使用时也是如此。如果用户关闭虚拟机，它将立即重新启动。在刷新、重构或重新平衡等管理任务完成后，虚拟机也会重新启动。</p> <p>如果您运行的批处理进程或系统管理工具必须在计划的时间与虚拟机通信，请选择确保计算机始终打开电源。</p>

电源策略	说明
挂起	<p>虚拟机在用户注销后进入挂起状态，但在用户断开连接时不挂起。</p> <p>您也可以将专用池中的计算机配置为在用户断开连接而不注销时挂起。如要配置该策略，您必须在 View LDAP 中设置一个属性。请参阅将专用计算机配置为在用户断开连接后挂起。</p> <p>当多台虚拟机从挂起状态恢复时，某些虚拟机可能会存在开机延迟。是否存在延迟主要取决于 ESXi 主机硬件和 ESXi 主机上所配置的虚拟机数量。从 Horizon Client 连接到桌面的用户可能会暂时收到一条“桌面不可用”的消息。用户可重新连接，以访问其桌面。</p>
关闭	虚拟机在用户注销时关闭，但在用户断开连接时不关闭。

注 当您将计算机添加到手动池时，**View** 会打开该计算机的电源，以确保对其进行完整配置，即使您选择了关闭或不执行任何电源操作电源策略。配置了 **Horizon Agent** 后，它即会被标记为“就绪”，并应用池的一般电源管理设置。

对于由 **vCenter Server** 管理计算机的手动池，**View** 会确保打开备用计算机的电源，以便用户可以连接。无论哪个电源策略有效，备用计算机都会打开电源。

表 12-8. View 何时应用电源策略 说明了 **View** 何时应用配置的电源策略。

表 12-8. View 何时应用电源策略

桌面池类型	应用的电源策略...
包含一个计算机（由 vCenter Server 管理的虚拟机）的手动池	<p>电源操作由会话管理启动。虚拟机在用户请求桌面时开机，并在用户注销时关机或挂起。</p> <p>注 无论单计算机池使用浮动分配还是专用分配，也无论计算机是否已分配，确保计算机始终打开电源策略始终适用。</p>
专用分配自动池	<p>仅应用于未分配的计算机。</p> <p>在已分配的计算机上，电源操作由会话管理启动。虚拟机在用户请求已分配的计算机时开机，在用户注销时关闭电源或挂起。</p> <p>注 确保计算机始终打开电源策略适用于已分配和未分配的计算机。</p>
浮动分配自动池	<p>计算机未在使用时，以及用户注销后。</p> <p>为浮动分配桌面池配置关闭或挂起电源策略时，应将断开连接后自动注销设置为立即，以防止出现丢弃的或孤立的会话。</p>
专用分配手动池	<p>仅应用于未分配的计算机。</p> <p>在已分配的计算机上，电源操作由会话管理启动。虚拟机在用户请求已分配的计算机时开机，在用户注销时关闭电源或挂起。</p> <p>注 确保计算机始终打开电源策略适用于已分配和未分配的计算机。</p>
浮动分配手动池	<p>计算机未在使用时，以及用户注销后。</p> <p>为浮动分配桌面池配置关闭或挂起电源策略时，应将断开连接后自动注销设置为立即，以防止出现丢弃的或孤立的会话。</p>

View 如何向自动池应用配置的电源策略，取决于是否有可用的计算机。请参阅[电源策略如何影响自动桌面池](#)了解更多信息。

将专用计算机配置为在用户断开连接后挂起

挂起电源策略会使虚拟机在用户注销时挂起，而不是在用户断开连接时挂起。您也可以将专用池中的计算机配置为在用户断开桌面连接而不注销时挂起。在用户断开连接时使用挂起功能有助于节约资源。

要为专用计算机启用断开连接时挂起的功能，您必须在 View LDAP 中设置一个属性。

步骤

- 1 在您的 View 连接服务器主机上启动“ADSI 编辑”实用程序。
- 2 在控制台树中，选择**连接到**。
- 3 在**选择或键入域或服务器**字段，键入服务器名称 **localhost:389**
- 4 在**连接点**下，单击**选择或键入可分辨名称或命名上下文**，键入可分辨名称 **DC=vdi,DC=vmware,DC=int**，然后单击**确定**。
将显示“ADAM ADSI 编辑”主窗口。
- 5 展开 ADAM ADSI 树并展开 **OU=Properties**。
- 6 选择 **OU=Global** 并在右侧窗格中选择 **CN=Common**
- 7 选择**操作 > 属性**，在 **pae-NameValuePair** 属性下添加新条目 **suspendOnDisconnect=1**。
- 8 重新启动 VMware Horizon View 连接服务器服务或 View 连接服务器。

电源策略如何影响自动桌面池

View 如何向自动池应用配置的电源策略，取决于是否有可用的计算机。

如果自动池中的计算机符合以下标准，则该计算机即被视为可用：

- 处于活动状态
- 不包含任何用户会话
- 未分配给用户

计算机上运行的 Horizon Agent 服务可确认 View 连接服务器是否可以使用该计算机。

配置自动池时，您可以指定必须置备的最大和最小虚拟机数量，以及在任意给定时间必须保持开启状态并且可用的备用计算机数量。

具有浮动分配的自动池电源策略示例

配置浮动分配的自动池时，可以指定在某个给定时间内可用计算机的数量。无论池策略的设置如何，可用的备用计算机始终保持开启状态。

电源策略示例 1

表 12-9. 具有浮动分配的自动桌面池设置示例 1 介绍了此示例中的浮动分配自动池。该池使用计算机命名模式置备及命名计算机。

表 12-9. 具有浮动分配的自动桌面池设置示例 1

桌面池设置	值
计算机数量 (下限)	10
计算机数量 (上限)	20
备用的已打开电源的计算机数量	2
远程计算机电源策略	关闭

置备该桌面池后，将创建 10 个计算机，其中有两个计算机处于开启状态并随时可用，另外八个计算机处于关闭状态。

每当一个新用户连接到该池时，就会启动一个计算机，以维持可用的备用计算机数量。当连接的用户数量超过八个时，将另外创建计算机（最多创建 20 个），以维持备用计算机的数量。达到最大值后，最早断开连接的两名用户的计算机将保持开启状态，以维持备用计算机的数量。根据电源策略，每个后续用户的计算机都将关闭。

电源策略示例 2

表 12-10. 具有浮动分配的自动桌面池设置示例 2 介绍了此示例中的浮动分配自动池。该池使用计算机命名模式置备及命名计算机。

表 12-10. 具有浮动分配的自动桌面池设置示例 2

桌面池设置	值
计算机数量 (下限)	5
计算机数量 (上限)	5
备用的已打开电源的计算机数量	2
远程计算机电源策略	关闭

置备该桌面池后，将创建五个计算机，其中有两个计算机处于开启状态并随时可用，另外三个计算机处于关闭状态。

如果该池中的第四个计算机关闭，那么某个现有计算机将开启。由于已经达到最大计算机数量，因此不会另外启动计算机。

具有专用分配的自动池电源策略示例

与浮动分配自动池中已打开电源的计算机不同，专用分配自动池中已打开电源的计算机并不一定可用。这类计算机只有在未分配给用户时才可用。

表 12-11. 具有专用分配的自动桌面池设置示例 介绍了此示例中的专用分配自动池。

表 12-11. 具有专用分配的自动桌面池设置示例

桌面池设置	值
计算机数量 (下限)	3
计算机数量 (上限)	5
备用的已打开电源的计算机数量	2
远程计算机电源策略	确保计算机始终打开电源

置备此桌面池时，会创建三个计算机并打开这些计算机的电源。如果在 vCenter Server 中关闭了这些计算机的电源，根据电源策略，将立即再次打开这些计算机的电源。

用户连接到池中某个计算机后，该计算机将永久分配给该用户。用户断开与该计算机的连接后，该计算机将不再对其他任何用户可用。但是，**确保计算机始终打开电源**策略仍然适用。如果在 vCenter Server 中关闭了分配的计算机的电源，将立即再次打开该计算机的电源。

当另一位用户连接时，将为其分配另一个计算机。由于备用计算机数量在第二个用户连接时降至限值以下，因此将再创建一个计算机并打开其电源。每次分配一个新用户时都会另外再创建一个计算机并打开其电源，直到达到最大的计算机数量限值为止。

防止 View 电源策略冲突

使用 View Administrator 配置电源策略时，您必须将电源策略和客户机操作系统“电源选项”控制面板中的设置进行对比，以防止发生电源策略冲突。

如果为计算机配置的电源策略与为客户机操作系统配置的电源选项不兼容，虚拟机可能会临时处于不可访问状态。如果同一池中有其他计算机，这些计算机也会受影响。

以下配置是一个电源策略冲突示例：

- 在 View Administrator 中，电源策略**挂起**是针对虚拟机配置的。此策略将导致虚拟机在不使用时进入挂起状态。
- 在客户机操作系统的“电源选项”控制面板中，**使计算机进入睡眠状态**选项设置为三分钟。

在此配置中，View 连接服务器和客户机操作系统都可以将虚拟机挂起。View 连接服务器期望虚拟机开机时，客户机操作系统的电源选项有可能导致虚拟机不可用。

为桌面配置 3D 呈现

创建或编辑虚拟机的桌面池时，您可以为您的桌面配置 3D 图形呈现。桌面可以利用虚拟共享图形加速 (vSGA)、虚拟专用图形加速 (vDGA) 或共享 GPU 硬件加速 (NVIDIA GRID vGPU)。vDGA 和 NVIDIA

GRID vGPU 是使用 ESXi 主机上安装的物理显卡的 vSphere 功能，并在多个虚拟机之间管理图形处理单元 (GPU) 资源。

注 此功能不可用于 Horizon 7.0 中的即时克隆。

最终用户可利用 3D 应用程序进行设计、建模和多媒体处理 等通常需要 GPU 硬件来执行的操作。对于不需要物理 GPU 的用户，软件选项提供了可支持诸如 Windows AERO、Microsoft Office 和 Google Earth 之类的要求相对低一些的应用程序的图形增强功能。下面是 3D 图形选项的简要描述：

NVIDIA GRID vGPU（共享 GPU 硬件加速）

该功能在 vSphere 6.0 和更高版本中提供，其允许多个虚拟机共享 ESXi 主机上的物理 GPU。此功能提供了从轻量级 3D 任务工作者到高端工作站图形超级用户的灵活硬件加速 3D 配置文件。

采用 vDGA 的 AMD 多用户 GPU

此功能随 vSphere 6.0 及更高版本一起提供，可使一个 AMD GPU 显示为多个 PCI 直通设备，从而允许多个虚拟机共享此 AMD GPU。此功能提供了从轻量级 3D 任务工作者到高端工作站图形超级用户的灵活硬件加速 3D 配置文件。

虚拟专用图形加速 (vDGA)

该功能在 vSphere 5.5 和更高版本中提供，其将 ESXi 主机上的单个物理 GPU 专用于单个虚拟机。如果需要高端硬件加速的工作站图形，可以使用该功能。

注 某些 Intel vDGA 卡需要特定的 vSphere 6 版本。请参阅位于 <http://www.vmware.com/resources/compatibility/search.php> 的《VMware 硬件兼容性列表》。此外，对于 Intel vDGA，使用的是 Intel 集成的 GPU 而不是分离式 GPU，其他供应商的情况也是如此。

虚拟共享图形加速 (vSGA)

该功能在 vSphere 5.1 和更高版本中提供，其允许多个虚拟机共享 ESXi 主机上的物理 GPU。该功能适用于中等程度的 3D 设计、建模和多媒体应用程序。

软 3D

软件加速的图形在 vSphere 5.0 和更高版本中提供，其允许您运行 DirectX 9 和 OpenGL 2.1 应用程序，而无需使用物理 GPU。对于要求不高的 3D 应用程序（如 Windows Aero 主题、Microsoft Office 2010 和 Google Earth）可以使用该功能。

由于 NVIDIA GRID vGPU、采用 vDGA 的 AMD 多用户 GPU 和所有 vDGA 解决方案在 ESXi 主机上使用 PCI 直通，因此不支持实时 VMotion。vSGA 和软 3D 支持实时 VMotion。

在某些情况下，如果应用程序（例如视频游戏或 3D 基准测试程序）强制桌面以全屏分辨率显示，则桌面会话可能会断开连接。可使用以下解决方法：将应用程序设置为在窗口模式下运行，或者将 View 会话桌面分辨率与应用程序所期望的默认分辨率匹配。

所有类型的 3D 呈现的要求

要启用 3D 图形呈现，您的池部署必须满足以下要求：

- 虚拟机必须为 Windows 7 或更高版本。

- 池必须使用 PCoIP 或 VMware Blast Extreme 作为默认显示协议。
- 不允许用户选择自己的协议。

重要事项 在配置或编辑 **3D 呈现器** 设置时，您必须关闭现有虚拟机的电源，确认已在 vCenter Server 中重新配置了虚拟机，然后重新打开虚拟机电源以使新的设置生效。重新启动虚拟机不会使新设置生效。

NVIDIA GRID vGPU 的其他要求

使用 NVIDIA GRID vGPU，多个虚拟机可以共享 ESXi 主机上的单个物理 GPU。要支持此类型的共享 GPU 硬件加速，池必须满足以下其他要求：

- 虚拟机必须在 ESXi 6.0 或更高版本的主机上运行，使用虚拟硬件版本 11 或更高版本，并由 vCenter Server 6.0 或更高版本的软件进行管理。

在 View 中创建桌面池之前，必须将父虚拟机或虚拟机模板配置为使用共享 PCI 设备。有关详细说明，请参阅《适用于 VMware Horizon 6.1 的 NVIDIA GRID vGPU 部署指南》。

- 必须在虚拟机的客户机操作系统中安装来自 GPU 供应商的图形驱动程序。

注 有关支持的 GPU 硬件的列表，请参阅位于 <http://www.vmware.com/resources/compatibility/search.php> 的《VMware 硬件兼容性列表》。

- 必须在 View Administrator 中将 **3D 呈现器** 选项设置为 **NVIDIA GRID vGPU**。

采用 vDGA 的 AMD 多用户 GPU 的其他要求

通过使用采用 vDGA 的 AMD 多用户 GPU，可使一个 AMD GPU 显示为多个 PCI 直通设备，从而允许多个虚拟机共享此 AMD GPU。要支持此类型的共享 GPU 硬件加速，池必须满足以下其他要求：

- 虚拟机必须在 ESXi 6.0 或更高版本的主机上运行，使用虚拟硬件版本 11 或更高版本，并由 vCenter Server 6.0 或更高版本的软件进行管理。
- 您必须在 ESXi 主机上启用 GPU 直通，配置 AMD SR-IOV（单根 I/O 虚拟化），并将单个虚拟机配置为使用专用 PCI 设备。请参阅[准备使用采用 vDGA 的 AMD 多用户 GPU 功能](#)。

注 此版本仅支持手动桌面池。

- 必须在虚拟机的客户机操作系统中安装来自 GPU 供应商的图形驱动程序。

注 有关支持的 GPU 硬件的列表，请参阅位于 <http://www.vmware.com/resources/compatibility/search.php> 的《VMware 硬件兼容性列表》。

- 必须在 View Administrator 中将 **3D 呈现器** 选项设置为使用 **vSphere Client 管理**。

使用 vDGA 的其他要求

vDGA 将 ESXi 主机上的一个物理 GPU 专用于一个虚拟机。要支持 vDGA，池必须满足以下其他要求：

- 虚拟机必须在 ESXi 5.5 或更高版本的主机上运行，使用虚拟硬件版本 9 或更高版本，并由 vCenter Server 5.5 或更高版本的软件进行管理。

您必须在 ESXi 主机上启用 GPU 直通功能，并在 View 中创建桌面池后将单个虚拟机配置为使用专用 PCI 设备。不能对父虚拟机或模板进行 vDGA 配置后创建桌面池，因为这样同一物理 GPU 将专用于池中的每个虚拟机。请参阅有关图形加速的 [VMware 白皮书](#) 中的“vDGA 的安装”。

对于链接克隆虚拟机，执行刷新、重构和重新平衡操作后会保留 vDGA 设置。

- 必须在虚拟机的客户机操作系统中安装来自 GPU 供应商的图形驱动程序。

注 有关支持的 GPU 硬件的列表，请参阅位于 <http://www.vmware.com/resources/compatibility/search.php> 的《VMware 硬件兼容性列表》。

- 必须将 **3D 呈现器** 选项设置为 **使用 vSphere Client 管理**。

使用 vSGA 的其他要求

vSGA 允许多个虚拟机共享 ESXi 主机上的物理 GPU。要支持 vSGA，池必须满足以下其他要求：

- 虚拟机必须在 ESXi 5.1 或更高版本的主机上运行，并由 vCenter Server 5.1 或更高版本的软件进行管理。
- GPU 显卡和相关的 vSphere 安装捆绑包 (vSphere Installation Bundle, VIB) 必须安装在 ESXi 主机上。有关支持的 GPU 硬件的列表，请参阅位于 <http://www.vmware.com/resources/compatibility/search.php> 的《VMware 硬件兼容性列表》。
- Windows 7 计算机必须使用虚拟硬件版本 8 或更高版本。Windows 8 计算机必须使用虚拟硬件版本 9 或更高版本。Windows 10 计算机必须使用虚拟硬件版本 10 或更高版本。
- 可以将 **3D 呈现器** 选项设置为以下任何设置：**使用 vSphere Client 管理**、**自动** 或 **硬件**。另请参阅 [3D 呈现器的视频 RAM 配置选项](#)。

如果 ESXi 主机中存在一个功能强大且可用的硬件 GPU，则 **自动** 使用硬件加速。如果硬件 GPU 不可用，则虚拟机会对任何 3D 任务使用软件 3D 呈现。

使用软 3D 的其他要求

要支持软件 3D 呈现，池必须满足以下附加要求：

- 虚拟机必须在 ESXi 5.0 或更高版本的主机上运行，并由 vCenter Server 5.0 或更高版本的软件进行管理。
- 计算机必须使用虚拟硬件版本 8 或更高版本。
- 必须将 **3D 呈现器** 选项设置为 **软件**。另请参阅 [3D 呈现器的视频 RAM 配置选项](#)。

3D 呈现器的视频 RAM 配置选项

启用 **3D 呈现器** 设置时，如果选择 **自动**、**软件** 或 **硬件** 选项，则可以移动为 **3D 客户机配置虚拟 RAM** 对话框中的滑块来配置分配给池中虚拟机的虚拟 RAM 大小。虚拟 RAM 最小为 64 MB。默认虚拟 RAM 大小取决于虚拟硬件版本：

- 对于虚拟硬件版本为 8 (vSphere 5.0) 的虚拟机，默认虚拟 RAM 大小为 64MB，最大可将其配置为 128MB。

- 对于虚拟硬件版本为 9 (vSphere 5.1) 和 10 (vSphere 5.5 Update 1) 的虚拟机，默认虚拟 RAM 大小为 96MB，最大可将其配置为 512MB。
- 对于虚拟硬件版本为 11 (vSphere 6.0) 的虚拟机，默认虚拟 RAM 大小为 96MB，最大可将其配置为 128MB。在 vSphere 6.0 和更高版本的虚拟机中，该设置仅引用显卡中的显示内存量，因此最大设置比更早的虚拟硬件版本（包含用于存储 3D 对象的显示内存和客户机内存）小。

除非选择使用 **vSphere Client 管理** 选项，否则您在 View Administrator 中配置的虚拟 RAM 设置优先于可在 vSphere Client 或 vSphere Web Client 中为虚拟机配置的虚拟 RAM 设置。

有关自动、软件或硬件 3D 呈现选项的详细信息，请参阅 [3D 呈现器选项](#)。

3D 呈现器选项

桌面池的 **3D 呈现器** 设置提供了各种选项，您可以采用不同方式配置图形呈现。

下表介绍了 View Administrator 中提供的各类 3D 呈现选项之间的差异，但未提供有关配置虚拟机和 ESXi 主机以使用虚拟共享图形加速 (Virtual Shared Graphics Acceleration, vSGA)、虚拟专用图形加速 (Virtual Dedicated Graphics Acceleration, vDGA)、采用 vDGA 的 AMD 多用户 GPU 以及 NVIDIA GRID vGPU 的完整信息。必须先使用 vSphere Web Client 完成这些任务，然后再尝试在 View Administrator 中创建桌面池。有关为 vSGA 和 vDGA 执行这些任务的说明，请参阅有关图形加速的 [VMware 白皮书](#)。有关 NVIDIA GRID vGPU 的说明，请参阅《[适用于 VMware Horizon 6.1 的 NVIDIA GRID vGPU 部署指南](#)》。有关采用 vDGA 的 AMD 多用户 GPU 的说明，请参阅[准备使用采用 vDGA 的 AMD 多用户 GPU 功能](#)。

表 12-12. 运行在 vSphere 5.1 或更高版本上的池的 3D 呈现器选项

选项	描述
使用 vSphere Client 管理	<p>在 vSphere Web Client（或 vSphere 5.1 或更高版本中的 vSphere Client）中为虚拟机设置的 3D 呈现器 选项决定了 3D 图形呈现的类型。View 不会控制 3D 呈现。</p> <p>在 vSphere Web Client 中，可配置自动、软件或硬件选项。这些选项与其在 View Administrator 中的效果相同。</p> <p>在配置 vDGA 和采用 vDGA 的 AMD 多用户 GPU 时使用此设置。此设置也是 vSGA 的一个选项。</p> <p>选择使用 vSphere Client 管理选项时，为3D 客户机配置虚拟 RAM、显示器最大数量和任意一台显示器的最大分辨率设置在 View Administrator 中无效。可以在 vSphere Web Client 中配置内存量。</p>
自动	<p>启用 3D 呈现。ESXi 主机可控制要发生的 3D 呈现的类型。</p> <p>例如，虚拟机开启时，ESXi 主机按照先到先得的原则预留 GPU 硬件资源。如果虚拟机开启时所有的 GPU 硬件资源均已预留，ESXi 将针对此虚拟机使用软件呈现器。</p> <p>在配置 vSGA 时，此设置是一个选项。</p> <p>ESXi 主机依据为 3D 客户机配置虚拟 RAM对话框中设置的值将虚拟 RAM 分配给虚拟机。</p>
软件	<p>启用 3D 呈现。ESXi 主机可使用软件 3D 图形呈现。如果 ESXi 主机上已安装 GPU 显卡，该池则不会使用 3D 呈现。</p> <p>使用此设置可配置软 3D。</p> <p>ESXi 主机依据为 3D 客户机配置虚拟 RAM对话框中设置的值将虚拟 RAM 分配给虚拟机。</p>

选项	描述
硬件	<p>启用 3D 呈现。虚拟机开启时，ESXi 主机按照先到先得的原则预留 GPU 硬件资源。</p> <p>在配置 vSGA 时，此设置是一个选项。</p> <p>ESXi 主机依据为 3D 客户机配置虚拟 RAM 对话框中设置的值将虚拟 RAM 分配给虚拟机。</p> <hr/> <p>重要事项 如果要配置硬件选项，请考虑以下潜在限制：</p> <ul style="list-style-type: none"> ■ 如果用户在预留了所有 GPU 硬件资源时尝试连接到计算机，虚拟机将不会开启，而用户将接收到错误消息。 ■ 如果使用 vMotion 将计算机移至未配置 GPU 硬件的 ESXi 主机，虚拟机将无法打开电源。 <hr/> <p>配置基于硬件的 3D 呈现时，可检查 ESXi 主机上每台虚拟机所分配的 GPU 资源。有关详细信息，请参阅 检查 ESXi 主机上的 GPU 资源。</p>
NVIDIA GRID vGPU	<p>已为 NVIDIA GRID vGPU 启用 3D 呈现。虚拟机开启时，ESXi 主机按照先到先得的原则预留 GPU 硬件资源。如果用户在所有 GPU 硬件资源正由主机上的其他虚拟机使用时尝试连接到计算机，View 连接服务器将尝试在打开电源之前将虚拟机移至群集中的其他 ESXi 主机。</p> <p>在配置 NVIDIA GRID vGPU 时使用此设置。</p> <p>选择 NVIDIA GRID vGPU 选项时，为 3D 客户机配置虚拟 RAM、显示器最大数量和任意一台显示器的最大分辨率设置在 View Administrator 中无效。使用 vSphere Web Client 配置父虚拟机或虚拟机模板时，系统将提示您保留所有内存。</p> <hr/> <p>重要事项 如果配置 NVIDIA GRID vGPU 选项，请考虑以下潜在限制：</p> <ul style="list-style-type: none"> ■ 虚拟机无法挂起或恢复。因此，用于挂起虚拟机的“远程计算机电源策略”选项不可用。 ■ 如果使用 vMotion 将计算机移至未配置 GPU 硬件的 ESXi 主机，虚拟机将无法打开电源。实时 vMotion 不可用。 ■ 群集中的所有 ESXi 主机均不得低于版本 6.0，而且虚拟机硬件不得低于版本 11。 ■ 如果 ESXi 群集包含一个已启用 NVIDIA GRID vGPU 的主机和一个未启用 NVIDIA GRID vGPU 的主机，则这些主机在 View Administrator 控制板中显示黄色（警告）状态。如果用户在所有 GPU 硬件资源正由主机上的其他虚拟机使用时尝试连接到计算机，View 连接服务器将尝试在打开电源之前将虚拟机移至群集中的其他 ESXi 主机。在这种情况下，未启用 NVIDIA GRID vGPU 的主机无法用于此类型的动态迁移。
已禁用	3D 呈现无效。

表 12-13. 运行在 vSphere 5.0 上的池的 3D 呈现器选项

选项	描述
已启用	<p>3D 呈现器选项已启用。ESXi 主机可使用软件 3D 图形呈现。</p> <p>当已配置软件呈现时，默认虚拟 RAM 大小为 64 MB，此为最小值。在为 3D 客户机配置虚拟 RAM 对话框中，可使用滑动条增加预留的虚拟 RAM 的大小。对于软件呈现，ESXi 主机可为每台虚拟机分配最大为 128 MB 的虚拟 RAM。如果设置了更高的虚拟 RAM 大小，则请忽略。</p>
已禁用	3D 呈现无效。

如果桌面池运行在比 5.0 更早的 vSphere 版本上，则 **3D 呈现器**设置无效，且在 View Administrator 中不可用。

配置 3D 呈现的最佳实践

3D 呈现选项和其他池设置具有多种优势和缺陷。选择最能支持 vSphere 硬件基础架构、最能满足用户对图形呈现要求的选项。

注 本主题概述了 View Administrator 中提供的控件。有关 3D 呈现功能的各种选项和要求的详细信息，请参阅有关图形加速的 [VMware 白皮书](#)。

何时选择“自动”选项

对于许多需要 3D 呈现的 View 部署来说，**自动**选项是最佳选择。已启用 vSGA（虚拟共享图形加速）的虚拟机可以在软件和硬件 3D 呈现之间进行动态切换，而无需重新配置。该选项可确保某些类型的 3D 呈现即使在 GPU 资源完全预留时也可发生。在包含 ESXi 5.1 和 ESXi 5.0 主机的混合群集中，该选项可确保虚拟机成功开启，并确保即使在 vMotion 将虚拟机移动到 ESXi 5.0 主机时仍可使用 3D 呈现。

自动选项的唯一缺陷是您无法轻松判断虚拟机使用的是硬件还是软件 3D 呈现。

何时选择“硬件”选项

硬件选项可保证池中的每一台虚拟机均使用硬件 3D 呈现，前提是 GPU 资源在 ESXi 主机上可用。当您的所有用户都运行图形密集型应用程序时，此选项或许为最佳选择。可以在配置 vSGA（虚拟共享图形加速）时使用该选项。

如果选择**硬件**选项，您必须严格控制 vSphere 环境。所有的 ESXi 主机必须是 5.1 版或更高版本，且必须安装 GPU 显卡。

如果 ESXi 主机上的所有 GPU 资源均被预留，View 将无法为下一个尝试登录到桌面的用户开启虚拟机。您必须管理 GPU 资源的分配和 vMotion 的使用来确保资源对桌面可用。

何时选择“使用 vSphere Client 管理”选项

选择**使用 vSphere Client 管理**选项时，可以使用 vSphere Web Client 通过不同选项和虚拟 RAM 值来配置单个虚拟机。

- 对于 vSGA（虚拟共享图形加速），可针对池中的虚拟机进行 3D 呈现和虚拟 RAM 大小的混合配置。
- 对于 vDGA（虚拟专用图形加速），必须将每个虚拟机单独配置为与 ESXi 主机共享特定 PCI 设备，且必须预留所有内存。有关详细信息，请参阅[准备 vDGA 功能](#)。

所有的 ESXi 主机必须是 5.5 版或更高版本，且必须安装 GPU 显卡。

注 某些 Intel vDGA 卡需要特定的 vSphere 6 版本。请参阅位于 <http://www.vmware.com/resources/compatibility/search.php> 的《VMware 硬件兼容性列表》。此外，对于 Intel vDGA，使用的是 Intel 集成的 GPU 而不是分离式 GPU，其他供应商的情况也是如此。

- 对于采用 vDGA 的 AMD 多用户 GPU，必须将每个虚拟机分别配置为与 ESXi 主机共享特定的 PCI 设备，并且必须预留所有内存。此功能可使一个 PCI 设备显示为多个不同的物理 PCI 设备，这样就能使 GPU 在 2 至 15 个用户之间共享。有关详细信息，请参阅[准备使用采用 vDGA 的 AMD 多用户 GPU 功能](#)。

所有的 ESXi 主机必须是 6.0 版或更高版本，且必须安装 GPU 显卡。

如果通过让克隆继承父虚拟机的设置，来显式管理克隆和链接克隆的图形设置，也可以选择该选项。

何时选择“NVIDIA GRID vGPU”选项

通过使用 **NVIDIA GRID vGPU** 选项，您可以在启用了 NVIDIA GRID vGPU 的 ESXi 主机上获得比使用 vDGA 更高的虚拟机整合率，同时保持相同的性能水平。与 vDGA（专用虚拟图形）一样，ESXi 和虚拟机也对 NVIDIA GRID vGPU 使用 GPU 直通。

注 要提高虚拟机整合比率，可以将 ESXi 主机设置为使用整合模式。在 ESXi 主机上编辑 `/etc/vmware/config` 文件，然后添加以下项：

```
vGPU.consolidation = "true"
```

默认情况下，ESXi 主机会将虚拟机分配给所分配到的虚拟机最少的物理 GPU。这称为“性能模式”。如果您希望 ESXi 主机将虚拟机分配给同一物理 GPU，直到达到虚拟机最大数量后再在下一物理 GPU 上放置虚拟机，则可以使用整合模式。

由于 GPU 不需要专用于某个特定的虚拟机，使用 **NVIDIA GRID vGPU** 选项可以创建父虚拟机或虚拟机模板并将其配置为启用 NVIDIA GRID vGPU，然后创建可共享相同物理 GPU 的虚拟机的桌面池。

如果 ESXi 主机上的所有 GPU 资源正由其他虚拟机使用，则在下一个用户尝试登录到桌面时，View 可以将虚拟机移至群集中其他已启用 NVIDIA GRID vGPU 的 ESXi Server，然后打开虚拟机的电源。所有的 ESXi 主机必须是 6.0 版或更高版本，且必须安装 GPU 显卡。

有关详细信息，请参阅[准备 NVIDIA GRID vGPU 功能](#)。

何时选择“软件”选项

如果您只有 ESXi 5.0 主机，或者 ESXi 5.1 或更高版本主机没有 GPU 显卡，又或者您的用户仅运行不需要硬件图形加速的应用程序（如 AERO 和 Microsoft Office），请选择**软件**选项。

配置桌面设置以管理 GPU 资源

您可配置其他的桌面设置以确保用户未积极使用 GPU 资源时也不会造成浪费。

对于浮动池，请设置会话超时，这样当用户未使用桌面时，GPU 资源可供其他用户使用。

对于专用池，您可以将**断开连接后自动注销**设置配置为**立即**和**挂起**电源策略（如果这些设置适合您的用户）。例如，对于执行长时间运行的模拟操作的研究人员的池，请勿使用这些设置。请注意，如果使用 **NVIDIA GRID vGPU** 选项，则**挂起**电源策略不可用。

准备 vDGA 功能

虚拟专用图形加速 (Virtual Dedicated Graphics Acceleration, vDGA) 向物理 GPU 提供直接直通，从而为用户提供对单个 vGPU 的无限制专用访问权限。在尝试创建具有 vDGA 功能的桌面池之前，必须在虚拟机和 ESXi 主机上执行特定的配置任务。

此概述是在 View Administrator 中创建或配置桌面池之前必须在 vSphere 中执行的任务概述。有关完整信息和详细步骤，请参阅有关图形加速的 [VMware 白皮书](#)。

注 某些 Intel vDGA 卡需要特定的 vSphere 6 版本。请参阅位于 <http://www.vmware.com/resources/compatibility/search.php> 的《VMware 硬件兼容性列表》。此外，对于 Intel vDGA，使用的是 Intel 集成的 GPU 而不是分离式 GPU，其他供应商的情况也是如此。

- 1 在 ESXi 主机上安装显卡。
- 2 安装 GPU vSphere 安装捆绑包 (vSphere Installation Bundle, VIB)。
- 3 验证是否已在 ESXi 主机上启用 VT-d 或 AMD IOMMU。
- 4 将 PCI 设备添加到虚拟机，并选择相应的 PCI 设备以在虚拟机上启用 GPU 直通。
- 5 在创建虚拟机时预留所有内存。
- 6 配置虚拟机视频卡 3D 功能。
- 7 从 GPU 供应商处获取 GPU 驱动程序，并在虚拟机的客户机操作系统中安装 GPU 设备驱动程序。
- 8 在客户机操作系统中安装 VMware Tools 和 Horizon Agent 并重新引导。

在执行这些任务后，必须将虚拟机添加到手动桌面池中，以便使用 PCoIP 或 VMware Blast Extreme 访问客户机操作系统。然后，可以在 PCoIP 或 VMware Blast 会话中激活客户机操作系统中的 NVIDIA、AMD 或 Intel 显示适配器。

准备 NVIDIA GRID vGPU 功能

NVIDIA GRID vGPU 允许使用本机显卡驱动程序直接访问 ESXi 主机上的物理 GPU，从而使多个用户可以共享一个 GPU。在尝试创建具有 NVIDIA GRID vGPU 功能的桌面池之前，必须在虚拟机和 ESXi 主机上执行特定的配置任务。

此概述是在 View Administrator 中创建或配置桌面池之前必须在 vSphere 中执行的任务概述。有关完整信息和详细步骤，请参阅《适用于 VMware Horizon 6.1 的 NVIDIA GRID vGPU 部署指南》。

- 1 在 ESXi 主机上安装显卡。
- 2 安装 GPU vSphere 安装捆绑包 (vSphere Installation Bundle, VIB)。
- 3 验证是否已在 ESXi 主机上启用 VT-d 或 AMD IOMMU。
- 4 在 ESXi 主机上启用 GPU 设备直通。
- 5 将共享 PCI 设备添加到虚拟机，并选择相应的 PCI 设备以在虚拟机上启用 GPU 直通。

添加共享 PCI 设备后，可以查看 ESXi 主机上的 GPU 卡中可用的所有受支持图形配置文件类型的列表。

- 6 在创建虚拟机时预留所有内存。
- 7 配置虚拟机视频卡 3D 功能。
- 8 从 GPU 供应商处获取 GPU 驱动程序，并在虚拟机的客户机操作系统中安装 GPU 设备驱动程序。
- 9 在客户机操作系统中安装 VMware Tools 和 Horizon Agent 并重新引导。

执行这些任务后，必须将虚拟机添加到手动池 - View 桌面池中，以便使用 PCoIP 访问客户机操作系统。然后，可以在 PCoIP 会话中激活客户机操作系统中的 NVIDIA 显示适配器。

此时，可以将虚拟机配置为模板，或生成要用作 View Composer 链接克隆池中的基础映像的虚拟机快照。

（必须在生成快照之前关闭虚拟机的电源。）使用“添加桌面池”向导时，在为 3D 呈现器选择 NVIDIA GRID vGPU 选项后，仅启用了 NVIDIA GRID vGPU 的 ESXi 主机和启用了 NVIDIA GRID vGPU 的虚拟机模板及快照显示在向导中，以供选择。

准备使用采用 vDGA 的 AMD 多用户 GPU 功能

采用 vDGA 的 AMD 多用户 GPU 向物理 GPU 提供直接直通，从而为用户提供对单个 GPU 的无限制专用访问权限。在尝试创建能够使用采用 vDGA 的 AMD 多用户 GPU 的桌面池之前，必须在虚拟机和 ESXi 主机上执行特定的配置任务。

此概述是在 View Administrator 中创建或配置桌面池之前必须在 vSphere 中执行的任务概述。有关启用 GPU 设备直通以及将 PCI 设备添加到虚拟机的信息，请参阅有关图形加速的 [VMware 白皮书](#)。

- 1 在 ESXi 主机上安装显卡。
- 2 安装 GPU vSphere 安装捆绑包 (vSphere Installation Bundle, VIB)。
- 3 验证是否已在 ESXi 主机上启用 VT-d 或 AMD IOMMU。
- 4 使用 `esxcfg-module` 命令配置用于 SR-IOV（单根 I/O 虚拟化）的显卡。
请参阅[配置采用 vDGA 的 AMD 多用户 GPU](#)。
- 5 重新引导 ESXi 主机。
- 6 将 PCI 设备添加到虚拟机，并选择相应的 PCI 设备以在虚拟机上启用 GPU 直通。
- 7 在创建虚拟机时预留所有内存。
- 8 配置虚拟机视频卡 3D 功能。
- 9 从 GPU 供应商处获取 GPU 驱动程序，并在虚拟机的客户机操作系统中安装 GPU 设备驱动程序。
- 10 在客户机操作系统中安装 VMware Tools 和 Horizon Agent 并重新引导。

在执行这些任务后，必须将虚拟机添加到手动桌面池中，以便使用 PCoIP 或 VMware Blast Extreme 访问客户机操作系统。如果尝试使用 vSphere 访问虚拟机，显示器将会黑屏。

配置采用 vDGA 的 AMD 多用户 GPU

您可以使用 `esxcfg-module` 命令行命令配置可共享 GPU 的用户数量、分配给每个用户的帧缓冲区量等参数，以及某些性能控件。

语法

```
esxcfg-module -s "adapter1_conf=bus#,device#,function#,number_of_VFs,FB_size,time_slice,mode" amdgpv
```

用法说明

`vicfg-module` 命令支持在 ESXi 主机上设置和检索 VMkernel 模块选项。有关此命令的常规参考信息，请访问 <http://pubs.vmware.com/vsphere-60/topic/com.vmware.vcli.ref.doc/vicfg-module.html>。

必需的标记

在配置采用 vDGA 的 AMD 多用户 GPU 时，必须指定若干标记。如果命令不包含所有必需的标记，则不会提供错误消息，配置而是会默认设置为简单的 4 SR-IOV 设备配置。

表 12-14. 用于配置 AMD SR-IOV 的标记

标记	说明
<i>bus#</i>	采用十进制格式的总线号。
<i>device#</i>	<p>受支持的 AMD 卡的 PCIe 设备 ID（采用十进制格式）。要查看列表，请使用命令 <code>lspci grep -i display</code>。</p> <p>例如，对于具有两个 AMD GPU 卡的系统，在运行此命令时，您可能会看到以下输出：</p> <pre>[root@host:~] lspci grep -i display 0000:04:00.0 Display controller: 0000:82:00.0 Display controller:</pre> <p>在此示例中，PCIe 设备 ID 为 04 和 82。请注意，这些 ID 以十六进制格式列出，必须将其转换为十进制格式，才能在 <code>vicfg-module</code> 命令中使用。</p> <p>AMD S7150 卡支持每卡仅一个 GPU，因此，对于这些卡，设备 ID 和功能 ID 均为 0。</p>
<i>function#</i>	采用十进制格式的功能号。
<i>number_of_VFs</i>	VF（虚拟功能）的数量（从 2 至 15）。此数值表示将共享 GPU 的用户数量。
<i>FB_size</i>	<p>分配给每个 VF 的帧缓冲区内容量（以 MB 为单位）。要确定大小，请查明卡上视频内存的总量，并将该总量除以 VF 的数量。然后，将所得数值舍入为最接近的 8 的倍数。例如，对于具有 8000 MB 的 AMD S7150 卡，您可以使用以下设置：</p> <ul style="list-style-type: none"> ■ 对于 2 个 VF，使用 4096。 ■ 对于 4 个 VF，使用 2048。 ■ 对于 8 个 VF，使用 1024。 ■ 对于 15 个 VF，使用 544。
<i>time_slice</i>	VF 切换的时间间隔（以微秒为单位）。此设置可调整 SR-IOV 设备之间的命令排队和处理延迟。使用介于 3000 和 40000 之间的一个值。如果您在多个 SR-IOV 桌面处于活动状态时发现显著的间断，请调整此值。
<i>mode</i>	以下是有效的值：0 = 回收的性能；1 = 固定的百分比性能。

重要事项 在运行 `esxcfg-module` 命令后，您必须重新引导 ESXi 主机以使设置生效。

示例

1 对于在 8 个用户之间共享的 PCI ID 4 上的单个 AMD S7150 卡：

```
esxcfg-module -s "adapter1_conf=4,0,0,8,1024,4000" amdgpuv
```


- 对于在 4 个超级用户之间共享的 PCI ID 4 和 PCI ID 82 上具有两个 AMD S7150 卡的单个服务器：

```
esxcfg-module -s "adapter1_conf=3,0,0,2,4096,4000 adapter2_conf=130,0,0,2,4096,4000" amdgpuv
```

- 对于具有两个 AMD S7150 卡的单个服务器，您可以通过不同的参数设置每个卡。例如，如果您的 View 环境需要支持 2 个超级用户和 16 个任务工作者：

```
esxcfg-module -s "adapter1_conf=3,0,0,2,4096,4000 adapter2_conf=130,0,0,15,544,7000" amdgpuv
```

- 在 ESXi 主机上启用 SR-IOV 选项。

某些主机在 BIOS 中将 SR-IOV 作为可配置选项。

检查 ESXi 主机上的 GPU 资源

为了更好地管理 ESXi 主机上的 GPU 资源，您可检查当前的 GPU 资源预留情况。ESXi 命令行查询实用程序 `gpvm` 能够列出安装在 ESXi 主机上的 GPU，并显示为主机上的每台虚拟机所预留的 GPU 内存容量。请注意该 GPU 内存预留与虚拟机虚拟 RAM 大小并不一样。

要运行此实用程序，请在 ESXi 主机上的 Shell 提示符中键入 `gpvm`。您可使用主机上的控制台或 SSH 连接。

例如，此实用程序可能会显示以下输出：

```
~ # gpvm
Xserver unix:0, GPU maximum memory 2076672KB
  pid 118561, VM "JB-w7-64-FC3", reserved 131072KB of GPU memory.
  pid 64408, VM "JB-w7-64-FC5", reserved 261120KB of GPU memory.
GPU memory left 1684480KB.
```

同样，可以在 ESXi 主机上使用 `nvidia-smi` 命令查看已启用 NVIDIA GRID vGPU 的虚拟机的列表、已消耗的帧缓冲区内存量以及虚拟机正使用的物理 GPU 的插槽 ID。

阻止通过 RDP 访问 View 桌面

在一定的 View 环境中，应优先考虑禁止通过 RDP 显示协议访问 View 桌面。您可以通过配置池设置和组策略设置来阻止用户和管理员使用 RDP 访问 View 桌面。

默认情况下，用户登录到 View 桌面会话时，可以使用 RDP 从 View 外部连接虚拟机。RDP 连接会终止 View 桌面会话，View 用户未保存的数据和设置可能会丢失。除非关闭外部 RDP 连接，否则 View 用户无法登录到桌面。为避免这种情况，请禁用 `AllowDirectRDP` 设置。

注 必须在用于创建池的虚拟机以及部署在这些池中的虚拟机上启动远程桌面服务。Horizon Agent 安装、SSO 和其他 View 会话管理操作都需要使用远程桌面服务。

前提条件

确认已在 Active Directory 中安装 Horizon Agent 配置管理模板 (ADM) 文件。请参阅[使用 View 组策略管理模板文件](#)。

步骤

- 1 选择 PCoIP 作为 View 连接服务器与 Horizon Client 设备进行通信时使用的显示协议。

选项	说明
创建一个桌面池	<ol style="list-style-type: none"> a 在 View Administrator 中，启动添加桌面池向导。 b 在“桌面池设置”页面中，选择 VMware Blast 或 PCoIP 作为默认显示协议。
编辑现有桌面池	<ol style="list-style-type: none"> a 在 View Administrator 中，选择所需的桌面池并单击编辑。 b 在桌面池设置选项卡上，选择 VMware Blast 或 PCoIP 作为默认显示协议。

- 2 对于允许用户选择协议设置，请选择否。
- 3 通过禁用 AllowDirectRDP 组策略设置阻止未运行 Horizon Client 的设备通过 RDP 直接连接 View 桌面。
 - a 在您的 Active Directory 服务器上，打开组策略管理控制台，并依次选择**计算机配置 > 策略 > 管理模板 > 经典管理模板 (ADM) > VMware Horizon Agent 配置**。
 - b 禁用 AllowDirectRDP 设置。

部署大型桌面池

当很多用户要求使用同一桌面映像时，您可通过一个模板或父虚拟机创建一个大型自动池。通过使用单一基础映像和池名称，您可以避免将计算机随意划分为更小的、必须单独管理的组。此策略简化了您的部署和管理任务。

要支持大型池，您可针对包含多达 32 个 ESXi 主机的 ESXi 群集创建池。您也可以将池配置为使用多个网络标签，从而使多个端口组的 IP 地址可供池中的虚拟机使用。

注 多个网络标签功能不可用于即时克隆。

在包含超过 8 个主机的群集上配置桌面池

在 vSphere 5.1 和更高版本中，您可在包含多达 32 个 ESXi 主机的群集上部署链接克隆桌面池。群集中的所有 ESXi 主机必须是 5.1 版或更高版本。主机可使用 VMFS 或 NFS 数据存储。VMFS 数据存储必须是 VMFS5 或更高版本。

在 vSphere 5.0 中，您可以在一个包含超过 8 个 ESXi 主机的群集中部署链接克隆，但您必须在 NFS 数据存储中存储副本磁盘。您可以在 VMFS 数据存储中存储副本磁盘，但其群集所包含的主机数量不得多于 8 个。

在 vSphere 5.0 中，当您在包含超过 8 个主机的群集中配置链接克隆池时，以下规则适用：

- 如果要在与操作系统磁盘相同的数据存储中存储副本磁盘，您必须将副本和操作系统磁盘存储在 NFS 数据存储中。
- 如果要在与操作系统磁盘不同的数据存储中存储副本磁盘，您必须将副本磁盘存储在 NFS 数据存储中。可将操作系统磁盘存储在 NFS 或 VMFS 数据存储中。

- 如果要将在 View Composer 永久磁盘存储在不同的数据存储中，则可在 NFS 或 VMFS 数据存储上配置永久磁盘。

在 vSphere 4.1 和更早版本中，仅可在包含 8 个或更少主机的群集中部署桌面池。

向桌面池分配多个网络标签

在 View 5.2 和更高版本中，您可以配置自动桌面池使用多个网络标签。可向链接克隆池或包含完整虚拟机的自动池分配多个网络标签。

注 多个网络标签功能不可用于即时克隆。

在过去的版本中，池中的虚拟机沿用了父虚拟机或模板上的网卡所使用的网络标签。典型的父虚拟机或模板包含一个网卡和一个网络标签。网络标签定义了端口组和 VLAN。通常 VLAN 的网络掩码可提供数量有限的可用 IP 地址。

在 View 5.2 和更高版本中，您可为部署桌面池的群集中的所有 ESXi 主机分配可在 vCenter Server 使用的网络标签。通过为池配置多个网络标签，可以大幅增加可分配给池中虚拟机的 IP 地址的数量。

必须使用 View PowerCLI cmdlet 将多个网络标签分配给池。在 View Administrator 中无法执行此任务。

有关使用 View PowerCLI 执行此任务的详细信息，请参阅《View 集成指南》文档的“使用 View PowerCLI”章节中的“向桌面池分配多个网络标签”。

授权用户和组

您通过配置授权来控制用户可以访问哪些远程桌面和应用程序。您可以配置受限制的授权功能，在用户选择远程桌面时根据他们连接的 **View** 连接服务器实例来控制桌面访问。您还可以限制网络外部一组用户的访问，禁止他们连接网络内部的远程桌面和应用程序。

在 **Cloud Pod** 架构环境中，您可以创建全局授权来授权用户或组访问容器联合中的多个容器的多个桌面。使用全局授权时，不需要为远程桌面配置和管理本地授权。有关全局授权和设置 **Cloud Pod** 架构环境的信息，请参阅《管理 **View Cloud Pod** 架构》文档。

本章讨论了以下主题：

- [为桌面池或应用程序池添加授权](#)
- [移除对桌面池或应用程序池的授权](#)
- [查看桌面或应用程序池授权](#)
- [限制远程桌面访问](#)
- [限制网络外部的远程桌面访问](#)

为桌面池或应用程序池添加授权

在用户能够访问远程桌面或应用程序前，必须授权这些用户使用桌面池或应用程序池。

前提条件

创建一个桌面池或应用程序池。

步骤

- 1 选择桌面池或应用程序池。

选项	操作
为桌面池添加授权	在 View Administrator 中，选择 目录 > 桌面池 ，然后单击桌面池的名称。
为应用程序池添加授权	在 View Administrator 中，选择 目录 > 应用程序池 ，然后单击应用程序池的名称。

- 2 从**授权**下拉菜单中选择**添加授权**。

- 单击**添加**，选择一个或多个搜索条件，然后单击**查找**根据搜索条件查找用户或组。

注 混合模式域搜索结果中将不包含域本地用户组。如果您的域是在混合模式下配置的，您将不能为域本地用户组中的用户授权。

- 选择要授权其使用池中桌面或应用程序的用户或组，然后单击**确定**。
- 单击**确定**保存更改。

移除对桌面池或应用程序池的授权

您可以移除对桌面池或应用程序池的授权，以阻止特定用户或组访问桌面或应用程序。

步骤

- 选择桌面池或应用程序池。

选项	描述
移除桌面池的授权	在 View Administrator 中，选择 目录 > 桌面池 ，然后单击桌面池的名称。
移除应用程序池的授权	在 View Administrator 中，选择 目录 > 应用程序池 ，然后单击应用程序池的名称。

- 从**授权**下拉菜单中选择**移除授权**。
- 选择您要移除其授权的用户或用户组，然后单击**移除**。
- 单击**确定**保存更改。

查看桌面或应用程序池授权

您可以查看某个用户或用户组有权访问的桌面池或应用程序池。

步骤

- 在 View Administrator 中，选择**用户和组**，然后单击用户或用户组的名称。
- 单击**授权**选项卡并查看某个用户或用户组有权访问的桌面池或应用程序池。

选项	操作
列出用户或组有权访问的桌面池	单击 桌面池 。
列出用户或组有权访问的应用程序池	单击 应用程序池 。

限制远程桌面访问

您可以配置受限制的授权功能，以根据用户在选择桌面时连接的 **View** 连接服务器实例限制远程桌面访问。

使用受限制的授权功能，您可以为一个 **View** 连接服务器实例分配一个或多个标签。在之后配置桌面池时，您可以选择希望其能够访问桌面池的 **View** 连接服务器实例的标签。

当用户通过带标签的 **View** 连接服务器实例登录时，他们只可以访问那些没有标签或至少有一个匹配标签的桌面池。

注 无法配置受限制的授权功能，以限制访问远程应用程序。

- **受限制的授权示例**

此示例展示了一种包含两个 **View** 连接服务器实例的 **View** 部署。其中一个实例用于支持内部用户。另一个实例则与安全服务器配对，用于支持外部用户。

- **标签匹配**

受限制的授权功能通过标签匹配的方法来确定 **View** 连接服务器实例能否访问特定的桌面池。

- **与受限制的授权相关的考虑因素及限制因素**

在实施受限制的授权之前，必须注意一些考虑因素和限制因素。

- **为 View 连接服务器实例分配标签**

当您向 **View** 连接服务器实例分配标签后，与该 **View** 连接服务器连接的用户只能访问带有匹配标签或不带标签的 **View** 桌面池。

- **为桌面池分配标签**

当您把标签分配给桌面池后，只有连接到带有匹配标签的 **View** 连接服务器实例的用户才能访问该池中的桌面。

受限制的授权示例

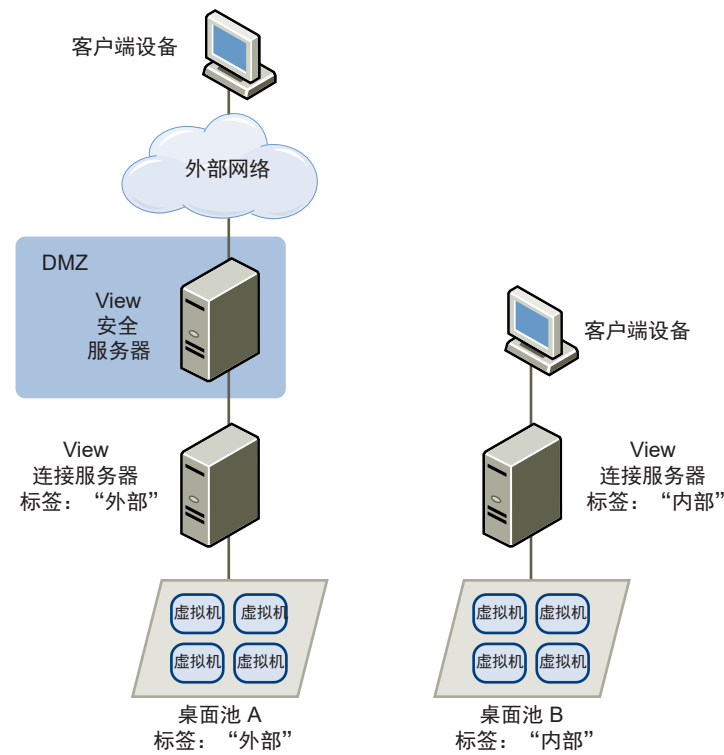
此示例展示了一种包含两个 **View** 连接服务器实例的 **View** 部署。其中一个实例用于支持内部用户。另一个实例则与安全服务器配对，用于支持外部用户。

为防止外部用户访问特定桌面，您可以采用以下操作设置受限制的授权：

- 将“内部”标签分配给支持内部用户的 **View** 连接服务器实例。
- 将“外部”标签分配给与安全服务器配对并支持外部用户的 **View** 连接服务器实例。
- 将“内部”标签分配给仅供内部用户访问的桌面池。
- 将“外部”标签分配给仅供外部用户访问的桌面池。

外部用户无法看到标记为“内部”的桌面池，因为他们是通过标记为“外部”的 **View** 连接服务器登录的，而内部用户是通过标记为“内部”的 **View** 连接服务器登录的，因此，他们无法看到标记为“外部”的桌面池。图 13-1. 受限制的授权配置说明了此配置。

图 13-1. 受限制的授权配置



您也可以使用受限制的授权功能，根据您为特定 **View** 连接服务器实例配置的用户身份验证方法控制桌面访问。例如，您可以仅允许经过智能卡身份验证的用户使用特定的桌面池。

标签匹配

受限制的授权功能通过标签匹配的方法来确定 **View** 连接服务器实例能否访问特定的桌面池。从最基本的层面来看，标签匹配方法可确定带有特定标签的 **View** 连接服务器实例能否访问带有相同标签的桌面池。如果未分配标签，还会影响到 **View** 连接服务器实例能否访问桌面池。例如，不带有任何标签的 **View** 连接服务器实例只能访问同样不带任何标签的桌面池。

表 13-1. 标签匹配规则 显示了受限制的授权功能如何确定 **View** 连接服务器在哪些情况下能访问桌面池。

表 13-1. 标签匹配规则

View 连接服务器	桌面池	是否允许访问
无标签	无标签	是
无标签	一个或多个标签	否
一个或多个标签	无标签	是
一个或多个标签	一个或多个标签	仅标签匹配时允许访问

受限制的授权功能只能强制执行标签匹配。您必须设计网络拓扑结构以强制特定的客户端通过特定的 **View** 连接服务器实例进行连接。

与受限制的授权相关的考虑因素及限制因素

在实施受限制的授权之前，必须注意一些考虑因素和限制因素。

- 一个 View 连接服务器实例或桌面池可以有多个标签。
- 多个 View 连接服务器实例和桌面池可以有相同的标签。
- 不带任何标签的桌面池可被任何 View 连接服务器实例访问。
- 不带任何标签的 View 连接服务器实例只能访问同样不带任何标签的桌面池。
- 如果使用安全服务器，必须在与其配对的 View 连接服务器实例上配置受限制的授权。您无法在安全服务器上配置受限制的授权。
- 如果 View 连接服务器实例的标签已被分配到桌面池，且不存在带有匹配标签的其他 View 连接服务器实例，您将无法修改或删除这些标签。
- 受限制的授权优先于其他桌面授权或分配。例如，即使已将用户分配给特定计算机，但如果此桌面池的标签与分配给用户所连接的 View 连接服务器实例的标签不匹配，用户也无法访问此计算机。
- 如果您想通过 VMware Identity Manager 提供桌面访问，并且配置了 View 连接服务器限制，则当桌面实际受到限制时，VMware Identity Manager 应用程序可能会向用户显示这些桌面。当 VMware Identity Manager 用户尝试登录桌面时，如果桌面池的标签与分配给用户所连接的 View 连接服务器实例的标签不匹配，该桌面将无法启动。

为 View 连接服务器实例分配标签

当您向 View 连接服务器实例分配标签后，与该 View 连接服务器连接的用户只能访问带有匹配标签或不带标签的 View 桌面池。

步骤

- 1 在 View Administrator 中，选择 **View 配置 > 服务器**。
- 2 单击**连接服务器**选项卡，选择 View 连接服务器实例，然后单击**编辑**。
- 3 在**标签**文本框中键入一个或多个标签。
用逗号或分号分隔多个标签。
- 4 单击**确定**保存更改。

后续步骤

为桌面池分配标签。

为桌面池分配标签

当您为桌面池分配标签后，只有连接到带有匹配标签的 View 连接服务器实例的用户才能访问该池中的桌面。

您可以在添加或编辑桌面池时分配标签。

前提条件

将标签分配给一个或多个 View 连接服务器实例。

步骤

1 在 View Administrator 中，选择目录 > 桌面池。

2 选择您想要为其分配标签的池。

选项	操作
为新池分配标签	单击 添加 启动“添加桌面池”向导，然后定义并标识该池。
为已有池分配标签	选择池，然后单击 编辑 。

3 转到“桌面池设置”页面。

选项	操作
新池的设置	单击“添加桌面池”向导中的 桌面池设置 。
已有池的设置	单击 桌面池设置 选项卡。

4 单击 **连接服务器限制**旁的**浏览**，然后配置可以访问桌面池的 View 连接服务器实例。

选项	操作
使池可供任意 View 连接服务器实例访问	选择 无限制 。
使池仅供带有这些标签的 View 连接服务器实例访问	选择 仅限这些标签 并选择一个或多个标签。您可以使用复选框选择多个标签。

5 单击**确定**保存更改。

限制网络外部的远程桌面访问

您可以允许特定的授权用户和组从外部网络访问远程桌面，而限制其他授权用户和组的访问。所有授权用户都将可以从内部网络访问桌面和应用程序。如果您选择不将访问权限限制给外部网络的特定用户，那么所有授权用户都将可以从外部网络进行访问。

出于安全原因，管理员可能会需要限制网络外部的用户和组访问网络内部的远程桌面和应用程序。当受限的用户从外部网络访问系统时，会显示一条消息，指明此用户无权使用该系统。此用户必须在内部网络中才有权访问桌面和应用程序池。

限制网络外部的用户

您可以允许一些用户和组从网络外部访问 View 连接服务器实例，同时限制其他用户和组的访问。

前提条件

- 必须在网络外部部署 Access Point 设备、安全服务器或负载平衡器，来作为用户有权访问的 View 连接服务器实例的网关。有关部署 Access Point 设备的更多信息，请参阅《部署和配置 Access Point》文档。

- 要进行远程访问的用户必须有权访问桌面或应用程序池。

步骤

- 1** 在 **View Administrator** 中，选择**用户和组**。
- 2** 单击**远程访问**选项卡。
- 3** 单击**添加**，选择一个或多个搜索条件，然后单击**查找**以根据搜索条件查找用户或组。
- 4** 要向某个用户或组提供远程访问权限，请选择相应用户或组，然后单击**确定**。
- 5** 要从远程访问中移除用户或组，请选择相应用户或组，单击**删除**，然后单击**确定**。

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 **Feature Pack Update** 版本中更新，也可以在核心 **View** 版本中更新。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**、实时音频-视频、**Windows Media 多媒体重定向 (MMR)**、**USB 重定向**、**扫描仪重定向**和**串行端口重定向**。

有关 **HTML Access** 的信息，请参阅位于 **VMware Horizon Client** 文档网页上的《使用 **HTML Access**》文档。

有关 **USB 重定向**的信息，请参阅第 15 章 [将 USB 设备与远程桌面和应用程序一起使用](#)。

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 **URL 内容重定向**
- 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
- 限制复制和粘贴操作的剪贴板格式

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。

在安装 **Unity Touch** 后，您可以通过配置启用 **Unity Touch** 组策略设置来禁用或启用它。请参阅 [Horizon Agent 配置 ADM 模板设置](#)。

面向 **iOS** 和 **Android** 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。

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。

View 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：

- 通过安装 View Agent 6.0 或更高版本来安装 Unity Touch 功能。请参阅 [在虚拟机上安装 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 2.0 或更高版本
- 适用于 Android 的 Horizon Client 2.0 或更高版本

移动设备操作系统

以下移动设备操作系统支持 Unity Touch：

- iOS 5.0 及更高版本
- Android 3 (Honeycomb)、Android 4 (Ice Cream Sandwich) 和 Android 4.1 与 4.2 (Jelly Bean)

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 View 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，列表中一个或多个应用程序未在 View 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，View 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，View 部署必须满足特定的软件和硬件要求。

View 桌面

- 您可以在静默安装 View Agent 6.0 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 [Horizon Agent 的静默安装属性](#)。
- 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。有关详细信息，请参阅《使用适用于 Windows 的 VMware Horizon Client》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[Horizon Agent 的静默安装属性](#)。

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

通过使用 Flash 重定向功能，可将 Flash 内容发送到客户端系统，并在使用 Flash Player ActiveX 版本的 Flash 容器窗口中播放该内容。

注 在 Horizon 7.0 中，Flash 重定向是一项技术预览版功能。在 Horizon 7.0.1 中，该功能受到完全支持。

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 14-1. 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
支持级别	Horizon 7.0 中的一项技术预览版功能，不提供技术支持。在 Horizon 7.0.1 中受到完全支持。	受到完全支持
支持该功能的 Horizon Client 类型	仅 Windows 客户端	Windows 客户端和 Linux 客户端
显示协议	在 Horizon 7.0 中，仅为 PCoIP。在 Horizon 7.0.1 中，则为 PCoIP 和 VMware Blast。	PCoIP
浏览器	适用于代理（远程桌面）的 Internet Explorer 9、10 或 11	当前在 Horizon Client 和 Horizon Agent 中支持的所有浏览器
配置机制	使用代理端 GPO 指定使用或不使用 Flash 重定向的网站白名单或黑名单	修改网页中的源代码以嵌入必需的 JavaScript

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** 网站就不能使用该功能。
- 在 **Horizon 7.0** 中，**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**”。
- 对于 **YouTube** 网站，为避免发生播放问题，默认情况下将禁用外部接口。因此，以下功能无法使用：“自动播放”、“下一个”和“上一个”按钮以及影院模式。要使 **YouTube** 网站的最新更新支持 **Flash** 媒体，您必须从**兼容性视图设置**中移除 **youtube.com**，然后手动将 **&nohtml5=1** 附加到视频的 **URL**。例如，**https://www.youtube.com/watch?v=NwmRD25HWGE&nohtml5=1**。
- 除非您在远程桌面上以 **Windows** 注册表项形式设置了 **appMode=1**，否则无法单击 **YouTube** 网站上的推荐视频。
- 如果客户端上没有音频设备，则在播放 **YouTube Flash** 媒体时将发生错误。
- **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 版本 4.1 使用 PCoIP 连接到 Horizon 7.0 桌面，Flash 重定向将失败。桌面的本地播放器将播放 Flash 内容，或者用户将看到白色屏幕。

Flash 重定向的要求

如果使用 Internet Explorer 9、10 或 11，可以通过 Flash 重定向将 Flash 内容发送到客户端系统。客户端系统播放媒体内容，这样可降低 ESXi 主机上的负载。

远程桌面

- Horizon Agent 7.0 或更高版本必须安装在单用户 (VDI) 远程桌面中，并选择 Flash 重定向选项。默认情况下，不会选择 Flash 重定向选项。
请参阅 [Horizon Agent 自定义安装选项](#)。
- 必须配置相应的组策略设置。请参阅[安装并配置 Flash 重定向](#)。
- 在 Windows 7、Windows 8、Windows 8.1 和 Windows 10 单用户远程桌面上支持 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，将启用 Flash 重定向选项。
请参阅《使用适用于 Windows 的 VMware Horizon Client》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 VMware Blast、PCoIP

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，并指定哪些网站将使用该功能。

要在客户端系统上安装该功能，必须使用 Horizon Client 4.0 或更高版本的安装程序。要在远程桌面上安装该功能，必须使用 Horizon Agent 7.0 或更高版本的安装程序，并选择正确的安装选项（默认不会选择）。要启用该功能并指定哪些网站将使用该功能，可使用组策略。

注 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

- 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。
- 确认已将 Horizon Agent 配置 ADM 模板（vdm_agent.adm 文件）添加到远程桌面的 OU。请参阅[将 View ADM 模板添加到 GPO 中](#)。
- 编译一个可以或无法重定向 Flash 内容的网站列表。编译一个白名单以确保仅在列表中指定的 URL 可以重定向 Flash 内容。编译一个黑名单以确保在列表中指定的 URL 无法重定向 Flash 内容。
- 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 Windows 7、Windows 8、Windows 8.1 或 Windows 10 客户端系统上，安装所需的 Horizon Client 版本和 Flash Player ActiveX 版本。
 - 安装 Horizon Client 4.0 或更高版本。请参阅《使用适用于 Windows 的 VMware Horizon Client》文档中有关安装 Horizon Client 的主题。
 - 必要时，安装 Flash Player 的 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，可能需要访问以下站点来下载并安装 Flash Player: <https://get.adobe.com/flashplayer/>。
- 2 在 Windows 7、Windows 8、Windows 8.1 或 Windows 10 远程桌面上，安装所需版本的 Horizon Agent 和 Internet Explorer 以及 Flash Player。
 - 安装 Horizon Agent 7.0 或更高版本，并确保选择 Flash 重定向（实验）所对应的选项。默认情况下，不会选择此选项。
 - 安装 Internet Explorer 9、10 或 11。
 - 必要时，安装 Flash Player 的 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，可能需要访问以下站点来下载并安装 Flash Player: <https://get.adobe.com/flashplayer/>。
- 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，然后编辑计算机配置下的 Flash 重定向策略设置。

这些设置位于计算机配置 > 策略 > 管理模板 > 经典管理模板 > VMware Horizon Agent 配置 > VMware FlashMMR 文件夹中。

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。
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， 400,300 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 320,200 。

5 在组策略管理编辑器中，编辑**用户配置**下的 **Flash 重定向策略**设置。

这些设置位于**用户配置 > 策略 > 管理模板 > 经典管理模板 > VMware Horizon Agent 配置 > VMware FlashMMR** 文件夹中。

- a 打开 **FlashMMR URL 列表**用法定义设置以定义要用于 **Flash 重定向**的主机 URL 列表，然后选择**已启用**单选按钮。
- b 在 URL 用法下拉列表中，选择以启用一个白名单或黑名单。
 - 要启用一个白名单，请选择**启用白名单**。
 - 要启用一个黑名单，请选择**启用黑名单**。默认情况下，将启用白名单。
- c 打开**要启用/禁用 FlashMMR 的主机 URL 列表**设置以添加使用或不使用 **Flash 重定向**的主机 URL 列表，然后选择**已启用**单选按钮。
- d 单击**显示**按钮。
- e 在“名称”列中输入作为前提条件编译的完整 URL，然后将“值”列保留空白。

确保包含 **http://** 或 **https://**。您可以使用正则表达式。例如，可以指定 **https://*.google.com** 和 **http://www.cnn.com**。

(Horizon 7.0) 将“值”列保留为空。

(Horizon 7.0.1) 在“值”列中，可以选择指定 **requireIECompatibility=true** 或 **appMode=0**，或者同时指定两者（使用逗号分隔两个字符串）。

网站默认支持 HTML5，**Flash 重定向**不适用于这些网站。必须设置

requireIECompatibility=true，才能对这些站点使用该功能。**YouTube** 网站不需要此参数。

默认情况下，在 **Flash 重定向**运行时会启用外部接口支持。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。

6 在代理计算机上，打开命令提示符，然后更改到以下目录：

```
%Program Files%\Common Files\VMware\Remote Experience
```

7 运行以下命令以将白名单或黑名单添加到 Internet Explorer 中。

```
cscript mergeflashmmrwhitelist.vbs
```

8 重新启动 Internet Explorer。

设置了参数 **requireIECompatibility=true** 的网站会被添加到 Internet Explorer 的兼容性视图。通过从菜单栏中选择**工具 > 兼容性视图设置**，可以验证此操作。

只有在 Horizon 7.0 中，这些站点还会被添加到 Internet Explorer 的受信任站点列表。通过从 Internet Explorer 菜单栏中选择**工具 > Internet 选项**，然后在**安全选项卡**上单击**站点**按钮，可以验证受信任的站点。

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 GPO 设置配置 Flash 重定向的替代方法。

前提条件

- 编译一个网站白名单以确保仅在列表中指定的 URL 可以重定向 Flash 内容。虽然您可以编译一个网站黑名单，但无法使用 Windows 注册表设置启用该黑名单。黑名单确保仅在列表中指定的 URL 无法重定向 Flash 内容。要启用黑名单，您必须使用 GPO 设置配置 Flash 重定向。
- 确认在远程桌面上安装了 Horizon Agent 7.0 或更高版本以及 Flash Player 和 Internet Explorer 9、10 或 11。请参阅[安装并配置 Flash 重定向](#)。
- 确认您使用的是 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（代理计算机）。
- 2 在代理计算机上打开 Windows 注册表编辑器 (regedit.exe)，导航到以下文件夹，并将 **FlashRedirection** 设置为 1:

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

注 此设置会启用 Flash 重定向功能，但如果在 HKLM\Software\Policies\VMware, Inc.\VMware FlashMMR 中禁用此设置（设置为 0），则意味着将在域范围禁用 Flash 重定向，并且需要由域管理员来启用该功能。

- 3 导航到以下文件夹:

```
HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMware FlashMMR
```

如果尚不存在此文件夹，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**，然后输入将使用 Flash 重定向的网站 URL 以作为名称。

您可以使用正则表达式。例如，可以指定 **https://*.google.com**。请确保将**数据**值保留为空。

- 6 （可选）（仅限 Horizon 7.0.1 和 7.0.2）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（使用逗号分隔两个字符串）。

网站默认支持 HTML5，Flash 重定向不适用于这些网站。必须设置 **requireIECompatibility=true**，才能对这些站点使用该功能。YouTube 网站不需要此参数。

默认情况下，在 Flash 重定向运行时会启用外部接口支持。这可能会降低性能。对于 Horizon 7.0.1 或更高版本，在特定情况下，设置 **appMode=0** 可提升性能，设置 **appMode=1** 可改善用户体验。

- 7 重复上述步骤以添加其他 URL，完成后，关闭注册表编辑器。
- 8 在代理计算机上，打开命令提示符，然后更改到以下目录：

```
%Program Files%\Common Files\VMware\Remote Experience
```

- 9 运行以下命令以将白名单添加到 Internet Explorer。

```
cscript mergeflashmmrwhitelist.vbs
```

- 10 重新启动 Internet Explorer。

设置了参数 **requireIECompatibility=true** 的网站会被添加到 Internet Explorer 的兼容性视图。通过从菜单栏中选择 **工具 > 兼容性视图设置**，可以验证此操作。

只有在 Horizon 7.0 中，这些站点还会被添加到 Internet Explorer 的受信任站点列表。通过从 Internet Explorer 菜单栏中选择 **工具 > Internet 选项**，然后在安全选项卡上单击 **站点** 按钮，可以验证受信任的站点。

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 配置为始终在客户端或者远程桌面或应用程序中打开。您可以重定向用户在 Internet Explorer 地址栏中键入的 URL 以及应用程序中用户可以单击的链接。您可以为重定向配置任意数量的协议，例如，HTTP、mailto 和 callto。

URL 内容重定向功能支持以下方向的 URL 重定向。

从客户端到远程桌面或应用程序（客户端到代理的重定向）

Horizon Client 会根据您设置的规则，打开远程桌面或远程应用程序来处理 URL。如果打开桌面，URL 协议的默认应用程序会处理该 URL。

要使用客户端到代理重定向，您必须为 Horizon Client 和 Horizon Agent 启用 URL 内容重定向功能。

从远程桌面或应用程序到客户端（代理到客户端的重定向）

Horizon Agent 会将 URL 发给 Horizon Client，后者将根据 URL 中指定的协议打开默认应用程序。

要使用代理到客户端重定向，您必须为 Horizon Agent 启用 URL 内容重定向功能。无需为 Horizon Client 启用 URL 内容重定向功能。

您可以将一些 URL 从远程桌面或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应用程序。配置组策略设置以指示对于每个协议，Horizon Agent 或 Horizon Client 应如何重定向 URL。

您可以在环境中的远程桌面上安装 Horizon Client，这意味着 Horizon Agent 和 Horizon Client 安装在同一台计算机上。例如，用户登录到瘦客户端设备，并连接到远程桌面。用户从该桌面运行 Horizon Client 来访问远程应用程序。在此桌面计算机上，您可以安装具有 URL 内容重定向功能的 Horizon Agent，或安装具有该功能的 Horizon Client，但不能同时安装两者。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。

URL 内容重定向的要求和限制

URL 内容重定向功能具有特定要求和限制。

URL 内容重定向功能要求

URL 内容重定向功能具有以下要求：

- 适用于 Windows 的 Horizon Client 4.0 或更高版本。
- 适用于 Mac 的 Horizon Client 4.2 和 4.3。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。
- 支持在 Internet Explorer 9、10 和 11 中键入或单击一个 URL 并重定向该 URL。
- 远程会话的显示协议必须是 VMware Blast 或 PCoIP。

URL 内容重定向功能限制

URL 内容重定向功能的行为可能会出现以下意外结果：

- 如果 URL 根据区域设置打开一个国家/地区特定的页面，打开的区域设置页面是由链接来源决定的。例如，如果远程桌面（代理来源）位于日本的数据中心，用户的计算机位于美国，并且将 URL 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本页面。
- 如果用户从网页中创建收藏项，将在重定向后创建收藏项。例如，假设用户在客户端计算机上单击一个链接，并且将 URL 重定向到远程桌面（代理）。如果用户为该页面创建一个收藏项，将在代理上创建该收藏项。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，但该收藏项存储在代理（远程桌面）上。
- 用户下载的文件被下载到用来打开 URL 的浏览器所在的计算机上，例如，如果用户在客户端计算机上单击链接，该 URL 会被重定向到远程桌面。如果链接用于下载文件，或者链接用于用户从中下载文件的网页，文件将下载到远程桌面，而不是客户端计算机。

不支持的 URL 内容重定向功能

在以下情况下，URL 内容重定向功能无法正常工作：

- 缩短的 URL（如 <https://goo.gl/abc>）可以根据过滤规则进行重定向，但过滤机制不会查看原始的未缩短 URL。例如，如果您的规则对包含 [acme.com](http://www.acme.com/some-really-long-path) 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。

解决办法：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 页面将绕过 URL 重定向。例如，假设用户访问与 URL 重定向规则不匹配的 URL。如果页面包含嵌入的 HTML 页面（iFrame 或内嵌框架）并且其 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。
- 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。

解决办法：使用 GPO 设置以防止用户禁用插件。这些设置包括以下内容：“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，可以在**计算机配置 > 管理模板 > Windows 组件 > Internet Explorer** 中找到这些设置。

Internet Explorer 特定的解决办法：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，可以在**计算机配置 > 管理模板 > Windows 组件 > Internet Explorer > 隐私**中找到这些设置。

这两种解决办法是推荐的最佳做法，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。

- 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，以便将其下载到个人计算机、平板电脑和手机）包括 Microsoft Edge 浏览器、Mail、Maps、Photos、Grove Music，等等。因此，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。

解决办法：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。

- 启用了安全引导的计算机将禁用 URL 内容重定向功能。无法从这些计算机中重定向 URL。不过，可以将 URL 重定向到这些计算机。

安装具有 URL 内容重定向功能的 Horizon Client

要支持从客户端到远程桌面或应用程序的 URL 内容重定向（客户端到代理的重定向），必须安装具有 URL 内容重定向功能的 Horizon Client。

对于适用于 Windows 的 Horizon Client，您必须使用命令行选项运行适用于 Windows 的 Horizon Client 安装程序。通过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。例如：

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

在按照提示完成安装后，可以通过检查 `vmware-url-protocol-launch-helper.exe` 文件和 `vmware-url-filtering-plugin.dll` 文件是否已安装在 `%PROGRAMFILES%\VMware\VMware Horizon View Client\` 目录中来确认已安装该功能。此外，还需确认已安装以下 Internet Explorer 加载项：VMware Horizon View URL 过滤插件。

注 适用于 Mac 的 Horizon Client 不支持客户端到代理重定向。

安装具有 URL 内容重定向功能的 Horizon Agent

要支持从远程桌面或应用程序到客户端的 URL 内容重定向（代理到客户端的重定向），必须安装具有 URL 内容重定向功能的 Horizon Agent。

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


在按照提示完成安装后，可以通过检查 `vmware-url-protocol-launch-helper.exe` 文件和 `vmware-url-filtering-plugin.dll` 文件是否已安装在 `%PROGRAMFILES%\VMware\VMware View\Agent\bin\UrlRedirection\` 目录中来确认已安装此功能。此外，还需确认已启用以下 Internet Explorer 加载项：VMware Horizon View URL 过滤插件。

在 Active Directory 中添加 URL 内容重定向 ADM 模板

您可以将 URL 内容重定向 ADM 文件 `urlRedirection-enUS.adm` 中的策略设置添加到 Active Directory 的组策略对象 (Group Policy Object, GPO) 中，并在组策略对象编辑器中配置这些设置。

前提条件

- 如果您打算为在远程桌面或应用程序中单击的链接设置策略，请确认您在安装 Horizon Agent 时将 URL 内容重定向功能包括在内。请参阅[配置 URL 内容重定向](#)。
- 如果您打算为在客户端浏览器或应用程序中单击的链接设置策略，请确认您在安装 Horizon Client 时将 URL 内容重定向功能包括在内。请参阅[配置 URL 内容重定向](#)。
- 验证是否为 URL 内容重定向组策略设置创建了 Active Directory GPO。对于有关从远程桌面或应用程序中单击的链接的规则，必须将 GPO 链接到包含桌面和 RDS 主机的 OU。对于从客户端系统中单击的链接，必须将 GPO 链接到包含客户端计算机的 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 URL 内容重定向组策略设置。请参阅 [VMware Horizon URL 内容重定向模板设置](#)。

步骤

- 1 从 VMware 下载站点中下载 View 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 View 提供组策略设置的所有 ADM 和 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 ADM 文件 `urlRedirection-enUS.adm` 复制到 Active Directory 服务器中。
- 3 在 Active Directory 服务器上编辑 GPO，方法是选择开始 > 管理工具 > 组策略管理，右键单击 GPO，然后选择编辑。
- 4 在组策略对象编辑器中，右键单击计算机配置 > 策略 > 管理模板文件夹，然后选择添加/删除模板。
- 5 单击添加，浏览到 `urlRedirection-enUS.adm` 文件，然后单击打开。
- 6 单击关闭以将 ADM 文件中的策略设置添加到 GPO 中。

这些设置位于计算机配置 > 策略 > 管理模板 > 经典管理模板 > VMware Horizon URL 重定向文件夹中。

- 7 配置 URL 内容重定向组策略设置。

将为 OU 中包含的 RDS 主机的客户端计算机或远程桌面组配置组策略。

VMware Horizon URL 内容重定向模板设置

Horizon URL 内容重定向 ADM 模板文件 (`urlRedirection-enUS.adm`) 包含与控制在客户端还是代理端（远程桌面或应用程序）中打开 URL 链接有关的策略设置。例如，为了提高安全性，管理员可以设置一个策略，以便在远程桌面或应用程序中为在公司网络内部工作的所有员工打开指向公司网络外部的所有 URL 链接。

该 ADM 文件包含在名为 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` 的捆绑 .zip 文件中，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，其中包含捆绑的 .zip 文件。

如果最终用户在浏览器或应用程序（如 Microsoft Word 文档或电子邮件）中单击 URL 链接，或者用户在 Internet Explorer 9、10 或 11 浏览器中单击或键入 URL，可能会发生 URL 内容重定向。URL 链接可以是指向网页、电话号码、电子邮件地址等的链接。

URL 内容重定向规则的语法

当指定在客户端或代理上打开哪些 URL 时，您可以使用正则表达式。请使用分号分隔多个条目。不允许在条目之间使用空格。

下面是一些示例。

条目	说明
<code>.*</code>	（点-星号）指定应重定向所有 URL。如果为 agentRules 选项使用该设置，所有 URL 将重定向到代理端，这意味着在远程桌面或应用程序中打开 URL。如果为 clientRules 选项使用该设置，指定的 URL 将重定向到客户端。
<code>.*.acme.com;.*.example.com</code>	指定应重定向包含文本 <code>.acme.com</code> 或 <code>example.com</code> 的所有 URL。
[空格或保留空白]	要指定不应重定向任何 URL，请使用空格或将该设置保留空白。例如，如果将 clientRules 保留空白，则指定不应将任何 URL 重定向到客户端。

对于 **agentRules**，您还必须使用 **brokerHostname** 选项指定连接服务器的 IP 地址或完全限定域名，并且必须使用 **remoteItem** 选项指定桌面或应用程序池的显示名称，如 View Administrator 中所示。

代理到客户端重定向

如果希望将某些 URL 重定向到客户端，请将模板添加到远程桌面或应用程序池的 GPO 中。

例如，可以使用代理到客户端重定向节约资源或作为额外的安全层。如果员工在远程桌面或应用程序中工作并希望观看视频，您可以将这些 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。或者，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，将与公司无关的内容（即，未指向公司网络的 URL）重定向在客户端计算机上打开。在这种情况下，您可以使用以下包含正则表达式的设置：

- 对于 **agentRules**: `.*.mycompany.com`

该规则意味着，应在代理上打开包含文本 `mycompany.com` 的任何 URL。

■ 对于 **clientRules**: `.*`

该规则意味着，应在客户端上使用默认客户端浏览器打开所有 URL。

该功能使用以下过程以应用规则：

- 1 当用户在远程应用程序或桌面中单击链接时，将先检查客户端规则。
- 2 如果 URL 中的模式与客户端规则匹配，则随后检查代理规则。
- 3 如果代理规则与客户端规则发生冲突，则将在本地打开链接，也就是在代理计算机上打开链接。
- 4 如果不发生冲突，则将 URL 重定向到客户端。

在上面的示例中，发生规则冲突，因为包含 **mycompany.com** 的 URL 是所有 URL 的一个子集。由于该冲突，将在本地打开包含 **mycompany.com** 的 URL。如果在远程桌面中单击 URL 包含 **mycompany.com** 的链接，将在该远程桌面上打开 URL。如果从客户端系统中单击 URL 包含 **mycompany.com** 的链接，将在客户端上打开 URL。

客户端到代理重定向

如果希望将某些 URL 重定向到远程桌面或应用程序，请将该模板添加到一组客户端计算机的 GPO 中。例如，为了安全起见，您可能希望在远程桌面或应用程序中打开指向公司网络的所有 URL。在这种情况下，您可以将 **agentRules** 设置为：

```
.*.mycompany.com
```

要将 URL 重定向到远程桌面或应用程序池，您还必须指定要使用的池。请使用 **brokerHostname** 选项指定连接服务器的 IP 地址或完全限定域名，并使用 **remoteltem** 选项指定桌面或应用程序池的显示名称，如 **View Administrator** 中所示。

如果将 URL 重定向到远程桌面，将在该桌面的默认浏览器中打开链接。如果将 URL 重定向到远程应用程序，将使用指定的应用程序池打开链接。最终用户必须有权访问指定的桌面或应用程序池。

您可以将该模板添加到代理和客户端的 GPO 中，但如果您这样做，请确保这些规则不会发生冲突，或者任何冲突是有意为之的。

模板设置详细信息

下表说明了 Horizon URL 内容重定向 ADM 模板文件中的策略设置。该模板仅包含“计算机配置”设置。

表 14-2. Horizon URL 内容重定向模板设置

设置	属性
IE Policy: Users can't disable URL Redirection plugin	确定用户是否可以禁用 URL 内容重定向。 默认情况下禁用此设置。
IE Policy: Automatically activate newly installed plugins	确定是否自动激活新安装的 Internet Explorer 插件。 默认情况下禁用此设置。
Url Redirection Enabled	确定是否启用该功能。 默认情况下启用此设置。即使已安装该组件，也可以使用该设置禁用该功能。

设置	属性
Url Redirection Protocol 'http'	<p>对于使用 HTTP 协议的所有 URL，请指定应重定向的 URL。</p> <p>例如，如果将 agentRules 设置为 .*.mycompany.com，则包含“mycompany.com”的所有 URL 将重定向到远程桌面或远程应用程序。您可以设置 brokerHostname 以进一步指定要使用的连接服务器，以及将 remoteItem 设置为池显示名称以指定要使用的桌面或应用程序池，如 View Administrator 中所示。</p> <p>如果将 clientRules 设置为 .*.mycompany.com，则包含“mycompany.com”的所有 URL 将重定向到基于 Windows 的客户端，并在客户端上的默认浏览器中打开。</p> <p>注 最佳做法是，为 HTTP 协议和 HTTPS 协议设置相同的规则。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 内容重定向功能将正常工作。在这种情况下，如果为 HTTPS 设置一个规则，但没有为 HTTP 设置规则，则不会重定向用户键入的部分 URL。</p> <p>默认情况下禁用此设置。</p>
Url Redirection Protocol 'https'	<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>注 最佳做法是，为 HTTPS 协议和 HTTP 协议设置相同的规则。</p> <p>默认情况下禁用此设置。</p>
Url Redirection Protocol 'callto'	<p>对于使用 callto 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>默认情况下禁用此设置。</p>
Url Redirection Protocol 'email'	<p>对于使用 email 或 mailto 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>默认情况下禁用此设置。</p>
Url Redirection Protocol '[...]'	<p>您可以为任何其他协议修改此模板。如果您不需要配置任何其他协议，可以在将 ADM 模板添加到 Active Directory 之前删除或注释掉此条目。</p>

注 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 GPO 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。

配置实时音频-视频

通过实时音频-视频功能，View 用户可以在其远程桌面上运行 Skype、Webex、Google Hangouts 和其他在线会议应用程序。使用实时音频-视频，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桌面。该功能可将视频和音频数据重定向到桌面，其占用的带宽远小于 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。

要使用此功能，需在桌面操作系统上安装 VMware Virtual Webcam 和 VMware Virtual Microphone。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。VMware Virtual Webcam 和 VMware Virtual Microphone 会显示在桌面操作系统的设备管理器中。

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 View 桌面中使用。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。也可以设置策略以禁用或启用该功能。利用 ADM 模板文件，您可以在 Active Directory 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到桌面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桌面时，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，您将无法在远程桌面上对其进行访问。

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，并支持 Skype、WebEx 和 Google Hangouts 等标准会议应用程序。要支持实时音频-视频，View 部署必须满足特定的软件和硬件要求。

View 远程桌面

您可以安装 View Agent 6.0 或更高版本或者 Horizon Agent 7.0 或更高版本以安装实时音频-视频功能。要在 RDS 桌面和远程应用程序中使用该功能，您必须安装 Horizon Agent 7.0.2 或更高版本。请参阅[在虚拟机上安装 Horizon Agent](#)。

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 处理器不支持该功能。
- 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详细信息，请参阅适用于相应系统或设备的《使用 VMware Horizon Client》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。要支持实时音频-视频，您不需要在安装了代理的桌面操作系统上安装设备驱动程序。

View 的显示协议

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

RDP 桌面会话不支持实时音频-视频。

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桌面。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

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或麦克风，远程桌面或应用程序将仅使用其中一个。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，则远程桌面或应用程序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，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，进而导致设备不能使用实时音频-视频功能。

此操作方法仅对适用于 Windows 的 Horizon Client 4.2 及更高版本才适用。对于较低的客户端版本，您必须修改注册表设置来选择首选网络摄像头，使用 Windows 操作系统中的“声音控制”来选择默认麦克风。有关更多信息，请参阅与您的 Horizon Client 版本对应的《使用适用于 Windows 的 VMware Horizon Client》文档。

前提条件

- 确认客户端系统中已安装 USB 网络摄像头或 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或应用程序中使用 VMware Blast 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**。

您可以通过单击桌面和应用程序屏幕右上角的**设置**（齿轮）图标，或通过右键单击桌面或应用程序图标，然后选择**设置**来打开“设置”对话框。

- 2 从**首选 Webcam** 下拉菜单中选择首选网络摄像头，从**首选麦克风**下拉菜单中选择首选麦克风。

这两个下拉菜单中会分别显示客户端系统上的可用网络摄像头和麦克风。

- 3 单击**确定**或**应用**保存更改。

当您在下一次启动远程桌面或应用程序时，会将您选择的首选网络摄像头和麦克风重定向到远程桌面或应用程序。

在 Mac 客户端系统上选择默认麦克风

如果您的客户端系统中有多多个麦克风，远程桌面只使用其中一个麦克风。您可以使用客户端系统上的“系统偏好设置”指定哪个麦克风是远程桌面上的默认麦克风。

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麦克风。管理员也可以使用 **Mac** 默认系统配置首选的麦克风。请参阅在 [Mac 客户端系统上配置首选的网络摄像头或麦克风](#)。

重要事项 如果使用 **USB** 麦克风，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 在客户端系统上，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客户端系统选择的默认麦克风。

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-视频的语法

可以使用以下命令来配置实时音频-视频功能。

表 14-3. 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-pid.log）的日志级别。可以将日志级别设置为 trace 或 debug。
<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 true。
<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率下的高分辨率。

在 Mac 客户端系统上配置首选的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或麦克风，在远程桌面中只能使用一个网络摄像头和一个麦克风。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 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。

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 客户端系统上选择默认麦克风](#)。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，请验证客户端系统中已安装网络摄像头并可正常使用。
- 如果要配置首选 USB 麦克风或其他类型的麦克风，请验证客户端系统中已安装麦克风并可正常使用。
- 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 Mac 客户端系统上，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`。

- 在 Terminal (/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： <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： <pre>defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"</pre>

- （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，该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个麦克风，View 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

- 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。

- 单击“声音首选项”对话框中的输入选项卡。
- 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 View 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 View 桌面上对控制实时音频-视频 (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 View 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 (ADM) 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-视频设置帧率和分辨率》(Setting Frame Rates and Resolution for Real-Time Audio-Video on Horizon View Clients)，网址为 <http://kb.vmware.com/kb/2053644>。

向 Active Directory 中添加 RTAV ADM 模板并配置设置

您可以将 RTAV ADM 文件 `vdm_agent_rtav.adm` 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

- 确认您的桌面中安装了 RTAV 设置选项。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[在虚拟机上安装 Horizon Agent](#)。
- 验证已经为 RTAV 组策略设置创建了 Active Directory GPO。这些 GPO 必须链接到包含桌面的组织单位 (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 View 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 View 提供组策略设置的所有 ADM 和 ADMX 文件均在此文件中提供。

- 2 解压 `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip` 文件，并将 RTAV ADM 文件 `vdm_agent_rtav.adm` 复制到 Active Directory 服务器。
- 3 在 Active Directory 服务器上编辑 GPO，方法是选择开始 > 管理工具 > 组策略管理，右键单击 GPO，然后选择编辑。
- 4 在组策略对象编辑器中，右键单击计算机配置 > 管理模板文件夹，然后选择添加/移除模板。
- 5 单击添加，浏览至 `vdm_agent_rtav.adm` 文件并单击打开。
- 6 单击关闭，将 ADM 文件中的策略设置应用到 GPO。

这些设置位于计算机配置 > 策略 > 管理模板 > 经典管理模板 > VMware Horizon Agent 配置 > View RTAV 配置文件夹中。

- 7 配置 RTAV 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 View 桌面，而不是已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 - 最大图像... 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 - 默认映像... 组策略设置确定当用户未设置分辨率值时所使用的默认值。

组策略设置	说明
禁用 RTAV	启用此设置时，会禁用实时音频-视频功能。 未配置或禁用此设置时，会启用实时音频-视频。 此设置位于 View RTAV 配置 文件夹中。
每秒最大帧数	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。 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。 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 每秒最大帧数 设置，则网络摄像头每秒捕捉 15 帧。 此设置位于 View RTAV 配置 > View RTAV 网络摄像头设置 文件夹中。
分辨率 - 最大图像像素宽度	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。 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。 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。 此设置位于 View RTAV 配置 > View RTAV 网络摄像头设置 文件夹中。
分辨率 - 最大图像像素高度	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。 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。 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。 此设置位于 View RTAV 配置 > View RTAV 网络摄像头设置 文件夹中。
分辨率 - 默认图像分辨率像素宽度	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。 未配置或禁用此设置时，默认映像宽度为 320 像素。 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。 此设置位于 View RTAV 配置 > View RTAV 网络摄像头设置 文件夹中。
分辨率 - 默认图像分辨率像素高度	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。 未配置或禁用此设置时，默认映像高度为 240 像素。 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。 此设置位于 View RTAV 配置 > View RTAV 网络摄像头设置 文件夹中。

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 14-4. 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 View 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 14-4. 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，View 用户可以通过与本地客户端计算机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。Horizon 6.0.2 及更高版本中提供了扫描仪重定向功能。

扫描仪重定向支持与 TWAIN 和 WIA 格式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 ADM 模板文件，您可以在 Active Directory 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，View 部署必须满足特定的软件和硬件要求。

View 远程桌面或应用程序

部署在单用户虚拟机上的 RDS 桌面、RDS 应用程序和 VDI 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，然后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

View 的显示协议

PCoIP

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 RDS 应用程序上，工具托盘图标可以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。
- 如果配置了多台北地连接的扫描仪，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 RDS 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 RDS 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 RDS 应用程序。

有关操作重定向扫描仪的最终用户说明，请参阅《使用适用于 Windows 的 VMware Horizon Client》文档。

配置扫描仪重定向组策略设置

您可以对控制 View 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 (ADM) 文件。

将扫描仪重定向 ADM 模板添加到 Active Directory 中

您可以将扫描仪重定向 ADM 文件 `vdm_agent_scanner.adm` 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

- 确认您的桌面和 RDS 主机中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[在虚拟机上安装 Horizon Agent](#)。
- 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 必须链接到包含桌面和 RDS 主机的组织单位 (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 View 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 View 提供组策略设置的所有 ADM 和 ADMX 文件均在此文件中提供。

- 2 解压 VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip 文件，并将扫描仪重定向 ADM 文件 vdm_agent_scanner.adm 复制到 Active Directory 服务器。
- 3 在 Active Directory 服务器上编辑 GPO，方法是选择开始 > 管理工具 > 组策略管理，右键单击 GPO，然后选择编辑。
- 4 在组策略对象编辑器中，右键单击计算机配置 > 管理模板文件夹，然后选择添加/移除模板。
- 5 单击添加，浏览至 vdm_agent_scanner.adm 文件并单击打开。
- 6 单击关闭，将 ADM 文件中的策略设置应用到 GPO。

这些设置位于计算机配置 > 策略 > 管理模板 > 经典管理模板 > VMware View Agent 配置 > 扫描仪重定向文件夹中。

大多数设置还会添加到用户配置文件夹，该文件夹位于用户配置 > 策略 > 管理模板 > 经典管理模板 > VMware View Agent 配置 > 扫描仪重定向中。

- 7 配置扫描仪重定向组策略设置。

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 ADM 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 VDI 桌面、RDS 桌面和 RDS 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。

组策略设置	描述
禁用功能	<p>禁用扫描仪重定向功能。</p> <p>该设置仅作为计算机配置策略使用。</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>
锁定配置	<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>该设置仅作为计算机配置策略使用。</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>

组策略设置	描述
压缩	<p>在图像传输到远程桌面或应用程序的过程中设置图像压缩率。</p> <p>您可以选择以下压缩模式：</p> <ul style="list-style-type: none"> ■ 禁用。禁用图像压缩。 ■ 无损。使用无损 (zlib) 压缩不会损坏图像质量。 ■ JPEG。使用 JPEG 压缩会损坏图像质量。您可在 JPEG 压缩质量 字段中指定图像质量的级别。JPEG 压缩质量的取值范围为 0 至 100。 <p>启用该设置后，所选压缩模式将适用于所有受此策略影响的用户。但是，用户可以在“VMware Horizon 扫描仪重定向首选项”对话框中更改压缩选项，以覆盖策略设置。</p> <p>禁用此策略设置或不对其进行配置时，将使用 JPEG 压缩模式。</p>
隐藏网络摄像头	<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>该设置作为计算机配置策略和用户配置策略使用。</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”对话框中更改隐藏网络摄像头选项。</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”对话框中更改隐藏网络摄像头选项。</p> <p>当您同时在计算机配置和用户配置中启用该设置时，计算机配置中的隐藏网络摄像头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，隐藏网络摄像头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>
默认扫描仪	<p>提供扫描仪自动选择的集中管理。</p> <p>该设置作为计算机配置策略和用户配置策略使用。</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"> ■ 无。不自动选择扫描仪。 ■ 自动选择：自动选择本地连接的扫描仪。 ■ 上次使用的扫描仪：自动选择上次使用的扫描仪。 ■ 指定扫描仪：选择您在指定扫描仪文本框中键入的扫描仪名称。 <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”对话框中更改默认扫描仪选项。</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”对话框中更改默认扫描仪选项。</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>

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。

在 Horizon 6 版本 6.1.1 和更高版本以及 Horizon Client for Windows 3.4 和更高版本中提供了串行端口重定向功能。

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，而无需进一步配置。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。使用 **ADM** 模板文件，您可以在 **Active Directory** 中或各个桌面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上使用，则您无法在本地计算机上访问该端口。相反地，如果 **COM** 端口正在本地计算机上使用，则您无法在远程桌面上访问该端口。

串行端口重定向的要求

通过使用该功能，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）重定向至其远程桌面。要支持串行端口重定向，您的 **View** 部署必须满足特定的软件和硬件要求。

View 远程桌面

远程桌面必须使用串行端口重定向安装选项在父或模板虚拟机上安装 **View Agent 6.1.1** 或更高版本或者 **Horizon Agent 7.0** 或更高版本。默认情况下，此安装选项处于未选中状态。

单用户虚拟机上支持以下客户机操作系统：

- 32 位或 64 位 Windows 7
- 32 位或 64 位 Windows 8.x
- 32 位或 64 位 Windows 10
- 配置为桌面的 Windows Server 2008 R2
- 配置为桌面的 Windows Server 2012 R2

Windows Server RDS 主机当前不支持该功能。

不需要在安装了代理的桌面操作系统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 客户端系统和 Windows 10 上支持串行端口重定向。
- 必须在客户端计算机上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。您不需要在安装了代理的远程桌面操作系统上安装设备驱动程序。

View 的显示协议

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

RDP 桌面会话中不支持 VMware Horizon 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 (🔌)。

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。

在将 COM 端口断开连接之前，您必须先要在应用程序中关闭该端口或关闭此应用程序。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，并通过从 **自定义端口名称** 下拉列表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《使用适用于 Windows 的 VMware Horizon Client》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。

有关组策略设置的详细信息，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

您可以对控制远程桌面中串行端口重定向行为的组策略设置进行配置。使用这些策略设置，您可以从 Active Directory 对用户桌面上 **VMware Horizon** 的串行 COM 重定向菜单中的可用选项进行集中控制。

您无需配置这些策略设置。串行端口重定向使用为远程桌面和客户端系统上的重定向 COM 端口配置的默认设置。

这些策略设置影响您的远程桌面，而不是已连接物理 COM 端口设备的客户端系统。要在桌面上配置这些设置，请在 Active Directory 中添加串行端口重定向组策略管理模板 (ADM) 文件。

将串行端口重定向 ADM 模板添加到 Active Directory 中

您可以将串行端口重定向 ADM 文件 `vdm_agent_serialport.adm` 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

- 确认您的桌面中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。请参阅[在虚拟机上安装 Horizon Agent](#)。
- 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 必须链接到包含桌面的组织单位 (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 View 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 View 提供组策略设置的所有 ADM 和 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，并将串行端口重定向 ADM 文件 `vdm_agent_serialport.adm` 复制到 Active Directory 服务器。
- 3 在 Active Directory 服务器上编辑 GPO，方法是选择开始 > 管理工具 > 组策略管理，右键单击 GPO，然后选择编辑。
- 4 在组策略对象编辑器中，右键单击计算机配置 > 管理模板文件夹，然后选择添加/移除模板。
- 5 单击添加，浏览至 `vdm_agent_serialport.adm` 文件并单击打开。
- 6 单击关闭，将 ADM 文件中的策略设置应用到 GPO。

这些设置位于计算机配置 > 策略 > 管理模板 > 经典管理模板 > VMware View Agent 配置 > 串行 COM 文件夹中。

大多数设置还会添加到用户配置文件夹，该文件夹位于用户配置 > 策略 > 管理模板 > 经典管理模板 > VMware View Agent 配置 > 串行 COM 中。

- 7 配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

串行端口重定向组策略设置可以控制重定向 COM 端口配置，包括远程桌面上“VMware Horizon 的串行 COM 重定向”菜单中可用的选项。

串行端口重定向 ADM 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 VDI 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。

组策略设置	描述
PortSettings	<p>确定客户端系统上的 COM 端口与远程桌面上的重定向 COM 端口之间的映射，并确定影响重定向 COM 端口的其他设置。</p> <p>您可以分别配置每个重定向 COM 端口。共有五个可用的 PortSettings 策略设置（从 PortSettings 1 至 PortSettings 5），最多可允许将五个 COM 端口从客户端映射到远程桌面。请为您想要配置的每个 COM 端口选择一个 PortSettings 策略设置。</p> <p>启用 PortSettings 政策设置时，您可以配置影响重定向 COM 端口的以下项：</p> <ul style="list-style-type: none"> ■ Source port number 设置用于指定连接到客户端系统的物理 COM 端口的编号。 ■ Destination virtual port number 设置用于指定远程桌面上重定向虚拟 COM 端口的编号。 ■ Autoconnect 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。 ■ IgnoreDSR 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。 ■ Pause before close port (in milliseconds) 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。 ■ Serial2USBModeChangeEnabled 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。 ■ Disable errors in wait mask 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 http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx。 ■ HandleBtDisappear 设置支持蓝牙 COM 端口行为。此设置用于故障排除。 ■ UsbToComTroubleShooting 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。 <p>如果您为某个特定的 COM 端口启用 PortSettings 设置，则用户可以连接重定向端口以及从其断开连接，但无法在远程桌面上配置此端口的属性。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>注 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 PortSettings 设置，则重定向 COM 端口将使用用户在远程桌面上配置的设置。VMware Horizon 的串行 COM 重定向 菜单选项处于活动状态且可供用户使用。</p> <p>该设置作为计算机配置策略和用户配置策略使用。</p>
Local settings priority	<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。</p> <p>该设置作为计算机配置策略和用户配置策略使用。</p>
Disable functionality	<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 VMware Horizon 的串行 COM 重定向 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。</p> <p>该设置仅作为计算机配置策略使用。</p>
Lock configuration	<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 VMware Horizon 的串行 COM 重定向 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 VMware Horizon 的串行 COM 重定向 菜单中的选项。</p> <p>如果未配置此设置，则远程桌面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>

组策略设置	描述
Bandwidth limit	<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 Bandwidth limit (in kilobytes per second) 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>该设置仅作为计算机配置策略使用。</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桌面。

要确保在 Prolific 芯片组适配器上正确传输数据，您可以在 **Active Directory** 中或单个桌面虚拟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

- 确认您的桌面中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。请参阅[在虚拟机上安装 Horizon Agent](#)。
- 确认在 **Active Directory** 中或桌面虚拟机上添加了串行端口重定向 ADM 文件。请参阅[将串行端口重定向 ADM 模板添加到 Active Directory 中](#)。
- 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** 中或虚拟机上，打开组策略对象编辑器。
- 2 浏览到**计算机配置 > 策略 > 管理模板 > 经典管理模板 > VMware View Agent 配置 > 串行 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**，然后关闭组策略对象编辑器。

现在，USB 到串口适配器就可以重定向到远程桌面，并且在用户启动其下一个桌面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

View 为 RDS 桌面和在单用户计算机上运行的 VDI 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，Horizon Client 与 View Secure Gateway 之间的 MMR 连接是安全的，但是从 View Secure Gateway 到桌面计算机的连接未加密。如果禁用安全加密链路，从 Horizon Client 到桌面计算机的 MMR 连接未加密。

启用 View 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 View 的 Horizon Client 系统访问。

默认情况下，View 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 View Administrator 中设置全局策略的说明，请参见 [View 策略](#)。

Windows Media MMR 的系统要求

要支持 Windows Media 多媒体重定向 (MMR)，View 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。

View 远程桌面

- RDS 桌面和在单用户虚拟机上部署的 VDI 桌面上支持该功能。
 - 要在 RDS 桌面上支持该功能，必须安装 View Agent 6.1.1 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。
- 以下是支持的客户机操作系统：
 - 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。

要使用 Internet Explorer，必须禁用“保护模式”。在“Internet 选项”对话框中，单击**安全选项卡**并取消选择**启用保护模式**。

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

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

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

View 策略

在 View 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 View 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 RDS 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 RDS 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 RDS 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
64 位 Windows Media Player	■ 对于 64 位桌面，使用以下注册表项：HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr
32 位 Windows Media Player	■ 对于 32 位桌面，使用以下注册表项：HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr ■ 对于 64 位桌面，使用以下注册表项：HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware tsmmr

- 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

在使用客户端驱动器重定向部署 Horizon Client 3.5 或更高版本以及 View Agent 6.2 或更高版本或者 Horizon Agent 7.0 或更高版本时，将以加密形式通过网络发送文件夹和文件。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。

对于 Horizon Client 4.2 或者 Horizon 7 版本 7.0.2 或更高版本，如果启用 VMware Blast Extreme，文件和文件夹将以加密形式通过虚拟通道进行传输。

对于早期版本的客户端或代理，客户端驱动器重定向文件夹和文件将以未加密的形式通过网络发送，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。如果 Horizon Client 早于 3.5 版或代理早于 6.2 版，请仅在安全网络上使用客户端驱动器重定向，以确保无法在网络上监视该数据。

默认情况下，代理安装程序中的**客户端驱动器重定向**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桌面池中启用**客户端驱动器重定向**安装选项。

使用组策略禁用客户端驱动器重定向

您可以在 Active Directory 中为远程桌面和 RDS 主机配置 Microsoft 远程桌面服务组策略设置，以禁用客户端驱动器重定向。

有关客户端驱动器重定向的详细信息，请参阅《使用 VMware Horizon Client》文档以了解桌面客户端设备的具体类型。请访问 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html。

注 此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

如果 View 部署在基于 DMZ 的安全服务器与内部网络之间配置了后台防火墙，请验证该防火墙是否允许将通信传输到单用户和 RDS 桌面上的端口 9427。需要通过端口 9427 进行 TCP 连接来支持客户端驱动器重定向。

对于 Horizon Client 4.2 或者 Horizon 7 版本 7.0.2 或更高版本，如果启用了 VMware Blast Extreme，并不要求必须打开端口 9427，因为客户端驱动器重定向通过虚拟通道传输数据。

步骤

- 1 在组策略编辑器中，转到计算机配置\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。

该导航路径适用于 Windows Server 2012 上的 Active Directory。在其他 Windows 操作系统上，该导航路径将有所不同。

- 2 启用不允许驱动器重定向组策略设置。

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。

限制复制和粘贴操作的剪贴板格式

您可以配置组策略设置，以控制允许用户在 **PCoIP** 和 **VMware Blast** 会话期间复制和粘贴数据时使用的剪贴板格式。如果您出于安全原因需要限制复制和粘贴操作，此功能会很有用。

您可以根据复制和粘贴操作的方向来配置剪贴板格式限制。例如，您可以针对从客户端系统复制到远程桌面的数据配置一组策略，而针对从远程桌面复制到客户端系统的数据配置另一组策略。

对于 PCoIP 会话，用于过滤剪贴板内容的组策略设置位于 PCoIP 组策略模板文件 `pcoip.adm` 中。请参阅 [PCoIP 剪贴板设置](#)。对于 VMware Blast 会话，用于过滤剪贴板内容的组策略设置位于 VMware Blast 组策略模板文件 `vdm_blast.adm` 中。请参阅 [VMware Blast 策略设置](#)。这些组策略设置仅适用于 Horizon Agent，且仅适用于版本 7.0.2 及更高版本。

剪贴板格式过滤示例

以下示例说明了如何使用组策略设置在执行复制和粘贴操作期间过滤剪贴板格式。

- 要在用户将数据从其客户端系统复制到远程桌面时，过滤掉非 Microsoft Office 应用程序（例如 Wordpad）的图像，请启用 `Filter images out of the incoming clipboard data` 组策略设置。
- 要在用户将数据从其客户端系统复制到远程桌面时，同时过滤掉非 Microsoft Office 应用程序和 Microsoft Office 应用程序的图像，请启用 `Filter Microsoft Chart and Smart Art data out of the incoming clipboard data` 和 `Filter images out of the incoming clipboard data` 组策略设置。`Filter Microsoft Chart and Smart Art data out of the incoming clipboard data` 组策略设置会过滤掉 Microsoft Office 图表和 Smart Art 数据，可能包括图像。
- 要在用户将数据从其客户端系统复制到远程桌面时，仅过滤掉 Microsoft Office 图表和 Smart Art 数据，请仅启用 `Filter Microsoft Chart and Smart Art data out of the incoming clipboard data` 组策略设置。
- 要在用户将数据从其客户端系统复制到远程桌面及从远程桌面复制到其客户端系统时，过滤掉 Microsoft Word 相关文本格式，请启用入站组策略设置 `Filter Microsoft Text Effects data out of the incoming clipboard data` 和 `Filter Rich Text Format data out of the incoming clipboard data`，以及出站组策略设置 `Filter Microsoft Text Effects data out of the outgoing clipboard data` 和 `Filter Rich Text Format data out of the outgoing clipboard data`。
- 要在用户将数据从其客户端系统复制到远程桌面及从远程桌面复制到其客户端系统时，过滤掉 Microsoft Word 的图像，请启用入站组策略设置 `Filter Rich Text Format data out of the incoming clipboard data` 和出站组策略设置 `Filter Rich Text Format data out of the outgoing clipboard data`。Microsoft Word 中的图像以复合 RTF 格式存储。

将 USB 设备与远程桌面和应用程序一起使用

15

管理员可以配置从远程桌面使用各种 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。该功能称为 **USB 重定向**，它支持使用 **Blast Extreme**、**PCoIP** 或 **Microsoft RDP** 显示协议。远程桌面最多可容纳 128 个 USB 设备。

还可以重定向本地连接的 USB 拇指闪存盘和硬盘以便在 RDS 桌面和应用程序中使用。RDS 桌面和应用程序中不支持其他类型的 USB 设备，包括其他类型的存储设备。

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，无法在客户端系统中和远程桌面或应用程序中同时使用 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某些类型的客户端。为确定某个特定类型的客户端是否支持该功能，请参阅针对特定桌面或移动客户端设备类型的“使用 VMware Horizon Client”文档中提供的功能支持表。请访问 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html。

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 View 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](#)
- [设置 USB 重定向概述](#)
- [网络流量和 USB 重定向](#)
- [自动连接到 USB 设备](#)
- [在安全 View 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

View 虽然没有明确阻止任何设备在远程桌面上运行，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。

在 Horizon 6.0.1 以及 Horizon Client 3.1 或更高版本中，您可以将 USB 3.0 设备插入到客户端计算机（Windows、Linux 和 Mac）上的 USB 3.0 端口中。仅支持单个流通过 USB 3.0 设备。由于本版本中未实现多流支持，因此 USB 设备性能未得到增强。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 VDI 会话中可能不起作用。

在较早的 View 版本中，虽然不支持超高速 USB 3.0 设备，但 USB 3.0 设备插入客户端计算机的 USB 2.0 端口后通常可以工作。但是，可能会有例外，这取决于客户端系统主板上的 USB 芯片集类型。

以下类型的设备可能不适合 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该功能正常运行，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。

类似地，USB CD/DVD 读取器以及扫描仪和触摸设备（例如签名平板电脑）在延迟的网络（例如 WAN）上工作效果不佳。

- 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。

您可以将以下类型的设备重定向至 RDS 桌面或应用程序：

- USB 拇指闪存驱动器
- USB 硬盘

对于 Horizon 7 版本 7.0.2，您可以将签名板、语音听写脚踏板和一些 Wacom 平板电脑重定向到 RDS 桌面或应用程序。默认情况下，系统会禁用这些设备。要启用这些设备，请从以下路径删除 Windows 注册表项设置 ExcludeAllDevices 和 IncludeFamily: HKLM\Software\Policies\VMware, Inc\VMware VDM\Agent\USB。

无法将其他类型的 USB 设备和其他类型的 USB 存储设备（如安全存储驱动器和 USB CD-ROM）重定向至 RDS 桌面或应用程序。

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 View 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 重定向功能仅在某些类型的客户端上可用，例如，Windows 客户端、Mac 客户端以及合作伙伴提供的 Linux 客户端。要确定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客户端设备的“使用 VMware Horizon Client”文档中的功能支持表。请访问 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html。

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 View 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，务必包括 USB 重定向组件。

默认已包括此组件。

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

在 View 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 客户端端点，您可以配置组策略；对于 Mac 端点，请使用命令行命令。有关这方面的说明，请参阅针对特定类型客户端设备的“使用 VMware Horizon Client”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。

网络流量和 USB 重定向

USB 重定向独立于显示协议（RDP 或 PCoIP）工作，而 USB 流量通常使用 TCP 端口 32111。

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。

- 1 如果客户端系统位于企业网络内部，使客户端与桌面或应用程序之间可以建立直接连接，USB 流量将使用 TCP 端口 32111。
- 2 如果客户端系统位于企业网络外部，客户端可以通过 View 安全服务器进行连接。

安全服务器位于 DMZ 内，充当受信任网络中的连接代理主机。这样的设计能保护 View 连接服务器实例免受公共 Internet 的威胁，并强制所有无保护的会话请求经过安全服务器传输，从而提供额外的安全保护层。

基于 DMZ 的安全服务器部署要求打开防火墙上的一些端口，以允许客户端与 DMZ 内的安全服务器进行连接。您还需要配置端口，以供内部网络中的安全服务器与 View 连接服务器实例通信使用。

有关具体端口的信息，请参见《View 体系结构规划指南》中的“基于 DMZ 的安全服务器的防火墙规则”。

- 3 如果客户端系统位于企业网络外部，您可以使用 View Administrator 启用 HTTPS 安全加密链路。然后，当用户连接到远程桌面或应用程序时，客户端会与 View 连接服务器或安全服务器主机再建立一个 HTTPS 连接。该连接使用 HTTPS 端口 443 通过安全加密链路连接至安全服务器，接着用于从服务器向远程桌面或应用程序传输 USB 流量的连接使用 TCP 端口 32111。使用这种安全加密链路时，USB 设备的性能会稍有下降。

注 如果您使用了零客户端，将使用 PCoIP 虚拟通道（而非通过 TCP 32111）重定向 USB 流量。数据由 PCoIP 安全网关通过 TCP/UDP 端口 4172 进行封装和加密。如果您仅使用零客户端，则没必要开启 TCP 端口 32111。

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。

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到远程桌面，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。在某些情况下，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：

- 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，远程桌面将接收触摸输入而非键盘输入。

如果您已将远程桌面设置为连接 USB 设备，可以配置一条策略来排除诸如触摸屏和网络设备的特定设备。有关更多信息，请参阅[为 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，设置 Horizon Client 仅将特定的一个或多个设备（如智能手机和平板电脑）重新连接到远程桌面。有关这方面的说明，请参阅《使用适用于 Windows 的 VMware Horizon Client》。

在安全 View 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 View 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 View 桌面和应用程序。或者，也可以禁用特定 USB 设备的重定向，以只允许用户访问其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 View 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** 设置选项。（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 View 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 RDS 桌面和应用程序池。无法为各个 RDS 桌面或应用程序池设置此策略。

- 在 View 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 上均可以设置该策略。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 15-1. 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
false 或未定义（包含所有 USB 设备）	false 或未定义（包含所有 USB 设备）	包含所有 USB 设备
false （包含所有 USB 设备）	true （排除所有 USB 设备）	排除所有 USB 设备
true （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 ADM 模板文件 (`vdm_agent.adm`) 中。有关详细信息，请参阅 [Horizon Agent 配置 ADM 模板中的 USB 设置](#)。

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，View 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 View 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《使用适用于 Mac 的 VMware Horizon Client》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 15-2. 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 C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log
Horizon Agent	%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt

客户端或代理	日志文件路径
Mac 客户端	/var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log /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。[表 15-3. USB 策略设置的兼容性](#)说明了 View 如何针对不同的 Horizon Agent 和 Horizon Client 组合应用策略。

表 15-3. 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	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。 注 在 View Agent 6.1 或更高版本以及 Horizon Client 3.3 或更高版本中，这些 USB 重定向策略设置适用于 RDS 桌面和应用程序以及在单用户计算机上运行的远程桌面。
5.1 或更高版本	5.0.x 或更低版本	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。
5.0.x 或更低版本	5.1 或更高版本	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。
5.0.x 或更低版本	5.0.x 或更低版本	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。

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，View 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 15-4. 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	false （自动拆分禁用）	自动拆分禁用
Allow – Default Client Setting	true （自动拆分启用）	自动拆分启用
Allow – Default Client Setting	未定义	自动拆分启用
Allow – Override Client Setting	任意或未定义	自动拆分启用
未定义	未定义	自动拆分禁用

注 这些策略包含在 Horizon Agent 配置 ADM 模板文件 (vdm_agent.adm) 中。有关更多信息，请参阅 [Horizon Agent 配置 ADM 模板中的 USB 设置](#)。

默认情况下，View 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。

View 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，View 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 View 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。**View** 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，**View** 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 15-5. **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 15-5. Horizon Agent 上设备拆分策略设置的拆分修改符

修改符	说明
m （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。
o （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 15-6. 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 15-6. 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 将设备从拆分中排除	根据 Horizon Client 上的供应商/产品 ID 将设备从拆分中排除	根据 Horizon Client 所使用的供应商/产品 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，View 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，View 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，View 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 ADM 模板文件 (vdm_agent.adm) 中。有关更多信息，请参阅 [Horizon Agent 配置 ADM 模板中的 USB 设置](#)。

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 15-7. 用于代理可强制执行的设置的过滤修改符

修改符	说明
m (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。
o (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 15-8. 用于在客户端上解释的设置的过滤修改符

修改符	说明
Default (注册表设置中为 d)	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。
Override (注册表设置中为 o)	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 15-9. 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 (注册表设置中为 d:false)	true (允许)	true (允许)
Disable – Override Client Setting (注册表设置中为 o:false)	true (允许)	false (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 过滤规则时，您可以指定一个系列。

注 有些设备不报告设备系列。

表 15-10. USB 设备系列

设备系列名称	描述
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	开机时除键盘和指针设备之外的其他可用人机接口设备。
imaging	成像设备，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 ADM 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 ADM 模板文件 (vdm_agent.adm) 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。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 ADM 模板文件中拆分复合 USB 设备的各个策略设置。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。关于 View 如何应用拆分复合 USB 设备策略的说明，请参阅[为复合 USB 设备配置设备拆分策略设置](#)。

表 15-11. Horizon Agent 配置模板：设备拆分设置

设置	属性
Allow Auto Device Splitting 属性: AllowAutoDeviceSplitting	允许复合 USB 设备的自动拆分。 未定义默认值，相当于 false 。
Exclude Vid/Pid Device From Split 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]... 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。 例如: o:vid-0781_pid-55** 未定义默认值。
Split Vid/Pid Device 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]) 或 {m o}:vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww]) 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。 例如: o:vid-0781_pid-554c(exintf:01;exintf:02) 注 View 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。 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 ADM 模板文件中代理强制执行的各个 USB 策略设置。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 View 如何应用策略以过滤 USB 设备的说明，请参阅[为 USB 设备配置过滤策略设置](#)。

表 15-12. Horizon Agent 配置模板：代理强制执行的设置

设置	属性
Exclude All Devices 属性: ExcludeAllDevices	<p>禁止转发所有 USB 设备。如果设置为 true，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 false，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。</p> <p>如果设置为 true 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。</p> <p>未定义默认值，相当于 false。</p>
Exclude Device Family 属性: ExcludeFamily	<p>禁止设备系列被转发。设置的格式为 {m o}:family_name_1[;family_name_2]...</p> <p>例如: o:bluetooth;smart-card</p> <p>如果您启用了自动设备拆分，则 View 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 View 会检查整个复合 USB 设备的设备系列。</p> <p>未定义默认值。</p>
Exclude Vid/Pid Device 属性: ExcludeVidPid	<p>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]...</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。</p> <p>例如: m:vid-0781_pid-****;vid-0561_pid-554c</p> <p>未定义默认值。</p>
Include Device Family 属性: IncludeFamily	<p>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]...</p> <p>例如: m:storage</p> <p>未定义默认值。</p>
Include Vid/Pid Device 属性: IncludeVidPid	<p>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]...</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。</p> <p>例如: o:vid-0561_pid-554c</p> <p>未定义默认值。</p>

在客户端上解释的 USB 设置

下表介绍了 Horizon Agent 配置 ADM 模板文件中在客户端上解释的各个策略设置。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 15-13. Horizon Agent 配置模板：在客户端上解释的设置

设置	属性
Allow Audio Input Devices 属性: AllowAudioIn	<p>允许转发音频输入设备。</p> <p>未定义默认值，相当于 true。</p>
Allow Audio Output Devices 属性: AllowAudioOut	<p>允许转发音频输出设备。</p> <p>未定义默认值，相当于 false。</p>
Allow HIDBootable 属性: AllowHIDBootable	<p>允许转发引导时可用的输入设备（也称为可引导的 hid 设备），键盘或鼠标除外。</p> <p>未定义默认值，相当于 true。</p>
Allow Other Input Devices	<p>允许转发输入设备（可引导的 hid 设备和具有集成指针设备的键盘）。</p> <p>未定义默认值。</p>

设置	属性
Allow Keyboard and Mouse Devices 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。 未定义默认值，相当于 false 。
Allow Smart Cards 属性: AllowSmartcard	允许转发智能卡设备。 未定义默认值，相当于 false 。
Allow Video Devices 属性: AllowVideo	允许转发视频设备。 未定义默认值，相当于 true 。

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

以下是可能造成 USB 重定向无法正确或按照预期运行的原因。

- 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](#)。
- 在部署远程桌面和应用程序的 Windows Server 2008 RDS 主机上不支持 USB 重定向。在装有 View Agent 6.1 及更高版本的 Windows Server 2012 RDS 主机上支持 USB 重定向，但该功能仅适用于 USB 存储设备。在用作单用户桌面的 Windows Server 2008 R2 和 Windows Server 2012 R2 系统上支持 USB 重定向。
- RDS 桌面和应用程序上仅支持 USB 闪存驱动器和硬盘。无法将其他类型的 USB 设备和其他类型的 USB 存储设备（如安全存储驱动器和 USB CD-ROM）重定向至 RDS 桌面或应用程序。
- 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 View 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 PCoIP 而不是 RDP 作为协议。
- ◆ 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 View Administrator 中，转到**策略 > 全局策略**，然后验证该 USB 访问是否已在 View 策略下设置为允许。
- ◆ 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。

降低并管理存储要求

在由 vCenter Server 管理的虚拟机上部署桌面，可以实现以前只有虚拟化服务器才能实现的存储效率。将即时克隆或 View Composer 链接克隆作为桌面计算机可以节约存储空间，因为池中的所有虚拟机与基础映像共享一个虚拟磁盘。

本章讨论了以下主题：

- 使用 vSphere 管理存储
- 使用即时克隆减少存储需求
- 使用 View Composer 降低存储要求
- 确定即时克隆和 View Composer 链接克隆桌面池的存储大小
- View Composer 链接克隆虚拟机的存储过载
- View Composer 链接克隆数据磁盘
- 在本地数据存储上存储 View Composer 链接克隆
- 将即时克隆和 View Composer 链接克隆的副本和克隆存储在不同的数据存储中
- 为 View Composer 链接克隆配置 View Storage Accelerator
- 在 View Composer 链接克隆上回收磁盘空间
- 将 VAAI 存储用于 View Composer 链接克隆
- 为 View Composer 链接克隆设置 Storage Accelerator 和空间回收中断时间

使用 vSphere 管理存储

vSphere 可以对磁盘卷和文件系统进行虚拟化，这样您在管理和配置存储时，就无需考虑数据的物理存储位置。

vSphere 支持光纤通道 SAN 阵列、iSCSI SAN 阵列和 NAS 阵列等目前广泛应用的存储技术，用以满足各种数据中心存储需求。存储阵列通过存储区域网络与各个服务器组相连，并在各服务器组之间共享存储资源。采用这种结构能够聚合存储资源，还能更加灵活地将这些资源置备给虚拟机。

兼容的 vSphere 5.0 和 5.1 或更高版本的功能

使用 vSphere 5.0 或更高版本时，可以使用以下功能：

- 利用 View 存储加速器功能，可以将 ESXi 主机配置为缓存虚拟机磁盘数据。

如果使用基于内容的读取缓存 (CBRC)，那么，在引导风暴期间，在多台计算机启动的同时运行防病毒扫描的情况下，IOPS 会减少，性能会提高。主机不再从存储系统中一遍遍地读取整个操作系统，而是从缓存中读取常规数据块。

- 如果远程桌面采用 vSphere 5.1 及更高版本所提供的节省空间的磁盘格式，则客户机操作系统中过期或已删除的数据将通过擦除和压缩流程自动回收。
- 您可以在一定的限制条件下，在最多包含 32 台 ESXi 主机的群集中部署桌面池。

副本磁盘必须存储在 VMFS5 或更高版本的数据存储中或 NFS 数据存储中。如果您将副本磁盘存储在 VMFS5 之前的版本中，群集最多可包含 8 台主机。可将操作系统磁盘和永久磁盘存储在 NFS 或 VMFS 数据存储中。

兼容的 vSphere 5.5 Update 1 或更高版本的功能

借助 vSphere 5.5 Update 1 或更高版本，您可以使用 Virtual SAN，将 ESXi 主机上的本地物理固态磁盘和硬盘驱动器虚拟化，成为一个由群集中所有主机共享的数据存储。Virtual SAN 通过基于策略的管理提供高性能存储，以便创建桌面池时仅指定一个数据存储，各种组件（如虚拟机文件、副本、用户数据和操作系统文件）将放置在适当的固态磁盘 (SSD) 或直连硬盘 (HDD) 上。

Virtual SAN 还通过使用存储策略配置文件来允许您管理虚拟机存储和性能。如果由于主机、磁盘或网络故障或者工作负载发生变化而使策略不合规，Virtual SAN 将重新配置受影响的虚拟机的数据，并优化整个群集内的资源使用情况。您可以在最多包含 20 台 ESXi 主机的群集中部署桌面池。

重要事项 与 vSphere 5.5 Update 1 中提供的功能相比，vSphere 6.0 和更高版本中提供的 Virtual SAN 功能包含了许多性能改进。对于 vSphere 6.0，此功能还具有更广泛的 HCL（硬件兼容性）支持。有关 vSphere 6 或更高版本中 Virtual SAN 的详细信息，请参阅《管理 VMware Virtual SAN》文档。

注 Virtual SAN 与 View 存储加速器功能兼容，但与节省空间的磁盘格式功能不兼容，后者通过擦除和压缩磁盘回收磁盘空间。

兼容的 vSphere 6.0 或更高版本的功能

使用 vSphere 6.0 或更高版本时，可以使用虚拟卷 (VVol)。此功能可将虚拟磁盘及其衍生产品、克隆、快照和副本直接映射到存储系统上名为虚拟卷的对象。此映射允许 vSphere 将密集型存储操作（如快照、克隆和复制）卸载到存储系统。

通过虚拟卷，还可以使用 vSphere 中的存储策略配置文件来管理虚拟机存储和性能。这些存储策略配置文件基于每个虚拟机规定了存储服务。此类型的粒度置备提高了容量利用率。您可以在最多包含 32 台 ESXi 主机的群集中部署桌面池。

注 虚拟卷与 View Storage Accelerator 功能兼容，但与节省空间的磁盘格式功能不兼容，后者通过擦除和压缩磁盘回收磁盘空间。

注 即时克隆不支持虚拟卷。

使用 Virtual SAN 实现高性能存储和基于策略的管理

VMware Virtual SAN 是软件定义的存储层，在 vSphere 5.5 Update 1 或更高版本中提供，用于虚拟化 vSphere 主机群集上提供的本地物理存储磁盘。可以在创建自动桌面池或自动场时仅指定一个数据存储，各种组件（如虚拟机文件、副本、用户数据和操作系统文件）将放在相应的固态硬盘 (SSD) 或直连硬盘 (HDD) 上。

Virtual SAN 实施基于策略的方法来进行存储管理。使用 Virtual SAN 时，View 以您可以修改的默认存储策略配置文件的形式定义虚拟机存储要求（如容量、性能和可用性）。存储根据分配的策略进行置备和自动配置。可以将 Virtual SAN 用于链接克隆桌面池、即时克隆桌面池、完整克隆桌面池或自动场。

无论在群集中的物理位置如何，每个虚拟机都会维护各自的策略。如果策略由于主机、磁盘或网络故障或者工作负载变化而不合规，Virtual SAN 都会重新配置受影响的虚拟机的数据并进行负载平衡，以符合每个虚拟机的策略。

支持需要共享存储的 VMware 功能（例如 HA、vMotion 和 DRS）时，Virtual SAN 不需要再使用外部共享存储基础架构，简化了存储配置和虚拟机置备活动。

重要事项 与 vSphere 5.5 Update 1 中提供的功能相比，vSphere 6.0 和更高版本中提供的 Virtual SAN 功能包含了许多性能改进。对于 vSphere 6.0，此功能还具有更广泛的 HCL（硬件兼容性）支持。此外，VMware Virtual SAN 6.0 还支持使用基于闪存的设备进行缓存和持久存储的全闪存架构。

View 中的 Virtual SAN 工作流

- 1 请使用 vCenter Server 5.5 Update 1 或更高版本以启用 Virtual SAN。有关 vSphere 5.5 Update 1 中的 Virtual SAN 的详细信息，请参见《vSphere 存储指南》文档。有关 vSphere 6 或更高版本中 Virtual SAN 的详细信息，请参见《管理 VMware Virtual SAN》文档。
- 2 在 View Administrator 中创建自动桌面池或自动场时，在**存储策略管理**下选择使用 **VMware Virtual SAN**，然后选择要使用的 Virtual SAN 数据存储。

选择使用 **VMware Virtual SAN** 后，将仅显示 Virtual SAN 数据存储。

将根据您选择的选项创建默认存储策略配置文件。例如，如果您创建了链接克隆，则将自动创建浮动桌面池、副本磁盘配置文件和操作系统磁盘配置文件。如果您创建了链接克隆，则将创建永久桌面池、副本磁盘配置文件和永久磁盘配置文件。对于自动场，将创建副本磁盘配置文件。对于两种类型的桌面池和自动场，将为虚拟机文件创建配置文件。

- 3 要将现有 View Composer 桌面池从另一类型的数据存储移至 Virtual SAN 数据存储，请在 View Administrator 中编辑该池以取消选择旧数据存储并改为选择 Virtual SAN 数据存储，然后使用重新平衡命令。无法为自动场执行该操作，因为您无法重新平衡自动场。
- 4 （可选）使用 vCenter Server 修改存储策略配置文件的参数，其中包括容许的故障次数以及要保留的 SSD 读取缓存量等内容。

这些策略的名称为 OS_DISK（针对操作系统文件）、PERSISTENT_DISK（针对用户数据文件）、REPLICA_DISK（针对副本）和 VM_HOME（针对虚拟机文件，例如 .vmx 和 .vmsn 文件）。对策略所做的更改将传播到新创建的虚拟机以及桌面池或自动场中的所有现有虚拟机。

- 5 使用 vCenter Server 监视 Virtual SAN 群集以及加入了数据存储的磁盘。有关更多信息，请参阅《vSphere 存储》文档和《vSphere 监控和性能》文档。对于 vSphere 6 或更高版本，请参见《管理 VMware Virtual SAN》文档。
- 6 （可选）对于 View Composer 链接克隆桌面池，请像平时一样使用刷新和重构命令。对于自动场，仅支持重构命令，而无论数据存储具有何种类型。

要求和限制

在 View 部署中使用，Virtual SAN 功能具有以下限制：

- 本版本不支持使用 View 节省空间的磁盘格式功能，该功能通过擦除和压缩磁盘回收磁盘空间。
- Virtual SAN 不支持 View Composer Array Integration (VCAI) 功能，因为 Virtual SAN 不使用 NAS 设备。

注 Virtual SAN 与 View Storage Accelerator 功能兼容。Virtual SAN 在 SSD 磁盘上提供一个缓存层，View Storage Accelerator 功能提供基于内容的缓存，该缓存可在发生引导风暴时降低 IOPS 并提高性能。

Virtual SAN 功能具有以下要求：

- vSphere 5.5 Update 1 或更高版本。
- 合适的硬件。例如，VMware 建议为每个对容量有贡献的节点使用 10GB 网卡以及至少一个 SSD 和一个 HDD。有关具体内容，请参阅《VMware 兼容性指南》。
- 至少包含三个 ESXi 主机的群集。您需要足够的 ESXi 主机来容纳您的设置，即使您结合使用两个 ESXi 主机和一个 Virtual SAN 延伸群集也是如此。有关更多信息，请参阅《vSphere 最高配置》文档。
- SSD 容量至少占 HDD 容量的 10%。
- 需要足够的 HDD 来容纳您的设置。磁盘上的利用率不要超过 75%。

有关 Virtual SAN 要求的详细信息，请参见《vSphere 5.5 Update 1 存储》文档中的“使用 Virtual SAN”。对于 vSphere 6 或更高版本，请参见《管理 VMware Virtual SAN》文档。有关为 VMware Virtual SAN 设计 View 虚拟桌面基础架构的关键组件及进行大小调整的指南，请参阅白皮书，网址为：<http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>。

Virtual SAN 数据存储的默认存储策略配置文件

使用 Virtual SAN 时，View 以您可以修改的默认存储策略配置文件的形式定义虚拟机存储要求（如容量、性能和可用性）。存储根据分配的策略进行置备和自动配置。

在桌面池创建过程中创建的默认策略取决于您所创建的池类型。这些策略的名称为 OS_DISK（针对操作系统文件）、PERSISTENT_DISK（针对用户数据文件）、REPLICA_DISK（针对副本）和 VM_HOME（针对虚拟机文件，例如 .vmx 和 .vmsn 文件）。例如，仅针对链接克隆池创建 REPLICA_DISK 策略。对策略所做的更改将传播给新创建的虚拟机以及桌面池中的所有现有虚拟机。

Virtual SAN 提供了一个存储策略框架，以便您可以控制位于 Virtual SAN 数据存储中的各种虚拟机对象的行为。Virtual SAN 中的对象的一个示例为虚拟磁盘 (VMDK) 文件，每个对象有四个通过策略控制的特性：

- **带：**数据带的数量。磁盘带的数量影响您拥有的磁盘 (HDD) 数量。

- **弹性：**容许的故障次数。当然，容许的主机故障次数取决于您拥有的主机数量。
- **存储置备：**复杂或精简。
- **缓存预留：**读取缓存预留。

带数和缓存预留设置用于控制性能。弹性设置用于控制可用性。存储置备设置用于控制容量。这些设置一起影响所需的 vSphere 主机和磁盘数量。

例如，如果将每个对象的磁盘带数设置为 2，则 Virtual SAN 将至少跨 2 个 HDD 使对象条带化。如果与该设置一起使用，将容许的主机故障次数设置为 1，则 Virtual SAN 将为了弹性创建另一个副本，因此需要 4 个 HDD。此外，将容许的主机故障次数设置为 1 需要至少 3 个 ESXi 主机，2 个用于弹性设置，第 3 个用于在分区时破坏连接。

注 如果无意中尝试使用了这些互相冲突的设置，则尝试应用这些设置时，操作将失败，例如，出现错误消息，提示您没有足够的主机。

对于与这些默认策略相关联的任何用户操作都没有任何要求。将为链接克隆桌面池、完整克隆桌面池和自动场创建策略。

您可以使用 vSphere 命令行界面 (esxcli) 或 vSphere Web Client 来更改默认存储策略配置文件。无论在群集中的物理位置如何，每个虚拟机都会维护各自的策略。如果策略由于主机、磁盘或网络故障或者工作负载变化而不合规，Virtual SAN 都会重新配置受影响的虚拟机的数据并进行负载平衡，以符合每个虚拟机的策略。

使用虚拟卷实现以虚拟机为中心的存储和基于策略的管理

使用随 vSphere 6.0 或更高版本提供的虚拟卷 (VVol)，单个虚拟机而非数据存储将变为存储管理的单元。存储硬件获得对虚拟磁盘内容、布局和管理控制。

使用虚拟卷，抽象存储容器可替代基于 LUN 或 NFS 共享的传统存储卷。虚拟卷可直接将虚拟磁盘及其衍生产品、克隆、快照和副本映射到存储系统上的对象，也称为虚拟卷。通过此映射，vSphere 可以将密集型存储操作（如拍摄快照、克隆和复制）卸载到存储系统。例如，这样之前需要一小时的克隆操作现在通过使用虚拟卷只需要几分钟。

重要事项 虚拟卷的主要优势之一是能够使用基于软件策略的管理 (Software Policy-Based Management, SPBM)。但是，对于此版本，View 并未创建 Virtual SAN 所创建的默认粒度存储策略。您而是可以在 vCenter Server 中设置一个全局默认存储策略，该策略将应用于所有虚拟卷数据存储。

虚拟卷具有以下优势：

- 虚拟卷支持将大量操作卸载到存储硬件。这些操作包括快照、克隆和 Storage DRS。
- 使用虚拟卷，您可以使用包括单个虚拟磁盘上的复制、加密、重复数据删除和压缩的高级存储服务。
- 虚拟卷支持此类 vSphere 功能，如 vMotion、Storage vMotion、快照、链接克隆、Flash Read Cache 和 DRS。
- 您可以将虚拟卷与支持 vSphere APIs for Array Integration (VAAI) 的存储阵列结合使用。

要求和限制

虚拟卷功能在 View 部署中使用时存在以下限制：

- 本版本不支持使用 View 节省空间的磁盘格式功能，该功能通过擦除和压缩磁盘回收磁盘空间。
- 虚拟卷不支持使用 View Composer Array Integration (VCAI)。
- 即时克隆桌面池不支持虚拟卷数据存储。

注 虚拟卷与 View Storage Accelerator 功能兼容。Virtual SAN 在 SSD 磁盘上提供一个缓存层，View Storage Accelerator 功能提供基于内容的缓存，该缓存可在发生引导风暴时降低 IOPS 并提高性能。

虚拟卷功能有以下要求：

- vSphere 6.0 或更高版本。
- 合适的硬件。某些存储供应商负责提供可与 vSphere 集成并提供虚拟卷支持的存储提供程序。每个存储提供程序都必须由 VMware 认证并进行正确部署。
- 您在虚拟数据存储上置备的所有虚拟磁盘都必须为 1 MB 的偶数倍数。

虚拟卷是 vSphere 6.0 功能。有关要求、功能、后台和设置要求的详细信息，请参阅《vSphere 存储》文档中有关虚拟卷的主题。

使用即时克隆减少存储需求

即时克隆功能利用 vSphere vmFork 技术（在 vSphere 6.0U1 和更高版本中提供）静默运行的基础映像或父虚拟机，然后对其进行热克隆以创建一个最多包含 2,000 个即时克隆的池。

即时克隆不仅在创建时与父虚拟机共享虚拟磁盘，而且还共享父虚拟机的内存。每个即时克隆都像一个独立的桌面，带有唯一的主机名和 IP 地址，但即时克隆的存储需求明显较少。即时克隆将所需的存储容量减少 50% 到 90%。在创建克隆时，总内存需求也会减少。

副本与即时克隆位于相同数据存储中

当您创建即时克隆桌面池时，首先需要从主虚拟机创建一个完整克隆。完整克隆（或副本）以及与之链接的克隆可存储在相同的数据存储或 LUN（逻辑单元号）上。

副本与即时克隆位于不同数据存储中

此外，您也可以将即时克隆副本和即时克隆分别存放在具有不同性能特征的数据存储中。例如，您可以将副本虚拟机存储在固态硬盘 (SSD) 中。固态硬盘具有低存储容量和高读取性能，通常支持的每秒 I/O 次数 (IOPS) 能达到上万次。

您可以将即时克隆存储在基于传统旋转介质的数据存储中。这种磁盘性能较低，但价格相对低廉，并具有较高存储容量，因此适合存储大型池中的大量即时克隆。分层存储配置能够经济高效地处理密集 I/O 负载，如同时运行计划内的病毒扫描任务。

如果您使用 Virtual SAN 数据存储，则无法手动为副本和即时克隆选择不同的数据存储。由于 Virtual SAN 自动将对象放在相应类型的磁盘上并缓存所有 I/O 操作，因此无需为 Virtual SAN 数据存储使用副本分层。在虚拟 SAN 数据存储上支持即时克隆池。在普通本地存储磁盘上不支持即时克隆池。

即时克隆和 View Composer 链接克隆之间的差异

由于即时克隆的创建速度比链接克隆的创建速度快得多，因此在置备即时克隆池时，不再需要链接克隆的以下功能：

- 即时克隆池不支持配置单独的一次性虚拟磁盘以存储客户机操作系统的页面文件和临时文件。每次用户注销即时克隆桌面时，View 将自动删除该克隆，然后根据池的最新可用操作系统映像置备并启动另一个即时克隆。在注销操作期间，将自动删除任何客户机操作系统页面文件和临时文件。
- 即时克隆池不支持为每个虚拟桌面创建单独的永久虚拟磁盘。相反，您可以在 App Volumes 的用户可写磁盘上存储最终用户的 Windows 配置文件和应用程序数据。在最终用户登录时，最终用户的用户可写磁盘将连接到即时克隆桌面上。此外，还可以使用用户可写磁盘永久保存用户安装的应用程序。
- 由于即时克隆桌面具有短期特性，不需要使用空间效率较高的磁盘格式（SE 稀疏）及其擦除和压缩过程。

使用 View Composer 降低存储要求

View Composer 可创建与基础映像共享虚拟磁盘的桌面映像，因此您可以将存储容量需求降低 50% 到 90%。

View Composer 使用基础映像或父虚拟机，可创建最多包含 2,000 个链接克隆虚拟机的池。每个链接克隆都像一个独立的桌面，带有唯一的主机名和 IP 地址，但链接克隆的存储需求明显较少。

副本与链接克隆位于相同数据存储中

在创建链接克隆桌面池或 Microsoft RDS 主机场时，将先从父虚拟机中创建一个完整克隆。完整克隆（或副本）以及与之链接的克隆可存储在相同的数据存储或 LUN（逻辑单元号）上。如有必要，您可以使用重新平衡功能在不同的 LUN 之间移动副本和链接克隆桌面池，以及在 LUN 和 Virtual SAN 数据存储之间移动副本和链接克隆桌面池。

副本与链接克隆位于不同数据存储中

此外，您也可以将 View Composer 副本和链接克隆分别存放在具有不同性能特征的数据存储中。例如，您可以将副本虚拟机存储在固态硬盘 (SSD) 中。固态硬盘具有低存储容量和高读取性能，通常支持的每秒 I/O 次数 (IOPS) 能达到上万次。您可以将链接克隆存储在基于传统旋转介质的数据存储中。这种磁盘性能较低，但价格相对低廉，并具有较高存储容量，因此适合存储大型池中的大量链接克隆。分层存储配置能够经济高效地处理密集 I/O 负载，如同时重新启动大量虚拟机，或者运行计划内的病毒扫描任务。

有关更多信息，请参阅名为《VMware View 的存储注意事项》的最佳实践指南。

如果您使用 Virtual SAN 数据存储或虚拟卷数据存储，则无法手动为副本和链接克隆选择不同的数据存储。由于 Virtual SAN 和虚拟卷功能自动将对象放在相应类型的磁盘上并缓存所有 I/O 操作，因此无需为 Virtual SAN 和虚拟卷数据存储使用副本分层。

适用于页面文件和临时文件的一次性磁盘

在创建链接克隆池或场时，您还可以选择配置一个单独的一次性虚拟磁盘以存储在用户会话期间生成的客户机操作系统页面文件和临时文件。虚拟机电源关闭后，将删除一次性磁盘。使用一次性磁盘可以减缓链接克隆的增长速度，同时降低已关闭虚拟机所占用的空间，这些都有助于节省存储空间。

适用于专用桌面的永久磁盘

当您创建专用分配桌面池时，View Composer 可选择性为每个虚拟桌面创建各自的永久虚拟磁盘。最终用户的 Windows 配置文件和应用程序数据将保存在永久磁盘中。刷新、重构或重新平衡链接克隆时，永久虚拟磁盘中的内容会被保留。VMware 建议您将 View Composer 永久磁盘存储在单独的数据存储中。这样可以备份保存永久磁盘的整个 LUN。

确定即时克隆和 View Composer 链接克隆桌面池的存储大小

View 提供了可帮助您确定即时克隆或链接克隆桌面池所需存储空间的高级指南。添加桌面池向导中的表格显示了对桌面池存储空间需求的一般预估方法。

存储大小表还会显示您选择用来存储操作系统磁盘、View Composer 永久磁盘（仅限 View Composer 链接克隆）以及副本的数据存储中的可用空间。您可以通过对比实际的可用空间和预估的桌面池需求来确定使用哪些数据存储。

View 使用的计算公式只能估算出大概的存储使用率。克隆的实际存储空间增长取决于诸多因素，例如：

- 分配给父虚拟机的内存容量
- 刷新操作的频率（仅限 View Composer 链接克隆）
- 客户机操作系统页面文件的大小
- 是否将页面和临时文件重定向到单独的磁盘（仅限 View Composer 链接克隆）
- 是否配置单独的 View Composer 永久磁盘（仅限 View Composer 链接克隆）
- 桌面计算机的工作负载，这主要由用户在客户机操作系统上运行的应用程序类型决定

注 在包含几百或几千个克隆的部署中，对您的桌面池进行配置，使特定的数据存储组专供特定的 ESXi 群集使用。请勿在所有数据存储中随机配置池，这样会导致多数或所有 ESXi 主机必须访问多数或全部 LUN。

当过多的 ESXi 主机试图向特定 LUN 中的操作系统磁盘执行写入时，会出现争用问题，这会导致性能下降并影响可扩展性。有关在大型部署中规划数据存储的更多信息，请参阅《View 架构规划指南》文档。

即时克隆和链接克隆池的大小调整原则

创建或编辑即时克隆或链接克隆桌面池时，**选择链接 (或即时) 克隆数据存储** 页面会显示一个表格，其中提供了存储大小调整原则。该表可帮助您决定为链接克隆磁盘选择哪些数据存储。这些原则将计算新链接克隆所需的空間。

操作系统磁盘和永久磁盘的大小表

表 16-1. 操作系统磁盘和永久磁盘大小表的示例显示了在父虚拟机拥有 1 GB 内存和 10 GB 副本的情况下，一个拥有 10 台虚拟机的池可能显示的推荐存储大小示例。在此示例中，为操作系统磁盘和 View Composer 永久磁盘选择了不同的数据存储。

注 永久磁盘信息仅适用于 View Composer 链接克隆。即时克隆不支持永久磁盘。

表 16-1. 操作系统磁盘和永久磁盘大小表的示例

数据类型	选择的可用空间 (GB)	推荐的最小值 (GB)	50% 使用率 (GB)	推荐的最大值 (GB)
操作系统磁盘	184.23	40.00	80.00	130.00
永久磁盘	28.56	4.00	10.00	20.00

选择的可用空间列显示您为某个磁盘类型（如操作系统磁盘）所选的所有数据存储的总可用空间量。

推荐的最小值列显示为一个池推荐的最小存储量。

50% 使用率列显示当磁盘增长到父虚拟机 50% 大小时推荐的存储量。

推荐的最大值列显示当磁盘接近整个父虚拟机大小时推荐的存储量。

如果将操作系统磁盘和永久磁盘存储在同一数据存储中，View 会计算这两种磁盘类型的存储要求。**数据类型**将显示为**链接克隆**或**即时克隆**，而不是某种特定的磁盘类型。

如果将 View Composer 副本存储在一个单独的数据存储中，该表还会显示针对副本的存储推荐并调整针对操作系统磁盘的存储推荐。

View Composer 链接克隆的大小调整原则

该表提供了一般的指导原则。您在计算存储时必须考虑可能会影响克隆中实际存储增长的其他因素。

对于操作系统磁盘而言，您估计的大小具体取决于刷新和重构池的频率。

如果您刷新链接克隆池的频率介于一天一次和一周一次之间，请确保**选择的可用空间**可以容纳介于**推荐的最小值**和**50% 使用率**预估值之间的存储使用量。

如果您很少刷新或重构池，链接克隆磁盘大小会持续增长。请确保**选择的可用空间**可以容纳介于**50% 使用率**和**推荐的最大值**预估值之间的存储使用量。

对于永久磁盘而言，您估计的大小取决于用户在桌面上生成的 Windows 配置文件的数据量。刷新和重构操作不会影响永久磁盘。

编辑现有桌面池时的大小调整原则

View 会预估新克隆所需的存储空间。创建桌面池时，大小调整原则适用于整个池。编辑现有桌面池时，这些指导原则仅适用于添加到池中的新克隆。

例如，如果您将 100 个克隆添加到某个桌面池并选择一个新数据存储，View 会预估这 100 个新克隆的空间需求。

如果您选择新数据存储，但保持桌面池大小不变或减少克隆数量，大小调整原则将显示为 0。值 0 表示不得在所选数据存储中创建新克隆。现有克隆的空间要求已考虑在内。

View 如何计算最小推荐大小

为计算出最小的操作系统磁盘推荐值，View 将每个克隆初次创建及启动时消耗的存储量估计为其内存量的两倍。如果没有为克隆预留内存，则该克隆启动时，系统会为其创建一个 ESXi 交换文件。客户机操作系统页面文件的大小也会影响克隆操作系统磁盘的增长。

View 在操作系统磁盘的最小推荐值中还包含了每个数据存储中的两个副本的空间。创建池时，View Composer 会创建一个副本。首次重构池时，View Composer 会在数据存储中创建第二个副本，然后将克隆绑定到新副本，如果没有其他克隆使用原始快照，View Composer 会同时删除第一个副本。重构操作过程中，数据存储的容量必须能存储两个副本。

默认情况下，副本使用 vSphere Thin Provisioning，但为了使指导原则简单易算，View 计为两个使用与父虚拟机所用空间量相同的副本。

为计算永久磁盘的最小推荐值，View 将计算您在[添加桌面池](#)向导的 **View Composer 磁盘**页面中所指定磁盘空间量的 20%。

注 针对永久磁盘的计算是以静态阈值为基础的，以千兆字节为单位。例如，如果您指定的永久磁盘大小值介于 1024 MB 和 2047 MB 之间，View 会按 1 GB 的永久磁盘大小进行计算。如果您指定的磁盘大小为 2048 MB，View 会按 2 GB 的磁盘大小进行计算。

为计算出在单独数据存储上存储副本的推荐值，View 会允许在数据存储上保留两个副本所用的空间量。计算最小及最大使用值时也会将该值计算在内。

有关详细信息，请参阅[即时克隆和链接克隆池的大小计算公式](#)。

View Composer 链接克隆的大小调整原则和存储过载

注 即时克隆不支持存储过载。

在您预估出存储要求、选择数据存储并置备池之后，View 会根据每个数据存储上的可用空间和已有克隆数在不同数据存储中置备链接克隆虚拟机。

根据您在“添加桌面池”向导中的[选择链接克隆数据存储](#)页面上选择的存储过载选项，View 会停止置备新克隆并为已有克隆预留可用空间。此行为可保证为数据存储中的每个计算机留出增长空间。

如果选择激进的存储过载级别，预估的存储要求可能会超出[已选可用空间](#)列中显示的容量。存储过载级别会影响 View 在一个数据存储中实际创建的虚拟机的数量。

有关详细信息，请参阅[设置链接克隆虚拟机的存储过载级别](#)。

即时克隆和链接克隆池的大小计算公式

存储大小计算公式可帮助您预估为操作系统磁盘、View Composer 永久磁盘和副本选择的数据存储所需的磁盘空间量。

注 永久磁盘信息仅适用于 View Composer 链接克隆。即时克隆不支持永久磁盘。

存储大小计算公式

表 16-2. 选定数据存储中克隆磁盘的存储大小计算公式显示了在创建池时以及克隆逐渐增长过程中计算磁盘预估大小的公式。这些公式会将随克隆一起存储在数据存储中的副本所占的磁盘空间计算在内。

如果您编辑现有池或将副本存储在单独的数据存储中，View 会使用不同的大小计算公式。请参阅[编辑池或在单独的数据存储中存储副本时创建克隆的大小计算公式](#)。

表 16-2. 选定数据存储中克隆磁盘的存储大小计算公式

数据类型	选择的可用空间 (GB)	推荐的最小值 (GB)	50% 使用率 (GB)	推荐的最大值 (GB)
操作系统磁盘	选定数据存储中的可用空间	虚拟机数量 * (2 * 虚拟机内存) + (2 * 副本磁盘)	虚拟机数量 * (副本磁盘的 50% + 虚拟机内存) + (2 * 副本磁盘)	虚拟机数量 * (副本磁盘的 100% + 虚拟机内存) + (2 * 副本磁盘)
永久磁盘	选定数据存储中的可用空间	虚拟机数量 * 永久磁盘的 20%	虚拟机数量 * 永久磁盘的 50%	虚拟机数量 * 永久磁盘的 100%

存储大小预估示例

在这个示例中，为父虚拟机配置的内存为 1 GB。父虚拟机的磁盘大小为 10 GB。使用 10 个计算机创建了一个池。永久磁盘的大小配置为 2048 MB。

操作系统配置在一个当前有 184.23 GB 可用空间的数据存储中。永久磁盘配置在另一个有 28.56 GB 可用空间的数据存储中。

表 16-3. 部署在选定数据存储中的克隆磁盘的大小预估示例显示了大小计算公式如何计算示例桌面池的预估存储要求。

表 16-3. 部署在选定数据存储中的克隆磁盘的大小预估示例

数据类型	选择的可用空间 (GB)	推荐的最小值 (GB)	50% 使用率 (GB)	推荐的最大值 (GB)
操作系统磁盘	184.23	10 * (2 * 1 GB) + (2 * 10 GB) = 40.00	10 * (10 GB 的 50% + 1 GB) + (2 * 10 GB) = 80.00	10 * (10 GB 的 100% + 1 GB) + (2 * 10 GB) = 130.00
永久磁盘	28.56	10 * (2 GB 的 20%) = 4.00	10 * (2 GB 的 50%) = 10.00	10 * (2 GB 的 100%) = 20.00

编辑池或在单独的数据存储中存储副本时创建克隆的大小计算公式

当您编辑现有桌面池或在单独的数据存储中存储副本时，View 使用的大小计算公式与您第一次创建池时使用的公式不同。

如果您编辑现有池，为该池选择数据存储，View Composer 会在选定数据存储中创建新克隆。新克隆会被绑定到现有快照并使用现有副本磁盘。不会创建新副本。

View 将估算添加到桌面池的新克隆的大小规模要求。View 不会将现有克隆计算在内。

如果您将副本存储在一个单独的数据存储中，其他选定的数据存储会专供操作系统磁盘使用。

表 16-4. 编辑池或在单独的数据存储中存储副本时克隆磁盘的存储大小计算公式显示了编辑池或在单独的数据存储中存储副本时计算克隆磁盘的预估大小所用的公式。

表 16-4. 编辑池或在单独的数据存储中存储副本时克隆磁盘的存储大小计算公式

数据类型	选择的可用空间 (GB)	推荐的最小值 (GB)	50% 使用率 (GB)	推荐的最大值 (GB)
操作系统磁盘	选定数据存储中的可用空间	新虚拟机数量 * (2 * 虚拟机内存)	新虚拟机数量 * (副本磁盘的 50% + 虚拟机内存)	新虚拟机数量 * (副本磁盘的 100% + 虚拟机内存)
永久磁盘	选定数据存储中的可用空间	新虚拟机数量 * 永久磁盘的 20%	新虚拟机数量 * 永久磁盘的 50%	新虚拟机数量 * 永久磁盘的 100%

编辑池或在单独的数据存储中存储副本时的存储大小预估示例

在这个示例中，为父虚拟机配置的内存为 1 GB。父虚拟机的磁盘大小为 10 GB。使用 10 个计算机创建了一个池。永久磁盘的大小配置为 2048 MB。

操作系统配置在一个当前有 184.23 GB 可用空间的数据存储中。永久磁盘配置在另一个有 28.56 GB 可用空间的数据存储中。

表 16-5. 编辑池或在单独的数据存储中存储副本时克隆磁盘的大小预估示例显示了大小计算公式如何计算示例池的预估存储要求。

表 16-5. 编辑池或在单独的数据存储中存储副本时克隆磁盘的大小预估示例

数据类型	选择的可用空间 (GB)	推荐的最小值 (GB)	50% 使用率 (GB)	推荐的最大值 (GB)
操作系统磁盘	184.23	10 * (2 * 1 GB) = 20.00	10 * (10 GB 的 50% + 1 GB) = 60.00	10 * (10 GB 的 100% + 1 GB) = 110.00
永久磁盘	28.56	10 * (2 GB 的 20%) = 4.00	10 * (2 GB 的 50%) = 10.00	10 * (2 GB 的 100%) = 20.00

View Composer 链接克隆虚拟机的存储过载

通过使用存储过载功能，您在数据存储中存放的链接克隆虚拟机的数量可以超过其能存放的完整虚拟机的数量，从而降低了存储成本。链接克隆可以使用容量为数据存储物理容量若干倍的逻辑存储空间。

注 即时克隆不支持存储过载。

此功能可帮助您选择一个允许您过量分配数据存储容量，并为 **View** 创建的链接克隆设置数量限制的存储级别。您可以避免由于置备过于保守而浪费存储，也可以避免链接克隆用尽磁盘空间并导致操作系统或应用程序失败。

例如，如果每个虚拟机的大小为 **10 GB**，则在 **100 GB** 的数据存储中，最多可以创建 **10** 个完整虚拟机。如果您从 **10 GB** 父虚拟机创建链接克隆，则每个克隆的大小都要远远小于 **10 GB**。

如果您设置保守的过载级别，按每个克隆的大小与父虚拟机相同计算，**View** 允许克隆使用的存储空间将是数据存储物理大小的 **4** 倍。在 **100 GB** 的数据存储中，如果父虚拟机大小为 **10 GB**，**View** 可置备大约 **40** 个链接克隆。即使数据存储中还有可用空间，**View** 也不会置备更多克隆。此限制为现有克隆的增长保留了空间。

表 16-6. 存储过载级别 显示了您可以设置的存储过载级别。

表 16-6. 存储过载级别

选项	存储过载级别
无	不允许存储过载。
保守	数据存储大小的 4 倍。这是默认级别。
适中	数据存储大小的 7 倍。
激进	数据存储大小的 15 倍。

存储过载级别为确定存储容量提供了高级指南。要确定最佳级别，请监视环境中链接克隆的增长情况。

如果操作系统磁盘不可能增至最大，请设置激进级别。设置激进的过载级别时，您需要密切关注。要确保链接克隆不会用尽磁盘空间，您可以定期刷新或重新平衡桌面池，将链接克隆的操作系统数据减小到其原始大小。自动场不支持刷新或重新平衡。如果自动场中的链接克隆存在磁盘空间不足的危险，请更改过载级别。

例如，如果将浮动分配桌面池中的虚拟机设置为在注销后删除或刷新，就应当为此浮动分配桌面池设置激进的过载级别。

您可以为不同类型的数据存储指定不同的存储过载级别，以满足每个数据存储的不同吞吐量级别要求。例如，**NAS** 数据存储的设置可以不同于 **SAN** 数据存储。

设置链接克隆虚拟机的存储过载级别

使用存储过载功能可以控制 **View** 在数据存储中创建链接克隆虚拟机时的激进程度。利用此功能，您创建的链接克隆的逻辑总大小可以超过数据存储的物理存储限制。

此功能仅适用于链接克隆池和自动场。

存储过载级别将计算在每个克隆都是完整虚拟机的情况下，克隆所用的超出数据存储物理大小的存储量。有关详细信息，请参阅 [View Composer 链接克隆虚拟机的存储过载](#)。以下过程适用于链接克隆桌面池。对于自动场，这些步骤是类似的。

步骤

- 1 在 View Administrator 中，选择目录 > 桌面池。
- 2 创建新桌面池或编辑已有池时，请导航至 **vCenter 设置** 页面。

选项	操作
新桌面池	<ol style="list-style-type: none"> a 单击添加。 b 按照添加桌面池向导中的提示进行操作，直到 vCenter 设置 页面出现。
已有桌面池	<ol style="list-style-type: none"> a 选择链接克隆池，然后单击编辑。 b 单击 vCenter 设置 选项卡。

- 3 在 **vCenter 设置** 页面上，单击**数据存储**旁边的**浏览**。
- 4 在**选择链接克隆数据存储**页面上选择数据存储。
选定数据存储的“存储过载”列中将显示一个下拉菜单。
- 5 从该下拉菜单中选择存储过载级别。

选项	描述
无	不允许存储过载。
保守	数据存储大小的 4 倍。这是默认级别。
适中	数据存储大小的 7 倍。
激进	数据存储大小的 15 倍。
无限制	View 不会限制其基于数据存储的物理容量创建的链接克隆计算机的数量。请仅在您确定数据存储有足够的存储容量容纳所有计算机及其未来增长时选择此级别。

- 6 单击**确定**。

View Composer 链接克隆数据磁盘

View Composer 会创建多个数据磁盘来存储链接克隆虚拟机的组件。

操作系统磁盘

View Composer 会为每个链接克隆创建一个操作系统磁盘。此磁盘将存储克隆为保持与基础映像的链接以及作为唯一的虚拟机运行所需的系统数据。

QuickPrep 配置数据磁盘

View Composer 在创建操作系统磁盘的同时会创建一个辅助磁盘。辅助磁盘将存储在刷新和重构操作时必须保留的 QuickPrep 配置数据和其他与操作系统相关的数据。该磁盘的容量较小，通常约为 20 MB。无论您使用 QuickPrep 还是 Sysprep 自定义虚拟机，都会创建此磁盘。

如果您配置单独的 **View Composer** 永久磁盘来存储用户配置文件，以下三个磁盘会与每个链接克隆相关联：操作系统磁盘、辅助虚拟机磁盘和 **View Composer** 永久磁盘。

辅助虚拟机磁盘与操作系统磁盘存储在同一个数据存储上。您不能配置该磁盘。

View Composer 永久磁盘

在专用分配池中，您可以配置单独的 **View Composer** 永久磁盘来存储 **Windows** 用户配置文件数据。该磁盘不是必需的。

您可以使用单独的永久磁盘保留用户数据和设置。**View Composer** 刷新、重构和重新平衡操作不会影响永久磁盘。您可以将永久磁盘从一个链接克隆中分离，然后将其附加到另一个链接克隆。

如果不配置单独的永久磁盘，**Windows** 配置文件将存储在操作系统磁盘中。用户数据和设置在刷新、重构和重新平衡期间将被移除。

您可以将永久磁盘与操作系统磁盘存储在同一个数据存储内，也可以将其存储在不同的数据存储中。

一次性数据磁盘

创建链接克隆池时，您可以配置一个单独的非永久磁盘，用来存储客户机操作系统在用户会话期间生成的页面文件和临时文件。您必须指定磁盘大小（以 **MB** 为单位）。

该磁盘不是必需的。

链接克隆关闭电源后，**View** 会将一次性数据磁盘替换为 **View Composer** 使用链接克隆池创建的原始磁盘副本。链接克隆的大小在用户与其桌面交互过程中会增长。使用一次性数据磁盘可以减缓链接克隆的增长速度，从而节省存储空间。

一次性数据磁盘与操作系统磁盘存储在同一个数据存储中。

在本地数据存储上存储 View Composer 链接克隆

链接克隆虚拟机可以存储在本地数据存储（**ESXi** 主机上的内部备用磁盘）中。本地存储存在以下优势：硬件价格低廉，虚拟机置备速度快，开关机性能高，管理简单，等等。但是，使用本地存储会限制您可用的 **vSphere** 基础架构配置选项。本地存储在某些 **View** 环境中可以发挥优势，但不适用于其他环境。

注 本主题中所述的限制不适用于 **Virtual SAN** 数据存储，该数据存储也使用本地存储磁盘，但需要特定硬件。

如果环境中的 **View** 桌面是无状态桌面，使用本地数据存储将是极为可行的。例如，您可在部署无状态的 **Kiosk** 或教室和培训中心时使用本地数据存储。

如果您的虚拟机具有浮动分配、不是专供单个最终用户使用、不需要持久磁盘来保留用户数据，并且可以按固定的时间间隔（例如用户注销时）删除或刷新，可以考虑使用本地数据存储。通过这种方法，您可以控制每个本地数据存储的磁盘使用情况，而无需在各数据存储之间移动虚拟机或对虚拟机执行负载平衡。

但是，您必须考虑使用本地数据存储给 **View** 桌面或场部署带来的限制：

- 您无法使用 **VMotion** 管理卷。

- 您无法对资源池中的虚拟机执行负载平衡。例如，您无法对存储在本地数据存储上的链接克隆使用 View Composer 重新平衡操作。
- 您无法使用 VMware High Availability。
- 您无法使用 vSphere Distributed Resource Scheduler (DRS)。
- 如果 View Composer 副本在本地数据存储上，您将无法把它与链接克隆存储在不同的数据存储上。
如果链接克隆存储在本地数据存储上，VMware 会强烈建议您将副本与链接克隆存储在同一个卷上。虽然当群集中的所有 ESXi 主机均可访问副本时，有可能将链接克隆和副本分别存储在本地数据存储和共享数据存储上，但是 VMware 不建议采用这种配置。
- 如果您选择本地旋转磁盘驱动器，其性能可能与商用存储阵列的性能不太一样。本地旋转磁盘驱动器也许具有与存储阵列相似的容量，但达不到与存储阵列相同的吞吐量。吞吐量会随着磁盘转轴数量的增加而增加。

如果您选择直连固态硬盘 (SSD)，则性能可能会超出很多存储阵列的性能。

如果在单个 ESXi 主机或包含单个 ESXi 主机的群集上配置桌面池或场，您可以将链接克隆存储在本地数据存储上而没有任何限制。但是，如果使用单个 ESXi 主机，则会限制可配置的桌面池或场大小。

要配置大型桌面池或场，您必须选择包含多个 ESXi 主机的群集，以便利用其集合容量来支持大量虚拟机。

如果您打算利用本地存储的优势，那么必须仔细考虑好无法使用 VMotion、HA、DRS 及其他功能的后果。如果您通过控制虚拟机数量及其磁盘增长速度来管理本地磁盘使用情况，且您使用的是浮动分配并定期进行刷新和删除操作，那么您就可以将链接克隆成功部署至本地数据存储。

将即时克隆和 View Composer 链接克隆的副本和克隆存储在不同的数据存储中

您可以将副本和克隆分别存放在具有不同性能特征的数据存储中。此配置可加快磁盘密集型操作，例如，置备或运行防病毒扫描，尤其是对 View Composer 链接克隆的效果更明显。

例如，您可以将副本虚拟机存储在支持固态硬盘的数据存储中。固态硬盘具有低存储容量和高读取性能，通常支持 20,000 I/O 每秒 (IOPS) 的速度。典型的环境中只有少量副本虚拟机，因此，副本不需要大量存储空间。

您可以将克隆存储在支持传统旋转介质的数据存储中。这种磁盘性能较低，通常支持 200 IOPS。这种磁盘价格低廉，但可提供高存储容量，从而适合存储大量克隆。

以这种方式配置副本和克隆可以减少一次创建多个克隆时出现的 I/O 风暴所带来的影响，尤其是对于 View Composer 链接克隆的效果更明显。例如，如果您置备一个具有“注销后删除计算机”策略的浮动分配池，并且用户在同一时间开始工作，View 将必须同时为他们置备新计算机。

重要事项 此功能面向由提供高性能磁盘解决方案的供应商所提供的特定存储配置。如果您的存储硬件不支持高读取性能，请不要将副本存储在单独的数据存储中。

将池中的副本和克隆存储在不同的数据存储中时，必须遵循以下特定要求：

- 您只能为一个池指定一个单独的副本数据存储。

- 必须能够从群集中的所有 ESXi 主机访问副本数据存储。
- 对于 View Composer 链接克隆，如果克隆位于本地数据存储上，VMware 会强烈建议您将副本与链接克隆存储在同一个卷上。虽然当群集中的所有 ESXi 主机均可访问副本时，有可能将链接克隆和副本分别存储在本地数据存储和共享数据存储上，但是 VMware 不建议采用这种配置。
- 使用 Virtual SAN 数据存储或虚拟卷数据存储时，此功能不可用。这些类型的数据存储使用基于软件策略的管理，以便存储配置文件可定义哪些组件用于哪些类型的磁盘。

将副本存储在单独数据存储中的可用性注意事项

您可以将副本虚拟机存储在单独的数据存储中，也可以存储在与克隆相同的数据存储中。这些配置会以不同方式影响池的可用性。

将副本存储在与克隆相同的数据存储中时，为增强可用性，每个数据存储中都会创建一个单独的副本。如果某个数据存储不可用，则只有该数据存储中的克隆才会受到影响。其他数据存储中的克隆仍可继续运行。

将副本存储在单独的数据存储中时，池中的所有克隆都会与该数据存储中的副本绑定。如果该数据存储不可用，整个池都将不可用。

为增强桌面池的可用性，您可以为存储副本的数据存储配置一个高可用性解决方案。

为 View Composer 链接克隆配置 View Storage Accelerator

您可以配置 View Composer 链接克隆桌面池，以使 ESXi 主机能够缓存虚拟机磁盘数据。这项称为 View Storage Accelerator 的功能可以使用 ESXi 主机中的 Content Based Read Cache (CBRC) 功能。当发生引导风暴，即大量桌面同时启动或运行防病毒扫描时，View Storage Accelerator 可以降低 IOPS 并提高性能。对于需要频繁加载应用程序或数据的管理员或用户来说，这项功能同样有益。为使用这项功能，您必须确保单个桌面池启用了 View Storage Accelerator。

注 如果您在现有的链接克隆桌面池中启用 View Storage Accelerator，而副本之前没有启用 View Storage Accelerator，此功能可能不会立即生效。当副本正在使用时，无法启用 View Storage Accelerator。您可以通过将桌面池重构到新的父虚拟机来强制启用 View Storage Accelerator。对于即时克隆，此功能会自动启用，而且不可对其进行配置。

创建虚拟机后，View 可为每个虚拟磁盘文件的内容创建索引。索引存储在虚拟机摘要文件中。在运行过程中，ESXi 主机读取摘要文件，并将通用数据块缓存在内存中。为保持 ESXi 主机缓存的最新状态，View 以特定的时间间隔以及在虚拟机重构时重新生成摘要文件。您可以修改重新生成缓存的时间间隔。

您可以在包含链接克隆的池和包含完整虚拟机的池中启用 View Storage Accelerator。

默认情况下，池的 View Storage Accelerator 已启用。可以在创建或编辑池时禁用或启用此功能。最佳方法是在首次创建桌面池时启用此功能。如果通过编辑现有池来启用此功能，您必须确保先创建新副本及其摘要磁盘，再置备链接克隆。可以通过将池重构为新的快照或者将池重新平衡为新的数据存储来创建副本。仅当桌面池中的虚拟机处于关闭状态时，才能为它们配置摘要文件。

View Storage Accelerator 现在可在使用 **View** 副本分层的配置下运行，在此配置中，副本存储于单独的数据存储中，而不是链接克隆中。虽然将 **View** 副本分层与 **View Storage Accelerator** 搭配使用在性能方面并没有太大的实质性提升，但是通过将副本存储到单独的数据存储，还是能够带来一些容量方面的好处。因此，我们对这种组合方式进行了测试，并提供支持。

重要事项 如果您计划使用此功能，并且正在使用多个共享某些 **ESXi** 主机的 **View** 容器，则必须为共享的 **ESXi** 主机上的所有池启用 **View Storage Accelerator** 功能。如果多个容器中的设置不一致，可能会导致共享 **ESXi** 主机上的虚拟机出现不稳定。

前提条件

- 确认 **vCenter Server** 和 **ESXi** 主机版本为 **5.0** 或更高。
在 **ESXi** 群集中，确认所有主机均为 **5.0** 版或更高版本。
- 确认在 **vCenter Server** 中为 **vCenter Server** 用户分配了 **主机 > 配置 > 高级设置** 特权。请参阅《**View** 安装指南》文档中介绍 **vCenter Server** 用户所需的 **View** 和 **View Composer** 特权的主题。
- 确认 **vCenter Server** 中的 **View Storage Accelerator** 已启用。请参阅《**View** 管理指南》文档。

步骤

- 1 在 **View Administrator** 中，显示**高级存储选项**页面。

选项	说明
新桌面池（建议）	启动“添加桌面池”向导开始创建自动桌面池。按照向导的配置提示操作，直至进行到 高级存储 页面。
已有桌面池	选择已有的池并单击 编辑 ，然后单击 高级存储 选项卡。 如果您修改已有桌面池的 View Storage Accelerator 设置，所做的更改将在桌面池中的虚拟机关闭电源之后才生效。

- 2 要为池启用 **View Storage Accelerator**，请确保已选中**使用 View Storage Accelerator** 复选框。
默认情况下，此设置已选中。要禁用此设置，请取消选中**使用 View Storage Accelerator** 复选框。
- 3 （可选）从**磁盘类型**菜单中仅选择**操作系统磁盘**或选择**操作系统磁盘和永久磁盘**，指定要缓存的磁盘类型。
默认情况下将选择**操作系统磁盘**。
如果您要为完整虚拟机配置 **View Storage Accelerator**，则无法选择磁盘类型。将在整个虚拟机上执行 **View Storage Accelerator**。
- 4 （可选）在**在以下时间后重新生成存储加速器**文本框中指定时间间隔，以天数表示，在此时间间隔后将重新生成 **View Storage Accelerator** 摘要文件。
默认重新生成摘要文件的时间间隔为七天。

后续步骤

您可配置中断天数和时间，在此期间不会回收磁盘空间，也不会重新生成 **View Storage Accelerator**。请参阅为 **View Composer** 链接克隆设置 **Storage Accelerator** 和空间回收中断时间。

如果通过编辑现有池来启用 **View Storage Accelerator**，先将桌面池重构为新的快照或者将池重新平衡为新的数据存储器，再置备链接克隆。

在 View Composer 链接克隆上回收磁盘空间

在 vSphere 5.1 及更高版本中，您可以为 View Composer 链接克隆桌面池和自动场配置磁盘空间回收功能。对于 vSphere 5.1 及更高版本，View 能够以高效的磁盘格式创建链接克隆虚拟机，这种磁盘格式允许 ESXi 主机回收链接克隆中未使用的磁盘空间，从而减少链接克隆所需的总存储空间。

注 对于即时克隆，不需要此功能，因为在用户注销时始终会重新创建这些克隆。

随着用户与虚拟机进行交互，链接克隆的操作系统磁盘会逐渐增大，最终可能会使用与完整克隆虚拟机几乎相同的磁盘空间。磁盘空间回收有助于减少操作系统磁盘的大小，无需刷新或重构链接克隆。在开启虚拟机并且用户与虚拟机交互时，可以回收空间。

在 **View Administrator** 中，您无法针对池直接启动磁盘空间回收。通过指定触发该操作所需的累积在链接克隆操作系统磁盘上的未使用磁盘空间的最小值，您可确定 View 何时启动磁盘空间回收。当未使用的磁盘空间超过指定的阈值时，View 将指示 ESXi 主机回收操作系统磁盘上的空间。View 将此阈值应用到池中的每个虚拟机上。

您可使用 `vdmadmin -M` 选项来启动特定虚拟机上的磁盘空间回收操作，以实现示范或排除故障的目的。请参阅《View 管理指南》文档。

创建新的池或编辑现有池时可在链接克隆上配置磁盘空间回收。对于现有池，请参见《View 升级指南》文档中的“升级池以使用空间回收的相关任务”。

注 此功能不可用于 Virtual SAN 数据存储或虚拟卷数据存储上存储的虚拟机。

如果 View Composer 正在刷新、重构或重新平衡链接克隆，则这些链接克隆上不会发生磁盘空间回收。

磁盘空间回收仅适用于链接克隆中的操作系统磁盘。此功能不影响 View Composer 永久磁盘，但不适用于完整克隆虚拟机。

如果池中包含具有能节省空间的磁盘的虚拟机，则不支持本地 NFS 快照技术 (VAAI)。

以下过程适用于链接克隆桌面池。对于自动场，这些步骤是类似的。

前提条件

- 确认 vCenter Server 和 ESXi 主机（包括群集中的所有 ESXi 主机）版本为 5.1，且具有 ESXi 5.1 下载补丁程序 ESXi510-201212001 或更高版本。
- 确认提供给 vSphere 5.1 或更高版本的 VMware Tools 已安装在池中的所有链接克隆虚拟机上。
- 确认池中的所有链接克隆虚拟机均为虚拟硬件版本 9 或更高版本。
- 确认虚拟机使用 SCSI 控制器。使用 IDE 控制器的虚拟机不支持磁盘空间回收。
- 对于 Windows 10 虚拟机，确认虚拟机在 vSphere 5.5 U3 或更高版本中运行。
- 对于 Windows 8 或 8.1 虚拟机，确认虚拟机在 vSphere 5.5 或更高版本中运行。在 vSphere 5.5 或更高版本中运行的 Windows 8 或 8.1 支持磁盘空间回收。

- 对于 Windows 7 虚拟机，确认虚拟机在 vSphere 5.1 或更高版本中运行。
- 确认 vCenter Server 中的磁盘空间回收功能已启用。该选项确保能够以回收磁盘空间所需的高效磁盘格式创建池中的虚拟机。请参阅《View 管理指南》文档。

步骤

- 1 在 View Administrator 中，显示**高级存储**页面。

选项	说明
新桌面池	启动“添加桌面池”向导开始创建自动桌面池。按照向导的配置提示操作，直至进行到 高级存储 页面。
已有桌面池	选择已有的池并单击 编辑 ，然后单击 高级存储 选项卡。要升级池以支持空间回收，请参见《View 升级指南》文档中的“升级桌面池以回收空间”。

- 2 选中回收虚拟机磁盘空间复选框。
- 3 在在虚拟机上的未使用空间超出以下值时启动回收文本框，键入 ESXi 开始回收磁盘空间前，链接克隆操作系统磁盘上必须累积的未使用磁盘空间的最小值（单位为千兆字节）。

例如：2 GB。

默认值为 1 GB。

后续步骤

您可配置中断天数和时间，在此期间不会发生磁盘空间回收和 View Storage Accelerator 重新生成。请参阅[为 View Composer 链接克隆设置 Storage Accelerator 和空间回收中断时间](#)。

在 View Administrator 中，您可以选择**目录 > 桌面池**并选择一个计算机，显示该计算机上最后一次进行空间回收的时间和最后一次回收的空间量。

将 VAAI 存储用于 View Composer 链接克隆

如果您的部署包含支持 vStorage APIs for Array Integration (VAAI) 的 NAS 设备，您可以在 View Composer 链接克隆桌面池上启用 View Composer Array Integration (VCAI) 功能。此功能使用本地 NFS 快照技术克隆虚拟机。

注 在 Horizon 7.0 中，即时克隆不支持 VAAI。

使用这项技术，NFS 磁盘阵列无需 ESXi 主机读写数据即可克隆虚拟机文件。虚拟机被克隆时，此操作可减少时间和网络负载。

请在使用本地 NFS 快照技术时应用这些指导原则：

- 只有在位于通过 VAAI 支持本地克隆操作的 NAS 设备中的数据存储上配置桌面池或自动场时，才能使用该功能。
- 您可以使用 View Composer 功能管理由本地 NFS 快照技术创建的链接克隆。例如，您可以刷新、重构、重新平衡、创建永久磁盘，并可以在这些克隆中运行 QuickPrepd 自定义脚本。
- 如果您将副本磁盘和操作系统磁盘存储在单独的数据存储中，则无法使用这些功能。

- vSphere 5.0 及更高版本支持此功能。

- 如果您编辑一个池并选择或取消选择本地 NFS 克隆功能，现有的虚拟机将不受影响。

要将现有虚拟机从本地 NFS 克隆更改为传统重做日志克隆，您必须取消选择本地 NFS 克隆功能并将池重构为新的基础映像。要为池中所有虚拟机更改克隆方法并使用不同的数据存储，您必须选择新的数据存储，取消选择本地 NFS 克隆功能，将池重新平衡到新的数据存储，并将池重构为新的基础映像。

同样，要将虚拟机从传统重做日志克隆更改为本地 NFS 克隆，您必须选择支持 VAAI 的 NAS 数据存储，选择 NFS 克隆功能，将池重新平衡到 NAS 数据存储，并重构池。有关更多信息，请参阅 <http://kb.vmware.com/kb/2088995>。

- 在 ESXi 群集上，要在 View Administrator 中选定的 NFS 数据存储上配置本地克隆，您可能需要安装特定供应商的 NAS 插件来支持群集中所有 ESXi 主机上的 VAAI 本地克隆操作。请参阅存储供应商文档以查看配置要求指导。
- 具有能节省空间的磁盘的虚拟机不支持本地 NFS 快照技术 (VAAI)。
- 如果使用 Virtual SAN 数据存储或虚拟卷数据存储，此功能不可用。
- 请参阅 VMware 知识库 (KB) 文章 2061611，了解有关 View 中的 VCAI 支持的常见问题解答。

重要事项 NAS 存储供应商可能会提供能影响 VAAI 性能和其他设置的其他设置。您应当遵循供应商的建议，在 NAS 存储阵列和 ESXi 上配置相应的设置。请参阅存储供应商文档，获取配置供应商建议设置方面的指导。

为 View Composer 链接克隆设置 Storage Accelerator 和空间回收中断时间

对于 View Composer 链接克隆，可以使用 ESXi 资源再次生成 View Storage Accelerator 摘要文件并回收虚拟机磁盘空间。为了确保必要时 ESXi 资源专供前台任务使用，您可以在指定日期的指定时段内禁止 ESXi 主机执行这些操作。

注 对于即时克隆，不需要此功能。

例如，您可以在工作日早上用户开始工作时，以及发生引导风暴和防病毒扫描 I/O 风暴时，指定中断时间。在不同的日期，您可以指定不同的中断时间。

在您设置的中断时间内不会发生磁盘空间回收操作，也不会重新生成 View Storage Accelerator 摘要文件。您无法为每个操作设置单独的中断时间。

View 允许在置备阶段为新计算机创建 View Storage Accelerator 摘要文件，甚至在中断时间内也可以。

以下过程适用于链接克隆桌面池。对于自动场，这些步骤是类似的。

前提条件

- 确认为 vCenter Server 选择了启用 **View Storage Accelerator** 和/或启用空间回收功能。
- 确认为桌面池选择了使用 **View Storage Accelerator** 和/或回收虚拟机磁盘空间功能。

步骤

- 1 在“添加桌面池”向导中的**高级存储**页面，转到**中断时间**，然后单击**添加**。
如果您正在编辑现有池，请单击**高级存储**选项卡。
- 2 检查中断日期，并指定开始时间和结束时间。
时间选择器使用 24 小时制。例如，10:00 是上午 10:00，22:00 是下午 10:00。
- 3 单击**确定**。
- 4 要添加其他中断时间，请单击**添加**并指定其他时间。
- 5 要修改或删除一个中断时间，请从“中断时间”列表中选择时间间隔并单击**编辑**或**移除**。

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 **View Administrator** 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 **View Administrator** 中设置策略
- 使用 智能策略
- 使用 **Active Directory** 组策略
- 使用 **View** 组策略管理模板文件
- **View ADM** 和 **ADMX** 模板文件
- **Horizon Agent** 配置 **ADM** 模板设置
- **PCoIP** 策略设置
- **VMware Blast** 策略设置
- 使用远程桌面服务组策略
- 设置基于位置的打印
- **Active Directory** 组策略示例

在 View Administrator 中设置策略

使用 **View 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 **RDS** 桌面和应用程序池。无法为 **RDS** 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 [View 策略](#)。

步骤

- 1 在 View 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 [View 策略](#)。

步骤

- 1 在 View 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 [View 策略](#)。

步骤

- 1 在 View 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 View 策略并单击**完成**保存更改。

View 策略

您可以将 View 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。

表 17-1. View 策略 中介绍了每个 View 策略设置。

表 17-1. View 策略

策略	描述
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。

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 View 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 客户端组件。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 RDS 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《User Environment Manager 管理员指南》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《User Environment Manager 管理员指南》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。

- 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。可将 `-HorizonViewMultiSession -r` 参数用于登录脚本，将 `-HorizonViewMultiSession -s` 参数用于注销脚本。

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 中远程桌面功能的行为。

表 17-2. 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 17-2. 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。
打印	确定是否在远程桌面上启用虚拟打印。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。
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"> ■ 禁用。双向禁用剪贴板重定向。 ■ 允许全部。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。 ■ 允许从客户端复制到代理。用户只能从客户端系统向远程桌面复制并粘贴内容。 ■ 允许从代理复制到客户端。用户只能从远程桌面向客户端系统复制并粘贴内容。
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"> ■ 禁用。在远程桌面上禁用客户端驱动器重定向。 ■ 允许全部。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。 ■ 只读。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。 <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，请参阅使用注册表设置配置客户端驱动器重定向。</p>
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 LAN。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，请参阅带宽配置文件引用。</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 中的远程桌面功能配置的 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 17-3. 带宽配置文件

带宽配置文件	最大会话 BW (Kbps)	最小会话		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
		BW (Kbps)	启用 BTL					
高速 LAN	900000	100	是	100	50	60	1600	50
LAN	900000	100	是	90	50	30	1600	50
专用 WAN	900000	100	否	80	40	30	500	50
宽带 WAN	5000	100	否	70	40	20	500	50
低速 WAN	2000	100	否	70	30	15	200	25
超低速连接	1000	100	否	70	30	5	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，您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《User Environment Manager 管理员指南》。

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 17-4. 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 17-4. 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"> ■ “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。 ■ “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。 <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《View 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 Access Point》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，请参阅限制远程桌面访问。</p>
池名称	ViewClient_Launch_ID	<p>指定桌面池 ID。仅当用户在启动远程桌面时选择的桌面池 ID 与指定的桌面池 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>注 您无法使用此属性指定应用程序池。</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《**User Environment Manager** 管理员指南》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《**User Environment Manager** 管理员指南》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，键入智能策略的名称。

例如，如果智能策略将影响客户端驱动器重定向功能，则您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 **View** 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 **View** 组件，以控制 **View** 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

您应当在 **Active Directory** 中创建一个专用于您的远程桌面的组织单位 (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 **View** 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 View 环境中，GPO 应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 环回处理仅是在 View 中处理 GPO 的一种方法。您可能还需要实施其他方法。

使用 View 组策略管理模板文件

View 提供了若干特定于组件的组策略管理（ADM 和 ADMX）模板文件。您可以将这些 ADM 和 ADMX 模板文件中的策略设置添加到 Active Directory 中现有的或新的 GPO 中，从而优化和保护远程桌面和应用程序。

为 View 提供组策略设置的所有 ADM 和 ADMX 文件包含在一个名为 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 的捆绑 .zip 文件中，其中 x.x.x 是版本号，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，其中包含捆绑的 .zip 文件。

View ADM 和 ADMX 模板文件同时包含计算机配置和用户配置组策略。

- 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。

View ADM 和 ADMX 模板文件

View ADM 和 ADMX 模板文件提供了组策略设置，让您可以控制和优化 View 组件。

表 17-5. View ADM 和 ADMX 模板文件

模板名称	模板文件	说明
Horizon Agent 配置	vdm_agent.adm	包含与 Horizon Agent 的身份验证和环境组件相关的策略设置。 请参阅 Horizon Agent 配置 ADM 模板设置 。
Horizon Client 配置	vdm_client.adm	包含与 Horizon Client for Windows 相关的策略设置。 从 View 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。 请参阅《使用适用于 Windows 的 VMware Horizon Client》文档。

模板名称	模板文件	说明
VMware Horizon URL 重定向	urlRedirection-enUS.adm	<p>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。</p> <p>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。</p> <p>请参阅 VMware Horizon URL 内容重定向模板设置 以及《使用适用于 Windows 的 VMware Horizon Client》文档。</p>
View Server 配置	vdm_server.adm	<p>包含与 View 连接服务器相关的策略设置。</p> <p>请参阅《View 管理指南》文档。</p>
View 公共配置	vdm_common.adm	<p>包含所有 View 组件中的常见策略设置。</p> <p>请参阅《View 管理指南》文档。</p>
View PCoIP 会话变量	pcoip.adm	<p>包含与 PCoIP 显示协议相关的策略设置。</p> <p>请参阅 PCoIP 策略设置。</p>
View PCoIP 客户端会话变量	pcoip.client.adm	<p>包含与影响 Horizon Client for Windows 的 PCoIP 显示协议相关的策略设置。</p> <p>请参阅《使用适用于 Windows 的 VMware Horizon Client》文档。</p>
View Persona Management 配置	ViewPM.adm ViewPM.admx	<p>包含与 View Persona Management 相关的策略设置。</p> <p>请参阅 View Persona Management 组策略设置。</p>
View 远程桌面服务	vmware_rdsh.admx vmware_rdsh_server.admx	<p>包含与远程桌面服务相关的策略设置。</p> <p>请参阅使用远程桌面服务组策略。</p>
实时音频-视频配置	vdm_agent_rtav.adm	<p>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。</p> <p>请参阅实时音频-视频组策略设置。</p>
扫描仪重定向	vdm_agent_scanner.adm	<p>包含与被重定向用于远程桌面和应用程序的扫描设备相关的策略设置。</p> <p>请参阅扫描仪重定向组策略设置。</p>
串行端口重定向	vdm_agent_serialport.adm	<p>包含与被重定向以用于远程 VDI 桌面的串行 (COM) 端口相关的策略设置。</p> <p>请参阅串行端口重定向组策略设置。</p>

Horizon Agent 配置 ADM 模板设置

Horizon Agent 配置 ADM 模板文件 (vdm_agent.adm) 包含与 Horizon Agent 的身份验证和环境组件相关的策略设置。

该 ADM 文件包含在名为 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip 的捆绑 .zip 文件中，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，其中包含捆绑的 .zip 文件。

下表介绍了 Horizon Agent 配置 ADM 模板文件中的策略设置（那些用于 USB 设备的设置除外）。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。

表 17-6. Horizon Agent 配置模板设置

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 建立且受 View 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。如果禁用该设置，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 View 桌面会话时，可以使用 RDP 从 View 外部连接虚拟机。RDP 连接会终止 View 桌面会话，View 用户未保存的数据和设置可能会丢失。除非关闭外部 RDP 连接，否则 View 用户无法登录到桌面。为避免这种情况，请禁用 AllowDirectRDP 设置。</p> <p>重要事项 为确保 View 正常运行，每个桌面的客户机操作系统中都必须运行 Windows 远程桌面服务。您可以使用该设置防止用户通过 RDP 直接连接到其桌面。</p> <p>默认情况下，将启用该设置。</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，将启用该设置。</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 View 桌面上运行命令 以了解详细信息。</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 View 桌面上运行命令 以了解详细信息。</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 View 桌面上运行命令 以了解详细信息。</p>

设置	计算机	用户	属性
ConnectionTicketTimeout	X		指定 View 连接票证的有效时间（以秒为单位）。 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。
CredentialFilterExceptions	X		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。
Disable Time Zone Synchronization	X	X	确定 View 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。 默认情况下禁用此设置。
Enable multi-media acceleration	X		确定是否在 View 桌面启用多媒体重定向 (MMR)。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。 默认情况下，将启用该设置。
Enable system tray redirection for Hosted Apps	X		确定用户在运行远程应用程序时是否已启用系统托盘重定向。此设置位于组策略管理编辑器中的 VMware View Agent 配置 > Unity Touch 和托管应用程序 文件夹中。 默认情况下，将启用该设置。
Enable Unity Touch	X		确定是否已在 View 桌面上启用 Unity Touch 功能。Unity Touch 支持交付 View 中的远程应用程序并允许移动设备用户访问 Unity Touch 边栏中的应用程序。 此设置位于组策略管理编辑器中的 VMware View Agent 配置 > Unity Touch 和托管应用程序 文件夹中。 默认情况下，将启用该设置。
ShowDiskActivityIcon	X		此设置在此发行版中不受支持。
Toggle Display Settings Control	X		确定当客户端会话采用 PCoIP 显示协议时是否禁用 Display（显示）控制面板上的 Settings（设置）选项卡。 默认情况下，将启用该设置。
DPI Synchronization	X	X	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。 默认情况下不配置此设置。 注 该设置仅适用于 7.0.2 或更高版本，以及安装了 Horizon Client 4.2 或更高版本的 Windows 客户端。
VMwareViewAgentCIT	X		启用 Internet Explorer 的远程连接以使用客户端的 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。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。

设置	计算机	用户	属性
ProxyDefaultAutoDetectSettings	X		自动检测“Internet 属性”和“局域网设置”中的设置的默认 Internet Explorer 连接设置。 默认情况下，不会启用该设置。
ProxyDefaultIEProxyServer	X		指定在“Internet 属性”和“局域网设置”中使用的代理服务器的默认 Internet Explorer 连接设置。 默认情况下，不会启用该设置。
UpdateJavaProxy	X		指示远程连接使用客户端的 IP 地址，而不是用于 Java Applet 的远程桌面计算机的 IP 地址。 默认情况下，不会启用该设置。
FlashMMRUrlListEnableType			指定允许或禁止 URL 使用 Flash 重定向的白名单或黑名单。要使用白名单，请设置 FlashMMRUrlListEnableType=0 以便仅允许 URL 列表中的 URL 使用 Flash 重定向。要使用黑名单，请设置 FlashMMRUrlListEnableType=1 以便 URL 列表中的 URL 无法使用 Flash 重定向。 默认情况下，该设置指定白名单。
FlashMMRUrlList			指定根据 FlashMMRUrlListEnableType 设置允许或禁止使用 Flash 重定向的 URL 列表。 确保包含 http:// 或 https://。您可以使用正则表达式。例如，可以指定 https://*.google.com 和 http://www.cnn.com。

注 Horizon 6 版本 6.1 中已移除 Connect using DNS Name 设置。您可以设置 View LDAP 属性 **pae-PreferDNS**，以告知 View 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《View 安装指南》文档中的“当 View 连接服务器返回地址信息时优先考虑 DNS 名称”。

Horizon Agent 的 USB 设置

请参阅 [Horizon Agent 配置 ADM 模板中的 USB 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 [View 桌面上运行命令](#) 了解更多信息。

表 17-7. 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 17-7. 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
ViewClient_IP_Address	客户端系统的 IP 地址。	是	VDI（单用户计算机） RDS	Windows、Linux、Mac、Android、iOS、Windows 应用商店
ViewClient_MAC_Address	客户端系统的 MAC 地址。	是	VDI（单用户计算机） RDS	Windows、Linux、Mac、Android
ViewClient_Machine_Name	客户端系统的计算机名。	是	VDI（单用户计算机） RDS	Windows、Linux、Mac、Android、iOS、Windows 应用商店
ViewClient_Machine_Domain	客户端系统的域。	是	VDI（单用户计算机） RDS	Windows、Windows 应用商店
ViewClient_LoggedOn_Username	用于登录客户端系统的用户名。		VDI（单用户计算机） RDS	Windows、Linux、Mac
ViewClient_LoggedOn_Domainname	用于登录客户端系统的域名。		VDI（单用户计算机） RDS	Windows、Windows 应用商店 对于 Linux 和 Mac 客户端，请参阅 ViewClient_Machine_Domain 。Linux 或 Mac 客户端没有提供 .ViewClient_LoggedOn_Domainname ，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） 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） 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） 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） 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） 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） 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。 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） RDS	Windows、Linux、Mac、Android、iOS
ViewClient_Windows_Timezone	GMT 标准时间。 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） 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） 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） 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） 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） 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） 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） 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） 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） RDS	Windows
ViewClient_Mouse.NumButtons	指定鼠标支持的按键数量。		VDI（单用户计算机） 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） RDS	Windows
ViewClient_Protocol	指定正在使用的协议。		VDI（单用户计算机） 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） RDS	Windows、Linux、Mac、Android、iOS、Windows 应用商店
ViewClient_Launch_ID	指定桌面池的唯一 ID。		VDI（单用户计算机）	Windows、Linux、Mac、Android、iOS、Windows 应用商店

注 表 17-7. 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 View 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 View 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:\procxp.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。

PCoIP 策略设置

PCoIP ADM 模板文件 (`pcoip.adm`) 包含与 PCoIP 显示协议相关的策略设置。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。

该 ADM 文件包含在名为 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip` 的捆绑 `.zip` 文件中，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，其中包含捆绑的 `.zip` 文件。

View PCoIP 会话变量 ADM 模板文件包含两个子类别：

管理员可覆盖的默认值	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 <code>HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults</code> 中。
管理员不可覆盖的设置	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 <code>HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin</code> 中。

该模板仅包含“计算机配置”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

View PCoIP ADM 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。

表 17-8. PCoIP 常规策略设置

设置	说明
Configure PCoIP client image cache size policy	<p>控制 PCoIP 客户端图像缓存的大小。客户端使用图像缓存来存储之前传送的显示部分。图像缓存减少了重传的数据量。</p> <p>Horizon Client、Horizon Agent 和 View 连接服务器为 View 5.0 或更高版本时，此设置仅适用于 Windows、Linux 和 Mac 客户端。</p> <p>未配置或禁用此设置时，PCoIP 使用 250 MB 的默认客户端图像缓存大小。</p> <p>在 Horizon Client 3.1 或更高版本中，如果您指定的数值小于可用内存量除以 2，则会使用以下公式设置缓存大小：</p> $\text{user-setting} - 10 \text{ MB}$ <p>在 Horizon Client 3.1 或更高版本中，如果您指定的数值大于可用内存量除以 2，则会使用以下公式设置缓存大小：</p> $\text{available-memory} / 2 - 10 \text{ MB}$ <p>例如，如果您指定的最大缓存大小为 1024 MB，而可用内存为 1600 MB，则最大缓存大小设置为 790 MB。</p> <p>对于所有 Horizon Client 版本，默认大小为 250 MB，最小大小为 50 MB。</p> <p>在 Horizon Client 1.6 或更高版本中，最大大小为 1024 MB。在 Horizon Client 1.5 或更低版本中，最大大小为 300 MB。</p>
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 m 时，超过 m 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>日志文件清理将在会话启动时执行一次。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 n 时，早于 n 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>日志文件清理将在会话启动时执行一次。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。最低图像质量、最高初始图像质量 和 最高帧速率 值交互作用，从而精密控制网络带宽受限环境。</p> <p>使用 最低图像质量 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 最高初始图像质量 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>最低图像质量 值不能超过 最高初始图像质量 值。</p> <p>使用 最高帧速率 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 禁用 AES-128-GCM 加密 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：SALSA20/12-256、AES-GCM-128 和 AES-GCM-256。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 1xxxxyyyy，其中 xxxx 是十六进制格式的 VID，yyyy 为十六进制格式的 PID。例如，授权或阻止某个 VID 为 0x1a2b、PID 为 0x3c4d 的设备的规则为 11a2b3c4d。</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：23XXXXXX 示例：23XXXXXX</td></tr> <tr> <td>允许具有特定类 ID 的 USB 设备</td><td>格式：22classXXXX 示例：22aaXXXX</td></tr> <tr> <td>允许特定子类</td><td>格式：21class-subclassXX 示例：21aabbXX</td></tr> <tr> <td>允许特定协议</td><td>格式：20class-subclass-protocol 示例：20aabbcc</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 2203XXXX 220eXXXX。禁用 USB 大容量存储设备（类 ID 0x08）的 USB 取消授权字符串为 2208XXXX。</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：23XXXXXX 示例：23XXXXXX	允许具有特定类 ID 的 USB 设备	格式：22classXXXX 示例：22aaXXXX	允许特定子类	格式：21class-subclassXX 示例：21aabbXX	允许特定协议	格式：20class-subclass-protocol 示例：20aabbcc
允许所有 USB 设备	格式：23XXXXXX 示例：23XXXXXX								
允许具有特定类 ID 的 USB 设备	格式：22classXXXX 示例：22aaXXXX								
允许特定子类	格式：21class-subclassXX 示例：21aabbXX								
允许特定协议	格式：20class-subclass-protocol 示例：20aabbcc								
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 mksvchan vdp_vdpvcbridge。</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 awk ward\channel 应输入为 awk ward\\channel。</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 Configure the PCoIP transport header 设置时，以下传输会话优先级可供使用：</p> <ul style="list-style-type: none"> ■ 高 ■ 中（默认值） ■ 低 ■ 未定义 <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，也未指定未定义的优先级，则会话将使用默认值，即中优先级。</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。</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>重要事项 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。</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>重要事项 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 the FIPS 140-2 approved mode of operation	<p>确定是否仅使用 FIPS 140-2 许可的加密算法和协议来建立远程 PCoIP 连接。</p> <p>启用此设置将覆盖禁用 AES128-GCM 加密设置。</p> <p>此设置适用于代理和客户端。您可以将一个终端或两个终端配置为以 FIPS 模式操作。将一个终端配置为以 FIPS 模式操作会限制会话协商可用的加密算法。</p> <p>对于 View 4.5 及更高版本，FIPS 模式可用。对于 View 4.0.x 及更低版本，FIPS 模式不可用，且配置此设置不起任何作用。</p> <p>禁用或未配置此设置时，不使用 FIPS 模式。</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>

设置	说明
Enable/disable microphone noise and DC offset filter in PCoIP session	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。 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。
Turn on PCoIP user default input language synchronization	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。 此设置仅适用于 Horizon Agent。

PCoIP 剪贴板设置

View PCoIP ADM 模板文件中包含为复制和粘贴操作配置剪贴板设置的组策略设置。

表 17-9. PCoIP 剪贴板策略设置

设置	说明
Configure clipboard memory size on server (in kilobytes)	<p>以 KB 为单位指定服务器的剪贴板内存大小值。客户端也具有剪贴板内存大小值。在设置会话后，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>您可以指定的最小值为 512 KB，最大值为 16384 KB。如果您指定的值为 0 或未指定值，则默认的服务器剪贴板内存大小为 1024 KB。</p> <p>此设置仅适用于版本 7.0.1 或更高版本，以及安装了 Horizon Client 4.1 或更高版本的 Windows、Linux 和 Mac 客户端。在早期版本中，剪贴板内存大小为 1 MB。</p> <p>注 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。VMware 建议您不要将剪贴板内存大小设置为大于 16 MB 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"> ■ 仅启用从客户端到代理（即仅允许从客户端系统向远程桌面执行复制和粘贴。） ■ 禁用两个方向 ■ 启用两个方向 ■ 仅启用从代理到客户端（即仅允许从远程桌面向客户端系统执行复制和粘贴。） <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 Horizon Agent。</p> <p>如果此设置已禁用或未配置，默认值为仅启用从客户端到代理。</p>
Filter text out of the incoming clipboard data	<p>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。</p> <p>此设置适用于版本 7.0.2 及更高版本。</p>
Filter Rich Text Format data out of the incoming clipboard data	<p>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。</p> <p>此设置适用于版本 7.0.2 及更高版本。</p>

设置	说明
Filter images out of the incoming clipboard data	<p>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。</p> <p>此设置适用于版本 7.0.2 及更高版本。</p>
Filter Microsoft Office text data out of the incoming clipboard data	<p>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。</p> <p>此设置适用于版本 7.0.2 及更高版本。</p>
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	<p>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。</p> <p>此设置适用于版本 7.0.2 及更高版本。</p>
Filter Microsoft Text Effects data out of the incoming clipboard data	<p>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。</p> <p>此设置适用于版本 7.0.2 及更高版本。</p>
Filter text out of the outgoing clipboard data	<p>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。</p> <p>此设置适用于版本 7.0.2 及更高版本。</p>
Filter Rich Text Format data out of the outgoing clipboard data	<p>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。</p> <p>此设置适用于版本 7.0.2 及更高版本。</p>
Filter images out of the outgoing clipboard data	<p>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。</p> <p>此设置适用于版本 7.0.2 及更高版本。</p>
Filter Microsoft Office text data out of the outgoing clipboard data	<p>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。</p> <p>此设置适用于版本 7.0.2 及更高版本。</p>
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	<p>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。</p> <p>此设置适用于版本 7.0.2 及更高版本。</p>
Filter Microsoft Text Effects data out of the outgoing clipboard data	<p>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。</p> <p>此设置适用于版本 7.0.2 及更高版本。</p>

PCoIP 带宽设置

View PCoIP ADM 模板文件包含用于配置 PCoIP 带宽特征的组策略设置。

表 17-10. View 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质量立体声音频，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质量立体声音频。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 PCoIP 无损构建功能。</p>

PCoIP 键盘设置

View PCoIP ADM 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。

表 17-11. 针对键盘的 View 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 Ctrl+Alt+Insert 而不是 Ctrl+Alt+Del。</p> <p>当用户按 Ctrl+Alt+Del 锁定客户端终端时，如果一个 SAS 被发送到主机和客户机，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 Horizon Agent，对客户端不起作用。</p> <p>未配置或禁用此策略时，用户可按 Ctrl+Alt+Del 或 Ctrl+Alt+Insert 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 Insert（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 Ctrl+Alt+Ins 按键序列。</p> <p>例如，用户可从 PCoIP 桌面启动 vSphere Client，并打开 vCenter Server 中虚拟机的控制台。如果在 vCenter Server 虚拟机的客户机操作系统中使用了 Ctrl+Alt+Ins 序列，则会将 Ctrl+Alt+Del SAS 发送至虚拟机。此设置允许通过 Ctrl+Alt+备用键 序列将 Ctrl+Alt+Del 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，Ctrl+Alt+Ins 按键序列用作 SAS。</p> <p>此设置仅适用于 Horizon Agent，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 组策略模板文件 `vdm_blast.adm` 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。

表 17-12. VMware Blast 策略设置

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。
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。
Max Bandwidth Slope for the Kbps Per Megapixel	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。
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。
UDP Protocol	指定使用 UDP 协议还是 TCP 协议。默认不使用 UDP 协议，即，使用 TCP 协议。启用此设置可使用 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。
H264	指定使用 H.264 编码还是 JPEG/PNG 编码。默认使用 H.264 编码。
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。 该设置适用于 7.0.2 和更高版本。
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。
Cookie Cleanup Interval	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。
Image Quality	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： <ul style="list-style-type: none"> ■ 低 JPEG 质量（可用值范围：1 - 100，默认值：25） ■ 低 JPEG 色度子采样（可用值范围：4:1:0（最低）、4:1:1、4:2:0、4:2:2 和 4:4:4（最高），默认值：4:1:0） ■ 中等 JPEG 质量（可用值范围：1 - 100，默认值：35） ■ 高 JPEG 质量（可用值范围：1 - 100，默认值：90） ■ 高 JPEG 色度子采样（可用值范围：4:1:0（最低）、4:1:1、4:2:0、4:2:2 和 4:4:4（最高），默认值：4:4:4）
H.264 Quality	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： <ul style="list-style-type: none"> ■ H264maxQP（可用值范围：0-51，默认值：36） ■ H264minQP（可用值范围：0-51，默认值：10） 要获得最佳图像质量，可将量化值设置为比可用值范围大 5 或小 5 范围内的值。

设置	说明
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。
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。
Configure clipboard redirection	<p>指定剪贴板重定向的许可行为。选项包括：</p> <ul style="list-style-type: none"> ■ 启用两个方向 ■ 禁用两个方向 ■ 仅启用从客户端到服务器（用户只能将客户端中的内容复制/粘贴到桌面。） ■ 仅启用从服务器到客户端（用户只能将桌面中的内容复制/粘贴到客户端。） <p>默认值为仅启用从客户端到服务器。</p>
Clipboard memory size on server(in kilobytes)	<p>以 KB 为单位指定服务器的剪贴板内存大小值。客户端也具有剪贴板内存大小值。在设置会话后，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>您可以指定的最小值为 512 KB，最大值为 16384 KB。如果您指定的值为 0 或未指定值，则默认的服务器的剪贴板内存大小为 1024 KB。</p> <p>该设置仅适用于 7.0.1 和更高版本，以及安装了 Horizon Client 4.1 或更高版本的 Windows、Linux 和 Mac 客户端。在早期版本中，剪贴板内存大小为 1 MB。</p> <p>注 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。VMware 建议您不要将剪贴板内存大小设置为大于 16 MB 的值。</p>
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。该设置仅适用于 Horizon Agent。</p> <p>注 仅适用于 Windows 的 Horizon Client 支持该功能。</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"> ■ 禁用上载和下载 ■ 启用上载和下载 ■ 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。） ■ 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。） <p>默认为仅启用文件上载。</p> <p>该设置适用于 7.0.1 和更高版本以及 HTML Access 4.1 和更高版本。</p>
Filter text out of the incoming clipboard data	<p>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。在禁用或不配置该设置时，将允许复制和粘贴此类数据。</p> <p>该设置适用于 7.0.2 和更高版本。</p>
Filter Rich Text Format data out of the incoming clipboard data	<p>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。在禁用或不配置该设置时，将允许复制和粘贴此类数据。</p> <p>该设置适用于 7.0.2 和更高版本。</p>
Filter images out of the incoming clipboard data	<p>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。在禁用或不配置该设置时，将允许复制和粘贴此类数据。</p> <p>该设置适用于 7.0.2 和更高版本。</p>
Filter Microsoft Office text data out of the incoming clipboard data	<p>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。在禁用或不配置该设置时，将允许复制和粘贴此类数据。</p> <p>该设置适用于 7.0.2 和更高版本。</p>

设置	说明
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。在禁用或不配置该设置时，将允许复制和粘贴此类数据。 该设置适用于 7.0.2 和更高版本。
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。在禁用或不配置该设置时，将允许复制和粘贴此类数据。 该设置适用于 7.0.2 和更高版本。
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。在禁用或不配置该设置时，将允许复制和粘贴此类数据。 该设置适用于 7.0.2 和更高版本。
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。在禁用或不配置该设置时，将允许复制和粘贴此类数据。 该设置适用于 7.0.2 和更高版本。
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。在禁用或不配置该设置时，将允许复制和粘贴此类数据。 该设置适用于 7.0.2 和更高版本。
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。在禁用或不配置该设置时，将允许复制和粘贴此类数据。 该设置适用于 7.0.2 和更高版本。
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。在禁用或不配置该设置时，将允许复制和粘贴此类数据。 该设置适用于 7.0.2 和更高版本。
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。在禁用或不配置该设置时，将允许复制和粘贴此类数据。 该设置适用于 7.0.2 和更高版本。

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 (RDS) 组策略控制 RDS 主机以及 RDS 桌面和应用程序会话的配置和性能。View 提供了包含在 View 中支持的 Microsoft RDS 组策略的 ADMX 文件。

作为最佳实践，请配置在 View ADMX 文件中提供的组策略，而不是相应的 Microsoft 组策略。View 组策略已通过认证，支持您的 View 部署。

配置 RDS 每设备 CAL 存储

您可以通过配置 RDS 每设备 CAL 存储选项来指定要将 CAL 存储到的位置。此功能允许您决定是否希望存储 CAL。

有时，可能会出现潜在过度使用每设备 CAL 的情况，例如，View RDS 部署可能会有 Windows Server 2008 和 Windows Server 2012 两个系统。启用此功能后，可提高 CAL 在 View RDS 部署中的使用效率。通过存储颁发的许可证，在客户端尝试连接到 RDS 主机时提供此许可证，并在有任何许可证升级时再次存储该许可证，可以实现此目的。

您可以在 View Administrator 中配置 RDS 每设备 CAL，也可以在 View LDAP 数据库中手动进行配置。

步骤

- 1 在 View Administrator 中，单击 **View 配置 > 全局设置**。
- 2 在“常规”窗格中，单击**编辑**。

3 从 RDS 每设备 CAL 存储选项下拉菜单中选择以下配置之一。

选项	说明
仅在代理上保存	<p>仅在代理上保存每设备 CAL。</p> <p>注 LDAP 条目 cs-enablerdslicensing=true 和 sendRdsLicense=false。</p>
在客户端和代理上保存	<p>在客户端和代理上都存储每设备 CAL。</p> <p>注 LDAP 条目 cs-enablerdslicensing=true 和 sendRdsLicense=true。</p>
不保存每设备 CAL	<p>不在任何位置存储每设备 CAL。</p> <p>注 LDAP 条目 cs-enablerdslicensing=false 和 sendRdsLicense=false。</p>

4 单击确定。

将远程桌面服务 ADMX 文件添加到 Active Directory

您可以将 View RDS ADMX 文件中的策略设置添加到 Active Directory 中的组策略对象 (GPO)。也可以将 RDS ADMX 文件安装到各个 RDS 主机上。

前提条件

- 为 RDS 组策略设置创建 GPO，并将其链接到包含您的 RDS 主机的组织单位。
- 确认在 Active Directory 服务器上可以使用组策略管理功能。

打开“组策略管理控制台”的步骤在 Windows 2012、Windows 2008 和 Windows 2003 Active Directory 版本中不同。请参阅[View 组策略创建 GPO](#)。

步骤

- 1 从 VMware 下载站点中下载 View 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 View 提供组策略设置的所有 ADM 和 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 RDS ADMX 文件复制到 Active Directory 或 RDS 主机。
 - a 将 vmware_rdsh.admx、vmware_rdsh_server.admx 文件和 en-US 文件夹复制到 Active Directory 或 RDS 主机上的 C:\Windows\PolicyDefinitions 文件夹中。
 - b （可选）将语言资源文件 vmware_rdsh.adml 和 vmware_rdsh_server.adml 复制到 Active Directory 或 RDS 主机上 C:\Windows\PolicyDefinitions\ 中的相应子文件夹。

3 在 Active Directory 主机上，打开组策略管理编辑器。

在单独 RDS 主机上，您可以使用 `gpedit.msc` 实用程序打开本地组策略编辑器。

View RDS 组策略设置安装在 **计算机配置 > 策略 > 管理模板 > Windows 组件 > Horizon View RDSH 服务 > 远程桌面会话主机文件夹**中。

4 （可选）配置 **Horizon View RDSH 服务 > 远程桌面会话主机文件夹**中的组策略设置。

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 17-13. RDS 应用程序兼容性组策略设置

设置	描述
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>如果禁用或不配置该策略设置，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> <div><code>explorer.exe</code> <code>mstsc.exe</code></div> <p>如果禁用或不配置该策略设置，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>如果禁用或不配置该策略设置，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>该策略设置指定当虚拟 IP 地址不可用时，会话是否使用远程桌面会话主机服务器的 IP 地址。</p> <p>如果启用该策略设置，则当虚拟 IP 不可用时，不使用 RD 会话主机服务器的 IP 地址。会话将没有网络连接。</p> <p>如果禁用或不配置该策略设置，则当虚拟 IP 不可用时，将使用 RD 会话主机服务器的 IP 地址。</p>

RDS 连接设置

RDS Connections 组策略设置允许您禁用 Fair Share CPU Scheduling。

表 17-14. RDS 连接组策略设置

设置	描述
Turn off Fair Share CPU Scheduling	<p>Fair Share CPU Scheduling 基于会话数量和每个会话内的处理器时间需求，跨同一 RD 会话主机服务器上的所有远程桌面服务会话动态分发处理器时间。</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。

表 17-15. RDS 设备和资源重定向组策略设置

设置	描述
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。

表 17-16. RDS 许可组策略设置

设置	描述
Use the specified Remote Desktop license servers	<p>此策略设置允许您指定 RD 会话主机服务器尝试查找远程桌面许可证服务器的顺序。</p> <p>如果启用此策略设置，RD 会话主机服务器会首先尝试查找您指定的许可证服务器。如果找不到指定的许可证服务器，RD 会话主机服务器将尝试自动发现许可证服务器。</p> <p>在自动发现许可证服务器过程中，基于 Windows Server 的域中的 RD 会话主机服务器尝试按以下列顺序联系许可证服务器：</p> <ol style="list-style-type: none"> 1 在远程桌面会话主机配置池中指定的许可证服务器 2 在 Active Directory 域服务中发布的许可证服务器 3 安装在 RD 会话主机服务器所在域中的域控制器上的许可证服务器 <p>如果您禁用或未配置此策略设置，RD 会话主机服务器将使用远程桌面会话主机配置工具中所指定的许可证服务器发现模式。</p>
Hide notifications about RD Licensing problems that affect the RD Session Host server	<p>此策略设置确定当出现了影响 RD 会话主机服务器的 RD 许可问题时，是否在 RD 会话主机服务器上显示通知。</p> <p>默认情况下，如果出现了影响 RD 会话主机服务器的 RD 许可问题，则在您以本地管理员身份登录 RD 会话主机服务器后，会显示相关通知。如果适用，还会显示一个通知，告知 RD 会话主机服务器许可宽限期到期前的剩余天数。</p> <p>如果启用此策略设置，将不会在 RD 会话主机服务器上显示这些通知。</p> <p>如果禁用或未配置此策略设置，将在您以本地管理员身份登录 RD 会话主机服务器后显示这些通知。</p>
Set the Remote Desktop licensing mode	<p>此策略设置允许您指定连接到该 RD 会话主机服务器所需的远程桌面服务客户端访问许可证 (RDS CAL) 的类型。</p> <p>您可以使用此策略设置选择两种许可模式之一：每用户或每设备。</p> <p>每用户许可模式要求连接到此 RD 会话主机服务器的每个用户帐户都具有 RDS 每用户 CAL。</p> <p>每设备许可模式要求连接到此 RD 会话主机服务器的每个设备都具有 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 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 17-17. RDS 配置文件组策略设置

设置	描述
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>注 如果您要限制单个用户配置文件的大小，请使用位于用户配置\策略\管理模板\系统\用户配置文件中的限制配置文件大小策略设置。</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：如果启用位于计算机配置\策略\管理模板\系统\用户配置文件中的防止漫游配置文件更改传播到服务器策略设置，将忽略此策略设置。</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>注 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	描述
Use mandatory profiles on the RD Session Host server	<p>此策略设置可指定远程桌面服务是否为所有远程连接到 RD 会话主机服务器的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设置远程桌面服务漫游用户配置文件的路径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。所有远程连接到 RD 会话主机服务器的用户将使用相同的用户配置文件。</p> <p>如果您禁用或未配置此策略设置，远程连接到 RD 会话主机服务器的用户将不会使用强制用户配置文件。</p> <p>注 要使此策略设置生效，您还必须启用并配置设置远程桌面服务漫游用户配置文件的路径策略设置。</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 RD 会话主机服务器本地存储所有用户配置文件。您可以使用此策略设置指定一个网络共享位置来集中存储用户配置文件，这样，在配置为使用该网络共享存储用户配置文件的所有 RD 会话主机服务器上，用户就可以使用同一配置文件建立会话。</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>\\Computername\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 RD 会话主机服务器上显示错误消息，并在 RD 会话主机服务器本地存储用户配置文件。</p> <p>如果您禁用或未配置此策略设置，将在 RD 会话主机服务器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"> 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。 2 要为远程连接到 RD 会话主机服务器的所有用户配置强制的远程桌面服务漫游用户配置文件，请将此策略设置与位于 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 中的在 RD 会话主机服务器上使用强制配置文件策略设置一起使用。设置远程桌面服务漫游用户配置文件的路径策略设置中设定的路径应包含强制配置文件。

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。

表 17-18. RDS 远程会话环境组策略设置

设置	描述
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“Windows 安全”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“Windows 安全”。这样，用户必须键入诸如 CTRL+ALT+END 的安全注意序列才能在客户端计算机上打开“Windows 安全”对话框。</p> <p>如果状态设置为“已禁用”或“未配置”，“Windows 安全”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。

表 17-19. RDS 安全组策略设置

设置	描述
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> <p>注 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 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 17-20. 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>注 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 Temp 文件夹中的用户配置文件文件夹下创建，并使用 sessionid 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 Temp 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>

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 **View** 桌面，使用户能够从 **View** 桌面使用本地打印机和网络打印机进行打印。

IT 组织可以通过基于位置的打印将 **View** 桌面映射到与端点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。

在 **Horizon 6.0.1** 和更高版本中，以下远程桌面和应用程序上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** 主机上部署的桌面，其中 **RDS** 主机为虚拟机
- 托管应用程序

■ 从远程桌面内的 Horizon Client 启动的托管应用程序

在 Horizon 6.0 及更早版本中，单用户 Windows Desktop 计算机上部署的桌面支持基于位置的打印。

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的 View 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 View 桌面以供某个特定客户端系统使用。

当用户连接到 View 桌面后，View 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，那么 View 会在用户会话过程中将该打印机映射到 View 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 View 桌面的信息存储在 View 桌面的一个注册表项中，其位置为：
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect。

基于位置的打印的打印机设置

在 Horizon 6.0.2 或更高版本中，用户注销或从桌面断开连接后，系统会保留基于位置的打印的打印机设置。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。

要保存托管应用程序中多个会话的打印机设置，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-yyyyyy.zip 的 .zip 文件中提供，其中，x.x.x 是版本，yyyyyy 是内部版本号。您可以从 VMware Horizon 6 下载站点下载该文件，网址为 <http://www.vmware.com/go/downloadview>。

早期的 View 版本提供 32 位和 64 位版本的 TPVMGPoACmap.dll，位于 View 连接服务器主机上的 *install_directory\VMware\VMware View\Server\extras\GroupPolicyFiles\ThinPrint* 目录中。

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 View 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 View 桌面的 OU。有关如何为 View 组策略创建 GPO 的示例，请参阅[为 View 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 View 桌面发送到打印机，因此请确认桌面上安装了必要的打印机驱动程序。

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">a 选择开始 > 所有程序 > 管理工具 > Active Directory 用户和计算机。b 右键单击包含您的 View 桌面的 OU，选择属性。c 在组策略选项卡上，单击打开以打开组策略管理插件。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。
Windows 2008	<ol style="list-style-type: none">a 选择开始 > 管理工具 > 组策略管理。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。

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 View 桌面的打印机，并定义其关联的转换表。
- 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 17-21. [转换表的列和值](#) 介绍了该转换表的语法。

基于位置的打印功能将本地打印机映射到远程桌面，但是不支持映射使用 UNC 路径配置的网络打印机。

表 17-21. 转换表的列和值

列	描述
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： <i>ip_address -ip_address</i></p> <p>例如： 10.112.116.0-10.112.119.255</p> <p>要指定特定子网中的所有 IP 地址，请使用以下表示法： <i>ip_address/subnet_mask_bits</i></p> <p>例如： 10.112.4.0/22</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>
Client Name	<p>指定计算机名的转换规则。</p> <p>例如： Mary's Computer</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"> ■ Windows 客户端使用连字符： 01-23-45-67-89-ab ■ Linux 客户端使用冒号： 01:23:45:67:89:ab <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： <i>\\domain\user_or_group</i></p> <p>例如： \\\\mydomain\\Mary</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： PRINTER-2-CLR</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>
Printer Driver	<p>打印机使用的驱动程序名称。</p> <p>例如： HP Color LaserJet 4700 PS</p> <p>重要事项 由于打印作业直接从桌面发送到打印机，因此桌面上必须安装打印机驱动程序。</p>
IP Port/ThinPrint Port	<p>对于网络打印机，其 IP 地址带有 IP_ 前缀。</p> <p>例如： IP_10.114.24.1</p> <p>默认端口为 9100。您可以通过将端口号附加到 IP 地址来指定非默认端口。</p> <p>例如： IP_10.114.24.1:9104</p>
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 17-22. 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 17-22. 基于位置的打印组策略设置示例

IP Range (IP 范围)	Client Name (客户端名称)	Mac Address (Mac 地址)	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。

Active Directory 组策略示例

在 View 中实施 Active Directory 组策略的一种方法是提供远程桌面会话的 View 计算机创建一个组织单位 (OU)，然后将一个或多个组策略对象 (GPO) 链接到该 OU。您可以使用这些 GPO 将组策略设置应用于 View 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 View 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 View 计算机创建 OU

要将组策略应用于提供远程桌面会话的 View 计算机且不影响同一 Active Directory 域中的其他 Windows 计算机，您可以为 View 计算机专门创建一个 OU。您可能会为整个 View 部署创建一个 OU 或者为单用户计算机和 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 View 计算机的域，并选择**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 View 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 View 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，View 计算机会显示在右侧窗格中。

后续步骤

为 View 组策略创建 GPO。

为 View 组策略创建 GPO

创建 GPO 以包含针对 View 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 View 计算机的组织单位 (OU)。

前提条件

- 为您的 View 计算机创建一个 OU。
- 确认在 Active Directory 服务器上可以使用组策略管理功能。

步骤

- 1 在 Active Directory 服务器上，打开组策略管理控制台。

AD 版本	导航路径
Windows 2012	选择 服务器管理器 > 工具 > 组策略管理 。
Windows 2008	选择 开始 > 管理工具 > 组策略管理 。
Windows 2003	<ol style="list-style-type: none">a 选择开始 > 所有程序 > 管理工具 > Active Directory 用户和计算机。b 右键单击包含您的 View 计算机的 OU，然后选择属性。c 在组策略选项卡上，单击打开以打开组策略管理插件。

- 2 展开您的域，右键单击包含您的 View 计算机的 OU，然后选择**在这个域中创建 GPO 并在此处链接**。
在 Windows 2003 Active Directory 中，此选项名为**在此处创建并链接 GPO**。
- 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）要将 GPO 仅应用于 OU 中的特定 View 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 View 计算机的计算机名，然后单击**确定**。
View 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 View ADM 模板添加到组策略 GPO 中。

将 View ADM 模板添加到 GPO 中

要将 View 组件组策略设置应用于您的远程桌面和应用程序，请将其 ADM 模板文件添加到 GPO。

前提条件

- 为 View 组件组策略设置创建 GPO，并将其链接到包含您的 View 虚拟机的组织单位。
- 确认在 Active Directory 服务器上可以使用组策略管理功能。

打开“组策略管理控制台”的步骤在 Windows 2012、Windows 2008 和 Windows 2003 Active Directory 版本中不同。请参阅[为 View 组策略创建 GPO](#)。

步骤

- 1 从 VMware 下载站点中下载 View 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 View 提供组策略设置的所有 ADM 和 ADMX 文件均在此文件中提供。

- 2 将文件复制到您的 Active Directory 服务器上并解压缩文件。
- 3 在 Active Directory 服务器上，打开组策略管理控制台。
- 4 展开您的域，右键单击为组策略设置创建的 GPO 并选择**编辑**。
- 5 在组策略管理编辑器中，右键单击**计算机配置 > 策略 > 管理模板:策略定义**文件夹，然后选择**添加/移除模板**。
- 6 单击**添加**，浏览到所需的 ADM 模板文件，然后单击**打开**。
- 7 单击**关闭**，将 ADM 模板文件中的策略设置应用到 GPO。

在 Windows Server 2012 或 2008 Active Directory 中，模板名称显示在**管理模板 > 经典管理模板 (ADM)** 下的左侧窗格中。在 Windows Server 2003 Active Directory 中，模板显示在**管理模板**下。

- 8 配置组策略设置。

后续步骤

为 View 虚拟机启用环回处理。

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 View 组件组策略设置创建 GPO，并将其链接到包含您的 View 虚拟机的组织单位。

- 确认在 Active Directory 服务器上可以使用组策略管理功能。

打开“组策略管理控制台”的步骤在 Windows 2012、Windows 2008 和 Windows 2003 Active Directory 版本中不同。请参阅[View 组策略创建 GPO](#)。

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
Merge（合并）	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。
Replace（替换）	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。

使用 View Persona Management 配置用户配置文件

18

使用 View Persona Management，您可以配置与远程配置文件存储库动态同步的用户配置文件。当用户登录到桌面时，此功能可为用户提供个性化的桌面体验。View Persona Management 可扩展此功能并提高 Windows 漫游配置文件性能，但不需要操作 Windows 漫游配置文件。

您可以将组策略设置配置为启用 View Persona Management 部署并控制 View Persona Management 的各个方面。

要启用并使用 View Persona Management，您必须拥有相应的 VMware Horizon 许可证。请参阅 <http://www.vmware.com/download/eula> 上的“VMware 最终用户许可协议 (EULA)”。

本章讨论了以下主题：

- 在 View 中提供用户配置
- 将 View Persona Management 用于独立系统
- 使用 View Persona Management 迁移用户配置文件
- 用户配置管理和 Windows 漫游配置文件
- 配置 View Persona Management 部署
- 配置 View Persona Management 部署的最佳实践
- View Persona Management 组策略设置

在 View 中提供用户配置

使用 View Persona Management 功能，用户的远程配置文件将在用户登录 View 桌面时动态下载。您可以配置 View，将用户配置文件存储于一个安全、集中的存储库中。View 可根据用户的需要下载用户配置信息。

View Persona Management 可以替代 Windows 漫游配置文件。与 Windows 漫游配置文件相比，View Persona Management 扩展了功能，并提高了性能。

您可以在 View 中完全配置和管理用户配置。而不需要配置 Windows 漫游配置文件。如果您具有 Windows 漫游配置文件配置，可以将现有的存储库设置与 View 配合使用。

用户配置文件与 View 桌面相互独立。无论用户登录哪个桌面，都会显示同一个用户配置文件。

例如，用户可以登录一个浮动分配的链接克隆桌面池，并更改桌面背景和 Microsoft Word 的设置。当用户启动下一个会话时，虚拟机会发生变化，但用户仍会看到同样的设置。

用户配置中包含各种由用户生成的信息：

- 针对用户的数据和桌面设置
- 应用程序数据和设置
- 由用户应用程序配置的 Windows 注册表项

此外，如果您使用 ThinApp 应用程序置备桌面，ThinApp 沙箱数据可以存储在用户配置文件中并随用户漫游。

View Persona Management 缩短了登录和注销桌面的时间。登录和注销时间是 Windows 漫游配置文件难以解决的一个问题。

- 在登录过程中，View 只下载 Windows 需要的文件，如用户注册表文件。其他文件将在用户或应用程序从本地配置文件夹打开它们时复制到本地桌面。
- View 将本地配置文件中的最近更改复制到远程存储库中，通常每隔几分钟复制一次。默认情况下，每 10 分钟一次。您可以指定上传本地配置文件的频率。
- 在注销过程中，只有在上次复制后更新的文件才会被复制到远程存储库中。

将 View Persona Management 用于独立系统

您可在不受 View 管理的物理机和虚拟机上安装独立版本的 View Persona Management。通过此软件，您可跨 View 桌面和独立系统管理用户配置文件。

单独的 View Persona Management 软件可以在 Windows 7、Windows 8、Windows 10、Windows Server 2008 R2 和 Windows Server 2012 R2 操作系统上运行。

您可使用独立的 View Persona Management 软件完成下列目标：

- 跨独立系统和 View 桌面共享用户配置文件。

用户可继续将 View Persona Management 用于独立系统和 View 桌面。如果您使用相同的 View Persona Management 组策略设置来控制 View 桌面和物理系统，则用户每次登录时都能接收到最新的配置文件，无论他们使用的是旧版计算机还是 View 桌面。

注 View Persona Management 不支持并行活动会话。用户必须注销一个会话才能登录另一个会话。

- 将用户配置文件从物理系统迁移到 View 桌面

如果您想重新定位旧版物理机以便用于 View 部署，您可以在旧版系统上安装独立的 View Persona Management 之后再向用户推出 View 桌面。用户登录旧版系统后，其配置文件存储在 View 远程配置文件存储库中。用户首次登录 View 桌面时，其现有的配置文件将会下载到 View 桌面。

- 分阶段从物理系统迁移到 View 桌面

如果您分阶段迁移部署，对 View 桌面还没有访问权的用户可以使用独立的 View Persona Management。部署完每一组 View 桌面后，用户便可以访问 View 桌面上的配置文件，此时可以淘汰旧版系统。此方案混合了前述各方案。

- 用户脱机时可保证配置文件为最新。

独立笔记本电脑用户可断开网络连接。用户重新连接时，View Persona Management 将用户本地配置文件中的最新更改上传至远程配置文件存储库。

注 用户脱机之前，必须将用户配置文件完全下载到本地系统。

使用 View Persona Management 迁移用户配置文件

通过 View Persona Management，您可将各种设置中的现有用户配置文件迁移到 View 桌面。当用户完成配置文件迁移后登录其 View 桌面时，系统会显示用户旧版系统上所使用的个人设置和数据。

通过迁移用户配置文件，您可完成以下桌面迁移目标：

- 您可以将 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面升级到 Windows 10 View 桌面。
- 您可将用户的系统从旧版 Windows XP 升级到 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2，并首次将用户从物理机迁移到 View。
- 您可以将旧版 Windows XP View 桌面升级到 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面。
- 您可从物理机迁移到 View 桌面，而无需升级操作系统。

为支持这些方案，View Persona Management 为未安装 View Agent 5.x 的物理机或虚拟机提供了配置文件迁移实用程序和独立的 View Persona Management 安装程序。

重要事项 View Agent 6.1 和更高版本不支持 Windows XP 和 Windows Vista 桌面。View Agent 6.0.2 是支持这些客户机操作系统的上一个 View 版本。与 Microsoft 签订有关 Windows XP 和 Vista 的扩展支持协议以及与 VMware 签订有关这些客户机操作系统的扩展支持协议的客户可以使用 View 连接服务器 6.1 部署其 Windows XP 和 Vista 桌面的 View Agent 6.0.2 版本。

使用 View 用户配置文件迁移实用程序，可以在从旧版 Windows XP 桌面部署迁移到未来 View 版本中将继续支持的桌面部署的过程中执行重要任务。

表 18-1. 用户配置文件迁移方案显示了不同的迁移方案，并概述了在每个方案中应执行的任务。

表 18-1. 用户配置文件迁移方案

原始部署方案...	目标部署方案...	请执行以下任务:
Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面	Windows 10 View 桌面	<ol style="list-style-type: none"> 1 使用 View Persona Management 为用户配置 Windows 10 View 桌面。请参阅配置 View Persona Management 部署。 <p>注 完成步骤 2 后再向用户推出 Windows 10 View 桌面。</p> <ol style="list-style-type: none"> 2 运行 View V2 到 V5 配置文件迁移实用程序。 <ul style="list-style-type: none"> ■ 对于源配置文件，请为现有的 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面指定远程配置文件存储库。 ■ 对于目标配置文件，请指定为 Windows 10 View 桌面配置的远程配置文件存储库。 <p>有关详细信息，请参阅《View 用户配置文件迁移》文档。</p> 3 允许用户登录 Windows 10 View 桌面。
Windows XP 物理机	Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面	<ol style="list-style-type: none"> 1 使用 View Persona Management 为用户配置 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面。请参阅配置 View Persona Management 部署。 <p>注 在完成步骤 2 之前，不要向用户推出 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面。</p> <ol style="list-style-type: none"> 2 运行 View V1 到 V2 配置文件迁移实用程序。 <ul style="list-style-type: none"> ■ 对于源配置文件，请指定 Windows XP 物理机上的本地配置文件。 ■ 对于目标配置文件，请指定您为 View 部署配置的远程配置文件存储库。 <p>有关详细信息，请参阅《View 用户配置文件迁移》文档。</p> 3 允许用户登录其 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面。

原始部署方案...	目标部署方案...	请执行以下任务:
<p>使用漫游用户配置文件解决方案的 Windows XP 物理机或虚拟机。例如，您的部署可能会使用以下解决方案之一：</p> <ul style="list-style-type: none"> ■ View Persona Management ■ RTO 虚拟配置文件 ■ Windows 漫游配置文件 <p>在这种情况下，原始用户配置文件必须保存在远程配置文件存储库中。</p>	<p>Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面</p>	<ol style="list-style-type: none"> 1 使用 View Persona Management 为用户配置 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面。请参阅配置 View Persona Management 部署。 <hr/> <p>注 在完成步骤 2 之前，不要向用户推出 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面。</p> <ol style="list-style-type: none"> 2 运行 View V1 到 V2 配置文件迁移实用程序。 <ul style="list-style-type: none"> ■ 对于源配置文件，请指定 Windows XP 系统的远程配置文件存储库。 ■ 对于目标配置文件，请指定您为 View 部署配置的远程配置文件存储库。 <p>有关详细信息，请参阅《View 用户配置文件迁移》文档。</p> 3 允许用户登录其 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面。
<p>Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 物理机或虚拟机。 旧版系统无法安装 View Agent 5.x。</p>	<p>Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面</p>	<ol style="list-style-type: none"> 1 使用 View Persona Management 为用户配置 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面。请参阅配置 View Persona Management 部署。 2 在 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 系统上安装独立的 View Persona Management 软件。请参阅安装独立的 View Persona Management。 3 配置旧版 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 系统，使其与 View 桌面使用同一个远程配置文件存储库。请参阅配置用户配置文件存储库。 <p>最简单的方法是在 Active Directory 中使用相同的 View Persona Management 组策略设置来控制旧版系统和 View 桌面。请参阅添加 View Persona Management ADM 或 ADMX 模板文件。</p> <ol style="list-style-type: none"> 4 向用户推出 Windows 7、Windows 8、Windows Server 2008 R2 或 Windows Server 2012 R2 View 桌面。

用户配置管理和 Windows 漫游配置文件

启用用户配置管理时，您无法使用 Windows 漫游配置文件的功能管理 View 用户配置。

例如，如果您登录到一个桌面的客户机操作系统，请导航至“系统属性”对话框中的**高级**选项卡，并将“用户配置文件”设置从**漫游配置文件**更改为**本地配置文件**，View Persona Management 将继续在本地桌面和远程用户配置存储库之间同步用户配置。

但是，您可以在用户配置中指定文件和文件夹，让 Windows 漫游配置文件功能而不是 View Persona Management 来管理它们。您可以使用 **Windows 漫游配置文件同步策略** 指定这些文件和文件夹。

配置 View Persona Management 部署

要配置 View Persona Management，您需要设置一个用于存储用户配置文件的远程存储库，在提供远程桌面会话的虚拟机上安装带有 **View Persona Management** 安装选项的 Horizon Agent，添加并配置 View Persona Management 组策略设置，然后部署桌面池。

也可以针对非 View 部署来配置 View Persona Management。在您在用户的非 View 笔记本电脑、桌面或虚拟机上安装 View Persona Management 的独立版本。还必须设置远程存储库并配置 View Persona Management 组策略设置。

设置 View Persona Management 部署概述

要为 View 桌面部署或独立计算机设置 View Persona Management，您必须执行几项高级任务。

您可以以其他顺序执行这些任务，但建议您遵循此处给出的顺序。例如，部署桌面池后，您可以在 Active Directory 中配置或重新配置组策略设置。

- 1 配置远程存储库以存储用户配置文件。

您可以配置一个网络共享位置或使用针对 Windows 漫游配置文件配置的现有 Active Directory 用户配置文件路径。

- 2 在用于创建桌面池的虚拟机上安装带有 **View Persona Management** 安装选项的 Horizon Agent。

要为非 View 笔记本电脑、桌面或虚拟机配置 View Persona Management，请在目标部署中的每个计算机上安装独立的 View Persona Management 软件。

- 3 将 View Persona Management ADM 模板文件或 View Persona Management ADMX 模板文件添加到 Active Directory 服务器或父虚拟机的本地计算机策略配置。

要为整个 View 或非 View 部署配置 View Persona Management，请将 ADM 模板文件或 ADMX 模板文件添加到 Active Directory 中。

要为一个桌面池配置 View Persona Management，可以采用以下方法：

- 将 ADM 模板文件或 ADMX 模板文件添加到用于创建该池的虚拟机中。
- 将 ADM 模板文件或 ADMX 模板文件添加到 Active Directory，并将组策略设置应用到包含池中计算机的 OU。

- 4 通过启用**管理用户配置**组策略设置启用 View Persona Management。

- 5 如果您为远程配置文件存储库配置了网络共享，请启用**用户配置存储库位置**组策略设置并指定网络共享路径。

- 6 （可选）在 Active Directory 或本地计算机策略配置中配置其他组策略设置。

- 7 在安装了 Horizon Agent（带有 **View Persona Management** 安装选项）的虚拟机上创建桌面池。

配置用户配置文件存储库

您可以配置一个远程存储库，以便存储用户数据和设置、特定于应用程序的数据以及用户配置文件中由用户生成的其他信息。如果您已在部署中配置 Windows 漫游配置文件，可以使用现有的 Active Directory 用户配置文件路径代替。

注 无需配置 Windows 漫游配置文件即可配置 View Persona Management。

前提条件

- 熟悉配置共享文件夹所需的最低访问权限。请参阅[为 View Persona Management 设置共享文件夹访问权限](#)。
- 熟悉创建用户配置文件存储库的指导信息。请参阅[为 View Persona Management 创建网络共享位置](#)。

步骤

- 1 确定使用现有的 Active Directory 用户配置文件路径，还是在网络共享位置上配置用户配置文件存储库。

选项	操作
使用现有的 Active Directory 用户配置文件路径	如果当前已配置 Windows 漫游配置文件，则可以使用 Active Directory 中支持漫游配置文件的用户配置文件路径。在此过程中，您可以跳过其余步骤。
配置网络共享位置以存储用户配置文件存储库	如果当前未配置 Windows 漫游配置文件，则必须为用户配置文件存储库配置一个网络共享位置。按照此过程的其余步骤进行操作。

- 2 在用户可以从桌面客户机操作系统访问的计算机上创建一个共享文件夹。

如果 %用户名% 不是您配置的文件夹路径的一部分，View Persona Management 将在路径后加上 %用户名%.%用户域%。

例如：\\server.domain.com\VPRepository\%username%.%userdomain%

- 3 为包含用户配置文件的共享文件夹设置访问权限。

小心 确保访问权限配置正确。共享文件夹访问权限配置错误是导致 View Persona Management 出现问题的最常见原因。

为 View Persona Management 设置共享文件夹访问权限

View Persona Management 和 Windows 漫游配置文件需要对用户配置文件存储库拥有特定的最小级别权限。View Persona Management 还要求在共享文件夹中存放数据的用户的安全组必须在共享上拥有读取属性。

请在您的用户配置文件存储库和重定向文件夹共享上设置必需的访问权限。

表 18-2. 用户配置文件存储库和重定向文件夹共享所必需的最低 NTFS 权限

用户帐户	必需的最低权限
创建者所有者	完全控制，仅子文件夹和文件
管理员	无。应启用 Windows 组策略设置：将管理员安全组添加到漫游用户配置文件。在组策略对象编辑器中，此策略设置位于：计算机配置\管理模板\系统\用户配置文件。
需要在共享上存放数据的用户的安全组	列出文件夹/读取数据、创建文件夹/附加数据、读取属性 - 仅此文件夹
每个人	无权限
本地系统	完全控制，此文件夹、子文件夹和文件

表 18-3. 用户配置文件存储库和重定向文件夹共享所必需的共享级别 (SMB) 权限

用户帐户	默认权限	必需的最低权限
每个人	只读	无权限
需要在共享上存放数据的用户的安全组	N/A	完全控制

有关漫游用户配置文件安全性的信息，请参阅 Microsoft TechNet 主题《Security Recommendations for Roaming User Profiles Shared Folders》（针对漫游用户配置文件共享文件夹的安全性建议）。[http://technet.microsoft.com/en-us/library/cc757013\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc757013(Ws.10).aspx)

为 View Persona Management 创建网络共享位置

当您创建一个共享文件夹作为配置文件存储库使用时，您必须遵循特定的指导原则。

- 如果使用 Windows 8 桌面，且网络共享使用 EMC Isilon NAS 设备上的 OneFS 文件系统，则 OneFS 文件系统必须是 6.5.5.11 版或更高版本。
- 您可以在服务器上创建共享文件夹、网络连接存储 (NAS) 设备或网络服务器。
- 该共享文件夹不必与 View 连接服务器位于同一个域中。
- 共享文件夹必须位于将配置文件存储于共享文件夹的用户所在的 Active Directory 林中。
- 您必须使用一个足够大的共享驱动器来为您的用户存储用户配置文件信息。要支持大型 View 部署，您可以为不同桌面池配置单独的存储库。

如果用户有权访问多个池，则共享用户的池必须使用相同的配置文件存储库进行配置。如果您授权用户访问两个位于不同配置文件存储库的池，则用户无法从每个池中的桌面访问相同版本的配置文件。

- 您必须创建完整的配置文件路径，用户配置文件将被创建于该路径下。如果该路径的某一部分不存在，Windows 将在第一个用户登录时创建缺失的文件夹，并将用户安全限制分配到这些文件夹。Windows 将相同的安全限制分配到该路径下创建的每个文件夹中。

例如，对于 user1 您可以配置 View Persona Management 路径 \\server\VPRepository\profiles\user1。如果您创建了网络共享位置 \\server\VPRepository，profiles 文件夹不存在，当 user1 登录时，Windows 将创建路径 \\profiles\user1。Windows 将限制 user1 帐户访问 \\profiles\user1 文件夹。如果另一个用户以配置文件路径 \\server\VPRepository\profiles 登录，则第二个用户无法访问存储库且用户配置文件复制失败。

使用 View Persona Management 选项安装 Horizon Agent

要在 View 桌面上使用 View Persona Management 功能，您必须在用于创建桌面池的虚拟机上安装带有 View Persona Management 安装选项的 Horizon Agent。

对于自动池，您可以在用作父项或模板的虚拟机上安装带有 View Persona Management 安装选项的 Horizon Agent。当您从虚拟机创建桌面池时，View Persona Management 软件将在您的 View 桌面上部署。

对于手动池，您必须在每个用作池中桌面的虚拟机上安装带有 View Persona Management 安装选项的 Horizon Agent。使用 Active Directory 为手动池配置 View Persona Management 组策略。另一种方法是在每个计算机上添加 ADM 模板文件或 ADMX 模板文件并配置组策略。

前提条件

- 确认您在 Windows 7、Windows 8、Windows 10、Windows Server 2008 R2 或 Windows Server 2012 R2 虚拟机上执行安装。View Persona Management 无法在 Microsoft RDS 主机上运行。
无法在物理机上安装带有 View Persona Management 安装选项的 Horizon Agent。您可以在物理机上安装独立的 View Persona Management 软件。请参阅[安装独立的 View Persona Management](#)。
- 确认您可以作为虚拟机的管理员登录。
- 确认本地 RTO 虚拟配置文件 2.0 未安装在虚拟机上。如果存在本地 RTO 虚拟配置文件 2.0，请在安装带有 View Persona Management 安装选项的 Horizon Agent 前将其卸载。
- 熟悉安装 Horizon Agent 的过程。请参阅[在虚拟机上安装 Horizon Agent](#)或在[未受管计算机上安装 Horizon Agent](#)。

步骤

- ◆ 在虚拟机上安装 Horizon Agent 时，请选择 View Persona Management 安装选项。

后续步骤

将 View Persona Management ADM 模板文件或 View Persona Management ADMX 模板文件添加到 Active Directory 服务器或虚拟机自身的本地计算机策略配置。请参阅[添加 View Persona Management ADM 或 ADMX 模板文件](#)。

安装独立的 View Persona Management

要在非 View 物理机或虚拟机上使用 View Persona Management，请安装独立版本的 View Persona Management。您可以通过命令行运行交互式安装或静默安装。

将独立的 View Persona Management 软件安装在目标部署中的每台单独的计算机或虚拟机上。

前提条件

- 确认您在 Windows 7、Windows 8、Windows 10、Windows Server 2008 R2 或 Windows Server 2012 R2 物理机或虚拟机上执行安装。View Persona Management 无法在 Windows Server 或 Microsoft RDS 主机上运行。确认系统满足《View 安装指南》文档的“独立 View Persona Management 支持的操作系统”中所述的要求。

- 确认您可以作为系统的管理员登录。
- 确认 View Agent 5.x 或更高版本未安装在该计算机上。
- 确认本地 RTO 虚拟配置文件 2.0 未安装在虚拟机上。
- 如果想要执行静默安装，请熟悉 MSI 安装程序命令行选项。请参阅 [Microsoft Windows Installer 命令行选项](#)。

步骤

- 1 从 VMware 产品页面 <http://www.vmware.com/products/> 下载独立的 View Persona Management 安装程序文件。

安装程序文件名为 VMware-personamanagement-y.y.y-xxxxxx.exe 或 VMware-personamanagement-x86_64-y.y.y-xxxxxx.exe，其中 y.y.y 是版本号，xxxxxx 是内部版本号。

- 2 运行交互式安装程序或执行静默安装。

选项	描述
交互式安装	<p>a 要启动安装程序，请双击安装程序文件。</p> <p>b 接受 VMware 许可条款。</p> <p>c 单击安装。</p> <p>默认情况下，View Persona Management 安装在 C:\Program Files\VMware\VMware View Persona Management 目录中。</p> <p>d 单击完成。</p>
静默安装	<p>在计算机上打开 Windows 命令提示符，在一行内键入安装命令。</p> <p>例如：VMware-personamanagement-y.y.y-xxxxxx.exe /s /v"/qn /l*v ""c:\persona.log"" ALLUSERS=1"</p> <p>重要事项 必须在命令行中包含 ALLUSERS=1 属性。</p>

- 3 重新启动系统以使安装更改生效。

后续步骤

将 View Persona Management ADM 模板文件添加到 Active Directory 或本地组策略配置中。

添加 View Persona Management ADM 或 ADMX 模板文件

View Persona Management ADM 模板文件和 View Persona Management ADMX 模板文件中包含可用于配置 View Persona Management 的组策略设置。在配置策略前，您必须向本地系统或 Active Directory 服务器添加 ADM 模板文件或 ADMX 模板文件。

要在单独的系统中配置 View Persona Management，您可以在本地系统中将组策略设置添加到本地计算机策略配置中。

要为桌面池配置 View Persona Management，您可以在用于部署桌面池的模板或父虚拟机上将组策略设置添加到本地计算机策略配置中。

要在整个域级别上配置 View Persona Management 并将配置应用到多个 View 计算机或整个部署，您可以将组策略设置添加到 Active Directory 服务器的组策略对象 (GPO)。在 Active Directory 中，您可以为使用 View Persona Management 的 View 计算机创建一个 OU，创建一个或多个 GPO，并将 GPO 与 OU 链接。要为不同类型的用户配置单独的 View Persona Management 策略，您可以为特定 View 计算机组创建 OU，并将不同的 GPO 应用到这些 OU。

例如，您可能会为安装了 View Persona Management 的 View 计算机创建一个 OU，为安装了单机版 View Persona Management 软件的物理机创建另一个 OU。

有关在 View 中执行 Active Directory 组策略的示例，请参见 [Active Directory 组策略示例](#)。

将用户配置管理 ADM 模板添加到单个系统

要为单一桌面池配置 View Persona Management，必须将用户配置管理 ADM 模板文件添加到用于创建该池的虚拟机上的本地计算机策略。要在单个系统中配置 View Persona Management，必须将用户配置管理 ADM 模板文件添加到该系统。

前提条件

- 确认在系统中安装了带有 View Persona Management 安装选项的 Horizon Agent。请参阅[使用 View Persona Management 选项安装 Horizon Agent](#)。
- 确认您可以作为系统的管理员登录。

步骤

- 1 从 VMware 下载站点中下载 View 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 View 提供组策略设置的所有 ADM 和 ADMX 文件均在此文件中提供。

- 2 解压缩文件，并将 ADM 文件 ViewPM.adm 复制到本地系统。
- 3 在本地系统上，单击开始 > 运行。
- 4 键入 gpedit.msc 并单击确定。
- 5 在本地计算机策略窗口中导航到计算机配置并右键单击管理模板。

注 请不要选择用户配置下的管理模板。

- 6 单击添加/移除模板并单击添加。
- 7 浏览到包含 ViewPM.adm 文件的目录。
- 8 选择 ViewPM.adm 文件并单击添加。
- 9 关闭添加/移除模板窗口。

View Persona Management 组策略设置即被添加到本地系统的本地计算机策略配置中。您必须使用 gpedit.msc 显示该设置。

后续步骤

在本地系统上配置 View Persona Management 组策略设置。请参阅[配置 View Persona Management 策略](#)。

将用户配置管理 ADM 模板添加到 Active Directory 中

要为您的部署配置 View Persona Management，可以将用户配置管理 ADM 模板文件添加到 Active Directory 服务器中的组策略对象 (GPO)。

前提条件

- 为您的 View Persona Management 部署创建 GPO，并将其链接到包含使用 View Persona Management 的 View 计算机的组织单位。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。
- 确认在 Active Directory 服务器可访问的系统中使用 View Persona Management 安装选项安装了 Horizon Agent。请参阅[使用 View Persona Management 选项安装 Horizon Agent](#)。

步骤

- 1 从 VMware 下载站点中下载 View 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 View 提供组策略设置的所有 ADM 和 ADMX 文件均在此文件中提供。

- 2 解压缩文件，并将 View Persona Management ADM 模板文件 ViewPM.adm 复制到 Active Directory 服务器。
- 3 在 Active Directory 服务器上，打开组策略管理控制台。
例如，启动“运行”对话框，键入 `gpmc.msc` 并单击**确定**。
- 4 在左窗格中，选择包含 View 计算机的域或组织单位。
- 5 在右侧窗格中，右键单击为组策略设置创建的 GPO 并选择**编辑**。
屏幕上将显示**组策略对象编辑器**窗口。
- 6 在“组策略对象编辑器”中，右键单击**计算机配置**下的**管理模板**，然后选择**添加/移除模板**。
- 7 单击**添加**，浏览到 ViewPM.adm 文件，然后单击**打开**。
- 8 单击**关闭**，将 ADM 模板文件中的策略设置应用到 GPO。

模板名称将显示在左侧窗格的**管理模板**下。

后续步骤

在 Active Directory 服务器上配置 View Persona Management 组策略设置。

将用户配置管理 ADMX 模板文件添加至 Active Directory 或单独的系统

您可以将用户配置管理 ADMX 模板文件添加至 Active Directory 服务器或单独的系统。

前提条件

- 确认安装了带有 View Persona Management 安装选项的 Horizon Agent。请参阅[使用 View Persona Management 选项安装 Horizon Agent](#)。
- 确认 gpedit.msc 或相应的组策略编辑器可用。

步骤

- 1 从 VMware 下载站点中下载 View 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 View 提供组策略设置的所有 ADM 和 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，然后将 View Persona Management ADMX 文件复制到您的 Active Directory 服务器或单独的用户配置主机（单独系统）。

a 将 ViewPM.admx 文件复制到 C:\Windows\PolicyDefinitions\ 目录。

b 将语言资源文件 ViewPM.adml 复制到 Active Directory 服务器或单独用户配置主机上 C:\Windows\PolicyDefinitions\ 中的相应子文件夹。

例如，对于简体中文区域设置，将 ViewPM.adml 文件复制到 C:\Windows\PolicyDefinitions\zh-CN\ 目录。

- 3 在您的 Active Directory 主机上，打开“组策略管理编辑器”，或者，在一个单独的用户配置主机上，使用 gpedit.msc 实用程序打开本地组策略编辑器。

在计算机配置 > 策略 > 管理模板 > 用户配置管理中安装 View Persona Management 组策略设置。

后续步骤

（可选）配置 View Persona Management 组策略设置。请参阅[配置 View Persona Management 策略](#)。

配置 View Persona Management 策略

要使用 View Persona Management，您必须启用管理用户配置组策略设置，此设置可以激活 View Persona Management 软件。要在不使用 Active Directory 用户配置文件路径的情况下设置用户配置文件存储库，您必须配置用户配置存储库位置组策略设置。

您可以配置可选的组策略设置来配置 View Persona Management 部署的其他设置。

如果部署中已配置 Windows 漫游配置文件，您可以使用现有的 Active Directory 用户配置文件路径。您可以禁用或不配置用户配置存储库位置。

前提条件

- 熟悉管理用户配置和用户配置存储库位置组策略设置。请参阅[漫游和同步组策略设置](#)。

- 如果您要在本地系统上设置组策略，请熟悉打开“组策略”窗口的方法。请参见[将用户配置管理 ADM 模板添加到单个系统](#)中的[步骤 3](#)和[步骤 4](#)。
- 如果您要在 Active Directory 服务器中设置组策略，请熟悉启动“组策略对象编辑器”的方法。请参见[将用户配置管理 ADM 模板添加到 Active Directory](#)中的[步骤 3](#)到[步骤 5](#)。

步骤

- 1 打开“组策略”窗口。

选项	描述
本地系统	打开“本地计算机策略”窗口。
Active Directory 服务器	打开“组策略对象编辑器”窗口。

- 2 展开计算机配置文件夹并导航至用户配置管理文件夹。

选项	描述
Windows 7 及更高版本或 Windows Server 2008 及更高版本	展开下列文件夹： 管理模板 、 传统管理模板 (ADM) 、 VMware View Agent 配置 、 用户配置管理
Windows Server 2003	展开下列文件夹： 管理模板 、 VMware View Agent 配置 、 用户配置管理

- 3 打开[漫游和同步](#)文件夹。

- 4 双击[管理用户配置](#)，然后单击已启用。

此设置将激活 View Persona Management。禁用或未配置此设置时，View Persona Management 管理无法工作。

- 5 键入配置文件上传时间间隔（以分钟为单位），然后单击[确定](#)。

配置文件上传时间间隔决定 View Persona Management 将用户配置文件更改复制到远程存储库的频率。默认上传时间间隔为 10 分钟。

- 6 双击[用户配置存储库位置](#)，然后单击已启用。

如果您已部署 Windows 漫游配置文件，可以为远程配置文件存储库使用 Active Directory 用户配置文件路径。您无需配置[用户配置存储库位置](#)。

- 7 键入指向存储用户配置文件的网络文件服务器共享位置的 UNC 路径。

例如：\\server.domain.com\UserProfilesRepository\%username%

您的部署中的虚拟机必须可以访问此网络共享。

如果您打算使用 Active Directory 用户配置文件路径，则无需指定 UNC 路径。

- 8 如果在您的部署中已配置 **Active Directory** 用户配置文件路径，请确定使用该路径还是覆盖该路径。

选项	操作
使用网络共享。	选中 覆盖 Active Directory 用户配置文件路径（如果已配置） 复选框。
使用 Active Directory 用户配置文件路径（如果存在）。	不选中 覆盖 Active Directory 用户配置文件路径（如果已配置） 复选框。

- 9 单击 **确定**。

- 10 （可选）配置其他 View Persona Management 组策略设置。

创建使用用户配置管理的桌面池

要为 View 桌面使用 View Persona Management，您必须创建桌面池并在每个计算机上安装 View Persona Management 代理。

您不能在 RDS 桌面池上使用 View Persona Management，这些桌面池运行在远程桌面服务 (RDS) 主机上。

前提条件

- 确认在您用于创建桌面池的虚拟机中安装了带有 **View Persona Management** 安装选项的 Horizon Agent。请参阅 [使用 View Persona Management 选项安装 Horizon Agent](#)。
- 如果您打算仅为桌面池配置 View Persona Management 策略，请确认已将 View Persona Management ADM 模板文件添加到虚拟机，并已在“本地计算机策略”配置中配置了组策略设置。请参阅 [将用户配置管理 ADM 模板添加到单个系统](#)和[配置 View Persona Management 策略](#)。

步骤

- ◆ 从虚拟机生成快照或模板，并创建自动桌面池。
您可以使用包含完整虚拟机或链接克隆的池配置 View Persona Management。这些池可使用专用分配或浮动分配。
- ◆ （可选）要在手动桌面池中使用 View Persona Management，请选择在其上安装了带有 **View Persona Management** 选项的 Horizon Agent 计算机。

注 在 View 桌面池中部署 View Persona Management 后，如果从 View 计算机中移除 **View Persona Management** 安装选项或完全卸载 Horizon Agent，则会从当前未登录的用户的计算机中移除本地用户配置文件。对于当前已登录的用户，会在卸载过程中从远程配置文件存储库中下载用户配置文件。

配置 View Persona Management 部署的最佳实践

您应当遵循配置 View Persona Management 的最佳实践以提升用户桌面体验，提高桌面性能并确保 View Persona Management 与其他 View 功能协同高效工作。

确定是否在注销时移除本地用户配置文件

默认情况下，在用户注销时，View Persona Management 不从本地计算机删除用户配置文件。**注销时移除本地用户配置**策略不可用。在许多情况下，默认设置是一种最佳实践，因为它可以减少 I/O 操作，避免多余的行为。

例如，如果您要部署浮动分配池并在注销时刷新或删除计算机，请禁用这一策略。刷新或删除虚拟机时，本地配置文件即被删除。在一个浮动分配自动池中，您可以在注销后删除完整的虚拟机。在一个浮动分配链接克隆池中，您可以在注销时刷新或删除克隆。

如果部署专用分配池，您可以保持该策略禁用，因为用户在每次会话中都返回到相同计算机。当禁用该策略时，一名用户登录，View Persona Management 不需要下载本地配置文件中的文件。如果使用永久磁盘配置了专用分配链接克隆池，保持该策略禁用可以避免永久磁盘中的用户数据被删除。

在某些情况下，您可能希望启用**注销时移除本地用户配置**策略。

处理包括 View Persona Management 和 Windows 漫游配置文件部署

在 Windows 漫游配置文件所在的部署中，用户使用 View Persona Management 访问 View 桌面或使用 Windows 漫游配置文件访问标准桌面时，最佳实践是为两种桌面环境使用不同配置文件。如果 View 桌面和启动桌面的客户端计算机处于同一域内，且您使用 Active Directory GPO 配置 Windows 漫游配置文件和 View Persona Management，请启用**用户配置存储库位置**策略，并选择**覆盖 Active Directory 用户配置文件路径 (如果已配置)**。

当用户从客户端计算机注销时，该做法可以防止 Windows 漫游配置文件覆盖 View Persona Management 配置文件。

如果用户打算在现有 Windows 漫游配置文件和 View Persona Management 配置文件间共享数据，您可以配置 Windows 文件夹重定向。

配置重定向文件夹的路径

当您使用**文件夹重定向**组策略设置时，配置的文件夹路径应包含 %username%，但请确保路径中的最后一个子文件夹使用重定向文件夹的名称（如 My Videos）。路径中的最后一个文件夹的名称将成为用户桌面上显示的文件夹名称。

例如，如果将路径配置为 \\myserver\videos\%username%\My Videos，用户桌面上显示的文件夹名称即为 My Videos。

如果 %username% 是路径中的最后一个子文件夹，则用户名即作为文件夹名显示。例如，用户 JDoe 在桌面上看不到名为 My Videos 的文件夹，但可以看到一个名为 JDoe 的文件夹，并且无法轻松识别该文件夹。

使用 Windows 事件日志监控 View Persona Management 部署

要帮助您管理部署，View Persona Management 提供了改进的日志消息和配置文件大小以及文件和文件夹计数跟踪功能。View Persona Management 根据文件和文件夹计数在 Windows 事件日志中建议需要重定向的文件夹，并提供这些文件夹的统计信息。例如，用户登录时，Windows 事件日志可能会显示以下建议以重定向文件夹：

```
Profile path: \\server.domain.com\persona\user1V2
...
Folders to redirect:
\\server.domain.com\persona\user1V2 Reason: Folder size larger than 1GB
\\server.domain.com\persona\user1V2\Documents Reason: More than 10000 files and folders
```

其他最佳实践

您也可以遵循以下建议：

- 默认情况下，许多防病毒产品不扫描脱机文件。例如，当用户登录到桌面时，这些防病毒产品不扫描**预加载的文件和文件夹**或 **Windows 漫游配置文件同步**组策略设置未指定的用户配置文件。对于许多部署，默认行为是最佳实践，因为它减少了按需扫描时下载文件所需的 I/O 负载。

如果你想从远程存储库中检索文件和启用脱机文件扫描，请参阅您的防病毒产品的文档。

- 强烈建议您采用标准实践做法备份 View Persona Management 用于存储配置文件存储库的网络共享位置。

注 请勿将 MozyPro 等备份软件或 Windows 卷备份服务与 View Persona Management 配合使用来备份 View 桌面上的用户配置文件。

View Persona Management 可确保将用户配置文件备份到远程配置文件存储库，用户无需使用其他工具来备份桌面上的用户数据。在某些情况下，MozyPro 之类的工具或 Windows 卷备份服务可能会干扰 View Persona Management，并导致数据丢失或损坏。

-
- 启动 ThinApp 应用程序时，用户可以设置 View Persona Management 策略以提高性能。请参阅 [将用户配置文件配置为包含 ThinApp 沙箱文件夹](#)。
 - 如果您的用户生成了大量的用户配置数据，并打算使用刷新和重构来管理专用分配链接克隆桌面，请配置您的桌面池来使用单独的 View Composer 永久磁盘。永久磁盘可以提高 View Persona Management 的性能。请参阅 [使用 View Persona Management 配置 View Composer 永久磁盘](#)。
 - 如果为独立笔记本电脑配置 View Persona Management，请确保用户脱机时配置文件保持同步。请参阅 [管理独立笔记本电脑上的用户配置文件](#)。
 - 不要结合使用 Windows 客户端缓存与 View Persona Management。Windows 客户端缓存系统是支持 Windows 脱机文件功能的机制。如果该系统在本地系统中生效，则文件夹重定向、登录期间脱机文件填充、后台下载及将本地配置文件复制到远程配置文件存储库等 View Persona Management 功能无法正常使用。

最好是在使用 View Persona Management 之前禁用 Windows 脱机文件功能。如果因为 Windows 客户端缓存在桌面中生效而遇到 View Persona Management 方面的问题，您可以通过同步当前驻留于本地客户端缓存数据库中的配置文件数据并禁用 Windows 脱机文件功能来解决这些问题。有关说明，请参见[知识库文章 2016416: View Persona Management features do not function when Windows Client-Side Caching is in effect](#)（如果 Windows 客户端缓存系统生效，则 View Persona Management 功能无法正常使用）。

将用户配置文件配置为包含 ThinApp 沙箱文件夹

View Persona Management 通过在用户配置文件中包含 ThinApp 沙箱文件夹来维护与 ThinApp 应用程序相关联的用户设置。启动 ThinApp 应用程序时，用户可以设置 View Persona Management 策略以提高性能。

当用户登录时，View Persona Management 在本地用户配置文件中预加载 ThinApp 沙箱文件夹和文件。在用户完成登录前，ThinApp 沙箱文件夹即创建完成。尽管在本地桌面创建的文件与用户远程配置文件中的 ThinApp 沙箱文件具有相同的基本属性和大小，但是为了提高性能，View Persona Management 不在登录时下载沙箱数据。

作为最佳实践，您可以在后台下载实际的 ThinApp 沙箱数据。启用[要在后台下载的文件组策略](#)设置，并添加 ThinApp 沙箱文件夹。请参阅[漫游和同步组策略设置](#)。

实际的 ThinApp 沙箱文件可能会很大。使用[要在后台下载的文件组策略](#)设置，用户在启动应用程序时，无需等待大文件下载。此外，如果为大文件进行了[预加载的文件和文件夹](#)设置，则用户无需在登录时等待文件预加载。

使用 View Persona Management 配置 View Composer 永久磁盘

使用 View Composer 永久磁盘，您可以在使用刷新、重构或重新平衡操作管理链接克隆操作系统磁盘时保留用户数据和设置。当用户生成大量用户配置信息时，配置永久磁盘可以提高 View Persona Management 的性能。您可以仅使用专用分配的链接克隆桌面配置永久磁盘。

View Persona Management 可以维护在网络共享位置上配置的远程存储库中的每个用户配置文件。用户登录到桌面后，用户配置文件将在用户需要时动态下载。

如果要使用 View Persona Management 配置永久磁盘，您可以刷新和重构链接克隆操作系统磁盘并将每个用户配置文件的本地副本保存在永久磁盘上。

永久磁盘可作为用户配置文件的缓存使用。当用户需要用户配置文件时，View Persona Management 无需下载与本地永久磁盘和远程存储库中相同的数据。只需下载不同步的用户配置数据。

如果要配置永久磁盘，请不要启用[注销时移除本地用户配置](#)策略。如果启用该策略，当用户注销时，永久磁盘中的用户数据将被删除。

管理独立笔记本电脑上的用户配置文件

如您在独立（非 View）笔记本电脑上安装 View Persona Management，请确保当用户的笔记本电脑脱机时，用户配置文件保持同步。

为确保独立笔记本电脑用户具有最新的本地配置文件，您可配置 View Persona Management 组策略设置 **Enable background download for laptops**。此设置可在后台将整个用户配置文件下载至独立笔记本电脑。

最佳实践是通知用户，确保他们在断开网络连接之前能够完整下载其用户配置文件。告知用户，应等待笔记本电脑屏幕上显示后台下载完成 通知后再断开网络连接。

要在用户笔记本电脑上显示后台下载完成通知，请配置 View Persona Management 组策略设置 **Show critical errors to users via tray icon alerts**。

如用户在配置文件下载完成前断开了网络连接，本地配置文件和远程配置文件可能会无法同步。用户处于脱机状态时，该用户可能会更新未完整下载的本地文件。当用户重新连接至网络时，将上传此本地配置文件，覆盖远程配置文件。可能会丢失原始远程配置文件中的数据。

您可能需要执行下列示例中的步骤。

前提条件

确认为用户的独立笔记本电脑配置了 View Persona Management。请参阅[配置 View Persona Management 部署](#)。

步骤

- 1 在控制独立笔记本电脑的 Active Directory OU 中，启用 **Enable background download for laptops** 设置。

在“组策略对象编辑器”中，展开下列文件夹：**计算机配置、管理模板、经典管理模板(ADM)、VMware View Agent 配置、用户配置管理、漫游和同步**。

仅在 Windows 7 或更高版本和 Windows Server 2008 或更高版本中显示**经典管理模板 (ADM)** 文件夹。

- 2 对于独立笔记本电脑，当用户登录时，您必须使用非 View 方法通知用户。

例如，您可发布此消息：

登录后会将您的个人数据动态下载至笔记本电脑中。将 笔记本电脑断开网络连接之前，请确保您的个人数据已完成下载。当您的个人数据完成下载时，弹出“后台下载完成”通知。

View Persona Management 组策略设置

View Persona Management ADM 模板文件和 View Persona Management ADMX 模板文件包含您添加到单个系统或 Active Directory 服务器的组策略配置中的组策略设置。您必须配置组策略设置来设置和控制 View Persona Management 的各个方面。

ADM 模板文件名为 ViewPM.adm。ADMX 模板文件名为 ViewPM.admx。

该 ADM 文件包含在名为 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip 的捆绑 .zip 文件中，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，其中包含捆绑的 .zip 文件。

在您将 ViewPM.adm 或 ViewPM.admx 文件添加到组策略配置之后，策略设置位于“组策略”窗口的用户配置管理文件夹中。

表 18-4. View Persona Management 在组策略窗口中的位置

操作系统	位置
Windows 7 及更高版本或 Windows Server 2008 及更高版本	Computer Configuration (计算机配置) > Administrative Templates (管理模板) > Classic Administrative Templates (ADM) (传统管理模板 (ADM)) > VMware View Agent Configuration (VMware View Agent 配置) > Persona Management (用户配置管理)
Windows Server 2003	Computer Configuration (计算机配置) > Administrative Templates (管理模板) > VMware View Agent Configuration (VMware View Agent 配置) > Persona Management (用户配置管理)

组策略设置包含在以下文件夹中：

- 漫游和同步
- 文件夹重定向
- 桌面 UI
- 日志记录

漫游和同步组策略设置

漫游和同步组策略设置可以打开或关闭 **View Persona Management**，设置远程存储库位置，确定哪些文件夹和文件属于用户配置文件，并且控制着同步文件夹和文件的方式。

组策略设置	说明
管理用户配置	<p>确定是使用 View Persona Management 还是 Windows 漫游配置文件来动态管理用户配置文件。此设置可打开或关闭 View Persona Management。</p> <p>启用此设置时，View Persona Management 管理用户配置文件。</p> <p>启用此设置时，您可以指定配置文件上传时间间隔（以分钟为单位）。该值可确定将用户配置文件中的更改复制到远程存储库的频率。默认值为 10 分钟。</p> <p>在禁用或未配置该设置时，用户配置文件由 Windows 管理。</p>
用户配置存储库位置	<p>指定用户配置文件存储库的位置。此设置还确定是使用 View Persona Management 中指定的网络共享位置，还是使用 Active Directory 中配置的路径来支持 Windows 漫游配置文件。</p> <p>启用此设置时，您可以使用 共享路径 来确定用户配置文件存储库的位置。</p> <p>在 共享路径 文本框中，您可以指定一个指向可供 View Persona Management 桌面访问的网络共享位置的 UNC 路径。此设置允许 View Persona Management 控制用户配置文件存储库的位置。</p> <p>例如: <code>\\server.domain.com\VPRepository</code></p> <p>如果 %用户名% 不是您配置的文件夹路径的一部分，View Persona Management 将在路径后加上 %用户名%.%用户域%。</p> <p>例如: <code>\\server.domain.com\VPRepository\%username%.%userdomain%</code></p> <p>如果您在 共享路径 中指定了一个位置，您无需在 Windows 中设置漫游配置文件或在 Active Directory 中配置用户配置文件路径以支持 Windows 漫游文件。</p> <p>有关为 View Persona Management UNC 网络共享的详细信息，请参阅配置用户配置文件存储库。</p> <p>默认情况下，使用 Active Directory 用户配置文件路径。</p> <p>具体来说，当 共享路径 留空时，将使用 Active Directory 用户配置文件路径。在禁用或未配置该设置时，共享路径 为空白且未激活。您也可以在启用此设置时留空路径。</p> <p>启用此设置后，您可以选中 覆盖 Active Directory 用户配置文件路径 (如果已配置) 复选框以确保 View Persona Management 使用 共享路径 中指定的路径。默认情况下，此复选框未选中，当两个位置均已配置时，View Persona Management 将使用 Active Directory 用户配置文件路径。</p>
注销时删除本地用户配置	<p>在用户注销时从 View 计算机中删除每个用户的本地存储配置文件。</p> <p>您还可以选中复选框以在用户配置文件被移除时删除每个用户的本地设置文件夹。选中此框将会移除 AppData\Local 文件夹。</p> <p>有关使用该设置的指导原则，请参阅配置 View Persona Management 部署的最佳实践。</p> <p>如果禁用或未配置此设置，当用户注销时，不会删除存储在本地用户配置文件（包括本地设置文件夹）。</p>
漫游本地设置文件夹	<p>与每个用户配置文件的其余部分一同漫游本地设置文件夹。</p> <p>此策略会影响 AppData\Local 文件夹。</p> <p>默认情况下，本地设置不漫游。</p> <p>如果使用 Microsoft OneDrive，您必须启用该设置。</p>

组策略设置	说明
预加载的文件和文件夹	<p>指定用户登录时下载到本地用户配置文件中的文件和文件夹列表。文件发生变更时其更改将被复制到远程存储库中。</p> <p>在某些情况下，您可能想要将特定的文件或文件夹预加载到本地存储的用户配置文件中。使用此设置来指定这些文件和文件夹。</p> <p>请指定相对于本地配置文件的根目录的路径，而不要在路径名中指定驱动器。</p> <p>例如: Application Data\Microsoft\Certificates</p> <p>预加载指定的文件和文件夹后，View Persona Management 将以与管理其他配置文件数据相同的方式管理这些文件和文件夹。用户更新预加载的文件或文件夹时，View Persona Management 会在会话过程中将更新的数据复制到远程配置文件存储库中，该过程在下次配置文件上传时间间隔间发生。</p>
预加载的文件和文件夹（例外）	<p>防止指定的文件和文件夹进行预加载。</p> <p>所选的文件夹路径必须位于预加载的文件和文件夹设置中指定的文件夹。</p> <p>请指定相对于本地配置文件的根目录的路径，而不要在路径名中指定驱动器。</p>
Windows 漫游配置文件同步	<p>指定由标准 Windows 漫游配置文件管理的文件和文件夹列表。用户登录时，将从远程存储库中检索文件和文件夹。用户注销前，不会将文件复制到远程存储库中。</p> <p>对于指定的文件和文件夹，View Persona Management 将忽略由管理用户管理设置中的配置文件上传时间间隔配置的配置文件的复制间隔。</p> <p>请指定相对于本地配置文件的根目录的路径，而不要在路径名中指定驱动器。</p>
Windows 漫游配置文件同步（例外）	<p>对于 Windows 漫游配置文件同步 设置中指定的路径，选中的文件和文件夹是例外。</p> <p>所选的文件夹路径必须位于您在 Windows 漫游配置文件同步 设置中指定的文件夹。</p> <p>请指定相对于本地配置文件的根目录的路径，而不要在路径名中指定驱动器。</p>
排除在漫游以外的文件和文件夹	<p>指定与其余的用户配置文件一同漫游的文件和文件夹列表。指定的文件和文件夹只能存在于本地系统中。</p> <p>在某些情况下，需要指定的文件和文件夹仅位于本地存储的用户配置文件中。例如，您可以将临时文件和缓存文件排除在漫游文件以外。无需将这些文件复制到远程存储库。</p> <p>请指定相对于本地配置文件的根目录的路径，而不要在路径名中指定驱动器。</p> <p>默认情况下，用户配置文件的临时文件夹、ThinApp 的缓存文件夹以及 Internet Explorer、Firefox、Chrome 和 Opera 的缓存文件夹将被排除在漫游文件夹以外。</p>
排除在漫游以外的文件和文件夹（例外）	<p>对于排除在漫游以外的文件和文件夹设置中指定的路径，选中的文件和文件夹是例外。</p> <p>所选的文件夹路径必须位于您在排除在漫游以外的文件和文件夹设置中指定的文件夹。</p> <p>请指定相对于本地配置文件的根目录的路径，而不要在路径名中指定驱动器。</p>
启用笔记本电脑的后台下载	<p>当用户登录到安装了 View Persona Management 软件的笔记本电脑时，下载用户配置文件中的所有文件。在后台下载文件。</p> <p>完成操作后，用户屏幕上会出现一个弹出式通知：后台下载完成 (Background download complete)。要允许此通知出现在用户的笔记本电脑上，您必须启用通过托盘图标警告向用户显示严重错误设置。</p> <p>注 如果您要启用此设置，最佳实践是通知用户确保在网络断开之前能将配置文件全部下载。</p> <p>如果用户在配置文件完全下载之前将独立的笔记本电脑脱机，用户将可能无法访问本地配置文件。用户脱机时将无法打开未完全下载的本地文件。</p> <p>请参阅管理独立笔记本电脑上的用户配置文件。</p>

组策略设置	说明
要在后台下载的文件夹	<p>用户登录到桌面后，选中的文件夹将在后台下载。</p> <p>在某些情况下，您可以通过在后台下载指定文件夹的内容来优化 View Persona Management。使用此设置，用户启动应用程序时无需等待大文件下载。此外，如果为大文件使用预加载的文件和文件夹设置，则用户登录时无需等待文件预加载。</p> <p>例如，您可以在要在后台下载的文件夹设置中包含 VMware ThinApp 沙箱文件夹。用户登录或在桌面上使用其他应用程序时，后台下载不会影响性能。用户启动 ThinApp 应用程序时，所需的 ThinApp 沙箱文件可能会从远程存储库下载，这样可以缩短应用程序启动时间。</p> <p>请指定相对于本地配置文件的根目录的路径，而不要在路径名中指定驱动器。</p>
要在后台下载的文件夹（例外）	<p>对于要在后台下载的文件夹设置中指定的路径，选中的文件夹是例外。</p> <p>所选的文件夹路径必须位于您在要在后台下载的文件夹设置中指定的文件夹。</p> <p>请指定相对于本地配置文件的根目录的路径，而不要在路径名中指定驱动器。</p>
已排除进程	<p>View Persona Management 忽略指定进程的 I/O。</p> <p>您可能需要将某些防病毒应用程序添加到已排除进程列表以防止出现性能问题。如果在按需扫描过程中，防病毒应用程序没有禁用脱机文件检索的功能，则已排除进程设置将防止应用程序进行不必要的文件检索。但是，View Persona Management 会将更改复制到已排除进程创建的用户配置文件中的文件和设置。</p> <p>要将进程添加到已排除进程列表，请启用此设置，单击显示，键入进程名称，然后单击确定。例如：process.exe。</p>
清理 CLFS 文件	<p>登录后从漫游配置文件中删除由公用日志文件系统 (CLFS) 针对 ntuser.dat 和 usrclass.dat 生成的文件。</p> <p>仅当必须修复这些文件出现问题的用户配置文件时，才启用此设置。否则，请禁用或不配置此设置。</p>

文件夹重定向组策略设置

使用文件夹重定向组策略设置，可以将用户配置文件文件夹重定向到网络共享。当一个文件夹被重定向，用户会话期间的所有数据都将直接存储在网络共享中。

您可以使用这些设置对必须高度可用的文件夹进行重定向。View Persona Management 以每分钟一次的频率从本地用户配置文件将更新复制到远程配置文件，具体取决于您为配置文件上传时间间隔所设置的值。但是，如果本地系统出现网络中断或连接失败，用户上次复制后的更新可能不会被保存在远程配置文件中。在某些情况下，用户无法承受丧失当前几分钟工作所带来的损失，这时可以重定向保存这些关键数据的文件夹。

以下规则和指导原则适用于文件夹重定向：

- 当您为一个文件夹启用此设置时，您必须键入文件夹重定向到的网络共享位置的 UNC 路径。
- 如果 %username% 不是您配置的文件夹路径的一部分，View Persona Management 将在 UNC 路径后面加上 %username% 。
- 作为最佳实践，配置的文件夹路径应包含 %username%，但请确保路径中的最后一个子文件夹使用重定向文件夹的名称（如 **My Videos**）。路径中的最后一个文件夹的名称将成为用户桌面上显示的文件夹名称。有关详细信息，请参阅[配置重定向文件夹的路径](#)。
- 您可以为每个文件夹配置单独的设置。您可以选择特定的文件夹进行重定向，并将其他文件夹保留在本地 View 桌面中。您还可以将不同的文件夹重定向到不同的 UNC 路径。
- 如果一个文件夹的重定向设置被禁用或未配置，该文件夹将存储在本地 View 桌面中，并根据 View Persona Management 组策略设置进行管理。

- 如果 View Persona Management 和 Windows 漫游配置文件被配置为重定向相同的文件夹，则 View Persona Management 的文件夹重定向将优先于 Windows 漫游配置文件。
- 文件夹重定向仅适用于使用 Windows shell API 重定向通用文件夹路径的应用程序。例如，如果一个应用程序将文件写入 %USERPROFILE%\AppData\Roaming，则该文件被写入本地配置文件而不被重定向到网络位置。
- 默认情况下，Windows 文件夹重定向会授予用户对重定向文件夹的独占权限。要授予域管理员对新重定向的文件夹的访问权限，您可以使用 View Persona Management 组策略设置。

Windows 文件夹重定向有一个名为**将用户独占权限授予 folder-name**的复选框，此复选框可用于向指定用户授予对重定向文件夹的专用权限。出于安全考虑，该复选框默认为选中。在选中此复选框时，管理员将无法访问重定向文件夹。如果管理员试图强制更改某个用户的重定向文件夹的访问权限，该用户将无法再使用 View Persona Management。

您可以使用**将管理员组添加到重定向文件夹**组策略设置使新重定向的文件夹可供域管理员访问。通过此设置，您可以授予域管理员组对每个重定向文件夹的完全控制。请参阅[表 18-5. 用于控制文件夹重定向的组策略设置](#)。

对于已有的重定向文件夹，请参阅[授予现有重定向文件夹的域管理员访问权限](#)。

您可指定将从文件夹重定向中排除的文件夹路径。请参阅[表 18-5. 用于控制文件夹重定向的组策略设置](#)。

小心 View 不支持将文件夹重定向到 View Persona Management 所管理的配置文件中已有的文件夹。此配置可能导致 View Persona Management 出现故障和用户数据丢失。

例如，如果远程配置文件存储库中的根文件夹为 \\Server\%username%，而您将文件夹重定向到 \\Server\%username%\Desktop，这些设置会导致 View Persona Management 中的文件夹重定向失败，并且之前位于 \\Server\%username%\Desktop 文件夹中的任何内容都将丢失。

您可以将下列文件夹重定向到网络共享：

- 应用程序数据（漫游）
- 联系人
- Cookie
- 桌面
- 下载
- 收藏夹
- 历史记录
- 链接
- 我的文档
- 我的音乐
- 我的图片
- 我的视频

- 网上邻居
- 打印机邻居
- 最近使用的项目
- 保存游戏
- 搜索
- 开始菜单
- 启动项目
- 模板
- Internet 临时文件

表 18-5. 用于控制文件夹重定向的组策略设置

组策略设置	描述
将管理员组添加到重定向文件夹	决定是否将管理员组添加到每个重定向文件夹。默认情况下，用户对重定向文件夹拥有独占权限。启用此设置后，管理员也可以访问重定向文件夹。 默认情况下未配置此设置。
从文件夹重定向中排除的文件和文件夹	选定的文件和文件夹路径未被重定向到网络共享。 在某些情况下，特定的文件和文件夹必须保留在本地用户配置文件中。 要将文件夹路径添加到 从文件夹重定向中排除的文件和文件夹 列表中，请启用该设置，单击 显示 ，键入路径名，然后单击 确定 。 请指定相对于用户的本地配置文件的根目录的文件夹路径。例如： Desktop\New Folder 。
从文件夹重定向中排除的文件和文件夹（例外情况）	对于 从文件夹重定向中排除的文件和文件夹 设置中指定的路径，选中的文件和文件夹路径是例外情况。 要将文件夹路径添加到 从文件夹重定向中排除的文件和文件夹（例外情况） 列表中，请启用该设置，单击 显示 ，键入路径名，然后单击 确定 。 请指定位于 从文件夹重定向中排除的文件和文件夹 设置中指定的文件夹内、且相对于用户本地配置文件的根目录的文件夹路径。例如： Desktop\New Folder\Unique Folder 。

授予现有重定向文件夹的域管理员访问权限

默认情况下，Windows 文件夹重定向会授予用户对重定向文件夹的独占权限。要授予域管理员对现有重定向文件夹的访问权限，必须使用 **icacls** 实用程序。

如果您要设置新的重定向文件夹以用于 View Persona Management，可以使用**将管理员组添加到重定向文件夹**组策略设置来使域管理员可以访问新重定向的文件夹。请参阅[表 18-5. 用于控制文件夹重定向的组策略设置](#)。

步骤

- 1 设置管理员对文件和文件夹的所有权。

```
icacls "\\文件服务器\persona 共享\*" /setowner "域\管理员" /T /C /L /Q
```

例如：`icacls "\\myserver-123abc\folders*" /setowner "mycompanydomain\vcadmin" /T /C /L /Q`

2 修改文件和文件夹的 ACL。

```
icacls "\\文件服务器\persona 共享\*" /grant "管理员组":F /T /C /L /Q
```

例如: `icacls "\\myserver-123abc\folders*" /grant "Domain-Admins":F /T /C /L /Q`

3 对于每个用户文件夹,将所有权从管理员还原为相应的用户。

```
icacls "\\文件服务器\persona 共享\*" /setowner "域\文件夹所有者" /T /C /L /Q
```

例如: `icacls "\\myserver-123abc\folders*" /setowner "mycompanydomain\user1" /T /C /L /Q`

桌面 UI 组策略设置

桌面 UI 组策略设置控制用户能够在其桌面上看到的 View Persona Management 设置。

组策略设置	描述
隐藏本地脱机文件图标	确定是否在用户查看属于用户配置文件的本地存储文件时隐藏脱机图标。启用此设置后,将在 Windows Explorer 和大多数 Windows 对话框中隐藏脱机图标。 默认情况下,隐藏脱机图标。
下载大文件时显示进度	确定当客户端从远程存储库获取大型文件时,是否在用户的桌面上显示进度窗口。 如果启用此设置,您可以指定开始显示进度窗口的最小文件大小(以 MB 为单位)。当 View Persona Management 确定将从远程存储库中获取指定数量的数据时,将显示该窗口。该值是一次获取的所有文件的总和。 例如,如果设置值为 50 MB,当获取一个 40 MB 的文件时,将不会显示该窗口。如果要在第一个文件下载过程中再获取一个 30 MB 的文件,这时总下载量超过设置值,则显示进度窗口。当此文件开始下载时,随即出现进度窗口。 默认情况下,该值为 50 MB。 默认情况下,不显示进度窗口。
通过托盘图标警告向用户显示严重错误	当复制或网络连接失败时,桌面托盘将显示严重错误图标警告。 默认情况下,这些图标警告是隐藏的。

日志组策略设置

日志组策略设置可确定 View Persona Management 日志文件的名称、位置和行为。

下表描述了各项日志记录组策略设置。

组策略设置	说明
Logging filename (日志文件名)	指定本地 View Persona Management 日志文件的完整路径名。 默认路径为 ProgramData\VMware\VDM\logs\filename。 默认日志文件名为 VMWVvp.txt。
Logging destination (日志目标)	确定是否将所有日志消息写入日志文件、调试端口或同时选择两者。 默认情况下,日志消息会发送到日志文件。
Logging flags (日志标记)	指定生成的日志消息的类型。 <ul style="list-style-type: none">■ Log information messages (记录信息消息)。■ Log debug messages (记录调试消息)。 如果此设置已禁用或未配置,并且如果默认情况下配置了该设置,日志消息将设置为信息级别。

组策略设置	说明
日志历史记录深度	确定 View Persona Management 所维护的历史日志文件数。 要维护的历史日志文件数最小可设置为 1，最大可设置为 10。 默认情况下维护一个历史日志文件。
将日志上传到网络	用户注销时，将 View Persona Management 日志文件上传到指定的网络共享。 启用此设置时，请指定网络共享路径。网络共享路径必须为 UNC 路径。View Persona Management 不创建网络共享。 默认情况下，日志文件不会上传到网络共享。

排除计算机和桌面池的问题

您可以采取多种操作来诊断和修复在创建和使用计算机及桌面池时遇到的问题。

用户在使用 **Horizon Client** 访问桌面和应用程序时可能会遇到困难。您可以采取故障排除操作来调查问题原因并尝试自行解决问题，也可以从 **VMware** 技术支持部门获取帮助。

本章讨论了以下主题：

- [显示出现问题的计算机](#)
- [向桌面用户发送消息](#)
- [桌面池置备或重新创建问题](#)
- [排除网络连接问题](#)
- [排除 USB 重定向故障](#)
- [管理未授权用户的计算机和策略](#)
- [使用 ViewDbChk 命令解决数据库不一致问题](#)
- [更多故障排除信息](#)

显示出现问题的计算机

您可以采用列表形式显示 **View** 检测到的、操作可疑的计算机。

View Administrator 会显示出现以下问题的计算机：

- 已开机但没有响应。
- 长时间保持置备状态。
- 已就绪但报告中指出不接受连接。
- 在 **vCenter Server** 中丢失。
- 当前有用户登录控制台、有未经授权的用户登录，或者未通过 **View** 连接服务器实例登录。

步骤

- 1 在 **View Administrator** 中，选择**资源 > 计算机**。
- 2 在 **vCenter** 虚拟机选项卡上，单击**问题计算机**。

后续步骤

您应当采取的措施取决于 View Administrator 所报告的计算机问题。

- 如果链接克隆计算机处于错误状态，View 自动恢复机制将试图开启，或关闭并重新启动链接克隆。如果多次恢复尝试失败，则此链接克隆将被删除。在特定情况下，链接克隆可重复删除和重新创建。请参阅[重复删除和重新创建的计算机故障排除](#)。
- 如果计算机已开启但没有响应，应重新启动该计算机的虚拟机。如果计算机仍没有响应，则需要验证计算机操作系统是否支持该 Horizon Agent 版本。您可以使用带 -A 选项的 vdmadmin 命令显示 Horizon Agent 版本。有关更多信息，请参阅《View 管理指南》文档。
- 如果计算机长时间保持置备状态，应删除其虚拟机并重新克隆。验证是否有足够的磁盘空间用来置备计算机。请参阅[虚拟机长时间处于“置备”状态](#)。
- 如果计算机报告其已经就绪，但不接受连接，请检查防火墙配置，确保显示协议未被阻止。请参阅[计算机与 View 连接服务器实例之间的连接问题](#)。
- 如果 vCenter Server 中缺少某个计算机，请验证是否已在预期的 vCenter Server 上配置该计算机的虚拟机，或者该计算机是否已被移到其他 vCenter Server 上。
- 如果计算机上当前有用户登录，但不是在控制台上登录，则必定是远程会话。如果无法联系已登录的用户，则可能需要重新启动虚拟机以强行注销这些用户。

向桌面用户发送消息

有些情况下，您可能需要向当前已登录桌面的用户发送消息。例如，如果您需要对计算机进行维护，可以要求用户临时注销或警告他们服务将会中断。您可向多个用户发送消息。

步骤

- 1 在 View Administrator 中，单击目录 > 桌面池。
- 2 双击一个池，然后单击会话选项卡。
- 3 选择一个或多个计算机，然后单击发送消息。
- 4 键入消息，选择消息类型，然后单击确定。

消息类型可以是信息、警告或错误。

消息将发送至活动会话中选定的所有计算机。

桌面池置备或重新创建问题

您可以使用多种方法来诊断和修复置备或重新创建桌面池时出现的问题。

即时克隆置备或推送映像故障

即时克隆桌面池的等待处理的映像处于故障状态。

问题

在池创建或推送映像操作期间，系统显示以下错误消息：故障类型为 `SERVER_FAULT_FATAL` – 运行时错误：启动关机后调用了方法 (`Fault type is SERVER_FAULT_FATAL – Runtime error: Method called after shutdown was initiated`)。

原因

副本连接服务器启动后，在其他连接服务器执行映像操作期间，偶尔可能会发生此错误。

解决方案

- ◆ 如果在池创建期间发生此错误，则启用置备（如果已将其禁用）。如果已启用置备，则先将其禁用后再启用。
- ◆ 如果在推送映像操作期间发生此错误，则对同一映像启动其他推送映像操作。

即时克隆映像发布失败

View Administrator 显示映像发布失败。

问题

创建即时克隆桌面池或启动推送映像后，在您检查操作的状态时，View Administrator 显示映像发布失败。

解决方案

- ◆ 如果已禁用置备，则将其重新启用。如果已启用置备，则先将其禁用后再启用。这会导致 View 触发新的初始发布操作。
- ◆ 如果确定当前映像存在某些问题，则使用其他映像启动另一个推送映像操作。

后续步骤

如果映像发布反复失败，请等待 30 分钟后重试。

在即时克隆置备期间无休止地进行错误恢复

在置备即时克隆桌面池期间，错误恢复陷入无休止的循环中

问题

在置备期间，即时克隆可能会进入错误状态，并显示消息“代理和连接服务器之间无网络连接 (No network connection between Agent and connection Server)”。自动错误恢复机制会删除并重新创建克隆，之后克隆又进入相同的错误状态，并且该过程会无限次地重复。

原因

可能的原因包括永久性网络错误或自定义后脚本的路径不正确。

解决方案

- ◆ 修复网络中或自定义后脚本的路径中存在的任何错误。

无法删除孤立的即时克隆

在置备期间，即时克隆可能会进入错误状态，并且您无法从 View Administrator 中删除桌面池，不过这种情况极少发生。

问题

要删除池，View 会向 vCenter Server 发送关闭克隆电源的请求。但是，对于孤立的克隆，这些请求会失败。结果是 View 无法删除池。

解决方案

- 1 从 vCenter Server 中，取消注册孤立的克隆。
- 2 从 View Administrator 中，删除这些克隆。

如果找不到自定义规范，创建池操作将失败

如果找不到自定义规范，创建桌面池的操作将失败。

问题

您将无法创建桌面池并在事件数据库中看到以下消息。

```
Provisioning error occurred for Machine<varname>Machine_Name</varname>:Customization failed for Machine (部署计算机“计算机名”时出现错误：自定义计算机失败)
```

原因

最有可能造成此问题的原因是，您的权限不足，无法访问自定义规范或创建池。另一个可能的原因是自定义规范已被重命名或删除。

解决方案

- ◆ 检验您是否具有足够的权限来访问自定义规范和创建池。
- ◆ 如果自定义规范因重命名或删除而不再存在，可选择另一个规范。

因权限问题导致池创建操作失败

如果存在 ESX/ESXi 主机、ESX/ESXi 群集或数据中心的访问权限问题，您将无法创建桌面池。

问题

您无法在 View Administrator 中创建桌面池，因为模板、ESX/ESXi 主机、ESX/ESXi 群集或数据中心不可访问。

原因

有很多原因可导致出现这种问题。

- 您没有创建池所需的适当权限。
- 您没有访问模板所需的适当权限。
- 您没有访问 ESX/ESXi 主机、ESX/ESXi 群集或数据中心所需的适当权限。

解决方案

- ◆ 如果“模板选择”屏幕未显示任何可用模板，请确认您有足够的权限来访问模板。
- ◆ 确认您有足够的权限来访问 ESX/ESXi 主机、ESX/ESXi 群集或数据中心。
- ◆ 确认您有足够的权限来创建池。

因配置问题导致池置备失败

如果模板不可用或虚拟机映像已被移动或删除，部署桌面池的操作就可能失败。

问题

您将无法置备桌面池并在事件数据库中看到以下消息。

```
Provisioning error occurred on Pool <varname>Desktop_ID</varname> because of a configuration problem  
(因配置问题导致池“桌面 ID”出现部署错误)
```

原因

有很多原因可导致出现这种问题。

- 模板无法访问。
- 模板名称已在 vCenter 中更改。
- 模板已被移到 vCenter 中的其他文件夹。
- 虚拟机映像已在 ESX/ESXi 主机之间移动或已被删除。

解决方案

- ◆ 确认模板可访问。
- ◆ 确认为模板指定的名称和文件夹正确无误。
- ◆ 如果在 ESX/ESXi 主机之间移动了虚拟机映像，请将虚拟机移到正确的 vCenter 文件夹下。
- ◆ 如果删除了虚拟机映像，请在 View Administrator 中删除该虚拟机条目并重新创建或还原映像。

由于 View 连接服务器实例无法连接 vCenter 导致池置备失败

如果连接服务器无法连接到 vCenter，部署桌面池的操作会失败。

问题

您将无法部署桌面池并在事件数据库中看到以下某个错误消息。

- Cannot log in to vCenter at address *VC_Address* (无法登录以 "VC_Address" 为地址的 vCenter)
- The status of vCenter at address *VC_Address* is unknown (以 "VC_Address" 为地址的 vCenter 的状态未知)

原因

导致 View 连接服务器实例无法连接 vCenter 的原因如下。

- vCenter Server 上的 Web 服务已停止。
- View 连接服务器主机与 vCenter Server 之间存在网络连接问题。
- vCenter 或 View Composer 的端口号及详细登录信息已更改。

解决方案

- ◆ 确认 vCenter 上正在运行 Web 服务。
- ◆ 确认 View 连接服务器主机与 vCenter 之间不存在网络连接问题。
- ◆ 在 View Administrator 中，确认为 vCenter 和 View Composer 配置了端口号和详细登录信息。

因数据存储问题导致池置备失败

如果数据存储的磁盘空间不足，或者您的权限不足以访问数据存储，置备桌面池的操作就会失败。

问题

您将无法部署桌面池并在事件数据库中看到以下某个错误消息。

- Provisioning error occurred for Machine *Machine_Name*:Cloning failed for Machine (部署计算机“计算机名”时出现错误：克隆计算机失败)
- Provisioning error occurred on Pool *Desktop_ID* because available free disk space is reserved for linked clones (可用磁盘空间已预留给链接克隆，因此在部署池“桌面 ID”时出现错误)
- Provisioning error occurred on Pool *Desktop_ID* because of a resource problem (因资源问题导致池“桌面 ID”出现部署错误)

原因

您的权限不足，无法访问所选的数据存储，或者该桌面池的数据存储空间不足。

解决方案

- ◆ 确认您有足够的权限来访问所选的数据存储。
- ◆ 检验配置了数据存储的磁盘空间是否已满。
- ◆ 如果磁盘已满或空间已被预留，请释放一些磁盘空间，重新平衡可用的数据存储，或者将数据存储迁移到较大的磁盘上。

vCenter Server 过载导致池置备失败

如果 vCenter Server 由于请求过多而过载，部署桌面池的操作可能会失败。

问题

您将无法部署桌面池并在事件数据库中看到以下错误消息。

```
Provisioning error occurred on Pool <varname id="varname_76C2270646664C0B89AC2F37A5F3F201">Desktop_ID</varname> because of a timeout while customizing (因自定义超时，池 <varname id="varname_76C2270646664C0B89AC2F37A5F3F201">Desktop_ID</varname> 出现置备错误)
```

原因

vCenter 由于请求过多而过载。

解决方案

- ◆ 在 View Administrator 中，减少 vCenter Server 并发部署和电源操作的最大次数。
- ◆ 配置其他 vCenter Server 实例。

有关配置 vCenter Server 的详细信息，请参阅《View 安装指南》文档。

虚拟机长时间处于“置备”状态

克隆完成后，虚拟机长时间处于“部署”状态。

问题

虚拟机长时间处于“部署”状态。

原因

最有可能造成此问题的原因是，您在克隆操作期间重新启动了 View 连接服务器实例。

解决方案

- ◆ 删除虚拟机，重新进行克隆。

虚拟机长时间处于“正在自定义”状态

克隆完成后，虚拟机长时间处于“正在自定义”状态。

问题

虚拟机长时间处于“自定义”状态。

原因

最有可能造成此问题的原因是，磁盘空间不足，无法启动虚拟机。必须先启动虚拟机，才能进行自定义。

解决方案

- ◆ 删除虚拟机，以便从长时间自定义状态中恢复。
- ◆ 如果磁盘已满，请释放一些磁盘空间，或者将数据存储迁移到较大的磁盘上。

移除孤立的或已删除的链接克隆

某些情况下，View、View Composer 和 vCenter Server 中的链接克隆数据可能会不同步，而您可能无法置备或删除链接克隆计算机。

问题

- 无法置备链接克隆桌面池。
- 置备链接克隆计算机失败，并出现以下错误：已存在此输入规范的虚拟机 (Virtual machine with Input Specification already exists)
- 在 View Administrator 中，链接克隆计算机长时间处于 Deleting 状态。无法在 View Administrator 中重新启动 Delete 命令，因为计算机已处于 Deleting 状态。

原因

当 View Composer 数据库包含的链接克隆信息与 View LDAP、Active Directory 或 vCenter Server 中的信息不一致时将会出现这个问题。下列几种情况可导致信息不一致：

- 创建池后在 vCenter Server 中手动更改了链接克隆虚拟机的名称，从而导致 View Composer 和 vCenter Server 会使用不同的名称来指代同一个虚拟机。
- 存储失败或手动操作导致虚拟机从 vCenter Server 中删除。View Composer 数据库、View LDAP 和 Active Directory 中仍然存在链接克隆虚拟机数据。
- 从 View Administrator 中删除池时，网络连接或其他故障导致虚拟机仍然存留在 vCenter Server 中。

如果置备桌面池后在 vSphere Client 中对虚拟机进行了重命名，请尝试将虚拟机重命名为在 View 中置备时所使用的名称。

如果其他的数据库信息不一致，请使用 SviConfig RemoveSviClone 命令移除以下项目：

- 来自 View Composer 数据库的链接克隆数据库条目
- 来自 Active Directory 的链接克隆虚拟机帐户

■ 来自 vCenter Server 的链接克隆虚拟机

该 SviConfig 实用程序与 View Composer 应用程序位于同一位置。默认路径为 C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe。

重要事项 只有经验丰富的 View Composer 管理员才可以使用 SviConfig 实用程序。该实用程序旨在解决 View Composer 服务的相关问题。

请采取以下步骤：

- 1 确认 View Composer 服务正在运行。
- 2 在 View Composer 计算机上的 Windows 命令提示符中运行 SviConfig RemoveSviClone 以下命令：

```
sviconfig -operation=removesviclone
          -VmName=虚拟机名称
          [-AdminUser=本地管理员用户名]
          -AdminPassword=本地管理员密码
          [-ServerUrl=View Composer Server URL]
```

例如：

```
sviconfig -operation=removesviclone -vmname=MyLinkedClone
          -adminuser=Admin -adminpassword=Pass -serverurl=ViewComposerURL
```

VmName 和 AdminPassword 参数是必须的。AdminUser 参数的默认值是 Administrator。

ServerURL 参数的默认值是 https://localhost:18443/SviService/v2_0

有关从 View LDAP 中移除虚拟机信息的更多信息，请参阅 VMware 知识库文章 2015112：《从 VMware View Manager 和 VMware Horizon View 中的 View Composer 数据库中手动删除链接克隆或失效虚拟桌面条目》。

重复删除和重新创建的计算机故障排除

View 可重复删除和重新创建处于错误状态的链接克隆计算机和完整克隆计算机。

问题

链接克隆计算机或完整克隆计算机在错误状态中创建、删除，然后又在错误状态中重新创建。此循环持续重复。

原因

大型桌面池置备完成后，一个或多个虚拟机将可能处于错误状态。View 自动恢复机制将尝试打开故障虚拟机的电源。尝试特定次数后如果虚拟机未打开电源，View 将删除此虚拟机。

根据池的大小要求，View 将创建新的虚拟机，使用的计算机名称往往与原计算机相同。如果新的虚拟机置备时出现同样的错误，此虚拟机将被删除，此过程将会重复执行。

可以对链接克隆计算机和完整克隆计算机执行自动恢复操作。

如果虚拟机的自动恢复尝试失败，则仅当虚拟机为浮动计算机或未分配给用户的专用计算机时，View 才会删除此虚拟机。此外，池置备禁用时，View 也不会删除虚拟机。

检查用于创建桌面池的父虚拟机或模板。检查虚拟机中的错误或可引起虚拟机错误的客户机操作系统。

对于链接克隆，解决父虚拟机中的错误并拍摄新的快照。

- 如果很多计算机都处于错误状态，则使用新的快照或模板重新创建池。
- 如果大部分计算机都处于正常运行状态，请选择 **View Administrator** 中的桌面池，单击**编辑**，选择“vCenter 设置”选项卡，选择新的快照作为默认基础映像，并保存编辑。

使用新的快照创建新的链接克隆计算机。

对于完整克隆，解决虚拟机中的错误，生成新的模板，并重新创建池。

排除 QuickPrep 自定义问题

造成 View Composer QuickPrep 自定义脚本故障的原因有很多。

问题

QuickPrep 同步后脚本或关机脚本无法执行。在某些情况下，脚本可能只会有一些链接克隆上成功执行，在另外一些上失败。

原因

导致 QuickPrep 脚本故障的常见原因包括：

- 脚本超时
- 脚本路径引用了一个需要使用解释程序的脚本
- 脚本运行时所用的帐户没有足够的权限来执行脚本任务

解决方案

- ◆ 查看自定义脚本日志。

QuickPrep 自定义信息被写入到 Windows temp 目录下的日志文件中：

`C:\Windows\Temp\vmware-viewcomposer-ga-new.log`

- ◆ 确定脚本是否超时。

View Composer 会终止用时超过 20 秒的自定义脚本。日志文件会显示一条提示脚本已经启动的消息，之后还会显示一条超时消息：

```
2010-02-21 21:05:47,687 [1500] INFO Ready -  
[Ready.cpp, 102] Running the PostSync script:cmd /c  
C:\temp\build\composer.bat  
2010-02-21 21:06:07,348 [1500] FATAL Guest -  
[Guest.cpp, 428] script cmd /c  
C:\temp\build\composer.bat timed out
```

要解决此超时问题，请提高脚本的超时限制值并重新运行脚本。

- ◆ 确定脚本路径是否有效。

如果您使用需要解释程序才能执行脚本的脚本语言，则脚本路径必须以解释程序二进制文件的路径为开头。

例如，如果您指定 `C:\script\myvb.vbs` 作为 QuickPrep 自定义脚本的路径，View Composer Agent 将无法执行该脚本。您必须指定一个以解释程序二进制文件路径开始的路径：

```
C:\windows\system32\cscript.exe c:\script\myvb.vbs
```

- ◆ 确定用于运行脚本的帐户是否具有合适的权限来执行脚本任务。

QuickPrep 在配置运行 VMware View Composer 客户机代理服务器服务的帐户下运行脚本。默认情况下，此帐户为 **Local System**。

请勿更改这个登录帐户。如果您更改登录帐户，链接克隆将不会启动。

查找并取消保护未使用的 View Composer 副本

在某些情况下，当 View Composer 副本不再具有任何与其相关联的链接克隆时，这些副本仍会保留在 vCenter Server 中。

问题

未使用的副本保留在 vCenter Server 文件夹中。您无法通过 vSphere Client 删除此副本。

原因

View Composer 操作过程中出现网络中断，或未使用正确的 View 命令直接从 vSphere 中删除相关联的链接克隆可能会在 vCenter Server 中留下未使用的副本。

在 vCenter Server 中，副本是受保护的实体。无法通过普通 vCenter Server 或 vSphere Client 管理命令删除这些副本。

使用 `SviConfig FindUnusedReplica` 命令可查找指定文件夹中的副本。您可使用 `-Move` 参数将副本移至另一个文件夹。`-Move` 参数会去除未使用副本的保护之后再移动该副本。

重要事项 只有经验丰富的 View Composer 管理员才可以使用 SviConfig 实用程序。该实用程序旨在解决 View Composer 服务的相关问题。

该 SviConfig 实用程序与 View Composer 应用程序位于同一位置。默认路径为 `C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe`。

开始前，请确认无链接克隆与此副本相关联。

熟悉了解 SviConfig FindUnusedReplica 的参数：

- **DsnName**。DSN 为必须用于连接数据库的 DSN。
- **UserName**。用来连接数据库的用户名。如果未指定该参数，则使用 Windows 身份验证。
- **Password**。连接数据库的用户的密码。如果未指定该参数且未使用 Windows 身份验证，系统会提示您稍后再输入密码。

- **ReplicaFolder**。副本文件夹的名称。根文件夹使用空字符串。默认值为 `VMwareViewComposerReplicaFolder`。
- **UnusedReplicaFolder**。包含所有未使用的副本的文件夹名称。默认值为 `UnusedViewComposerReplicaFolder`。使用 `Move` 参数时，使用该参数指定目标文件夹。
- **OutputDir**。生成包含未使用副本列表（存储在 `unused-replica-*.txt` 文件中）的输出目录的目录名。默认值为当前工作目录。
- **Move**。确定是否去除未使用副本虚拟机的保护，以及是否将它们移至指定的文件夹。`UnusedReplicaFolder` 参数指定目标文件夹。`Move` 参数的默认值为 `false`。

`DsnName`、`Username` 和 `Password` 为必需参数。`DsnName` 不得为空字符串。

请采取以下步骤：

- 1 停止 View Composer 服务。
- 2 在 View Composer 计算机上的 Windows 命令提示符中运行 `SviConfig FindUnusedReplica` 以下命令：

```
sviconfig -operation=findunusedreplica
          -DsnName=DSN 的名称
          -Username=数据库管理员用户名
          -Password=数据库管理员密码
          [-ReplicaFolder=副本文件夹名称]
          [-UnusedReplicaFolder=未使用的副本文件夹名称。]
          [-OutputDir=输出文件目录]
          [-Move=true or false]
```

例如：

```
sviconfig -operation=FindUnusedReplica -DsnName=SVI
          -Username=SVIUser -Password=1234 -Move=True
```

- 3 重新启动 View Composer 服务。
- 4 （可选）将副本移至新文件夹之后，从 vCenter Server 中删除副本虚拟机。

View Composer 置备错误

如果 View Composer 置备或重构链接克隆计算机时发生错误，错误代码可指明发生故障的原因。错误代码显示在 View Administrator 中的计算机状态栏中。

[表 19-1. View Composer 置备错误](#) 介绍了 View Composer 置备错误代码。

此表列出了与 View Composer 和 QuickPrep 自定义相关的错误。View 连接服务器和其他 View 组件中可能还会发生其他干扰计算机置备的错误。

表 19-1. View Composer 置备错误

错误	描述
0	策略已成功应用。 注 结果代码 0 不会出现在 View Administrator 中。除非 View Composer 域外部发生 View 错误，否则链接克隆计算机将进入“就绪”状态。此结果代码用于表示完整性。
1	未能设置计算机名称。
2	未能将用户配置文件重定向到 View Composer 永久磁盘。
3	未能设置计算机的域帐户密码。
4	未能备份用户配置文件密钥。进行重构操作后，当用户下次登录该链接克隆计算机时，操作系统会为其创建一个新的配置文件目录。创建新的配置文件后，用户将看不到旧的配置文件数据。
5	未能还原用户的配置文件。在此情况下，用户不应登录计算机，因为配置文件的状态还没有定义。
6	其他错误代码未涵盖的错误。客户机操作系统中的 View Composer Agent 日志文件可提供有关这些错误原因的详细信息。 例如，Windows Plug and Play (PnP) 服务超时会生成此错误代码。在此情况下，等待 PnP 服务为链接克隆虚拟机安装新卷之后，View Composer 将会超时。 根据池的配置方式，PnP 最多可以装载三个磁盘： <ul style="list-style-type: none"> ■ View Composer 永久磁盘 ■ 用于重定向客户机操作系统临时文件和页面文件的非永久磁盘 ■ 存储 QuickPrep 配置数据和其他操作系统相关数据的内部磁盘。此磁盘始终与链接克隆一起配置。 超时长度为 10 分钟。如果 PnP 在 10 分钟内未完成磁盘装载，View Composer 将出现故障，并显示错误代码 6。
7	附加到链接克隆的 View Composer 永久磁盘过多。一个克隆最多可以具有三个 View Composer 永久磁盘。
8	某个永久磁盘无法装载到创建池时选定的数据存储。
9	View Composer 无法将一次性数据文件重定向到非永久磁盘。页面文件或临时文件目录没有被重定向。
10	View Composer 在指定的内部磁盘上找不到 QuickPrep 配置策略文件。
12	View Composer 找不到包含 QuickPrep 配置策略文件和其他操作系统相关数据的内部磁盘。
13	不只一个永久磁盘被配置为重定向 Windows 用户配置文件。
14	View Composer 卸载内部磁盘失败。
15	首次启动链接克隆后，View Composer 从配置策略文件中读取的计算机名称与当前系统名称不符。
16	由于客户机操作系统的批量许可证未激活，因此 View Composer Agent 没有启动。
17	View Composer Agent 未启动。代理在等待 Sysprep 启动时超时。
18	View Composer Agent 在自定义期间未能将链接克隆虚拟机加入域中。
19	View Composer Agent 未能执行同步后脚本。
20	View Composer Agent 未能处理机器密码同步事件。 这个错误可能是暂时的。如果链接克隆加入到域，则密码没有问题。 如果克隆未能加入域，请重新执行您在错误发生之前进行的操作。如果您此前重新启动了克隆，请再次重新启动。如果您此前刷新了克隆，请再次刷新。如果克隆仍然无法加入域，请重构克隆。
21	View Composer Agent 无法装载系统一次性磁盘。
22	View Composer Agent 无法装载 View Composer 永久磁盘。

排除网络连接问题

您可以采取多种操作来诊断和修复计算机、Horizon Client 设备和 View 连接服务器实例的网络连接问题。

计算机与 View 连接服务器实例之间的连接问题

计算机与 View 连接服务器实例之间可能会出现连接问题。

问题

如果计算机与 View 连接服务器实例之间出现连接故障，您将在事件数据库中看到以下某个消息。

- 计算机 *Machine_Name* 出现置备错误：因 Horizon Agent 和连接服务器之间不存在网络通信导致自定义错误 (Provisioning error occurred for Machine Machine_Name: Customization error due to no network communication between the Horizon Agent and Connection Server)
- 置备池 *Desktop_ID* 时因 Horizon Agent 存在网络问题而出现错误 (Provisioning error occurred on Pool Desktop_ID because of a networking problem with a Horizon Agent)
- 用户 *User_Display_Name* 无法从池 *Desktop_ID* 启动：未能使用 *Protocol* 连接到计算机 *MachineName* (Unable to launch from Pool Desktop_ID for user User_Display_Name: Failed to connect to Machine MachineName using Protocol)

原因

有多种原因可导致计算机与 View 连接服务器实例之间出现连接问题。

- 在计算机上查找 View 连接服务器主机的 DNS 名称失败。
- 用于 JMS、RDP 或 AJP13 通信的端口被防火墙规则阻止。
- View 连接服务器主机上的 JMS 路由器发生故障。

解决方案

- ◆ 在计算机的命令提示符处，键入 `nslookup` 命令。

```
nslookup CS_FQDN
```

其中 *CS FQDN* 是 View 连接服务器主机的完全限定域名 (Fully Qualified Domain Name, FQDN)。如果该命令未能返回 View 连接服务器主机的 IP 地址，可运用常规的网络故障排除技术来修改 DNS 配置。

- ◆ 在计算机的命令提示符处，键入 `telnet` 命令以确认 Horizon Agent 与 View 连接服务器主机建立 JMS 通信时使用的 TCP 端口 4001 工作正常。

```
telnet CS_FQDN 4001
```

如果建立了 `telnet` 连接，说明 JMS 的网络连接正常。

- ◆ 如果在 DMZ 中部署了安全服务器，请验证是否已在内部防火墙中配置了例外规则来允许通过 TCP 端口 3389 在安全服务器与虚拟机之间建立 RDP 连接。

- ◆ 如果未使用安全连接，请验证防火墙规则是否允许客户端通过 TCP 端口 3389 与虚拟机建立直接 RDP 连接，或者通过 TCP 端口 4172 和 UDP 端口 4172 与虚拟机建立直接 PCoIP 连接。
- ◆ 检验是否配置了内部防火墙异常规则以允许每个安全服务器通过 TCP 端口 4001 (JMS) 和 TCP 端口 8009 (AJP13)，和与其关联的 View 连接服务器主机建立连接。

Horizon Client 与 PCoIP 安全网关之间的连接问题

在配置了 PCoIP 安全网关对通过 PCoIP 进行通信的外部用户进行身份验证时，Horizon Client 与安全服务器或 View 连接服务器主机之间可能会出现连接问题。

问题

使用 PCoIP 的客户端无法连接或显示 View 桌面。安全服务器或 View 连接服务器实例的初始登录成功，但当用户选择一个 View 桌面时，连接失败。在安全服务器或 View 连接服务器主机上配置了 PCoIP 安全网关时会发生此问题。

注 通常，PCoIP 安全网关应用在安全服务器上。在外部客户端直接连接到 View 连接服务器主机的网络配置中，PCoIP 安全网关也可以配置在 View 连接服务器上。

原因

导致 PCoIP 安全网关连接问题的原因有多种。

- Windows 防火墙关闭了 PCoIP 安全网关所需的端口。
- 在安全服务器或 View 连接服务器实例上未启用 PCoIP 安全网关。
- 未正确配置 PCoIP 外部 URL 设置。必须将该设置指定为客户端可通过 Internet 访问的外部 IP 地址。
- PCoIP 外部 URL、安全加密链路外部 URL、Blast 外部 URL 或其他地址被配置为指向其他安全服务器或 View 连接服务器主机。在安全服务器或 View 连接服务器主机上配置上述地址时，所有地址都必须允许客户端系统连接当前主机。
- 客户端通过关闭了 PCoIP 安全网关所需端口的外部 Web 代理进行连接。例如，酒店网络或公共无线连接中的 Web 代理可能会阻止所需端口。
- 与配置了 PCoIP 安全网关的安全服务器配对的 View 连接服务器实例的版本 View 4.5 或更低版本。安全服务器及配对的 View 连接服务器实例必须为 View 4.6 或更高版本。

解决方案

- ◆ 查看是否在防火墙上为安全服务器或 View 连接服务器主机打开了以下端口。

端口	描述
TCP 4172	从 Horizon Client 到安全服务器或 View 连接服务器主机的通信。
UDP 4172	Horizon Client 与安全服务器或 View 连接服务器主机之间的双向通信。
TCP 4172	从安全服务器或 View 连接服务器主机到 View 桌面的通信。
UDP 4172	安全服务器或 View 连接服务器主机与 View 桌面之间的双向通信。

- ◆ 在 View Administrator 中，确保已启用 PCoIP 安全网关。
 - a 单击 **View 配置 > 服务器**。
 - b 在**连接服务器**选项卡中，选择 View 连接服务器实例，然后单击**编辑**。
 - c 选中**使用 PCoIP 安全网关与计算机建立 PCoIP 连接**。
默认禁用 PCoIP 安全网关。
 - d 单击**确定**。
- ◆ 在 View Administrator 中，确保已正确配置 PCoIP 外部 URL。
 - a 单击 **View 配置 > 服务器**。
 - b 选择要配置的主机。
 - 如果用户连接到安全服务器上的 PCoIP 安全网关，请在**安全服务器**选项卡上选择该安全服务器。
 - 如果用户连接到 View 连接服务器实例上的 PCoIP 安全网关，请在**连接服务器**选项卡上选择该实例。
 - c 单击**编辑**。
 - d 在 **PCoIP 外部 URL** 文本框中，确保 URL 包含客户端可通过 Internet 访问的安全服务器或 View 连接服务器主机的外部 IP 地址。
指定端口 4172。请勿包含协议名。
例如: **10.20.30.40:4172**
 - e 确保此对话框中的所有地址都允许客户端系统连接此主机。
“编辑安全服务器设置”对话框中的所有地址都必须允许客户端系统连接此安全服务器主机。“编辑 View 连接服务器设置”对话框中的所有地址都必须允许客户端系统连接此 View 连接服务器实例。
 - f 单击**确定**。
为用户用于连接到 PCoIP 安全网关的每个安全服务器和 View 连接服务器实例重复上述步骤。
- ◆ 如果用户通过网络外部的 Web 代理进行连接，且代理阻止所需端口，请引导用户通过其他网络位置进行连接。

计算机与 View 连接服务器实例之间的连接问题

计算机与 View 连接服务器实例之间可能会出现连接问题。

问题

如果计算机与 View 连接服务器实例之间出现连接故障，您将在事件数据库中看到以下某个消息。

- 计算机 *Machine_Name* 出现置备错误：因 Horizon Agent 和连接服务器之间不存在网络通信导致自定义错误 (Provisioning error occurred for Machine Machine_Name: Customization error due to no network communication between the Horizon Agent and Connection Server)
- 置备池 *Desktop_ID* 时因 Horizon Agent 存在网络问题而出现错误 (Provisioning error occurred on Pool Desktop_ID because of a networking problem with a Horizon Agent)
- 用户 *User_Display_Name* 无法从池 *Desktop_ID* 启动：未能使用 *Protocol* 连接到计算机 *MachineName* (Unable to launch from Pool Desktop_ID for user User_Display_Name: Failed to connect to Machine MachineName using Protocol)

原因

有多种原因可导致计算机与 View 连接服务器实例之间出现连接问题。

- 在计算机上查找 View 连接服务器主机的 DNS 名称失败。
- 用于 JMS、RDP 或 AJP13 通信的端口被防火墙规则阻止。
- View 连接服务器主机上的 JMS 路由器发生故障。

解决方案

- ◆ 在计算机的命令提示符处，键入 `nslookup` 命令。

```
nslookup CS_FQDN
```

其中 *CS FQDN* 是 View 连接服务器主机的完全限定域名 (Fully Qualified Domain Name, FQDN)。如果该命令未能返回 View 连接服务器主机的 IP 地址，可运用常规的网络故障排除技术来修改 DNS 配置。

- ◆ 在计算机的命令提示符处，键入 `telnet` 命令以确认 Horizon Agent 与 View 连接服务器主机建立 JMS 通信时使用的 TCP 端口 4001 工作正常。

```
telnet CS_FQDN 4001
```

如果建立了 `telnet` 连接，说明 JMS 的网络连接正常。

- ◆ 如果在 DMZ 中部署了安全服务器，请验证是否已在内部防火墙中配置了例外规则来允许通过 TCP 端口 3389 在安全服务器与虚拟机之间建立 RDP 连接。
- ◆ 如果未使用安全连接，请验证防火墙规则是否允许客户端通过 TCP 端口 3389 与虚拟机建立直接 RDP 连接，或者通过 TCP 端口 4172 和 UDP 端口 4172 与虚拟机建立直接 PCoIP 连接。

- ◆ 检验是否配置了内部防火墙异常规则以允许每个安全服务器通过 TCP 端口 4001 (JMS) 和 TCP 端口 8009 (AJP13)，和与其关联的 View 连接服务器主机建立连接。

由于将 IP 地址错误地分配给克隆计算机而导致的连接问题

如果克隆计算机使用静态 IP 地址，则可能无法与之连接。

问题

无法使用 Horizon Client 连接克隆计算机。

原因

克隆计算机错误地配置为使用静态 IP 地址，而不是使用 DHCP 来获取其 IP 地址。

解决方案

- 1 验证 vCenter Server 上的桌面池的模板是否配置为使用 DHCP 为计算机分配 IP 地址。
- 2 在 vSphere Web Client 中，以手动方式从桌面池克隆一个虚拟机，并验证其是否从 DHCP 正确获取其 IP 地址。

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

以下是可能造成 USB 重定向无法正确或按照预期运行的原因。

- 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](#)。
- 在部署远程桌面和应用程序的 Windows Server 2008 RDS 主机上不支持 USB 重定向。在装有 View Agent 6.1 及更高版本的 Windows Server 2012 RDS 主机上支持 USB 重定向，但该功能仅适用于 USB 存储设备。在用作单用户桌面的 Windows Server 2008 R2 和 Windows Server 2012 R2 系统上支持 USB 重定向。
- RDS 桌面和应用程序上仅支持 USB 闪存驱动器和硬盘。无法将其他类型的 USB 设备和其他类型的 USB 存储设备（如安全存储驱动器和 USB CD-ROM）重定向至 RDS 桌面或应用程序。
- 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 View 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 PCoIP 而不是 RDP 作为协议。
- ◆ 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 View Administrator 中，转到**策略 > 全局策略**，然后验证该 USB 访问是否已在 View 策略下设置为允许。
- ◆ 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。

管理未授权用户的计算机和策略

您可以显示分配给授权已被移除的用户的计算机，还可以显示已应用于未授权用户的策略。

未授权用户可能已永久离开组织，或者您在较长时间内暂停了他们的帐户。尽管为这些用户分配了计算机，但是他们不再有权使用计算机池。

您也可以使用带有 `-O` 或 `-P` 选项的 `vdadmin` 命令来显示未授权的计算机和策略。有关更多信息，请参阅《View 管理指南》文档。

步骤

- 1 在 View Administrator 中，选择**资源 > 计算机**。
- 2 选择**更多命令 > 查看未授权的计算机**。
- 3 移除未授权用户的计算机分配。
- 4 选择**更多命令 > 查看未授权的计算机**或**更多命令 > 查看未授权的策略**（视情况而定）。
- 5 更改或移除应用于未授权用户的策略。

使用 ViewDbChk 命令解决数据库不一致问题

通过使用 `ViewDbChk` 命令，您可以解决存储有关自动桌面池中的桌面虚拟机和自动场中的 RDS 主机的信息的数据库中的不一致问题。

在 View 环境中，有关桌面虚拟机和自动场中的 RDS 主机的信息存储在以下位置：

- LDAP 数据库
- vCenter Server 数据库
- 仅限 View Composer 链接克隆计算机：View Composer 数据库

通常，您可以使用 **View Administrator** 移除或重置桌面虚拟机或 RDS 主机，以从置备或其他操作期间出现的错误中恢复。在极少情况下，不同数据库中有关处于错误状态的计算机的信息可能变得不一致，且无法使用 **View Administrator** 从错误中恢复。您可能会看到以下症状之一：

- 置备失败，并显示错误消息：带有输入规范的虚拟机已存在 (Virtual machine with Input Specification already exists)。
- 重构桌面池失败，并显示错误消息：桌面 Composer 故障：带有输入规范的虚拟机已存在 (Desktop Composer Fault: Virtual Machine with Input Specification already exists)。
- View Administrator 显示桌面计算机或 RDS 主机长时间处于“正在删除”状态。
- 您无法删除桌面池或自动场。
- 您无法删除桌面计算机或 RDS 主机。
- 在 View Administrator 的“清单”选项卡中，桌面计算机或 RDS 主机的状态丢失。

如果数据库不一致导致桌面计算机或 RDS 主机处于无法恢复的错误状态或导致无法成功完成 View Administrator 任务，您可以使用 ViewDbChk 命令解决不一致问题。ViewDbChk 命令具有以下特性：

- 在安装 View 标准服务器或 View 副本服务器时，会自动安装 ViewDbChk。在安装 View 安全服务器时，不会安装该实用程序。
- ViewDbChk 是一种可从 Windows 命令提示符或脚本运行的命令。
- ViewDbChk 支持完整虚拟机以及 View Composer 链接克隆的自动场和自动桌面池。
- 在您希望移除某个计算机时，ViewDbChk 在该计算机上执行运行状况检查，并提示您进一步确认该计算机是否运行正常。
- ViewDbChk 可以删除错误的或不完整的 LDAP 条目。
- ViewDbChk 使用 I18N 字符集支持输入和输出。
- ViewDbChk 不会移除用户数据。对于完整桌面虚拟机，ViewDbChk 从清单中移除该虚拟机，而不会将其从磁盘中删除。对于链接克隆桌面虚拟机，ViewDbChk 删除该虚拟机并将用户磁盘存档到根文件夹（对于 VMFS 数据存储）或名为 archiveUDD 的子文件夹（对于 Virtual SAN 和虚拟卷数据存储）中。
- ViewDbChk 不支持未管理的桌面计算机或手动场中的 RDS 主机。

ViewDbChk 语法

```
ViewDbChk --findDesktop --desktopName <desktop pool or farm name> [--verbose]

ViewDbChk --enableDesktop --desktopName <desktop pool or farm name> [--verbose]

ViewDbChk --disableDesktop --desktopName <desktop pool or farm name> [--verbose]

ViewDbChk --findMachine --desktopName <desktop pool or farm name> --machineName <machine name> [--verbose]

ViewDbChk --removeMachine --machineName <machine name> [--desktopName <desktop pool or farm name>] [--force] [--noErrorCheck] [--verbose]

ViewDbChk --scanMachines [--desktopName <desktop pool or farm name>] [--limit <maximum deletes>] [--force] [--verbose]

ViewDbChk --help [--commandName] [--verbose]
```

ViewDbChk 参数

参数	说明
--findDesktop	查找桌面池或场。
--enableDesktop	启用桌面池或场。
--disableDesktop	禁用桌面池或场。
--findMachine	查找计算机。
--removeMachine	从桌面池或场中移除计算机。在移除计算机之前，ViewDbChk 提示用户禁用桌面池或场。在移除计算机后，ViewDbChk 提示用户重新启用桌面池或场。

参数	说明
--scanMachines	搜索处于错误或克隆错误状态或丢失虚拟机的计算机，列出按桌面池或场分组的问题计算机并提供移除计算机的选项。在移除计算机之前，ViewDbChk 提示用户禁用桌面池或场。在桌面池或场中移除所有错误计算机后，ViewDbChk 提示用户重新启用桌面池或场。
--help	显示 ViewDbChk 的语法。
--desktopName <desktop name>	指定桌面池或场名称。
--machineName <machine name>	指定计算机名称。
--limit <maximum deletes>	限制 ViewDbChk 可以移除的计算机数目。默认值为 1。
--force	强制移除计算机，而无需用户确认。
--noErrorCheck	强制移除没有错误的计算机。
--verbose	启用详细的日志记录。

注 所有参数名称都区分大小写。

ViewDbChk 使用情况示例

一个名为 lc-pool2-2 的桌面计算机处于错误状态，我们无法使用 View Administrator 将其移除。我们使用 ViewDbChk 将其从 View 环境中移除。

```
C:\>viewdbchk --removeMachine --machineName lc-pool2-2
Looking for desktop pool "lc-pool2" in LDAP...
  Desktop Pool Name: lc-pool2
  Desktop Pool Type: AUTO_LC_TYPE
  VM Folder: /vdi/vm/lc-pool2/
  Desktop Pool Disabled: false
  Desktop Pool Provisioning Enabled: true
Looking for machine "/vdi/vm/lc-pool2/lc-pool2-2" in vCenter...
  Connecting to vCenter "https://10.133.17.3:443/sdk". This may take some time...
Checking connectivity...
  Connecting to View Composer "https://10.133.17.3:18443". This may take some time...
The desktop pool "lc-pool2" must be disabled before proceeding. Do you want to disable the desktop pool? (yes/no):yes
Found machine "lc-pool2-2"
  VM Name: lc-pool2-2
  Creation Date: 1/25/15 1:20:26 PM PST
  MOID: vm-236
  Clone Id: b12a9ed2-8535-44ee-a9d6-6c9b5cf6f878
  VM Folder: /vdi/vm/lc-pool2/lc-pool2-2
  VM State: ERROR
Do you want to remove the desktop machine "lc-pool2-2"? (yes/no):yes
Shutting down VM "/vdi/vm/lc-pool2/lc-pool2-2"...
Archiving persistent disks...
Destroying View Composer clone "b12a9ed2-8535-44ee-a9d6-6c9b5cf6f878"...
Removing ThinApp entitlements for machine "/vdi/vm/lc-pool2/lc-pool2-2"...
Removing machine "/vdi/vm/lc-pool2/lc-pool2-2" from LDAP...
Running delete VM scripts for machine "/vdi/vm/lc-pool2/lc-pool2-2"...
Do you want to enable the desktop pool "lc-pool2"? (yes/no):yes
```

更多故障排除信息

您可以在 VMware 知识库文章中找到更多故障排除信息。

VMware 知识库 (Knowledge Base, KB) 经常更新，以纳入新的 VMware 产品故障排除信息。

有关对 View 进行故障排除的更多信息，请参阅 VMware 知识库网站上提供的知识库文章：

<http://kb.vmware.com/selfservice/microsites/microsite.do>