

设置桌面 Horizon 7 for Linux

2019 年 7 月

VMware Horizon 7 7.9



vmware®

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

如果您对本文档有任何意见或建议, 请将反馈信息发送至:

docfeedback@vmware.com

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 © 2016-2019 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

目录

设置 Horizon 7 for Linux 桌面 6

1 功能和系统要求 7

- Horizon Linux 桌面的功能 7
- Horizon 7 for Linux 桌面的配置步骤概述 12
- Horizon 7 for Linux 的系统要求 13
 - 2D 和 vSGA 图形的虚拟机设置 22
 - 在 Linux 桌面上配置会话协作 24

2 为桌面部署准备 Linux 虚拟机 26

- 创建虚拟机并安装 Linux 26
- 为远程桌面部署准备 Linux 计算机 27
- 安装 Horizon Agent 的依赖项包 29

3 为 Linux 桌面设置 Active Directory 集成 30

- 将 Linux 与 Active Directory 集成 30
 - 使用 OpenLDAP 服务器直通身份验证 31
 - 设置针对 Microsoft Active Directory 的 SSSD LDAP 身份验证 31
 - 使用加入 Windbind 域解决方案 31
 - 配置 PowerBroker Identity Services Open (PBISO) 身份验证 32
 - 为 Ubuntu 桌面配置 Samba 脱机域加入 33
- 设置单点登录 35
- 设置智能卡重定向 36
 - 将 RHEL 桌面与 Active Directory 集成以进行智能卡重定向 37
 - 将 Ubuntu 桌面与 Active Directory 集成以进行智能卡重定向 39
 - 将 SLED/SLES 桌面与 Active Directory 集成以进行智能卡重定向 43
 - 为 RHEL 桌面设置智能卡重定向 45
 - 为 Ubuntu 桌面设置智能卡重定向 48
 - 为 SLED/SLES 桌面设置智能卡重定向 54
- 为 Linux 桌面设置 True SSO 57
 - 将 RHEL/CentOS 桌面与 Active Directory 集成以进行 True SSO 58
 - 将 Ubuntu 桌面与 Active Directory 集成以进行 True SSO 59
 - 将 SLED/SLES 桌面与 Active Directory 集成以进行 True SSO 62
 - 在 RHEL/CentOS 桌面上配置 True SSO 64
 - 在 Ubuntu 桌面上配置 True SSO 66
 - 在 SLED/SLES 桌面上配置 True SSO 67

4 为 Linux 桌面设置图形 70

- 为 vGPU 配置支持的 RHEL 和 SLED 分发包 70
 - 为 ESXi 主机上的 NVIDIA GRID vGPU 显卡安装 VIB 71
 - 在 Linux 虚拟机上为 vGPU 配置共享 PCI 设备 72
 - 安装 NVIDIA GRID vGPU 显卡驱动程序 74
 - 验证是否安装了 NVIDIA 显卡驱动程序 75
- 配置 RHEL 6 以使用 vDGA 75
 - 在主机上为 NVIDIA GRID 启用 DirectPath I/O 76
 - 向 RHEL 6 虚拟机添加 vDGA 直通设备 76
 - 为 vDGA 安装 NVIDIA 显卡驱动程序 77
 - 验证是否安装了 NVIDIA 显卡驱动程序 78
- 为 RHEL 7.x 配置 vSGA 79
 - 为 ESXi 主机上用于 vSGA 的 NVIDIA 显卡安装 VIB 79
 - 在 Linux 虚拟机上为 vSGA 配置 3D 功能 80
 - 验证是否正在 Linux 虚拟机上运行 vSGA 81

5 安装 Horizon Agent 83

- 在 Linux 虚拟机上安装 Horizon Agent 83
 - install_viewagent.sh 命令行选项 84
- 配置 Linux 代理的证书 85
- 在 Linux 虚拟机上升级 Horizon Agent 86
 - 在 Linux 虚拟机上升级 Horizon Agent 87
- 卸载 Horizon 7 for Linux 计算机 88

6 Linux 桌面的配置选项 89

- 在 Linux 桌面上的配置文件中设置选项 89
- 使用 智能策略 96
 - 智能策略的要求 96
 - 安装 User Environment Manager 97
 - 配置 User Environment Manager 97
 - Horizon 智能策略设置 97
 - 将条件添加到 Horizon 智能策略定义 98
 - 在 User Environment Manager 中创建 Horizon 智能策略 98
- 适用于 Linux 桌面的 Blast 设置示例 100
- 适用于 Linux 桌面的客户端驱动器重定向选项示例 100
- 禁止在 vSphere 控制台中显示 Linux 桌面 101

7 创建和管理 Linux 桌面池 102

- 创建适用于 Linux 的手动桌面池 102
- 管理适用于 Linux 的桌面池 103

- 创建适用于 Linux 的自动完整克隆桌面池 105
- 创建适用于 Linux 的即时克隆浮动桌面池 107
- 代理 PowerCLI 命令 109

8 为手动桌面池批量部署 Horizon 7 112

- Linux 桌面批量部署概览 112
- Linux 桌面批量升级概览 114
- 为克隆 Linux 桌面计算机创建虚拟机模板 114
- 用于部署 Linux 桌面的示例 PowerCLI 脚本的输入文件 116
- 用于克隆 Linux 虚拟机的示例脚本 117
- 用于将克隆的虚拟机加入 AD 域的示例脚本 121
- 使用 SSH 将克隆的虚拟机加入 Active Directory 域的示例脚本 124
- 用于将配置文件上载至 Linux 虚拟机的示例脚本 127
- 使用 SSH 将配置文件上载至 Linux 虚拟机的示例脚本 131
- 用于在 Linux 桌面计算机上升级 Horizon Agent 的示例 PowerCLI 脚本 135
- 使用 SSH 在 Linux 虚拟机上升级 Horizon Agent 的示例脚本 140
- 用于在 Linux 虚拟机上执行操作的示例脚本 145

9 对 Linux 桌面进行故障排除 150

- 在 Horizon Console 中使用 Horizon Help Desk Tool 150
 - 在 Horizon Console 中启动 Horizon Help Desk Tool 151
 - 在 Horizon Help Desk Tool 中对用户进行故障排除 151
 - Horizon Help Desk Tool 的会话详细信息 153
 - Horizon Help Desk Tool 的会话进程 156
 - 在 Horizon Help Desk Tool 中对 Linux 桌面会话进行故障排除 156
- 收集 Horizon 7 for Linux 计算机的诊断信息 157
- 对远程桌面和客户端主机之间的复制和粘贴问题进行故障排除 157
- Horizon Agent 在 iPad Pro Horizon Client 上无法断开连接 158
- SLES 12 SP1 桌面不自动刷新 158
- SSO 无法连接到关机代理 159
- 在创建适用于 Linux 的手动桌面池后无法访问虚拟机 159

设置 Horizon 7 for Linux 桌面

《设置 Horizon 7 for Linux 桌面》文档提供了有关设置 Linux 虚拟机以用作 VMware Horizon® 7 for Linux 桌面的信息。这些信息包括准备 Linux 客户机操作系统，在虚拟机上安装 Horizon Agent，以及在 Horizon Administrator 中配置计算机以在 Horizon 7 部署中使用。

目标读者

本文档中的信息适用于希望配置并使用在 Linux 客户机操作系统上运行的远程桌面的任何人。本文档中的信息是专门为熟练掌握虚拟机技术和数据中心操作并具有丰富经验的 Linux 系统管理员编写的。

功能和系统要求

使用 Horizon 6.2.x 或更高版本，用户可以连接至运行 Linux 操作系统的远程桌面。

本章讨论了以下主题：

- [Horizon Linux 桌面的功能](#)
- [Horizon 7 for Linux 桌面的配置步骤概述](#)
- [Horizon 7 for Linux 的系统要求](#)

Horizon Linux 桌面的功能

以下列表显示 Horizon Linux 桌面支持的主要功能。

在 Linux 桌面上支持的功能

Active Directory 集成

运行以下 Linux 分发包的即时克隆桌面可以使用 PowerBroker Identity Services Open (PBISO) 脱机加入 Active Directory 域中。

- Ubuntu 16.04 和 18.04
- SLED/SLES 11 和 12.x

请参阅[将 Linux 与 Active Directory 集成](#)中的“PowerBroker Identity Services Open (PBISO) 身份验证”部分，以了解更多信息。

运行以下 Linux 分发包的即时克隆桌面可以使用 Samba 脱机加入 Active Directory 域中。

- Ubuntu 16.04 和 18.04
- RHEL 6.9 和 7.3
- CentOS 6.9/7.3
- SLED 11 SP4/12

音频输入

支持从客户端主机到远程 Linux 桌面的音频输入重定向。该功能不基于 USB 重定向功能。如果您要启用该功能，则必须在安装过程中选择该功能。您必

须在音频输入应用程序中选择系统默认音频输入设备“PulseAudio 服务器(本地)”。以下 Linux 分发版支持该功能。

- 具有 MATE 或 Gnome Flashback (Metacity) 桌面环境的 Ubuntu 16.04 x64
- 具有 MATE 或 Gnome Ubuntu 桌面环境的 Ubuntu 18.04 x64
- 具有 KDE 或 Gnome 桌面环境的 RHEL 7 Workstation x64
- SLED 11 SP4 x64
- SLED/SLES 12 SP3 x64

音频输出

支持音频输出重定向。该功能在默认情况下为启用状态。要禁用此功能，您必须将 `RemoteDisplay.allowAudio` 选项设置为 **false**。在使用 **Chrome** 和 **Firefox** 浏览器访问时，VMware Horizon HTML Access 为 Linux 桌面提供音频输出支持。

自动完整克隆桌面池

您可以为 Linux 桌面创建自动完整克隆桌面池。

客户端驱动器重定向

在启用客户端驱动器重定向 (Client Drive Redirection, CDR) 功能时，您可以访问本地系统的共享文件夹和驱动器。可以使用位于远程 Linux 桌面上的主目录中的 `tsclient` 文件夹。要使用此功能，您必须安装 CDR 组件。

剪贴板重定向

通过剪贴板重定向功能，您可以在客户端主机和远程 Linux 桌面之间复制并粘贴富文本或纯文本。您可以使用 **Horizon Agent** 选项设置复制/粘贴方向和最大文本大小。该功能在默认情况下为启用状态。您可以在安装过程中禁用该功能。

FIPS 140-2 模式

为 Linux 桌面提供了联邦信息处理标准 (Federal Information Processing Standard, FIPS) 140-2 模式支持，但该支持尚未经过 NIST 加密模块验证程序 (Cryptographic Module Validation Program, CMVP) 验证。

适用于 Linux 的 Horizon 7 Agent 将实施专为 FIPS 140-2 合规性设计的加密模块。这些模块已在 CMVP 证书 #2839 和 #2866 中列出的操作环境中进行了验证，并已移植到此平台。但是，在产品路线图中，将新操作环境包括到 VMware NIST CAVP 和 CMVP 证书中的 CAVP 和 CMVP 测试要求仍有待完成。

注 要支持 FIPS 140-2 模式，需要传输层安全 (Transport Layer Security, TLS) 协议版本 1.2。

技术支持工具

Horizon Help Desk Tool 是一个 Web 应用程序，可用于对 Linux 桌面会话进行故障排除。您可以使用 Horizon Help Desk Tool 获取 Horizon 7 用户会话的状态，并执行故障排除和维护操作。请参阅在 [Horizon Console 中使用 Horizon Help Desk Tool](#)。

Horizon 智能策略

您可以使用 VMware User Environment Manager™ 9.4 或更高版本创建 Horizon 智能策略，以控制特定远程 Linux 桌面上的 USB 重定向、剪贴板重定向和客户端驱动器重定向功能的行为。请参阅[使用 智能策略](#)。

H.264 编码器

H.264 可以提高 Horizon 桌面的 Blast Extreme 性能，特别是在使用低带宽网络时。如果客户端系统禁用了 H.264，则 Blast Extreme 自动改用 JPEG/PNG 编码。

H.264 编码器包括硬件 H.264 支持和软件编码器支持。硬件 H.264 支持具有以下要求。

- 为 vGPU 配置了 NVIDIA 显卡。
- 在 NVIDIA 显卡中安装了 NVIDIA 驱动程序 384 系列或更高版本。

当系统满足上述要求时，Horizon 7 for Linux 便会使用硬件 H.264 编码器。否则，将使用软件 H.264 编码器。

即时克隆浮动桌面池

您可以为 Linux 桌面创建即时克隆浮动桌面池。只有在安装了以下 Linux 分发包的系统上，才支持使用此功能。

- Ubuntu 16.04 和 18.04
- RHEL 7.1 或更高版本
- SLED/SLES 11 和 12

有关更多信息，请参阅[创建适用于 Linux 的即时克隆浮动桌面池](#)。

K 桌面环境

在以下 Linux 分发包上支持 K 桌面环境 (K Desktop Environment, KDE)。

- CentOS 6 和 7
- RHEL 6 和 7
- Ubuntu 16.04 和 18.04
- SLED 11 SP4

键盘布局和区域设置同步

该功能指定是否将客户端的系统区域设置和当前键盘布局与 Horizon Linux 代理桌面同步。启用或未配置此设置时，允许同步。禁用此设置时，不允许同步。

只有适用于 Windows 的 VMware Horizon 支持该功能，并且该功能仅适用于英语、法语、德语、日语、韩语、西班牙语、简体中文和繁体中文区域设置。

无损 PNG

桌面上生成的图像和视频将在客户端设备上以精确到像素的方式进行渲染。

手动桌面池

计算机源。

- 受管虚拟机 - vCenter 虚拟机的计算机源。新部署和升级部署都支持受管虚拟机。

- 未受管的虚拟机 - 其他源的计算机源。只有从未受管的虚拟机部署升级的部署才支持未受管的虚拟机。

注 要确保尽可能获得最佳性能，请勿使用未受管的虚拟机。

MATE 桌面环境

在以下 Linux 分发版上支持 MATE 桌面环境。

- Ubuntu 16.04
- Ubuntu 18.04

多显示器

- vDGA/vGPU 桌面在 4 个显示器上支持最大分辨率 2560x1600。
- VMware vSphere® 6.0 或更高版本上的 2D/vSGA 桌面在 4 个显示器上支持最大分辨率 2048x1536，或者在 3 个显示器上支持最大分辨率 2560x1600。

对于 Ubuntu 16.04 和 18.04，您必须使用 Gnome、KDE 或 MATE 桌面环境才能使用多显示器功能。有关更多信息，请参阅 <http://kb.vmware.com/kb/2151294>。

对于 SLES 12 SP1，您必须将默认软件包与内核级别 kernel-default-3.12.49-11.1 一起使用。如果升级该软件包，则多显示器功能将无法使用，并会在一个显示器中显示桌面。

从 VMware Horizon HTML Access™ 5.0 版开始，在 Horizon 7 for Linux 桌面中支持多显示器功能。

为 VMware Blast 提供网络智能支持

VMware Blast 支持网络智能传输。该功能在默认情况下为启用状态。

启用用户数据报协议 (User Datagram Protocol, UDP) 后，Blast 可同时建立传输控制协议 (Transmission Control Protocol, TCP) 连接和 UDP 连接。根据当前网络状况，Blast 会在传输数据时动态选择一种数据传输方式以提供最佳用户体验。例如，在局域网中，TCP 的性能优于 UDP，因此 Blast 选择通过 TCP 来传输数据。同样，在广域网 (Wide Area Network, WAN) 中，UDP 的性能优于 TCP，那么 Blast 在该环境中便选择 UDP 传输。

如果使用的某个内嵌组件不支持 UDP，则 Blast 将仅建立 TCP 连接。例如，如果您的连接使用的是 Horizon 连接服务器或安全服务器的 Blast 安全网关组件，则会仅建立 TCP 连接。即使客户端和代理都启用了 UDP，连接也会使用 TCP，因为 Blast 安全网关不支持 UDP。如果用户从企业网络外部进行连接，UDP 组件将需要使用支持 UDP 的 VMware Unified Access Gateway（以前称为 Access Point）。

请使用以下信息建立基于 UDP 的 Blast 连接。

- 如果客户端直接连接到 Linux 桌面，请在客户端和代理中启用 UDP。默认情况下，UDP 在客户端和代理中均处于启用状态。

- 如果客户端使用 **Unified Access Gateway** 连接到 **Linux** 桌面，请在客户端、代理和 **Unified Access Gateway** 中启用 **UDP**。

会话协作

通过使用会话协作功能，用户可以邀请其他用户加入现有的远程 **Linux** 桌面会话，也可以在收到其他用户的邀请后加入协作会话。只有在安装了以下 **Linux** 分发包的远程 **Linux** 桌面上，才支持使用此功能。

- 具有 **Gnome** 桌面环境的 **Ubuntu 18.04**
- 具有 **Gnome** 桌面环境的 **RHEL 7.5** 或更高版本

单点登录

以下 **Linux** 分发包支持单点登录 (**Single Sign-On, SSO**)。

- **RHEL 7/6 Workstation x64**
- **CentOS 7/6 x64**
- **SLED/SLES 12.x SP3/SP2/SP1**
- **SLED 11.x SP4/SP3 x64**
- **Ubuntu 18.04/16.04 x64**

通过 **SSO** 实现智能卡重定向

在以下 **Linux** 分发包上支持智能卡重定向。

- **RHEL 7.1** 和更高版本
- **RHEL 6.6** 和更高版本
- **Ubuntu 18.04/16.04**
- **SLED/SLES 12.x SP3**
- **SLED 11.x SP4**

该功能支持个人身份验证 (**Personal Identity Verification, PIV**) 卡和通用访问卡 (**Common Access Card, CAC**)。有关更多信息，请参阅[设置智能卡重定向](#)。

True SSO 支持

在以下 **Linux** 分发包上支持 **True SSO**。

- **RHEL 7**
- **CentOS 7**
- **SLED/SLES 12.x SP3**
- **Ubuntu 18.04/16.04**

有关更多信息，请参阅[Linux 桌面设置 True SSO](#)。

USB 重定向

通过使用 **USB** 重定向功能，您可以从远程 **Linux** 桌面中访问本地连接的 **USB** 设备。您必须安装 **USB** 重定向组件和 **USB VHCI** 驱动程序内核模块，才能使用 **USB** 功能。请确保您已被授予足够的特权来使用要重定向的 **USB** 设备。

3Dconnexion 鼠标

要开始使用 3Dconnexion 鼠标，必须安装相应的设备驱动程序，并使用 Linux 桌面上的“连接 USB 设备”菜单，将鼠标进行配对。

3D 图形

3D 图形功能支持以下 Linux 版本和显卡的组合：

- 在具有 NVIDIA GRID K1 或 K2 显卡的 RHEL 7.x Workstation x64 上支持 vSGA。
- 在具有 NVIDIA GRID K1 或 K2 显卡的 RHEL 6.x Workstation x64 上支持 vDGA。
- 在具有 NVIDIA Tesla M6、M10、M60 或 P40 显卡的 RHEL 6.x、RHEL 7.x 或 SLED 12.x Workstation x64 上支持 vGPU。

Linux 桌面和桌面池的限制

Linux 桌面和桌面池具有以下限制：

- 不支持虚拟打印、基于位置的打印和实时视频。
- 不支持 VMware HTML Access 文件传输功能。

注 使用安全服务器时，必须在内部防火墙中打开端口 22443 才能允许安全服务器与 Linux 桌面之间的通信。

Horizon 7 for Linux 桌面的配置步骤概述

在安装和配置 Horizon 7 for Linux 桌面时，您必须按照一组不同的步骤进行操作，具体取决于在虚拟机上安装 2D 图形还是 3D 图形。

2D 图形 - 配置步骤概述

对于 2D 图形，请执行以下步骤：

- 1 查看设置 Horizon 7 for Linux 部署的系统要求。请参阅 [Horizon 7 for Linux 的系统要求](#)。
- 2 在 vSphere 中创建一个虚拟机并安装 Linux 操作系统。请参阅[创建虚拟机并安装 Linux](#)。
- 3 准备客户机操作系统以在 Horizon 7 环境中部署为桌面。请参阅[为远程桌面部署准备 Linux 计算机](#)。
- 4 配置 Linux 客户机操作系统以使用 Active Directory 进行身份验证。此步骤是根据您的环境要求使用第三方软件执行的。请参阅[将 Linux 与 Active Directory 集成](#)了解更多信息。
- 5 在 Linux 虚拟机上安装 Horizon Agent。请参阅[在 Linux 虚拟机上安装 Horizon Agent](#)。
- 6 创建一个桌面池以包含配置的 Linux 虚拟机。请参阅[创建适用于 Linux 的手动桌面池](#)。

3D 图形 - 配置步骤概述

您必须先在 Linux 虚拟机上完成 NVIDIA GRID vGPU、vDGA 或 vSGA 的配置，然后再在计算机上安装 Horizon Agent，并在 Horizon Administrator 中部署桌面池。

- 1 查看设置 Horizon 7 for Linux 部署的系统要求。请参阅 [Horizon 7 for Linux 的系统要求](#)。
- 2 在 vSphere 中创建一个虚拟机并安装 Linux 操作系统。请参阅[创建虚拟机并安装 Linux](#)。
- 3 准备客户机操作系统以在 Horizon 7 环境中部署为桌面。请参阅[为远程桌面部署准备 Linux 计算机](#)。
- 4 配置 Linux 客户机操作系统以使用 Active Directory 进行身份验证。此步骤是根据您的环境要求使用第三方软件执行的。请参阅[将 Linux 与 Active Directory 集成](#)了解更多信息。
- 5 在 ESXi 主机和 Linux 虚拟机上配置 3D 功能。按照要安装的 3D 功能的步骤进行操作。
 - 请参阅[为 vGPU 配置支持的 RHEL 和 SLED 分发包](#)。
 - 请参阅[配置 RHEL 6 以使用 vDGA](#)。
 - 请参阅[为 RHEL 7.x 配置 vSGA](#)。
- 6 在 Linux 虚拟机上安装 Horizon Agent。请参阅[在 Linux 虚拟机上安装 Horizon Agent](#)。
- 7 创建一个桌面池以包含配置的 Linux 虚拟机。请参阅[创建适用于 Linux 的手动桌面池](#)。

批量部署

使用 Horizon Administrator，您只能在手动桌面池中部署 Linux 虚拟机。使用 vSphere PowerCLI，您可以开发用于自动部署 Linux 桌面计算机池的脚本。请参阅[第 8 章 为手动桌面池批量部署 Horizon 7](#)。

Horizon 7 for Linux 的系统要求

要安装 Horizon 7 for Linux，您的 Linux 系统必须满足操作系统、Horizon 7 和 vSphere 平台的特定要求。

Horizon Agent 支持的 Linux 版本

[表 1-1. Horizon Agent 支持的 Linux 操作系统](#)中列出了桌面池中的虚拟机支持的 Linux 操作系统。

表 1-1. Horizon Agent 支持的 Linux 操作系统

Linux 分发包	架构
Ubuntu 16.04 和 18.04	x64
注 您必须应用 VMware 知识库文章 http://kb.vmware.com/kb/2151294 中所述的解决方案之一。	
RHEL 6.6、6.7、6.8、6.9、6.10、7.2、7.3、7.4、7.5 和 7.6	x64
CentOS 6.6、6.7、6.8、6.9、6.10、7.2、7.3、7.4、7.5 和 7.6	x64
NeoKylin 6 Update 1	x64
SLED 11.x SP3/SP4	x64

Linux 分发包	架构
SLED 12.x SP1/SP2/SP3	x64
SLES 12.x SP1/SP2/SP3	x64

注 Linux 代理在某些 Linux 分发包中具有依赖项包。有关详细信息，请参阅[安装 Horizon Agent 的依赖项包](#)。

所需的平台和 Horizon 7 软件版本

要安装并使用 Horizon 7 for Linux，您的部署必须满足 vSphere 平台、Horizon 7 和 Horizon Client 软件的特定要求。

表 1-2. 所需的平台和 Horizon 7 软件版本

平台和软件	支持的版本
vSphere 平台版本	<ul style="list-style-type: none"> ■ vSphere 6.0 U2 或更高版本 ■ vSphere 6.5 U1 或更高版本 ■ vSphere 6.7 或更高版本
Horizon 环境	<ul style="list-style-type: none"> ■ Horizon 连接服务器 7.9
Horizon Client 软件	<ul style="list-style-type: none"> ■ 适用于 Android 的 Horizon Client 5.1.0 ■ 适用于 Windows 的 Horizon Client 5.1.0 ■ 适用于 Linux 的 Horizon Client 5.1.0 ■ 适用于 Mac OS X 的 Horizon Client 5.1.0 ■ 适用于 iOS 的 Horizon Client 5.1.0 (iPad Pro) ■ Chrome、Firefox 和 Internet Explorer 上的 HTML Access 5.1.0 ■ 不支持零客户端。

Linux 虚拟机使用的 TCP/UDP 端口

Horizon Agent 和 Horizon Client 使用 TCP 或 UDP 端口进行相互之间以及它们与各种 Horizon Server 组件之间的网络访问。

表 1-3. Linux 虚拟机使用的 TCP/UDP 端口

源	端口	目标	端口	协议	说明
Horizon Client	*	Linux 代理	22443	TCP/UDP	如果未使用 Blast 安全网关，则为 Blast
安全服务器、 Horizon 连接服务器 或 Access Point 设备	*	Linux 代理	22443	TCP/UDP	如果使用了 Blast 安全网关，则为 Blast
Horizon Agent	*	Horizon 连接服务器	4001、4002	TCP	JMS SSL 流量。

注 有关客户端使用的 TCP 和 UDP 端口的更多信息，请参阅《Horizon Client 和 Agent 安全指南》文档中的“客户端和 Horizon Agent 使用的 TCP 和 UDP 端口”部分。

要允许用户连接到其 Linux 桌面，这些桌面必须可以接受来自 Horizon Client 设备、安全服务器和 Horizon Connection Server 的入站 TCP 连接。

在 Ubuntu 和 Kylin 分发版中，已默认配置 iptables 防火墙并设置了一条“ACCEPT”的输入策略。

在 RHEL 和 CentOS 分发版中，如果可能，Horizon Agent 安装程序脚本将配置 iptables 防火墙并设置一条“ACCEPT”的输入策略。

请确保 RHEL 或 CentOS 客户机操作系统上的 iptables 具有一条“ACCEPT”的输入策略，用于接受来自 Blast 端口 22443 的新连接。

启用 BSG 时，将通过安全服务器或 Horizon Connection Server 上的 BSG 在 Horizon Client 设备与 Linux 桌面之间建立客户端连接。未启用 BSG 时，将直接在 Horizon Client 设备与 Linux 桌面之间建立连接。

验证 Linux 虚拟机使用的 Linux 帐户

表 1-4. 帐户名称和帐户类型中列出了 Linux 虚拟机使用的帐户名称和帐户类型。

表 1-4. 帐户名称和帐户类型

帐户名称	帐户类型	使用者
根	Linux 操作系统内置	Java Standalone Agent、 mksvchanserver、Shell 脚本
vmwblast	由 Linux 代理安装程序创建	VMwareBlastServer
<当前登录用户>	Linux 操作系统内置或 AD 用户或 LDAP 用户	Python 脚本

桌面环境

Horizon 7 for Linux 支持不同 Linux 分发版中的多种桌面环境。表 1-5. 支持的桌面环境中列出了每个 Linux 分发版的默认桌面环境，以及 Horizon 7 for Linux 支持的其他桌面环境。

表 1-5. 支持的桌面环境

Linux 分发版	默认桌面环境	Horizon 7 for Linux 桌面支持的桌面环境
Ubuntu 18.04	Gnome	Gnome Ubuntu、K 桌面环境 (KDE)、MATE
Ubuntu 16.04	Unity	Gnome Flashback (Metacity)、KDE、MATE
RHEL/CentOS 6.x	Gnome	Gnome、KDE
RHEL/CentOS 7.x	Gnome	Gnome、KDE
SLED 11 SP4	Gnome	Gnome、KDE
SLED 12 SP1/SP2/SP3	Gnome	Gnome
SLES 12 SP1/SP2/SP3	Gnome	Gnome
NeoKylin 6 Update 1	Mate	Mate

要更改在某个支持的 Linux 分发版中使用的默认桌面环境，您必须执行以下步骤并使用适用于您的 Linux 桌面的命令。

注 仅当您的 Linux 桌面使用默认欢迎程序（登录屏幕）时，才可对 KDE 和 MATE 桌面环境使用单点登录 (SSO)。您必须使用表 1-6. 用于安装桌面环境的命令中列出的命令安装 KDE 和 MATE。

使用 SLED 11 SP3/SP4、RHEL/CentOS 7 和 Ubuntu 18.04/16.04 分发版时，SSO 无法对锁定的 KDE 会话解锁。您必须手动输入密码才能对锁定的会话解锁。

- 1 使用默认桌面环境设置安装支持的 Linux 分发版的操作系统。
- 2 为您的特定 Linux 分发版运行表 1-6. 用于安装桌面环境的命令中的相应命令。

表 1-6. 用于安装桌面环境的命令

Linux 分发版	新的默认桌面环境	用于更改默认桌面环境的命令
RHEL/CentOS 6	KDE	<code># yum groupinstall "X Window System" "KDE Desktop"</code>
RHEL/CentOS 7	KDE	<code># yum groupinstall "KDE Plasma Workspaces"</code>
SLED 11 SP4	KDE	<code># zypper install -t pattern desktop-kde</code>
Ubuntu 18.04/16.04	KDE	<code># apt install plasma-desktop</code>
Ubuntu 18.04	MATE 1.225	<code># apt install ubuntu-mate-desktop</code>

Linux 分发包	新的默认桌面环境	用于更改默认桌面环境的命令
Ubuntu 16.04	MATE 1.16	<pre># apt-add-repository ppa:ubuntu-mate-dev/xenial-mate # apt update # apt upgrade # apt install mate # apt install ubuntu-mate-themes</pre>
Ubuntu 16.04	Gnome Flashback (Metacity)	<pre># apt install gnome-session-flashback</pre>

3 要开始使用新的默认桌面环境，请重新启动桌面。

如果您在装有多个桌面环境的 Linux 桌面上启用了 SSO，请使用以下信息选择要在 SSO 会话中使用的桌面环境。

- 对于 Ubuntu 18.04/16.04 和 RHEL/CentOS 7.x，请使用 [表 1-7. SSODesktopType 选项](#) 中的信息设置 `/etc/vmware/viewagent-custom.conf` 文件中的 `SSODesktopType` 选项，以指定要用于 SSO 的桌面环境。

表 1-7. SSODesktopType 选项

桌面类型	SSODesktopType 选项设置
MATE	SSODesktopType=UseMATE
GnomeUbuntu	SSODesktopType=UseGnomeUbuntu
GnomeFlashback	SSODesktopType=UseGnomeFlashback
KDE	SSODesktopType=UseKdePlasma
GnomeClassic	SSODesktopType=UseGnomeClassic

- 对于 RHEL/CentOS 6.x 和 SLED 11 SP3/SP4，要让 SSO 登录会话使用 KDE，请从 `/usr/share/xsession` 目录中移除 KDE 启动文件以外的所有桌面启动文件。例如，可使用下面的一组命令。

```
# cd /usr/share/xsessions
# mkdir backup
# mv *.desktop backup
# mv backup/kde*.desktop ./
```

初始设置完成后，最终用户必须注销或重新引导其 Linux 桌面，才能使 KDE 成为下一个 SSO 会话中的默认桌面。

如果您在装有多个桌面环境的 Linux 桌面上禁用了 SSO，则无需执行前面所述的任何步骤。最终用户在登录该 Linux 桌面时，必须选择其所需的桌面环境。

网络要求

VMware Blast Extreme 支持用户数据报协议 (UDP) 和传输控制协议 (TCP)。网络状况会影响 UDP 和 TCP 的性能。为获得最佳用户体验，请根据网络条件选择 UDP 或 TCP。

- 如果网络条件良好（例如处于局域网 (LAN) 环境中），请选择 TCP。

- 如果网络条件较差（例如处于广域网 (WAN) 环境中，在该环境中可能会发生数据包丢失和时间延迟），请选择 UDP。

使用网络分析器工具（例如，Wireshark）来确定 VMware Blast Extreme 使用的是 TCP 还是 UDP。可使用下面的一组步骤（使用 Wireshark）作为参考示例。

- 1 在您的 Linux 虚拟机上下载并安装 Wireshark。

对于 RHEL/CentOS 6:

```
sudo yum install wireshark
```

对于 Ubuntu 18.04/16.04:

```
sudo apt install tshark
```

对于 SLED/SLES 11/12:

```
sudo zypper install wireshark
```

- 2 使用 VMware Horizon Client 连接到 Linux 桌面。
- 3 打开终端窗口并运行以下命令，此命令将显示 VMware Blast Extreme 使用的 TCP 软件包或 UDP 软件包。

```
sudo tshark -i any | grep 22443
```

USB 重定向和客户端驱动器重定向 (CDR) 功能容易受网络条件的影响。如果网络条件不佳（例如带宽受限，并且伴有时间延迟和数据包丢失），用户体验会变差。在此类条件下，最终用户可能会遇到以下情形。

- 复制远程文件的速度可能较慢。在这种情况下，请改为传输较小的文件。
- 远程 Linux 桌面中不显示 USB 设备。
- USB 数据无法完整传输。例如，在复制大型文件时，获得的文件可能小于原始文件。

用于 USB 重定向的 VHCI 驱动程序

USB 重定向功能依赖于 USB 虚拟主机控制器接口 (Virtual Host Controller Interface, VHCI) 内核驱动程序。您必须修补 VHCI 驱动程序才能支持 USB 3.0。

Horizon for Linux 安装程序中包含受支持 Linux 分发包的默认内核的 VHCI 驱动程序二进制文件。选择 USB 重定向功能后，安装程序会安装 VHCI 驱动程序。[表 1-8. 默认内核版本](#)中列出了 Horizon for Linux 安装程序安装的默认内核版本。

表 1-8. 默认内核版本

Linux 分发包	默认内核版本
RHEL/CentOS 6.9	2.6.32-696.el6.x86_64
RHEL/CentOS 6.10	2.6.32-754.el6.x86_64
RHEL/CentOS 7.5	3.10.0-862.el7.x86_64

Linux 分发包	默认内核版本
SUSE 12 SP2	4.4.21-69-default
Ubuntu 16.04	4.4.0-21-generic
Ubuntu 18.04	4.15.0-20-generic

如果 Linux 系统使用的内核版本与 Horizon for Linux 安装程序中包含的默认版本不同，必须从 <https://sourceforge.net/projects/usb-vhci/files/linux%20kernel%20module/> 下载 USB VHCI 源代码。然后，必须对 VHCI 驱动程序源代码进行编译，并在 Linux 系统上安装所生成的二进制文件。

注 VHCI 驱动程序的安装必须在安装 Horizon for Linux 之前完成。

下载最新版本的 USB VHCI 驱动程序源代码后，使用表 1-9. 编译并安装 USB VHCI 驱动程序中的命令对其进行编译，然后将其安装在您的 Linux 系统上。例如，如果在 /install_tmp/ 目录下解压缩安装文件 VMware-horizonagent-linux-x86_64-<version>-<build-number>.tar.gz，那么，*full-path_to_patch-file* 是 /install_tmp/VMware-horizonagent-linux-x86_64-<version>-<buildnumber>/resources/vhci/patch/vhci.patch，需要使用的 patch 命令是

```
# patch -p1 < /install_tmp/VMware-horizonagent-linux-x86_64-<version>-<build-number>/resources/vhci/patch/vhci.patch
```

表 1-9. 编译并安装 USB VHCI 驱动程序

Linux 分发包	编译并安装 USB VHCI 驱动程序的步骤
Ubuntu 18.04	<ol style="list-style-type: none"> 1 安装依赖项包。 <pre># apt-get install make # apt-get install gcc # apt-get install libelf-dev</pre> 2 编译并安装 VHCI 驱动程序。 <pre># tar -xzvf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < full-path_to_patch-file # make clean && make && make install</pre>
Ubuntu 16.04	编译并安装 VHCI 驱动程序。 <pre># tar -xzvf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < full-path_to_patch-file # make clean && make && make install</pre>

Linux 分发包	编译并安装 USB VHCI 驱动程序步骤
RHEL/CentOS 6.9/6.10	1 安装依赖项包。
RHEL/CentOS 7	<pre># yum install gcc-c++ # yum install kernel-devel-\$(uname -r) # yum install kernel-headers-\$(uname -r) # yum install patch</pre>
	2 编译并安装 VHCI 驱动程序。
	<pre># tar -xzvf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < full-path_to_patch-file # make clean && make && make install</pre>
SLED/SLES 11 SP4	1 确定当前内核软件包的版本
SLED/SLES 12 SP2	<pre># rpm -qa grep kernel-default-\$(echo \$(uname -r) cut -d '-' -f 1,2)</pre> <p>输出为当前安装的内核软件包的名称。例如，如果软件包名称为 <code>kernel-default-3.0.101-63.1</code>，那么，当前内核软件包的版本为 <code>3.0.101-63.1</code>。</p>
	2 安装依赖项包。
	<p>a 对于 SUSE 11，安装与当前内核相匹配的 <code>kernel-source</code> 和 <code>kernel-default-devel</code> 软件包，即 <code>gcc</code> 和 <code>patch</code> 软件包。</p> <pre># zypper install --oldpackage kernel-source-<kernel-package-version> \ kernel-default-devel-<kernel-package-version> gcc patch</pre> <p>例如：</p> <pre># zypper install --oldpackage kernel-source-3.0.101-63.1 kernel-default-devel-3.0.101-63.1 gcc patch</pre>
	<p>b 对于 SUSE 12，安装 <code>kernel-devel</code>、<code>kernel-default-devel</code>、<code>kernel-macros</code> 和 <code>patch</code> 软件包。</p> <pre># zypper install --oldpackage kernel-devel-<kernel-package-version> \ kernel-default-devel-<kernel-package-version> kernel-macros-<kernel-package-version> patch</pre> <p>例如：</p> <pre># zypper install --oldpackage kernel-devel-4.4.21-90.1 kernel-default-devel-4.4.21-90.1 kernel-macros-4.4.21-90.1 patch</pre>
	3 编译并安装 VHCI 驱动程序。
	<pre># tar -xzvf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < full-path_to_patch-file # mkdir -p linux/\$(echo \$(uname -r) cut -d '-' -f 1)/drivers/usb/core # cp /lib/modules/\$(uname -r)/source/include/linux/usb/hcd.h linux/\$(echo \$(uname -r) cut -d '-' -f 1)/drivers/usb/core # make clean && make && make install</pre>

如果您的 Linux 内核版本发生更改，您必须重新编译并重新安装 VHCI 驱动程序，但无需重新安装 Horizon for Linux。

您还可以使用与以下 Ubuntu 18.04/16.04 系统示例类似的步骤，为 VHCI 驱动程序添加动态内核模块支持 (Dynamic Kernel Module Support, DKMS)。

- 1 安装内核头文件。

```
# apt install linux-headers-`uname -r`
```

- 2 使用以下命令安装 dkms。

```
# apt install dkms
```

- 3 提取和修补 VHCI TAR 文件。

```
# tar xzvf vhci-hcd-1.15.tar.gz
# cd vhci-hcd-1.15
# patch -p1 <full-path-to-patch-file>
# cd ..
```

- 4 将提取的 VHCI 源文件复制到 /usr/src 目录。

```
# cp -r vhci-hcd-1.15 /usr/src/usb-vhci-hcd-1.15
```

- 5 创建一个名为 dkms.conf 的文件，并将其放在 /usr/src/usb-vhci-hcd-1.15 目录中。

```
# touch /usr/src/usb-vhci-hcd-1.15/dkms.conf
```

- 6 向 dkms.conf 文件添加以下内容。

```
PACKAGE_NAME="usb-vhci-hcd"
PACKAGE_VERSION=1.15
MAKE_CMD_TMPL="make KVERSION=$kernelver"

CLEAN="$MAKE_CMD_TMPL clean"

BUILT_MODULE_NAME[0]="usb-vhci-iocifc"
DEST_MODULE_LOCATION[0]="/kernel/drivers/usb/host"
MAKE[0]="$MAKE_CMD_TMPL"

BUILT_MODULE_NAME[1]="usb-vhci-hcd"
DEST_MODULE_LOCATION[1]="/kernel/drivers/usb/host"
MAKE[1]="$MAKE_CMD_TMPL"

AUTOINSTALL="YES"
```

- 7 在 dkms 中添加此 VHCI 驱动程序。

```
# dkms add usb-vhci-hcd/1.15
```

- 8 生成 VHCI 驱动程序。

```
# dkms build usb-vhci-hcd/1.15
```

9 安装 VHCI 驱动程序。

```
# dkms install usb-vhci-hcd/1.15
```

2D 和 vSGA 图形的虚拟机设置

在创建某些 Horizon 7 for Linux 虚拟机时，您必须将内存设置和配置参数更改为建议的最小值。

配置为使用 NVIDIA vDGA 的虚拟机使用 NVIDIA 物理显卡。配置为使用 NVIDIA GRID vGPU 的虚拟机使用 NVIDIA 虚拟显卡，它基于 NVIDIA 物理图形加速器。您不需要更改这些虚拟机的显存 (vRAM) 设置和配置参数。

配置为使用 2D 或 vSGA 图形的虚拟机使用 VMware 虚拟显卡，并且必须为这些类型的虚拟机更改以下设置：

- 显存 (vRAM) 设置
- 配置参数
- 3D 显存设置
- vCPU 和虚拟内存设置以满足性能要求

显存 (vRAM) 设置

在 vSphere Client 中创建 Linux 虚拟机时，请按照表 1-10. 2D 或 vSGA 图形的推荐 vRAM 设置 所示配置 vRAM 大小。针对您为虚拟机配置的显示器数量和分辨率设置建议的 vRAM 大小。

表 1-10. 2D 或 vSGA 图形的推荐 vRAM 设置

vRAM 大小	显示器数量	最大分辨率
10 MB	1	1600x1200 或 1680x1050
12 MB	1	1920x1440
32 MB	1	2560x1600
48 MB	2	2048x1536
80 MB	2	2560x1600
128 MB	3	2560x1600
128 MB	4	2048x1536

这些 vRAM 大小是最小的建议值。如果虚拟机上有更多资源可供使用，请将 vRAM 设置为更大的值以提高视频性能。

对于在最低分辨率下配置了单个显示器的虚拟机，10 MB 是建议的最低 vRAM 大小。

您必须关闭虚拟机电源以设置要使用的显示器数和显存量，如[创建虚拟机并安装 Linux](#)中所述。

与在 Windows 虚拟机上一样，Horizon 连接服务器 7 不会自动在 Linux 虚拟机上配置 vRAM 设置。您必须在 vSphere Client 中手动配置 vRAM 设置。

如果为 Linux 虚拟机配置的 vRAM 大小比建议值小，则可能会出现以下问题：

- 在最初建立连接后，可能会立即断开桌面会话。
- 自动适应可能无法正常工作。将在较小的屏幕区域中显示桌面。

如果 Linux 虚拟机的**显示器数量**值少于实际所需的数量，一个或多个显示器会显示空白桌面。

如果您在使用建议的设置时遇到自动适应问题，可以指定更大的 vRAM 大小。vSphere Client 允许的最大 vRAM 大小为 128 MB。如果指定的大小超过 128 MB，您必须手动修改 vmx 配置文件。以下示例指定的 vRAM 大小为 256 MB：

```
svga.vramSize = "268435456"
```

配置参数

要在多个显示器上显示 Linux 远程桌面，您必须为虚拟机设置某些配置参数。为虚拟机设置配置参数的一般步骤如下所示：

- 1 关闭虚拟机的电源，
- 2 在 vSphere Web Client 中，右键单击虚拟机，然后选择**编辑设置**。
- 3 单击**虚拟机选项**选项卡，然后单击**高级**。
- 4 单击**编辑配置**，然后单击**添加行**。
- 5 输入配置参数名称和值。
- 6 要保存更改，请单击**确定**。

您必须设置以下配置参数：

- 将 svga.autodetect 设置为 false。

```
svga.autodetect="false"
```

- 根据显示器数量和方向（水平或垂直）计算 svga.maxWidth 和 svga.maxHeight 值。一般而言，svga.maxWidth 和 svga.maxHeight 值必须足够大才能支持所有显示器。例如，要支持 4 个最大分辨率为 2560x1600 的显示器，您必须设置以下值：

```
svga.maxHeight="3200"
svga.maxWidth="10240"
```

如果具有多个显示器，您必须设置这些配置参数。否则，可能遇到以下一个或多个问题：

- 将在某些显示器上显示桌面，其他显示器为空白。
- 一个按键显示多次。
- 桌面速度变慢。
- 在较小的屏幕区域中显示桌面。

8192x8192 显示器的屏幕大小限制

对于 RHEL 6.8/6.9/6.10/7.3/7.4、CentOS 6.8/6.9/6.10/7.3/7.4、Ubuntu 16.04、SLED 12 SP2/SP3 和 SLES 12 SP2/SP3，2D 和 vSGA 的最大屏幕大小为 4096x4096。在运行 `xrandr` 命令时，输出的第一行包含 `maximum 4096x4096`。

对于 Ubuntu 18.04、RHEL 7.5 和 CentOS 7.5，2D 和 vSGA 的最大屏幕大小为 8192x8192。

多显示器连接可能需要大于 4096x4096 的屏幕大小。要绕过此限制，可使用以下解决方案之一：

- 如果您必须为虚拟机使用 VMware 硬件版本 11 (HWv11) 或更高版本，请将以下行添加到虚拟机的 VMX 配置文件中：

```
mks.enable3d = TRUE
```

通过此解决方案，Linux 操作系统可将 3D 功能报告给软件应用程序，例如 Chrome。但是，这样做可能会影响 Linux 系统的性能。

- 如果您的虚拟机可以使用 VMware 硬件版本 10，请在虚拟机的 VMX 文件中使用以下行：

```
virtualHW.version = "10"
```

此解决方案不适用于 RHEL 6.8 和 CentOS 6.8。

要使此解决方案在 Ubuntu 16.04 系统上适用，您必须安装来自官方 Ubuntu 存储库的最新修补程序。

vCPU 和内存设置

要提高 2D 或 vSGA 桌面的性能，请为 Linux 虚拟机设置更多 vCPU 和虚拟内存。例如，设置 2 个 vCPU 和 2 GB 虚拟内存。

对于多个显示器（如 4 个显示器）的较大屏幕，请为虚拟机设置 4 个 vCPU 和 4 GB 虚拟内存。

要在 2D 或 vSGA 桌面中播放视频，请为虚拟机设置 4 个 vCPU 和 4 GB 虚拟内存。

3D 显存设置

要在 vSGA 多显示器环境中提高性能，请将虚拟机的 3D 显存设置设为 1 GB 或更大。

在 Linux 桌面上配置会话协作

通过使用会话协作功能，用户可以邀请其他用户加入现有的 Linux 远程桌面会话。

会话协作的系统要求

要支持会话协作功能，您的 Horizon 部署必须满足特定要求。

表 1-11. 会话协作的系统要求

组件	要求
客户端系统	会话所有者和协作者必须已在客户端系统上安装了适用于 Windows、Mac 或 Linux 的 Horizon Client 4.10 或更高版本，否则，必须使用 HTML Access 4.10 或更高版本。
Linux 远程桌面	必须在 Linux 虚拟桌面中安装 Horizon Agent 7.7 或更高版本。必须在桌面池及 VDI 级别启用会话协作功能。
连接服务器	连接服务器实例使用企业许可证。
显示协议	VMware Blast

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

在配置文件中设置会话协作选项

在 `/etc/vmware/viewagent-custom.conf` 文件中设置以下选项，以启用或禁用会话协作功能。

■ CollaborationEnable

在 `/etc/vmware/config` 文件中设置以下选项，以配置要在协作会话期间使用的设置。

- `collaboration.logLevel`
- `collaboration.maxCollabors`
- `collaboration.enableEmail`
- `collaboration.serverUrl`
- `collaboration.enableControlPassing`

请参阅[在 Linux 桌面上的配置文件中设置选项](#)了解更多信息。

会话协作功能的限制

用户无法在协作会话中使用以下远程桌面功能。

- USB 重定向
- 音频输入重定向
- 客户端驱动器重定向
- 智能卡重定向
- 剪贴板重定向

用户无法在协作会话中更改远程桌面分辨率。

用户不能在同一台客户端计算机上进行多个协作会话。

为桌面部署准备 Linux 虚拟机

设置 Linux 桌面需要创建 Linux 虚拟机，并准备操作系统以进行远程桌面部署。

本章讨论了以下主题：

- 创建虚拟机并安装 Linux
- 为远程桌面部署准备 Linux 计算机
- 安装 Horizon Agent 的依赖项包

创建虚拟机并安装 Linux

您可以在 vCenter Server 中为在 Horizon 7 中部署的每个远程桌面创建新虚拟机。您必须在虚拟机上安装 Linux 分发包。

前提条件

- 确认您的部署满足支持 Linux 桌面的相关要求。请参阅 [Horizon 7 for Linux 的系统要求](#)。
- 熟悉有关在 vCenter Server 中创建虚拟机和安装客户机操作系统的步骤。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“创建和准备虚拟机”。
- 熟悉打算用于虚拟机的显示器的显存 (vRAM) 设置要求。请参阅 [Horizon 7 for Linux 的系统要求](#)。

步骤

1 在 vSphere Web Client 或 vSphere Client 中，创建新虚拟机。

2 配置自定义配置选项。

- a 右键单击虚拟机，然后单击**编辑设置**。
- b 指定 vCPU 数量和显存大小。

有关所需的设置，请遵循 Linux 分发包安装指南中的准则。

例如，Ubuntu 18.04 指定配置 2048 MB 显存和 2 个 vCPU。

- c 选择**视频卡**并指定显示器数量和显存 (vRAM) 总大小。

对于使用 2D 或 vSGA 的虚拟机（使用 VMware 驱动程序），请在 vSphere Web Client 中设置 vRAM 大小。vRAM 的大小对 vDGA 或 NVIDIA GRID vGPU 计算机（使用 NVIDIA 驱动程序）没有影响。

有关所需的设置，请遵循 [Horizon 7 for Linux 的系统要求](#)中的准则。请勿使用显存计算器。

- 3 打开虚拟机的电源并安装 Linux 分发版。
- 4 配置要用于特定 Linux 分发版的桌面环境。

请参阅 [Horizon 7 for Linux 的系统要求](#) 中的“桌面环境”部分，以了解更多信息。

- 5 确保系统主机名可解析为 127.0.0.1。

为远程桌面部署准备 Linux 计算机

要准备 Linux 计算机以使其在 Horizon 7 部署中用作桌面，您必须执行特定的任务。

Linux 计算机必须可以与连接服务器通信，然后 Horizon 7 才可以管理此计算机。您必须在 Linux 计算机上配置网络，以便 Linux 计算机可以使用其完全限定域名 (FQDN) 对连接服务器实例执行 ping 操作。

Open VMware Tools (OVT) 预安装在 RHEL 7、CentOS 7、SLED 12 和 SLES 12 计算机上。如果准备其中任何一种计算机以用作远程桌面，您可以在以下过程中跳过步骤 1 至 5，该过程介绍了如何通过手动运行安装程序来安装 VMware Tools。

如果使用 Ubuntu 16.04/18.04 计算机，请在该计算机上安装 OVT。如果准备该计算机以用作远程桌面，您可以跳过以下过程中的步骤 1 至 5，然后使用以下命令在 Ubuntu 16.04/18.04 计算机上手动安装 OVT：

```
apt-get install open-vm-tools-desktop
```

前提条件

- 确认已在 vCenter Server 中创建了新虚拟机 (VM)，并且已在虚拟机上安装了您的 Linux 分发版
- 熟悉有关在 Linux 虚拟机上挂载和安装 VMware Tools 的步骤。请参阅《vSphere 虚拟机管理》文档中的“在 Linux 虚拟机中手动安装或升级 VMware Tools”。
- 熟悉有关将 Linux 虚拟机配置为可通过 DNS 解析的步骤。这些步骤因不同的 Linux 分发版和版本而异。有关说明，请参考您的 Linux 分发版和版本的文档。

步骤

- 1 在 vSphere Web Client 或 vSphere Client 中，将 VMware Tools 虚拟磁盘挂载到虚拟机上。
- 2 右键单击 VMware Tools 安装程序文件 VMwareTools.x.x.x-xxxx.tar.gz，单击**提取到**，然后为您的 Linux 分发版选择桌面。

vmware-tools-distrib 文件夹将提取到桌面。

- 3 在虚拟机上，以 root 用户身份登录，然后打开终端窗口。
- 4 解压缩 VMware Tools tar 安装程序文件。

例如：

```
tar xzpf /mnt/cdrom/VMwareTools-x.x.x-yyyy.tar.gz
```

5 运行安装程序并配置 VMware Tools。

该命令在不同的 Linux 分发版中可能略有不同。例如：

```
cd vmware-tools-distrib
sudo ./vmware-install.pl -d
```

通常情况下，安装程序文件运行完毕后会运行 `vmware-config-tools.pl` 配置文件。

6 在 `/etc/hosts` 文件中，将 Linux 计算机的主机名映射到 127.0.0.1。

对于 RHEL、CentOS、SLES 和 SLED，您必须手动将主机名映射到 127.0.0.1，因为不会自动映射主机名。对于 Ubuntu，不需要执行该步骤，因为默认映射主机名。在批量部署桌面时也不必执行此步骤，因为克隆过程中会添加此映射。

注 如果在安装 Horizon Agent 后更改 Linux 计算机的主机名，您必须在 `/etc/hosts` 文件中将新主机名映射到 127.0.0.1。否则，将继续使用旧主机名。

7 对于 RHEL 7 和 CentOS 7，确认已禁用 `virbr0`。

```
virsh net-destroy default
virsh net-undefine default
service libvirtd restart
```

8 确保容器中的 Horizon Connection Server 实例可以通过 DNS 解析。

9 配置 Linux 计算机，以使默认运行级别为 5。

运行级别必须为 5，Linux 桌面才能正常工作。

10 在配置为使用 OpenLDAP 服务器进行身份验证的 Ubuntu 计算机上，在计算机上设置完全限定域名。

该步骤确保可以在 Horizon Administrator 的“会话”页上的“用户”字段中正确显示该信息。按如下方式编辑 `/etc/hosts` 文件：

- a # nano `/etc/hosts`
- b 添加完全限定域名。例如：127.0.0.1 hostname.domainname hostname。
- c 退出并保存该文件。

11 对于 SUSE，禁用“通过 DHCP 更改主机名”。设置主机名或域名。

- a 在“Yast”中，单击**网络设置**。
- b 单击**主机名/DNS**选项卡。
- c 取消选择**通过 DHCP 更改主机名**。
- d 输入主机名和域名。
- e 单击**确定**。

在安装 VMware Tools 之后，如果您升级 Linux 内核，则 VMware Tools 可能会停止运行。要解决此问题，请参阅 <http://kb.vmware.com/kb/2050592>。

安装 Horizon Agent 的依赖项包

Horizon Agent for Linux 具有一些 Linux 分发包特有的依赖项包。在安装 Horizon Agent for Linux 之前，必须先安装这些依赖项包。

前提条件

确认已在 vCenter Server 中创建新虚拟机 (Virtual Machine, VM)，并且已在该虚拟机上安装 Linux 分发包。

步骤

1 安装默认情况下未安装或升级的必需依赖项包。如果任何包都不满足要求，安装程序会中断安装。

表 2-1. 必需依赖项包

Linux 分发包	依赖项包
RHEL 7.5	<code>yum install libappindicator-gtk3</code>
SLED 11 SP3/SP4 将 <code>xorg-x11-server</code> 升级到高于 7.4.27.111.1 的版本。	<code>zypper update xorg-x11-server</code>
SLES 12 SP1/SLED 12 SP1 从 SUSE 存储库中将 <code>xf86-video-vmware</code> 升级到高于 13.0.2-3.2 的版本。	<ol style="list-style-type: none"> 注册 SUSE 12 以启用 SUSE 存储库。 <code>SUSEConnect -r 注册代码 -e 电子邮件</code> 更新 <code>xf86-video-vmware</code> 版本。 <code>zypper update xf86-video-vmware</code>
SLES 12	<p>安装 Horizon Agent 时，需要为 SLES 12 Linux 桌面安装 <code>python-gobject2</code>。</p> <ol style="list-style-type: none"> 注册 SUSE 12 以启用 SUSE 存储库。 <code>SUSEConnect -r 注册代码 -e 电子邮件</code> 安装 <code>python-gobject2</code>。 <code>zypper install python-gobject2</code>
Ubuntu 16.04	<code>apt-get install python-dbus python-gobject</code>
Ubuntu 18.04	<code>apt-get install python python-dbus python-gobject</code>

2 安装 Horizon Agent 的可选软件包。

- 默认情况下，RHEL 或 CentOS 6.7 安装了 `glibc-2.12-1.166.el6.x86_64`，这可能会导致死锁问题。其结果是，桌面连接将停止。要解决该问题，您必须从联机存储库中将 `glibc` 升级到最新版本。

```
sudo yum install glibc
```

为 Linux 桌面设置 Active Directory 集成

3

Horizon 7 使用现有的 Microsoft Active Directory (AD) 基础架构来进行用户身份验证和管理。您可以将 Linux 桌面与 Active Directory 集成，以便用户可以使用其 Active Directory 用户帐户登录到 Linux 桌面。

注 Horizon Agent 要求 Linux 桌面和客户端用户位于同一个 Active Directory 域中。如果桌面和用户位于不同的域中，Horizon Agent 可能会将桌面域错误地识别为用户域。

本章讨论了以下主题：

- 将 Linux 与 Active Directory 集成
- 设置单点登录
- 设置智能卡重定向
- 为 Linux 桌面设置 True SSO

将 Linux 与 Active Directory 集成

有多种解决方案可将 Linux 与 Microsoft Active Directory (AD) 集成，并且 Horizon 7 for Linux 桌面不依赖于所使用的解决方案。

已知以下解决方案可用于 Horizon 7 for Linux 桌面环境。

- OpenLDAP 服务器直通身份验证
- 针对 Microsoft Active Directory 的系统安全服务守护进程 (System Security Services Daemon, SSSD) LDAP 身份验证
- 加入 Winbind 域
- PowerBroker Identity Services Open (PBISO) 身份验证
- Samba 脱机域加入

如果使用基于 LDAP 的解决方案，必须在模板虚拟机中进行相应配置，但不需要在克隆的虚拟机中执行任何其他步骤。

注 为方便部署，可使用针对 Microsoft Active Directory 进行 SSSD LDAP 身份验证的解决方案。

使用 OpenLDAP 服务器直通身份验证

您可以设置 OpenLDAP 服务器并使用直通身份验证 (Pass-Through Authentication, PTA) 机制来针对 Active Directory 验证用户凭据。

OpenLDAP 直通身份验证解决方案主要包含以下步骤。

步骤

- 1 要启用 LDAPS（基于 SSL 的轻量级目录访问协议），需在 Active Directory 上安装证书服务。
- 2 设置 OpenLDAP 服务器。
- 3 从 Active Directory 向 OpenLDAP 服务器同步用户信息（密码除外）。
- 4 配置 OpenLDAP 服务器以将密码验证委派给一个单独的进程（例如 `saslauthd`），此进程可以对 Active Directory 执行密码验证。
- 5 将 Linux 桌面配置为使用 LDAP 客户端在 OpenLDAP 服务器上对用户进行身份验证。

设置针对 Microsoft Active Directory 的 SSSD LDAP 身份验证

通过在 Linux 桌面中配置系统安全服务守护进程 (SSSD)，您可以对 Windows Active Directory 使用 LDAP 身份验证。

使用以下简要步骤可设置 SSSD LDAP 身份验证解决方案。

步骤

- 1 要启用 LDAPS（基于安全套接字层的轻量级目录访问协议），需在 Active Directory 服务器上安装证书服务。
- 2 要直接对 Microsoft Active Directory 使用 LDAP 身份验证，需在 Linux 桌面中配置 SSSD。

使用加入 Windbind 域解决方案

加入 Windbind 域解决方案是基于 Kerberos 的身份验证解决方案，是对 Active Directory 进行身份验证的另一种方法。

使用以下简要步骤可设置加入 Windbind 域解决方案。

步骤

- 1 在 Linux 桌面上安装 `winbind`、`samba` 和 Kerberos 软件包。
- 2 将 Linux 桌面加入 Microsoft Active Directory。

后续步骤

如果使用加入 Winbind 域解决方案或其他基于 Kerberos 身份验证的解决方案，请将模板虚拟机加入 Active Directory，并将克隆的虚拟机重新加入到 Active Directory。例如，使用以下命令：

```
sudo /usr/bin/net ads join -U <domain_user>%<domain_password>
```

对于 Winbind 解决方案，可以使用以下方法在克隆的虚拟机上运行域重新加入命令：

- 通过 SSH 或 vSphere PowerCLI 等方式远程连接到每个虚拟机并运行该命令。有关脚本的更多信息，请参阅第 8 章 [为手动桌面池批量部署 Horizon 7](#)。
- 将该命令包含到 shell 脚本中，并设置 `/etc/vmware/viewagent-custom.conf` 文件中 Horizon Agent RunOnceScript 选项的脚本路径。有关更多信息，请参阅在 [Linux 桌面上的配置文件中设置选项](#)。

配置 PowerBroker Identity Services Open (PBISO) 身份验证

PowerBroker Identity Services Open (PBISO) 身份验证方法是支持执行脱机域加入的解决方案之一。

执行以下步骤可使用 PBISO 将 Linux 桌面加入到 Active Directory。

步骤

- 1 从 <https://www.beyondtrust.com/products/powerbroker-identity-services-open/> 下载 PBISO 8.5.6 或更高版本。
- 2 在 Linux 虚拟机上安装 PBISO。

```
sudo ./pbis-open-8.5.6.2029.linux.x86_64.deb.sh
```

- 3 安装 Horizon 7 Agent for Linux。
- 4 使用 PBISO 将 Linux 桌面加入 AD 域。

在以下示例中，**lxdc.vdi** 是域名，**administrator** 是域用户名。

```
sudo domainjoin-cli join lxdc.vdi administrator
```

- 5 为域用户设置默认配置。

```
sudo /opt/pbis/bin/config UserDomainPrefix lxdc
sudo /opt/pbis/bin/config AssumeDefaultDomain true
sudo /opt/pbis/bin/config LoginShellTemplate /bin/bash
sudo /opt/pbis/bin/config HomeDirTemplate %H/%U
```

- 6 编辑 `/etc/pamd.d/common-session` 文件。
 - a 找到内容为 **session sufficient pam_lsass.so** 的行。
 - b 将这一行替换为 **session [success=ok default=ignore] pam_lsass.so**。

注 重新安装或更新 Horizon Agent for Linux 后，必须重复此步骤。

- 对于 Ubuntu 16.04，将以下行附加到 `/usr/share/lightdm/lightdm.conf.d/50-unity-greeter.conf` 配置文件。

```
allow-guest=false
greeter-show-manual-login=true
```

注 如果您使用的是 Ubuntu 18.04，则不需要更改 `lightdm` 配置文件。

- 重新引导系统，然后登录。

后续步骤

注

- 如果将 `/opt/pbis/bin/config AssumeDefaultDomain` 选项设置为 **false**，必须更新 `/etc/vmware/viewagent-custom.conf` 文件中的 `SSOUserFormat=<username>@<domain>` 设置。
- 使用 Horizon 即时克隆浮动桌面池功能时，为避免在向克隆虚拟机添加新网络适配器时丢失 DNS 服务器设置，需修改 Linux 系统的 `resolv.conf` 文件。对于 Ubuntu 16.04 系统，在向 `/etc/resolvconf/resolv.conf.d/head` 文件添加必要的行时，可将以下示例作为指南。

```
nameserver 10.10.10.10
search mydomain.org
```

为 Ubuntu 桌面配置 Samba 脱机域加入

要在 Horizon 7 Linux 桌面环境中的即时克隆虚拟机上支持 SSO，请在 Ubuntu 系统中的主 Linux 虚拟机上配置 Samba。

在 Ubuntu 系统上执行以下步骤可使用 Samba 对即时克隆 Linux 桌面执行脱机域加入，以将其加入到 Active Directory。

步骤

- 在主 Linux 虚拟机上，安装 `winbind` 和 `samba` 软件包，包括其他任何依赖的库，如 `smbfs` 和 `smbclient`。
- 使用以下命令安装 Samba `tdb-tools` 软件包。

```
sudo apt-get install tdb-tools
```

- 安装 Horizon 7 Agent for Linux。
- 对 `/etc/samba/smb.conf` 配置文件进行编辑，使其具有类似于以下示例的内容。

```
[global]
security = ads
realm = LAB.EXAMPLE.COM
workgroup = LAB
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
```

```
winbind enum group = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
```

- 5 对 `/etc/krb5.conf` 配置文件进行编辑，使其具有类似于以下示例的内容。

```
[libdefaults]
default_realm = EXAMPLE.COM

krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms

kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true

[realms]
YOUR-DOMAIN = {
kdc = 10.111.222.33
}

[domain_realm]
your-domain = EXAMPLE.COM
.your-domain = EXAMPLE.COM
```

- 6 按照下例所示编辑 `/etc/nsswitch.conf` 配置文件。

```
passwd: files winbind
group: files winbind
shadow: files winbind
gshadow: files
```

- 7 确认主机名正确无误，且系统日期和时间已与 DNS 系统同步。
- 8 在 `/etc/vmware/viewagent-custom.conf` 文件中设置以下选项，告知 Horizon Agent for Linux 已使用 Samba 方法对 Linux 虚拟机执行域加入。

```
OfflineJoinDomain=samba
```

- 9 重新引导系统，然后重新登录。

设置单点登录

要设置单点登录 (SSO)，您必须执行一些配置步骤。

Horizon 单点登录模块会与 Linux 中的 PAM（可插入身份验证模块）通信，这不取决于您将 Linux 与 Active Directory (AD) 集成所使用的方法。Horizon SSO 可以用于 OpenLDAP 及 Winbind 这两种将 Linux 与 AD 集成的解决方案。

默认情况下，SSO 假定 AD 的 sAMAccountName 属性是登录 ID。如果使用 OpenLDAP 或 Winbind 解决方案，您必须执行以下配置步骤以确保 SSO 使用正确的登录 ID：

- 对于 OpenLDAP，将 sAMAccountName 设置为 uid。
- 对于 Winbind，将以下语句添加到配置文件 `/etc/samba/smb.conf`。

```
winbind use default domain = true
```

如果用户必须指定登录的域名，您必须在 Linux 桌面上设置 SSUserFormat 选项。有关更多信息，请参阅[在 Linux 桌面上的配置文件中设置选项](#)。SSO 始终使用大写的短域名。例如，如果域是 mydomain.com，SSO 将使用 MYDOMAIN 作为域名。因此，在设置 SSUserFormat 选项时必须指定 MYDOMAIN。关于短域名和长域名，请遵循以下规则：

- 对于 OpenLDAP，您必须使用大写的短域名。
- Winbind 同时支持长短两种域名。

AD 支持在登录名称中使用特殊字符，而 Linux 则不支持。因此，在设置 SSO 时，请不要在登录名称中使用特殊字符。

在 AD 中，如果用户的 UserPrincipalName (UPN) 属性和 sAMAccount 属性不匹配，而用户使用 UPN 登录，则 SSO 将失败。例如，如果您在 AD mycompany.com 中有一个用户 juser，但该用户的 UPN 设置为 juser123@mycompany.com 而不是 juser@mycompany.com，则 SSO 将失败。解决办法是，用户使用 sAMAccount 中存储的名称登录。例如，juser。

Horizon 7 不要求用户名区分大小写。您必须确保 Linux 操作系统可以处理不区分大小写的用户名。

- 对于 Winbind，用户名默认不区分大小写。
- 对于 OpenLDAP，Ubuntu 使用 NSCD 对用户进行身份验证，并且默认不区分大小写。RHEL 和 CentOS 使用 SSSD 对用户进行身份验证，并且默认区分大小写。要更改该设置，请编辑文件 `/etc/sss/sss.conf`，并在 `[domain/default]` 部分添加以下行：

```
case_sensitive = false
```

如果您的 Linux 桌面中安装了多个桌面环境，请参阅[桌面环境](#)来选择要用于 SSO 的桌面环境。

设置智能卡重定向

要设置智能卡重定向，您必须执行一些配置步骤。

智能卡重定向概述

在运行以下 Linux 分发包且安装了指定版本的 Horizon Agent 的桌面上，支持智能卡重定向。

表 3-1. 智能卡重定向的系统要求

Linux 分发包	Horizon Agent
RHEL 7.1 或更高版本	Horizon Agent 7.8 或更高版本
RHEL 6.6 或更高版本	Horizon Agent 6.2.1 或更高版本
Ubuntu 18.04/16.04	Horizon Agent 7.9 或更高版本
SLED/SLES 12.x SP3	Horizon Agent 7.9 或更高版本
SLED 11.x SP4	Horizon Agent 7.9 或更高版本

在安装 Horizon Agent 时，您必须先禁用 SELinux。您还必须专门选择智能卡重定向组件，因为该组件默认未被选中。有关更多信息，请参阅 [install_viewagent.sh 命令行选项](#)。

如果在虚拟机上启用了智能卡重定向功能，vSphere Client 的 USB 重定向无法使用智能卡。

智能卡重定向仅支持一个智能卡读卡器。如果两个或更多读卡器连接客户端设备，该功能将无法正常使用。

智能卡重定向只支持卡上的一个证书。如果卡上有多个证书，将使用第一个插槽中的证书，其他证书将被忽略。此行为是 Linux 的一个限制。

注 智能卡重定向在 Linux 桌面上支持 PIV 卡。在使用适用于 Linux 的 Horizon Client 通过 PIV 卡对代理进行身份验证时，您必须为 PIV 智能卡配置 TLSv1.2 支持以避免出现 SSL 错误。请使用 VMware 知识库文章 <http://kb.vmware.com/kb/2150470> 中所述的解决方案。

注 在 Horizon 7 版本 7.0.1 或更高版本中，智能卡 SSO 处于启用状态。RHEL 6 桌面支持智能卡 SSO，但 RHEL 7 桌面不支持该功能。

配置智能卡重定向

要配置智能卡重定向，请执行以下任务。

- 1 按照 Linux 分销商和智能卡供应商的说明为桌面设置智能卡。
- 2 将桌面与 Active Directory 集成，如将 [RHEL 桌面与 Active Directory 集成以进行智能卡重定向](#) 中所述。
- 3 完成设置智能卡重定向的过程，如为 [RHEL 桌面设置智能卡重定向](#) 中所述。

将 RHEL 桌面与 Active Directory 集成以进行智能卡重定向

要在 RHEL 桌面上支持智能卡重定向，请使用 Samba 和 Winbind 解决方案将桌面与 Active Directory (AD) 域集成在一起。

可以使用以下过程将 RHEL 桌面与 AD 域集成以进行智能卡重定向。

该过程中的一些示例使用占位符值以表示网络配置中的实体，例如，AD 域的 DNS 名称。请将占位符值替换为您的配置特定的信息，如下表中所述。

占位符值	描述
dns_IP_ADDRESS	DNS 名称服务器的 IP 地址
mydomain.com	AD 域的 DNS 名称
MYDOMAIN.COM	AD 域的 DNS 名称，全部为大写字母
MYDOMAIN	包含 Samba 服务器的工作组或 NT 域的 DNS 名称，全部为大写字母
ads-hostname	AD 服务器的主机名

注 在运行 RHEL 6 或更高版本或者 RHEL 7.1 或更高版本的桌面上支持智能卡重定向。

步骤

- 1 在 RHEL 桌面上，安装所需的软件包。

```
# yum install nscd samba-winbind krb5-workstation pam_krb5 samba-winbind-clients authconfig-gtk
```

- 2 编辑系统连接的网络设置。打开 NetworkManager 控制面板，然后导航到系统连接的 **IPv4 Settings (IPv4 设置)**。对于 IPv4 Method (IPv4 方法)，请选择 **Automatic (DHCP) (自动 (DHCP))**。在 DNS 文本框中，输入 DNS 名称服务器的 IP 地址。然后，单击 **Apply (应用)**。

- 3 运行以下命令，并确认它返回 RHEL 桌面的完全限定域名 (Fully Qualified Domain Name, FQDN)。

```
# hostname -f
```

- 4 编辑 /etc/resolv.conf 配置文件，如以下示例中所示。

```
search mydomain.com
nameserver dns_IP_ADDRESS
```

- 5 在 RHEL 桌面上禁用安全增强 Linux (SELinux)。编辑 /etc/selinux/config 配置文件，如以下示例中所示。

```
SELINUX=disabled
```

- 6 编辑 /etc/krb5.conf 配置文件，如以下示例中所示。

```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
```

```

renew_lifetime = 7d
forwardable = true
rdns = false
default_realm = MYDOMAIN.COM
default_ccache_name = KEYRING:persistent:%{uid}

[realms]
  MYDOMAIN.COM = {
    kdc = ads-hostname
    admin_server = ads-hostname
    default_domain = ads-hostname
  }

[domain_realm]
  .mydomain.com = MYDOMAIN.COM
  mydomain.com = MYDOMAIN.COM

```

- 7 编辑 `/etc/samba/smb.conf` 配置文件，如以下示例中所示。

```

[global]
  workgroup = MYDOMAIN
  password server = ads-hostname
  realm = MYDOMAIN.COM
  security = ads
  idmap config * : range = 16777216-33554431
  template homedir = /home/MYDOMAIN/%U
  template shell = /bin/bash
  kerberos method = secrets and keytab
  winbind use default domain = true
  winbind offline logon = false
  winbind refresh tickets = true

  passdb backend = tdbsam

```

- 8 打开 `authconfig-gtk` 工具并配置设置，如下所示。

- a 选择 **Identity & Authentication (身份和身份验证)** 选项卡。对于 User Account Database (用户帐户数据库)，请选择 **Winbind**。
- b 选择 **Advanced Options (高级选项)** 选项卡，然后选中 **Create home directories on the first login (在首次登录时创建主目录)** 复选框。
- c 选择 **Identity & Authentication (身份和身份验证)** 选项卡，然后单击 **Join Domain (加入域)**。在显示警报以要求您保存更改时，请单击 **Save (保存)**。
- d 在出现提示时，输入域管理员的用户名和密码，然后单击 **OK (确定)**。

您的 RHEL 桌面将加入 AD 域。

- 9 在 PAM Winbind 上设置票证缓存。编辑 `/etc/security/pam_winbind.conf` 配置文件，以使其包含以下示例中显示的行。

```

[global]

# authenticate using kerberos

```

```
;krb5_auth = yes

# create homedirectory on the fly
;mkhomedir = yes
```

10 重新启动 Winbind 服务。

```
# sudo service winbind restart
```

11 要验证 AD 加入，请运行以下命令并检查是否返回正确的输出。

- net ads testjoin
- net ads info

12 重新引导系统，然后重新登录。

后续步骤

为 [RHEL 桌面设置智能卡重定向](#)

将 Ubuntu 桌面与 Active Directory 集成以进行智能卡重定向

要在 Ubuntu 桌面上支持智能卡重定向，需使用 Samba 和 Winbind 解决方案将桌面与 Active Directory (AD) 域集成在一起。

可以使用以下过程将 Ubuntu 桌面与 AD 域集成以进行智能卡重定向。

该过程中的一些示例使用占位符值以表示网络配置中的实体，例如，AD 域的 DNS 名称。请将占位符值替换为您的配置特定的信息，如下表中所述。

占位符值	描述
dns_IP_ADDRESS	DNS 名称服务器的 IP 地址
mydomain.com	AD 域的 DNS 名称
MYDOMAIN.COM	AD 域的 DNS 名称，全部为大写字母
MYDOMAIN	包含 Samba 服务器的工作组或 NT 域的 DNS 名称，全部为大写字母
ads-hostname	AD 服务器的主机名
ads-hostname.mydomain.com	AD 服务器的完全限定域名 (FQDN)
mytimeserver.mycompany.com	NTP 时间服务器的 DNS 名称
AdminUser	Linux 桌面管理员的用户名

步骤

1 在 Ubuntu 桌面上，通过编辑 `/etc/hostname` 配置文件来定义桌面的主机名。

2 配置 DNS。

- a 将 DNS 服务器名称和 IP 地址添加到 `/etc/hosts` 配置文件中。
- b 将 DNS 名称服务器的 IP 地址和 AD 域的 DNS 名称添加到 `/etc/network/interfaces` 配置文件中，如以下示例中所示。

```
dns-nameservers dns_IP_ADDRESS
dns-search mydomain.com
```

3 安装 resolvconf 软件包。

- a 运行安装命令。

```
# apt-get install -y resolvconf
```

允许系统安装该软件包并重新引导。

- b 验证 `/etc/resolv.conf` 文件中的 DNS 配置，如以下示例中所示。

```
# cat /etc/resolv.conf
...
nameserver dns_IP_ADDRESS
search mydomain.com
```

4 配置网络时间同步。

- a 安装 ntpdate 软件包。

```
# apt-get install -y ntpdate
```

- b 将 NTP 服务器信息添加到 `/etc/systemd/timesyncd.conf` 配置文件中，如以下示例中所示。

```
[Time]
NTP=mytimeserver.mycompany.com
```

5 重新启动 NTP 服务。

```
sudo service ntpdate restart
```

6 安装所需的 AD 加入软件包。

- a 运行安装命令。

```
# apt-get install -y samba krb5-config krb5-user winbind libpam-winbind
libnss-winbind
```

- b 在出现要求输入默认 Kerberos 领域的安装提示时，以大写字母形式输入您的 AD 域的 DNS 名称（例如，MYDOMAIN.COM）。然后，选择**确定**。

7 编辑 `/etc/krb5.conf` 配置文件，如以下示例中所示。

```
[libdefaults]
    dns_lookup_realm = false
```



```

ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
default_realm = MYDOMAIN.COM
default_ccache_name = KEYRING:persistent:%{uid}

[realms]
  MYDOMAIN.COM = {
    kdc = ads-hostname.mydomain.com
    admin_server = ads-hostname.mydomain.com
    default_domain = ads-hostname.mydomain.com
    pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
    pkinit_cert_match = <KU>digitalSignature
    pkinit_kdc_hostname = ads-hostname.mydomain.com
  }

[domain_realm]
  .mydomain.com = MYDOMAIN.COM
  mydomain.com = MYDOMAIN.COM

```

- 8 要验证 Kerberos 认证，请运行以下命令。

```

# kinit Administrator@MYDOMAIN.COM

# klist

```

确认命令返回的输出与以下示例类似。

```

Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@MYDOMAIN.COM
principal
2019-05-27T17:12:03    2019-05-28T03:12:03    krbtgt/MYDOMAIN.COM@MYDOMAIN.COM
renew until 2019-05-28T17:12:03

```

- 9 编辑 /etc/samba/smb.conf 配置文件，如以下示例中所示。

```

[global]
  workgroup = MYDOMAIN
  realm = MYDOMAIN.COM
  password server = ads-hostname.mydomain.com
  security = ads
  kerberos method = secrets only
  winbind use default domain = true
  winbind offline logon = false
  template homedir = /home/%D/%U
  template shell = /bin/bash
  client use spnego = yes
  client ntlmv2 auth = yes
  encrypt passwords = yes
  passdb backend = tdbsam

```

```
winbind enum users = yes
winbind enum groups = yes
idmap uid = 10000-20000
idmap gid = 10000-20000
```

10 加入 AD 域，然后检查集成。

a 运行 AD 加入命令。

```
# net ads join -U AdminUser@mydomain.com
# systemctl stop samba-ad-dc
# systemctl enable smbd nmbd winbind
# systemctl restart smbd nmbd winbind
```

b 修改 /etc/nsswitch.conf 配置文件，如以下示例中所示。

```
passwd:    compat systemd winbind
group:     compat systemd winbind
shadow:    compat
gshadow:   files
```

c 要检查 AD 加入结果，请运行以下命令并验证是否返回正确的输出。

```
# wbinfo -u

# wbinfo -g
```

d 要检查 Winbind 名称服务切换，请运行以下命令并验证是否返回正确的输出。

```
# getent group|grep 'domain admins'

# getent passwd|grep 'ads-hostname'
```

11 启用所有 PAM 配置文件。

```
# pam-auth-update
```

在“PAM 配置”屏幕中，选择所有 PAM 配置文件，包括在登录时创建主目录，然后选择确定。

12 在 Ubuntu 16.04 上，在登录屏幕中启用用户切换。修改 /usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf 文件，如以下示例中所示。

```
user-session=ubuntu
greeter-show-manual-login=true
```

后续步骤

为 [Ubuntu 桌面设置智能卡重定向](#)

将 SLED/SLES 桌面与 Active Directory 集成以进行智能卡重定向

要在 SLED/SLES 桌面上支持智能卡重定向，需使用 Samba 和 Winbind 解决方案将桌面与 Active Directory (AD) 域集成在一起。

可以使用以下过程将 SLED/SLES 桌面与 AD 域集成以进行智能卡重定向。

该过程中的一些示例使用占位符值以表示网络配置中的实体，例如，AD 域的 DNS 名称。请将占位符值替换为您的配置特定的信息，如下表中所述。

占位符值	描述
dns_IP_ADDRESS	DNS 名称服务器的 IP 地址
mydomain.com	AD 域的 DNS 名称
MYDOMAIN.COM	AD 域的 DNS 名称，全部为大写字母
MYDOMAIN	包含 Samba 服务器的工作组或 NT 域的 DNS 名称，全部为大写字母
ads-hostname	AD 服务器的主机名
ads-hostname.mydomain.com	AD 服务器的完全限定域名 (FQDN)
mytimeserver.mycompany.com	NTP 时间服务器的 DNS 名称
AdminUser	Linux 桌面管理员的用户名

步骤

- 1 为您的 SLED/SLES 桌面配置网络设置。
 - a 通过编辑 `/etc/hostname` 和 `/etc/hosts` 配置文件来定义桌面的主机名。
 - b 配置 DNS 服务器 IP 地址，并禁用**自动 DNS**。对于 SLED 11 SP4 和 SLES 12 SP3，还需禁用**通过 DHCP 更改主机名**。
 - c 要配置网络时间同步，请将 NTP 服务器信息添加到 `/etc/ntp.conf` 文件中，如以下示例中所示。

```
server mytimeserver.mycompany.com
```

- 2 安装所需的 AD 加入软件包。

```
# zypper in krb5-client samba-winbind
```

3 编辑所需的配置文件。

- a 编辑 `/etc/samba/smb.conf` 文件，如以下示例中所示。

```
[global]
    workgroup = MYDOMAIN
    usershare allow guests = NO
    idmap gid = 10000-20000
    idmap uid = 10000-20000
    kerberos method = secrets and keytab
    realm = MYDOMAIN.COM
    security = ADS
    template homedir = /home/%D/%U
    template shell = /bin/bash
    winbind use default domain=true
    winbind offline logon = yes
    winbind refresh tickets = yes

[homes]
    ...
```

- b 编辑 `/etc/krb5.conf` 文件，如以下示例中所示。

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    clocks skew = 300

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname.mydomain.com
        default_domain = mydomain.com
        admin_server = ads-hostname.mydomain.com
    }

[logging]
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log
    default = SYSLOG:NOTICE:DAEMON

[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM

[appdefaults]
    pam = {
        ticket_lifetime = 1d
        renew_lifetime = 1d
        forwardable = true
        proxiable = false
        minimum_uid = 1
    }
```

- c 编辑 `/etc/security/pam_winbind.conf` 文件，如以下示例中所示。

```
cached_login = yes
krb5_auth = yes
krb5_ccache_type = FILE
```

- d 编辑 `/etc/nsswitch.conf` 文件，如以下示例中所示。

```
passwd: compat winbind
group: compat winbind
```

- 4 加入 AD 域，如以下示例中所示。

```
# net ads join -U AdminUser
```

- 5 启用 Winbind 服务。

- a 要启用并启动 Winbind，请运行以下命令序列。

```
# pam-config --add --winbind
# pam-config -a --mkhomedir
# systemctl enable winbind
# systemctl start winbind
```

- b 要确保 AD 用户可以登录到桌面而无需重新启动 Linux 服务器，请运行以下命令序列。

```
# systemctl stop nscd
# nscd -i passwd
# nscd -i group
# systemctl start nscd
```

- 6 要确认 AD 加入成功，请运行以下命令并检查是否返回正确的输出。

```
# wbinfo -u

# wbinfo -g
```

后续步骤

为 [SLED/SLES 桌面设置智能卡重定向](#)

为 RHEL 桌面设置智能卡重定向

要在 RHEL 桌面上配置智能卡重定向，请安装该功能依赖的库、支持受信任的智能卡身份验证的根 CA 证书以及所需的 PC/SC Lite 库。此外，您还必须编辑某些配置文件以完成身份验证设置。

可以使用以下过程为 RHEL 桌面设置智能卡重定向。

该过程中的一些示例使用占位符值以表示网络配置中的实体，例如，AD 域的 DNS 名称。请将占位符值替换为您的配置特定的信息，如下表中所述。

占位符值	描述
dns_IP_ADDRESS	DNS 名称服务器的 IP 地址
mydomain.com	AD 域的 DNS 名称
MYDOMAIN.COM	AD 域的 DNS 名称，全部为大写字母
MYDOMAIN	包含 Samba 服务器的工作组或 NT 域的 DNS 名称，全部为大写字母
ads-hostname	AD 服务器的主机名

注 在运行 RHEL 6 或更高版本或者 RHEL 7.1 或更高版本的桌面上支持智能卡重定向。

前提条件

将 [RHEL 桌面与 Active Directory 集成](#) 以进行智能卡重定向

步骤

- 1 安装所需的库。

```
yum install nss-tools nss-pam-ldapd esc pam_pkcs11 pam_krb5 opensc pcsc-lite-ccid authconfig
authconfig-gtk krb5-libs krb5-workstation krb5-pkinit pcsc-lite pcsc-lite-libs
```

- 2 安装根证书颁发机构 (Certification Authority, CA) 证书。

- a 下载一个根 CA 证书，并将其保存到桌面上的 /tmp/certificate.cer 中。请参阅[如何导出根证书颁发机构证书](#)。
- b 找到下载的根 CA 证书，并将其传输到 .pem 文件。

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

- c 使用 certutil 命令将根 CA 证书安装到系统数据库 /etc/pki/nssdb 中。

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- d 将根 CA 证书复制到 /etc/pam_pkcs11/cacerts 目录中。

```
mkdir -p /etc/pam_pkcs11/cacerts

cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

- 3 导航到 **Applications (应用程序) > Sundry (杂项) > Authentication (身份验证)**，选中 **Enable smart card support (启用智能卡支持)** 复选框，然后单击 **Apply (应用)**。
- 4 复制智能卡驱动程序，并将驱动程序库添加到系统数据库 /etc/pki/nssdb 中。

```
cp libcmP11.so /usr/lib64/
modutil -add "piv card 2.0" -libfile /usr/lib64/libcmP11.so -dbdir /etc/pki/nssdb/
```

- 5 在 `/etc/pam_pkcs11/pam_pkcs11.conf` 配置文件中编辑 `module` 设置，如以下示例中所示。

```
pkcs11_module coolkey {
    module = libcmP11.so;
    description = "Cool Key";
    slot_num = 0;
    ca_dir = /etc/pam_pkcs11/cacerts;
    nss_dir = /etc/pki/nssdb;
    cert_policy = ca, signature;
}
```

- 6 编辑 `/etc/pam_pkcs11/cn_map` 文件，以使其包含类似于以下示例的内容。要包含特定的内容，请参阅智能卡证书中列出的用户信息。

```
user sc -> user-sc
```

- 7 编辑 `/etc/krb5.conf/` 配置文件，如以下示例中所示。

```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_realm = MYDOMAIN.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname
        admin_server = ads-hostname
        default_domain = ads-hostname
        pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
        pkinit_cert_match = <KU>digitalSignature
        pkinit_kdc_hostname = ads-hostname
    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COMmydomain.com = MYDOMAIN.COM
```

- 8 编辑 `/etc/pam.d/system-auth` 配置文件，以使其包含以下示例中显示的行。

```
auth optional pam_krb5.so use_first_pass no_subsequent_prompt
preauth_options=X509_user_identity=PKCS11:/usr/lib64/libcmP11.so
```

- 9 重新启动 PC/SC 守护进程。

```
chkconfig pcscd on
service pcscd start
```

10 为您的 RHEL 分发包安装所需的 PC/SC Lite 版本。

- 对于 RHEL 7.x, 请安装 PC/SC Lite 版本 1.8.8。

```
yum install git flex autoconf automake libtool libudev-devel flex
git clone https://salsa.debian.org/rousseau/PCSC.git
cd PCSC
git checkout -b 1.8.8 pcsc-1.8.8
./bootstrap
./configure --build=x86_64-redhat-linux-gnu --host=x86_64-redhat-linux-gnu --program-prefix=
--disable-dependency-tracking --prefix=/usr --exec-prefix=/usr --bindir=/usr/bin --
sbindir=/usr/sbin
--sysconfdir=/etc --datadir=/usr/share --includedir=/usr/include --libdir=/usr/lib64
--libexecdir=/usr/libexec --localstatedir=/var --sharedstatedir=/var/lib --mandir=/usr/
share/man
--infodir=/usr/share/info --disable-static --enable-usbdropdir=/usr/lib64/pcsc/drivers
make
make install
```

- 对于 RHEL 6.x, 请安装 PC/SC Lite 版本 1.7.4。

```
yum groupinstall "Development tools"
yum install libudev-devel
service pcscd stop
wget https://alioth.debian.org/frs/download.php/file/3598/pcsc-lite-1.7.4.tar.bz2
tar -xjvf pcsc-lite-1.7.4.tar.bz2
cd ./pcsc-lite-1.7.4
./configure --prefix=/usr/ --libdir=/usr/lib64/ --enable-usbdropdir=/usr/lib64/pcsc/drivers
--enable-conffdir=/etc --enable-ipcdirdir=/var/run --disable-libusb --disable-serial --disable-
usb
--disable-libudev
make
make install
service pcscd start
```

11 安装 Horizon Agent 软件包并启用智能卡重定向。

```
sudo ./install_viewagent.sh -m yes
```

注 对于 RHEL 6.x, 您必须安装 View Agent 6.2.1 或更高版本。对于 RHEL 7.x, 您必须安装 Horizon Agent 7.8 或更高版本。

12 重新引导系统, 然后重新登录。**为 Ubuntu 桌面设置智能卡重定向**

要在 Ubuntu 桌面上配置智能卡重定向, 需安装该功能所依赖的库以及用于支持智能卡的受信任身份验证的根 CA 证书。此外, 您还必须编辑某些配置文件以完成身份验证设置。

该过程中的一些示例使用占位符值以表示网络配置中的实体, 例如, AD 域的 DNS 名称。请将占位符值替换为您的配置特定的信息, 如下表中所述。

占位符值	描述
dns_IP_ADDRESS	DNS 名称服务器的 IP 地址
mydomain.com	AD 域的 DNS 名称
MYDOMAIN.COM	AD 域的 DNS 名称，全部为大写字母
MYDOMAIN	包含 Samba 服务器的工作组或 NT 域的 DNS 名称，全部为大写字母
ads-hostname	AD 服务器的主机名
ads-hostname.mydomain.com	AD 服务器的完全限定域名 (FQDN)
mytimeserver.mycompany.com	NTP 时间服务器的 DNS 名称
AdminUser	Linux 桌面管理员的用户名

前提条件

将 [Ubuntu 桌面与 Active Directory 集成](#) 以进行智能卡重定向

步骤

1 安装所需的库。

```
# apt-get install -y pcscd pcsc-tools pkg-config libpam-pkcs11 openssl
libengine-pkcs11-openssl libnss3-tools
```

2 安装根证书颁发机构 (Certification Authority, CA) 证书。

- 下载一个根 CA 证书，并将其保存到桌面上的 `/tmp/certificate.cer` 中。请参阅[如何导出根证书颁发机构证书](#)。
- 找到下载的根 CA 证书，并将其传输到 `.pem` 文件。

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

- 使用 `certutil` 命令将根 CA 证书安装到系统数据库 `/etc/pki/nssdb` 中。

```
# certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- 将根 CA 证书复制到 `/etc/pam_pkcs11/cacerts` 目录中。

```
# mkdir -p /etc/pam_pkcs11/cacerts

# cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

3 创建一个 pkcs11 哈希文件。

```
# chmod a+r certificate.pem
# pkcs11_make_hash_link
```

4 复制所需的驱动程序，并将必要的库文件添加到 `nssdb` 目录。

a 运行以下命令。

```
# cp libcmP11.so /usr/lib/
# mkdir -p /etc/pki/nssdb
# certutil -N -d /etc/pki/nssdb
# certutil -A -n rootca -i certificate.pem -t "CT,CT,CT" -d /etc/pki/nssdb
# modutil -dbdir /etc/pki/nssdb/ -add "piv card 2.0" -libfile /usr/lib/libcmP11.so
```

b 确认已成功加载所需的证书。

```
# certutil -L -d /etc/pki/nssdb

Certificate Nickname

rootca
```

c 确认已成功添加所需的库。

```
modutil -dbdir /etc/pki/nssdb -list

Listing of PKCS #11 Modules
-----
1. NSS Internal PKCS #11 Module
   slots: 2 slots attached
   status: loaded

   slot: NSS Internal Cryptographic Services
   token: NSS Generic Crypto Services

   slot: NSS User Private Key and Certificate Services
   token: NSS Certificate DB

2. piv card 2.0
   library name: /usr/lib/libcmP11.so
   slots: There are no slots attached to this module
   status: loaded
-----
```

5 配置 pam_pkcs11 库。

- a 使用默认示例内容创建一个 `pam_pkcs11.conf` 文件。

```
# mkdir /etc/pam_pkcs11
# zcat /usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz |
tee /etc/pam_pkcs11/pam_pkcs11.conf
```

- b 编辑 `/etc/pam_pkcs11/pam_pkcs11.conf` 文件，如以下示例中所示。

```
use_pkcs11_module = mysc;

pkcs11_module mysc {
    module = /usr/lib/libcmP11.so;
    description = "LIBCMP11";
    slot_num = 0;
    ca_dir = /etc/pki/cacerts;
    nss_dir = /etc/pki/nssdb;
    cert_policy = ca;
}
...
use_mappers = cn, null;
...
mapper cn {
    debug = false;
    module = internal;
    # module = /lib/pam_pkcs11/cn_mapper.so;
    ignorecase = true;
    mapfile = file:///etc/pam_pkcs11/cn_map;
    # mapfile = "none";
}
```

- c 编辑 `/etc/pam_pkcs11/cn_map` 文件，使其包含以下行。

```
ads-hostname -> ads-hostname
```

6 配置 PAM 身份验证。

- a 编辑 `/etc/pam.d/gdm-password` 配置文件。将 `pam_pkcs11.so` 授权行放置在 `common-auth` 行之前，如以下示例中所示。

```
##PAM-1.0
auth    requisite      pam_nologin.so
auth    required       pam_succeed_if.so user != root quiet_success
auth    sufficient
pam_pkcs11.so
@include common-auth
auth    optional       pam_gnome_keyring.so
@include common-account
```

- b 对于 Ubuntu 16.04，请编辑 `/etc/pam.d/lightdm` 配置文件。将 `pam_pkcs11.so` 授权行放置在 `common-auth` 行之前，如以下示例中所示。

```
##PAM-1.0
auth    requisite      pam_nologin.so debug
auth    sufficient     pam_succeed_if.so user ingroup nopasswdlogin debug
auth    [success=3 default=ignore] pam_pkcs11.so
@include common-auth
auth    optional       pam_gnome_keyring.so
auth    optional       pam_kwallet.so
```

- c 对于 Ubuntu 16.04，请编辑 `/etc/pam.d/unity` 配置文件。将 `pam_pkcs11.so` 授权行放置在 `common-auth` 行之前，如以下示例中所示。

```
auth    [success=3 default=ignore] pam_pkcs11.so
@include common-auth
auth    optional       pam_gnome_keyring.so
```

- 7 要确认已在智能卡上安装智能卡硬件和证书，请运行以下命令。

```
# pcsc_scan

# pkcs11_listcerts

# pkcs11_inspect
```

8 配置 Gnome 屏幕保护程序，使其在移除智能卡后锁定。

a 安装屏幕保护程序软件包。

```
# apt-get install gnome-screensaver
```

b 要配置屏幕保护程序，请编辑 /etc/pam_pkcs11/pkcs11_eventmgr.conf 文件，如以下示例中所示。

```
pkcs11_eventmgr {
    # Run in background? Implies debug=false if true
    daemon = true;

    # show debug messages?
    debug = false;

    # polling time in seconds
    polling_time = 1;

    # expire time in seconds
    # default = 0 ( no expire )
    expire_time = 0;

    # pkcs11 module to use
    pkcs11_module = /usr/lib/libcmP11.so;

    #
    # list of events and actions
    # Card inserted
    event card_insert {
        # what to do if an action fail?
        # ignore : continue to next action
        # return : end action sequence
        # quit : end program
        on_error = ignore ;

        # You can enter several, comma-separated action entries
        # they will be executed in turn
        action = "gnome-screensaver-command --poke";
    }

    # Card has been removed
    event card_remove {
        on_error = ignore;
        action = "gnome-screensaver-command --lock";
    }

    # Too much time card removed
    event expire_time {
```

```

    on_error = ignore;
    action = "/bin/false";
}
}

```

c 运行 `pkcs11_eventmgr`。

```
# /usr/bin/pkcs11_eventmgr &
```

9 安装 Horizon Agent 软件包并启用智能卡重定向。

```
# sudo ./install_viewagent.sh -m yes
```

注 您必须安装 Horizon Agent 7.9 或更高版本。

10 重新引导系统，然后重新登录。

为 SLED/SLES 桌面设置智能卡重定向

要在 SLED/SLES 桌面上配置智能卡重定向，需安装该功能所依赖的库以及用于支持智能卡的受信任身份验证的根 CA 证书。此外，您还必须编辑某些配置文件以完成身份验证设置。

该过程中的一些示例使用占位符值以表示网络配置中的实体，例如，AD 域的 DNS 名称。请将占位符值替换为您的配置特定的信息，如下表中所述。

占位符值	描述
<code>dns_IP_ADDRESS</code>	DNS 名称服务器的 IP 地址
<code>mydomain.com</code>	AD 域的 DNS 名称
<code>MYDOMAIN.COM</code>	AD 域的 DNS 名称，全部为大写字母
<code>MYDOMAIN</code>	包含 Samba 服务器的工作组或 NT 域的 DNS 名称，全部为大写字母
<code>ads-hostname</code>	AD 服务器的主机名
<code>ads-hostname.mydomain.com</code>	AD 服务器的完全限定域名 (FQDN)
<code>mytimeserver.mycompany.com</code>	NTP 时间服务器的 DNS 名称
<code>AdminUser</code>	Linux 桌面管理员的用户名

前提条件

将 SLED/SLES 桌面与 [Active Directory](#) 集成以进行智能卡重定向

步骤**1 安装所需的库软件包。****a 安装 PAM 库和其他软件包。**

```
# zypper install pam_pkcs11 mozilla-nss mozilla-nss-tools
pcsc-lite pcsc-ccid opensc coolkey pcsc-tools
```

b 执行相应的步骤以安装 PC/SC 工具。

- 对于 SLED/SLES 12 SP3，请运行以下命令系列。

```
# SUSEConnect --list-extensions
# SUSEConnect -p PackageHub/12.3/x86_64
# zypper in pcsc-tools
```

- 对于 SLED 11 SP4，请从以下网页下载并安装 PC/SC 工具：

https://download.opensuse.org/repositories/security:/chipcard/SLE_11_SP4/

2 安装根证书颁发机构 (Certification Authority, CA) 证书。**a 下载一个根 CA 证书，并将其保存到桌面上的 /tmp/certificate.cer 中。请参阅[如何导出根证书颁发机构证书](#)。****b 找到您下载的根 CA 证书，将其传输到 .pem 文件，然后创建一个哈希文件。**

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
# cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
# chmod a+r /etc/pam_pkcs11/cacerts/certificate.pem
# cd /etc/pam_pkcs11/cacerts
# pkcs11_make_hash_link
```

c 将信任定位点安装到 NSS 数据库。

```
# mkdir /etc/pam_pkcs11/nssdb
# certutil -N -d /etc/pam_pkcs11/nssdb
# certutil -L -d /etc/pam_pkcs11/nssdb
# certutil -A -n rootca -i certificate.pem -t "CT,CT,CT" -d /etc/pam_pkcs11/nssdb
```

d 安装所需的驱动程序。

```
# cp libcmP11.so /usr/lib64/
# modutil -add "piv card 2.0" -libfile /usr/lib64/libcmP11.so -dbdir /etc/pam_pkcs11/nssdb/
```

3 编辑 /etc/pam_pkcs11/pam_pkcs11.conf 文件。

- a 删除 `use_pkcs11_module = nss` 行。在其位置中，添加 `use_pkcs11_module = mysc` 行。
- b 添加 `mysc` 模块，如以下示例中所示。

```
pkcs11_module mysc {
    module = /usr/lib64/libcmP11.so;
    description = "MY Smartcard";
    slot_num = 0;
    nss_dir = /etc/pam_pkcs11/nssdb;
    cert_policy = ca, ocsp_on, signature, crl_auto;
}
```

- c 更新公用名映射程序配置，如以下示例中所示。

```
# Assume common name (CN) to be the login
mapper cn {
    debug = false;
    module = internal;
    # module = /usr/lib64/pam_pkcs11/cn_mapper.so;
    ignorecase = true;
    mapfile = file:///etc/pam_pkcs11/cn_map;}
```

- d 删除 `use_mappers = ms` 行。在其位置中，添加 `use_mappers = cn, null` 行。

4 编辑 /etc/pam_pkcs11/cn_map 配置文件，使其包含以下行。

```
ads-hostname -> ads-hostname
```

5 修改 PAM 配置。

- a 先禁用 `pam_config` 工具，然后才能配置智能卡身份验证。

```
# find /etc/pam.d/ -type l -iname "common-*" -delete
# for X in /etc/pam.d/common-*-pc; do cp -ivp $X ${X:0:-3}; done
```

- b 在 /etc/pam.d/ 目录下，创建一个名为 `common-auth-smartcard` 的文件。在该文件中添加以下内容。

auth	required	pam_env.so	
auth	sufficient	pam_pkcs11.so	
auth	optional	pam_gnome_keyring.so	
auth	[success=1 default=ignore]	pam_unix.so	nullok_secure try_first_pass
auth	required	pam_winbind.so	use_first_pass

- c 对于 SLED/SLES 12 SP3，请将以下两个文件中的 `auth include common-auth` 行替换为 `auth include common-auth-smartcard` 行：/etc/pam.d/gdm 和 /etc/pam.d/xscreensaver。
- d 对于 SLED 11 SP4，请将以下两个文件中的 `auth include common-auth` 行替换为 `auth include common-auth-smartcard` 行：/etc/pam.d/gdm 和 /etc/pam.d/gnome-screensaver。

6 禁用防火墙。

```
# rcSuSEfirewall2 stop
# chkconfig SuSEfirewall2_setup off
# chkconfig SuSEfirewall2_init off
```

注 启用防火墙后，智能卡重定向有时会失败。

7 安装智能卡重定向所需的库软件包。

- a 对于 SLED/SLES 12 SP3 和 SLED 11 SP4，请运行以下安装命令。

```
# SUSEConnect -p sle-sdk/12.3/x86_64
# zypper in git autoconf automake libtool flex libudev-devel gcc
```

- b 对于 SLES 12 SP3，请安装 `systemd-devel`。

```
# zypper in systemd-devel
```

- c 对于 SLED 11 SP4，请安装以下软件包：

- perl-Error、autoconf、automake、flex rpm
- git、gcc
- libtool

8 安装 Horizon Agent 软件包并启用智能卡重定向。

```
# sudo ./install_viewagent.sh -m yes
```

注 您必须安装 Horizon Agent 7.9 或更高版本。

9 重新引导系统，然后重新登录。

为 Linux 桌面设置 True SSO

通过使用 True 单点登录 (True SSO) 功能，在用户使用智能卡、RSA SecurID 或 RADIUS 身份验证登录到 VMware Identity Manager 后，用户无需再次输入 Active Directory 凭据即可使用 Linux 虚拟桌面或发布的桌面或应用程序。

如果用户使用 Active Directory (AD) 凭据进行身份验证，则不需要使用 True SSO 功能。不过，您甚至可以在这种情况下配置使用 True SSO，以便桌面可以支持 AD 凭据和 True SSO。

在连接到 Linux 虚拟桌面或者发布的桌面或应用程序时，用户可以选择使用本机 Horizon Client 或 HTML Access。

True SSO 具有以下限制：

- 仅在具有以下分发包的桌面上支持该功能：RHEL/CentOS 7、Ubuntu 16.04 和 18.04 以及 SLED/SLES 12.x SP3。

- 对于 RHEL/CentOS 7 桌面，仅以下加入方法支持该功能：默认加入域工具、Samba、系统安全服务守护进程 (SSSD) 以及 Kerberos 网络身份验证协议。

要在 Linux 环境中设置 True SSO，请执行以下任务。

- 1 在 Horizon 7 环境中设置和配置 True SSO。请参阅《《Horizon 7 管理指南》》文档中的“设置 True SSO”。
- 2 按照 Linux 分发过程将桌面与 AD 域集成在一起。
- 3 按照 Linux 分发过程在桌面上配置 True SSO。

将 RHEL/CentOS 桌面与 Active Directory 集成以进行 True SSO

要使 RHEL/CentOS 系统上 Horizon 7 Linux 桌面环境中的即时克隆虚拟机支持 True SSO，必须在主 Linux 虚拟机上配置 Samba。

通过 RHEL 7 `realm` 功能，可轻松发现并加入身份域。该功能不是直接将系统连接到域本身，而是对底层 Linux 系统服务（如 SSSD 或 Winbind）进行配置以将其连接到域。可以执行以下步骤以使用 Samba 将 RHEL/CentOS 桌面脱机加入 Active Directory 域中。

前提条件

- Red Hat Enterprise Linux (RHEL) 系统已订阅 Red Hat Network (RHN) 或已在本地安装 `yum` 工具。
- 在 Linux 系统上，Active Directory (AD) 服务器可通过 DNS 解析。
- 在 Linux 系统上配置了网络时间协议 (Network Time Protocol, NTP)。

步骤

- 1 确认 RHEL/CentOS 系统可以发现 AD 服务器。可使用以下示例，但须将其中的 `ADdomain.example.com` 替换为您的 AD 服务器信息。

```
sudo realm discover ADdomain.example.com
```

- 2 安装 Samba `tdb-tools` 软件包。

Samba `tdb-tools` 软件包无法从官方 Red Hat 存储库中下载。您必须手动下载该软件包。例如，可以使用以下命令从 CentOS 7.5 系统中下载该软件包，然后将其安装到您的 RHEL 系统。

```
yumdownloader tdb-tools
```

如果您没有 CentOS 系统，请转到 <https://rpmfind.net/linux/rpm2html/search.php?query=tdb-tools&submit=Search+...&system=&arch=>，下载 `tdb-tools-1.3.15-1.el7.x86_64.rpm` 软件包，然后将其安装到您的 RHEL 系统。

- 3 安装 Samba 和依赖项包。

```
sudo yum install sssd-tools sssd adcli samba-common pam_ldap pam_krb5 samba samba-client krb5-workstation
```

- 4 可使用以下示例运行 `join` 命令，但须将其中中的 `DNSdomain.example.com` 替换为特定于您环境的 DNS 域路径。

```
sudo realm join DNSdomain.example.com -U administrator
```

成功运行加入命令后，您会收到以下消息。

```
已成功在领域中注册计算机
```

- 5 重新引导系统，然后重新登录。

后续步骤

在 [RHEL/CentOS 桌面上配置 True SSO](#)

将 Ubuntu 桌面与 Active Directory 集成以进行 True SSO

要在 Ubuntu 16.04 或 18.04 桌面上支持 True SSO，请使用 Samba 和 Winbind 解决方案将桌面与 Active Directory 域集成在一起。

可以使用以下过程将 Ubuntu 16.04 或 18.04 桌面与 AD 域集成在一起。

该过程中的一些示例使用占位符值以表示网络配置中的实体，例如，Ubuntu 桌面的主机名。请将占位符值替换为您的配置特定的信息，如下表中所述。

占位符值	描述
<code>dns_IP_ADDRESS</code>	DNS 名称服务器的 IP 地址
<code>mydomain.com</code>	AD 域的 DNS 名称
<code>MYDOMAIN.COM</code>	AD 域的 DNS 名称，全部为大写字母
<code>myhost</code>	Ubuntu 桌面的主机名
<code>MYDOMAIN</code>	包含 Samba 服务器的工作组或 NT 域的 DNS 名称，全部为大写字母
<code>ads-hostname</code>	AD 服务器的主机名
<code>admin-user</code>	AD 域管理员的用户名

前提条件

- 在 Linux 系统上，Active Directory (AD) 服务器可通过 DNS 解析。
- 在 Linux 系统上配置了网络时间协议 (Network Time Protocol, NTP)。

步骤

- 1 在 Ubuntu 16.04 或 18.04 桌面上，安装 `samba` 和 `winbind` 软件包。

```
sudo apt install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind
```

2 在出现提示时，配置 Kerberos 身份验证设置，如下所示。

- a 对于 **Default Kerberos version 5 realm (默认 Kerberos 版本 5 领域)**，请输入 AD 域的 DNS 名称（全部为大写字母）。

例如，如果 AD 域名为 **mydomain.com**，请输入 **MYDOMAIN.COM**。

- b 对于 **Kerberos servers for your realm (领域的 Kerberos 服务器)**，请输入 AD 服务器的主机名（在该过程的示例中表示为 **ads_hostname**）。

- c 对于 **Administrative server for your Kerberos realm (Kerberos 领域的管理服务器)**，再次输入 AD 服务器的主机名。

3 更新 PAM 配置。

- a 打开 PAM 配置页面。

```
pam-auth-update
```

- b 选择 **Create home directory on login (在登录时创建主目录)**，然后选择 **Ok (确定)**。

4 按照下例所示编辑 `/etc/nsswitch.conf` 配置文件。

```
passwd: compat winbind
group: compat winbind
shadow: compat
gshadow: files
```

5 要确保自动生成的 `resolv.conf` 文件将 AD 域引用为搜索域，请编辑系统连接的 NetworkManager 设置。

- a 打开 NetworkManager 控制面板，然后导航到系统连接的 **IPv4 Settings (IPv4 设置)**。对于 **Method (方法)**，请选择 **Automatic (DHCP) addresses only (仅自动 (DHCP) 地址)**。在 **DNS servers (DNS 服务器)** 文本框中，输入 DNS 名称服务器的 IP 地址（在该过程的示例中表示为 **dns_IP_ADDRESS**）。然后，单击 **Save (保存)**。
- b 编辑位于 `/etc/NetworkManager/system-connections` 中的系统连接配置文件。请使用以下示例。

```
[ipv4]
dns=dns_IP_ADDRESS
dns-search=mydomain.com
ignore-auto-dns=true
method=auto
```

注 在创建新的即时克隆虚拟桌面时，将添加新的虚拟网络适配器。在即时克隆虚拟桌面中添加新的网络适配器时，虚拟桌面模板上的网络适配器中的任何设置（如 DNS 服务器）将会丢失。为了避免在克隆虚拟桌面中添加新的网络适配器时丢失 DNS 服务器设置，您必须为 Linux 系统指定 DNS 服务器。

- c 编辑 `/etc/resolv.conf` 配置文件以指定 DNS 服务器，如以下示例中所示。

```
nameserver dns_IP_ADDRESS

search mydomain.com
```

- d 重新引导系统，然后重新登录。

- 6 编辑 `/etc/hosts` 配置文件，如以下示例中所示。

```
127.0.0.1    localhost
127.0.1.1    myhost.mydomain.com myhost
```

- 7 编辑 `/etc/samba/smb.conf` 配置文件，如以下示例中所示。

```
[global]
security = ads
realm = MYDOMAIN.COM
workgroup = MYDOMAIN
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum group = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
kerberos method = secrets and keytab
winbind refresh tickets = true
```

- 8 重新启动 `smbd` 服务。

```
sudo systemctl restart smbd.service
```

- 9 编辑 `/etc/krb5.conf` 配置文件，以使其具有类似于以下示例的内容。

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    dns_lookup_realm = true
    dns_lookup_kdc = true

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname
        admin_server = ads-hostname
    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COMmydomain.com = MYDOMAIN.COM
```

10 将 Ubuntu 桌面加入 AD 域。

- a 启动 Kerberos 票证。

```
sudo kinit admin-user
```

在出现提示时，输入管理员密码。

- b 确认已成功创建票证。

```
sudo klist
```

该命令返回有关票证的信息，包括有效期开始时间和到期时间。

- c 创建一个 Kerberos keytab 文件。

```
sudo net ads keytab create -U admin-user
```

- d 加入 AD 域。

```
sudo net ads join -U admin-user
```

11 重新启动并验证 Winbind 服务。

- a 重新启动 Winbind 服务。

```
sudo systemctl restart winbind.service
```

- b 要验证 Winbind 服务，请运行以下命令并检查是否返回正确的输出。

- `wbinfo -u`
- `wbinfo -g`
- `getend passwd`
- `getend group`

12 重新引导系统，然后重新登录。**后续步骤**

在 [Ubuntu 桌面上配置 True SSO](#)

将 SLED/SLES 桌面与 Active Directory 集成以进行 True SSO

要在 SLED 12.x SP3 或 SLES 12.x SP3 桌面上支持 True SSO，请使用 Samba 和 Winbind 解决方案将桌面与 Active Directory 域集成在一起。

可以使用以下过程将 SLED/SLES 桌面与 AD 域集成在一起。

前提条件

- 在 Linux 系统上，Active Directory (AD) 服务器可通过 DNS 解析。
- 在 Linux 系统上配置了网络时间协议 (Network Time Protocol, NTP)。

步骤

- 1 在 SLED/SLES 桌面上，安装 **samba** 和 **winbind** 软件包。

```
zypper install samba-winbind krb5-client samba-winbind-32bit
```

- 2 打开 YaST 安装工具，然后导航到 **Network Services (网络服务) > Windows Domain Membership (Windows 域成员身份)**。
- 3 在 Windows Domain Membership (Windows 域成员身份) 屏幕上配置设置，如下所示。
 - a 对于 **Domain or Workgroup (域或工作组)**，请输入包含 Samba 服务器的工作组或 NT 域的 DNS 名称（全部为大写字母）。例如，如果工作组名称为 **mydomain**，请输入 **MYDOMAIN**。
 - b 选择 **Also Use SMB Information for Linux Authentication (还使用 SMB 信息进行 Linux 身份验证)**。
 - c 选择 **Create Home Directory on Login (在登录时创建主目录)**。
 - d 选择 **Offline Authentication (脱机身份验证)**。
 - e 选择 **Single Sign-on for SSH (SSH 单点登录)**。
- 4 在出现提示以询问您是否要加入域时，请选择 **Yes (是)**。
- 5 为指定的工作组输入管理员用户名和密码，然后选择 **OK (确定)**。
将显示一条消息以确认 SLED/SLES 桌面成功加入域。选择 **OK (确定)**。
- 6 编辑 **/etc/samba/smb.conf** 配置文件，以使其包含以下参数。

```
[global]
...
winbind use default domain = yes
```

- 7 重新引导系统，然后重新登录。
- 8 测试并验证 SLED/SLES 桌面集成。

运行以下测试命令，并检查是否返回正确的输出。将 **mydomain** 替换为 Samba 服务器工作组或 NT 域的名称。

- `net ads testjoin`
- `net ads info`
- `wbinfo --krb5auth=mydomain\\open%open`
- `ssh localhost -l mydomain\\open`

后续步骤

在 SLED/SLES 桌面上配置 [True SSO](#)

在 RHEL/CentOS 桌面上配置 True SSO

要在 RHEL/CentOS 7.x 桌面上启用 True SSO 功能，请安装 True SSO 功能依赖的库、支持受信任的身份验证的根 CA 证书以及 Horizon Agent。此外，您还必须编辑某些配置文件以完成身份验证设置。

可以使用以下过程在 RHEL 7.x 和 CentOS 7.x 桌面上启用 True SSO。要在这些桌面上支持 True SSO，您必须安装 Horizon Agent 7.6 或更高版本。

该过程中的一些示例使用占位符值以表示网络配置中的实体，例如，AD 域的 DNS 名称。请将占位符值替换为您的配置特定的信息，如下表中所述。

占位符值	描述
dns_server	DNS 名称服务器的路径
mydomain.com	AD 域的 DNS 名称
MYDOMAIN.COM	AD 域的 DNS 名称，全部为大写字母

前提条件

- 为 VMware Identity Manager 和 Horizon Connection Server 配置 True SSO。
- 将 RHEL/CentOS 桌面与 Active Directory 集成以进行 True SSO
- 获取一个根证书颁发机构证书，并将其保存到 RHEL/CentOS 7.x 桌面上的 /tmp/certificate.cer 中。请参阅[如何导出根证书颁发机构证书](#)。

步骤

- 1 安装 PKCS11 支持软件包组。

```
yum install -y nss-tools nss-pam-ldapd pam_krb5 krb5-libs krb5-workstation krb5-pkinit
```

- 2 安装根证书颁发机构 (Certification Authority, CA) 证书。

- a 找到下载的根 CA 证书，并将其传输到 .pem 文件。

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

- b 使用 certutil 命令将根 CA 证书安装到系统数据库 /etc/pki/nssdb 中。

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- c 将根 CA 证书添加到在 RHEL/CentOS 7.x 系统上信任的 CA 证书列表中，并使用 update-ca-trust 命令更新系统范围的信任存储配置。

```
cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
update-ca-trust
```

- 3 在系统的 SSSD 配置文件中修改您的域的相应部分，如以下示例中所示。

```
[domain/mydomain.com]
ad_domain = mydomain.com
```



```

krb5_realm = MYDOMAIN.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
#set the next line to false, so you can use the short name instead of the full domain name.
use_fully_qualified_names = False
fallback_homedir = /home/%u@%d
access_provider = ad

```

- 4 修改 Kerberos 配置文件 `/etc/krb5.conf`，如以下示例中所示。

```

[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_ccache_name = KEYRING:persistent:%{uid}
    # Add following line, if the system doesn't add it automatically
    default_realm = MYDOMAIN.COM

[realms]
    MYDOMAIN.COM = {
        kdc = dns_server
        admin_server = dns_server
        # Add the following three lines for pkinit_*
        pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
        pkinit_kdc_hostname = your_org_DNS_server
        pkinit_eku_checking = kpServerAuth
    }

[domain_realm]
    mydomain.com = MYDOMAIN.COM
    .mydomain.com = MYDOMAIN.COM

```

- 5 安装 Horizon Agent 软件包并启用 True SSO。

```
sudo ./install_viewagent.sh -T yes
```

注 您必须安装 Horizon Agent 7.6 或更高版本。

- 6 将以下参数添加到 Horizon Agent 自定义配置文件 `/etc/vmware/viewagent-custom.conf` 中。使用以下示例，其中，`NETBIOS_NAME_OF_DOMAIN` 是您的组织的域的 NetBIOS 名称。

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

- 7 重新引导系统，然后重新登录。

在 Ubuntu 桌面上配置 True SSO

要在 Ubuntu 16.04 或 18.04 桌面上启用 True SSO 功能，请安装 True SSO 功能依赖的库、支持受信任的身份验证的根 CA 证书以及 Horizon Agent。此外，您还必须编辑某些配置文件以完成身份验证设置。

可以使用以下过程在 Ubuntu 16.04 和 18.04 桌面上启用 True SSO。要在这些桌面上支持 True SSO，您必须安装 Horizon Agent 7.8 或更高版本。

前提条件

- 为 VMware Identity Manager 和 Horizon Connection Server 配置 True SSO。
- 将 [Ubuntu 桌面与 Active Directory 集成以进行 True SSO](#)
- 获取一个根证书颁发机构证书，并将其保存到桌面上的 `/tmp/certificate.cer` 中。请参阅[如何导出根证书颁发机构证书](#)。

步骤

- 1 在 Ubuntu 16.04 或 18.04 桌面上，安装 `pkcs11` 支持软件包。

```
sudo apt install libpam-pkcs11
```

- 2 安装 `libnss3-tools` 软件包。

```
sudo apt install libnss3-tools
```

- 3 安装根证书颁发机构 (Certification Authority, CA) 证书。

- a 找到下载的根 CA 证书，并将其传输到 `.pem` 文件。

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

- b 使用 `certutil` 命令将根 CA 证书安装到系统数据库 `/etc/pki/nssdb` 中。

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- c 将根 CA 证书复制到 `/etc/pam_pkcs11/cacerts` 目录中。

```
mkdir -p /etc/pam_pkcs11/cacerts

cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

- d 为根 CA 证书创建一个哈希链接。在 `/etc/pam_pkcs11/cacerts` 目录中，运行以下命令。

```
pkcs11_make_hash_link
```

- 4 安装 Horizon Agent 软件包并启用 True SSO。

```
sudo ./install_viewagent.sh -T yes
```

注 要使用 True SSO 功能，您必须安装 Horizon Agent 7.8 或更高版本。

- 5 将以下参数添加到 Horizon Agent 自定义配置文件 `/etc/vmware/viewagent-custom.conf` 中。使用以下示例，其中，`NETBIOS_NAME_OF_DOMAIN` 是您的组织的域的 NetBIOS 名称。

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

- 6 编辑 `/etc/pam_pkcs11/pam_pkcs11.conf` 配置文件。
 - a 如果需要，请创建 `/etc/pam_pkcs11/pam_pkcs11.conf` 配置文件。在 `/usr/share/doc/libpam-pkcs11/examples` 中找到示例文件，将其复制到 `/etc/pam_pkcs11` 目录中，并将该文件重命名为 `pam_pkcs11.conf`。根据需要，将您的系统信息添加到文件内容中。
 - b 修改 `/etc/pam_pkcs11/pam_pkcs11.conf` 配置文件，以使其包含类似于以下示例的内容。

```
use_pkcs11_module = coolkey;
pkcs11_module coolkey {
    module = /usr/lib/vmware/viewagent/sso/libvmwpkcs11.so;
    slot_num = 0;
    ca_dir = /etc/pam_pkcs11/cacerts;
    nss_dir = /etc/pki/nssdb;
}
```

- 7 在 PAM 配置文件中修改 `auth` 参数。
 - a 打开 PAM 配置文件。
 - 对于 Ubuntu 16.04，请打开 `/etc/pam.d/lightdm`。
 - 对于 Ubuntu 18.04，请打开 `/etc/pam.d/gdm-vmwcred`。
 - b 编辑 PAM 配置文件，如以下示例中所示。

```
auth requisite pam_vmw_cred.so
auth sufficient pam_pkcs11.so try_first_pass
```

- 8 重新引导系统，然后重新登录。

在 SLED/SLES 桌面上配置 True SSO

要在 SLED/SLES 12.x SP3 桌面上启用 True SSO 功能，请安装 True SSO 功能依赖的库、支持受信任的身份验证的根 CA 证书以及 Horizon Agent。此外，您还必须编辑某些配置文件以完成身份验证设置。

可以使用以下过程在 SLED 12.x SP3 和 SLES 12.x SP3 桌面上启用 True SSO。要在这些桌面上支持 True SSO，您必须安装 Horizon Agent 7.8 或更高版本。

前提条件

- 为 VMware Identity Manager 和 Horizon Connection Server 配置 True SSO。
- 将 [SLED/SLES 桌面与 Active Directory 集成以进行 True SSO](#)
- 获取一个根证书颁发机构证书，并将其保存到 SLED/SLES 12.x SP3 桌面上的 `/tmp/certificate.cer` 中。请参阅[如何导出根证书颁发机构证书](#)。

步骤

- 1 对于 SLES 12.x SP3 桌面，请运行以下命令以安装所需的软件包。

```
zypper install mozilla-nss-tools pam_krb5 krb5-client krb5-plugin-preauth-pkinit
```

- 2 对于 SLED 12.x SP3 桌面，请执行以下步骤以安装所需的软件包。

- a 将一个 SLES .iso 文件下载到 SLED 桌面的本地磁盘中（例如 /tmp/SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso）。

您必须将 SLES .iso 文件添加为 SLED 桌面的软件包源文件，因为所需的 krb5-plugin-preauth-pkinit 软件包仅适用于 SLES 系统。

- b 在 SLED 桌面上挂载 SLES .iso 文件，并安装所需的软件包。

```
sudo mkdir -p /mnt/sles
sudo mount -t iso9660 /tmp/SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso /mnt/sles
sudo zypper ar -f /mnt/sles sles
zypper install mozilla-nss-tools pam_krb5 krb5-client krb5-plugin-preauth-pkinit
```

- c 安装完成后，卸载 SLES .iso 文件。

```
sudo umount /mnt/sles
```

- 3 安装根证书颁发机构 (Certification Authority, CA) 证书。

- a 找到下载的根 CA 证书，并将其传输到 .pem 文件。

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

- b 使用 certutil 命令将根 CA 证书安装到系统数据库 /etc/pki/nssdb 中。

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- c 将根 CA 证书添加到 pam_pkcs11 中。

```
cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
```

- 4 编辑 /etc/krb5.conf 配置文件，以使其具有类似于以下示例的内容。

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname
        admin_server = ads-hostname
```

```
pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
pkinit_kdc_hostname = ads-hostname
pkinit_eku_checking = kpServerAuth
}

[domain_realm]
.mydomain.com = MYDOMAIN.COMmydomain.com = MYDOMAIN.COM
```

将示例中的占位符值替换为您的网络配置特定的信息，如下表中所述。

占位符值	描述
mydomain.com	AD 域的 DNS 名称
MYDOMAIN.COM	AD 域的 DNS 名称（全部为大写字母）
ads-hostname	AD 服务器的主机名（区分大小写）

5 安装 Horizon Agent 软件包并启用 True SSO。

```
sudo ./install_viewagent.sh -T yes
```

注 要使用 True SSO 功能，您必须安装 Horizon Agent 7.8 或更高版本。

6 将以下参数添加到 Horizon Agent 自定义配置文件 /etc/vmware/viewagent-custom.conf 中。使用以下示例，其中，NETBIOS_NAME_OF_DOMAIN 是您的组织的域的 NetBIOS 名称。

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

7 重新引导系统，然后重新登录。

为 Linux 桌面设置图形

可以配置当前支持的 RHEL 分发版，以在 ESXi 主机或客户机操作系统上利用 NVIDIA 功能。

设置 3D 图形的虚拟机克隆要求

在设置 3D 图形之前，您必须考虑以下虚拟机克隆要求。

- 对于 vGPU 和 vSGA，在基础虚拟机上完成图形设置。克隆这些虚拟机。图形设置可用于克隆的虚拟机，无需执行进一步设置。
- 对于 vDGA，在基础虚拟机上完成图形设置。克隆这些虚拟机。但是，在打开克隆虚拟机的电源之前，您必须先从克隆的虚拟机中移除现有 NVIDIA 直通 PCI 设备，然后再向克隆的虚拟机中添加新的 NVIDIA 直通 PCI 设备。无法在虚拟机之间共享 NVIDIA 直通 PCI 设备。每个虚拟机都使用一个专用的 NVIDIA 直通 PCI 设备。

本章讨论了以下主题：

- 为 vGPU 配置支持的 RHEL 和 SLED 分发版
- 配置 RHEL 6 以使用 vDGA
- 为 RHEL 7.x 配置 vSGA

为 vGPU 配置支持的 RHEL 和 SLED 分发版

您可以设置支持的 RHEL 或 SLED 分发版，以在 ESXi 主机上利用 NVIDIA vGPU（共享的 GPU 硬件加速）功能。

您必须使用与 ESXi 主机 GPU 驱动程序 (.vib) 匹配的 NVIDIA Linux 虚拟机显卡驱动程序。有关驱动程序包的信息，请参阅 NVIDIA 网站。

重要事项 在 NVIDIA Tesla M6、M10、M60 和 P40 显卡上支持 NVIDIA vGPU。该功能在其他 NVIDIA 显卡（如 GRID K1 或 K2）上无法正常工作。

小心 在开始之前，请确认未在 Linux 虚拟机上安装 Horizon Agent。如果在配置计算机以使用 NVIDIA vGPU 之前安装 Horizon Agent，则会覆盖 xorg.conf 文件中的所需配置参数，并且 NVIDIA vGPU 无法正常工作。您必须在完成 NVIDIA vGPU 配置后安装 Horizon Agent。

为 ESXi 主机上的 NVIDIA GRID vGPU 显卡安装 VIB

您必须为 ESXi 6.0 U1 或更高版本的主机上的 NVIDIA GRID 显卡下载并安装 VIB。

NVIDIA 提供了一个包含 vGPU 管理器（在此步骤中安装到 ESXi 主机上）和 Linux 显卡驱动程序（在后面的步骤中安装到 Linux 虚拟机上）的 vGPU 软件包。

前提条件

- 确认在您的环境中安装了 vSphere 6.0 U1 或更高版本。
- 确认在 ESXi 主机上安装了 NVIDIA Tesla M6、M10、M60 或 P40 GPU。

步骤

- 1 从 [NVIDIA 驱动程序下载](#) 站点中下载用于 NVIDIA GRID vGPU 显卡的 VIB。

从下拉菜单中选择相应的 VIB 版本。

选项	说明
产品类型	GRID
产品系列	选择 NVIDIA GRID vGPU 。
产品	选择 ESXi 主机上安装的版本（例如 GRID K2 ）。
操作系统	选择 VMware vSphere ESXi 版本。

- 2 解压缩 vGPU 软件包 .zip 文件。
- 3 将 vGPU 管理器文件夹上载到 ESXi 主机中。

注 将在后面的步骤中在 Linux 虚拟机上安装 Linux 显卡驱动程序。

- 4 关闭电源或挂起 ESXi 主机上的所有虚拟机。
- 5 使用 SSH 连接到 ESXi 主机。
- 6 停止 xorg 服务。

```
# /etc/init.d/xorg stop
```

- 7 安装 NVIDIA VIB。

例如：

```
# esxcli system maintenanceMode set --enable true
# esxcli software vib install -v /path-to-vib/NVIDIA-VIB-name.vib
# esxcli system maintenanceMode set --enable false
```

8 重新引导或更新 ESXi 主机。

- ◆ 对于安装的 ESXi 主机，请重新引导该主机。
- ◆ 对于无状态 ESXi 主机，请执行以下步骤以更新该主机。（这些步骤也适用于安装的主机。）

```
Update vmkdevmgr:
# kill -HUP $(cat /var/run/vmware/vmkdevmgr.pid)

Wait for the update to complete:
# localcli --plugin-dir /usr/lib/vmware/esxcli/int deviceInternal bind

This is a new requirement with the NVIDIA 352.* host driver:
# /etc/init.d/nvidia-vgpu start

Restart xorg, which is used for GPU assignment:
# /etc/init.d/xorg start
```

9 在重新启动主机后，验证是否正在运行 xorg 服务。

在 Linux 虚拟机上为 vGPU 配置共享 PCI 设备

要使用 NVIDIA vGPU，您必须为 Linux 虚拟机配置共享 PCI 设备。

前提条件

- 确认准备好将 Linux 虚拟机作为桌面。请参阅[创建虚拟机并安装 Linux](#)和[为远程桌面部署准备 Linux 计算机](#)。
- 确认未在 Linux 虚拟机上安装 Horizon Agent。
- 确认在 ESXi 主机上安装了 NVIDIA VIB。请参阅[为 ESXi 主机上的 NVIDIA GRID vGPU 显卡安装 VIB](#)。
- 熟悉适用于 NVIDIA vGPU 的虚拟 GPU 类型，您可以通过 **GPU 配置文件** 设置进行选择。虚拟 GPU 类型在 ESXi 主机上安装的物理 GPU 中提供了各种不同的功能。请参阅[NVIDIA 虚拟 GPU 类型](#)。

步骤

- 1 关闭虚拟机的电源，
- 2 在 vSphere Web Client 中，选择虚拟机，然后在**虚拟机硬件**选项卡下，单击**编辑设置**。
- 3 在**新设备**菜单中，选择**共享 PCI 设备**。
- 4 单击**添加**，然后从下拉菜单中选择 **NVIDIA GRID vGPU**。
- 5 对于 **GPU 配置文件** 设置，请从下拉菜单中选择一种虚拟 GPU 类型。
- 6 单击**保留所有内存**，然后单击**确定**。

您必须保留所有虚拟机内存，以使 GPU 能够支持 NVIDIA GRID vGPU。

- 7 启动虚拟机。

NVIDIA 虚拟 GPU 类型

通过使用 vSphere Web Client 的“虚拟硬件”页中的 **GPU 配置文件** 设置，您可以选择一种虚拟 GPU 类型以在 ESXi 主机上的物理 NVIDIA GPU 中提供特定的功能。

在 Linux 虚拟机上，在 NVIDIA Tesla M60、M10、M60 或 P40 GPU 上支持 NVIDIA GRID vGPU。

表 4-1. 适用于 Linux 虚拟机上的 NVIDIA GRID M60 vGPU 的虚拟 GPU 类型

虚拟 GPU 类型	物理主板	物理 GPU	每个虚拟 GPU 的 FB 数	显示器数	最大分辨率	每个物理 GPU 的最大虚拟 GPU 数	每个物理主板的最大虚拟 GPU 数
GRID M60-1q	Tesla M60	2	1G	2	2560x1600	8	16
GRID M60-2q	Tesla M60	2	2G	4	2560x1600	4	8
GRID M60-4q	Tesla M60	2	4G	4	3840x2160	2	4
GRID M60-8q	Tesla M60	2	8G	4	3840x2160	1	2

表 4-2. 适用于 Linux 虚拟机上的 NVIDIA GRID M6 vGPU 的虚拟 GPU 类型

虚拟 GPU 类型	物理主板	物理 GPU	每个虚拟 GPU 的 FB 数	显示器数	最大分辨率	每个物理 GPU 的最大虚拟 GPU 数	每个物理主板的最大虚拟 GPU 数
GRID M6-1q	Tesla M6	1	1G	2	2560x1600	8	8
GRID M6-2q	Tesla M6	1	2G	4	2560x1600	4	4
GRID M6-4q	Tesla M6	1	4G	4	3840x2160	2	2
GRID M6-8q	Tesla M6	1	8G	4	3840x2160	1	1

表 4-3. 适用于 Linux 虚拟机上的 NVIDIA GRID M10 vGPU 的虚拟 GPU 类型

虚拟 GPU 类型	物理主板	物理 GPU	每个虚拟 GPU 的 FB 数	显示器数	最大分辨率	每个物理 GPU 的最大虚拟 GPU 数	每个物理主板的最大虚拟 GPU 数
GRID M10-1q	Tesla M10	4	1G	2	4096x2160	8	16
GRID M10-2q	Tesla M10	4	2G	4	4096x2160	4	8
GRID M10-4q	Tesla M10	4	4G	4	4096x2160	2	4
GRID M10-8q	Tesla M10	4	8G	4	4096x2160	1	2

表 4-4. 适用于 Linux 虚拟机上的 NVIDIA GRID P40 vGPU 的虚拟 GPU 类型

虚拟 GPU 类型	物理主板	物理 GPU	每个虚拟 GPU 的 FB 数	显示器数	最大分辨率	每个物理 GPU 的最大虚拟 GPU 数	每个物理主板的最大虚拟 GPU 数
GRID P40-1q	Tesla P40	1	1G	2	4096x2160	24	24
GRID P40-2q	Tesla P40	1	2G	4	4096x2160	12	12
GRID P40-3q	Tesla P40	1	3G	4	4096x2160	8	8

虚拟 GPU 类型	物理主板	物理 GPU	每个虚拟 GPU 的 FB 数	显示器数	最大分辨率	每个物理 GPU 的最大虚拟 GPU 数	每个物理主板的最大虚拟 GPU 数
GRID P40-4q	Tesla P40	1	4G	4	4096x2160	6	6
GRID P40-6q	Tesla P40	1	6G	4	5120x2880	4	4
GRID P40-8q	Tesla P40	1	8G	4	5120x2880	3	3
GRID P40-12q	Tesla P40	1	12G	4	5120x2880	2	4
GRID P40-24q	Tesla P40	1	24G	4	5120x2880	1	2

安装 NVIDIA GRID vGPU 显卡驱动程序

要安装 NVIDIA GRID vGPU 显卡驱动程序，您必须禁用默认 NVIDIA 驱动程序，下载 NVIDIA 显卡驱动程序，然后在虚拟机上配置 PCI 设备。

前提条件

- 确认您从 NVIDIA 下载站点中下载了 vGPU 软件包，解压缩该软件包，然后将 Linux 显卡驱动程序（一个软件包组件）准备就绪。请参阅[ESXi 主机上的 NVIDIA GRID vGPU 显卡安装 VIB](#)。

还要确认在虚拟机中添加了共享 PCI 设备。请参阅[Linux 虚拟机上为 vGPU 配置共享 PCI 设备](#)。

步骤

- 1 将 NVIDIA Linux 显卡驱动程序复制到虚拟机中。
- 2 打开虚拟机的远程终端，或通过键入 Ctrl-Alt-F2 切换到文本控制台，以 root 用户身份登录，然后运行 `init 3` 命令以禁用 X Windows。
- 3 安装 NVIDIA 驱动程序所需的其他组件。

```
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
```

- 4 为 NVIDIA GRID vGPU 驱动程序包添加可执行标记。

```
chmod +x NVIDIA-Linux-x86_64-version-grid.run
```

- 5 启动 NVIDIA GRID vGPU 安装程序。

```
sudo ./NVIDIA-Linux-x86_64-version-grid.run
```

- 6 接受 NVIDIA 软件许可协议，然后选择是以自动更新 X 配置设置。

后续步骤

在 Linux 虚拟机上安装 Horizon Agent。请参阅[Linux 虚拟机上安装 Horizon Agent](#)。

创建一个桌面池以包含配置的 Linux 虚拟机。请参阅[创建适用于 Linux 的手动桌面池](#)。

验证是否安装了 NVIDIA 显卡驱动程序

您可以在 Horizon 桌面会话中显示 NVIDIA 驱动程序输出，以验证是否在 Linux 虚拟机上安装了 NVIDIA 显卡驱动程序。

前提条件

- 确认安装了 NVIDIA 显卡驱动程序。
- 确认 Linux 虚拟机上安装了 Horizon Agent。请参阅[在 Linux 虚拟机上安装 Horizon Agent](#)。
- 确认在桌面池中部署了 Linux 虚拟机。请参阅[创建适用于 Linux 的手动桌面池](#)。

步骤

- 1 重新启动 Linux 虚拟机。

Horizon Agent 启动脚本将初始化 X 服务器和显示器拓扑。

您无法再通过 vSphere 控制台查看虚拟机显示器。

- 2 从 Horizon Client 中连接到 Linux 桌面。

- 3 在 Linux 桌面会话中，验证是否安装了 NVIDIA 显卡驱动程序。

打开终端窗口，运行 `glxinfo | grep NVIDIA` 命令。

此时将显示 NVIDIA 驱动程序输出。例如：

```
[root]# glxinfo | grep NVIDIA
server glx vendor string: NVIDIA Corporation
client glx vendor string: NVIDIA Corporation
OpenGL vendor string: NVIDIA Corporation
OpenGL version string: 4.5.0 NVIDIA 346.47
OpenGL shading language version string: 4.50 NVIDIA
```

用户可以在远程桌面上访问 NVIDIA 图形功能。

在确认已安装 NVIDIA 显卡驱动程序后，请执行以下任务来使安装的程序正常运行。

- 如果升级 Linux 内核，Horizon Agent 可能无法与 Horizon 连接服务器进行通信。要解决此问题，请重新安装 NVIDIA 驱动程序。
- 在 Linux 虚拟机中设置 NVIDIA GRID 许可。有关更多信息，请参阅 NVIDIA 文档。如果未设置许可，Linux 桌面将无法正常工作。例如，无法使用自动调整。

配置 RHEL 6 以使用 vDGA

您可以设置 RHEL 6 客户机操作系统，以便 Horizon 7 for Linux 桌面可以利用 ESXi 主机上的 vDGA 功能。

小心 在开始之前，请确认未在 Linux 虚拟机上安装 Horizon Agent。如果在配置计算机以使用 vDGA 之前安装 Horizon Agent，则会覆盖 `xorg.conf` 文件中的所需配置参数，并且 vDGA 无法正常工作。您必须在完成 vDGA 配置后安装 Horizon Agent。

在主机上为 NVIDIA GRID 启用 DirectPath I/O

在您将 Linux 虚拟机配置为使用 vDGA 之前，必须使 NVIDIA GRID GPU PCI 设备可用于 ESXi 主机上的 DirectPath I/O 传送。

前提条件

- 确认您的环境中安装了 vSphere 6.0 或更高版本。
- 确认 ESXi 主机上安装了 NVIDIA GRID K1 或 K2 显卡。

步骤

- 1 在 vSphere Web Client 中，浏览到 ESXi 主机。
- 2 单击**管理**选项卡，然后单击**设置**。
- 3 在“硬件”部分中，单击 **PCI 设备**。
- 4 要为 NVIDIA GRID GPU 启用 DirectPath I/O 传送，请单击**编辑**。

图标	说明
绿色图标	PCI 设备处于活动状态并且可以启用。
橙色图标	设备的状态已更改。您必须先重新引导主机，然后才能使用该设备。

- 5 选择 NVIDIA GRID GPU，然后单击**确定**。
PCI 设备将添加到表“可用于虚拟机的 DirectPath I/O PCI 设备”中。
- 6 重新引导主机，以便使 PCI 设备可用于 Linux 虚拟机。

向 RHEL 6 虚拟机添加 vDGA 直通设备

要将 RHEL 6 虚拟机配置为使用 vDGA，您必须向虚拟机添加 PCI 设备。通过此步骤，可以将 ESXi 主机上的物理设备进行传送，以便在虚拟机上使用。

前提条件

- 确认准备好将 Linux 虚拟机作为桌面。请参阅[创建虚拟机并安装 Linux](#)和[为远程桌面部署准备 Linux 计算机](#)。
- 确认未在 Linux 虚拟机上安装 Horizon Agent。
- 确认 NVIDIA GRID GPU PCI 设备在主机上可用于 DirectPath I/O 直通。请参阅[在主机上为 NVIDIA GRID 启用 DirectPath I/O](#)。

步骤

- 1 以配置有 sudo 权限的本地用户身份登录 RHEL 6 客户机操作系统。
- 2 在 vSphere Web Client 中，选择虚拟机，然后在**虚拟机硬件**选项卡下，单击**编辑设置**。
- 3 在**新设备**菜单中，选择 **PCI 设备**。
- 4 单击**添加**并从下拉菜单选择 PCI 设备。

- 5 单击**保留所有内存**，然后单击**确定**。

您必须保留所有虚拟机内存才能使 GPU 支持 vDGA。

- 6 打开虚拟机的电源，然后打开 vSphere 控制台以连接到计算机。

- 7 确认 NVIDIA GRID 设备已传送到虚拟机。

打开终端窗口，运行以下命令：

```
lspci | grep NVIDIA
```

此时会显示与 VGA 兼容的控制器 XX:00.0。例如：

```
NVIDIA Corporation GK104GL [GRID K2]
```

为 vDGA 安装 NVIDIA 显卡驱动程序

要为 vDGA 安装 NVIDIA 显卡驱动程序，您必须禁用默认 NVIDIA 驱动程序，下载 NVIDIA 显卡驱动程序，然后在虚拟机上配置 PCI 设备。

前提条件

- 确认已将 PCI 设备添加到 RHEL 6.x 虚拟机中。请参阅[向 RHEL 6 虚拟机添加 vDGA 直通设备](#)。

步骤

- 1 禁用默认的 NVIDIA Nouveau 驱动程序并将其列入黑名单。

- a 编辑 `grub.conf` 文件。

对于 RHEL 6，此文件是 `/boot/grub/grub.conf`。

RHEL 版本	命令
6	<code>sudo vi /boot/grub/grub.conf</code>

- b 在内核选项的末尾添加 `rdblacklist=nouveau` 行。

- c 编辑 `blacklist.conf` 文件。

```
sudo vi /etc/modprobe.d/blacklist.conf
```

- d 在 `blacklist.conf` 文件中的任意位置添加以下行。

```
blacklist nouveau
```

- 2 重新启动虚拟机。

显示器的外观将发生更改。

- 3 （可选） 确认已禁用 Nouveau 驱动程序。

```
/sbin/lsmmod | grep nouveau
```

如果 `grep` 搜索没有返回任何结果，则表示 Nouveau 驱动程序已被禁用。

- 4 从 [NVIDIA 驱动程序下载](#) 站点中下载 NVIDIA 驱动程序。

从 NVIDIA 下拉菜单中选择相应的驱动程序版本：

选项	说明
产品类型	GRID
产品系列	GRID 系列
产品	选择 ESXi 主机上安装的版本（例如 GRID K2 ）。
操作系统	Linux 64 位或 Linux 32 位

- 5 要连接到虚拟机，请打开远程终端，或键入 **Ctrl-Alt-F2** 以使用文本控制台，以 **root** 用户身份登录，然后运行 `init 3` 命令以禁用 X Windows。
- 6 安装 NVIDIA 驱动程序所需的其它组件。

```
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
```

- 7 为 vDGA 的 NVIDIA 驱动程序包添加可执行标记。

```
chmod +x NVIDIA-Linux-x86_64-version.run
```

- 8 运行 NVIDIA 安装程序。

```
sudo ./NVIDIA-Linux-x86_64-version.run
```

- 9 接受 NVIDIA 软件许可协议，然后选择 **是** 以更新 X 配置设置。

后续步骤

在 Linux 虚拟机上安装 Horizon Agent。请参阅[在 Linux 虚拟机上安装 Horizon Agent](#)。

创建一个桌面池以包含配置的 Linux 虚拟机。请参阅[创建适用于 Linux 的手动桌面池](#)。

验证是否安装了 NVIDIA 显卡驱动程序

您可以在 Horizon 桌面会话中显示 NVIDIA 驱动程序输出，以验证是否在 Linux 虚拟机上安装了 NVIDIA 显卡驱动程序。

前提条件

- 确认安装了 NVIDIA 显卡驱动程序。
- 确认 Linux 虚拟机上安装了 Horizon Agent。请参阅[在 Linux 虚拟机上安装 Horizon Agent](#)。

- 确认在桌面池中部署了 Linux 虚拟机。请参阅[创建适用于 Linux 的手动桌面池](#)。

步骤

- 1 重新启动 Linux 虚拟机。

Horizon Agent 启动脚本将初始化 X 服务器和显示器拓扑。

您无法再通过 vSphere 控制台查看虚拟机显示器。

- 2 从 Horizon Client 中连接到 Linux 桌面。

- 3 在 Linux 桌面会话中，验证是否安装了 NVIDIA 显卡驱动程序。

打开终端窗口，运行 `glxinfo | grep NVIDIA` 命令。

此时将显示 NVIDIA 驱动程序输出。例如：

```
[root]# glxinfo | grep NVIDIA
server glx vendor string: NVIDIA Corporation
client glx vendor string: NVIDIA Corporation
OpenGL vendor string: NVIDIA Corporation
OpenGL version string: 4.5.0 NVIDIA 346.47
OpenGL shading language version string: 4.50 NVIDIA
```

用户可以在远程桌面上访问 NVIDIA 图形功能。

在确认已安装 NVIDIA 显卡驱动程序后，请执行以下任务来使安装的程序正常运行。

- 如果升级 Linux 内核，Horizon Agent 可能无法与 Horizon 连接服务器进行通信。要解决此问题，请重新安装 NVIDIA 驱动程序。
- 在 Linux 虚拟机中设置 NVIDIA GRID 许可。有关更多信息，请参阅 NVIDIA 文档。如果未设置许可，Linux 桌面将无法正常工作。例如，无法使用自动调整。

为 RHEL 7.x 配置 vSGA

您可以设置 RHEL 7.x 客户机操作系统，以便 Horizon 7 for Linux 桌面可以利用 vSGA 功能。

为 ESXi 主机上用于 vSGA 的 NVIDIA 显卡安装 VIB

您必须为 ESXi 6.0 U1 或更高版本的主机上的 NVIDIA GRID 显卡下载并安装 VIB。

NVIDIA 提供了用于 vSGA 的 VMware vSphere ESXi 驱动程序。对于 vSGA，不会在 Linux 虚拟机上安装 NVIDIA 显卡驱动程序。

前提条件

- 确认在您的环境中安装了 vSphere 6.0 U1 或更高版本。
- 确认在您的环境中安装了 NVIDIA 驱动程序。
- 确认在 ESXi 主机上安装了 NVIDIA GRID K1 或 K2 GPU。

步骤

- 1 从 [NVIDIA 驱动程序下载](#) 站点中下载用于 NVIDIA GRID vGPU 显卡的 VIB。

从下拉菜单中选择相应的 VIB 版本。

选项	说明
产品类型	GRID
产品系列	选择 GRID 系列。
产品	选择 ESXi 主机上安装的版本（例如 GRID K2 ）。
操作系统	选择 VMware vSphere ESXi 版本。

- 2 将用于 vSGA 的 VMware vSphere ESXi 驱动程序上载到 ESXi 6.0 U1 主机中。
- 3 关闭电源或挂起 ESXi 主机上的所有虚拟机。
- 4 使用 SSH 连接到 ESXi 主机。
- 5 停止 xorg 服务。

```
# /etc/init.d/xorg stop
```

- 6 安装 NVIDIA VIB。

例如：

```
# esxcli system maintenanceMode set --enable true
# esxcli software vib install -v /path-to-vib/NVIDIA-VIB-name.vib
# esxcli system maintenanceMode set --enable false
```

- 7 重新启动 xorg（用于 GPU 分配）：

```
# /etc/init.d/xorg start
```

- 8 重新引导 ESXi 主机。
- 9 在重新启动主机后，验证是否正在运行 xorg 服务。

在 Linux 虚拟机上为 vSGA 配置 3D 功能

要配置 RHEL 7 虚拟机以使用 vSGA，您必须在 vSphere Web Client 中为虚拟机显卡配置 3D 设置。

前提条件

- 确认 Linux 虚拟机已准备好用作桌面，已安装 Horizon Agent，并且已在桌面池中部署计算机。
- 确认在 ESXi 主机上安装了 NVIDIA VIB。请参阅[为 ESXi 主机上用于 vSGA 的 NVIDIA 显卡安装 VIB](#)。

步骤

- 1 关闭虚拟机的电源，

- 2 在 vSphere Web Client 中，选择虚拟机，然后在**虚拟机硬件**选项卡下，单击**编辑设置**。
- 3 在“虚拟硬件”选项卡中，单击**显卡**以展开菜单设置。
- 4 将**总显存**设置为 128 MB。
- 5 对于 **3D 图形**，请选择**启用 3D 支持**。
- 6 对于 **3D 呈现器**，请从下拉菜单中选择**硬件**。
- 7 对于 **3D 显存**，请选择符合您的应用程序要求的值。
如果您的用户连接到超过 3 个显示器，请将该值设置为至少 1024 MB。
- 8 单击**确定**。
- 9 打开虚拟机电源。

后续步骤

验证是否正在 Linux 虚拟机上运行 vSGA。

接下来，在 Linux 虚拟机上安装 Horizon Agent。请参阅[在 Linux 虚拟机上安装 Horizon Agent](#)。

验证是否正在 Linux 虚拟机上运行 vSGA

您可以检查虚拟机日志文件和客户机操作系统以验证是否正在 RHEL 7 虚拟机上运行 vSGA。

步骤

- 1 打开虚拟机的 `vmware.log` 文件。

如果正确安装了支持的 GPU 和 NVIDIA VIB，日志文件将显示类似以下示例中的行：

```
2015-06-24T22:19:25.259Z| mks| I120: OpenGL Version: "4.0.0 NVIDIA 346.69" (4.0.0)
2015-06-24T22:19:25.259Z| mks| I120: GLSL Version: "4.00 NVIDIA" (4.00.0)
2015-06-24T22:19:25.259Z| mks| I120: OpenGL Vendor: "NVIDIA Corporation"
2015-06-24T22:19:25.259Z| mks| I120: OpenGL Renderer: "Quadro 4000/PCIe/SSE2"
```

如果未正确安装支持的 GPU 和 NVIDIA VIB，则虚拟机使用软件呈现器。`vmware.log` 文件显示类似以下示例中的行：

```
2015-07-06T17:09:26.423Z| vmx| I120: [msg.mks.noGPUResourceFallback] Hardware GPU resources are
not available. The virtual machine uses software rendering.
2015-07-06T17:09:26.423Z| vmx| I120: -----
2015-07-06T17:09:26.425Z| svga| I120: MKS-SWP: plugin started - llvmpipe (LLVM 3.3, 256 bits)
2015-07-06T17:09:26.426Z| svga| I120: Started Shim3D
2015-07-06T17:09:26.426Z| svga| I120: MKS-RenderMain: Starting SWRenderer
```

- 2 在虚拟机上的客户机操作系统中，键入以下命令。

```
glxinfo|grep Gallium
```

如果 vSGA 正常工作，该命令将返回以下文本：

```
OpenGL renderer string: Gallium 0.4 on SVGA3D; build : RELEASE;
```

如果 vSGA 无法正常工作，该命令将返回以下文本：

```
OpenGL renderer string: Gallium 0.4 on llvmpipe (LLVM 3.3, 256 bits)
```

后续步骤

在 Linux 虚拟机上安装 Horizon Agent。请参阅[在 Linux 虚拟机上安装 Horizon Agent](#)。

安装 Horizon Agent

您必须在 Linux 桌面上安装 Horizon Agent，这样 Horizon Connection Server 才能与桌面通信并管理桌面。

本章讨论了以下主题：

- 在 Linux 虚拟机上安装 Horizon Agent
- 配置 Linux 代理的证书
- 在 Linux 虚拟机上升级 Horizon Agent
- 卸载 Horizon 7 for Linux 计算机

在 Linux 虚拟机上安装 Horizon Agent

您必须先在 Linux 虚拟机上安装 Horizon Agent，然后才能将该虚拟机部署为远程桌面。

从 Horizon 7.0.1 版本开始，Horizon Agent for Linux 使用受 vCenter 管理的虚拟机。受管虚拟机提供以下增强功能。

- Linux 桌面部署强制要求使用 vCenter。
- 在 Linux 上安装 Horizon Agent 不需要注册。
- 如需部署大量 Linux 桌面，可以将 Horizon Agent 安装在基础虚拟机上。

小心 如果要使用 NVIDIA GRID vGPU、vDGA 或 vSGA，必须先在 Linux 虚拟机上配置这些 3D 功能，然后再安装 Horizon Agent。如果先安装 Horizon Agent，则会覆盖 `xorg.conf` 文件中的所需参数，并且 3D 图形功能无法正常工作。

请参阅[为 vGPU 配置支持的 RHEL 和 SLED 分发](#)、[配置 RHEL 6 以使用 vDGA](#) 或为 RHEL 7.x 配置 [vSGA](#)。在 3D 图形配置完成后，安装 Horizon Agent。

对于 2D 图形配置，您可以在完成[为远程桌面部署准备 Linux 计算机](#)中的步骤后安装 Horizon Agent。

前提条件

- 确认已准备好 Linux 客户机操作系统以供桌面使用。请参阅[为远程桌面部署准备 Linux 计算机](#)。
- 熟悉用于 Linux 的 Horizon Agent 安装程序脚本。请参阅 [install_viewagent.sh](#) 命令行选项。

步骤

- 1 从 VMware 下载站点 <https://my.vmware.com/web/vmware/downloads> 下载 Horizon Agent for Linux 安装程序文件。

在“桌面和最终用户计算”部分，选择“查看 VMware Horizon 的下载组件”。在“Horizon 7 for Linux”下，选择适用于 64 位 Linux 系统的 VMware Horizon 7 所对应的“下载”页面。

对于 64 位 Linux，安装程序文件名为 `VMware-horizonagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz`，其中 `y.y.y` 是版本号，`xxxxxxx` 是内部版本号。

- 2 在客户机操作系统上解压缩 Linux 分发包的 tarball。

例如：

```
tar -xzf VMware-horizonagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz
```

- 3 浏览到 tar ball 文件夹。
- 4 以超级用户身份运行 `install_viewagent.sh` 脚本。

请参阅 [install_viewagent.sh 命令行选项](#)，获取命令行选项列表。

例如：

```
sudo ./install_viewagent.sh
```

- 5 如果您运行 `install_viewagent.sh` 而未指定 `-A` 选项，请键入 **Yes** 以接受 EULA。
- 6 重新引导 Linux 以使更改生效。

安装后，将启动 `viewagent` 服务。可使用 `sudo service viewagent status` 确认此服务已经启动。

后续步骤

在桌面池中部署虚拟机。请参阅[创建适用于 Linux 的手动桌面池](#)。

install_viewagent.sh 命令行选项

`install_viewagent.sh` 脚本在 Linux 客户机操作系统上安装 Horizon Agent。

在 `gnome` 桌面环境中的命令窗口中使用以下形式的 `install_viewagent.sh` 脚本。

```
install_viewagent.sh command_option argument [command_option argument] . . .
```

`install_viewagent.sh` 脚本包括必需参数和可选参数。

表 5-1. install_viewagent.sh 可选但必需的参数

可选参数（必需信息）	说明
-A yes no	接受或拒绝最终用户许可协议 (End User License Agreement, EULA) 和联邦信息处理标准 (FIPS) 声明。您必须指定 yes 才能继续进行安装。

表 5-2. install_viewagent.sh 可选参数

可选参数	描述
-a yes no	安装或绕过音频输入重定向支持。默认值为 yes 。
-f yes no	安装或绕过为联邦信息处理标准 (FIPS) 140-2 设计的加密模块支持。默认值为 no 。有关详细信息，请参阅 Horizon Linux 桌面的功能 中的 FIPS 140-2 模式描述。
-j	JMS SSL 密钥库密码。默认情况下，安装程序将生成一个随机字符串。
-m yes no	安装或绕过智能卡重定向支持。默认值为 no 。
-r yes no	在安装后自动重新启动系统。默认值为 no 。
-s	自签名证书主体 DN。默认情况下，安装程序将使用 Blast。
-C yes no	安装或绕过剪贴板重定向支持。默认值为 yes 。
-F yes no	安装或绕过 CDR 支持。默认值为 yes 。
-M yes no	将 Linux 代理升级为受管或未受管的代理。默认值为 yes 。
-S yes no	安装或绕过单点登录 (SSO) 支持。默认值为 yes 。
-T yes no	安装或绕过 True 单点登录 (True SSO) 支持。默认值为 no 。
-U yes no	安装或绕过 USB 支持。默认值为 no 。

表 5-3. install_viewagent.sh 参数的示例

条件	示例
全新安装	<pre>sudo ./install_viewagent.sh -A yes</pre> <p>全新安装始终需要创建新桌面池。</p>
从未受管虚拟机升级，并保留未受管虚拟机样式	<pre>sudo ./install_viewagent.sh -A yes-M no</pre> <p>此类型的升级不需要创建新桌面池。您可以重用现有的桌面池。</p> <p>注 要确保尽可能获得最佳性能，请勿使用未受管的虚拟机。</p>
从未受管虚拟机部署升级并转换为受管虚拟机样式。该升级需要在代理上创建新桌面池	<pre>sudo ./install_viewagent.sh -A yes</pre> <p>此类型的升级需要创建新桌面池。您必须删除现有的桌面池。</p>

配置 Linux 代理的证书

安装 Linux 代理时，安装程序会为 VMwareBlastServer 生成一个自签名证书。

- 在代理上禁用 Blast 安全网关后，VMwareBlastServer 会向使用 HTML Access 连接到 Linux 桌面的浏览器提供该证书。

- 在代理上启用 **Blast** 安全网关后，**Blast** 安全网关的证书会将该证书提供给浏览器。

为了遵循行业或安全法规，您可以将该自签名证书替换为由证书颁发机构 (Certificate Authority, CA) 签名的证书。

步骤

- 1 向 **VMwareBlastServer** 安装私有密钥和证书。
 - a 将私有密钥重命名为 **rui.key**，将证书重命名为 **rui.crt**。
 - b 运行 `sudo chmod 550 /etc/vmware/ssl`。
 - c 将 **rui.crt** 和 **rui.key** 复制到 **/etc/vmware/ssl**。
 - d 运行 `chmod 440 /etc/vmware/ssl`。
- 2 将根和中间证书颁发机构安装到 Linux 操作系统证书颁发机构存储中。

注 查看您的 Linux 分发包文档，了解 Linux 系统设置更改信息。

在 Linux 虚拟机上升级 Horizon Agent

您可以通过安装最新版本的 **Horizon Agent** 来升级 Linux 虚拟机上的 **Horizon Agent**。

未受管虚拟机：代理安装程序将该虚拟机注册到需要代理管理员信息的代理。**桌面池创建**向导使用“计算机源”页面中的**其他源**来选择已注册的虚拟机。

受管虚拟机：安装程序不与代理通信。**桌面池创建**向导使用“计算机源”页面中的**vCenter 虚拟机**来通过 **vCenter** 选择虚拟机。受管虚拟机部署支持以下功能。

- 远程计算机电源策略
- 允许用户重置其计算机

注 **Horizon Agent for Linux 7.0.0** 及更低版本作为未受管虚拟机来运行。**Horizon Agent for Linux 7.0.1** 作为受管虚拟机支持来运行。

您可以使用以下方法从未受管虚拟机部署升级到受管虚拟机部署。

- 保留未受管虚拟机部署并升级到所需的版本。此类型的升级不需要在 **Horizon Connection Server** 中修改任何配置。
- 从未受管虚拟机部署升级到受管虚拟机部署的任何版本。此类型的升级需要在 **Horizon Connection Server** 上创建新桌面池。

注 对于从受管虚拟机部署进行的升级，您可以保留受管虚拟机部署并升级到所需的版本。但是，不支持在升级过程中将受管虚拟机部署转换为未受管虚拟机部署。

以下参数可用于升级。

表 5-4. 用于 Horizon Agent 升级的可选参数

参数	说明
-A yes	EULA 和 FIPS 声明接受。您必须指定 yes 才能继续进行安装。如果未指定该参数，安装脚本将提示输入该值。
-a yes no	安装或绕过音频输入重定向支持。
-f yes no	安装或绕过为联邦信息处理标准 (FIPS) 140-2 设计的加密模块支持。默认值为 no 。有关详细信息，请参阅 Horizon Linux 桌面的功能 中的 FIPS 140-2 模式描述。
-m yes no	安装或绕过智能卡重定向支持。默认值为 no 。
-r yes no	安装后重新引导操作系统。默认值为 no 。
-C yes no	安装或绕过剪贴板重定向支持。默认值为 yes 。
-F yes no	安装或绕过 CDR 支持。默认值为 yes 。
-M yes no	将 Linux 代理升级为受管 未受管代理。默认值为 yes 。
-S yes no	安装或绕过单点登录 (SSO) 支持。默认值为 yes 。
-U yes no	安装或绕过 USB 支持。默认值为 no 。

在 Linux 虚拟机上升级 Horizon Agent

您可以通过安装最新版本的 Horizon Agent 来升级 Linux 计算机上的 Horizon Agent。

前提条件

- 确认 VMwareBlastServer 进程未运行。

要停止该进程，请确保用户注销计算机并且没有活动的桌面会话，或者重新引导计算机。

步骤

- 1 从 VMware 下载站点下载最新的 Horizon Agent for Linux 安装程序文件，网址为 <https://my.vmware.com/web/vmware/downloads>。

在“桌面和最终用户计算”下面，选择以下载 VMware Horizon 7，其中包括 Horizon Agent for Linux 安装程序。

对于 64 位 Linux，安装程序文件名为 VMware-viewagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz，其中 y.y.y 是版本号，xxxxxxx 是内部版本号。

- 2 在客户机操作系统上解压缩 Linux 分发包的 tarball。

例如：

```
tar -xzf <Horizon Agent tar ball>
```

- 3 浏览到 tar ball 文件夹。

- 4 要升级未受管虚拟机，请使用以下部署方案之一运行 `install_viewagent.sh` 脚本。

选项	说明
升级未受管虚拟机部署并保留未受管虚拟机部署	<pre>sudo ./install_viewagent.sh -A yes -M no</pre> <p>注 要确保尽可能获得最佳性能，请勿使用未受管的虚拟机。</p>
升级未受管虚拟机部署并将其更改为受管虚拟机部署	<pre>sudo ./install_viewagent.sh -A yes -M yes</pre> <p>注 在 Horizon Administrator 中，为未受管虚拟机部署删除现有的桌面池，并为受管虚拟机部署创建一个桌面池。有关更多信息，请参阅创建适用于 Linux 的手动桌面池。</p>
升级受管虚拟机部署	<pre>sudo ./install_viewagent.sh -A yes -M yes</pre> <p>注 升级后，可以重用您的现有桌面池。</p>

卸载 Horizon 7 for Linux 计算机

要卸载虚拟机上的 Horizon 7 for Linux，您必须卸载 Horizon Agent 并移除配置文件。

前提条件

确认 VMwareBlastServer 进程未运行。要停止该进程，请确保您注销计算机并且没有活动的桌面会话，或者重新引导计算机。

步骤

- 1 在虚拟机上打开终端窗口，然后运行 Horizon Agent 卸载脚本。

```
sudo /usr/lib/vmware/viewagent/bin/uninstall_viewagent.sh
```

此脚本将停止 Horizon Agent 进程，并从安装目录 `/usr/lib/vmware/viewagent` 中删除 Horizon Agent 服务和软件。

- 2 手动删除位于 `/etc/vmware` 目录下的 Horizon 7 for Linux 配置文件。

Linux 桌面的配置选项

您可以使用配置文件配置各种选项，以便自定义用户体验。

本章讨论了以下主题：

- 在 Linux 桌面上的配置文件中设置选项
- 使用 智能策略
- 适用于 Linux 桌面的 Blast 设置示例
- 适用于 Linux 桌面的客户端驱动器重定向选项示例
- 禁止在 vSphere 控制台中显示 Linux 桌面

在 Linux 桌面上的配置文件中设置选项

您可以向文件 `/etc/vmware/config` 或 `/etc/vmware/viewagent-custom.conf` 添加条目，以配置某些选项。

在 Horizon Agent 的安装过程中，安装程序将两个配置模板文件 `config.template` 和 `viewagent-custom.conf.template` 复制到 `/etc/vmware` 中。此外，如果 `/etc/vmware/config` 和 `/etc/vmware/viewagent-custom.conf` 不存在，安装程序会将 `config.template` 复制到 `config`，并将 `viewagent-custom.conf.template` 复制到 `viewagent-custom.conf`。在模板文件中会列出并记录所有配置选项。要设置某个选项，只需移除注释和更改相关值即可。

例如，`/etc/vmware/config` 中的以下行用于启用构建无损 PNG 模式。

```
RemoteDisplay.buildToPNG=TRUE
```

在进行配置更改后，重新引导 Linux 以使更改生效。

`/etc/vmware/config` 中的配置选项

VMwareBlastServer 及其相关插件使用配置文件 `/etc/vmware/config`。

注 下表介绍了 Horizon Agent 配置文件中的各个代理强制执行的 USB 策略设置。Horizon Agent 使用这些设置确定是否能够将 USB 转发至主机。Horizon Agent 还会将这些设置传递到 Horizon Client 进行解释和执行。根据您是指定合并 (m) 修改符以同时应用 Horizon Agent 筛选策略设置和 Horizon Client 筛选策略设置，还是覆盖 (o) 修改符以使用 Horizon Agent 筛选策略设置而不使用 Horizon Client 筛选策略设置来执行。

表 6-1. /etc/vmware/config 中的配置选项

选项	值/格式	默认	说明
Clipboard.Direction	0, 1, 2, 或 3	2	使用该选项指定剪贴板重定向策略。有效值如下： <ul style="list-style-type: none"> ■ 0 - 禁用剪贴板重定向。 ■ 1 - 启用双向剪贴板重定向。 ■ 2 - 仅启用从客户端到远程桌面的剪贴板重定向。 ■ 3 - 仅启用从远程桌面到客户端的剪贴板重定向。
RemoteDisplay.allowAudio	true 或 false	true	设置该选项以启用/禁用音频输出。
RemoteDisplay.allowH264	true 或 false	true	设置该选项以启用或禁用 H.264 编码。
RemoteDisplay.buildToPNG	true 或 false	false	图形应用程序（尤其是图形设计应用程序）要求图像在 Linux 桌面的客户端显示器中呈现时精确至像素级别。您可以为 Linux 桌面上生成并在客户端设备上呈现的图像和视频回放配置无损构建 PNG 模式。该功能会占用客户端与 ESXi 主机之间额外的带宽。启用该选项将禁用 H.264 编码。
RemoteDisplay.enableNetworkContinuity	true 或 false	true	设置该选项以在 Horizon Agent for Linux 中启用或禁用持续网络连接功能。
RemoteDisplay.enableNetworkIntelligence	true 或 false	true	设置该选项以在 Horizon Agent for Linux 中启用或禁用网络智能功能。
RemoteDisplay.enableStats	true 或 false	false	启用或禁用 mks 日志中的 VMware Blast 显示协议统计信息，例如带宽、FPS、RTT 等。
RemoteDisplay.enableUDP	true 或 false	true	设置该选项以在 Horizon Agent for Linux 中启用或禁用 UDP 协议支持。
RemoteDisplay.maxBandwidthKbps	整数	1000000	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、虚拟通道以及 VMware Blast 控制流量。有效值必须小于 4 Gbps (4096000)。
RemoteDisplay.minBandwidthKbps	整数	256	指定 VMware Blast 会话的最小带宽，以千比特/秒 (kbps) 为单位。此带宽包括所有图像处理、音频、虚拟通道以及 VMware Blast 控制流量。
RemoteDisplay.maxFPS	整数	60	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。有效值必须介于 3 和 60 之间。默认值为每秒更新 60 次。
RemoteDisplay.maxQualityJPEG	可用值范围：1-100	90	指定使用 JPEG/PNG 编码时桌面显示的图像质量。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。
RemoteDisplay.midQualityJPEG	可用值范围：1-100	35	指定使用 JPEG/PNG 编码时桌面显示的图像质量。用于设置桌面显示的中等质量设置。
RemoteDisplay.minQualityJPEG	可用值范围：1-100	25	指定使用 JPEG/PNG 编码时桌面显示的图像质量。低质量设置用于经常变化的屏幕区域，例如，发生滚动时。
RemoteDisplay.qpmaxH264	可用值范围：0-51	36	使用此选项可设置 H264minQP 量化参数，该参数用来为配置为使用 H.264 编码的远程显示指定最佳图像质量。应将该值设置为大于为 RemoteDisplay.qpminH264 设置的值。

选项	值/格式	默认	说明
RemoteDisplay.qpminH264	可用值范围: 0-51	10	使用此选项可设置 H264maxQP 量化参数, 该参数用来为配置为使用 H.264 编码的远程显示指定最低图像质量。应将该值设置为小于为 RemoteDisplay.qpmaxH264 设置的值。
UsbRedirPlugin.log.logLevel	error、warn、info、debug、trace 或 verbose	info	使用该选项设置 USB 重定向插件的日志级别。
UsbRedirServer.log.logLevel	error、warn、info、debug、trace 或 verbose	info	使用该选项设置 USB 重定向服务器的日志级别。
VMWPkcs11Plugin.log.enable	true 或 false	false	设置该选项为 True SSO 功能启用或禁用日志记录模式。
VMWPkcs11Plugin.log.logLevel	error、warn、info、debug、trace 或 verbose	info	使用该选项为 True SSO 功能设置日志级别。
VVC.RTAV.Enable	true 或 false	true	设置该选项以启用/禁用音频输入。
VVC.ScRedir.Enable	true 或 false	true	设置该选项以启用/禁用智能卡重定向。
VVC.logLevel	fatal error、warn、info、debug 或 trace	info	使用该选项设置 VVC 代理节点的日志级别。
cdrserver.cacheEnable	true 或 false	true	设置该选项以启用或禁用从代理向客户端的写入缓存功能。
cdrserver.forcedByAdmin	true 或 false	false	设置该选项以控制客户端是否可以共享未通过 cdrserver.shareFolders 选项指定的其他文件夹。
cdrserver.logLevel	error、warn、info、debug、trace 或 verbose	info	使用该选项设置 vmware-CDRserver.log 文件的日志级别。
cdrserver.permissions	R	RW	<p>使用该选项应用 Horizon Agent 对 Horizon Client 共享的文件夹具有的额外读取/写入权限。例如:</p> <ul style="list-style-type: none"> ■ 如果 Horizon Client 共享的文件夹具有 read 和 write 权限, 而您设置了 cdrserver.permissions=R, 则 Horizon Agent 只具有 read 访问权限。 ■ 如果 Horizon Client 共享的文件夹只具有 read 权限, 而您设置了 cdrserver.permissions=RW, 则 Horizon Agent 仍然只具有 read 访问权限。Horizon Agent 无法更改 Horizon Client 设置的仅 read 属性。Horizon Agent 只能移除写入访问权限。 <p>典型用法如下:</p> <ul style="list-style-type: none"> ■ cdrserver.permissions=R ■ #cdrserver.permissions=R (例如, 将其注释掉或删除该条目)

选项	值/格式	默认	说明
cdserver.sharedFolders	<i>file_path1,R; file_path2,; file_path3,R; . . .</i>	未定义	指定客户端可与 Linux 桌面共享的一个或多个文件夹的文件路径。例如： <ul style="list-style-type: none"> ■ 对于 Windows 客户端： C:\spreadsheets,;D:\ebooks,R ■ 对于非 Windows 客户端： /tmp/spreadsheets;/tmp/ebooks,;/home/finance,R
collaboration.logLevel	error、info 或 debug	info	使用此选项设置协作会话所使用的日志级别。如果日志级别为 debug ，则会记录对 collabui 函数和 collabor 列表内容进行的所有调用。
collaboration.maxCollabors	小于 10 的整数	5	指定可邀请加入会话的协作者的最大数量。
collaboration.enableEmail	true 或 false	true	设置该选项以允许或禁止通过已安装的电子邮件应用程序发送协作邀请。如果禁用该选项，您无法使用电子邮件邀请协作者，即使安装了电子邮件应用程序。
collaboration.serverUrl	[URL]	未定义	指定要包含在协作邀请中的服务器 URL。
collaboration.enableControlPassing	true 或 false	true	设置该选项以允许或限制协作者控制 Linux 桌面。要指定只读协作会话，请将该选项设置为 false 。
mksVNCServer.useUInputButtonMapping	true 或 false	false	设置该选项以在 Ubuntu 或 RHEL 7 上启用左手鼠标支持。CentOS 和 RHEL 6 支持左手鼠标，您不需要设置该选项。
mksVNCServer.useXExtButtonMapping	true 或 false	false	设置该选项以在 SLED 11 SP3 上启用或禁用左手鼠标支持。
mksvhan.clipboardSize	整数	1024	使用该选项指定用于复制和粘贴操作的剪贴板最大大小。
vdpserver.log.logLevel	fatal error、warn、info、debug 或 trace	info	使用该选项设置 vdpserver 的日志级别。
viewusb.AllowAudioIn	{m o}: {true false}	未定义，等同于 true	使用该选项允许或禁止对音频输入设备进行重定向。示例： o:false
viewusb.AllowAudioOut	{m o}: {true false}	未定义，等同于 false	设置该选项以允许或禁止对音频输出设备进行重定向。
viewusb.AllowAutoDeviceSplitting	{m o}: {true false}	未定义，等同于 false	设置该选项以允许或禁止自动拆分复合 USB 设备。 示例： m:true
viewusb.AllowDevDescFailsafe	{m o}: {true false}	未定义，等同于 false	设置该选项以便即使在 Horizon Client 未能获取配置或设备描述符时，也允许或禁止对设备进行重定向。要在设备未能获取配置或设备描述符时仍然允许对其进行重定向，可将该设备包含在 Include 筛选器中，例如 IncludeVidPid 或 IncludePath 。
viewusb.AllowHIDBootable	{m o}: {true false}	未定义，等同于 true	使用该选项允许或禁止对引导时除键盘或鼠标之外的其他可用输入设备（又称为可引导的 HID 设备）进行重定向。
viewusb.AllowKeyboardMouse	{m o}: {true false}	未定义，等同于 false	使用该选项允许或禁止对键盘以及集成指针设备（例如，鼠标、轨迹球或触摸板）进行重定向。

选项	值/格式	默认	说明
viewusb.AllowSmartcard	{m o}: {true false}	未定义，等同于 false	设置该选项以允许或禁止对智能卡设备进行重定向。
viewusb.AllowVideo	{m o}: {true false}	未定义，等同于 true	使用该选项允许或禁止对视频设备进行重定向。
viewusb.DisableRemoteConfig	{m o}: {true false}	未定义，等同于 false	设置该选项以禁止或允许在执行 USB 设备筛选时使用 Horizon Agent 设置。
viewusb.ExcludeAllDevices	{true false}	未定义，等同于 false	使用该选项在重定向中排除或包含所有 USB 设备。如果设置为 true ，可以使用其他策略设置来允许对特定设备或设备系列进行重定向。如果设置为 false ，可以使用其他策略设置来禁止对特定设备或设备系列进行重定向。如果将 Horizon Agent 上的 ExcludeAllDevices 值设置为 true ，并将该设置传递到 Horizon Client，Horizon Agent 设置将覆盖 Horizon Client 设置。
viewusb.ExcludeFamily	{m o}: <i>family_name_1</i> ; <i>family_name_2</i> ;...	未定义	<p>使用该选项从重定向中排除设备系列。例如： m:bluetooth;smart-card</p> <p>如果启用了自动设备拆分，Horizon 将检查复合 USB 设备的每个接口的设备系列，以确定必须排除哪些接口。如果禁用了自动设备拆分，Horizon 将检查整个复合 USB 设备的设备系列。</p> <p>注 默认情况下会从重定向中排除鼠标和键盘，因而不需要使用此设置来排除这些设备。</p>
viewusb.ExcludePath	{m o}: <i>bus-x1</i> [/ <i>y1</i>].../ <i>port-z1</i> ; <i>bus-x2</i> [/ <i>y2</i>].../ <i>port-z2</i> ;...	未定义	<p>使用该选项从重定向中排除位于指定集线器或端口路径的设备。您必须以十六进制格式指定总线和端口号。在路径中不能使用通配符。</p> <p>例如： m:bus-1/2/3_port- 02;bus-1/1/4_port-ff</p>
viewusb.ExcludeVidPid	{m o}: <i>vid-xxx1</i> <i>pid-yyy1</i> ; <i>vid-xxx2</i> <i>pid-yyy2</i> ;...	未定义	<p>设置该选项以从重定向中排除具有指定供应商和产品 ID 的设备。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-0781_pid- ****;vid-0561_pid-554c</p>
viewusb.IncludeFamily	{m o}: <i>family_name_1</i> ; <i>family_name_2</i> ...	未定义	<p>设置该选项以包含可重定向的设备系列。</p> <p>例如：o:storage; smart-card</p>
viewusb.IncludePath	{m o}: <i>bus-x1</i> [/ <i>y1</i>].../ <i>port-z1</i> ; <i>bus-x2</i> [/ <i>y2</i>].../ <i>port-z2</i> ;...	未定义	<p>使用该选项包含位于指定集线器或端口路径的可重定向设备。您必须以十六进制格式指定总线和端口号。在路径中不能使用通配符。</p> <p>例如：m:bus-1/2_port- 02;bus-1/7/1/4_port-0f</p>
viewusb.IncludeVidPid	{m o}: <i>vid-xxx1</i> <i>pid-yyy1</i> ; <i>vid-xxx2</i> <i>pid-yyy2</i> ;...	未定义	<p>设置该选项以包含具有指定供应商和产品 ID 的可重定向设备。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-***_pid-0001;vid-0561_pid-554c</p>

选项	值/格式	默认	说明
viewusb.SplitExcludeVidPid	{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]	未定义	<p>使用该选项按供应商和产品 ID 在拆分中排除或包含指定的复合 USB 设备。该设置的格式为 vid-xxx1_pid-yyy1[;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。</p> <p>示例: m:vid-0f0f_pid-55**</p>
viewusb.SplitVidPid	{m o}: vid-xxxx_pid-yyyy([exintf:zz[;exintf:ww]])[;...]	未定义	<p>设置该选项以将由供应商和产品 ID 指定的复合 USB 设备的组件视为单独设备。该设置的格式为 vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww])。可以使用 exintf 关键字通过指定组件的接口号从重定向中排除组件。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。</p> <p>示例: o:vid-0f0f_pid-***(exintf-01);vid-0781_pid-554c(exintf:01;exintf:02)</p> <p>注 Horizon 不会自动包含未明确排除的组件。您必须指定一个筛选策略（如 Include VidPid Device）来包含这些组件。</p>

/etc/vmware/viewagent-custom.conf 中的配置选项

Java Standalone Agent 使用配置文件 /etc/vmware/viewagent-custom.conf。

表 6-2. /etc/vmware/viewagent-custom.conf 中的配置选项

选项	值	默认	说明
CDREnable	true 或 false	true	使用该选项以启用或禁用客户端驱动器重定向 (CDR) 功能。
CollaborationEnable	true 或 false	true	使用此选项可在 Linux 桌面上启用或禁用会话协作功能。
EndpointVPNEnable	true 或 false	false	<p>设置该选项以指定在根据 User Environment Manager 控制台使用的端点 IP 地址范围评估端点 IP 地址时，是使用客户端的物理网卡 IP 地址还是 VPN IP 地址。如果将该选项设置为 false，将使用客户端的物理网卡 IP 地址。否则，将使用 VPN IP 地址。</p>
HelpDeskEnable	true 或 false	true	设置该选项以启用或禁用技术支持工具功能。
KeyboardLayoutSync	true 或 false	true	<p>使用该选项指定是否将客户端的系统区域设置列表和当前键盘布局与适用于 Linux 的 Horizon Agent 桌面同步。</p> <p>启用或未配置此设置时，允许同步。禁用此设置时，不允许同步。</p> <p>只有适用于 Windows 的 Horizon Client 支持该功能，并且该功能仅适用于英语、法语、德语、日语、韩语、西班牙语、简体中文和繁体中文区域设置。</p>

选项	值	默认	说明
LogCnt	整数	-1	<p>使用该选项设置在 <code>/tmp/vmware-root</code> 中保留的日志文件计数。</p> <ul style="list-style-type: none"> ■ -1 - 全部保留 ■ 0 - 全部删除 ■ > 0 - 保留的日志计数。
NetbiosDomain	全部为大写形式的文本字符串		在配置 True SSO 时, 可以使用该选项设置您的组织的域的 NetBIOS 名称。
OfflineJoinDomain	pbis 或 samba	pbis	<p>可使用此选项来设置即时克隆脱机域加入。可执行脱机域加入的方法包括 PowerBroker Identity Services Open (PBISO) 身份验证和 Samba 脱机域加入。如果此属性的值不是 pbis 或 samba, 则将忽略脱机域加入。</p>
RunOnceScript			<p>使用该选项将克隆的虚拟机重新加入 Active Directory。</p> <p>设置主机名更改后的 RunOnceScript 选项。指定的脚本只在首次主机名更改后运行一次。如果在安装代理后更改了主机名, 在代理服务启动时, 将以 root 权限运行该脚本。</p> <p>例如, 对于 Winbind 解决方案, 您必须通过 Winbind 将基础虚拟机加入 Active Directory, 并将该选项设置为一个脚本路径。该脚本必须包含域重新加入命令 <code>/usr/bin/net ads join -U <ADUserName>%<ADUserPassword></code>。在虚拟机克隆后, 操作系统自定义将更改主机名。当代理服务启动时, 将运行该脚本以将克隆的虚拟机加入 Active Directory。</p>
RunOnceScriptTimeout		120	<p>使用此选项设置 RunOnceScript 选项的超时时间, 以秒为单位。</p> <p>例如, 设置 <code>RunOnceScriptTimeout=120</code></p>
SSLCiphers	文本字符串	!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES	<p>使用该选项以指定密码列表。您必须使用 https://www.openssl.org/docs/manmaster/man1/ciphers.html 中定义的格式。</p>
SSLProtocols	文本字符串	TLSv1_1:TLSv1_2	<p>使用该选项以指定安全协议。支持的协议是 TLSv1.0、TLSv1.1 和 TLSv1.2。</p>
SSODesktopType	UseGnomeClassic 、 UseGnomeFlashback 、 UseGnomeUbuntu 、 UseMATE 或 UseKdePlasma		<p>此选项指定在启用了 SSO 时要使用的桌面环境, 而不是默认桌面环境。</p> <p>在指定使用所选的桌面环境之前, 您必须先确保桌面上已安装该桌面环境。在 Ubuntu 16.04/18.04 桌面中设置此选项后, 无论是否启用 SSO 功能, 此选项都会生效。如果在 RHEL/CentOS 7.x 桌面中指定此选项, 则只有在启用了 SSO 的情况下, 才会使用所选的桌面环境。</p> <p>注 RHEL/CentOS 6 和 SLED 11 桌面不支持此选项。有关如何在这些桌面中启用了 SSO 时将 KDE 设置为默认桌面环境的更多信息, 请参阅《设置 Horizon 7 for Linux 桌面》文档。</p>
SSOEnable	true 或 false	true	<p>设置该选项以启用/禁用单点登录 (Single Sign-On, SSO)。</p>

选项	值	默认	说明
SSOUserFormat	文本字符串	[username]	使用该选项以指定用于单点登录的登录名称格式。默认值只包含用户名。如果还需要域名，请设置该选项。通常，登录名称是域名加上一个特殊字符，再加上用户名。如果特殊字符是反斜杠，则必须使用另一个反斜杠对其进行转义。登录名称格式的示例如下： <ul style="list-style-type: none"> ■ SSOUserFormat=[domain]\\[username] ■ SSOUserFormat=[domain]+[username] ■ SSOUserFormat=[username]@[domain]
Subnet	采用 CIDR IP 地址格式的值	[subnet]	将此选项设置为其他计算机可用于连接到 Horizon Agent for Linux 的子网。如果存在多个具有不同子网的本地 IP 地址，则将使用所配置的子网中的本地 IP 地址连接到 Horizon Agent for Linux。您必须指定 CIDR IP 地址格式的值。例如，Subnet=123.456.7.8/24。
UEMEnable	true 或 false	false	设置该选项以启用或禁用 User Environment Manager 智能策略。如果将该选项设置为启用，并且满足 User Environment Manager 智能策略中的条件，将强制执行这些策略。
UEMNetworkPath	文本字符串		必须将此选项设置为在 User Environment Manager 控制台中设置的相同网络路径。路径格式必须类似于 //10.111.22.333/view/LinuxAgent/UEMConfig。

注 VMwareBlastServer 进程有三个安全选项：SSLCiphers、SSLProtocols 和 SSLCipherServerPreference。在启动 VMwareBlastServer 进程时，Java Standalone Agent 将这些选项作为参数传递。启用 Blast 安全网关 (BSG) 时，这些选项会影响 BSG 和 Linux 桌面之间的连接。当 BSG 被禁用时，这些选项会影响客户端和 Linux 桌面之间的连接。

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 Linux 桌面上 USB 重定向、剪贴板重定向和客户端驱动器重定向功能的行为。

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 Horizon 7 环境必须满足特定的要求。

- 必须在要通过智能策略进行管理的远程桌面上安装 Horizon Agent 7.5 或更高版本以及 VMware User Environment Manager 9.4 或更高版本。
- 用户必须使用 Horizon Client 4.8 或更高版本连接到要通过智能策略进行管理的远程 Linux 桌面。
- 必须启用 UEMEnable 选项，并且必须在 /etc/vmware/viewagent-custom.conf 文件中设置 UEMNetworkPath 选项。请参阅[在 Linux 桌面上的配置文件中设置选项](#)。

安装 User Environment Manager

要使用 Horizon 智能策略控制远程 Linux 桌面上远程桌面功能的行为，您必须在远程 Linux 桌面上安装 User Environment Manager 9.4 或更高版本。

您可以从 VMware 下载页面下载 User Environment Manager 安装程序。您可以在要从中管理 User Environment Manager 环境的任何桌面上安装 User Environment Manager 管理控制台组件。

对于链接克隆池，可在用作链接克隆的基础映像的父虚拟机中安装 User Environment Manager。对于 RDS 桌面池，可在提供已发布桌面会话的 RDS 主机上安装 User Environment Manager。

有关 User Environment Manager 系统要求和完整的安装说明，请参阅《安装和配置 VMware User Environment Manager》文档。

配置 User Environment Manager

您必须先配置 User Environment Manager，才能使用它为远程桌面功能创建智能策略。

要配置 User Environment Manager，请按照《VMware User Environment Manager 管理指南》中的配置说明进行操作。

Horizon 智能策略设置

您可以通过创建 Horizon 智能策略来控制 User Environment Manager 中远程功能的行为。

表 6-3. Horizon 智能策略设置描述了使用 User Environment Manager 为远程 Linux 桌面定义 Horizon 智能策略时可选择的设置。

表 6-3. Horizon 智能策略设置

设置	说明
USB 重定向	确定是否在远程桌面上启用 USB 重定向。通过 USB 重定向功能，用户可以从远程桌面使用本地连接的 USB 设备，如闪存、照相机和打印机。如果使用智能策略配置 USB 重定向，您必须使用 User Environment Manager 9.5 或更高版本。
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>如果不配置此设置，则共享的驱动器和文件夹是否可写入取决于您是否已在 <code>/etc/vmware/viewagent-custom.conf</code> 文件中启用了 <code>CDREnable</code> 选项。有关更多信息，请参阅在 Linux 桌面上的配置文件中设置选项。</p>

总之，为 User Environment Manager 中的远程功能配置的 Horizon 智能策略设置会覆盖任何等效的注册表项和组策略设置。

将条件添加到 Horizon 智能策略定义

在 User Environment Manager 中定义 Horizon 智能策略时，可以添加要使策略生效所必须满足的条件。例如，您可以添加一个条件，以便仅当用户从企业网络外部连接到远程桌面时，才禁用客户端驱动器重定向功能。

重要事项 要使所支持的策略设置在远程 Linux 桌面中生效，必须将以下条件添加到 Horizon 智能策略定义中。目前只支持这些条件。如果设置了其他条件，条件评估的最终结果将为 **false**。

表 6-4. 远程 Linux 桌面所需的条件

条件	说明
Operating System Architecture	检查操作系统的架构。值必须设置为 Linux 。
Endpoint IP address	检查端点 IP 地址是否在指定的范围内。范围开始处的空字段被解释为 0，结尾处的空字段被解释为 255。

但是，可以设置多个 Endpoint IP address 条件，如下示例所示。

```
Operating system is Linux
AND Endpoint IP address is in range 11.22.33.44 – 11.22.33.54
OR Endpoint IP address is in range 11.22.33.66 – 11.22.33.77
```

有关在 User Environment Manager 管理控制台中添加和编辑条件的详细信息，请参阅《VMware User Environment Manager 管理指南》。

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](#)。
- 在 `/etc/vmware/viewagent-custom.conf` 文件中启用 `UEMEnable` 选项，并配置 `UEMNetworkPath` 选项。请参阅[在 Linux 桌面上的配置文件中设置选项](#)。

注 在高延迟网络中，保存新的智能策略或更新的智能策略后，请至少等待一分钟，以便让 User Environment Manager 完成更改处理，然后再通知最终用户连接到受影响的桌面。

有关使用 User Environment Manager 管理控制台的完整信息，请参阅《VMware User Environment Manager 管理指南》文档。

步骤

- 1 在 User Environment Manager 管理控制台中，选择**用户环境**选项卡，然后单击树视图中的 **Horizon 智能策略**。

现有的 Horizon 智能策略定义（如果有）会显示在“Horizon 智能策略”窗格中。

- 2 右键单击 **Horizon 智能策略**，并选择**创建 Horizon 智能策略定义**，以创建新的智能策略。

此时会显示“Horizon 智能策略”对话框。

- 3 选择**设置**选项卡，并定义智能策略设置。

- a 在“常规设置”部分的**名称**文本框中，输入智能策略的名称。

例如，如果智能策略会影响客户端驱动器重定向功能，可以将智能策略命名为 **CDR**。

- b 在“Horizon 智能策略设置”部分，选择要包含在智能策略中的远程桌面功能和设置。

您可以选择多个远程桌面功能。

- 4 添加将新智能策略用于远程 Linux 桌面所需满足的条件。

- a 选择**条件**选项卡，单击**添加**，然后选择**操作系统架构**条件。

- b 将值设置为 **Linux**。

```
Operating System is Linux
```

- c 单击**添加**，然后选择**端点 IP 地址**条件。

默认情况下，将添加 **AND** 运算符。

- d 在“端点 IP 地址”对话框中，设置端点 IP 地址范围，然后单击**确定**。

以下是条件语句的示例。

```
Operating System is Linux
AND Endpoint IP address is in range 11.22.33.44 - 11.22.33.54
```

- 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 **Ubuntu1604** 的桌面池禁用 USB 重定向，则在 **Sue** 连接到 **Ubuntu1604** 桌面池中的远程桌面时，将会启用 USB 重定向功能。

适用于 Linux 桌面的 Blast 设置示例

您可以调整远程桌面显示的图像质量，以改善用户体验。在网络连接状态较差时，改善图像质量有助于保持一致的用户体验。

VMware Blast Extreme 协议设置示例

VMwareBlastServer 及其相关插件使用配置文件 `/etc/vmware/config`。

表 6-5. `/etc/vmware/config` 中的 Blast 配置选项示例

选项名称	参数	高速 LAN	LAN	专用 WAN	宽带 WAN	低速 WAN	超低速
带宽设置	RemoteDisplay.maxBandwidthKbps	1000000 (1 Gbps)	1000000 (1 Gbps)	1000000 (1 Gbps)	5000 (5 Mbps)	2000 (2 Mbps)	1000 (1 Mbps)
最大 FPS	RemoteDisplay.maxFPS	60	30	30	20	15	5
音频播放	RemoteDisplay.allowAudio	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE
显示质量 (JPEG/PNG)	RemoteDisplay.maxQualityJPEG	90	90	90	70	60	50
显示质量 (JPEG/PNG)	RemoteDisplay.midQualityJPEG	35	35	35	35	35	35
显示质量 (JPEG/PNG)	RemoteDisplay.minQualityJPEG	25	25	25	20	20	20
显示质量 (H.264)	RemoteDisplay.qpmaxH264	28	36	36	36	36	42
显示质量 (H.264)	RemoteDisplay.qpminH264	10	10	10	10	10	10

适用于 Linux 桌面的客户端驱动器重定向选项示例

可以配置客户端驱动器重定向 (Client Drive Redirection, CDR) 选项，以确定本地系统的共享文件夹和驱动器是否可从远程 Linux 桌面进行访问。

可通过向 `/etc/vmware/config` 文件中添加条目来配置 CDR 设置。

以下配置示例共享了 `d:\ebooks` 和 `C:\spreadsheets` 文件夹，使这两个文件夹只能读取，并禁止客户端共享更多文件夹。

```
cdrserver.forcedByAdmin=true
cdrserver.sharedFolders=d:\ebooks,;c:\spreadsheets,
cdrserver.permissions=R
```

在以上示例中，必须将逗号 “,” 置于 `ebooks` 和 `spreadsheets` 之后，以确保正确解析选项。

`cdserver.sharedFolders` 选项中包含的任何“**R**”将影响该设置中列出的所有文件夹。在以下示例中，即使将 **R** 值仅置于 `/home/jsmith` 文件夹路径之后，**ebooks** 和 **spreadsheets** 文件夹也都为只读。

```
cdserver.sharedFolders=d:\ebooks,;c:\spreadsheets,;/home/jsmith,R
```

禁止在 vSphere 控制台中显示 Linux 桌面

用户连接到 Linux 桌面时，该桌面还可以显示在 Linux 虚拟机的 vSphere 控制台中。您可以对 Linux 虚拟机进行配置，以确保在用户连接到其桌面时 vSphere 控制台中不显示任何桌面。

步骤

- ◆ 在 ESXi 主机上，将以下行添加到 Linux 虚拟机的 `vmx` 文件中。

```
RemoteDisplay.maxConnections = "0"
```

甚至当您在用户已从桌面注销的情况下连接到虚拟机时，vSphere 控制台仍不会显示任何桌面。

创建和管理 Linux 桌面池

要配置 Linux 虚拟机以用作远程桌面，您必须创建包含 Linux 虚拟机的桌面池。

适用于 Linux 的 Horizon 支持以下桌面池类型：

- 含 vCenter 虚拟机的手动桌面池
- 自动完整克隆桌面池
- 即时克隆浮动桌面池

要创建含 vCenter 虚拟机的手动桌面池，您必须在所有虚拟机上安装 Horizon Agent。然后，使用连接服务器桌面池创建向导将虚拟机添加到桌面池。要克隆大量虚拟机，请参阅 [Linux 桌面批量部署概览](#)。

要创建自动完整克隆桌面池，您必须在 Linux 虚拟机模板上安装 Horizon 7 Agent。然后，使用连接服务器桌面池创建向导克隆完整虚拟机。

要创建即时克隆浮动桌面池，您必须在设置了 PBIS Open 环境的 Linux 虚拟机上安装 Horizon 7 Agent，并从中创建一个模板。然后，使用连接服务器桌面池创建向导创建即时克隆浮动桌面池。

本章讨论了以下主题：

- [创建适用于 Linux 的手动桌面池](#)
- [管理适用于 Linux 的桌面池](#)
- [创建适用于 Linux 的自动完整克隆桌面池](#)
- [创建适用于 Linux 的即时克隆浮动桌面池](#)
- [代理 PowerCLI 命令](#)

创建适用于 Linux 的手动桌面池

您可以为 Linux 虚拟机创建手动桌面池。

前提条件

- 确认在 Linux 客户机操作系统上已安装 Horizon Agent。请参阅[在 Linux 虚拟机上安装 Horizon Agent](#)。
- 确认已将 VMware vCenter Server 添加到 Horizon Connection Server。

步骤

- 1 在 Horizon Administrator 中，添加手动桌面池。
选择目录 > 桌面池 > 添加。
- 2 选择手动桌面池。
- 3 在“用户分配”页面上，为桌面池中的计算机选择专用或浮动用户分配，然后单击下一步。
- 4 在“计算机源”页面上，选择 **vCenter 虚拟机**，然后单击下一步。
- 5 在 vCenter Server 页面中，选择相应的 vCenter Server，然后单击下一步。
- 6 输入桌面池 ID。
- 7 在“桌面池设置”页面上，设置以下选项。

选项	说明
默认显示协议	VMware Blast
允许用户选择协议	否
3D 呈现器	使用 vSphere Client 管理（对于 2D、vSGA 或 vDGA 桌面）和 NVIDIA GRID vGPU（对于 vGPU 桌面）

注 必须配置这些池设置。否则，您可能无法连接到桌面，并会收到协议错误或遇到黑屏问题。

- 8 在“添加 vCenter 虚拟机”页面上，选择 Linux 虚拟机。单击**添加**，然后单击下一步。

注 请勿在同一个桌面池中同时创建 Windows 和 Linux 虚拟机。

- 9 要完成该过程，请按照提示进行操作。

授权用户使用桌面池中的虚拟机。在 Horizon Administrator 中，选择桌面池，选择**授权 > 添加授权**，然后添加用户或组。

此时，Linux 虚拟机便已准备好在 Horizon 7 部署中用作远程桌面。

管理适用于 Linux 的桌面池

在创建手动桌面池并向该池中添加 Linux 计算机时，可以通过配置一些设置来管理手动桌面池。您必须只将 Linux 客户机操作系统添加到手动桌面池中。如果池同时包含 Windows 和 Linux 客户机操作系统，则将该池视为 Windows 池，并且无法连接到 Linux 桌面。

管理操作支持

- 禁用或启用桌面池
- 克隆自动桌面池
- 删除桌面池

您可以从 Horizon 7 中移除虚拟机，或者从磁盘中删除虚拟机。

远程设置支持

表 7-1. 远程设置

远程设置	选项
远程计算机电源策略	<ul style="list-style-type: none"> ■ 不执行任何电源操作 ■ 确保计算机始终打开电源 ■ 挂起 ■ 关闭
断开连接后自动注销	<ul style="list-style-type: none"> ■ 立即 ■ 从不 ■ n 分钟之后
允许用户重置/重新启动计算机	<ul style="list-style-type: none"> ■ 是 ■ 否
允许用户从不同的客户端设备启动单独的会话	<ul style="list-style-type: none"> ■ 是 ■ 否
适用于完整克隆和浮动自动桌面池的“注销后删除计算机”	<ul style="list-style-type: none"> ■ 是 ■ 否

Horizon Administrator 操作支持

- 断开会话
- 注销会话
- 重置/重新启动桌面
- 发送消息

对于专用桌面池，可以添加或移除每个虚拟机的用户分配。如需执行大量操作，您必须使用 Horizon PowerCLI Cmdlet。

- Update-UserOwnership
- Remove-UserOwnership

注 请勿更改**远程显示协议**设置。该设置必须始终与创建桌面池时的设置相同。

设置	选项
默认显示协议	VMware Blast
允许用户选择协议	否
3D 呈现器	<ul style="list-style-type: none"> ■ 使用 vSphere Client 管理（对于 2D、vSGA 或 vDGA） ■ NVIDIA GRID vGPU

有关更多信息，请参阅《Horizon 7 管理指南》文档。

创建适用于 Linux 的自动完整克隆桌面池

您可以为 Linux 虚拟机创建自动完整克隆桌面池。创建自动完整克隆桌面池以后，您可以在 Horizon 7 部署中将 Linux 虚拟机用作远程桌面。

前提条件

- 确认在 Linux 客户机操作系统上已安装 Horizon Agent。请参阅[在 Linux 虚拟机上安装 Horizon Agent](#)。
- 在执行虚拟机克隆之前，需创建克隆所基于的虚拟机模板。请参阅[为克隆 Linux 桌面计算机创建虚拟机模板](#)。
- 如果您通过 Winbind 解决方案将 Linux 虚拟机加入 Active Directory，必须在虚拟机模板中完成 Winbind 解决方案的配置。
- 如果您使用 Winbind 解决方案，必须在虚拟机上运行域加入命令。将该命令包含在 Shell 脚本中，并在 `/etc/vmware/viewagent-custom.conf` 中指定到 Horizon Agent 选项 `RunOnceScript` 的脚本路径。有关更多信息，请参阅[在 Linux 桌面上的配置文件中设置选项](#)。
- 确认已将 vCenter Server 添加到 Horizon 连接服务器。

步骤

1 创建客户机自定义规范。

请参阅《vSphere 虚拟机管理指南》文档中的“在 vSphere Web Client 中为 Linux 创建自定义规范”。创建规范时，确保您正确指定以下设置。

设置	值
目标虚拟机操作系统	Linux
计算机名称	使用虚拟机名称。
域	指定 Horizon 7 环境的域。
网络设置	使用标准网络设置。
主 DNS	指定有效地址。

注 有关客户机操作系统自定义支持表的更多信息，请参阅 <http://partnerweb.vmware.com/programs/guestOS/guest-os-customization-matrix.pdf>。

- 2 在 Horizon Administrator 中，选择目录 > 桌面池 > 添加。
- 3 选择自动桌面池，并单击下一步。
- 4 为桌面池中的计算机选择专用或浮动用户分配，并单击下一步。
- 5 在“vCenter Server”页面上，选择完整虚拟机，选择相应的 vCenter Server，然后单击下一步。
- 6 在“桌面池标识”页面中，输入桌面池 ID，然后单击下一步。

- 7 在“桌面池设置”页面上，设置以下选项，然后单击**下一步**。

选项	说明
默认显示协议	VMware Blast
允许用户选择协议	否
3D 呈现器	使用 vSphere Client 管理（对于 2D、vSGA 或 vDGA 桌面）和 NVIDIA GRID vGPU（对于 vGPU 桌面）

注 必须配置这些池设置。否则，您可能无法连接到桌面，并会收到协议错误或遇到黑屏问题。

- 8 在“置备设置”页面上，设置**虚拟机命名**选项，然后单击**下一步**。

选项	说明
手动指定名称	手动输入名称。
使用一种命名模式	例如，指定 <code>LinuxVM-{n}</code> 。 您还必须指定以下桌面池尺寸调整选项： <ul style="list-style-type: none"> ■ 计算机的最大数量 ■ 备用的已打开电源的计算机数量

- 9 在“存储优化”页面上，选择存储管理策略，然后单击**下一步**。
- 10 在“vCenter 设置”页面上，您必须单击“浏览”，按顺序选择 vCenter Server 设置，然后单击**下一步**。

您不能跳过任何 vCenter Server 设置：

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

- 11 在“高级存储选项”页面上，选择相应的存储选项，然后单击**下一步**。
- 12 在“客户机自定义”页面上，选择针对 Linux 的客户机自定义，然后单击**下一步**。
- 13 在“即将完成”页面上，检查详细信息，然后选择**此向导完成后授权用户**。
- 14 单击**完成**。
- 15 要向用户授予使用桌面池中计算机的权限，请选择相应桌面池，单击**授权 > 添加授权**，然后添加用户和组。
- 16 等到桌面池中的所有 Linux 虚拟机变为可用。

创建适用于 Linux 的即时克隆浮动桌面池

您可以使用[添加桌面池](#)向导，为 Linux 虚拟机创建即时克隆浮动桌面池。创建即时克隆浮动桌面池后，您可以将 Linux 虚拟机用作 Horizon 7 部署中的远程桌面。

前提条件

- 熟悉有关在 vCenter Server 中创建虚拟机和安装 Linux 操作系统的步骤。有关更多信息，请参阅[创建虚拟机并安装 Linux](#)。
- 了解使用 PBISO 身份验证解决方案进行 AD 集成的步骤。要了解更多信息，请参阅[将 Linux 与 Active Directory 集成](#)中的“PowerBroker Identity Services Open (PBISO) 身份验证”部分。
- 熟悉 Horizon 7 Agent for Linux 的安装步骤。有关更多信息，请参阅[在 Linux 虚拟机上安装 Horizon Agent](#)。
- 了解使用 VMware vSphere® Web Client 为关闭电源的 Linux 虚拟机拍摄快照的步骤。请参阅《vSphere 单台主机管理 - VMware Host Client》中的“在 VMware Host Client 中拍摄快照”部分。
- 确认已将 vCenter Server 添加到 Horizon 连接服务器。

步骤

- 1 创建一个安装了 Ubuntu 18.04/16.04 或者 RHEL 7.1 或更高版本的 Linux 虚拟机 (VM)。

注 仅在具有 Ubuntu 18.04/16.04 或者 RHEL 7.1 或更高版本的系统上支持该功能。

有关更多信息，请参阅[创建虚拟机并安装 Linux](#)。

- 2 使用以下命令在 Ubuntu 18.04/16.04 计算机上手动安装 Open VMware Tools (OVT):

```
# apt-get install open-vm-tools
```

有关更多信息，请参阅[为远程桌面部署准备 Linux 计算机](#)。

- 3 安装 Linux 分发所需的全部依赖项包。

请参阅[安装 Horizon Agent 的依赖项包](#)了解更多信息。

- 4 在 Linux 虚拟机中安装 Horizon Agent for Linux。

```
# sudo ./install_viewagent.sh -A yes
```

有关详细信息，请参阅[在 Linux 虚拟机上安装 Horizon Agent](#)。

- 5 将 Linux 虚拟机与 Active Directory 相集成。

- 要使用 PBISO 身份验证解决方案，请执行以下步骤：

- a 从 <https://www.beyondtrust.com/products/powerbroker-identity-services-open/> 下载 PBIS Open 8.5.6 或更高版本，并安装到您的 Linux 虚拟机上。

```
# sudo ./pbis-open-8.5.6.2029.linux.x86_64.deb.sh
```

- b 使用将 [Linux 与 Active Directory 集成](#) 的“PowerBroker Identity Services Open (PBISO) 身份验证”部分中的信息，将 Linux 虚拟机与 Active Directory 相集成。
- 如果您选择不使用 PBISO 将 Linux 虚拟机与 Active Directory 相集成，则必须在 `/etc/vmware/viewagent-custom.conf` 文件中将 `OfflineJoinDomain` 选项设置为 **none**。否则，即时克隆浮动桌面池的创建会失败。

6 如果 DHCP 服务器不广播到 DNS 服务器，请为 Linux 系统指定一个 DNS 服务器。

创建新的即时克隆虚拟机时，会添加一个新的虚拟网络适配器。在向即时克隆虚拟机添加新网络适配器时，虚拟机模板中网络适配器的任何设置（例如，DNS 服务器）都将丢失。PBIS 需要一个有效的 DNS 服务器，但不接受 `/etc/hosts` 中的 FQDN 映射。为了避免在向克隆虚拟机添加新网络适配器时丢失 DNS 服务器设置，必须在 Linux 系统中指定一个 DNS 服务器。例如，在 Ubuntu 16.04 系统中，可通过在 `/etc/resolvconf/resolv.conf.d/head` 文件中添加以下行来指定 DNS 服务器。

```
nameserver 10.10.10.10
search mydomain.org
```

7 （可选）如果您想要在主 Linux VDI 即时克隆代理的 `/etc/fstab` 文件中添加 NFS 装载项，请使用以下方法之一。

- 在 `/etc/fstab` 中添加“soft”标记，例如：

```
10.111.222.333:/share /home/nfsmount nfs
size=8192,ws=8192,timeo=14,soft,intr,tcp
```

- 如果您不想在 `/etc/fstab` 中使用“soft”标记，就无法在主 Linux 虚拟机映像中配置 `/etc/fstab`。您可以编写关机脚本以配置 `/etc/fstab` 文件，然后在 Horizon Administrator 的即时克隆桌面池向导的“客户机自定义”窗格中指定该关机脚本。
- 8 关闭 Linux 虚拟机，然后通过使用 VMware vSphere® Web Client 创建已关闭电源的 Linux 虚拟机的快照来创建主映像。**

请参阅《vSphere 单台主机管理 - VMware Host Client》中的“在 VMware Host Client 中拍摄快照”部分，以了解相关信息。

9 在 Horizon Administrator 中，选择目录 > 桌面池 > 添加。

10 定义桌面池。

- a 在“类型”窗格中，选择**自动桌面池**，然后单击**下一步**。
- b 在“用户分配”窗格中，选择**浮动**。单击**下一步**。
- c 在 vCenter Server 窗格中选择**即时克隆**。

11 在“桌面池标识”窗格中输入桌面池 ID，然后单击下一步。

12 在“桌面池设置”窗格中，接受默认设置并启用 HTML Access。单击下一步。

13 在“置备设置”窗格中设置以下虚拟机命名**选项，然后单击下一步。**

- 选择**启用置备**和**出现错误时停止置备**。

- 在**命名模式**文本框中指定一个模式，Horizon 7 将其作为所有桌面虚拟机名称中的前缀，后跟唯一编号。例如，指定 **LinuxVM-{n}**。
- 在**计算机的最大数量**文本框中，指定池中的总计算机数。
- 在**备用 (已打开电源) 计算机数量**文本框中，指定可供用户使用的桌面虚拟机数。
- 选择**预先置备所有计算机**，以让 Horizon 7 置备在**计算机的最大数量**中指定的虚拟机数。

14 在“存储优化”窗格中，为存储管理策略选择**使用 VMware Virtual SAN**，然后单击**下一步**。

15 在“vCenter 设置”窗格中，单击每个 vCenter Server 设置的**浏览**按钮，为每个设置选择相应的值，然后单击**下一步**。

16 在“客户机自定义”窗格中，指定域设置、AD 容器以及在克隆虚拟机后必须运行的任何额外的自定义脚本。单击**下一步**。

重要事项 在使用 ClonePrep 关机或同步后脚本时，确保这些脚本位于 `/var/userScript` 文件夹中，归 root 用户所有，并将文件权限设置为 700。

17 在“即将完成”窗格中选择**此向导完成后授权用户**，然后查看详细信息。

18 单击**完成**。

在 Horizon 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，如果该池存在，请不要删除主映像或将其从 vCenter Server 清单中移除。如果您由于误操作将主映像虚拟机从 vCenter Server 清单中移除，则必须将其添加回去，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《在 Horizon 7 中设置虚拟桌面》中的“向桌面池添加授权”。

代理 PowerCLI 命令

用于在连接服务器和 Windows 桌面上执行各种管理任务的 Horizon PowerCLI cmdlet 也可以用于 Linux 桌面。

创建手动桌面池

```
Add-ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -threedRender usevc|vgpu -
Pool_id <pool id> [more parameters]
```

对于 Linux 桌面，必须提供以下选项和值。

- DefaultProtocol Blast
- AllowProtocolOverride \$false
- threedRender usevc|vgpu。对于 vGPU 桌面，请使用 `-threedRender vgpu`，对于 2D/vSGA/vDGA 桌面，请使用 `-threedRender usevc`。

示例

- 通过虚拟机 (VM) LinuxVM-01, 创建一个名为 LinuxDesktop 的浮动 Linux 桌面池。

```
Add-ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadRender usevc -Pool_id
LinuxDesktop -Id (Get-DesktopVM -Name LinuxVM-01).id -Persistence NonPersistent -Vc_name
myvc.myorg.org
```

- 通过虚拟机名称以 LinuxVM- 开头的所有虚拟机, 创建一个名为 LinuxDesktop 的专用 Linux vGPU 桌面池。

```
Get-DesktopVM | Where-Object {$_.Name.StartsWith("LinuxVM-")} | Add-ManualPool -DefaultProtocol
Blast -AllowProtocolOverride $false -Persistence Persistent -threadRender vgpu -Pool_id
LinuxDesktop
```

- 通过第一个 RHEL 6 x64 虚拟机, 创建浮动 Linux 桌面池 LinuxDesktop。

```
Get-DesktopVM | Where-Object {$_.GuestID -eq "rhel6_64Guest"} | Select-Object -Index 0 | Add-
ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -Persistence NonPersistent -
threadRender usevc -Pool_id LinuxDesktop
```

创建完整克隆自动桌面池

```
Add-AutomaticPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadRender usevc|vgpu `
-Pool_id <pool id> -Vc_id <vCenter id> `
-NamePrefix <VM Name Prefix> " `
-templatePath <Virtual Machine Template Path> `
-VmFolderPath <Virtual Machine Folder Path> `
-ResourcePoolPath <Resource Pool Path> `
-dataStorePaths <Datastore Path> `
-customizationSpecName <Customization Specification Name> `
[more parameters]
```

对于 Linux 桌面, 必须提供以下选项和值。

- DefaultProtocol Blast
- AllowProtocolOverride \$false
- threadRender usevc|vgpu 对于 vGPU 桌面, 请使用 -threadRender vgpu, 对于 2D/vSGA 桌面, 请使用 -threadRender usevc。

示例

```
Add-AutomaticPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadRender usevc `
-pool_id FullClone-Linux `
-Vc_id (Get-ViewVC -serverName myvc.myorg.org).vc_id `
-NamePrefix "FullClone-{n:fixed=3}" `
-Persistence NonPersistent -deletePolicy DeleteOnUse `
-VmFolderPath "/LinuxVDI/vm/FullClone" `
-ResourcePoolPath "/LinuxVDI/host/LinuxVDICluster/Resources" `
```

```
-templatePath "/LinuxVDI/vm/LinuxTemplate" `
-dataStorePaths "/LinuxVDI/host/LinuxVDICluster/datastore" `
-customizationSpecName "linux-spec" `
-maximumCount 100
```

添加或移除桌面池授权

- 授权域 mydomain.org 的域用户组访问 LinuxDesktop。

```
Add-PoolEntitlement -Pool_id LinuxDesktop -Sid (Get-User -Name "domain user" -Domain
"mydomain.org").sid
```

- 从 LinuxDesktop 中移除 mydomain.org 域的域用户组的授权。

```
Remove-PoolEntitlement -Pool_id LinuxDesktop -Sid (Get-User -Name "domain user" -Domain
"mydomain.org").sid
```

将用户分配给专用桌面池中的虚拟机，或从中移除用户

- 将 myuser 用户分配给位于专用桌面池中的 LinuxVM-01 虚拟机。

```
Update-UserOwnership -Machine_id (Get-DesktopVM -Name "LinuxVM-01").machine_id -Sid (Get-User -
Name "myuser" | Where-Object {$_.cn -eq "myuser"}).sid
```

- 将 myuser 用户从位于专用桌面池中的 LinuxVM-01 虚拟机中移除。

```
Remove-UserOwnership -Machine_id (Get-DesktopVM -Name "LinuxVM-01").machine_id
```

注销桌面连接

- 从 myuser 的桌面会话中注销。

```
Get-RemoteSession -Username "mydomain.org\myuser" | Send-SessionLogoff
```

有关代理 PowerCLI cmdlet 的更多信息，请参阅《Horizon 7 集成指南》中的“使用 Horizon PowerCLI 模块”。

为手动桌面池批量部署 Horizon 7

使用 Horizon Administrator，您可以自动创建 Windows（而不是 Linux）桌面计算机池。但是，您可以开发用于自动部署 Linux 桌面计算机池的脚本。

提供的示例脚本仅作为说明之用。对于在使用示例脚本时可能出现的问题，VMware 概不负责。

本章讨论了以下主题：

- [Linux 桌面批量部署概览](#)
- [Linux 桌面批量升级概览](#)
- [为克隆 Linux 桌面计算机创建虚拟机模板](#)
- [用于部署 Linux 桌面的示例 PowerCLI 脚本的输入文件](#)
- [用于克隆 Linux 虚拟机的示例脚本](#)
- [用于将克隆的虚拟机加入 AD 域的示例脚本](#)
- [使用 SSH 将克隆的虚拟机加入 Active Directory 域的示例脚本](#)
- [用于将配置文件上载至 Linux 虚拟机的示例脚本](#)
- [使用 SSH 将配置文件上载至 Linux 虚拟机的示例脚本](#)
- [用于在 Linux 桌面计算机上升级 Horizon Agent 的示例 PowerCLI 脚本](#)
- [使用 SSH 在 Linux 虚拟机上升级 Horizon Agent 的示例脚本](#)
- [用于在 Linux 虚拟机上执行操作的示例脚本](#)

Linux 桌面批量部署概览

部署 Linux 手动桌面的过程涉及几个步骤。如果您计划部署多个桌面，则可以使用 PowerCLI 脚本来自动完成某些步骤。

对于某些操作，您可以选择使用 PowerCLI 或 SSH 在 Linux 计算机上执行命令。下表介绍了这两种方法的区别。

PowerCLI	SSH
无需安装额外工具。	<ul style="list-style-type: none"> ■ 对于 Ubuntu，您需要使用命令 <code>sudo apt-get install openssh-server</code> 安装 SSH 服务器。对于 RHEL 和 CentOS，<code>openssh-server</code> 是默认安装的，但您需要确保防火墙设置允许 SSH。 ■ 需要下载 SSH 客户端应用程序 <code>pscp.exe</code> 和 <code>plink.exe</code>，并将它们和 PowerCLI 脚本置于同一个文件夹。
上载文件和命令执行速度较慢。	上载文件和命令执行速度较快。
需要提供 ESXi 主机的管理员凭据。	不需要提供 ESXi 主机的管理员凭据。
在运行用于安装 Horizon Agent 的脚本时无法处理管理员密码中的特殊字符，或在运行用于加入域脚本时无法处理 AD 用户密码中的特殊字符。	在运行用于安装 Horizon Agent 的脚本时可以处理管理员密码中的特殊字符，或在运行用于加入域脚本时可以处理 AD 用户密码中的特殊字符。

注 基于 PowerCLI 的脚本和基于 SSH 的脚本均可以处理 vCenter Server 管理员和 Linux 管理员的密码中的特殊字符。基于 PowerCLI 的脚本还可以处理 ESXi 主机管理员密码中的特殊字符。在以上所有情况下，均不必使用转义字符。

有关 vSphere PowerCLI 的更多信息，请参阅 <https://www.vmware.com/support/developer/PowerCLI>。

Linux 桌面池的批量部署过程涉及以下步骤：

- 1 创建虚拟机模板并在虚拟机上安装 Horizon Agent。

请参阅[为克隆 Linux 桌面计算机创建虚拟机模板](#)。

- 2 创建客户机自定义规范。

请参阅《vSphere 虚拟机管理指南》文档中的“在 vSphere Web Client 中为 Linux 创建自定义规范”。创建规范时，确保您正确指定以下设置。

设置	值
目标虚拟机操作系统	Linux
计算机名称	使用虚拟机名称。
域	指定 Horizon 7 环境的域。
网络设置	使用标准网络设置。
主 DNS	指定有效地址。

注 有关客户机操作系统自定义支持表的更多信息，请参阅 <http://partnerweb.vmware.com/programs/guestOS/guest-os-customization-matrix.pdf>。

- 3 克隆虚拟机。

请参阅[用于克隆 Linux 虚拟机的示例脚本](#)。

- 4 如果您使用的是 Winbind 解决方案，请将克隆的虚拟机加入 Active Directory (AD) 域。您可以通过以下示例脚本运行域加入命令，或者使用 `/etc/vmware/viewagent-custom.conf` 中的 `RunOnceScript` 选项（在模板虚拟机中配置）。

请参阅[用于将克隆的虚拟机加入 AD 域的示例脚本](#)或使用 [SSH 将克隆的虚拟机加入 Active Directory 域的示例脚本](#)。

5 更新虚拟机中的配置选项。

请参阅[用于将配置文件上载至 Linux 虚拟机的示例脚本](#)或使用 [SSH 将配置文件上载至 Linux 虚拟机的示例脚本](#)。

6 创建桌面池。

请参阅[创建适用于 Linux 的手动桌面池](#)。

有关执行打开电源、关闭、重新启动或删除虚拟机等操作的示例脚本，请参阅[用于在 Linux 虚拟机上执行操作的示例脚本](#)。该脚本可以从 vCenter Server 中删除虚拟机。

Linux 桌面批量升级概览

批量升级 Linux 手动桌面的过程涉及几个步骤。您可以使用 PowerCLI 脚本来自动完成其中的部分步骤。

批量升级未受管桌面

要将未受管虚拟机批量升级为受管或未受管虚拟机，您必须使用示例升级脚本，将新的 Horizon Agent 上载到现有虚拟机并运行升级命令。

- 如果保留未受管虚拟机，则可以重用现有的桌面池。
- 如果从未受管虚拟机升级到受管虚拟机，则必须删除现有的桌面池并创建新的桌面池。有关更多信息，请参阅[在 Linux 虚拟机上升级 Horizon Agent](#)。

批量升级受管桌面

要批量升级受管虚拟机，请选择以下方法之一。

方法	说明
在模板虚拟机中，安装或升级新的 Horizon Agent 并创建快照。	<ul style="list-style-type: none"> ■ 用户数据和配置文件会因现有虚拟机被删除而丢失，除非用户数据和配置文件位于共享服务器（例如 NFS 服务器）上。 ■ 在替换虚拟机后，View Administrator 中可能会缺少虚拟机的状态。您必须重新启动代理服务来修复它。 ■ 如果您使用链接克隆，此方法可避免每个虚拟机上存在重复的数据。
使用示例升级脚本，将新的 Horizon Agent 上载到现有虚拟机并运行升级命令。	<ul style="list-style-type: none"> ■ 用户数据和配置文件会被保留。 ■ 如果您使用链接克隆，此方法会在每个虚拟机上引入重复的数据。

为克隆 Linux 桌面计算机创建虚拟机模板

在执行虚拟机克隆之前，您必须创建克隆所基于的虚拟机模板。

前提条件

- 确认您的部署满足支持 Linux 桌面的相关要求。请参阅[Horizon 7 for Linux 的系统要求](#)。

- 熟悉有关在 vCenter Server 中创建虚拟机和安装客户机操作系统的步骤。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“创建和准备虚拟机”。
- 熟悉您必须用于虚拟机的显示器的必需显存 (vRAM) 值。请参阅 [Horizon 7 for Linux 的系统要求](#)。
- 熟悉 AD 集成的步骤。请参阅第 3 章 [为 Linux 桌面设置 Active Directory 集成](#)。
- 熟悉在 Linux 上安装 Horizon Agent 的步骤。请参阅第 5 章 [安装 Horizon Agent](#)。
- 如果需要，熟悉使用 Horizon 7 配置文件配置选项的步骤。请参阅第 6 章 [Linux 桌面的配置选项](#)。
- 如果您打算设置图形，请熟悉相关步骤。请参阅第 4 章 [为 Linux 桌面设置图形](#)。

步骤

- 1 在 vSphere Web Client 或 vSphere Client 中，创建新虚拟机。
- 2 配置自定义配置选项。
 - a 右键单击虚拟机，然后单击**编辑设置**。
 - b 指定 vCPU 数量和显存大小。
请遵循 Linux 分发包安装指南中的 vCPU 数量和显存大小准则。
例如，Ubuntu 18.04 指定配置 2048 MB 显存和 2 个 vCPU。
 - c 选择**视频卡**并指定显示器数量和显存 (vRAM) 总大小。
对于使用 2D 或 vSGA 的虚拟机（使用 VMware 驱动程序），请在 vSphere Web Client 中设置 vRAM 大小。vRAM 的大小对 vDGA 或 NVIDIA GRID vGPU 计算机（使用 NVIDIA 驱动程序）没有影响。
请遵循《Horizon 7 for Linux 系统要求》中的相关准则。请勿使用显存计算器。
- 3 打开虚拟机的电源并安装 Linux 分发包。
- 4 创建具有 root 特权的用户，例如 ViewUser。此用户仅用于安装和卸载 Horizon Agent。
- 5 编辑 /etc/sudoers 并添加行 ViewUser ALL=(ALL) NOPASSWD:ALL。
如果 /etc/sudoers 中包含此行，则无需密码就能以 ViewUser 身份运行 sudo。当您通过运行本章中提供的示例脚本来安装 Horizon Agent 时，需要将 ViewUser 指定为输入。
- 6 如果 Linux 分发包是 RHEL、CentOS 或 NeoKylin，请编辑 /etc/sudoers 并注释掉以下行：


```
Defaults requiretty
Defaults !visiblepw
```
- 7 如果 Linux 分发包不是 RHEL 7、CentOS 7、SLED 12 或 SLES 12，请安装 VMware Tools。
默认情况下，RHEL 7、CentOS 7、SLED 12 或 SLES 12 已安装 Open VM Tools。

8 安装和配置依赖项包。

- a 如果 Linux 分发版是 RHEL 7、CentOS 7 或 SLES 12，请安装 `deployPkg` 插件。

<http://kb.vmware.com/kb/2075048> 中提供了相应的说明。

- b 如果 Linux 分发版是 Ubuntu，请参阅以下知识库文章来确定要在虚拟机中安装和配置的依赖项包。

- 对于 Ubuntu 18.04 和 16.04，请参阅知识库文章 <https://kb.vmware.com/s/article/2051469> 和 <https://kb.vmware.com/s/article/59687>。

- 对于 Ubuntu 18.04，另请参阅知识库文章 <https://kb.vmware.com/s/article/56409>。

9 对于 RHEL 和 CentOS，启用网络连接设置“自动连接”。

10 执行 AD 集成步骤。

11 执行步骤设置图形。

12 安装 Horizon Agent。

```
sudo ./install_viewagent.sh -A yes
```

请参阅第 5 章 [安装 Horizon Agent](#)。

13 使用 Horizon 7 配置文件执行其他配置。

14 关闭虚拟机并创建快照。

用于部署 Linux 桌面的示例 PowerCLI 脚本的输入文件

用于部署 Linux 桌面的示例 PowerCLI 脚本会读取一个包含桌面计算机信息的输入文件。

输入文件的类型为 `csv`，其中包含以下信息：

- 桌面虚拟机名称
- 父虚拟机名称
- 客户机自定义规范
- 克隆的桌面计算机所在的数据存储
- 托管桌面计算机的 ESXi Server
- 用于克隆的父虚拟机的快照
- 用于指示是否删除桌面虚拟机（如果存在）的标记

以下示例显示了输入文件可能包含的内容。

```
VMName,Parentvm,CustomSpec,Datastore,Host,FromSnapshot,DeleteIfPresent
linux-001,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-002,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-003,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-004,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-005,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
```

在示例脚本中，假定此输入文件名称为 CloneVMs.csv，并且该文件与脚本位于同一文件夹中。

用于克隆 Linux 虚拟机的示例脚本

您可以自定义和使用以下示例脚本来克隆任意数量的虚拟机 (VM)。

要复制和粘贴不包含分页符的脚本内容，请使用此主题的 HTML 版本，您可以从位于 <https://docs.vmware.com/cn/VMware-Horizon-7/index.html> 的 Horizon 7 文档页面找到该版本。

脚本输入

此脚本将读取一个输入文件，[用于部署 Linux 桌面的示例 PowerCLI 脚本](#)的输入文件中对此做了介绍。此脚本还会以交互方式要求提供以下信息：

- vCenter Server 的 IP 地址
- vCenter Server 的管理员登录名称
- vCenter Server 的管理员密码
- 克隆类型，可以是链接克隆或完整克隆
- 是否禁用 vSphere 虚拟机控制台

脚本内容

```
<#
Create Clones from a Master VM

The Tool supports creation of Full clone and linked clone from Master VM.
The parent VM is required for the linked-clone to work and the parent VMs file cannot be renamed or
moved.
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
```

```

[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($input))
}
else
{
    $input = Read-Host
}

[Console]::ResetColor()
return $input
}

function IsVMExists ()
{
    Param($VMExists)
    Write-Host "Checking if the VM $VMExists already Exists"
    [bool]$Exists = $false

    #Get all VMS and check if the VMs is already present in VC
    $listvm = Get-vm
    foreach ($lvm in $listvm)
    {
        if($VMExists -eq $lvm.Name )
        {
            $Exists = $true
        }
    }
    return $Exists
}

function Disable_VM_Console()
{
    Param($VMToDisableConsole)
    $vmConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
    $extra = New-Object VMware.Vim.optionvalue
    $extra.Key="RemoteDisplay.maxConnections"
    $extra.Value="0"
    $vmConfigSpec.extraconfig += $extra
    $vm = Get-VM $VMToDisableConsole | Get-View
    $vm.ReconfigVM($vmConfigSpec)
}

function Delete_VM()
{
    Param($VMToDelete)
    Write-Host "Deleting VM $VMToDelete"
    Get-VM $VMToDelete | where { $_.PowerState -eq "PoweredOn" } | Stop-VM -confirm:$false
    Get-VM $VMToDelete | Remove-VM -DeleteFromDisk -confirm:$false
}

#----- Main Script -----

$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true

```

```

$cloneType = GetInput -prompt 'Clone Type ("linked" or "full")' -IsPassword $false
$disableVMConsole = GetInput -prompt 'Disable vSphere VM Console ("yes" or "no", recommend "yes")' -
IsPassword $false
"-----"
$csvFile = '.\CloneVMs.csv'

# Check that user passed only linked or full clone
if (($cloneType.length > 0) -and ($cloneType -ne "linked" -or $cloneType -ne "full"))
{
    write-host -ForegroundColor Red "Clone type supports only 'linked' or 'full' (case sensitive)"
    exit
}
if (($disableVMConsole.length > 0) -and ($disableVMConsole -ne "yes" -or $disableVMConsole -ne "no"))
{
    write-host -ForegroundColor Red "Disable vSphere VM Console supports only 'yes' or 'no' (case
sensitive)"
    exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File $CSVFile not found"
    exit
}

# Connect to the VC (Parameterize VC)
#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile
#$csvData = Import-CSV $csvFile -
header("VMName","Parentvm","CustomSpec","Datastore","Host","FromSnapshot","DeleteIfPresent")
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $destVMName=$line.VMName
    $srcVM = $line.Parentvm
    $cSpec = $line.CustomSpec
    $targetDSName = $line.Datastore
    $destHost = $line.Host
    $srcSnapshot = $line.FromSnapshot

```

```

$deleteExisting = $line.DeleteIfPresent
if (IsVMExists ($destVMName))
{
    Write-Host "VM $destVMName Already Exists in VC $vcAddress"
    if($deleteExisting -eq "TRUE")
    {
        Delete_VM ($destVMName)
    }
    else
    {
        Write-Host "Skip clone for $destVMName"
        continue
    }
}
$vm = get-vm $srcvm -ErrorAction Stop | get-view -ErrorAction Stop
$cloneSpec = new-object VMware.VIM.VirtualMachineCloneSpec
$cloneSpec.Location = new-object VMware.VIM.VirtualMachineRelocateSpec
if ($CloneType -eq "linked")
{
    $cloneSpec.Location.DiskMoveType =
[VMware.VIM.VirtualMachineRelocateDiskMoveOptions]::createNewChildDiskBacking
}
Write-Host "Using Datastore $targetDSName"
$newDS = Get-Datastore $targetDSName | Get-View
$cloneSpec.Location.Datastore = $newDS.summary.Datastore
Set-VM -vm $srcVM -snapshot (Get-Snapshot -vm $srcVM -Name $srcSnapshot) -confirm:$false
$cloneSpec.Snapshot = $vm.Snapshot.CurrentSnapshot
$cloneSpec.Location.Host = (get-vmhost -Name $destHost).Extensiondata.MoRef
$cloneSpec.Location.Pool = (Get-ResourcePool -Name Resources -Location (Get-VMHost -Name
$destHost)).Extensiondata.MoRef
# Start the Clone task using the above parameters
$task = $vm.CloneVM_Task($vm.parent, $destVMName, $cloneSpec)
# Get the task object
$task = Get-Task | where { $_.id -eq $task }
#Wait for the taks to Complete
Wait-Task -Task $task

$newvm = Get-vm $destVMName
$customSpec = Get-OSCustomizationSpec $cSpec
Set-vm -OSCustomizationSpec $cSpec -vm $newvm -confirm:$false
if ($disableVMConsole -eq "yes")
{
    Disable_VM_Console($destVMName)
}
# Start the VM
Start-VM $newvm
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```


脚本执行

下面是执行脚本时显示的消息：

```
PowerCLI C:\scripts> .\CloneVMs.ps1
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
Clone Type<"linked" or "Full"> : linked
Disable vSphere VM Console ("yes" or "no", recommend "yes") : yes
```

克隆过程所花的时间取决于桌面计算机数，可能需要几分钟到几小时的时间。要确认该过程完成，请从 vSphere Client 中确保最后一个桌面虚拟机已打开电源，具有唯一的主机名，并且 VMware Tools 正在运行。

用于将克隆的虚拟机加入 AD 域的示例脚本

您可以自定义并使用以下示例脚本来将克隆的虚拟机 (VM) 加入 Active Directory (AD) 域。

如果使用 Winbind 解决方案进行 AD 集成，您需要运行此脚本，因为将克隆的虚拟机加入域的步骤会失败。此脚本会运行一个命令以在每个虚拟机上加入域。如果使用 OpenLDAP 解决方案，则您无需运行此脚本。

要复制和粘贴不包含分页符的脚本内容，请使用此主题的 HTML 版本，您可以从位于 https://www.vmware.com/support/pubs/view_pubs.html 的 Horizon 7 文档页面找到该版本。

脚本输入

此脚本将读取一个输入文件，[用于部署 Linux 桌面的示例 PowerCLI 脚本的输入文件](#)中对此做了介绍。此脚本还会以交互方式要求提供以下信息：

- vCenter Server 的 IP 地址
- vCenter Server 的管理员登录名称
- vCenter Server 的管理员密码
- ESXi 主机的管理员登录名称
- ESXi 主机的管理员密码
- Linux 虚拟机的用户登录名称
- Linux 虚拟机的用户密码
- 有权将计算机加入域中的 AD 用户的登录名称
- 获授权的 AD 用户的密码

脚本内容

```
<#
.SYNOPSIS
run command "sudo /usr/bin/net ads join"

.DESCRIPTION
The tool is to run the command "sudo /usr/bin/net ads join" to join Linux to AD

.NOTES
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
#----- Handle input -----
"-----"
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$adUser = GetInput -prompt 'Type the AD user name to join the AD' -IsPassword $false
""
"Please type the AD user password."
"Please note that special character in password may not work with the script"
$adUserPassword = GetInput -prompt 'Your AD user password' -IsPassword $true
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'
```

```
#----- Main Script -----

#Connect to vCenter
#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "sudo /usr/bin/net ads join -U $adUser%$adUserPassword"
    Write-Host "Run cmd 'sudo /usr/bin/net ads join' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit
```

脚本执行

下面是执行脚本时显示的消息：

```
PowerCLI C:\scripts> .\ClonedVMs_JoinDomain.ps1

-----
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****
-----
```

```
Type the AD user name to join the AD: viewadmin
Please type the AD user password.
Please note that special character in password may not work with the script.
Your AD user password: *****
```

使用 SSH 将克隆的虚拟机加入 Active Directory 域的示例脚本

您可以自定义并使用以下示例脚本来将克隆的虚拟机 (VM) 加入 Active Directory (AD) 域。此脚本会使用 SSH 在 Linux 虚拟机上运行命令。

如果使用 Winbind 解决方案进行 AD 集成，您需要运行此脚本，因为将克隆的虚拟机加入域的步骤会失败。此脚本会运行一个命令以在每个虚拟机上加入域。如果使用 OpenLDAP 解决方案，则您无需运行此脚本。

要复制和粘贴不包含分页符的脚本内容，请使用此主题的 HTML 版本，您可以从位于 https://www.vmware.com/support/pubs/view_pubs.html 的 Horizon 7 文档页面找到该版本。

脚本输入

此脚本将读取一个输入文件，[用于部署 Linux 桌面的示例 PowerCLI 脚本的输入文件](#)中对此做了介绍。此脚本还会以交互方式要求提供以下信息：

- vCenter Server 的 IP 地址
- vCenter Server 的管理员登录名称
- vCenter Server 的管理员密码
- Linux 虚拟机的用户登录名称
- Linux 虚拟机的用户密码
- 有权将计算机加入域中的 AD 用户的登录名称
- 获授权的 AD 用户的密码

脚本内容

```
<#
.SYNOPSIS
run command "sudo /usr/bin/net ads join" via SSH

.DESCRIPTION
The tool is to run the command "sudo /usr/bin/net ads join" to join Linux machine to AD via SSH

.NOTES
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
```

```

[Console]::ForegroundColor = "Blue"
if ($IsPassword)
{
    $input = Read-Host -AsSecureString
    $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
}
else
{
    $input = Read-Host
}

[Console]::ResetColor()
return $input
}

function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
    if ($IsPSCP)
    {
        if (Test-Path ".\pscp.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
            exit
        }
    }
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"

```

```

    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + "'" + $cmd + "'"
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file: $command"
    Invoke-Expression $command
}

#----- Handle input -----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $false
"-----"
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$adUser = GetInput -prompt 'Type the AD user name to join the AD' -IsPassword $false
""
"\nPlease type the AD user password."
[Console]::ForegroundColor = "Yellow"
"Plase note that special character should be escaped. For example, $ should be \$\"
[Console]::ResetColor()
$adUserPassword = GetInput -prompt 'Your AD user password' -IsPassword $true
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#----- Main Script -----

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}

```

```

}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "sudo /usr/bin/net ads join -U $adUser%$adUserPassword"
    Write-Host "Run cmd 'sudo /usr/bin/net ads join' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

脚本执行

下面是执行脚本时显示的消息：

```

PowerCLI C:\scripts> .\ClonedVMs_JoinDomain_SSH.ps1

-----
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****

-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

-----
Type the AD user name to join the AD: viewadmin
Please type the AD user password.
Please note that special character should be escaped. For example, $ should be \$
Your AD user password: *****

```

用于将配置文件上载至 Linux 虚拟机的示例脚本

您可以自定义并使用以下示例脚本来将配置文件 `config` 和 `viewagent-custom.conf` 上载至多个 Linux 虚拟机 (VM)。

要复制和粘贴不包含分页符的脚本内容，请使用此主题的 HTML 版本，您可以从位于 https://www.vmware.com/support/pubs/view_pubs.html 的 Horizon 7 文档页面找到该版本。

脚本输入

此脚本将读取一个输入文件，[用于部署 Linux 桌面的示例 PowerCLI 脚本的输入文件](#)中对此做了介绍。此脚本还会以交互方式要求提供以下信息：

- vCenter Server 的 IP 地址
- vCenter Server 的管理员登录名称
- vCenter Server 的管理员密码
- ESXi 主机的管理员登录名称
- ESXi 主机的管理员密码
- Linux 虚拟机的用户登录名称
- Linux 虚拟机的用户密码

脚本内容

```
<#
Upload the configuration files config and viewagent-custom.conf to Linux VMs
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

#----- Handle Input -----
"-----"
write-host -ForegroundColor Blue 'Please ensure your config file and viewagent-custom.conf file are
in current working directory'
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$shostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
```



```

$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"

$csvFile = '.\CloneVMs.csv'
$setConfig = $false
$setCustomConf = $false
$config_File = "config"
$customConf_File = "viewagent-custom.conf"

#check if config file exists
if(Test-Path $config_File)
{
    $setConfig = $true
    write-host -ForegroundColor Yellow '"config" file found'
}
else
{
    write-host -ForegroundColor Yellow '"config" file not found, skip it'
}

if(Test-Path $customConf_File)
{
    $setCustomConf = $true
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file found'
}
else
{
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file not found, skip it'
}

if (($setConfig -eq $false)-AND ($setCustomConf -eq $false))
{
    write-host -ForegroundColor Red 'Both file not found, exit'
    exit
}

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

```

```

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    #Try to delete the configuration file from home folder on destination VM
    $cmd = "rm -rf config viewagent-custom.conf"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    if ($setConfig)
    {
        Write-Host "Upload File '$config_File' to '$destFolder' of VM '$VMName' with user '$guestUser'"
        Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $config_File

        $cmd = "sudo mv ./ $config_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
        Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
    }

    if ($setCustomConf)
    {
        Write-Host "Upload File '$customConf_File' to '$destFolder' of VM '$VMName' with user
'$guestUser'"
        Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $customConf_File

        $cmd = "sudo mv ./ $customConf_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
        Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
    }
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

脚本执行

下面是执行脚本时显示的消息：

```

PowerCLI C:\scripts> .\UpdateOptionFile.ps1
-----
Please ensure your config file and view-agent.conf file are in current working directory.
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator

```

```

Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

```

使用 SSH 将配置文件上载至 Linux 虚拟机的示例脚本

您可以自定义并使用以下示例脚本来将配置文件 `config` 和 `viewagent-custom.conf` 上载至多个 Linux 虚拟机 (VM)。此脚本会使用 SSH 在 Linux 虚拟机上运行命令。

要复制和粘贴不包含分页符的脚本内容，请使用此主题的 HTML 版本，您可以从位于 https://www.vmware.com/support/pubs/view_pubs.html 的 Horizon 7 文档页面找到该版本。

脚本输入

此脚本将读取一个输入文件，[用于部署 Linux 桌面的示例 PowerCLI 脚本的输入文件](#)中对此做了介绍。此脚本还会以交互方式要求提供以下信息：

- vCenter Server 的 IP 地址
- vCenter Server 的管理员登录名称
- vCenter Server 的管理员密码
- Linux 虚拟机的用户登录名称
- Linux 虚拟机的用户密码

脚本内容

```

<#
Upload the configuration files config and viewagent-custom.conf to Linux VMs using SSH
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }
}

```

```

    }

    [Console]::ResetColor()
    return $input
}
function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
    if ($IsPSCP)
    {
        if (Test-Path ".\pscp.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
            exit
        }
    }
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + '"' + $cmd + '"'
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        {
            echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
        }
    }
}
}

```

```

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file: $command"
    Invoke-Expression $command
}

#----- Handle Input -----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $true
"-----"
write-host -ForegroundColor Blue 'Please ensure your config file and viewagent-custom.conf file are
in current working directory'
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"

$csvFile = '.\CloneVMs.csv'
$setConfig = $false
$setCustomConf = $false
$config_File = "config"
$customConf_File = "viewagent-custom.conf"

#check if config file exists
if(Test-Path $config_File)
{
    $setConfig = $true
    write-host -ForegroundColor Yellow '"config" file found'
}
else
{
    write-host -ForegroundColor Yellow '"config" file not found, skip it'
}

if(Test-Path $customConf_File)
{
    $setCustomConf = $true
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file found'
}
else
{
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file not found, skip it'
}

if (($setConfig -eq $false)-AND ($setCustomConf -eq $false))
{

```

```

    write-host -ForegroundColor Red 'Both file not found, exit'
    exit
}

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    #Try to delete the configuration file from home folder on destination VM
    $cmd = "rm -rf config viewagent-custom.conf"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

    if ($setConfig)
    {
        Write-Host "Upload File '$config_File' to '$destFolder' of VM '$VMName' with user '$guestUser'"
        UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
$config_File -DestPath $destFolder

        $cmd = "sudo mv ./ $config_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
        RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
    }

    if ($setCustomConf)
    {
        Write-Host "Upload File '$customConf_File' to '$destFolder' of VM '$VMName' with user
'$guestUser'"
        UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
$customConf_File -DestPath $destFolder

        $cmd = "sudo mv ./ $customConf_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
        RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
    }
}

```

```

    }
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

脚本执行

下面是执行脚本时显示的消息：

```

PowerCLI C:\scripts> .\UpdateOptionFile.ps1
-----
Please ensure your config file and view-agent.conf file are in current working directory.
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

```

用于在 Linux 桌面计算机上升级 Horizon Agent 的示例 PowerCLI 脚本

您可以自定义并使用以下示例脚本在多个 Linux 虚拟机 (VM) 上升级 Horizon Agent。

此脚本会先将安装程序 tar ball 上载至每个虚拟机，然后再安装 Horizon Agent。上载任务可能非常耗时，在涉及大量虚拟机和网络速度缓慢时尤其如此。为节省时间，您可以运行使用 SSH 的脚本，或者将安装程序 tar ball 置于每个虚拟机均可访问的共享的位置，这样就不必上载文件。

要复制和粘贴不包含分页符的脚本内容，请使用此主题的 HTML 版本，您可以从位于 <https://docs.vmware.com/cn/VMware-Horizon-7/index.html> 的 Horizon 7 文档页面找到该版本。

脚本输入

此脚本将读取一个输入文件，[用于部署 Linux 桌面的示例 PowerCLI 脚本的输入文件](#)中对此做了介绍。此脚本还会以交互方式要求提供以下信息：

- 接受 Horizon Agent EULA（最终用户许可协议）
- vCenter Server 的 IP 地址
- vCenter Server 的管理员登录名称
- vCenter Server 的管理员密码
- ESXi 主机的管理员登录名称
- ESXi 主机的管理员密码
- Linux 客户机操作系统的用户登录名称
- Linux 客户机操作系统的用户密码
- Horizon Agent tar ball 路径

- 升级到受管虚拟机
- 安装智能卡重定向功能

脚本内容

```
<#
Upload the Linux Agent installer tar ball and re-install
#>

#-----
Functions-----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
#-----Handle
input-----
"-----"
$acceptEULA = GetInput -prompt 'Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no")' -
IsPassword $false
if ($acceptEULA -ne "yes")
{
    write-host -ForegroundColor Red "You need accept the EULA with 'yes'(case sensitive)"
    exit
}
$svcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$svcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$svcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
```



```

$agentInstaller = GetInput -prompt 'Type the Horizon Agent tar ball path' -IsPassword $false
"-----"
$UpgradeToManagedVM = GetInput -prompt 'Upgrade to managed VM ("yes" or "no")' -IsPassword $false
if (($UpgradeToManagedVM -ne "yes") -AND $UpgradeToManagedVM -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
$installSmartcard = GetInput -prompt 'Install the Smartcard redirection feature ("yes" or "no")' -
IsPassword $false
if (($installSmartcard -ne "yes") -AND $installSmartcard -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#check if file exists
if (!(Test-Path $agentInstaller))
{
    write-host -ForegroundColor Red "installer File not found"
    exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File not found"
    exit
}
#-----
Functions-----
function GetSourceInstallerMD5()
{
    $agentInstallerPath = Convert-Path $agentInstaller;
    $md5 = New-Object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider;
    $md5HashWithFormat =
[System.BitConverter]::ToString($md5.ComputeHash([System.IO.File]::ReadAllBytes($agentInstallerPath)))
;
    $md5Hash = ($md5HashWithFormat.replace("-", "")).ToLower();
    return $md5Hash;
}

#-----
Main-----
#Get installer MD5Sum
$installerMD5Hash = GetSourceInstallerMD5;

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{

```

```

    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "rm -rf VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    #Upload installer tar ball to Linux VM
    Write-Host "Upload File '$agentInstaller' to '$destFolder' of VM '$VMName' with user '$guestUser'"
    Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $agentInstaller

    #Check the uploaded installer md5sum
    $cmd = "md5sum VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    $output = Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -
GuestUser $guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    if($output.Contains($installerMD5Hash))
    {
        Write-Host $VMName": Uploaded installer's MD5Sum matches the local installer's MD5Sum";
        Write-Host $VMName": Extract the installer and do installation";
        $cmd = "tar -xzvf VMware-*linux-*.tar.gz"
        Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
        Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

        $cmd = "sudo setenforce 0";
        Write-Host "Set the selinux to permissive mode: $cmd"
        Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

        $cmd = "sudo killall /usr/lib/vmware/viewagent/VMwareBlastServer/VMwareBlastServer"
        Write-Host "Stop VMwareBlastServer before upgrading: $cmd"
        Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
    }
}

```

```

#Run the upgrade command.
$cmd = "cd VMware-*linux-* && sudo ./install_viewagent.sh -A yes -m $installSmartcard -M
$UpgradeToManagedVM"
Write-Host "Run upgrade cmd in VM '$VMName' with user '$guestUser': $cmd"
Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

$cmd = "sudo shutdown -r +1&"
Write-Host "Reboot to apply the Horizon Agent installation"
Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
}
else
{
    Write-Host $VMName": Uploaded installer's MD5Sum does NOT match the local installer's MD5Sum";
    Write-Host $VMName": Skip the installation. Please check your network and VMware Tools
status";
    exit;
}
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

脚本执行

下面是执行脚本时显示的消息：

```

PowerCLI C:\scripts> .\InstallAgent.ps1

-----
Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no"): yes
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****

-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****

-----
Your VM guest OS user name: HorizonUser
Your VM guest OS user password: *****

-----
Type the Horizon Agent tar ball path. Please take care of the installer arch: .\VMware-viewagent-
linux-x86_64-x.y.z-1234567.tar.gz

-----
Upgrade to managed VM ("yes" or "no"): yes
Install the Smartcard redirection feature ("yes" or "no"): no

```

使用 SSH 在 Linux 虚拟机上升级 Horizon Agent 的示例脚本

您可以自定义并使用以下示例脚本在多个 Linux 虚拟机 (Virtual Machine, VM) 上升级 Horizon Agent。此脚本会使用 SSH 在 Linux 虚拟机上运行命令。

要复制和粘贴不包含分页符的脚本内容，请使用此主题的 HTML 版本，您可以从位于 https://www.vmware.com/support/pubs/view_pubs.html 的 Horizon 7 文档页面找到该版本。

脚本输入

此脚本将读取一个输入文件，[用于部署 Linux 桌面的示例 PowerCLI 脚本的输入文件](#)中对此做了介绍。此脚本还会以交互方式要求提供以下信息：

- 接受 Horizon Agent EULA（最终用户许可协议）
- vCenter Server 的 IP 地址
- vCenter Server 的管理员登录名称
- vCenter Server 的管理员密码
- ESXi 主机的管理员登录名称
- ESXi 主机的管理员密码
- Linux 客户机操作系统的用户登录名称
- Linux 客户机操作系统的用户密码
- Horizon Agent tar ball 路径
- 升级到受管虚拟机
- 安装智能卡重定向功能

脚本内容

```
<#
Upload the Linux Agent installer tar ball and re-install
#>

#-----
Functions-----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
```

```

TR($input))
}
else
{
    $input = Read-Host
}

[Console]::ResetColor()
return $input
}
function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
    if ($IsPSCP)
    {
        if (Test-Path ".\pscp.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
            exit
        }
    }
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + '"' + $cmd + '"'
        $output = Invoke-Expression $command
        return $output
    }
    else

```

```

    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file $LocalPath to VM $VM_Name with user $User"
    Invoke-Expression $command
}

#-----Handle
input-----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $true
"-----"
$acceptEULA = GetInput -prompt 'Accept Linux View Agent EULA in tar bundle ("yes" or "no")' -
IsPassword $false
if ($acceptEULA -ne "yes")
{
    write-host -ForegroundColor Red "You need accept the EULA with 'yes'(case sensitive)"
    exit
}
$svcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$svcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$svcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$agentInstaller = GetInput -prompt 'Type the View Agent tar ball path' -IsPassword $false
"-----"
$UpgradeToManagedVM = GetInput -prompt 'Upgrade to managed VM ("yes" or "no")' -IsPassword $false
if (($UpgradeToManagedVM -ne "yes") -AND $UpgradeToManagedVM -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
$installSmartcard = GetInput -prompt 'Install the Smartcard redirection feature ("yes" or "no")' -
IsPassword $false
if (($installSmartcard -ne "yes") -AND $installSmartcard -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

```

```

#check if file exists
if (!(Test-Path $agentInstaller))
{
write-host -ForegroundColor Red "installer File not found"
exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
write-host -ForegroundColor Red "CSV File not found"
exit
}
#-----
Functions-----
function GetSourceInstallerMD5()
{
    $agentInstallerPath = Convert-Path $agentInstaller;
    $md5 = New-Object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider;
    $md5HashWithFormat =
[System.BitConverter]::ToString($md5.ComputeHash([System.IO.File]::ReadAllBytes($agentInstallerPath)))
;
    $md5Hash = ($md5HashWithFormat.replace("-", "").ToLower());
    return $md5Hash;
}

#-----
Main-----
#Get installer MD5Sum
$installerMD5Hash = GetSourceInstallerMD5;

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"
}

```

```

$cmd = "rm -rf VMware-*--linux-*"
Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

#Upload installer tar ball to Linux VM
Write-Host "Upload File '$agentInstaller' to '$destFolder' of VM '$VMName' with user '$guestUser'"
UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
$agentInstaller -DestPath $destFolder

#Check the uploaded installer md5sum
$cmd = "md5sum VMware-*--linux-*"
Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
$output = RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd -
$returnOutput $true

if($output.Contains($installerMD5Hash))
{
    Write-Host $VMName": Uploaded installer's MD5Sum matches the local installer's MD5Sum";
    Write-Host $VMName": Extract the installer and do installation";

    $cmd = "tar -xzf VMware-*--linux-*.tar.gz"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

    $cmd = "sudo setenforce 0";
    Write-Host "Set the selinux to permissive mode: $cmd"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

    $cmd = "sudo killall /usr/lib/vmware/viewagent/VMwareBlastServer/VMwareBlastServer"
    Write-Host "Stop VMwareBlastServer before upgrading: $cmd"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

    #Run the upgrade command.
    $cmd = "cd VMware-*--linux-* && sudo ./install_viewagent.sh -r yes -A yes -m $installSmartcard
-M $UpgradeToManagedVM"
    Write-Host "Run upgrade cmd in VM '$VMName' with user '$guestUser': $cmd"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
    Write-Host -ForegroundColor Yellow "Linux Agent installer will reboot the Linux VM after
upgrade, and you may hit the ssh connection closed error message, which is expectation"
}
else
{
    Write-Host $VMName": Uploaded installer's MD5Sum does NOT match the local installer's MD5Sum";
    Write-Host $VMName": Skip the installation. Please check your network and VMware Tools
status";
    exit;
}
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```


脚本执行

下面是执行脚本时显示的消息：

```
PowerCLI C:\scripts> .\InstallAgent.ps1

-----

Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no"): yes
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****

-----

Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

-----

Type the Horizon Agent tar ball path. Please take care of the installer arch: .\VMware-viewagent-
linux-x86_64-x.y.z-1234567.tar.gz

-----

Upgrade to managed VM ("yes" or "no"): yes
Install the Smartcard redirection feature ("yes" or "no"): no
```

用于在 Linux 虚拟机上执行操作的示例脚本

您可以自定义和使用以下示例脚本来在多个虚拟机 (VM) 上执行操作。这些操作包括打开电源、关闭电源、关闭、重新启动和删除虚拟机。

该脚本可以从 vCenter Server 中删除虚拟机，但不能从 View 中删除虚拟机。

要复制和粘贴不包含分页符的脚本内容，请使用此主题的 HTML 版本，您可以从位于 https://www.vmware.com/support/pubs/view_pubs.html 的 Horizon 7 文档页面找到该版本。

脚本输入

此脚本将读取一个输入文件，[用于部署 Linux 桌面的示例 PowerCLI 脚本的输入文件](#)中对此做了介绍。此脚本还会以交互方式要求提供以下信息：

- vCenter Server 的 IP 地址
- vCenter Server 的管理员登录名称
- vCenter Server 的管理员密码
- 要执行的操作，可以是打开电源、关闭电源、关闭客户机、重新启动虚拟机、重新启动虚拟机客户机或删除虚拟机。
- 虚拟机上的操作之间的等待时间（以秒为单位）。

脚本内容

```
<#
.DESCRIPTION
The Tool supports:
1. Power off VMs
```

```

2. Power on VMs
3. Shutdown VMs
4. Restart VMs
5. Restart VM guest
6. Delete VMs from Disk
.NOTES
#>

#----- Functions -----

function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

function IsVMExists ($VMExists)
{
    Write-Host "Checking if the VM $VMExists Exists"
    [bool]$Exists = $false

    #Get all VMS and check if the VMs is already present in VC
    $listvm = Get-vm
    foreach ($lvm in $listvm)
    {
        if($VMExists -eq $lvm.Name )
        {
            $Exists = $true
            Write-Host "$VMExists is Exist"
        }
    }
    return $Exists
}

function Delete_VM($VMToDelete)
{
    Write-Host "Deleting VM $VMToDelete"
    Get-VM $VMToDelete | where { $_.PowerState -eq "PoweredOn" } | Stop-VM -confirm:$false
    Get-VM $VMToDelete | Remove-VM -DeleteFromDisk -confirm:$false
}

```

```

}

#----- Handle input -----
"-----"
SvcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
SvcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
SvcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"

$action = GetInput -prompt 'Select action: 1). Power On 2). Power Off 3) Shutdown VM Guest 4).
Restart VM 5). Restart VM Guest 6). Delete VM' -IsPassword $false
$sleepTime = GetInput -prompt 'Wait time (seconds) between each VM' -IsPassword $false
"-----"

[Console]::ForegroundColor = "Yellow"
switch ($action)
{
    1
    {
        "Your selection is 1). Power On"
    }
    2
    {
        "Your selection is 2). Power Off"
    }
    3
    {
        "Your selection is 3) Shutdown"
    }
    4
    {
        "Your selection is 4). Restart VM"
    }
    5
    {
        "Your selection is 5). Restart VM Guest"
    }
    6
    {
        "Your selection is 6). Delete VM"
    }
    default
    {
        "Invalid selection for action: $action"
        exit
    }
}

[Console]::ResetColor()
$csvFile = '.\CloneVMs.csv'

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File not found"
    exit
}
"-----"

```

```

#----- Main -----
#Read input CSV file
Disconnect-VIServer $vcAddress -Confirm:$false
#Connect-VIServer $vcAddress -ErrorAction Stop -user $vcAdmin -password $vcPassword
Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
$csvData = Import-CSV $csvFile

foreach ($line in $csvData)
{
    $VMName = $line.VMName
    switch ($action)
    {
        1
        {
            Get-VM $VMName | Start-VM -Confirm:$false
        }
        2
        {
            Get-VM $VMName | Stop-VM -Confirm:$false
        }
        3
        {
            Get-VM $VMName | Shutdown-VMGuest -Confirm:$false
        }
        4
        {
            Get-VM $VMName | Restart-VM -Confirm:$false
        }
        5
        {
            Get-VM $VMName | Restart-VMGuest -Confirm:$false
        }
        6
        {
            if (IsVMExists ($VMName))
            {
                Delete-VM ($VMName)
            }
        }
        default{}
    }
    Start-Sleep -s $sleepTime
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

脚本执行

下面是执行脚本时显示的消息：

```
PowerCLI C:\scripts> .\VM0perations.ps1
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****

-----

Select action: 1). Power On 2). Power Off 3) Shutdown VM Guest 4). Restart VM 5). Restart VM Guest
6). Delete VM: 1
Wait time (seconds) between each VM: 20

-----

Your selection is 6). Delete VM
```

对于打开电源、重新启动虚拟机和重新启动虚拟机客户机操作，将虚拟机之间的等待时间指定为至少 20 秒可避免出现引导风暴的情况，否则可能导致某些操作失败。

对 Linux 桌面进行故障排除

在管理 Linux 桌面时可能出现某些问题。您可以按照不同的步骤诊断并解决问题。

本章讨论了以下主题：

- 在 [Horizon Console](#) 中使用 [Horizon Help Desk Tool](#)
- 收集 [Horizon 7 for Linux](#) 计算机的诊断信息
- 对远程桌面和客户端主机之间的复制和粘贴问题进行故障排除
- [Horizon Agent](#) 在 [iPad Pro Horizon Client](#) 上无法断开连接
- [SLES 12 SP1](#) 桌面不自动刷新
- [SSO](#) 无法连接到关机代理
- 在创建适用于 [Linux](#) 的手动桌面池后无法访问虚拟机

在 Horizon Console 中使用 Horizon Help Desk Tool

Horizon Help Desk Tool 是一个 Web 应用程序，可用于获取 Horizon 7 用户会话的状态以及执行故障排除和维护操作。

在 Horizon Help Desk Tool 中，您可以查找要对问题进行故障排除的用户会话，还可以执行桌面维护操作，如重新启动或重置桌面。

要配置 Horizon Help Desk Tool，必须满足以下要求：

- Horizon 7 的 Horizon Enterprise 版许可证或 Horizon Apps Advanced 版许可证。要确认您具有正确的许可证，请参阅《[Horizon 7 管理指南](#)》文档。
- 用来存储 Horizon 7 组件相关信息的事件数据库。有关配置事件数据库的更多信息，请参阅《[Horizon 7 安装指南](#)》文档。
- 用来登录到 Horizon Help Desk Tool 的“技术支持管理员”角色或“技术支持管理员 (只读)”角色。有关这些角色的更多信息，请参阅《[Horizon 7 管理指南](#)》文档。
- 在每个连接服务器实例上启用时间安排分析器，以查看登录分段。

使用以下 `vdadmin` 命令可在每个连接服务器实例上启用时间安排分析器：

```
vdadmin -I -timingProfiler -enable
```

使用以下 **vdmadmin** 命令可在使用管理端口的连接服务器实例上启用时间安排分析器：

```
vdmadmin -I -timingProfiler -enable -server {ip/server}
```

- 在 `/etc/vmware/viewagent-custom.conf` 配置文件中启用 `HelpDeskEnable` 选项。

在 Horizon Console 中启动 Horizon Help Desk Tool

Horizon Help Desk Tool 已集成到 Horizon Console 中。您可以搜索要在 Horizon Help Desk Tool 中为其排除故障的用户。

步骤

- 1 在 Horizon Console 的“用户搜索”字段中输入用户名。

Horizon Console 会在搜索结果中显示用户的列表。搜索最多可返回 100 个匹配结果。

- 2** 选择一个用户名。

用户卡中将会显示相应的用户信息。

后续步骤

要对问题进行故障排除，请单击用户卡中的相关选项卡。

在 Horizon Help Desk Tool 中对用户进行故障排除

在 **Horizon Help Desk Tool** 中，您可以在用户卡中查看基本用户信息。您可以单击用户卡中的选项卡以获取有关特定组件的更多详细信息。

用户详细信息有时会显示在表中。您可以按表列对这些用户详细信息进行排序。

- 要按升序对某列进行排序，请单击该列一次。
- 要按降序对某列进行排序，请单击该列两次。
- 要不对该列进行排序，请单击该列三次。

基本用户信息

显示基本用户信息，例如用户的用户名、电话号码和电子邮件地址，以及用户的状态（已连接或已断开连接）。如果用户具有桌面会话，则用户的状态为已连接。如果用户没有任何桌面会话，则用户的状态为已断开连接。

您可以单击电子邮件地址来向用户发送消息。

会话

会话选项卡显示有关用户连接到的桌面会话的信息。

您可以使用**筛选器**文本框筛选桌面会话。

注 对于从 vSphere Client 或 ESXi 访问虚拟机的会话，会话选项卡不会显示其会话信息。

会话选项卡包含以下信息:

表 9-1. “会话” 选项卡

选项	说明
状态	<p>显示有关桌面会话状态的信息。</p> <ul style="list-style-type: none"> 如果会话已连接，则显示绿色。 如果会话是本地会话或在本地容器中运行的会话，则显示 L。
计算机名称	<p>桌面会话名称。单击该名称可在一个信息卡中打开会话信息。您可以单击会话信息卡中的选项卡以查看其他信息：</p> <ul style="list-style-type: none"> 详细信息选项卡显示虚拟机信息、CPU 或内存使用情况等用户信息。 进程选项卡显示有关 CPU 和内存相关进程的信息。
协议	用于远程会话的桌面协议。
类型	显示桌面是已发布的桌面，还是虚拟机桌面。
连接时间	会话连接到连接服务器的时间。
会话持续时间	会话保持连接到连接服务器的时长。

桌面

桌面选项卡显示有关用户有权使用的已发布桌面或虚拟桌面的信息。

表 9-2. 桌面

选项	说明
状态	<p>显示有关桌面会话状态的信息。</p> <ul style="list-style-type: none"> 如果会话已连接，则显示绿色。
桌面池名称	会话的桌面池的名称。
桌面类型	<p>显示桌面是已发布的桌面，还是虚拟机桌面。</p> <p>注 如果会话在容器联合内的其他容器中运行，则不会显示任何信息。</p>
类型	<p>显示有关桌面授权类型的信息。</p> <ul style="list-style-type: none"> 对于本地授权，显示“本地”。
vCenter	<p>显示 vCenter Server 中虚拟机的名称。</p> <p>注 如果会话在容器联合内的其他容器中运行，则不会显示任何信息。</p>
默认协议	桌面会话的默认显示协议。

活动

活动选项卡显示有关用户活动的事件日志信息。您可以按时间范围（如过去 12 小时或过去 30 天）或按管理员名称筛选活动。单击**仅技术支持事件**可仅按 Horizon Help Desk Tool 活动进行筛选。单击刷新图标可刷新事件日志。单击导出图标可将事件日志导出为文件。

注 在 Cloud Pod 架构环境中，不会显示用户的事件日志信息。

表 9-3. 活动

选项	说明
时间	选择时间范围。默认值为过去 12 小时。 <ul style="list-style-type: none"> ■ 过去 12 小时 ■ 过去 24 小时 ■ 过去 7 天 ■ 过去 30 天 ■ 全部
管理员	管理员用户的名称。
消息	向用户或管理员显示特定于用户或管理员所执行活动的消息。
资源名称	显示有关执行活动时所在的桌面池或虚拟机名称的信息。

Horizon Help Desk Tool 的会话详细信息

单击会话选项卡的计算机名称选项中的用户名时，会话详细信息会显示在详细信息选项卡中。您可以查看 Horizon Client、虚拟或已发布桌面以及 CPU 和内存的详细信息。

客户端

显示的信息取决于 Horizon Client 的类型，这些信息包括用户名、Horizon Client 的版本、客户端计算机的 IP 地址和客户端计算机的操作系统等详细信息。

注 如果升级了 Horizon Agent，您还必须将 Horizon Client 升级到最新版本。否则，不会显示 Horizon Client 的版本。有关升级 Horizon Client 的更多信息，请参阅《Horizon 7 升级指南》文档。

虚拟机

显示有关虚拟桌面或已发布桌面的信息。

表 9-4. 虚拟机详细信息

选项	说明
计算机名称	桌面会话名称。
代理版本	Horizon Agent 版本。
操作系统版本	操作系统版本。
连接服务器	会话连接到的连接服务器。
池	桌面池名称。
vCenter	vCenter Server 的 IP 地址。
会话状态	桌面会话的状态。会话状态可能是已连接或已断开。
会话持续时间	会话保持连接到连接服务器的时间。
状态持续时间	会话保持处于同一状态的时间。
登录时间	用户登录到会话的时间。
登录时长	用户在 Linux 桌面上处于已登录状态的持续时间。

用户体验衡量指标

显示使用 VMware Blast 显示协议的虚拟或已发布桌面会话的性能详细信息。要查看这些性能详细信息，请单击[更多](#)。要刷新这些详细信息，请单击刷新图标。

表 9-5. Blast 显示协议详细信息

选项	说明
帧速率	Blast 会话中的帧速率（帧/秒）。
Skype 状态	对于 Linux 桌面会话，此选项显示为“不适用”。
BLAST 会话计数器	<ul style="list-style-type: none"> ■ 估计的带宽 (上行链路)。上行链路信号的估计带宽。 ■ 数据包丢失 (上行链路)。上行链路信号的数据包丢失百分比。
BLAST 图像处理计数器	<ul style="list-style-type: none"> ■ 发送的字节数。为进行 Blast 会话而发送的图像处理数据的总字节数。 ■ 接收的字节数。为进行 Blast 会话而接收的图像处理数据的总字节数。
BLAST 音频计数器	<ul style="list-style-type: none"> ■ 发送的字节数。为进行 Blast 会话而发送的音频数据的总字节数。 ■ 接收的字节数。为进行 Blast 会话而接收的音频数据的总字节数。
BLAST CDR 计数器	<ul style="list-style-type: none"> ■ 发送的字节数。为进行 Blast 会话而发送的客户端驱动器重定向数据的总字节数。 ■ 接收的字节数。为进行 Blast 会话而接收的客户端驱动器重定向数据的总字节数。

CPU 和内存使用情况及网络和磁盘性能

显示虚拟或已发布桌面的 CPU 和内存使用情况图表，以及 Blast 显示协议的网络或磁盘性能图表。

注 在桌面上启动或重新启动 Horizon Agent 后，性能图表可能不会立即显示时间轴。时间轴会在几分钟后显示。

表 9-6. CPU 使用情况

选项	说明
会话 CPU	当前会话的 CPU 使用情况。
主机 CPU	向其分配会话的虚拟机的 CPU 使用情况。

表 9-7. 内存使用情况

选项	说明
会话内存	当前会话的内存使用情况。
主机内存	向其分配会话的虚拟机的内存使用情况。

表 9-8. 网络性能

选项	说明
延迟	显示 PCoIP 或 Blast 会话的延迟图表。 延迟时间为往返时间（以毫秒为单位）用于跟踪此延迟时间的性能计数器是 VMware Blast 会话计数器 > RTT 。

表 9-9. 磁盘性能

选项	说明
读取	每秒读取输入/输出 (Input/Output, I/O) 操作的次数。
写入	每秒写入 I/O 操作的数量。
磁盘延迟	显示磁盘延迟的图表。磁盘延迟是从 Windows 性能计数器中检索每秒输入/输出操作 (Input/Output Operations Per Second, IOPS) 数据的时间（以毫秒为单位）。
平均读取速率	每秒随机读取 I/O 操作的平均次数。
平均写入速率	每秒随机写入 I/O 操作的平均次数。
平均延迟	从 Windows 性能计数器中检索 IOPS 数据的平均延迟时间（以毫秒为单位）。

会话登录分段

显示登录时长以及在登录过程中创建的使用情况分段。

表 9-10. 会话登录分段

选项	说明
登录时长	从用户单击桌面池到用户登录到 Linux 桌面所用的时间长度。
会话登录时间	用户登录到会话的时间长度。
登录分段	<p>显示在登录过程中创建的分段。</p> <ul style="list-style-type: none"> ■ 代理。连接服务器处理会话连接或重新连接的总时间。从用户单击桌面池时开始计算，直到设置了安全加密链路连接时为止。包括完成各项连接服务器任务（例如用户身份验证、计算机选择和为设置安全加密链路连接准备计算机）所用的时间。 ■ 交互式。Horizon Agent 处理会话连接或重新连接的总时间。从 Blast Extreme 使用隧道连接时开始计算，直到用户登录到 Linux 桌面时为止。 ■ 协议连接。在登录过程中完成 PCoIP 或 Blast 协议连接所用的总时间。 ■ 登录脚本。登录脚本从开始执行到完成所用的总时间。 ■ 身份验证。连接服务器对会话进行身份验证的总时间。 ■ 虚拟机启动。启动虚拟机所用的总时间。该时间包括引导操作系统、恢复挂起的计算机的时间，以及 Horizon Agent 发出信号表明它已做好连接准备的时间。

Horizon Help Desk Tool 的会话进程

单击会话选项卡的计算机名称选项中的用户名时，会话进程会显示在进程选项卡中。

进程

对于每个会话，您可以查看有关 CPU 和内存相关进程的其他详细信息。例如，如果您发现会话的 CPU 和内存使用情况异常高，则可以在进程选项卡中查看该进程的详细信息。

对于 RDS 主机会话，进程选项卡会显示由当前用户或当前系统进程启动的当前 RDS 主机会话进程。

表 9-11. 会话进程详细信息

选项	说明
进程名称	会话进程的名称。例如，chrome.exe。
CPU	进程的 CPU 使用情况，以百分比为单位。
内存	进程的内存使用情况，以 KB 为单位。
磁盘	内存磁盘 IOPS。使用以下公式进行计算： (当前时间的 I/O 总字节数) - (当前时间前一秒的 I/O 总字节数)。 如果任务管理器显示正值，此计算可以显示值为 0 KB/秒。
用户名	进程所属的用户的用户名。
主机 CPU	向其分配会话的虚拟机的 CPU 使用情况。
主机内存	向其分配会话的虚拟机的内存使用情况。
进程	虚拟机中的进程计数。
刷新	刷新图标可刷新进程列表。
结束进程	结束正在运行的进程。
	<p>注 您必须具有技术支持管理员角色才能结束进程。</p> <p>要结束进程，请选择相应的进程，然后单击结束进程按钮。</p> <p>您无法结束进程选项卡中可能会列出的关键进程，例如 Windows 核心进程。如果要结束某个关键进程，则 Horizon Help Desk Tool 会显示一条消息，指示其无法结束此系统进程。</p>

在 Horizon Help Desk Tool 中对 Linux 桌面会话进行故障排除

在 Horizon Help Desk Tool 中，您可以根据用户的连接状态对 Linux 桌面会话进行故障排除。

前提条件

- 启动 Horizon Help Desk Tool。

步骤

- 1 在用户卡上，单击会话选项卡。

此时将出现一个性能卡，其中显示了 CPU 和内存使用情况，并包含有关 Horizon Client 以及虚拟桌面或已发布的桌面的信息。

2 选择一个故障排除选项。

选项	操作
发送消息	向已发布的桌面或虚拟桌面上的用户发送消息。您可以选择消息的严重性以包含“警告”、“信息”或“错误”。 单击 发送消息 ，输入严重性类型和消息详细信息，然后单击 提交 。
重新启动	在虚拟桌面上启动重新启动过程。此功能不适用于已发布的桌面会话。 单击 重新启动 VDI 。
断开连接	断开桌面或应用程序会话连接。 单击 更多 > 断开连接 。
注销	为已发布的桌面或虚拟桌面启动注销过程。 单击 更多 > 注销 。
重置	启动虚拟机重置操作。此功能不适用于已发布的桌面。 单击 更多 > 重置虚拟机 。
	注 用户可能会丢失未保存的工作。

收集 Horizon 7 for Linux 计算机的诊断信息

您可以收集诊断信息以协助 VMware 技术支持部门诊断并解决 Horizon 7 for Linux 计算机存在的问题。您可以创建数据收集工具 (Data Collection Tool, DCT) 捆绑包，用来收集计算机的配置信息并记录到压缩的 tarball 中。

步骤

- 1 以具有必需特权的用户身份登录 Linux 虚拟机。
- 2 打开命令提示符，然后运行 `dct-debug.sh` 脚本。

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

该脚本将生成包含 DCT 捆绑包的 tarball。例如：

```
ubuntu-12-vdm-sdct-20150201-0606-agent.tgz
```

将在执行该脚本的目录（当前的工作目录）中生成 tarball。

对远程桌面和客户端主机之间的复制和粘贴问题进行故障排除

在远程桌面和客户端主机之间复制和粘贴所支持的最大 1 MB 数据时，需要超过 3 秒钟时间。如果复制和粘贴少量数据，则不会出现此问题。

问题

如果为 SLED 11 SP3/SP4 桌面配置 1 个 vCPU 和 1 GB 内存，则在远程桌面和本地客户端主机之间进行复制和粘贴操作所需的时间可能超过 3 秒钟。

原因

复制和粘贴操作发生延迟可能是由于 SLED 11 SP3/SP4 的操作系统 API 较旧所导致。

解决方案

- ◆ 为 SLED 11 SP3/SP4 配置两个 vCPU 和 2 GB 内存。

Horizon Agent 在 iPad Pro Horizon Client 上无法断开连接

在 iPad Pro Horizon Client 上执行重新启动或关机操作后，无法断开 SUSE Horizon Agent 连接。

问题

当您在 iPad Pro Horizon Client 上重新启动或关闭 SUSE 虚拟机时，桌面没有响应。Horizon Agent 无法断开连接。

原因

SUSE 计算机在执行重新启动或关闭操作后可能没有将消息正确发送到 Horizon Client。

解决方案

- ◆ 从 iPad Pro Horizon Client 手动断开桌面连接。

SLES 12 SP1 桌面不自动刷新

在多显示器模式下，SLES 12 SP1 在您拖动 GNOME 终端时不会自动刷新。

问题

在多显示器模式下启动 SLES 12 SP1 并返回到窗口模式后，桌面在您拖动 GNOME 终端时不会自动刷新。

原因

GNOME 终端不对拖动操作做出响应。

解决方案

- 1 结束 GNOME Shell 会话。

```
kill -9 <process id of gnome-shell>
```

- 2 再次重新启动 GNOME Shell 会话。

SSO 无法连接到关机代理

单点登录 (SSO) 无法连接到关机代理。

问题

在以代理身份登录并连接到某个代理时，SSO 无法连接到关机代理。

解决方案

- ◆ 手动登录到桌面，或断开代理连接，然后再重新连接到代理。

在创建适用于 Linux 的手动桌面池后无法访问虚拟机

虚拟机状态没有响应。

问题

在您创建手动桌面池后，虚拟机状态可能为“正在等待代理”或“无法访问”。

原因

可能有几个用户错误配置或设置导致虚拟机状态为“无法访问”或“正在等待代理”。

- 确认虚拟机 vmx 配置文件中存在 machine.id 选项。

如果该选项不存在，则确认虚拟机已被正确添加到桌面池中。否则，请重新创建桌面池，以让代理将该选项重新写入 vmx 配置文件。

- 确认已正确安装 VMware Tool 或 Open VM Tool。

如果未正确执行安装 VMware Tool 或 Open VM Tool 的步骤，则 Linux 虚拟机中的 PATH 下可能不存在 vmware-rpctool 命令。您必须按照向导来安装 VMware Tool 或 Open VM Tool。

完成安装后，请运行以下命令。

```
#vmware-rpctool "machine.id.get"
```

将从虚拟机 vmx 配置文件中列出 machine.id 值。

- 确认代理的 FQDN 可在代理 Linux 虚拟机中被解析为 IP 地址。