



Linux Virtual Delivery Agent 7.15

Contents

新增功能	3
已修复的问题	3
已知问题	5
第三方声明	6
系统要求	6
安装概述	10
配置 Delivery Controller	10
轻松安装	12
安装 Linux Virtual Delivery Agent for RHEL/CentOS	22
安装 Linux Virtual Delivery Agent for SUSE	50
安装 Linux Virtual Delivery Agent for Ubuntu	73
配置 Linux VDA	96
将 NIS 与 Active Directory 集成	96
发布应用程序	102
打印	103
PDF 打印	108
配置图形	109
非 GRID 3D 图形	114
配置策略	116
策略支持列表	118
配置 IPv6	123
配置 Citrix 客户体验改善计划 (CEIP)	124
配置 USB 重定向	126

客户端输入法编辑器 (IME)	134
HDX Insight	135
启用跟踪	136
配置未经身份验证的会话	139
配置 LDAPS	141
配置 Xauthority	145

新增功能

October 9, 2022

发布日期: 2022 年 7 月 7 日

7.15 中的新增功能

累积更新 9 (CU9) 是 Linux VDA 7.15 LTSR 的最新版本。与 Linux VDA 7.15 CU8 相比, CU9 增加了一个[修复](#)。

PDF 打印

以前作为实验性功能提供的 [PDF 打印](#)在此版本中完全受支持。此功能允许 Citrix Receiver for Chrome 和 Citrix Receiver for HTML5 的用户打印从其 Linux VDA 会话内部转换的 PDF。

系统行为变更

自此版本起, 不必在升级 Linux VDA 后运行 `ctxsetup.sh` 脚本。

已修复的问题

August 8, 2022

CU9 中已修复的问题

- 在 SUSE 或 RHEL 上卸载 Linux VDA 可能不会删除 `/opt/Citrix/` 位置中的空文件夹。[CVADHELP-18241]

CU8 中已修复的问题

- 启用通道绑定后, 尝试向 Delivery Controller 注册 Linux VDA 可能会失败。[CVADHELP-14481]

CU6 中已修复的问题

- 如果鼠标和键盘的焦点不在同一窗口中或者鼠标无法更改焦点, Linux 会话可能会变得无响应。[CVADHELP-12768]

- 通常情况下，尝试将可移动 USB 驱动器重定向到 Linux VDA 可能会失败。USB 驱动器为 NTFS（New Technology File System，新技术文件系统）格式化时会出现此问题。[CVADHELP-13675]
- Linux VDA 可能无法达到目标帧速率 (FramesPerSecond) 设置中指定的每秒帧数。在 Linux VDA 上安装 GPU 时会出现此问题。[CVADHELP-14267]

CU5 中已修复的问题

- 尝试使用剪贴板功能在客户端与会话之间复制和粘贴内容可能会失败。[LD2047]
- 在 Linux VDA 上启动会话并执行操作时，会话可能会断开连接。[LD2257]

CU4 中已修复的问题

- 尝试从端点复制内容并将其粘贴到在 Linux VDA 上运行的应用程序中时，可能不会复制该内容。[LC8760]
- 键盘可能无法在 SUSE Linux Enterprise Server 11 Service Pack 4 上起作用。因此，屏幕上不显示击键，键盘布局设置不正确。[LC9906]
- **ctxctl** 进程可能无法在 Linux VDA 上的用户会话中运行。[LD0353]

CU3 中已修复的问题

- Linux VDA 可能无法应用 Citrix 策略。配置要在 NetScaler Gateway 中使用访问控制元素连接类型的策略时会出现此问题。[LC9842]

CU2 中已修复的问题

- 使用 Delivery Controller 注册 Linux VDA 可能会间歇性失败。[LC7982]
- 在 Red Hat Enterprise Linux Server 7.3 中运行的 Citrix Director 7.13 可能不显示计算机的会话详细信息。此时将显示以下错误消息：
无法检索数据。[LC8204]
- 一段时间后，Linux VDA 可能会在 Delivery Controller 中注册并取消注册。[LC8205]
- 用于检查 Linux VDA 的会话显示的某些第三方应用程序可能无法显示所有像素。[LC8419]
- 存在多个 LDAP 服务器时，在更新了策略并且会话超时时，尝试在 Linux VDA 上启动应用程序可能会失败。[LC8444]
- 与 Linux VDA 连接会话时，ctxhdx 进程可能会意外退出并显示 **segfault** 错误。[LC8611]
- 使用 Linux VDA 7.16 早期访问版本时，Broker 代理可能无法获取应用程序名称。此故障会导致 Director 显示错误已请求代理，之后将开始重新注册。[LC9243]

CU1 中已修复的问题

- 一段时间后，Linux VDA 可能会在 Delivery Controller 中注册并取消注册。[LC8205]
- 用于检查 Linux VDA 的会话显示的某些第三方应用程序可能无法显示所有像素。[LC8419]
- 存在多个 LDAP 服务器时，在更新了策略并且会话超时后，尝试在 Linux VDA 上启动应用程序可能会失败。[LC8444]

7.15 LTSR 中已修复的问题

本 Linux VDA 版本中解决了以下问题：

- 输入 DNS IP 地址时，轻松安装可能会导致 Linux VDA 与网络断开连接。[LNXVDA-2152]
- 播放视频时，从 Citrix Receiver for Windows 到 Citrix Receiver for Android 的会话漫游失败。[LNXVDA-2164]

已知问题

August 8, 2022

在本版本中确定了以下问题：

- 与 XenApp 和 XenDesktop 7.15 LTSR CU6 集成的 Citrix Scout 无法从 Linux VDA 7.15 收集日志。Linux VDA 7.15 不支持 Citrix Scout 用于收集日志的 Citrix Telemetry Service。
- `indicator-datetime-service` 进程不使用 `$TZ` 环境变量。当客户端和会话位于不同的时区时，Ubuntu 16.04 Unity Desktop 上的 unity 面板不显示客户端的时间。[LNXVDA-2128]
- Ubuntu 图形：在 HDX 3D Pro 中，调整 Desktop Viewer 的大小后，应用程序周围可能会显示一个黑框，或者有时背景会显示为黑色。
- 注销会话后，可能不会删除 Linux VDA 打印重定向创建的打印机。
- 目录中包含大量文件和子目录时会遗失 CDM 文件如果客户端有太多文件或目录，则可能会出现此问题。
- 在本版本中，仅支持对非英语语言使用 UTF-8 编码。
- Citrix Receiver for Android 的 Caps Lock 键状态可能会在会话漫游期间反转。与 Citrix Receiver for Android 的现有连接漫游时，Caps Lock 键的状态可能会丢失。解决方法：使用扩展键盘上的 Shift 键在大写与小写之间切换。
- 使用 Citrix Receiver for Mac 连接至 Linux VDA 时，含 Alt 的快捷键有时不起作用。默认情况下，对于左侧和右侧 Options/Alt 键，Citrix Receiver for Mac 都会发送 AltGr。您可以在 Citrix Receiver 设置中修改此行为，但是结果因不同的应用程序而异。

- Linux VDA 重新加入域时注册失败。重新加入将生成一组全新的 Kerberos 密钥。但是，Broker 可能会根据先前的一组 Kerberos 密钥使用缓存的过时 VDA 服务票据。VDA 尝试连接到 Broker 时，Broker 可能无法与 VDA 建立返回安全上下文。常见症状是 VDA 注册失败。

VDA 服务票据过期并续订后，此问题最终会自行解决。但是，由于服务票据的有效期很长，因此可能需要很长时间。

解决方法：清除 Broker 的票据缓存。重新启动 Broker 或在 Broker 上以管理员身份从命令提示窗口运行以下命令：

```
1 klist -li 0x3e4 purge
2 <!--NeedCopy-->
```

此命令会清除 Citrix Broker Service 运行所在的网络服务主体持有的 LSA 缓存中的所有服务票据。此命令也会删除其他 VDA 的服务票据，因而可能会影响其他服务。但是，此操作不会造成负面影响，因为这些服务可在需要时从 KDC 重新获取这些服务票据。

- 不支持音频即插即用。您可以先将音频捕获设备连接到客户端计算机，然后开始在 ICA 会话中录制音频。如果在启动了音频录制应用程序后连接捕获设备，应用程序可能会无响应，因此您必须将其重新启动。如果在录制期间拔下捕获设备，可能会出现类似的问题。
- Citrix Receiver for Windows 可能会在音频录制期间遇到音频失真问题。

第三方声明

August 11, 2022

[Linux Virtual Desktop Version 7.15](#) (PDF 下载)

此 Linux VDA 版本可能包含根据该文档中定义的条款许可使用的第三方软件。

系统要求

November 8, 2021

Linux 发行版

Linux VDA 支持以下 Linux 发行版：

- SUSE Linux Enterprise:
 - Desktop 12 Service Pack 2

- Server 12 Service Pack 2
- Server 11 Service Pack 4
- Red Hat Enterprise Linux
 - Workstation 7.3
 - Workstation 6.9
 - Workstation 6.6
 - Server 7.3
 - Server 6.9
 - Server 6.6
- CentOS Linux
 - CentOS 7.3
 - CentOS 6.6
- Ubuntu Linux
 - Ubuntu Desktop 16.04 (配备了 4.4.x 内核)
 - Ubuntu Server 16.04 (配备了 4.4.x 内核)

有关此 Linux VDA 版本支持的 Linux 发行版和 Xorg 版本列表，请参阅下表。有关详细信息，请参阅 [XorgModuleABIVersions](#)。

Linux 发行版	Xorg 版本
RHEL 7.3、CentOS 7.3	1.17
RHEL 6.9	1.17
RHEL 6.6、CentOS 6.6	1.15
Ubuntu 16.04	1.18
SUSE 12.2	1.18
SUSE 11.4	1.6.5

请勿在 Ubuntu 16.04 上使用 HWE Xorg server 1.19。

在所有情况下，受支持的处理器架构均为 x86-64。

注意：

当 Linux 操作系统供应商提供的支持过期时，Citrix 对该操作系统平台和版本的支持也将过期。

重要：

Gnome 和 KDE 桌面在 SUSE、RHEL 和 CentOS 中受支持。仅 Ubuntu 支持 Unity 桌面。至少必须安装一种

桌面。

XenDesktop

Linux VDA 与当前所有受支持的 XenDesktop 版本兼容。要获取有关 XenDesktop 产品生命周期的信息，以及了解何时 Citrix 会停止支持特定的产品版本，请参阅 [Citrix 产品生命周期表](#)。

Linux VDA 与 Windows VDA 的配置过程略有差别。但是，所有 Delivery Controller 场都能为 Windows 和 Linux 桌面提供代理服务。

注意：

Linux VDA 与 XenDesktop 7.0 版或更低版本不兼容。

Citrix Receiver

支持使用以下版本的 Citrix Receiver：

- Citrix Receiver for UWP（通用 Windows 平台）1.0 版
- Citrix Receiver for Windows 4.8 版或更高版本
- Citrix Receiver for Linux 13.5 版
- Citrix Receiver for Mac OSX 12.6 版
- Citrix Receiver for Android 3.11 版
- Citrix Receiver for iOS 7.2 版
- Citrix Receiver for Chrome 2.5 版
- Citrix Receiver for HTML5 2.5 版（只能通过 Access Gateway 使用）

虚拟机管理程序

支持使用以下虚拟机管理程序托管 Linux VDA 客户机虚拟机：

- XenServer
- VMware ESX 和 ESXi
- Microsoft Hyper-V
- Nutanix AHV

也支持裸机托管。

提示：

有关受支持平台的列表，请参阅供应商的文档。

Active Directory 集成软件包

Linux VDA 支持以下 Active Directory 集成软件包或产品：

- Samba Winbind
- Quest Authentication Services v4.1 或更高版本
- Centrify DirectControl
- SSSD

提示：

有关受支持平台的列表，请参阅 Active Directory 集成软件包供应商提供的文档。

HDX 3D Pro

需要以下虚拟机管理程序、Linux 发行版和 NVIDIA GRID™ GPU 才能支持 HDX 3D Pro。

虚拟机管理程序

支持以下虚拟机管理程序：

- XenServer
- VMware ESX 和 ESXi
- Nutanix AHV

Linux 发行版

以下 Linux 发行版支持 HDX 3D Pro：

- Red Hat Enterprise Linux - Workstation 7.3
- Red Hat Enterprise Linux - Server 7.3
- Red Hat Enterprise Linux - Workstation 6.9
- Red Hat Enterprise Linux - Server 6.9
- Red Hat Enterprise Linux - Workstation 6.6
- Red Hat Enterprise Linux - Server 6.6
- SUSE Linux Enterprise Desktop 12 Service Pack 2
- SUSE Linux Enterprise Server 12 Service Pack 2
- Ubuntu Linux Desktop 16.04
- Ubuntu Linux Server 16.04

GPU

以下 GPU 支持 GPU 直通：

- NVIDIA GTX750Ti
- NVIDIA GRID - Tesla M60
- NVIDIA GRID - K2

以下 GPU 支持 vGPU：

- NVIDIA GRID - Tesla M60
- NVIDIA GRID - Tesla M10

安装概述

February 15, 2019

安装 Linux Virtual Delivery Agent (VDA) 与所有受支持的 Linux 发行版遵循相同的常规步骤。

1. 准备安装。
2. 准备虚拟机管理程序。
3. 向 Windows 域中添加 Linux 虚拟机 (VM)。
4. 安装 Linux VDA。
5. 配置 Linux VDA。
6. 在 XenApp 或 XenDesktop 中创建计算机目录。
7. 在 XenApp 或 XenDesktop 中创建交付组。

各种变体和特定命令按发行版进行记录。

配置 **Delivery Controller**

May 7, 2020

XenDesktop 7.6 及更早版本需要更改才能支持 Linux VDA。对于这些版本，需要运行修补程序或更新脚本。安装和验证信息在本文中提供。

更新 **Delivery Controller** 配置

对于 XenDesktop 7.6 SP2，请应用 Hotfix Update 2 更新 Linux 虚拟桌面的 Broker。Hotfix Update 2 可在以下位置找到：

- [CTX142438](#): Hotfix Update 2 - 适用于 Delivery Controller 7.6 (32 位) - 英文版
- [CTX142439](#): Hotfix Update 2 - 适用于 Delivery Controller 7.6 (64 位) - 英文版

对于早于 XenDesktop 7.6 SP2 的版本，可使用名为 **Update-BrokerServiceConfig.ps1** 的 PowerShell 脚本来更新 Broker Service 配置。以下软件包中提供此脚本：

- citrix-linuxvda-scripts.zip

对场内的每个 Delivery Controller 重复以下步骤：

1. 将 **Update-BrokerServiceConfig.ps1** 脚本复制到 Delivery Controller 计算机。
2. 在本地管理员上下文中打开 Windows PowerShell 控制台。
3. 浏览到包含 **Update-BrokerServiceConfig.ps1** 脚本的文件夹。
4. 运行 **Update-BrokerServiceConfig.ps1** 脚本：

```
1 .\Update-BrokerServiceConfig.ps1
2 <!--NeedCopy-->
```

提示：

PowerShell 的默认配置是禁止执行 PowerShell 脚本。如果脚本运行失败，请先更改 PowerShell 执行策略，然后再重试：

```
1 Set-ExecutionPolicy Unrestricted
2 <!--NeedCopy-->
```

Update-BrokerServiceConfig.ps1 脚本会使用 Linux VDA 所需的新 WCF 端点更新 Broker Service 配置文件，然后重新启动 Broker Service。该脚本会自动确定 Broker Service 配置文件的位置。系统会在同一个目录中为原始配置文件创建备份，并向文件名附加 **.prelinux**。

这些更改不会影响配置为使用同一个 Delivery Controller 场的 Windows VDA 的代理。一个 Controller 场可同时进行无缝管理和代理 Windows 和 Linux VDA 的会话。

验证 **Delivery Controller** 配置

当所需的配置更改已应用于 Delivery Controller 时，**EndpointLinux** 字符串会在 **%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config** 文件中出现五次。

在 Windows 命令提示窗口中，以本地管理员身份登录进行检查：

```
1 cd "%PROGRAMFILES%\Citrix\Broker\Service\
2 findstr EndpointLinux BrokerService.exe.config
3 <!--NeedCopy-->
```

轻松安装

June 21, 2022

从 Linux VDA 7.13 版起正式支持轻松安装。轻松安装通过自动安装必需的软件包并自定义配置文件来帮助您设置 Linux VDA 的运行环境。

支持的发行版

	Winbind	SSSD	Centrify
RHEL 7.3	是	是	是
RHEL 6.9	是	是	是
RHEL 6.6	是	是	是
CentOS 7.3	是	是	是
Ubuntu 16.04	是	是	是
SUSE 12.2	是	否	是

使用轻松安装

要使用此功能，请执行以下操作：

1. 准备配置信息和 Linux 计算机。
2. 安装 Linux VDA 软件包。
转至 Citrix Web 站点并根据您的 Linux 发行版下载相应的 Linux VDA 软件包。
3. 设置运行时环境以完成 Linux VDA 安装。

步骤 1：准备配置信息和 **Linux** 计算机

收集轻松安装所需的以下配置信息：

- 主机名 - 要安装 Linux VDA 的计算机的主机名
- 域名服务器的 IP 地址
- NTP 服务器的 IP 地址或字符串名称
- 域名 - 域的 NetBIOS 名称
- 领域名称 - Kerberos 领域名称
- 活动域的 FQDN - 完全限定域名

重要:

- 要安装 Linux VDA，请确认是否在 Linux 计算机上正确添加了存储库。
- 要启动会话，请确认是否安装了 X Windows 系统和桌面环境。

步骤 2: 安装 **Linux VDA** 软件包

运行以下命令为 Linux VDA 设置环境。

对于 RHEL 和 CentOS 发行版:

```
1 sudo yum -y localinstall <PATH>/<Linux VDA RPM>
2 <!--NeedCopy-->
```

对于 Ubuntu 发行版:

```
1 sudo dpkg -i <PATH>/<Linux VDA deb>
2 sudo apt-get install -f
3 <!--NeedCopy-->
```

对于 SUSE 发行版:

```
1 zypper -i install <PATH>/<Linux VDA RPM>
2 <!--NeedCopy-->
```

步骤 3: 设置运行时环境以完成安装

安装 Linux VDA 软件包后，使用 `ctxinstall.sh` 脚本来配置运行环境。可以在交互模式或无提示模式下运行该脚本。

交互模式:

要执行手动配置，请运行以下命令并在每个提示处键入相关参数。

```
1 sudo /opt/Citrix/VDA/sbin/ctxinstall.sh
2 <!--NeedCopy-->
```

无提示模式:

要在无提示模式下使用轻松安装，请先设置以下环境变量，然后再运行 `ctxinstall.sh`。

- **CTX_EASYINSTALL_HOSTNAME**=host-name -表示 Linux VDA 服务器的主机名。
- **CTX_EASYINSTALL_DNS**=ip-address-of-dns -DNS 的 IP 地址。
- **CTX_EASYINSTALL_NTPS**=address-of-ntps -NTP 服务器的 IP 地址或字符串名称。
- **CTX_EASYINSTALL_DOMAIN**=domain-name -域的 NetBIOS 名称
- **CTX_EASYINSTALL_REALM**=realm-name -Kerberos 领域名称。
- **CTX_EASYINSTALL_FQDN**=ad-fqdn-name

- **CTX_EASYINSTALL_ADINTEGRATIONWAY**=winbind | sssd | centrify -表示 Active Directory 集成方法。
- **CTX_EASYINSTALL_USERNAME**=domain-user-name -表示域用户的名称；用于加入域。
- **CTX_EASYINSTALL_PASSWORD**=password -指定域用户的密码；用于加入域。

以下变量由 ctxsetup.sh 使用：

- **CTX_XDL_SUPPORT_DDC_AS_CNAME**=Y | N - Linux VDA 支持使用 DNS CNAME 记录指定 Delivery Controller 名称。
- **CTX_XDL_DDC_LIST**=list-ddc-fqdns -Linux VDA 要求提供由空格分隔的 Delivery Controller 完全限定域名 (FQDN) 列表以用于向 Delivery Controller 注册。必须至少指定一个 FQDN 或 CNAME。
- **CTX_XDL_VDA_PORT**=port-number -Linux VDA 将通过 TCP/IP 端口与 Delivery Controller 通信。
- **CTX_XDL_REGISTER_SERVICE**=Y | N -在启动计算机后启动 Linux Virtual Desktop 服务。
- **CTX_XDL_ADD_FIREWALL_RULES**=Y | N -Linux Virtual Desktop 服务要求允许传入网络连接通过系统防火墙。您可以在系统防火墙中自动为 Linux Virtual Desktop 打开所需端口（默认为端口 80 和 1494）。
- **CTX_XDL_HDX_3D_PRO**=Y | N -Linux VDA 支持 HDX 3D Pro，这是一组 GPU 加速技术，旨在优化富图形应用程序的虚拟化水平。如果选择了 HDX 3D Pro，则要为 VDI 桌面（单会话）模式配置 VDA -（即 CTX_XDL_VDI_MODE=Y）。
- **CTX_XDL_VDI_MODE**=Y | N -将计算机配置为专用桌面交付模型 (VDI) 还是托管共享桌面交付模型。对于 HDX 3D Pro 环境，将该值设置为 Y。
- **CTX_XDL_SITE_NAME**=dns-name -Linux VDA 通过 DNS 发现 LDAP 服务器。要将 DNS 搜索结果限制为本地站点，应指定 DNS 站点名称。如果不需要，可以将其设置为 **<none>**。
- **CTX_XDL_LDAP_LIST**=list-ldap-servers -Linux VDA 查询 DNS 来发现 LDAP 服务器。如果 DNS 无法提供 LDAP 服务记录，您可以提供以空格分隔的 LDAP FQDN（带有 LDAP 端口）列表。例如 ad1.mycompany.com:389。如果不需要，可以将其设置为 **<none>**。
- **CTX_XDL_SEARCH_BASE**=search-base-set -Linux VDA 通过设置为 Active Directory 域根的搜索库来查询 LDAP（例如，DC=mycompany,DC=com）。为提高搜索性能，可以指定搜索基础（例如 OU=VDI,DC=mycompany,DC=com）。如果不需要，可以将其设置为 **<none>**。
- **CTX_XDL_START_SERVICE**=Y | N -在完成配置后，是否启动 Linux VDA 服务。

如果未设置任何参数，安装将回滚到交互模式，提示用户输入。已通过环境变量设置所有参数时，ctxinstall.sh 脚本不会提示要求提供答案。

在无提示模式下，必须运行以下命令以设置环境变量，然后运行 ctxinstall.sh 脚本。

```

1 export CTX_EASYINSTALL_HOSTNAME=host-name
2
3 export CTX_EASYINSTALL_DNS=ip-address-of-dns
4
5 export CTX_EASYINSTALL_NTPS=address-of-ntps
6
7 export CTX_EASYINSTALL_DOMAIN=domain-name
8
9 export CTX_EASYINSTALL_REALM=realm-name
10
```

```
11 export CTX_EASYINSTALL_FQDN=ad-fqdn-name
12
13 export CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify
14
15 export CTX_EASYINSTALL_USERNAME=domain-user-name
16
17 export CTX_EASYINSTALL_PASSWORD=password
18
19 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N
20
21 export CTX_XDL_DDC_LIST=list-ddc-fqdns
22
23 export CTX_XDL_VDA_PORT=port-number
24
25 export CTX_XDL_REGISTER_SERVICE=Y | N
26
27 export CTX_XDL_ADD_FIREWALL_RULES=Y | N
28
29 export CTX_XDL_HDX_3D_PRO=Y | N
30
31 export CTX_XDL_VDI_MODE=Y | N
32
33 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
34
35 export CTX_XDL_LDAP_LIST=list-ldap-servers | '<none>'
36
37 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
38
39 export CTX_XDL_START_SERVICE=Y | N
40
41 sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh
42 <!--NeedCopy-->
```

运行 `sudo` 命令时，键入 `-E` 选项以将现有环境变量传递给它创建的新 shell。Citrix 建议使用前面的命令并加上 `#!/bin/bash` 作为第一行来创建 shell 脚本文件。

或者，您可以使用单个命令指定所有参数：

```
1 sudo CTX_EASYINSTALL_HOSTNAME=host-name \  
2  
3 CTX_EASYINSTALL_DNS=ip-address-of-dns \  
4  
5 CTX_EASYINSTALL_NTPS=address-of-ntp \  
6  
7 CTX_EASYINSTALL_DOMAIN=domain-name \  
8  
9 CTX_EASYINSTALL_REALM=realm-name \  
10  
11 .....  
12  
13 CTX_XDL_SEARCH_BASE=search-base-set \  
14  
15 CTX_XDL_START_SERVICE=Y \  
16
```

```

16
17 /opt/Citrix/VDA/sbin/ctxinstall.sh
18 <!--NeedCopy-->

```

注意事项

- 默认情况下，工作组名称是域名。要在您的环境中自定义工作组，请执行以下操作：
 - a. 在 Linux VDA 计算机上创建 tmp/ctxinstall.conf 文件。
 - b. 将 “wworkgroup=\< 您的工作组 \>” 行添加到文件中。
- Centrify 不支持纯 IPv6 DNS 配置。/etc/resolv.conf 中至少需要有一个使用 IPv4 的 DNS 服务器，`adclient` 才能正确查找 AD 服务。
- 对于 CentOS 上的 Centrify，轻松安装可能会在 Centrify 环境检查工具 `adcheck` 处失败，并报告以下错误：

日志：

```

1  ADSITE    : Check that this machine's subnet is in a site known by
      AD      : Failed
2           : This machine's subnet is not known by AD.
3           : We guess you should be in the site Site1.
4  <!--NeedCopy-->

```

此问题是由 Centrify 的特殊配置所致。要解决此问题，请执行以下操作：

- a. 在 Delivery Controller 上打开管理工具。
 - b. 选择 **Active Directory** 站点和服务。
 - c. 为子网添加正确的子网地址。
- 如果选择 Centrify 作为加入域的方法，ctxinstall.sh 脚本需要 Centrify 软件包。ctxinstall.sh 获取 Centrify 软件包的方法有两种：
 - 轻松安装可帮助自动从 Internet 下载 Centrify 软件包。下面是每个发行版的给定 URL：
 - RHEL: `wget http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-rhel4-x86_64.tgz?_ga=1.178323680.558673738.1478847956`
 - CentOS: `wget http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-rhel4-x86_64.tgz?_ga=1.186648044.558673738.1478847956`
 - SUSE: `wget http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-suse10-x86_64.tgz?_ga=1.10831088.558673738.1478847956`
 - Ubuntu: `wget http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-deb7-x86_64.tgz?_ga=1.178323680.558673738.1478847956`
 - 从本地目录中提取 Centrify 软件包。要指定 Centrify 软件包的目录，请执行以下操作：

- a. 在 Linux VDA 服务器上创建 tmp/ctxinstall.conf 文件（如果该文件不存在）。
- b. 在文件中添加 “centrifypkgpath=<path name>” 行。

例如：

```

1  cat /tmp/ctxinstall.conf
2  set "centrifypkgpath=/home/mydir"
3  ls -ls /home/mydir
4      9548 -r-xr-xr-x. 1 root root 9776688 May 13
      2016 adcheck-rhel4-x86_64
5      4140 -r--r--r--. 1 root root 4236714 Apr 21
      2016 centrifysda-3.3.1-rhel4-x86_64.rpm
6      33492 -r--r--r--. 1 root root 34292673 May
13  2016 centrifysdc-5.3.1-rhel4-x86_64.rpm
7      4 -rw-rw-r--. 1 root root 1168 Dec 1
      2015 centrifysdc-install.cfg
8      756 -r--r--r--. 1 root root 770991 May 13
      2016 centrifysdc-ldapproxy-5.3.1-rhel4-x86_64.rpm
9      268 -r--r--r--. 1 root root 271296 May 13
      2016 centrifysdc-nis-5.3.1-rhel4-x86_64.rpm
10     1888 -r--r--r--. 1 root root 1930084 Apr 12
      2016 centrifysdc-openssh-7.2p2-5.3.1-rhel4-x86_64.rpm
11     124 -rw-rw-r--. 1 root root 124543 Apr 19
      2016 centrifys-suite.cfg
12     0 lrwxrwxrwx. 1 root root 10 Jul 9
      2012 install-express.sh -> install.sh
13     332 -r-xr-xr--. 1 root root 338292 Apr 10
      2016 install.sh
14     12 -r--r--r--. 1 root root 11166 Apr 9
      2015 release-notes-agent-rhel4-x86_64.txt
15     4 -r--r--r--. 1 root root 3732 Aug 24
      2015 release-notes-da-rhel4-x86_64.txt
16     4 -r--r--r--. 1 root root 2749 Apr 7
      2015 release-notes-nis-rhel4-x86_64.txt
17     12 -r--r--r--. 1 root root 9133 Mar 21
      2016 release-notes-openssh-rhel4-x86_64.txt
18  <!--NeedCopy-->

```

故障排除

请使用此部分中的信息对可能因使用此功能而引发的问题进行故障排除。

使用 **SSSD** 加入域失败

尝试加入域时可能会出现错误，输出类似如下（要进行屏幕打印，请验证日志）：

```
Step 6: join Domain!Enter ctxadmin's password:Failed to join domain:
failed to lookup DC info for domain 'CITRIXLAB.LOCAL'over rpc: The
network name cannot be found
```

/var/log/xdl/vda.log:

```

1 2016-11-04 02:11:52.317 [INFO ] - The Citrix Desktop Service
  successfully obtained the following list of 1 delivery controller(s)
  with which to register: 'CTXDDC.citrixlab.local (10.158.139.214)'.
2 2016-11-04 02:11:52.362 [ERROR] - RegistrationManager.
  AttemptRegistrationWithSingleDdc: Failed to register with http://
  CTXDDC.citrixlab.local:80/Citrix/CdsController/IRegistrar. Error:
  General security error (An error occurred in trying to obtain a TGT:
  Client not found in Kerberos database (6))
3 2016-11-04 02:11:52.362 [ERROR] - The Citrix Desktop Service cannot
  connect to the delivery controller 'http://CTXDDC.citrixlab.local
  :80/Citrix/CdsController/IRegistrar' (IP Address '10.158.139.214')
4 Check the following:- The system clock is in sync between this machine
  and the delivery controller.
5 - The Active Directory provider (e.g. winbind daemon) service is
  running and correctly configured.
6 - Kerberos is correctly configured on this machine.
7 If the problem persists, please refer to Citrix Knowledge Base article
  CTX117248 for further information.
8 Error Details:
9 Exception 'General security error (An error occurred in trying to
  obtain a TGT: Client not found in Kerberos database (6))' of type '
  class javax.xml.ws.soap.SOAPFaultException'.
10 2016-11-04 02:11:52.362 [INFO ] - RegistrationManager.
  AttemptRegistrationWithSingleDdc: The current time for this VDA is
  Fri Nov 04 02:11:52 EDT 2016.
11 Ensure that the system clock is in sync between this machine and the
  delivery controller.
12 Verify the NTP daemon is running on this machine and is correctly
  configured.
13 2016-11-04 02:11:52.364 [ERROR] - Could not register with any
  controllers. Waiting to try again in 120000 ms. Multi-forest - false
14 2016-11-04 02:11:52.365 [INFO ] - The Citrix Desktop Service failed to
  register with any controllers in the last 470 minutes.
15 <!--NeedCopy-->

```

/var/log/messages:

```

Nov 4 02:15:27 RH-WS-68 [sssd[ldap_child[14867]]]: Failed to initialize
  credentials using keytab [MEMORY:/etc/krb5.keytab]: Client 'RH-WS-68
  $@CITRIXLAB.LOCAL'not found in Kerberos database. Unable to create
  GSSAPI-encrypted LDAP connection.Nov 4 02:15:27 RH-WS-68 [sssd[
  ldap_child[14867]]]: Client 'RH-WS-68$@CITRIXLAB.LOCAL'not found
  in Kerberos database

```

要解决此问题，请执行以下操作：

1. 运行 `rm -f /etc/krb5.keytab` 命令。
2. 运行 `net ads leave $REALM -U $domain-administrator` 命令。
3. 在 Delivery Controller 上删除计算机目录和交付组。

4. 运行 `/opt/Citrix/VDA/sbin/ctxinstall.sh`。
5. 在 Delivery Controller 上创建计算机目录和交付组。

Ubuntu 桌面会话显示灰屏

启动会话时会出现此问题，随后将在空桌面中阻止启动会话功能。此外，使用本地用户帐户登录时，服务器操作系统计算机的控制台也显示灰屏。

要解决此问题，请执行以下操作：

1. 运行 `sudo apt-get update` 命令。
2. 运行 `sudo apt-get install unity lightdm` 命令。
3. 向 `/etc/lightdm/lightdm.conf` 中添加以下行：
`greeter-show-manual-login=true`

由于缺少主目录，启动 **Ubuntu** 桌面会话失败

`/var/log/xdl/hdx.log`:

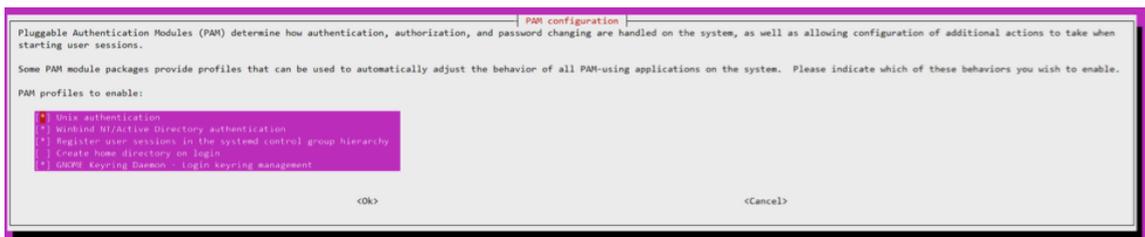
```
1 2016-11-02 13:21:19.015 <P22492:S1> citrix-ctxlogin: StartUserSession:  
   failed to change to directory(/home/CITRIXLAB/ctxadmin) errno(2)  
2  
3 2016-11-02 13:21:19.017 <P22227> citrix-ctxhdx: logSessionEvent:  
   Session started for user ctxadmin.  
4  
5 2016-11-02 13:21:19.023 <P22492:S1> citrix-ctxlogin: ChildPipeCallback:  
   Login Process died: normal.  
6  
7 2016-11-02 13:21:59.217 <P22449:S1> citrix-ctxgfx: main: Exiting  
   normally.  
8 <!--NeedCopy-->
```

提示：

此问题的根本原因是没有为域管理员创建主目录。

要解决此问题，请执行以下操作：

1. 在命令行中，键入 **pam-auth-update**。
2. 在生成的弹出窗口中，确认是否已选中 **Create home directory login**（创建主目录登录信息）。



会话无法启动或快速结束并显示 **dbus** 错误

/var/log/messages (适用于 RHEL 或 CentOS):

```
1 Oct 27 04:17:16 CentOS7 citrix-ctxhdx[8978]: Session started for user
  CITRIXLAB\ctxadmin.
2
3 Oct 27 04:17:18 CentOS7 kernel: traps: gnome-session[19146] trap int3
  ip:7f89b3bde8d3 sp:7fff8c3409d0 error:0
4
5 Oct 27 04:17:18 CentOS7 gnome-session[19146]: ERROR: Failed to connect
  to system bus: Exhausted all available authentication mechanisms (
  tried: EXTERNAL, DBUS_COOKIE_SHA1, ANONYMOUS) (available: EXTERNAL,
  DBUS_COOKIE_SHA1, ANONYMOUS)#012aborting...
6
7 Oct 27 04:17:18 CentOS7 gnome-session: gnome-session[19146]: ERROR:
  Failed to connect to system bus: Exhausted all available
  authentication mechanisms (tried: EXTERNAL, DBUS_COOKIE_SHA1,
  ANONYMOUS) (available: EXTERNAL, DBUS_COOKIE_SHA1, ANONYMOUS)
8
9 Oct 27 04:17:18 CentOS7 gnome-session: aborting...
10
11 Oct 27 04:17:18 CentOS7 citrix-ctxgfx[18981]: Exiting normally.
12
13 Oct 27 04:17:18 CentOS7 citrix-ctxhdx[8978]: Session stopped for user
  CITRIXLAB\ctxadmin.
14 <!--NeedCopy-->
```

或者, 对于 Ubuntu 发行版, 请使用日志 /var/log/syslog:

```
1 Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] pid.c:
  Stale PID file, overwriting.
2
3 Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] bluez5-
  util.c: Failed to get D-Bus connection: Did not receive a reply.
  Possible causes include: the remote application did not send a reply
  , the message bus security policy blocked the reply, the reply
  timeout expired, or the network connection was broken.
4
5 Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] hashmap
  .c: Assertion 'h' failed at pulsecore/hashmap.c:116, function
  pa_hashmap_free(). Aborting.
6
7 Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] core-
  util.c: Failed to connect to system bus: Did not receive a reply.
  Possible causes include: the remote application did not send a reply
  , the message bus security policy blocked the reply, the reply
  timeout expired, or the network connection was broken.
8
9 Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: message repeated 10
  times: [ [pulseaudio] core-util.c: Failed to connect to system bus:
  Did not receive a reply. Possible causes include: the remote
  application did not send a reply, the message bus security policy
```

```

    blocked the reply, the reply timeout expired, or the network
    connection was broken.]
10
11 Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] pid.c:
    Daemon already running.Nov  3 11:03:58 user01-HVM-domU citrix-ctxgfx
    [24693]: Exiting normally
12 <!--NeedCopy-->

```

某些组或模块在重新启动后才会生效。如果日志中出现 **dbus** 错误消息，Citrix 建议您重新启动系统并重试。

SELinux 可以防止 **SSHD** 访问主目录

用户可以启动会话，但不能登录。

/var/log/ctxinstall.log:

```

1 Jan 25 23:30:31 yz-rhel72-1 setroubleshoot[3945]: SELinux is preventing
  /usr/sbin/sshd from setattr access on the directory /root. For
  complete SELinux messages. run sealert -l 32f52c1f-8ff9-4566-a698
  -963a79f16b81
2
3 Jan 25 23:30:31 yz-rhel72-1 python[3945]: SELinux is preventing /usr/
  sbin/sshd from setattr access on the directory /root.
4
5 ***** Plugin catchall_boolean (89.3 confidence) suggests
  *****
6
7 If you want to allow polyinstantiation to enabled
8
9 Then you must tell SELinux about this by enabling the '
  polyinstantiation_enabled' boolean.
10
11 You can read 'None' man page for more details.
12
13 Do
14
15     setsebool -P polyinstantiation_enabled 1
16
17 ***** Plugin catchall (11.6 confidence) suggests
  *****
18
19 If you believe that sshd should be allowed setattr access on the root
  directory by default.
20
21 Then you should report this as a bug.
22
23 You can generate a local policy module to allow this access.
24
25 Do
26
27     allow this access for now by executing:
28

```

```
29 # grep sshd /var/log/audit/audit.log | audit2allow -M mypol
30
31 # semodule -i mypol.pp
32 <!--NeedCopy-->
```

要解决此问题，请执行以下操作：

1. 通过对 `/etc/selinux/config` 进行以下更改来禁用 SELinux。
`SELINUX=disabled`
2. 重新启动 VDA。

安装 Linux Virtual Delivery Agent for RHEL/CentOS

June 21, 2022

可以选择按照本文中的步骤进行手动安装，也可以使用[轻松安装](#)进行自动安装和配置。轻松安装省时又省力，与手动安装相比，更不易于出错。

注意：

请仅对全新安装使用轻松安装功能。请勿使用轻松安装更新现有安装。

步骤 1：为 VDA 安装准备 RHEL 7/CentOS 7、RHEL 6/CentOS 6

步骤 1a：验证网络配置

Citrix 建议先连接并正确配置网络，然后再继续操作。

步骤 1b：设置主机名

注意：

Linux VDA 当前不支持 NetBIOS 名称截断。因此，主机名不得超过 15 个字符。

为确保正确报告计算机的主机名，请更改 `/etc/hostname` 文件，使其仅包含计算机的主机名。

`HOSTNAME=hostname`

步骤 1c：为主机名分配环回地址

注意：

Linux VDA 当前不支持 NetBIOS 名称截断。因此，主机名不得超过 15 个字符。

为确保正确报告计算机的 DNS 域名和完全限定域名 (FQDN)，请更改 **/etc/hosts** 文件中的以下行，使其前两个条目为 FQDN 和主机名：

```
127.0.0.1 hostname-fqdn hostname localhost localhost.localdomain localhost4 localhost4.localdomain4
```

例如：

```
127.0.0.1 vda01.example.com vda01 localhost localhost.localdomain localhost4 localhost4.localdomain4
```

从文件中的其他条目中删除对 **hostname-fqdn** 或 **hostname** 的任何其他引用。

提示：

只能使用字符 a-z、A-Z、0-9 和连字符 (-)。请避免使用下划线 (_)、空格和其他符号。主机名不得以数字开头和以连字符结尾。此规则也适用于 Delivery Controller 主机名。

步骤 1d：检查主机名

验证主机名设置是否正确无误：

```
1 hostname
2 <!--NeedCopy-->
```

此命令仅返回计算机的主机名，而不返回其完全限定域名 (FQDN)。

验证 FQDN 设置是否正确无误：

```
1 hostname -f
2 <!--NeedCopy-->
```

此命令返回计算机的 FQDN。

步骤 1e：检查名称解析和服务可访问性

确认可以解析 FQDN 并对域控制器和 Delivery Controller 执行 ping 操作：

```
1 nslookup domain-controller-fqdn
2
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
8 <!--NeedCopy-->
```

如果无法解析 FQDN 或 Ping 不通上述任一计算机，请先检查相关步骤，然后再继续。

步骤 1f: 配置时钟同步 (chrony)

确保 VDA、Delivery Controller 和域控制器之间的时钟始终精确同步至关重要。将 Linux VDA 托管为虚拟机可能会导致时钟偏差问题。出于此原因，最好使用远程时间服务来同步时间。

RHEL 6.x 及早期版本使用 NTP 守护程序 (ntpd) 同步时钟，而 RHEL 7.x 默认环境则转而使用较新的 Chrony 守护程序 (chronyd)。两个服务的配置和操作过程十分类似。

配置 **NTP** 服务（仅限 **RHEL 6/CentOS 6**） 以 root 用户身份，编辑 **/etc/ntp.conf** 并为每个远程时间服务器添加一个服务器条目：

```
1 server peer1-fqdn-or-ip-address iburst
2
3 server peer2-fqdn-or-ip-address iburst
4 <!--NeedCopy-->
```

在典型部署中，时间从本地域控制器同步，而不是直接从公共 NTP 池服务器同步。为域中的每个 Active Directory 域控制器添加一个服务器条目。

删除列出的任何其他 **server** 条目，包括环回 IP 地址、localhost 和公共服务器 ***.pool.ntp.org** 条目。

保存更改并重新启动 NTP 守护程序：

```
1 sudo /sbin/service ntpd restart
2 <!--NeedCopy-->
```

配置 **Chrony** 服务（仅限 **RHEL 7/CentOS 7**） 以 root 用户身份，编辑 **/etc/chrony.conf** 并为每个远程时间服务器添加一个服务器条目：

```
1 server peer1-fqdn-or-ip-address iburst
2
3 server peer2-fqdn-or-ip-address iburst
4 <!--NeedCopy-->
```

在典型部署中，时间从本地域控制器同步，而不是直接从公共 NTP 池服务器同步。为域中的每个 Active Directory 域控制器添加一个服务器条目。

删除列出的任何其他 server 条目，包括环回 IP 地址、localhost 和公共服务器 ***.pool.ntp.org** 条目。

保存更改并重新启动 Chrony 守护程序：

```
1 sudo /sbin/service chronyd restart
2 <!--NeedCopy-->
```

步骤 1g: 安装 OpenJDK

Linux VDA 依赖于 OpenJDK。通常，运行时环境作为操作系统安装的一部分进行安装。

确认版本是否正确：

- RHEL 7/CentOS 7:

```
1 sudo yum info java-1.8.0-openjdk
2 <!--NeedCopy-->
```

- RHEL 6/CentOS 6:

```
1 sudo yum info java-1.7.0-openjdk
2 <!--NeedCopy-->
```

预先封装的 OpenJDK 可能为早期版本。请根据需要更新为最新版本：

- RHEL 7/CentOS 7:

```
1 sudo yum -y update java-1.8.0-openjdk
2 <!--NeedCopy-->
```

- RHEL 6/CentOS 6:

```
1 sudo yum -y update java-1.7.0-openjdk
2 <!--NeedCopy-->
```

将以下行添加到 `~/.bashrc` 文件，从而设置 `JAVA_HOME` 环境变量：

```
export JAVA_HOME=/usr/lib/jvm/java
```

打开新的 shell，然后确认 Java 版本：

```
1 java -version
2 <!--NeedCopy-->
```

提示：

为避免出现问题，请务必在操作系统为 RHEL 6/CentOS 6 时仅安装 OpenJDK 1.7.0 或 1.8.0 版，或者在操作系统为 RHEL 7/CentOS 7 时仅安装 OpenJDK 1.8.0 版。删除系统中的所有其他版本的 Java。

步骤 1h：安装 PostgreSQL

Linux VDA 要求在 RHEL 6 上使用 PostgreSQL 8.4 或更高版本，或者在 RHEL 7 上使用 PostgreSQL 9.2 或更高版本。

安装以下软件包：

```
1 sudo yum -y install postgresql-server
2
3 sudo yum -y install postgresql-jdbc
4 <!--NeedCopy-->
```

此时需要执行一些安装后步骤，以便初始化数据库，并确保服务在计算机启动时启动。此操作会在 `/var/lib/pgsql/data` 下创建数据库文件。此命令在 PostgreSQL 8 和 PostgreSQL 9 上有所差别：

- 仅限 RHEL 7: PostgreSQL 9

```
1 sudo postgresql-setup initdb
2 <!--NeedCopy-->
```

- 仅限 RHEL 6: PostgreSQL 8

```
1 sudo /sbin/service postgresql initdb
2 <!--NeedCopy-->
```

步骤 1i: 启动 PostgreSQL

在计算机启动时启动服务和立即启动服务：

- 仅限 RHEL 7: PostgreSQL 9

```
1 sudo systemctl enable postgresql
2
3 sudo systemctl start postgresql
4 <!--NeedCopy-->
```

- 仅限 RHEL 6: PostgreSQL 8

```
1 sudo /sbin/chkconfig postgresql on
2
3 sudo /sbin/service postgresql start
4 <!--NeedCopy-->
```

使用以下命令检查 PostgreSQL 版本：

```
1 psql --version
2 <!--NeedCopy-->
```

使用 `psql` 命令行实用程序确认数据目录已设置：

```
1 sudo -u postgres psql -c 'show data_directory'
2 <!--NeedCopy-->
```

重要：

在此版本中，为 `gperftools-libs` 添加了一个新的依赖项，但它在原始存储库中并不存在。可以使用 `sudo rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm` 命令添加新存储库。

只有 RHEL 6/CentOS 6 会受到影响。应在安装 Linux VDA 软件包之前运行该命令。

步骤 2: 准备虚拟机管理程序

在支持的虚拟机管理程序上将 Linux VDA 当作虚拟机运行时，需要作出一些更改。根据使用的虚拟机管理程序平台作出以下更改。如果正在裸机硬件上运行 Linux 计算机，则无需作出任何更改。

修复 Citrix XenServer 上的时间同步问题

启用了 XenServer 时间同步功能时，在每个半虚拟化 Linux VM 中，您会发现 NTP 和 XenServer 都尝试管理系统时钟。为避免时钟与其他服务器不同步，请确保每个 Linux 客户机中的系统时钟都与 NTP 同步。这种情况要求禁用主机时间同步。无需在 HVM 模式下进行任何更改。

在某些 Linux 发行版中，如果正在运行半虚拟化 Linux 内核，并安装了 XenServer Tools，您可以检查 XenServer 时间同步功能是否存在，以及是否已在 Linux VM 中启用：

```
1 su -
2 cat /proc/sys/xen/independent_wallclock
3 <!--NeedCopy-->
```

此命令返回 0 或 1：

- 0 - 时间同步功能已启用，且必须禁用。
- 1 - 时间同步功能已禁用，无需采取任何操作。

如果 `/proc/sys/xen/indepent_wallclock` 文件不存在，则不需要执行以下步骤。

如果已启用，请通过向该文件写入 1 以禁用时间同步功能：

```
1 sudo echo 1 > /proc/sys/xen/independent_wallclock
2 <!--NeedCopy-->
```

要使其更改成为永久更改，并在重新启动后仍然有效，请编辑 `/etc/sysctl.conf` 文件并添加以下行：

```
xen.independent_wallclock = 1
```

要验证这些更改，请重新启动系统：

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--NeedCopy-->
```

此命令返回值 1。

在 Microsoft Hyper-V 上修复时间同步问题

安装了 Hyper-V Linux 集成服务的 Linux VM 可应用 Hyper-V 时间同步功能来使用主机操作系统的时间。为确保系统时钟始终精确可靠，必须一同启用此功能与 NTP 服务。

从管理操作系统中：

1. 打开 Hyper-V 管理器控制台。
2. 对于 Linux VM 的设置，请选择 **Integration Services**（集成服务）。
3. 确保已选择 **Time synchronization**（时间同步）。

注意：

此方法与 VMware 和 XenServer 不同，这两种产品会禁用主机时间同步功能，以免与 NTP 发生冲突。Hyper-V 时间同步可以与 NTP 时间同步共存并互补。

修复 ESX 和 ESXi 上的时间同步问题

启用了 VMware 时间同步功能时，在每个半虚拟化 Linux VM 中，您会发现 NTP 和虚拟机管理程序都尝试同步系统时钟。为避免时钟与其他服务器不同步，请确保每个 Linux 客户机中的系统时钟都与 NTP 同步。这种情况要求禁用主机时间同步。

如果正在运行安装了 VMware Tools 的半虚拟化 Linux 内核：

1. 打开 vSphere Client。
2. 编辑 Linux VM 设置。
3. 在 **Virtual Machine Properties**（虚拟机属性）对话框中，打开 **Options**（选项）选项卡。
4. 选择 **VMware Tools**。
5. 在 **Advanced**（高级）框中，取消选中 **Synchronize guest time with host**（与主机同步客户机时间）。

步骤 3：向 Windows 域中添加 Linux 虚拟机 (VM)

Linux VDA 支持多种向 Active Directory (AD) 域添加 Linux 计算机的方法：

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl
- SSSD

根据所选的方法，按说明执行操作。

注意：

为 Linux VDA 中的本地帐户和 AD 中的帐户使用相同的用户名时，会话启动可能会失败。

Samba Winbind

安装或更新所需软件包：

```
1 sudo yum -y install samba-winbind samba-winbind-clients krb5-  
   workstation authconfig oddjob-mkhomedir  
2 <!--NeedCopy-->
```

在计算机启动时启用要启动的 **Winbind** 守护程序 Winbind 守护程序必须配置为在计算机启动时启动：

```
1 sudo /sbin/chkconfig winbind on  
2 <!--NeedCopy-->
```

配置 **Winbind** 身份验证 通过使用 Winbind 将计算机配置为执行 Kerberos 身份验证：

```
1 sudo authconfig --disablecache --disablesssd --disablesssdauth --  
   enablewinbind --enablewinbindauth --disablewinbindoffline --  
   smbsecurity=ads --smbworkgroup=domain --smbrealm=REALM --krb5realm=  
   REALM --krb5kdc=fqdn-of-domain-controller --winbindtemplateshell=  
   bin/bash --enablemkhomedir --updateall  
2 <!--NeedCopy-->
```

其中，**REALM** 是大写的 Kerberos 领域名称，而 **domain** 是域的 NetBIOS 名称。

如果需要通过 DNS 查找 KDC 服务器和领域名称，请将以下两个选项添加至前面的命令：

```
--enablekrb5kdcdns --enablekrb5realmdns
```

请忽略 `authconfig` 命令返回的有关 `winbind` 服务无法启动的任何错误。`authconfig` 尝试在计算机尚未加入域的情况下启动 `winbind` 服务时，可能会出现这些错误。

打开 `/etc/samba/smb.conf` 并将以下条目添加到 [Global] 部分下方，但要放在 `authconfig` 工具生成的部分后面：

```
kerberos method = secrets and keytab  
winbind refresh tickets = true
```

Linux VDA 需要使用系统 keytab 文件 `/etc/krb5.keytab` 以执行身份验证并向 Delivery Controller 注册。计算机首次加入域后，前面的 `kerberos method` 设置将强制 Winbind 创建系统 keytab 文件。

加入 **Windows** 域 您的域控制器必须可访问，而且您必须具有有权将计算机添加到域的 Active Directory 用户帐户。

```
1 sudo net ads join REALM -U user  
2 <!--NeedCopy-->
```

REALM 是大写的 Kerberos 领域名称，**user** 是有权将计算机添加到域的域用户。

为 **Winbind** 配置 **PAM** 默认情况下, Winbind PAM 模块 (pam_winbind) 的配置不启用 Kerberos 票据缓存和主目录的创建。打开 `/etc/security/pam_winbind.conf`, 并在 [Global] 部分下添加或更改以下条目:

```
krb5_auth = yes
krb5_ccache_type = FILE
mkhomedir = yes
```

确保删除每个设置中的任何前置分号。这些更改要求重新启动 Winbind 守护程序:

```
1 sudo /sbin/service winbind restart
2 <!--NeedCopy-->
```

提示:

仅当计算机加入域后, winbind 守护程序才会始终保持运行状态。

打开 `/etc/krb5.conf` 并将 [libdefaults] 部分下方的以下设置从 KEYRING 更改为 FILE 类型:

```
default_ccache_name = FILE:/tmp/krb5cc_%{ uid }
```

验证域成员身份 Delivery Controller 要求所有 VDA 计算机 (Windows 和 Linux) 都要在 Active Directory 中有一个计算机对象。

运行 Samba 的 **net ads** 命令验证计算机是否已加入域:

```
1 sudo net ads testjoin
2 <!--NeedCopy-->
```

运行以下命令验证额外的域和计算机对象信息:

```
1 sudo net ads info
2 <!--NeedCopy-->
```

验证 **Kerberos** 配置 为了确保 Kerberos 已正确配置为可与 Linux VDA 配合使用, 请检查系统 `keytab` 文件是否已创建并包含有效密钥:

```
1 sudo klist -ke
2 <!--NeedCopy-->
```

此命令显示各种主体名称与密码套件组合可用的密钥列表。运行 Kerberos `kinit` 命令, 使用这些密钥向域控制器验证计算机的身份:

```
1 sudo kinit -k MACHINE$@REALM
2 <!--NeedCopy-->
```

计算机和领域名称必须指定为大写。美元符号 (\$) 必须使用反斜杠 (\) 进行转义, 以免发生 shell 替换。在某些环境中, DNS 域名与 Kerberos 领域名称不同。请确保使用领域名称。如果此命令成功运行, 则不会显示任何输出。

使用以下命令验证计算机帐户的 TGT 票据已缓存:

```
1 sudo klist
2 <!--NeedCopy-->
```

使用以下命令检查计算机的帐户详细信息：

```
1 sudo net ads status
2 <!--NeedCopy-->
```

验证用户身份验证 使用 **wbinfo** 工具验证是否可向域验证域用户的身份：

```
1 wbinfo --krb5auth=domain\username%password
2 <!--NeedCopy-->
```

这里指定的域为 AD 域名，而不是 Kerberos 领域名称。对于 bash shell，必须使用另一个反斜杠对反斜杠 (\) 字符进行转义。此命令返回一条成功或失败消息。

要验证 Winbind PAM 模块是否已正确配置，请使用域用户帐户登录 Linux VDA。该域用户帐户以前未曾使用过。

```
1 ssh localhost -l domain\username
2
3 id -u
4 <!--NeedCopy-->
```

检查 Kerberos 凭据缓存中的票据是否有效且未过期：

```
1 klist
2 <!--NeedCopy-->
```

退出会话：

```
1 exit
2 <!--NeedCopy-->
```

直接登录 GNOME 或 KDE 控制台也可以执行类似的测试。在进行域加入验证后继续执行 [步骤 4: 安装 Linux VDA](#)。

Quest Authentication Service

在域控制器上配置 **Quest** 假定您已在 Active Directory 域控制器上安装并配置了 Quest 软件，而且已获得管理权限，有权在 Active Directory 中创建计算机对象。

允许域用户登录 **Linux VDA** 计算机 为了让域用户能够在 Linux VDA 计算机上建立 HDX 会话：

1. 在 Active Directory 用户和计算机管理控制台中，为该用户帐户打开 Active Directory 用户属性。
2. 选择 **Unix Account** (Unix 帐户) 选项卡。
3. 选中 **Unix-enabled** (已启用 Unix)。
4. 将 **Primary GID Number** (首选 GID 编号) 设置为实际域用户组的组 ID。

注意：

这些说明相当于设置域用户，以便他们可以使用控制台、RDP、SSH 或任何其他远程协议进行登录。

在 **Linux VDA** 上配置 **Quest**

SELinux 策略强制实施解决方法 默认 RHEL 环境会强制实施 SELinux。此强制功能会影响 Quest 使用的 Unix 域套接字 IPC 机制，并阻止域用户登录。

解决此问题的最便捷的方法是禁用 SELinux。以 root 用户身份，编辑 `/etc/selinux/config` 并更改 **SELinux** 设置：

`SELINUX=permissive`

此更改要求重新启动计算机：

```
1 reboot
2 <!--NeedCopy-->
```

重要：

请谨慎使用此设置。禁用后重新启用 SELinux 策略强制实施会导致完全锁定，即便是对 root 用户和其他本地用户也是如此。

配置 VAS 守护程序 必须启用并断开自动续订 Kerberos 票据功能。必须禁用身份验证（脱机登录）功能。

```
1 sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
   interval 32400
2
3 sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
   auth false
4 <!--NeedCopy-->
```

此命令将续订间隔设为 9 小时（32400 秒），即比默认的 10 小时票据生命周期短 1 小时。请在票据生命周期较短的系统上设置较低的值。

配置 PAM 和 NSS 要启用通过 HDX 进行的域用户登录以及其他服务（例如 su、ssh 和 RDP），请运行以下命令以手动配置 PAM 和 NSS：

```
1 sudo /opt/quest/bin/vastool configure pam
2
3 sudo /opt/quest/bin/vastool configure nss
4 <!--NeedCopy-->
```

加入 **Windows** 域 使用 Quest `vastool` 命令将 Linux 计算机加入到 Active Directory 域中:

```
1 sudo /opt/quest/bin/vastool -u user join domain-name
2 <!--NeedCopy-->
```

`user` 为有权将计算机加入 Active Directory 域的任何域用户。**domain-name** 为域的 DNS 名称, 例如 `example.com`。

验证域成员身份 Delivery Controller 要求所有 VDA 计算机 (Windows 和 Linux) 都要在 Active Directory 中有一个计算机对象。验证 Quest 加入的 Linux 计算机是否位于域中:

```
1 sudo /opt/quest/bin/vastool info domain
2 <!--NeedCopy-->
```

如果计算机已加入域, 此命令会返回域名。如果计算机未加入任何域, 则会显示以下错误:

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined
to domain
```

验证用户身份验证 要验证 Quest 是否可以通过 PAM 对域用户进行身份验证, 请使用域用户帐户登录 Linux VDA。该域用户帐户以前未曾使用过。

```
1 ssh localhost -l domain\username
2
3 id -u
4 <!--NeedCopy-->
```

检查是否为 `id -u` 命令返回的 UID 创建了对应的 Kerberos 凭据缓存文件:

```
1 ls /tmp/krb5cc_uid
2 <!--NeedCopy-->
```

检查 Kerberos 凭据缓存中的票据是否有效且未过期:

```
1 /opt/quest/bin/vastool klist
2 <!--NeedCopy-->
```

退出会话:

```
1 exit
2 <!--NeedCopy-->
```

直接登录 Gnome 或 KDE 控制台也可以执行类似的测试。在进行域加入验证后继续执行 [步骤 4: 安装 Linux VDA](#)。

Centrify DirectControl

加入 **Windows** 域 安装 Centrify DirectControl Agent 后，请使用 Centrify `adjoin` 命令将 Linux 计算机加入 Active Directory 域：

```
1 su -
2 adjoin -w -V -u user domain-name
3 <!--NeedCopy-->
```

`user` 参数为有权将计算机加入 Active Directory 域的任何 Active Directory 域用户。**domain-name** 是将 Linux 计算机加入到的域的名称。

验证域成员身份 Delivery Controller 要求所有 VDA 计算机（Windows 和 Linux）都要在 Active Directory 中有一个计算机对象。验证 Centrify 加入的 Linux 计算机是否位于域中：

```
1 su -
2
3 adinfo
4 <!--NeedCopy-->
```

检查 `Joined to domain` 值是否有效以及 `CentrifyDC mode` 是否返回了 `connected`。如果模式仍然卡在启动状态，则表明 Centrify 客户端遇到了服务器连接或身份验证问题。

使用以下命令可获得更全面的系统和诊断信息：

```
1 adinfo --sysinfo all
2
3 adinfo -diag
4 <!--NeedCopy-->
```

测试与各种 Active Directory 和 Kerberos 服务的连接。在进行域加入验证后继续执行 [步骤 4: 安装 Linux VDA](#)。

```
1 adinfo --test
2 <!--NeedCopy-->
```

SSSD

如果您使用的是 SSSD，请按照此部分中的说明进行操作。此部分包含有关如何将 Linux VDA 计算机加入 Windows 域的说明以及如何配置 Kerberos 身份验证的指导。

要在 RHEL 和 CentOS 上设置 SSSD，请执行以下操作：

1. 使用 Samba 加入域并创建主机 keytab
2. 设置 SSSD
3. 配置 NSS/PAM
4. 验证 Kerberos 配置
5. 验证用户身份验证

必备软件 Active Directory 提供程序最初是在 SSSD 版本 1.9.0 中引入的。如果您使用的是早期版本，请按照[为 LDAP 提供程序配置 Active Directory](#) 中提供的说明进行操作。

已按照本文中的说明测试和验证了以下环境。

- RHEL 7.3 或更高版本/CentOS 7.3 或更高版本
- Linux VDA 1.3 版或更高版本

使用 **Samba** 加入域并创建主机 **keytab** SSSD 并不提供用于加入域和管理系统 keytab 文件的 Active Directory 客户端功能。可以改为使用 **adcli**、**realmd**、**Winbind** 或 **Samba**。

本节信息只介绍 **Samba** 方法。对于 **realmd**，请参阅 RHEL 或 CentOS 文档。必须在配置 SSSD 之前执行这些步骤。

在正确配置了以下文件的 Linux 客户端上：

- /etc/krb5.conf
- /etc/samba/smb.conf:

为计算机配置 Samba 和 Kerberos 身份验证：

```
1 sudo authconfig --smbsecurity=ads --smbworkgroup=domain --smbrealm=
   REALM --krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --update
2 <!--NeedCopy-->
```

其中，**REALM** 是大写的 Kerberos 领域名称，**domain** 是 Active Directory 域的简短 NetBIOS 名称。

如果需要通过 DNS 查找 KDC 服务器和领域名称，请将以下两个选项添加至前面的命令：

```
--enablekrb5kdcdns --enablekrb5realmdns
```

打开 **/etc/samba/smb.conf** 并将以下条目添加到 **[Global]** 部分下方，但要放在 **authconfig** 工具生成的部分后面：

```
kerberos method = secrets and keytab
```

加入 Windows 域。请确保域控制器可访问，而且您具有有权将计算机添加到域的 Active Directory 用户帐户。

```
1 sudo net ads join REALM -U user
2 <!--NeedCopy-->
```

REALM 是大写的 Kerberos 领域名称，**user** 是有权将计算机添加到域的域用户。

设置 **SSSD** 设置 SSSD 的步骤如下：

- 在 Linux VDA 上安装 **sssd-ad** 软件包。
- 对各种文件（例如 sssd.conf）进行配置更改。
- 启动 **sssd** 服务。

sssd.conf 配置示例 (可以根据需要添加额外的选项):

```
1 [sssd]
2 config_file_version = 2
3 domains = ad.example.com
4 services = nss, pam
5
6 [domain/ad.example.com]
7 # Uncomment if you need offline logins
8 # cache_credentials = true
9
10 id_provider = ad
11 auth_provider = ad
12 access_provider = ad
13 ldap_id_mapping = true
14 ldap_schema = ad
15
16 # Should be specified as the lower-case version of the long version of
17   the Active Directory domain.
18 ad_domain = ad.example.com
19
20 # Kerberos settings
21 krb5_ccachedir = /tmp
22 krb5_ccname_template = FILE:%d/krb5cc_%U
23
24 # Uncomment if service discovery is not working
25 # ad_server = server.ad.example.com
26
27 # Comment out if the users have the shell and home dir set on the AD
28   side
29 default_shell = /bin/bash
30 fallback_homedir = /home/%d/%u
31
32 # Uncomment and adjust if the default principal SHORTNAME$@REALM is not
33   available
34 # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
35 <!--NeedCopy-->
```

将 **ad.example.com**、**server.ad.example.com** 替换为相应的值。有关详细信息, 请参阅 [sssd-ad\(5\) - Linux 手册页](#)。

对 sssd.conf 设置文件所有权和权限:

```
chown root:root /etc/sssds/sssds.conf
chmod 0600 /etc/sssds/sssds.conf
restorecon /etc/sssds/sssds.conf
```

配置 NSS/PAM RHEL/CentOS:

使用 `authconfig` 启用 SSSD。安装 **oddjob mkhomedir** 以确保主目录创建与 SELinux 兼容:

```
1 authconfig --enablesssd --enablesssdauth --enablemkhomedir - -update
```

```
2
3 sudo service sssd start
4
5 sudo chkconfig sssd on
6 <!--NeedCopy-->
```

验证 **Kerberos** 配置 检查系统 **keytab** 文件是否已创建并包含有效密钥：

```
1 sudo klist -ke
2 <!--NeedCopy-->
```

此命令显示各种主体名称与密码套件组合可用的密钥列表。运行 Kerberos **kinit** 命令，以使用这些密钥向域控制器验证计算机的身份：

```
1 sudo kinit -k MACHINE$@REALM
2 <!--NeedCopy-->
```

计算机和领域名称必须指定为大写。美元符号 (\$) 必须使用反斜杠 (****) 进行转义，以免发生 shell 替换。在某些环境中，DNS 域名与 Kerberos 领域名称不同。请确保使用领域名称。如果此命令成功运行，则不会显示任何输出。

使用以下命令验证计算机帐户的 TGT 票据已缓存：

```
1 sudo klist
2 <!--NeedCopy-->
```

验证用户身份验证 使用 **getent** 命令确认支持的登录格式以及 NSS 是否工作：

```
1 sudo getent passwd DOMAIN\username
2 <!--NeedCopy-->
```

DOMAIN 参数指示简短形式的域名。如果需要使用另一种登录格式，请先使用 **getent** 命令进行验证。

支持的登录格式如下：

- 低级别登录名称: **DOMAIN\username**
- UPN: **username@domain.com**
- NetBIOS 前缀格式: **username@DOMAIN**

要验证 SSSD PAM 模块是否已正确配置，请使用域用户帐户登录 Linux VDA。该域用户帐户以前未曾使用过。

```
1 sudo ssh localhost -l DOMAIN\username
2
3 id -u
4 <!--NeedCopy-->
```

检查是否为以下命令返回的 **uid** 创建了对应的 Kerberos 凭据缓存文件：

```
1 ls /tmp/krb5cc_{
2 uid }
```

```
3
4 <!--NeedCopy-->
```

检查用户 Kerberos 凭据缓存中的票据是否有效且未过期。在进行域加入验证后继续执行[步骤 4: 安装 Linux VDA](#)。

```
1 klist
2 <!--NeedCopy-->
```

步骤 4: 安装 Linux VDA

步骤 4a: 卸载旧版本

如果之前安装了更低版本的 Linux VDA，请先卸载该版本，然后再安装新版本。

1. 停止 Linux VDA 服务:

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx stop
4 <!--NeedCopy-->
```

2. 卸载软件包:

```
1 sudo rpm -e XenDesktopVDA
2 <!--NeedCopy-->
```

注意:

支持从先前的两个版本进行升级。

注意:

自版本 1.3 起，安装路径已更改。在早期版本中，安装组件位于 **/usr/local/**。在新版本中，安装组件位于 **/opt/Citrix/VDA/**。

要运行命令，需要提供完整路径；或者，也可以将 **/opt/Citrix/VDA/sbin** 和 **/opt/Citrix/VDA/bin** 添加到系统路径。

步骤 4b: 下载 Linux VDA 软件包

转至 Citrix Web 站点并根据您的 Linux 发行版下载相应的 Linux VDA 软件包。

步骤 4c: 安装 Linux VDA

使用 Yum 安装 Linux VDA 软件:

对于 **RHEL 7/CentOS 7**:

```
1 sudo yum install -y XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
2 <!--NeedCopy-->
```

对于 **RHEL 6.9**:

```
1 sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
2 <!--NeedCopy-->
```

对于 **RHEL 6.6/CentOS 6.6**:

```
1 sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
2 <!--NeedCopy-->
```

使用 RPM 软件包管理器安装 Linux VDA 软件。在此之前，您必须解决以下依赖项：

对于 **RHEL 7/CentOS 7**:

```
1 sudo rpm -i XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
2 <!--NeedCopy-->
```

对于 **RHEL 6.9**:

```
1 sudo rpm -i XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
2 <!--NeedCopy-->
```

对于 **RHEL 6.6/CentOS 6.6**:

```
1 sudo rpm -i XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
2 <!--NeedCopy-->
```

RHEL 7 的 **RPM** 依赖项列表：

```
1 postgresql-server >= 9.2
2
3 postgresql-jdbc >= 9.2
4
5 java-1.8.0-openjdk >= 1.8.0
6
7 ImageMagick >= 6.7.8.9
8
9 firewalld >= 0.3.9
10
11 policycoreutils-python >= 2.0.83
12
13 dbus >= 1.6.12
14
15 dbus-x11 >= 1.6.12
16
17 xorg-x11-server-utils >= 7.7
18
19 xorg-x11-xinit >= 1.3.2
20
```

```
21 libXpm >= 3.5.10
22
23 libXrandr >= 1.4.1
24
25 libXtst >= 1.2.2
26
27 motif >= 2.3.4
28
29 pam >= 1.1.8
30
31 util-linux >= 2.23.2
32
33 bash >= 4.2
34
35 findutils >= 4.5
36
37 gawk >= 4.0
38
39 sed >= 4.2
40
41 cups >= 1.6.0
42
43 foomatic-filters >= 4.0.9
44
45 openldap >= 2.4
46
47 cyrus-sasl >= 2.1
48
49 cyrus-sasl-gssapi >= 2.1
50
51 libxml2 >= 2.9
52
53 python-requests >= 2.6.0
54
55 gperftools-libs >= 2.4
56
57 xorg-x11-server-Xorg >= 1.17
58
59 xorg-x11-server-Xorg < 1.18
60
61 rpmlib(FileDigests) <= 4.6.0-1
62
63 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
64
65 rpmlib(CompressedFileNames) <= 3.0.4-1
66
67 rpmlib(PayloadIsXz) <= 5.2-1
68 <!--NeedCopy-->
```

RHEL 6.9 的 RPM 依赖项列表:

```
1 postgresql-jdbc >= 8.4
2
```

```
3 postgresql-server >= 8.4
4
5 java-1.7.0-openjdk >= 1.7.0
6
7 ImageMagick >= 6.5.4.7
8
9 GConf2 >= 2.28.0
10
11 system-config-firewall-base >= 1.2.27
12
13 policycoreutils-python >= 2.0.83
14
15 xorg-x11-server-utils >= 7.7
16
17 xorg-x11-xinit >= 1.0.9
18
19 ConsoleKit >= 0.4.1
20
21 dbus >= 1.2.24
22
23 dbus-x11 >= 1.2.24
24
25 libXpm >= 3.5.10
26
27 libXrandr >= 1.4.1
28
29 libXtst >= 1.2.2
30
31 openmotif >= 2.3.3
32
33 pam >= 1.1.1
34
35 util-linux-ng >= 2.17.2
36
37 bash >= 4.1
38
39 findutils >= 4.4
40
41 gawk >= 3.1
42
43 sed >= 4.2
44
45 cups >= 1.4.0
46
47 foomatic >= 4.0.0
48
49 openldap >= 2.4
50
51 cyrus-sasl >= 2.1
52
53 cyrus-sasl-gssapi >= 2.1
54
55 libxml2 >= 2.7
```

```
56
57 python-requests >= 2.6.0
58
59 gperftools-libs >= 2.0
60
61 xorg-x11-server-Xorg >= 1.17
62
63 xorg-x11-server-Xorg < 1.18
64
65 rpmlib(FileDigests) <= 4.6.0-1
66
67 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
68
69 rpmlib(CompressedFileNames) <= 3.0.4-1
70
71 rpmlib(PayloadIsXz) <= 5.2-1
72 <!--NeedCopy-->
```

RHEL 6.6/CentOS 6.6 的 RPM 依赖项列表:

```
1 postgresql-jdbc >= 8.4
2
3 postgresql-server >= 8.4
4
5 java-1.7.0-openjdk >= 1.7.0
6
7 ImageMagick >= 6.5.4.7
8
9 GConf2 >= 2.28.0
10
11 system-config-firewall-base >= 1.2.27
12
13 policycoreutils-python >= 2.0.83
14
15 xorg-x11-server-utils >= 7.7
16
17 xorg-x11-xinit >= 1.0.9
18
19 ConsoleKit >= 0.4.1
20
21 dbus >= 1.2.24
22
23 dbus-x11 >= 1.2.24
24
25 libXpm >= 3.5.10
26
27 libXrandr >= 1.4.1
28
29 libXtst >= 1.2.2
30
31 openmotif >= 2.3.3
32
33 pam >= 1.1.1
```

```
34
35 util-linux-ng >= 2.17.2
36
37 bash >= 4.1
38
39 findutils >= 4.4
40
41 gawk >= 3.1
42
43 sed >= 4.2
44
45 cups >= 1.4.0
46
47 foomatic >= 4.0.0
48
49 openldap >= 2.4
50
51 cyrus-sasl >= 2.1
52
53 cyrus-sasl-gssapi >= 2.1
54
55 libxml2 >= 2.7
56
57 python-requests >= 2.6.0
58
59 gperftools-libs >= 2.0
60
61 xorg-x11-server-Xorg >= 1.15
62
63 xorg-x11-server-Xorg < 1.16
64
65 rpmlib(FileDigests) <= 4.6.0-1
66
67 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
68
69 rpmlib(CompressedFileNames) <= 3.0.4-1
70
71 rpmlib(PayloadIsXz) <= 5.2-1
72 <!--NeedCopy-->
```

步骤 4d: 升级 Linux VDA (可选)

可以使用 Yum 将 Linux VDA 软件从 7.14 版和 7.13 版进行升级:

对于 RHEL 7/CentOS 7:

```
1 sudo yum install -y XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
2 <!--NeedCopy-->
```

对于 RHEL 6.9:

```
1 sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
```

```
2 <!--NeedCopy-->
```

对于 **RHEL 6.6/CentOS 6.6**:

```
1 sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
2 <!--NeedCopy-->
```

使用 RPM 软件包管理器升级 Linux VDA 软件:

对于 **RHEL 7/CentOS 7**:

```
1 sudo rpm -U XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
2 <!--NeedCopy-->
```

对于 **RHEL 6.9**:

```
1 sudo rpm -U XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
2 <!--NeedCopy-->
```

对于 **RHEL 6.6/CentOS 6.6**:

```
1 sudo rpm -U XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
2 <!--NeedCopy-->
```

重要:

升级软件后重新启动 Linux VDA 计算机。

步骤 5: 安装 **NVIDIA GRID** 驱动程序

启用 HDX 3D Pro 需要执行额外的安装步骤, 以在虚拟机管理程序和 VDA 计算机上安装必备的图形驱动程序。

配置以下设置:

1. Citrix XenServer
2. VMware ESX

根据所选的虚拟机管理程序, 按以下说明执行操作。

Citrix XenServer:

本部分内容详细介绍了如何在 [Citrix XenServer](#) 中逐步安装和配置 NVIDIA GRID 驱动程序。

VMware ESX:

请按照本指南中包含的信息进行操作, 为 [VMware ESX](#) 安装和配置 NVIDIA GRID 驱动程序。

VDA 计算机:

按照这些步骤为每个 Linux VM 客户机安装和配置驱动程序:

1. 开始前, 请确保 Linux VM 已关闭。

2. 在 XenCenter 中，将处于 GPU 直通模式的 GPU 添加至 VM。
3. 启动 RHEL VM。

要准备计算机以使用 NVIDIA GRID 驱动程序，请运行以下命令：

```
1 yum install gcc
2
3 yum install "kernel-devel-$(uname -r)"
4
5 systemctl set-default multi-user.target
6 <!--NeedCopy-->
```

请按照 [Red Hat Enterprise Linux 文档](#) 中的步骤安装 NVIDIA GRID 驱动程序。

注意：

安装 GPU 驱动程序期间，为每个问题选择默认答案 (no)。

重要：

在启用 GPU 直通后，无法再通过 XenCenter 访问 Linux VM。使用 SSH 进行连接。

`nvidia-smi`

```
+-----+
| NVIDIA-SMI 352.70      Driver Version: 352.70      |
+-----+-----+
| GPU  Name           Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp   Perf    Pwr:Usage/Cap|      Memory-Usage | GPU-Util  Compute M. |
+-----+-----+-----+-----+-----+-----+
|   0   Tesla M60                Off | 0000:00:05.0   Off |                    Off |
| N/A   20C    P0              37W / 150W |  19MiB /  8191MiB |         0%      Default |
+-----+-----+-----+-----+-----+-----+

+-----+-----+
| Processes:                                     GPU Memory |
|  GPU       PID  Type  Process name                               Usage      |
+-----+-----+-----+-----+-----+
| No running processes found
+-----+-----+
```

为图形卡设置正确的配置：

`etc/X11/ctx-nvidia.sh`

要利用高分辨率和多监视器功能，您需要有效的 NVIDIA 许可证。要申请许可证，请按照“GRID Licensing Guide.pdf - DU-07757-001 September 2015”产品文档执行操作。

步骤 6：配置 Linux VDA

安装软件包后，必须运行 `ctxsetup.sh` 脚本来配置 Linux VDA。执行任何更改之前，该脚本都会验证环境，确保所有依赖项都已安装。如有必要，可以随时重新运行该脚本以更改设置。

可以按照提示手动运行脚本，也可以采用预先配置的响应自动运行脚本。继续操作前，请查看该脚本的帮助信息：

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
2 <!--NeedCopy-->
```

提示配置

运行会提示各种问题的手动配置：

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
2 <!--NeedCopy-->
```

自动配置

自动安装时，通过环境变量提供设置脚本所需的选项。如果所需的所有变量都存在，脚本不会提示您提供任何信息。

支持的环境变量包括：

- **CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N** -Linux VDA 支持使用 DNS CNAME 记录指定 Delivery Controller 名称。默认情况下设置为 N。
- **CTX_XDL_DDC_LIST = list-ddc-fqdns** -Linux VDA 要求提供由空格分隔的 Delivery Controller 完全限定域名 (FQDN) 列表以用于向 Delivery Controller 注册。必须至少指定一个 FQDN 或 CNAME 别名。
- **CTX_XDL_VDA_PORT = port-number** -Linux VDA 通过 TCP/IP 端口（默认为端口 80）与 Delivery Controller 通信。
- **CTX_XDL_REGISTER_SERVICE = Y | N** -在启动计算机后启动 Linux Virtual Desktop 服务。默认情况下，该值设置为 Y。
- **CTX_XDL_ADD_FIREWALL_RULES = Y | N** -Linux Virtual Desktop 服务要求允许传入网络连接通过系统防火墙。您可以在系统防火墙中自动为 Linux Virtual Desktop 打开所需端口（默认为端口 80 和 1494）。默认情况下设置为 Y。
- **CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 | 4** - Linux VDA 要求使用 Kerberos 配置设置向 Delivery Controller 进行身份验证。Kerberos 配置根据系统上已安装和已配置的 Active Directory 集成工具确定。指定要使用且受支持的 Active Directory 集成方法：
 - 1 -Samba Winbind
 - 2 -Quest Authentication Service
 - 3 - Centrify DirectControl
 - 4 - SSSD
- **CTX_XDL_HDX_3D_PRO = Y | N** -Linux VDA 支持 HDX 3D Pro，这是一组 GPU 加速技术，旨在优化富图形应用程序的虚拟化水平。如果选择了 HDX 3D Pro，则要为 VDI 桌面（单会话）模式配置 Virtual Delivery Agent -（即 CTX_XDL_VDI_MODE=Y）。
- **CTX_XDL_VDI_MODE = Y | N** -将计算机配置为专用桌面交付模型 (VDI) 还是托管共享桌面交付模型。对于 HDX 3D Pro 环境，将此变量设置为 Y。默认情况下，此变量设置为 N。

- **CTX_XDL_SITE_NAME = dns-name** -Linux VDA 通过 DNS 发现 LDAP 服务器。要将 DNS 搜索结果限制为本地站点，应指定 DNS 站点名称。默认情况下，此变量设置为 **<none>**。
- **CTX_XDL_LDAP_LIST = list-ldap-servers** -Linux VDA 查询 DNS 来发现 LDAP 服务器。如果 DNS 无法提供 LDAP 服务记录，您可以提供以空格分隔的 LDAP FQDN（带有 LDAP 端口）列表。例如 ad1.mycompany.com:389。默认情况下，此变量设置为 **<none>**。
- **CTX_XDL_SEARCH_BASE = search-base-set** -Linux VDA 通过设置为 Active Directory 域根的搜索库来查询 LDAP（例如，DC=mycompany,DC=com）。为提高搜索性能，可以指定搜索基础（例如 OU=VDI,DC=mycompany,DC=com）。默认情况下，此变量设置为 **<none>**。
- **CTX_XDL_START_SERVICE = Y | N** -在完成 Linux VDA 配置后，是否启动 Linux VDA 服务。默认情况下设置为 Y。

设置环境变量并运行配置脚本：

```

1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
2
3 export CTX_XDL_DDC_LIST=list-ddc-fqdns
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-name
18
19 export CTX_XDL_LDAP_LIST=list-ldap-servers
20
21 export CTX_XDL_SEARCH_BASE=search-base-set
22
23 export CTX_XDL_START_SERVICE=Y|N
24
25 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
26 <!--NeedCopy-->

```

运行 `sudo` 命令时，键入 **-E** 选项以将现有环境变量传递给它创建的新 shell。Citrix 建议使用前面的命令并加上 **#!/bin/bash** 作为第一行来创建 shell 脚本文件。

或者，您可以使用单个命令指定所有参数：

```

1 sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3 CTX_XDL_DDC_LIST=list-ddc-fqdns \
4
5 CTX_XDL_VDA_PORT=port-number \

```

```
6
7 CTX_XDL_REGISTER_SERVICE=Y|N \
8
9 CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST=list-ldap-servers \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_START_SERVICE=Y|N \
24
25 /opt/Citrix/VDA/sbin/ctxsetup.sh
26 <!--NeedCopy-->
```

删除配置更改

在某些情形下，您可能需要删除 **ctxsetup.sh** 脚本对配置所做的更改，但不卸载 Linux VDA 软件包。

继续操作前，请查看此脚本的帮助信息：

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
2 <!--NeedCopy-->
```

删除配置更改：

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
2 <!--NeedCopy-->
```

重要：

此脚本会从数据库删除所有配置数据，从而使 Linux VDA 无法使用。

配置日志

ctxsetup.sh 和 **ctxcleanup.sh** 脚本会在控制台上显示错误，并将其他信息写入配置日志文件 **/tmp/xdl.configure.log**：

重新启动 Linux VDA 服务，确保更改生效。

步骤 7: 运行 **Linux VDA**

使用 **ctxsetup.sh** 脚本配置 Linux VDA 后, 可以运行以下命令来控制 Linux VDA。

启动 **Linux VDA**:

启动 Linux VDA 服务:

```
1 sudo /sbin/service ctxhdx start
2
3 sudo /sbin/service ctxvda start
4 <!--NeedCopy-->
```

停止 **Linux VDA**:

停止 Linux VDA 服务:

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx stop
4 <!--NeedCopy-->
```

重新启动 **Linux VDA**:

重新启动 Linux VDA 服务:

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx restart
4
5 sudo /sbin/service ctxvda start
6 <!--NeedCopy-->
```

检查 **Linux VDA** 的状态:

要检查 Linux VDA 服务的运行状态, 请执行以下操作:

```
1 sudo /sbin/service ctxvda status
2
3 sudo /sbin/service ctxhdx status
4 <!--NeedCopy-->
```

步骤 8: 在 **XenApp** 或 **XenDesktop** 中创建计算机目录

创建计算机目录和添加 Linux VDA 计算机的过程与传统的 Windows VDA 方法类似。有关如何完成这些任务的更加详细的说明, 请参阅[创建计算机目录](#)和[管理计算机目录](#)。

创建包含 Linux VDA 计算机的计算机目录时会面临一些限制, 使得该过程不同于为 Windows VDA 计算机创建计算机目录:

- 对于操作系统, 请选择:

- “服务器操作系统”选项（对于托管共享桌面交付模型）。
- “桌面操作系统”选项（对于 VDI 专用桌面交付模型）。
- 确保计算机未执行电源管理设置。
- 由于 Linux VDA 不支持 MCS，请选择 [PVS](#) 或其他服务或技术（现有映像）部署方法。
- 请勿在同一个计算机目录中混合使用 Linux 和 Windows VDA 计算机。

注意：

早期版本的 Citrix Studio 不支持“Linux 操作系统”的概念。但是，选择 Windows Server 操作系统或服务器操作系统选项等同于使用托管共享桌面交付模型。选择 Windows 桌面操作系统或桌面操作系统选项等同于使用每计算机一个用户交付模型。

提示：

如果删除计算机后将其重新加入 Active Directory 域，则必须删除计算机，然后将其重新添加到计算机目录。

步骤 9：在 **XenApp** 或 **XenDesktop** 中创建交付组

创建交付组和添加包含 Linux VDA 计算机的计算机目录的过程与 Windows VDA 计算机几乎相同。有关如何完成这些任务的更加详细的说明，请参阅 [创建交付组](#)。

创建含有 Linux VDA 计算机目录的交付组时会面临以下限制：

- 对于交付类型，请选择“桌面”或“应用程序”。
- 确保所选的 AD 用户和组已正确配置，可以登录到 Linux VDA 计算机。
- 请勿允许未经身份验证的（匿名）用户登录。
- 请勿在交付组中混入含有 Windows 计算机的计算机目录。

重要：

Linux VDA 1.4 及更高版本支持发布应用程序。但是，Linux VDA 不支持将桌面和应用程序交付给相同的计算机。

安装 **Linux Virtual Delivery Agent for SUSE**

February 9, 2024

可以选择按照本文中的步骤进行手动安装，也可以使用 [轻松安装](#) 进行自动安装和配置。轻松安装省时又省力，与手动安装相比，更不易于出错。

注意：

请仅对全新安装使用轻松安装功能。请勿使用轻松安装更新现有安装。

步骤 1: 准备安装

步骤 1a: 启动 YaST 工具

SUSE Linux Enterprise YaST 工具用于对操作系统执行方方面面的配置。

启动基于文本的 YaST 工具:

```
1 su -
2
3 yast
4 <!--NeedCopy-->
```

或者, 启动基于 UI 的 YaST 工具:

```
1 su -
2
3 yast2 &
4 <!--NeedCopy-->
```

步骤 1b: 配置网络连接

以下各部分介绍了如何配置 Linux VDA 使用的各种网络设置和服务。网络配置通过 YaST 工具执行, 而不得使用其他方法, 例如 Network Manager。以下说明介绍的是使用基于 UI 的 YaST 工具的情形。也可以使用基于文本的 YaST 工具, 但导航方法稍有不同, 对此本文未作介绍。

配置主机名和 DNS

1. 打开 YaST 网络设置。
2. 仅限 SLED 12: 在 **Global Options** (全局选项) 选项卡上, 将 **Network Setup Method** (网络设置方法) 更改为 **Wicked Service** (Wicked 服务)。
3. 打开 **Hostname/DNS** (主机名/DNS) 选项卡。
4. 取消选中 **Change hostname via DHCP** (通过 DHCP 更改主机名)。
5. 选中 **Assign Hostname to Loopback IP** (向环回 IP 分配主机名)。
6. 编辑以下内容, 以反映所作的网络设置:
 - 主机名 - 添加计算机的 DNS 主机名。
 - 域名 - 添加计算机的 DNS 域名。
 - 名称服务器 - 添加 DNS 服务器的 IP 地址。通常是 AD 域控制器的 IP 地址。
 - 域搜索列表 - 添加 DNS 域名。

注意:

Linux VDA 当前不支持 NetBIOS 名称截断。因此, 主机名不得超过 15 个字符。

提示:

只能使用字符 a-z、A-Z、0-9 和连字符 (-)。请避免使用下划线 (_)、空格和其他符号。主机名不得以数字开头和以连字符结尾。此规则也适用于 Delivery Controller 主机名。

禁用多播 DNS 只有在 SLED 上，默认设置才会启用多播 DNS (mDNS)，而这可能会导致名称解析结果不一致。默认情况下，SLES 上未启用 mDNS，因此无需任何操作。

要禁用 mDNS，请编辑 `/etc/nsswitch.conf` 并更改包含以下内容的行：

```
hosts: files mdns_minimal [NOTFOUND=return] dns
```

更改为：

```
hosts: files dns
```

检查主机名 验证主机名设置是否正确无误：

```
1 hostname
2 <!--NeedCopy-->
```

此命令仅返回计算机的主机名，而不返回其完全限定域名 (FQDN)。

验证 FQDN 设置是否正确无误：

```
1 hostname -f
2 <!--NeedCopy-->
```

此命令返回计算机的 FQDN。

检查名称解析和服务可访问性 确认可以解析 FQDN 并对域控制器和 Delivery Controller 执行 ping 操作：

```
1 nslookup domain-controller-fqdn
2
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
8 <!--NeedCopy-->
```

如果无法解析 FQDN 或 Ping 不通上述任一计算机，请先检查相关步骤，然后再继续。

步骤 1c: 配置 NTP 服务

维护 VDA、Delivery Controller 和域控制器之间的时钟始终精确同步至关重要。将 Linux VDA 托管为虚拟机可能会导致时钟偏差问题。出于此原因，最好使用远程 NTP 服务来保持时间同步。默认 NTP 设置可能需要作一些更改：

1. 打开 YaST 的“NTP Configuration”（NTP 配置），然后选择 **General Settings**（常规设置）选项卡。

2. 在“Start NTP Daemon”（启动 NTP 守护程序）部分，选中 **Now and on Boot**（现在及引导时）。
3. 如果存在 **Undisciplined Local Clock (LOCAL)**（无序本地时钟 (LOCAL)）项，选择该项，然后单击 **Delete**（删除）。
4. 单击 **Add**（添加），添加一个 NTP 服务器条目。
5. 选择 **Server Type**（服务器类型），然后单击 **Next**（下一步）。
6. 在“Address”（地址）字段键入 NTP 服务器的 DNS 名称。此服务通常托管在 Active Directory 域控制器上。
7. 将“Options”（选项）字段保持不变。
8. 单击 **Test**（测试）检查 NTP 服务是否可访问。
9. 在随后的一系列窗口中一直单击 **OK**（确定）保存更改。

注意：

对于 SLES 12 实施，NTP 守护程序可能会因 SUSE 上与 AppArmor 策略有关的一个已知问题而无法启动。请单击[解决方案](#)了解其他信息。

步骤 1d：安装 Linux VDA 依赖软件包

适用于 SUSE Linux Enterprise 的 Linux VDA 软件依赖于以下软件包：

- PostgreSQL
 - SLED/SLES 11: 9.1 版或更高版本
 - SLED/SLES 12: 9.3 版或更高版本
- OpenJDK 1.7.0
- OpenMotif Runtime Environment 2.3.1 或更高版本
- Cups
 - SLED/SLES 11: 1.3.7 版或更高版本
 - SLED/SLES 12: 1.6.0 版或更高版本
- Foomatic 过滤器
 - SLED/SLES 11: 3.0.0 版或更高版本
 - SLED/SLES 12: 1.0.0 版或更高版本
- ImageMagick
 - SLED/SLES 11: 6.4.3.6 版或更高版本
 - SLED/SLES 12: 6.8 版或更高版本

添加存储库 某些 SUSE Linux Enterprise 存储库中不提供一些必需的软件包：

- SLED 11: PostgreSQL 在 SLES 11 中可用，但在 SLED 11 中不可用。
- SLES 11: OpenJDK 和 OpenMotif 在 SLED 11 中可用，但在 SLES 11 中不可用。

- SLED 12: PostgreSQL 在 SLES 12 中可用，但在 SLED 12 中不可用。ImageMagick 可通过 SLE 12 SDK ISO 或联机存储库提供。
- SLES 12: 没有问题。所有软件包都可用。ImageMagick 可通过 SLE 12 SDK ISO 或联机存储库提供。

要解决该问题，请从正在安装的替换 SLE 版本的介质中获取缺失的软件包。也就是说，从 SLES 介质中获取 SLED 安装缺失的软件包，以及从 SLED 介质中获取 SLES 安装缺失的软件包。以下方法会装载 SLED 和 SLES ISO 介质文件并添加存储库。

- 在 SLED 11 中，运行以下命令：

```
1 sudo mkdir -p /mnt/sles
2
3 sudo mount -t iso9660 path-to-iso/SLES-11-SP4-DVD-x86_64-GM-DVD1.iso /
  mnt/sles
4
5 sudo zypper ar -f /mnt/sles sles
6 <!--NeedCopy-->
```

- 在 SLES 11 中，运行以下命令：

```
1 sudo mkdir -p /mnt/sled
2
3 sudo mount -t iso9660 path-to-iso/SLED-11-SP4-DVD-x86_64-GM-DVD1.iso /
  mnt/sled
4
5 sudo zypper ar -f /mnt/sled sled
6 <!--NeedCopy-->
```

- 在 SLED 12 中，运行以下命令：

```
1 sudo mkdir -p /mnt/sles
2
3 sudo mount -t iso9660 path-to-iso/SLES-12-SP2-DVD-x86_64-GM-DVD1.iso /
  mnt/sles
4
5 sudo zypper ar -f /mnt/sles sles
6 <!--NeedCopy-->
```

- 在 SLED/SLES 12 中，运行以下命令：

```
1 sudo mkdir -p /mnt/sdk
2
3 sudo mount -t iso9660 path-to-iso/SLE-12-SP3-SDK-DVD-x86_64-GM-DVD1.iso
  /mnt/sdk
4
5 sudo zypper ar -f /mnt/sdk sdk
6 <!--NeedCopy-->
```

安装 **Kerberos** 客户端 安装 Kerberos 客户端，在 Linux VDA 与 Delivery Controller 之间实现双向身份验证：

```
1 sudo zypper install krb5-client
2 <!--NeedCopy-->
```

Kerberos 客户端配置依赖于所使用的 Active Directory 集成方法。请参阅下面的说明。

安装 **OpenJDK** Linux VDA 依赖于 OpenJDK 1.7.0。

提示：

为避免出现问题，请务必仅安装 OpenJDK 1.7.0 版。删除系统中的所有其他版本的 Java。

- **SLED:**

1. 在 SLED 上，Java 运行时环境通常随操作系统一起安装。检查是否已安装它：

```
1 sudo zypper info java-1_7_0-openjdk
2 <!--NeedCopy-->
```

2. 如果状态显示为过时，请更新为最新版本：

```
1 sudo zypper update java-1_7_0-openjdk
2 <!--NeedCopy-->
```

3. 检查 Java 版本：

```
1 java -version
2 <!--NeedCopy-->
```

- **SLES:**

1. 在 SLES 上，安装 Java 运行时环境：

```
1 sudo zypper install java-1_7_0-openjdk
2 <!--NeedCopy-->
```

2. 检查 Java 版本：

```
1 java -version
2 <!--NeedCopy-->
```

安装 **PostgreSQL**

- 在 SLED/SLES 11 中，安装以下软件包：

```
1 sudo zypper install libecpg6
2
3 sudo zypper install postgresql-init
4
5 sudo zypper install postgresql
```

```
6
7  sudo zypper install postgresql-server
8
9  sudo zypper install postgresql-jdbc
10 <!--NeedCopy-->
```

此时需要执行安装后步骤，以便初始化数据库服务，并确保 PostgreSQL 在计算机启动时启动：

```
1  sudo /sbin/insserv postgresql
2
3  sudo /etc/init.d/postgresql restart
4  <!--NeedCopy-->
```

- 在 SLED/SLES 12 中，安装以下软件包：

```
1  sudo zypper install postgresql-init
2
3  sudo zypper install postgresql-server
4
5  sudo zypper install postgresql-jdbc
6  <!--NeedCopy-->
```

此时需要执行安装后步骤，以便初始化数据库服务，并确保 PostgreSQL 在计算机启动时启动：

```
1  sudo systemctl enable postgresql
2
3  sudo systemctl restart postgresql
4  <!--NeedCopy-->
```

数据库文件位于 `/var/lib/pgsql/data`。

删除存储库 安装依赖的软件包后便可以删除之前设置的替代版本存储库并卸载介质：

- 在 SLED 11 中，运行以下命令以删除软件包：

```
1  sudo zypper rr sles
2
3  sudo umount /mnt/sles
4
5  sudo rmdir /mnt/sles
6  <!--NeedCopy-->
```

- 在 SLES 11 中，运行以下命令以删除软件包：

```
1  sudo zypper rr sled
2
3  sudo umount /mnt/sled
4
5  sudo rmdir /mnt/sled
6  <!--NeedCopy-->
```

- 在 SLED 12 中，运行以下命令以删除软件包：

```
1 sudo zypper rr sles
2
3 sudo umount /mnt/sles
4
5 sudo rmdir /mnt/sles
6 <!--NeedCopy-->
```

- 在 SLED/SLES 12 中，运行以下命令以删除软件包：

```
1 sudo zypper rr sdk
2
3 sudo umount /mnt/sdk
4
5 sudo rmdir /mnt/sd
6 <!--NeedCopy-->
```

步骤 2：为虚拟机管理程序准备 Linux VM

在支持的虚拟机管理程序上将 Linux VDA 当作虚拟机运行时，需要作出一些更改。根据使用的虚拟机管理程序平台作出以下更改。如果正在裸机硬件上运行 Linux 计算机，则无需作出任何更改。

修复 Citrix XenServer 上的时间同步问题

如果启用了 XenServer 时间同步功能，则在每个半虚拟化 Linux VM 中，您会发现 NTP 和 XenServer 都在尝试管理系统时钟。为避免时钟与其他服务器不同步，每个 Linux 客户机中的系统时钟都必须与 NTP 同步。这种情况要求禁用主机时间同步。无需在 HVM 模式下进行任何更改。

在某些 Linux 发行版中，如果正在运行半虚拟化 Linux 内核，并安装了 XenServer Tools，您可以检查 XenServer 时间同步功能是否存在，以及是否已在 Linux VM 中启用：

```
1 su -
2
3
4
5 cat /proc/sys/xen/independent_wallclock
6 <!--NeedCopy-->
```

此命令返回 0 或 1：

- 0 - 时间同步功能已启用，且必须禁用。
- 1 - 时间同步功能已禁用，无需采取任何操作。

如果 `/proc/sys/xen/indepent_wallclock` 文件不存在，则不需要执行以下步骤。

如果已启用，请通过向该文件写入 **1** 来禁用时间同步功能：

```
1 sudo echo 1 > /proc/sys/xen/independent_wallclock
2 <!--NeedCopy-->
```

要使此更改成为永久更改，并在重新启动后仍然有效，请编辑 **/etc/sysctl.conf** 文件并添加以下行：

```
xen.independent_wallclock = 1
```

要验证这些更改，请重新启动系统：

```
1 reboot
2 <!--NeedCopy-->
```

重新启动后，检查此设置是否正确：

```
1 su -
2 cat /proc/sys/xen/independent_wallclock
3 <!--NeedCopy-->
```

此命令返回值 1。

修复 **Microsoft Hyper-V** 上的时间同步问题

安装了 Hyper-V Linux 集成服务的 Linux VM 可应用 Hyper-V 时间同步功能来使用主机操作系统的时间。为确保系统时钟始终精确可靠，请一同启用此功能与 NTP 服务。

从管理操作系统中：

1. 打开 Hyper-V 管理器控制台。
2. 对于 Linux VM 的设置，请选择 **Integration Services**（集成服务）。
3. 确保已选择 **Time synchronization**（时间同步）。

注意：

此方法与 VMware 和 XenServer 不同，这两种产品会禁用主机时间同步功能，以免与 NTP 发生冲突。Hyper-V 时间同步可以与 NTP 时间同步共存并互补。

修复 **ESX** 和 **ESXi** 上的时间同步问题

如果启用了 VMware 时间同步功能，则在每个半虚拟化 Linux VM 中，您会发现 NTP 和虚拟机管理程序都在尝试同步系统时钟。为避免时钟与其他服务器不同步，每个 Linux 客户机中的系统时钟都必须与 NTP 同步。这种情况要求禁用主机时间同步。

如果正在运行安装了 VMware Tools 的半虚拟化 Linux 内核：

1. 打开 vSphere Client。
2. 编辑 Linux VM 设置。

3. 在 **Virtual Machine Properties** (虚拟机属性) 对话框中, 打开 **Options** (选项) 选项卡。
4. 选择 **VMware Tools**。
5. 在 **Advanced** (高级) 框中, 取消选中 **Synchronize guest time with host** (与主机同步客户机时间)。

步骤 3: 向 **Windows** 域中添加 **Linux** 虚拟机 (VM)

Linux VDA 支持多种向 Active Directory (AD) 域添加 Linux 计算机的方法:

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl

根据所选的方法, 按说明执行操作。

Samba Winbind

加入 **Windows** 域 您的域控制器必须可访问, 并且您必须具有有权将计算机添加到域的 Active Directory 用户帐户:

1. 打开 YaST 的 “Windows Domain Membership” (Windows 域成员身份)。
2. 进行以下更改:
 - 将域或工作组设为 Active Directory 域的名称或域控制器的 IP 地址。确保域名为大写。
 - 选中 **Also Use SMB information for Linux Authentication** (同时为 Linux 身份验证使用 SMB 信息)。
 - 选中 **Create Home Directory on Login** (在登录时创建主目录)。
 - 选中 **Single Sign-on for SSH** (为 SSH 使用单点登录)。
 - 确保未选中 **Offline Authentication** (脱机身份验证)。此选项与 Linux VDA 不兼容。
3. 单击确定。如果提示安装某些软件包, 请单击 **Install** (安装)。
4. 如果找到域控制器, 则会询问您是否要加入域。单击是。
5. 出现提示时, 键入有权将计算机添加到域的域用户的凭据, 然后单击 **OK** (确定)。
6. 此时会显示一条消息, 说明操作成功。
7. 如果提示安装某些 samba 和 krb5 软件包, 请单击 **Install** (安装)。

YaST 可能会说明这些更改需要重新启动计算机或一些服务。我们建议您重新启动计算机:

```
1 su -
2
3 reboot
4 <!--NeedCopy-->
```

仅限 **SLED/SLES 12**: 修补了 **Kerberos** 凭据缓存名称。SLED/SLES 12 已将默认 Kerberos 凭据缓存名称规范从常用的 **FILE:/tmp/krb5cc_%{uid}** 更改为 **DIR:/run/user/%{uid}/krb5cc**。这种全新 DIR 缓存方法与 Linux VDA 不兼容, 必须进行手动更改。以 root 用户身份, 编辑 **/etc/krb5.conf** 并在 **[libdefaults]** 部分下添加以下设置 (如果尚未设置):

```
default_ccache_name = FILE:/tmp/krb5cc_%{ uid }
```

验证域成员身份 Delivery Controller 要求所有 VDA 计算机 (Windows 和 Linux VDA) 都要在 Active Directory 中有一个计算机对象。

运行 Samba 的 **net ads** 命令以验证计算机是否已加入域:

```
1 sudo net ads testjoin
2 <!--NeedCopy-->
```

运行以下命令验证额外的域和计算机对象信息:

```
1 sudo net ads info
2 <!--NeedCopy-->
```

验证 **Kerberos** 配置 为了确保 Kerberos 已正确配置为可与 Linux VDA 配合使用, 请检查系统 keytab 文件是否已创建并且包含有效密钥:

```
1 sudo klist -ke
2 <!--NeedCopy-->
```

此命令显示各种主体名称与密码套件组合可用的密钥列表。运行 Kerberos **kinit** 命令, 使用这些密钥向域控制器验证计算机的身份:

```
1 sudo kinit -k MACHINE$@REALM
2 <!--NeedCopy-->
```

计算机和领域名称必须指定为大写。美元符号 (\$) 必须使用反斜杠 (\) 进行转义, 以免发生 shell 替换。在某些环境中, DNS 域名与 Kerberos 领域名称不同。请确保使用领域名称。如果此命令成功运行, 则不会显示任何输出。

请使用以下命令验证计算机帐户的 TGT 票据已缓存:

```
1 sudo klist
2 <!--NeedCopy-->
```

请使用以下命令检查计算机帐户详细信息:

```
1 sudo net ads status
2 <!--NeedCopy-->
```

验证用户身份验证 使用 **wbinfo** 工具验证是否可向域验证域用户的身份:

```
1 wbinfo --krb5auth=domain\username%password
2 <!--NeedCopy-->
```

这里指定的域为 AD 域名，而不是 Kerberos 领域名称。对于 bash shell，必须使用另一个反斜杠对反斜杠 (\) 字符进行转义。此命令返回一条成功或失败消息。

要验证 Winbind PAM 模块是否已正确配置，请使用域用户帐户登录 Linux VDA。该域用户帐户以前未曾使用过。

```
1 ssh localhost -l domain\username
2
3 id -u
4 <!--NeedCopy-->
```

检查是否为 **id -u** 命令返回的 uid 创建了对应的 Kerberos 凭据缓存文件：

```
1 ls /tmp/krb5cc_uid
2 <!--NeedCopy-->
```

检查用户 Kerberos 凭据缓存中的票据是否有效且未过期：

```
1 klist
2 <!--NeedCopy-->
```

退出会话

```
1 exit
2 <!--NeedCopy-->
```

直接登录 Gnome 或 KDE 控制台也可以执行类似的测试。在进行域加入验证后继续执行[步骤 4: 安装 Linux VDA](#)。

Quest Authentication Service

在域控制器上配置 **Quest** 假定您已在 Active Directory 域控制器上安装并配置了 Quest 软件，而且已获得管理权限，有权在 Active Directory 中创建计算机对象。

允许域用户登录 **Linux VDA** 计算机 为了让域用户能够在 Linux VDA 计算机上建立 HDX 会话：

1. 在 Active Directory 用户和计算机管理控制台中，为该用户帐户打开 Active Directory 用户属性。
2. 选择 **Unix Account** (Unix 帐户) 选项卡。
3. 选中 **Unix-enabled** (已启用 Unix)。
4. 将 **Primary GID Number** (首选 GID 编号) 设置为实际域用户组的组 ID。

注意：

这些说明相当于设置域用户，以便他们可以使用控制台、RDP、SSH 或任何其他远程协议进行登录。

在 **Linux VDA** 上配置 **Quest**

配置 **VAS** 守护程序 必须启用并断开自动续订 Kerberos 票据功能。必须禁用身份验证（脱机登录）功能：

```
1 sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-  
   interval 32400  
2  
3 sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-  
   auth false  
4 <!--NeedCopy-->
```

此命令将续订间隔设为 9 小时（32400 秒），即比默认的 10 小时票据生命周期短 1 小时。请在票据生命周期较短的系统上设置较低的值。

配置 **PAM** 和 **NSS** 要启用通过 HDX 进行的域用户登录以及其他服务（例如 su、ssh 和 RDP），请运行以下命令以手动配置 PAM 和 NSS：

```
1 sudo /opt/quest/bin/vastool configure pam  
2  
3 sudo /opt/quest/bin/vastool configure nss  
4 <!--NeedCopy-->
```

加入 **Windows** 域 使用 Quest `vastool` 命令将 Linux 计算机加入到 Active Directory 域中：

```
1 sudo /opt/quest/bin/vastool -u user join domain-name  
2 <!--NeedCopy-->
```

user 为有权将计算机加入 Active Directory 域的任何域用户。**domain-name** 为域的 DNS 名称，例如 `example.com`。

验证域成员身份 Delivery Controller 要求所有 VDA 计算机（Windows 和 Linux VDA）都要在 Active Directory 中有一个计算机对象。要验证加入了 Quest 的 Linux 计算机是否位于域中，请执行以下操作：

```
1 sudo /opt/quest/bin/vastool info domain  
2 <!--NeedCopy-->
```

如果计算机已加入域，此命令会返回域名。如果计算机未加入任何域，则会显示以下错误：

```
ERROR: No domain could be found.  
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm  
default_realm not configured in vas.conf. Computer may not be joined  
to domain
```

验证用户身份验证 要验证 Quest 是否可以通过 PAM 对域用户进行身份验证，请使用域用户帐户登录 Linux VDA。该域用户帐户以前未曾使用过。

```
1 ssh localhost -l domain\username
2
3 id -u
4 <!--NeedCopy-->
```

检查是否为 **id -u** 命令返回的 **uid** 创建了对应的 Kerberos 凭据缓存文件：

```
1 ls /tmp/krb5cc_uid
2 <!--NeedCopy-->
```

检查 Kerberos 凭据缓存中的票据是否有效且未过期：

```
1 /opt/quest/bin/vastool klist
2 <!--NeedCopy-->
```

退出会话。

```
1 exit
2 <!--NeedCopy-->
```

直接登录 Gnome 或 KDE 控制台也可以执行类似的测试。在进行域加入验证后继续执行[步骤 4: 安装 Linux VDA](#)。

Centrify DirectControl

加入 **Windows** 域 安装 Centrify DirectControl Agent 后，请使用 Centrify **adjoin** 命令将 Linux 计算机加入 Active Directory 域：

```
1 su -
2
3 adjoin -w -V -u user domain-name
4 <!--NeedCopy-->
```

user 为有权将计算机加入 Active Directory 域的任何 Active Directory 域用户。**domain-name** 是将 Linux 计算机加入到的域的名称。

验证域成员身份 Delivery Controller 要求所有 VDA 计算机 (Windows 和 Linux VDA) 都要在 Active Directory 中有一个计算机对象。要验证加入了 Centrify 的 Linux 计算机是否位于域中，请执行以下操作：

```
1 su -
2
3 adinfo
4 <!--NeedCopy-->
```

检查 **Joined to domain** 值是否有效以及 **CentrifyDC mode** 是否返回了 **connected**。如果模式仍然卡在正在启动状态，则表明 Centrify 客户端遇到了服务器连接或身份验证问题。

请使用以下命令可获得更全面的系统和诊断信息：

```
1 adinfo --sysinfo all
2
3 adinfo -diag
4 <!--NeedCopy-->
```

测试与各种 Active Directory 和 Kerberos 服务的连接。

```
1 adinfo --test
2 <!--NeedCopy-->
```

在进行域加入验证后继续执行[步骤 4: 安装 Linux VDA](#)。

步骤 4: 安装 Linux VDA

步骤 4a: 卸载旧版本

如果安装了除先前的两个版本和 LTSR 版本之外的早期版本，请在安装新版本之前将其卸载。

1. 停止 Linux VDA 服务：

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx stop
4 <!--NeedCopy-->
```

2. 卸载软件包：

```
1 sudo rpm -e XenDesktopVDA
2 <!--NeedCopy-->
```

重要提示：

支持从先前的两个版本进行升级。

注意：

安装组件位于 **/opt/Citrix/VDA/** 中。

要运行命令，需要提供完整路径；或者，也可以将 **/opt/Citrix/VDA/sbin** 和 **/opt/Citrix/VDA/bin** 添加到系统路径。

步骤 4b: 下载 Linux VDA 软件包

转至 Citrix Web 站点并根据您的 Linux 发行版下载相应的 Linux VDA 软件包。

步骤 4c: 安装 Linux VDA

使用 Zypper 安装 Linux VDA 软件:

对于 **SUSE 12**:

```
1 sudo zypper install XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
2 <!--NeedCopy-->
```

对于 **SUSE 11**:

```
1 sudo zypper install XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
2 <!--NeedCopy-->
```

使用 RPM 软件包管理器安装 Linux VDA 软件。在此之前, 请解决以下依赖项:

对于 **SUSE 12**:

```
1 sudo rpm -i XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
2 <!--NeedCopy-->
```

对于 **SUSE 11**:

```
1 sudo rpm -i XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
2 <!--NeedCopy-->
```

步骤 4d: 升级 Linux VDA (可选)

可以使用 RPM 软件包管理器将 Linux VDA 软件从 7.14 版和 7.13 版进行升级:

对于 **SUSE 12**:

```
1 sudo rpm -U XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
2 <!--NeedCopy-->
```

对于 **SUSE 11**:

```
1 sudo rpm -U XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
2 <!--NeedCopy-->
```

SUSE 12 的 RPM 依赖项列表:

```
1 postgresql-server >= 9.3
2
3 postgresql-jdbc >= 9.2
4
5 java-1.7.0-openjdk >= 1.7.0
6
7 ImageMagick >= 6.8
8
9 dbus-1 >= 1.8.8
```

```
10
11 dbus-1-x11 >= 1.8.8
12
13 libXpm4 >= 3.5.11
14
15 libXrandr2 >= 1.4.2
16
17 libXtst6 >= 1.2.2
18
19 motif >= 2.3
20
21 pam >= 1.1.8
22
23 bash >= 4.2
24
25 findutils >= 4.5
26
27 gawk >= 4.1
28
29 sed >= 4.2
30
31 cups >= 1.6.0
32
33 cups-filters-foomatic-rip >= 1.0.0
34
35 openldap2 >= 2.4
36
37 cyrus-sasl >= 2.1
38
39 cyrus-sasl-gssapi >= 2.1
40
41 libxml2 >= 2.9
42
43 python-requests >= 2.8.1
44
45 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
46
47 rpmlib(CompressedFileNames) <= 3.0.4-1
48
49 rpmlib(PayloadIsLzma) <= 4.4.6-1
50 <!--NeedCopy-->
```

SUSE 11 的 RPM 依赖项列表:

```
1 postgresql-server >= 9.1.
2
3 postgresql-jdbc >= 9.1
4
5 java-1_7_0-openjdk >= 1.7.0.6
6
7 ImageMagick >= 6.4.3.6
8
9 ConsoleKit >= 0.2.10
```

```
10
11 dbus-1 >= 1.2.10
12
13 dbus-1-x11 >= 1.2.10
14
15 xorg-x11-libXpm >= 7.4
16
17 xorg-x11-libs >= 7.4
18
19 openmotif-libs >= 2.3.1
20
21 pam >= 1.1.5
22
23 libdrm >= 2.4.41
24
25 libpixman-1-0 >= 0.24.4
26
27 Mesa >= 9.0
28
29 openssl >= 0.9.8j
30
31 xorg-x11 >= 7.4
32
33 xorg-x11-fonts-core >= 7.4
34
35 xorg-x11-libXau >= 7.4
36
37 xorg-x11-libXdmcp >= 7.4
38
39 bash >= 3.2
40
41 findutils >= 4.4
42
43 gawk >= 3.1
44
45 sed >= 4.1
46
47 cups >= 1.3.7
48
49 foomatic-filters >= 3.0.0
50
51 openldap2 >= 2.4
52
53 cyrus-sasl >= 2.1
54
55 cyrus-sasl-gssapi >= 2.1
56
57 libxml2 >= 2.7
58
59 python-requests >= 2.0.1
60
61 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
62
```

```
63 rpmlib(CompressedFileNames) <= 3.0.4-1
64
65 rpmlib(PayloadIsLzma) <= 4.4.6-1
66 <!--NeedCopy-->
```

重要提示：

在升级后重新启动 Linux VDA 计算机。

步骤 5: 配置 Linux VDA

安装软件包后，必须运行 `ctxsetup.sh` 脚本来配置 Linux VDA。执行任何更改之前，该脚本都会验证环境，确保所有依赖项都已安装。如有必要，可以随时重新运行该脚本以更改设置。

可以按照提示手动运行脚本，也可以采用预先配置的反应自动运行脚本。继续操作前，请查看该脚本的帮助信息：

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh - help
2 <!--NeedCopy-->
```

提示配置

运行会提示各种问题的手动配置：

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
2 <!--NeedCopy-->
```

自动配置

自动安装时，通过环境变量提供设置脚本所需的选项。如果所需的所有变量都存在，脚本不会提示您提供任何信息。

支持的环境变量包括：

- **CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N** - Linux VDA 支持使用 DNS CNAME 记录指定 Delivery Controller 名称。默认情况下设置为 N。
- **CTX_XDL_DDC_LIST = list-ddc-fqdns** - Linux VDA 要求提供由空格分隔的 Delivery Controller 完全限定域名 (FQDN) 列表以用于向 Delivery Controller 注册。必须至少指定一个 FQDN 或 CNAME 别名。
- **CTX_XDL_VDA_PORT = port-number** - Linux VDA 通过 TCP/IP 端口（默认为端口 80）与 Delivery Controller 通信。
- **CTX_XDL_REGISTER_SERVICE = Y | N** - 在启动计算机后启动 Linux Virtual Desktop 服务。默认情况下，该值设置为 Y。
- **CTX_XDL_ADD_FIREWALL_RULES = Y | N** - Linux Virtual Desktop 服务要求允许传入网络连接通过系统防火墙。您可以在系统防火墙中自动为 Linux Virtual Desktop 打开所需端口（默认为端口 80 和 1494）。默认情况下设置为 Y。

- **CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 | 4** - Linux VDA 要求使用 Kerberos 配置设置向 Delivery Controller 进行身份验证。Kerberos 配置根据系统上已安装和已配置的 Active Directory 集成工具确定。指定要使用且受支持的 Active Directory 集成方法：
 - 1 - Samba Winbind
 - 2 - Quest Authentication Service
 - 3 - Centrify DirectControl
 - 4 - SSSD
- **CTX_XDL_HDX_3D_PRO = Y | N** - Linux VDA 支持 HDX 3D Pro，这是一组 GPU 加速技术，旨在优化富图形应用程序的虚拟化水平。如果选择了 HDX 3D Pro，则要为 VDI 桌面（单会话）模式配置 Virtual Delivery Agent -（即 CTX_XDL_VDI_MODE=Y）。
- **CTX_XDL_VDI_MODE = Y | N** - 将计算机配置为专用桌面交付模型 (VDI) 还是托管共享桌面交付模型。对于 HDX 3D Pro 环境，将此变量设置为 Y。默认情况下，此变量设置为 N。
- **CTX_XDL_SITE_NAME = dns-name** - Linux VDA 通过 DNS 发现 LDAP 服务器。要将 DNS 搜索结果限制为本地站点，应指定 DNS 站点名称。默认情况下，此变量设置为 **<none>**。
- **CTX_XDL_LDAP_LIST = list-ldap-servers** - Linux VDA 查询 DNS 来发现 LDAP 服务器。如果 DNS 无法提供 LDAP 服务记录，您可以提供以空格分隔的 LDAP FQDN（带有 LDAP 端口）列表。例如 ad1.mycompany.com:389。默认情况下，此变量设置为 **<none>**。
- **CTX_XDL_SEARCH_BASE = search-base-set** - Linux VDA 通过设置为 Active Directory 域根的搜索库来查询 LDAP（例如，DC=mycompany,DC=com）。为提高搜索性能，可以指定搜索基础（例如 OU=VDI,DC=mycompany,DC=com）。默认情况下，此变量设置为 **<none>**。
- **CTX_XDL_START_SERVICE = Y | N** - 在完成 Linux VDA 配置后，是否启动 Linux VDA 服务。默认情况下设置为 Y。

设置环境变量并运行配置脚本：

```
1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
2
3 export CTX_XDL_DDC_LIST=list-ddc-fqdns
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-name
18
19 export CTX_XDL_LDAP_LIST=list-ldap-servers
20
```

```
21 export CTX_XDL_SEARCH_BASE=search-base-set
22
23 export CTX_XDL_START_SERVICE=Y|N
24
25 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
26 <!--NeedCopy-->
```

运行 `sudo` 命令时，键入 **-E** 选项以将现有环境变量传递给其创建的新 shell。Citrix 建议使用前面的命令并加上 **#!/bin/bash** 作为第一行来创建 shell 脚本文件。

另外，您可以使用单个命令指定所有参数：

```
1 sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3 CTX_XDL_DDC_LIST=list-ddc-fqdns \
4
5 CTX_XDL_VDA_PORT=port-number \
6
7 CTX_XDL_REGISTER_SERVICE=Y|N \
8
9 CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST=list-ldap-servers \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_START_SERVICE=Y|N \
24
25 /opt/Citrix/VDA/sbin/ctxsetup.sh
26 <!--NeedCopy-->
```

删除配置更改

在某些情形下，您可能需要删除 **ctxsetup.sh** 脚本对配置所做的更改，但不卸载 Linux VDA 软件包。

继续操作前，请查看此脚本的帮助信息：

```
1 sudo /usr/local/sbin/ctxcleanup.sh --help
2 <!--NeedCopy-->
```

删除配置更改：

```
1 sudo /usr/local/sbin/ctxcleanup.sh
```

```
2 <!--NeedCopy-->
```

重要提示:

此脚本会从数据库删除所有配置数据,从而使 Linux VDA 无法使用。

配置日志

ctxsetup.sh 和 **ctxcleanup.sh** 脚本会在控制台上显示错误,并将其他信息写入配置日志文件:

`/tmp/xdl.configure.log`

重新启动 Linux VDA 服务,确保更改生效。

步骤 6: 运行 Linux VDA

使用 **ctxsetup.sh** 脚本配置 Linux VDA 后,可以运行以下命令来控制 Linux VDA。

启动 **Linux VDA**:

启动 Linux VDA 服务:

```
1 sudo /sbin/service ctxhdx start
2
3 sudo /sbin/service ctxvda start
4 <!--NeedCopy-->
```

停止 **Linux VDA**:

要停止 Linux VDA 服务,请执行以下操作:

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx stop
4 <!--NeedCopy-->
```

重新启动 **Linux VDA**:

重新启动 Linux VDA 服务:

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx restart
4
5 sudo /sbin/service ctxvda start
6 <!--NeedCopy-->
```

检查 **Linux VDA** 状态:

要检查 Linux VDA 服务的运行状态,请执行以下操作:

```
1 sudo /sbin/service ctxvda status
2
3 sudo /sbin/service ctxhdx status
4 <!--NeedCopy-->
```

步骤 7: 在 **XenApp** 或 **XenDesktop** 中创建计算机目录

创建计算机目录和添加 Linux VDA 计算机的过程与传统的 Windows VDA 方法类似。有关如何完成这些任务的更加详细的说明, 请参阅[创建计算机目录](#)和[管理计算机目录](#)。

创建包含 Linux VDA 计算机的计算机目录时会面临一些限制, 使得该过程不同于为 Windows VDA 计算机创建计算机目录:

- 对于操作系统, 请选择:
 - “服务器操作系统” 选项 (对于托管共享桌面交付模型)。
 - “桌面操作系统” 选项 (对于 VDI 专用桌面交付模型)。
- 确保计算机未执行电源管理设置。
- 由于 Linux VDA 不支持 MCS, 请选择 [PVS](#) 或其他服务或技术 (现有映像) 部署方法。
- 请勿在同一个计算机目录中混合使用 Linux 和 Windows VDA 计算机。

注意:

早期版本的 Citrix Studio 不支持 “Linux 操作系统” 的概念。但是, 选择 Windows Server 操作系统或服务器操作系统选项等同于使用托管共享桌面交付模型。选择 Windows 桌面操作系统或桌面操作系统选项等同于使用每计算机一个用户交付模型。

提示:

如果删除计算机后将其重新加入 Active Directory 域, 则必须删除计算机, 然后将其重新添加到计算机目录。

步骤 8: 在 **XenApp** 或 **XenDesktop** 中创建交付组

创建交付组和添加包含 Linux VDA 计算机的计算机目录的过程与 Windows VDA 计算机几乎相同。有关如何完成这些任务的更加详细的说明, 请参阅[创建交付组](#)。

创建含有 Linux VDA 计算机目录的交付组时会面临以下限制:

- 对于交付类型, 请选择 “桌面” 或 “应用程序”。
- 确保所选的 AD 用户和组已正确配置, 可以登录到 Linux VDA 计算机。
- 请勿允许未经身份验证的 (匿名) 用户登录。
- 请勿在交付组中混入含有 Windows 计算机的计算机目录。

重要提示：

Linux VDA 1.4 及更高版本支持发布应用程序。但是，Linux VDA 不支持将桌面和应用程序交付给相同的计算机。

安装 Linux Virtual Delivery Agent for Ubuntu

June 21, 2022

可以选择按照本文中的步骤进行手动安装，也可以使用[轻松安装](#)进行自动安装和配置。轻松安装省时又省力，与手动安装相比，更不易于出错。

注意：

请仅对全新安装使用轻松安装功能。请勿使用轻松安装更新现有安装。

步骤 1：为 VDA 安装准备 Ubuntu

步骤 1a：验证网络配置

请确保您先连接并正确配置网络，然后再继续操作。

步骤 1b：设置主机名

为确保正确报告计算机的主机名，请更改 `/etc/hostname` 文件，使其仅包含计算机的主机名。

`hostname`

步骤 1c：为主机名分配环回地址

为确保正确报告计算机的 DNS 域名和完全限定域名 (FQDN)，请更改 `/etc/hosts` 文件中的以下行，使其前两个条目为 FQDN 和主机名：

```
127.0.0.1 hostname-fqdn hostname localhost
```

例如：

```
127.0.0.1 vda01.example.com vda01 localhost
```

从文件中的其他条目中删除对 `hostname-fqdn` 或 `hostname` 的任何其他引用。

注意：

Linux VDA 当前不支持 NetBIOS 名称截断。因此，主机名不得超过 15 个字符。

提示：

只能使用字符 a-z、A-Z、0-9 和连字符 (-)。请避免使用下划线 (_)、空格和其他符号。主机名不得以数字开头和以连字符结尾。此规则也适用于 Delivery Controller 主机名。

步骤 1d: 检查主机名

验证主机名设置是否正确无误：

```
1 hostname
2 <!--NeedCopy-->
```

此命令仅返回计算机的主机名，而不返回其 FQDN。

验证 FQDN 设置是否正确无误：

```
1 hostname -f
2 <!--NeedCopy-->
```

此命令返回计算机的 FQDN。

步骤 1e: 禁用多播 DNS

默认设置启用了多播 DNS (mDNS)，而这会导致名称解析结果不一致。

要禁用 mDNS，请编辑 `/etc/nsswitch.conf` 并更改包含以下内容的行：

```
hosts: files mdns_minimal [NOTFOUND=return] dns
```

更改为：

```
hosts: files dns
```

步骤 1f: 检查名称解析和服务可访问性

确认可以解析 FQDN 并对域控制器和 Delivery Controller 执行 ping 操作：

```
1 nslookup domain-controller-fqdn
2
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
8 <!--NeedCopy-->
```

如果无法解析 FQDN 或 Ping 不通上述任一计算机，请先检查相关步骤，然后再继续。

步骤 1g: 配置时钟同步 (chrony)

确保 VDA、Delivery Controller 和域控制器之间的时钟始终精确同步至关重要。将 Linux VDA 托管为虚拟机可能会导致时钟偏差问题。出于此原因，最好使用远程时间服务来同步时间。

安装 chrony:

```
1 apt-get install chrony
2 <!--NeedCopy-->
```

以 root 用户身份，编辑 `/etc/chrony/chrony.conf` 并为每个远程时间服务器添加一个服务器条目:

```
server peer1-fqdn-or-ip-address iburst
server peer2-fqdn-or-ip-address iburst
```

在典型部署中，时间从本地域控制器同步，而不是直接从公共 NTP 池服务器同步。为域中的每个 Active Directory 域控制器添加一个服务器条目。

删除列出的任何其他 **server** 或 **pool** 条目，包括环回 IP 地址、localhost 和公共服务器 ***.pool.ntp.org** 条目。

保存更改并重新启动 Chrony 守护程序:

```
1 sudo systemctl restart chrony
2 <!--NeedCopy-->
```

步骤 1h: 安装 OpenJDK

Linux VDA 依赖于 OpenJDK。通常，运行时环境作为操作系统安装的一部分进行安装。使用以下命令检查是否已安装它:

```
1 sudo apt-get install -y default-jdk
2 <!--NeedCopy-->
```

步骤 1i: 安装 PostgreSQL

Linux VDA 要求在 Ubuntu 16.04 上安装 PostgreSQL 9.x 版:

```
1 sudo apt-get install -y postgresql
2
3 sudo apt-get install -y libpostgresql-jdbc-java
4 <!--NeedCopy-->
```

步骤 1j: 安装 Motif

```
1 sudo apt-get install -y libxm4
2 <!--NeedCopy-->
```

步骤 1k: 安装其他软件包

```
1 sudo apt-get install -y libsasl2-2
2
3 sudo apt-get install -y libsasl2-modules-gssapi-mit
4
5 sudo apt-get install -y libldap-2.4-2
6
7 sudo apt-get install -y krb5-user
8
9 sudo apt-get install -y cups
10 <!--NeedCopy-->
```

步骤 2: 准备虚拟机管理程序

在支持的虚拟机管理程序上将 Linux VDA 当作虚拟机运行时，需要作出一些更改。根据使用的虚拟机管理程序平台作出以下更改。如果正在裸机硬件上运行 Linux 计算机，则无需作出任何更改。

修复 **Citrix XenServer** 上的时间同步问题

启用了 XenServer 时间同步功能时，在每个半虚拟化 Linux VM 中，您会发现 NTP 和 XenServer 都尝试管理系统时钟。为避免时钟与其他服务器不同步，请确保每个 Linux 客户机中的系统时钟都与 NTP 同步。这种情况要求禁用主机时间同步。无需在 HVM 模式下进行任何更改。

在某些 Linux 发行版中，如果正在运行半虚拟化 Linux 内核，并安装了 XenServer Tools，您可以检查 XenServer 时间同步功能是否存在，以及是否已在 Linux VM 中启用：

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--NeedCopy-->
```

此命令返回 0 或 1：

- 0 - 时间同步功能已启用，且必须禁用。
- 1 - 时间同步功能已禁用，无需采取任何操作。

如果 `/proc/sys/xen/indepent_wallclock` 文件不存在，则不需要执行以下步骤。

如果已启用，请通过向该文件写入 1 以禁用时间同步功能：

```
1 sudo echo 1 > /proc/sys/xen/independent_wallclock
2 <!--NeedCopy-->
```

要使此更改成为永久更改，并在重新启动后仍然有效，请编辑 `/etc/sysctl.conf` 文件并添加以下行：

```
xen.independent_wallclock = 1
```

要验证这些更改，请重新启动系统：

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--NeedCopy-->
```

此命令返回值 1。

在 **Microsoft Hyper-V** 上修复时间同步问题

安装了 Hyper-V Linux 集成服务的 Linux VM 可以使用 Hyper-V 时间同步功能来使用主机操作系统的的时间。为确保系统时钟始终精确可靠，此功能必须随 NTP 服务一同启用。

从管理操作系统中：

1. 打开 Hyper-V 管理器控制台。
2. 对于 Linux VM 的设置，请选择 **Integration Services**（集成服务）。
3. 确保已选择 **Time synchronization**（时间同步）。

注意：

此方法与 VMware 和 XenServer 不同，这两种产品会禁用主机时间同步功能，以免与 NTP 发生冲突。Hyper-V 时间同步可以与 NTP 时间同步共存并互补。

修复 **ESX** 和 **ESXi** 上的时间同步问题

启用了 VMware 时间同步功能时，在每个半虚拟化 Linux VM 中，您会发现 NTP 和虚拟机管理程序都尝试同步系统时钟。为避免时钟与其他服务器不同步，请确保每个 Linux 客户机中的系统时钟都与 NTP 同步。这种情况要求禁用主机时间同步。

如果正在运行安装了 VMware Tools 的半虚拟化 Linux 内核：

1. 打开 vSphere Client。
2. 编辑 Linux VM 设置。
3. 在 **Virtual Machine Properties**（虚拟机属性）对话框中，打开 **Options**（选项）选项卡。
4. 选择 **VMware Tools**。
5. 在 **Advanced**（高级）框中，取消选中 **Synchronize guest time with host**（与主机同步客户机时间）。

步骤 3：向 **Windows** 域中添加 **Linux** 虚拟机 (VM)

Linux VDA 支持多种向 Active Directory (AD) 域添加 Linux 计算机的方法：

- Samba Winbind

- Quest Authentication Service
- Centrify DirectControl
- SSSD

根据所选的方法，按说明执行操作。

Samba Winbind

安装或更新所需软件包

```
1 sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-  
   config krb5-locales krb5-user  
2 <!--NeedCopy-->
```

在计算机启动时启用要启动的 **Winbind** 守护程序 Winbind 守护程序必须配置为在计算机启动时启动：

```
1 sudo systemctl enable winbind  
2 <!--NeedCopy-->
```

配置 **Kerberos** 以 root 用户身份，打开 `/etc/krb5.conf` 并配置以下设置：

```
1 [libdefaults]  
2  
3 default_realm = REALM  
4  
5 dns_lookup_kdc = false  
6  
7  
8  
9 [realms]  
10  
11 REALM = {  
12  
13  
14 admin_server = domain-controller-fqdn  
15  
16 kdc = domain-controller-fqdn  
17  
18 }  
19  
20  
21  
22  
23 [domain_realm]  
24  
25 domain-dns-name = REALM  
26  
27 .domain-dns-name = REALM  
28 <!--NeedCopy-->
```

此上下文中的 **domain-dns-name** 属性为 DNS 域名，例如 **example.com**。**REALM** 是大写的 Kerberos 领域名称，例如 **EXAMPLE.COM**。

配置 Winbind 身份验证 手动配置 Winbind，因为 Ubuntu 没有诸如 RHEL 中的 `authconfig` 和 SUSE 中的 `yast2` 这类工具。

打开 `/etc/samba/smb.conf` 并配置以下设置：

```
1 [global]
2
3 workgroup = WORKGROUP
4
5 security = ADS
6
7 realm = REALM
8
9 encrypt passwords = yes
10
11 idmap config *:range = 16777216-33554431
12
13 winbind trusted domains only = no
14
15 kerberos method = secrets and keytab
16
17 winbind refresh tickets = yes
18
19 template shell = /bin/bash
20 <!--NeedCopy-->
```

WORKGROUP 是 **REALM** 中的第一个字段，**REALM** 是大写的 Kerberos 领域名称。

配置 nsswitch 打开 `/etc/nsswitch.conf` 并将 `winbind` 附加到以下行：

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

加入 Windows 域 您的域控制器必须可访问，而且您必须具有有权将计算机添加到域的 Active Directory 用户帐户。

```
1 sudo net ads join REALM -U user
2 <!--NeedCopy-->
```

其中，**REALM** 是大写的 Kerberos 领域名称，**user** 是有权将计算机添加到域的域用户。

重新启动 winbind

```
1 sudo systemctl restart winbind
2 <!--NeedCopy-->
```

为 **Winbind** 配置 **PAM** 运行以下命令，确保选中 **Winbind NT/Active Directory authentication** (Winbind NT/Active Directory 身份验证) 和 **Create home directory on login** (在登录时创建主目录) 选项：

```
1 sudo pam-auth-update
2 <!--NeedCopy-->
```

提示：

仅当计算机加入域后，winbind 守护程序才会始终保持运行。

验证域成员身份 Delivery Controller 要求所有 VDA 计算机（不论是 Windows 还是 Linux）都要在 Active Directory 中有一个计算机对象。

运行 Samba 的 `net ads` 命令验证计算机是否已加入域：

```
1 sudo net ads testjoin
2 <!--NeedCopy-->
```

运行以下命令验证额外的域和计算机对象信息：

```
1 sudo net ads info
2 <!--NeedCopy-->
```

验证 **Kerberos** 配置 要验证 Kerberos 是否已正确配置为可与 Linux VDA 配合使用，请检查系统 **keytab** 文件是否已创建并包含有效密钥：

```
1 sudo klist -ke
2 <!--NeedCopy-->
```

此命令显示各种主体名称与密码套件组合可用的密钥列表。运行 Kerberos `kinit` 命令，使用这些密钥向域控制器验证计算机的身份：

```
1 sudo kinit -k MACHINE$@REALM
2 <!--NeedCopy-->
```

计算机和领域名称必须指定为大写。美元符号 (\$) 必须使用反斜杠 (\) 进行转义，以免发生 shell 替换。在某些环境中，DNS 域名与 Kerberos 领域名称不同。请确保使用领域名称。如果此命令成功运行，则不会显示任何输出。

使用以下命令验证计算机帐户的 TGT 票据已缓存：

```
1 sudo klist
2 <!--NeedCopy-->
```

使用以下命令检查计算机的帐户详细信息：

```
1 sudo net ads status
2 <!--NeedCopy-->
```

验证用户身份验证 使用 **wbinfo** 工具验证是否可向域验证域用户的身份：

```
1 wbinfo --krb5auth=domain\username%password
2 <!--NeedCopy-->
```

这里指定的域为 AD 域名，而不是 Kerberos 领域名称。对于 bash shell，必须使用另一个反斜杠对反斜杠 (\) 字符进行转义。此命令返回一条成功或失败消息。

要验证 Winbind PAM 模块是否已正确配置，请使用域用户帐户登录 Linux VDA。该域用户帐户以前未曾使用过。

```
1 ssh localhost -l domain\username
2
3 id -u
4 <!--NeedCopy-->
```

检查是否为 **id -u** 命令返回的 uid 创建了对应的 Kerberos 凭据缓存文件：

```
1 ls /tmp/krb5cc_uid
2 <!--NeedCopy-->
```

检查用户 Kerberos 凭据缓存中的票据是否有效且未过期：

```
1 klist
2 <!--NeedCopy-->
```

退出会话。

```
1 exit
2 <!--NeedCopy-->
```

直接登录 GNOME 或 KDE 控制台也可以执行类似的测试。在进行域加入验证后继续执行 [步骤 4: 安装 Linux VDA](#)。

提示：

如果使用域帐户登录时成功执行用户身份验证，但无法显示您的桌面，请重新启动计算机并重试。

Quest Authentication Service

在域控制器上配置 **Quest** 假定您已在 Active Directory 域控制器上安装并配置了 Quest 软件，而且已获得管理权限，有权在 Active Directory 中创建计算机对象。

允许域用户登录 **Linux VDA** 计算机 为了让域用户能够在 Linux VDA 计算机上建立 HDX 会话：

1. 在 Active Directory 用户和计算机管理控制台中，为该用户帐户打开 Active Directory 用户属性。
2. 选择 **Unix Account** (Unix 帐户) 选项卡。
3. 选中 **Unix-enabled** (已启用 Unix)。
4. 将 **Primary GID Number** (首选 GID 编号) 设置为实际域用户组的组 ID。

注意：

这些说明相当于设置域用户，以便他们可以使用控制台、RDP、SSH 或任何其他远程协议进行登录。

在 **Linux VDA** 上配置 **Quest**

SELinux 策略强制实施解决方法 默认 RHEL 环境会强制实施 SELinux。此强制功能会影响 Quest 使用的 Unix 域套接字 IPC 机制，并阻止域用户登录。

解决此问题的最便捷的方法是禁用 SELinux。以 root 用户身份，编辑 `/etc/selinux/config` 并更改 **SELinux** 设置：

`SELINUX=disabled`

此更改要求重新启动计算机：

```
1 reboot
2 <!--NeedCopy-->
```

重要：

请谨慎使用此设置。禁用后重新启用 SELinux 策略强制实施会导致完全锁定，即便是对 root 用户和其他本地用户也是如此。

配置 VAS 守护程序 必须启用并断开自动续订 Kerberos 票据功能。必须禁用身份验证（脱机登录）功能：

```
1 sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
   interval 32400
2
3 sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
   auth false
4 <!--NeedCopy-->
```

此命令将续订间隔设为 9 小时（32400 秒），即比默认的 10 小时票据生命周期短 1 小时。请在票据生命周期较短的系统上设置较低的值。

配置 PAM 和 NSS 要启用通过 HDX 进行的域用户登录以及其他服务（例如 su、ssh 和 RDP），请运行以下命令以手动配置 PAM 和 NSS：

```
1 sudo /opt/quest/bin/vastool configure pam
2
3 sudo /opt/quest/bin/vastool configure nss
4 <!--NeedCopy-->
```

加入 **Windows** 域 使用 Quest `vastool` 命令将 Linux 计算机加入到 Active Directory 域中:

```
1 sudo /opt/quest/bin/vastool -u user join domain-name
2 <!--NeedCopy-->
```

`user` 为有权将计算机加入 Active Directory 域的域用户。`domain-name` 为域的 DNS 名称, 例如 `example.com`。

验证域成员身份 Delivery Controller 要求所有 VDA 计算机 (不论是 Windows 还是 Linux) 都要在 Active Directory 中有一个计算机对象。验证 Quest 加入的 Linux 计算机是否位于域中:

```
1 sudo /opt/quest/bin/vastool info domain
2 <!--NeedCopy-->
```

如果计算机已加入域, 此命令会返回域名。如果计算机未加入任何域, 则会显示以下错误:

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined
to domain
```

验证用户身份验证 要验证 Quest 是否可以通过 PAM 对域用户进行身份验证, 请使用域用户帐户登录 Linux VDA。该域用户帐户以前未曾使用过。

```
1 ssh localhost -l domain\username
2
3 id -u
4 <!--NeedCopy-->
```

检查是否为 `id -u` 命令返回的 UID 创建了对应的 Kerberos 凭据缓存文件:

```
1 ls /tmp/krb5cc_uid
2 <!--NeedCopy-->
```

检查 Kerberos 凭据缓存中的票据是否有效且未过期:

```
1 /opt/quest/bin/vastool klist
2 <!--NeedCopy-->
```

退出会话。

```
1 exit
2 <!--NeedCopy-->
```

在进行域加入验证后继续执行 [步骤 4: 安装 Linux VDA](#)。

Centrify DirectControl

加入 **Windows** 域 安装 Centrify DirectControl Agent 后，请使用 Centrify `adjoin` 命令将 Linux 计算机加入 Active Directory 域：

```
1 su -
2
3 adjoin -w -V -u user domain-name
4 <!--NeedCopy-->
```

user 参数为有权将计算机加入 Active Directory 域的任何 Active Directory 域用户。**domain-name** 参数是将 Linux 计算机加入到的域的名称。

验证域成员身份 Delivery Controller 要求所有 VDA 计算机（不论是 Windows 还是 Linux）都要在 Active Directory 中有一个计算机对象。验证 Centrify 加入的 Linux 计算机是否位于域中：

```
1 su -
2
3 adinfo
4 <!--NeedCopy-->
```

检查 **Joined to domain** 值是否有效以及 **CentrifyDC mode** 是否返回了 **connected**。如果模式仍然卡在启动状态，则表明 Centrify 客户端遇到了服务器连接或身份验证问题。

使用以下命令可获得更全面的系统和诊断信息：

```
1 adinfo --sysinfo all
2
3 adinfo --diag
4 <!--NeedCopy-->
```

测试与各种 Active Directory 和 Kerberos 服务的连接。

```
1 adinfo --test
2 <!--NeedCopy-->
```

在进行域加入验证后继续执行[步骤 4: 安装 Linux VDA](#)。

SSSD

配置 **Kerberos** 运行以下命令以安装 Kerberos：

```
1 sudo apt-get install krb5-user
2 <!--NeedCopy-->
```

要配置 Kerberos，请以 root 用户身份打开 `/etc/krb5.conf` 并配置以下设置：

```
1 [libdefaults]
```

```
2
3 default_realm = REALM
4
5 dns_lookup_kdc = false
6
7 [realms]
8
9 REALM = {
10
11     admin_server = domain-controller-fqdn
12
13     kdc = domain-controller-fqdn
14
15 }
16
17
18
19 [domain_realm]
20
21 domain-dns-name = REALM
22
23 .domain-dns-name = REALM
24 <!--NeedCopy-->
```

此上下文中的 `domain-dns-name` 属性为 DNS 域名，例如 `example.com`。REALM 是大写的 Kerberos 领域名称，例如 `EXAMPLE.COM`。

加入域 必须将 SSSD 配置为使用 Active Directory 作为其身份提供程序并且使用 Kerberos 进行身份验证。但是，SSSD 并不提供用于加入域和管理系统 keytab 文件的 AD 客户端功能。可以改为使用 `adcli`、`realmd` 或 `Samba`。

注意：

本部分内容仅提供 `adcli` 和 `Samba` 的信息。

使用 **adcli** 加入域：

安装 **adcli**：

安装所需的软件包：

```
1 sudo apt-get install adcli
2 <!--NeedCopy-->
```

通过 **adcli** 加入域：

使用以下命令删除旧系统 keytab 文件并加入域：

```
1 su -
2
3 rm -rf /etc/krb5.keytab
```

```
4
5 adcli join domain-dns-name -U user -H hostname-fqdn
6 <!--NeedCopy-->
```

user 是拥有将计算机添加到域的域用户。**hostname-fqdn** 是计算机的 FQDN 格式的主机名。

需要 **-H** 选项，adcli 才能生成格式为 host/hostname-fqdn@REALM 的 SPN (Linux VDA 要求使用此格式)。

验证系统 **keytab**：

Adcli 工具的功能有限，不提供测试计算机是否已加入域的方法。最佳备用方法为确保已创建系统 keytab 文件：

```
1 sudo klist -ket
2 <!--NeedCopy-->
```

验证每个键的时间戳是否与将计算机加入域的时间相匹配。

使用 **samba** 加入域：

安装软件包：

```
1 sudo apt-get install samba
2 <!--NeedCopy-->
```

配置 **samba**：

打开 `/etc/samba/smb.conf` 并配置以下设置：

```
1 [global]
2
3     workgroup = WORKGROUP
4
5     security = ADS
6
7     realm = REALM
8
9     client signing = yes
10
11     client use spnego = yes
12
13     kerberos method = secrets and keytab
14 <!--NeedCopy-->
```

WORKGROUP 是 **REALM** 中的第一个字段，**REALM** 是大写的 Kerberos 领域名称。

使用 **samba** 加入域：

您的域控制器必须可访问，而且您必须具有有权将计算机添加到域的 Windows 帐户。

```
1 sudo net ads join REALM -U user
2 <!--NeedCopy-->
```

其中，**REALM** 是大写的 Kerberos 领域名称，**user** 是拥有将计算机添加到域的域用户。

设置 **SSSD** 安装或更新所需软件包:

如果尚未安装, 请安装所需的 SSSD 和配置软件包:

```
1 sudo apt-get install sssd
2 <!--NeedCopy-->
```

如果已安装软件包, 则建议进行更新:

```
1 sudo apt-get update sssd
2 <!--NeedCopy-->
```

注意:

默认情况下, Ubuntu 中的安装过程将自动配置 **nsswitch.conf** 和 PAM 登录模块。

配置 **SSSD** 启动 SSSD 守护程序之前, 需要更改 SSSD 配置。对于某些版本的 SSSD, 默认不安装 **/etc/sss-d/sss.conf** 配置文件, 必须手动创建。以 root 用户身份创建或打开 **/etc/sss-d/sss.conf** 并配置以下设置:

```
1 [sss-d]
2
3 services = nss, pam
4
5 config_file_version = 2
6
7 domains = domain-dns-name
8
9 [domain/domain-dns-name]
10
11 id_provider = ad
12
13 access_provider = ad
14
15 auth_provider = krb5
16
17 krb5_realm = REALM
18
19 # Set krb5_renewable_lifetime higher if TGT renew lifetime is longer
20   than 14 days
21 krb5_renewable_lifetime = 14d
22
23 # Set krb5_renew_interval to lower value if TGT ticket lifetime is
24   shorter than 2 hours
25 krb5_renew_interval = 1h
26
27 krb5_ccachedir = /tmp
28
29 krb5_ccname_template = FILE:%d/krb5cc_%U
30
31 # This ldap_id_mapping setting is also the default value
```

```
32
33 ldap_id_mapping = true
34
35 override_homedir = /home/%d/%u
36
37 default_shell = /bin/bash
38
39 ad_gpo_map_remote_interactive = +ctxhdx
40 <!--NeedCopy-->
```

注意：

ldap_id_mapping 设置为 **true**，以便 SSSD 本身负责将 Windows SID 映射到 Unix UID。否则，Active Directory 必须能够提供 POSIX 扩展程序。PAM 服务 `ctxhdx` 已添加到 `ad_gpo_map_remote_interactive`。

此上下文中的 **domain-dns-name** 属性为 DNS 域名，例如 `example.com`。**REALM** 是大写的 Kerberos 领域名称，例如 `EXAMPLE.COM`。不需要配置 NetBIOS 域名。

提示：

有关这些配置设置的信息，请参阅 `sssd.conf` 和 `sssd-ad` 的手册页。

SSSD 守护程序要求配置文件必须仅具有所有者读取权限：

```
1 sudo chmod 0600 /etc/sssd/sssd.conf
2 <!--NeedCopy-->
```

启动 **SSSD** 守护程序 运行以下命令立即启动 SSSD 守护程序，以及使守护程序在计算机启动时启动：

```
1 sudo systemctl start sssd
2
3 sudo systemctl enable sssd
4 <!--NeedCopy-->
```

PAM 配置 运行以下命令，确保选中 **SSS authentication**（SSS 身份验证）和 **Create home directory on login**（在登录时创建主目录）选项：

```
1 sudo pam-auth-update
2 <!--NeedCopy-->
```

验证域成员身份 Delivery Controller 要求所有 VDA 计算机（Windows 和 Linux）都要在 Active Directory 中有一个计算机对象。

使用 **adcli** 验证域成员关系：

通过运行以下命令显示域信息：

```
1 sudo adcli info domain-dns-name
2 <!--NeedCopy-->
```

使用 **samba** 验证域成员关系：

运行 Samba 的 `net ads` 命令验证计算机是否已加入域：

```
1 sudo net ads testjoin
2 <!--NeedCopy-->
```

运行以下命令验证额外的域和计算机对象信息：

```
1 sudo net ads info
2 <!--NeedCopy-->
```

验证 Kerberos 配置 要验证 Kerberos 是否已正确配置为可与 Linux VDA 配合使用，请检查系统 `keytab` 文件是否已创建并包含有效密钥：

```
1 sudo klist -ke
2 <!--NeedCopy-->
```

此命令显示各种主体名称与密码套件组合可用的密钥列表。运行 Kerberos `kinit` 命令，使用这些密钥向域控制器验证计算机的身份：

```
1 sudo kinit -k MACHINE$@REALM
2 <!--NeedCopy-->
```

计算机和领域名称必须指定为大写。美元符号 (\$) 必须使用反斜杠 (\) 进行转义，以免发生 shell 替换。在某些环境中，DNS 域名与 Kerberos 领域名称不同。请确保使用领域名称。如果此命令成功运行，则不会显示任何输出。

使用以下命令检查计算机帐户的 TGT 票据是否已缓存：

```
1 sudo klist
2 <!--NeedCopy-->
```

验证用户身份验证 SSSD 不直接通过守护程序提供用于测试身份验证的命令行工具，只能通过 PAM 完成。

要验证 SSSD PAM 模块是否已正确配置，请使用域用户帐户登录 Linux VDA。该域用户帐户以前未曾使用过。

```
1 ssh localhost -l domain\username
2
3 id -u
4
5 klist
6
7 exit
8 <!--NeedCopy-->
```

检查 **klist** 命令返回的 Kerberos 票据是否适用于该用户并且尚未过期。

以 root 用户身份，检查是否已为前面的 **id -u** 命令返回的 uid 创建相应的票据缓存文件：

```
1 ls /tmp/krb5cc_uid
2 <!--NeedCopy-->
```

可以通过登录 KDE 或 Gnome Display Manager 执行类似的测试。在进行域加入验证后继续执行 [步骤 4: 安装 Linux VDA](#)。

步骤 4: 安装 Linux VDA

步骤 4a: 下载 Linux VDA 软件包

转至 Citrix Web 站点并根据您的 Linux 发行版下载相应的 Linux VDA 软件包。

步骤 4b: 安装 Linux VDA

使用 Debian 软件包管理器安装 Linux VDA 软件：

```
1 sudo dpkg -i xendesktopvda_7.15.0.404-1.ubuntu16.04_amd64.deb
2 <!--NeedCopy-->
```

Ubuntu 的 Debian 依赖项列表：

```
1 postgresql >= 9.5
2
3 libpostgresql-jdbc-java >= 9.2
4
5 default-jdk >= 2:1.8
6
7 imagemagick >= 8:6.8.9.9
8
9 ufw >= 0.35
10
11 ubuntu-desktop >= 1.361
12
13 libxrandr2 >= 2:1.5.0
14
15 libxtst6 >= 2:1.2.2
16
17 libxm4 >= 2.3.4
18
19 util-linux >= 2.27.1
20
21 bash >= 4.3
22
23 findutils >= 4.6.0
24
```

```

25 sed >= 4.2.2
26
27 cups >= 2.1
28
29 libldap-2.4-2 >= 2.4.42
30
31 libsasl2-modules-gssapi-mit >= 2.1.~
32
33 python-requests >= 2.9.1
34
35 libgoogle-perftools4 >= 2.4~
36 <!--NeedCopy-->

```

步骤 4c: 配置 Linux VDA

安装软件包后，必须运行 `ctxsetup.sh` 脚本来配置 Linux VDA。执行任何更改之前，该脚本都会验证环境，确保所有依赖项都已安装。如有必要，可以随时重新运行该脚本以更改设置。

可以按照提示手动运行脚本，也可以采用预先配置响应自动运行脚本。继续操作前，请查看该脚本的帮助信息：

```

1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh - help
2 <!--NeedCopy-->

```

提示配置 运行会提示各种问题的手动配置：

```

1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
2 <!--NeedCopy-->

```

自动配置 自动安装时，设置脚本所需的选项可由环境变量提供。如果所需的所有变量都存在，则脚本不会提示用户提供任何信息，从而允许通过脚本完成安装过程。

支持的环境变量包括：

- **CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N** - Linux VDA 支持使用 DNS CNAME 记录指定 Delivery Controller 名称。默认情况下设置为 N。
- **CTX_XDL_DDC_LIST = list-ddc-fqdns** - Linux VDA 要求提供由空格分隔的 Delivery Controller 完全限定域名 (FQDN) 列表以用于向 Delivery Controller 注册。必须至少指定一个 FQDN 或 CNAME 别名。
- **CTX_XDL_VDA_PORT = port-number** - Linux VDA 通过 TCP/IP 端口（默认为端口 80）与 Delivery Controller 通信。
- **CTX_XDL_REGISTER_SERVICE = Y | N** - 在启动计算机后启动 Linux Virtual Desktop 服务。默认情况下设置为 Y。
- **CTX_XDL_ADD_FIREWALL_RULES = Y | N** - Linux Virtual Desktop 服务要求允许传入网络连接通过系统防火墙。您可以在系统防火墙中自动为 Linux Virtual Desktop 打开所需端口（默认为端口 80 和 1494）。默认情况下设置为 Y。

- **CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 | 4** - Linux VDA 要求使用 Kerberos 配置设置向 Delivery Controller 进行身份验证。Kerberos 配置根据系统上已安装和已配置的 Active Directory 集成工具确定。指定要使用且受支持的 Active Directory 集成方法：
 - 1 - Samba Winbind
 - 2 - Quest Authentication Service
 - 3 - Centrify DirectControl
 - 4 - SSSD
- **CTX_XDL_HDX_3D_PRO = Y | N** - Linux VDA 支持 HDX 3D Pro，这是一组 GPU 加速技术，旨在优化富图形应用程序的虚拟化水平。如果选择了 HDX 3D Pro，则要为 VDI 桌面（单会话）模式配置 Virtual Delivery Agent -（即 CTX_XDL_VDI_MODE=Y）。
- **CTX_XDL_VDI_MODE = Y | N** - 将计算机配置为专用桌面交付模型 (VDI) 还是托管共享桌面交付模型。对于 HDX 3D Pro 环境，将此变量设置为 Y。默认情况下，此变量设置为 N。
- **CTX_XDL_SITE_NAME = dns-name** - Linux VDA 通过 DNS 发现 LDAP 服务器。要将 DNS 搜索结果限制为本地站点，应指定 DNS 站点名称。默认情况下，此变量设置为 **<none>**。
- **CTX_XDL_LDAP_LIST = list-ldap-servers** - Linux VDA 查询 DNS 来发现 LDAP 服务器。如果 DNS 无法提供 LDAP 服务记录，您可以提供以空格分隔的 LDAP FQDN（带有 LDAP 端口）列表。例如 ad1.mycompany.com:389。默认情况下，此变量设置为 **<none>**。
- **CTX_XDL_SEARCH_BASE = search-base-set** - Linux VDA 通过设置为 Active Directory 域根的搜索库来查询 LDAP（例如，DC=mycompany,DC=com）。但是，为提高搜索效能，可以指定搜索基础（例如 OU=VDI,DC=mycompany,DC=com）。默认情况下，此变量设置为 **<none>**。
- **CTX_XDL_START_SERVICE = Y | N** - 在完成 Linux VDA 配置后，是否启动 Linux VDA 服务。默认情况下设置为 Y。

设置环境变量并运行配置脚本：

```

1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
2
3 export CTX_XDL_DDC_LIST=list-ddc-fqdns
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-name
18
19 export CTX_XDL_LDAP_LIST=list-ldap-servers
20
```

```
21 export CTX_XDL_SEARCH_BASE=search-base-set
22
23 export CTX_XDL_START_SERVICE=Y|N
24
25 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
26 <!--NeedCopy-->
```

运行 `sudo` 命令时，键入 **-E** 选项以将现有环境变量传递给它创建的新 shell。Citrix 建议使用前面的命令并加上 **#!/bin/bash** 作为第一行来创建 shell 脚本文件。

或者，您可以使用单个命令指定所有参数：

```
1 sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3 CTX_XDL_DDC_LIST=list-ddc-fqdns \
4
5 CTX_XDL_VDA_PORT=port-number \
6
7 CTX_XDL_REGISTER_SERVICE=Y|N \
8
9 CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST=list-ldap-servers \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_START_SERVICE=Y|N \
24
25 /opt/Citrix/VDA/sbin/ctxsetup.sh
26 <!--NeedCopy-->
```

删除配置更改 在某些情形下，您可能需要删除 **ctxsetup.sh** 脚本对配置所做的更改，但不卸载 Linux VDA 软件包。

继续操作前，请查看此脚本的帮助信息：

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
2 <!--NeedCopy-->
```

删除配置更改：

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
2 <!--NeedCopy-->
```

重要:

此脚本会从数据库删除所有配置数据，从而使 Linux VDA 无法使用。

配置日志 **ctxsetup.sh** 和 **ctxcleanup.sh** 脚本会在控制台上显示错误，并将其他信息写入配置日志文件 **/tmp/xdl.config.log**:

重新启动 Linux VDA 服务，确保更改生效。

卸载 **Linux VDA** 软件 要检查 Linux VDA 是否已安装并查看已安装软件包的版本，请运行以下命令：

```
1 dpkg -l xendesktopvda
2 <!--NeedCopy-->
```

查看更多详细信息：

```
1 apt-cache show xendesktopvda
2 <!--NeedCopy-->
```

要卸载 Linux VDA 软件，请执行以下操作：

```
1 dpkg -r xendesktopvda
2 <!--NeedCopy-->
```

注意:

卸载 Linux VDA 软件会删除关联的 PostgreSQL 和其他配置数据。但是，不会删除在安装 Linux VDA 之前设置的 PostgreSQL 软件包和其他依赖软件包。

提示:

本节中的信息未介绍包括 PostgreSQL 在内的依赖软件包的删除操作。

步骤 5：运行 **Linux VDA**

使用 **ctxsetup.sh** 脚本配置 Linux VDA 后，请使用以下命令控制 Linux VDA。

启动 Linux VDA:

启动 Linux VDA 服务：

```
1 sudo systemctl start ctxhdx
2
3 sudo systemctl start ctxvda
4 <!--NeedCopy-->
```

停止 Linux VDA:

停止 Linux VDA 服务：

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl stop ctxhdx
4 <!--NeedCopy-->
```

重新启动 Linux VDA:

重新启动 Linux VDA 服务:

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl restart ctxhdx
4
5 sudo systemctl restart ctxvda
6 <!--NeedCopy-->
```

检查 Linux VDA 状态:

要检查 Linux VDA 服务的运行状态, 请执行以下操作:

```
1 sudo systemctl status ctxvda
2
3 sudo systemctl status ctxhdx
4 <!--NeedCopy-->
```

步骤 6: 在 XenApp 或 XenDesktop 中创建计算机目录

创建计算机目录和添加 Linux VDA 计算机的过程与传统的 Windows VDA 方法类似。有关如何完成这些任务的更加详细的说明, 请参阅[创建计算机目录](#)和[管理计算机目录](#)。

创建包含 Linux VDA 计算机的计算机目录时会面临一些限制, 使得该过程不同于为 Windows VDA 计算机创建计算机目录:

- 对于操作系统, 请选择:
 - “服务器操作系统” 选项 (对于托管共享桌面交付模型)。
 - “桌面操作系统” 选项 (对于 VDI 专用桌面交付模型)。
- 确保计算机未执行电源管理设置。
- 由于 Linux VDA 不支持 MCS, 请选择 [PVS](#) 或其他服务或技术 (现有映像) 部署方法。
- 请勿在同一个计算机目录中混合使用 Linux 和 Windows VDA 计算机。

注意:

早期版本的 Citrix Studio 不支持 “Linux 操作系统” 的概念。但是, 选择 Windows Server 操作系统或服务器操作系统选项等同于使用托管共享桌面交付模型。选择 Windows 桌面操作系统或桌面操作系统选项等同于使用每计算机一个用户交付模型。

提示:

如果删除计算机后将其重新加入 Active Directory 域，则必须删除计算机，然后将其重新添加到计算机目录。

步骤 7: 在 **XenApp** 或 **XenDesktop** 中创建交付组

创建交付组和添加包含 Linux VDA 计算机的计算机目录的过程与 Windows VDA 计算机几乎相同。有关如何完成这些任务的更加详细的说明，请参阅[创建交付组](#)。

创建含有 Linux VDA 计算机目录的交付组时会面临以下限制：

- 对于交付类型，请选择桌面。适用于 Ubuntu 的 Linux VDA 不支持应用程序交付。
- 确保所选的 AD 用户和组已正确配置，可以登录到 Linux VDA 计算机。
- 请勿允许未经身份验证的（匿名）用户登录。
- 请勿在交付组中混入含有 Windows 计算机的计算机目录。

配置 **Linux VDA**

November 21, 2020

本部风内容详细介绍了 Linux VDA 的功能，包括功能说明、配置和故障排除。

将 **NIS** 与 **Active Directory** 集成

November 30, 2022

本文介绍如何在 Linux VDA 中使用 SSSD 将 NIS 与 Windows Active Directory (AD) 集成。Linux VDA 被视为 Citrix XenApp & XenDesktop 的一个组件。因此，它与 Windows AD 环境紧密结合。

使用 NIS（而非 AD）作为 UID 和 GID 提供程序要求帐户信息（用户名和密码组合）在 AD 和 NIS 中相同。

注意：

仍由 AD 服务器执行身份验证。不支持 NIS+。如果使用 NIS 作为 UID 和 GID 提供程序，则不再使用来自 Windows 服务器的 POSIX 属性。

提示：

此方法代表已弃用的 Linux VDA 部署方法，这种方法仅用于特殊用例。对于 RHEL/CentOS 发行版，请按照[安装 Linux Virtual Delivery Agent for RHEL/CentOS](#) 中的说明进行操作。对于 Ubuntu 发行版，请按照[安装 Linux Virtual Delivery Agent for Ubuntu](#) 中的说明进行操作。

SSSD:

SSSD 是系统守护程序。其主要功能是为了实现通过可以为系统提供缓存和脱机支持的通用框架来识别远程资源并对其进行身份验证。它提供 PAM 和 NSS 两种模块，将来可以为扩展用户信息支持基于 D-BUS 的接口。此外它还提供更好的数据库来存储本地用户帐户和扩展用户数据。

必备软件

AD 提供程序最初是在 SSSD 版本 1.9.0 中引入的。

已按照本文中的说明测试和验证了以下环境。

- RHEL 7.3 或更高版本/CentOS 7.3 或更高版本
- Linux VDA 1.3 版或更高版本

将 NIS 与 AD 相集成

要将 NIS 与 AD 集成，请执行以下操作：

1. 将 [Linux VDA](#) 添加为 NIS 客户端
2. 使用 [Samba](#) 加入域并创建主机 keytab
3. [设置 SSSD](#)
4. [配置 NSS/PAM](#)
5. [验证 Kerberos 配置](#)
6. [验证用户身份验证](#)

将 Linux VDA 添加为 NIS 客户端

配置 NIS 客户端：

```
1 yum -y install ypbind rpcbind oddjob-mkhomedir
2 <!--NeedCopy-->
```

设置 NIS 域：

```
1 ypdomainname nis.domain
2 echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
3 <!--NeedCopy-->
```

在 `/etc/hosts` 中添加 NIS 服务器和客户端的 IP 地址：

```
{ NIS server IP address } server.nis.domain nis.domain
```

通过 `authconfig` 配置 NIS：

```
1 sudo authconfig --enablenis --nisdomain=nis.domain --nisserver=server.nis.domain --enablemkhomedir --update
2 <!--NeedCopy-->
```

nis.domain 表示 NIS 服务器的域名。**server.nis.domain** 是 NIS 服务器的主机名，也可以是 NIS 服务器的 IP 地址。

配置 NIS 服务：

```
1 sudo systemctl start rpcbind ypbind
2
3 sudo systemctl enable rpcbind ypbind
4 <!--NeedCopy-->
```

确保 NIS 配置正确：

```
1 ypwhich
2 <!--NeedCopy-->
```

验证可从 NIS 服务器获得帐户信息：

```
1 getent passwd nisaccount
2 <!--NeedCopy-->
```

注意：

nisaccount 表示 NIS 服务器上的实际 NIS 帐户。确保 UID、GID、主目录和登录 shell 都已正确配置。

使用 **Samba** 加入域并创建主机 **keytab**

SSSD 并不提供用于加入域和管理系统 keytab 文件的 AD 客户端功能。实现这些功能可以采用几种方法，包括：

- adcli
- realmd
- Winbind
- Samba

本节信息只介绍 Samba 方法。对于 **realmd**，请参阅 RHEL 或 CentOS 供应商的文档。必须在配置 SSSD 之前执行这些步骤。

使用 **Samba** 加入域并创建主机 **keytab**：

在正确配置了以下文件的 Linux 客户端上：

- /etc/krb5.conf
- /etc/samba/smb.conf:

为计算机配置 Samba 和 Kerberos 身份验证：

```
1 sudo authconfig --smbsecurity=ads --smbworkgroup=domain --smbrealm=
   REALM --krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --update
2 <!--NeedCopy-->
```

其中，**REALM** 是大写的 Kerberos 领域名称，而 **domain** 是域的 NetBIOS 名称。

如果需要通过 DNS 查找 KDC 服务器和领域名称，请将以下两个选项添加至前面的命令：

```
--enablekrb5kdcdns --enablekrb5realmdns
```

打开 **/etc/samba/smb.conf** 并将以下条目添加到 **[Global]** 部分下方，但要放在 **authconfig** 工具生成的部分后面：

```
kerberos method = secrets and keytab
```

加入 Windows 域要求您的域控制器可访问，而且您具有有权将计算机添加到域的 AD 用户帐户。

```
1 sudo net ads join REALM -U user
2 <!--NeedCopy-->
```

REALM 是大写的 Kerberos 领域名称，**user** 是有权将计算机添加到域的域用户。

设置 SSSD

设置 SSSD 的步骤如下：

- 在 Linux 客户端计算机上安装 **sssd-ad** 和 **sssd-proxy** 软件包。
- 对各种文件（例如 **sssd.conf**）进行配置更改。
- 启动 **sssd** 服务。

/etc/sss/sss.conf **sss.conf** 配置示例（可以根据需要添加更多选项）：

```
1 [sss]
2 config_file_version = 2
3 domains = example
4 services = nss, pam
5
6 [domain/example]
7 # Uncomment if you need offline logins
8 # cache_credentials = true
9 re_expression = (((?P<domain>[^\]+)\((?P<name>.+))\)|((?P<name>[^\]+)@
   (?P<domain>.+))\|^((?P<name>[^\]+)$))
10 id_provider = proxy
11 proxy_lib_name = nis
12 auth_provider = ad
13 access_provider = ad
14
15 # Should be specified as the lower-case version of the long version of
   the Active Directory domain.
```

```

16 ad_domain = ad.example.com
17
18 # Kerberos settings
19 krb5_ccachedir = /tmp
20 krb5_ccname_template = FILE:%d/krb5cc_%U
21
22 # Uncomment if service discovery is not working
23 # ad_server = server.ad.example.com
24
25 # Comment out if the users have the shell and home dir set on the AD
    side
26 default_shell = /bin/bash
27 fallback_homedir = /home/%d/%u
28
29 # Uncomment and adjust if the default principal SHORTNAME$@REALM is not
    available
30 # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
31 <!--NeedCopy-->

```

将 **ad.domain.com**、**server.ad.example.com** 替换为相应的值。有关详细信息，请参阅 [sssd-ad\(5\) - Linux 手册页](#)。

对 **sssd.conf** 设置文件所有权和权限：

```

chown root:root /etc/sssds/sssds.conf
chmod 0600 /etc/sssds/sssds.conf
restorecon /etc/sssds/sssds.conf

```

配置 NSS/PAM

RHEL/CentOS:

使用 **authconfig** 启用 SSSD。安装 **oddjob mkhomedir** 以确保主目录创建与 SELinux 兼容：

```

1 authconfig --enablesssd --enablesssdauth --enablemkhomedir --update
2
3 sudo systemctl start sssd
4
5 sudo systemctl enable sssd
6 <!--NeedCopy-->

```

提示：

配置 Linux VDA 设置时，要为 SSSD 考虑上述操作，而对 Linux VDA 客户端无需特殊设置。对于 **ctxsetup.sh** 脚本中的其他解决方案，请使用默认值。

验证 Kerberos 配置

为了确保 Kerberos 已正确配置为可与 Linux VDA 配合使用，请检查系统 **keytab** 文件是否已创建并包含有效密钥：

```
1 sudo klist -ke
2 <!--NeedCopy-->
```

此命令显示各种主体名称与密码套件组合可用的密钥列表。运行 Kerberos **kinit** 命令，以使用这些密钥向域控制器验证计算机的身份：

```
1 sudo kinit -k MACHINE$@REALM
2 <!--NeedCopy-->
```

计算机和领域名称必须指定为大写。美元符号 (\$) 必须使用反斜杠 (\) 进行转义，以免发生 shell 替换。在某些环境中，DNS 域名与 Kerberos 领域名称不同。请确保使用领域名称。如果此命令成功运行，则不会显示任何输出。

使用以下命令验证计算机帐户的 TGT 票据已缓存：

```
1 sudo klist -ke
2 <!--NeedCopy-->
```

验证用户身份验证

使用 **getent** 命令确认支持的登录格式以及 NSS 是否工作：

```
1 sudo getent passwd DOMAIN\username
2 <!--NeedCopy-->
```

DOMAIN 参数指示简短形式的域名。如果需要使用另一种登录格式，请先使用 **getent** 命令进行验证。

支持的登录格式如下：

- 低级别登录名称：DOMAIN\username
- UPN: username@domain.com
- NetBIOS 前缀格式：username@DOMAIN

要验证 SSSD PAM 模块是否已正确配置，请使用域用户帐户登录 Linux VDA。该域用户帐户以前未曾使用过。

```
1 sudo localhost -l DOMAIN\username
2
3 id -u
4 <!--NeedCopy-->
```

检查是否为以下命令返回的 **uid** 创建了对应的 Kerberos 凭据缓存文件：

```
1 ls /tmp/krb5cc_{
2   uid }
3
```

```
4 <!--NeedCopy-->
```

检查用户 Kerberos 凭据缓存中的票据是否有效且未过期：

```
1 klist
2 <!--NeedCopy-->
```

发布应用程序

July 7, 2022

借助 Linux VDA 7.13 版，Citrix 向所有受支持的 Linux 平台中添加了无缝应用程序功能。不需要执行任何特定安装过程即可使用此功能。

提示：

在 Linux VDA 1.4 中，Citrix 增加了对已发布的非无缝应用程序和会话共享功能的支持。

使用 **Citrix Studio** 发布应用程序

您可以在创建交付组或将应用程序添加到现有交付组时发布 Linux VDA 上安装的应用程序。该过程与发布 Windows VDA 上安装的应用程序类似。有关详细信息，请参阅 [Citrix Virtual Apps and Desktops 文档](#)（根据使用的 Citrix Virtual Apps and Desktops 版本）。

提示：

配置交付组时，请确保交付类型设置为桌面和应用程序或应用程序。

重要：

Linux VDA 1.4 及更高版本支持发布应用程序。但是，Linux VDA 不支持将桌面和应用程序交付给相同的计算机。要解决此问题，Citrix 建议您为应用程序和桌面交付创建单独的交付组。

注意：

要使用无缝应用程序，请勿在 StoreFront 上禁用无缝模式。无缝模式默认处于启用状态。如果您已通过设置 TWIMode=Off 禁用该模式，请删除此设置，而非将其更改为 TWIMode=On。否则可能无法启动已发布的桌面。

故障排除

您可能会遇到启动已发布的应用程序所需的时间超过两分钟，并且在无缝模式下窗口无法显示的情况。如果出现该问题，请确认是否在 Linux VDA 和 StoreFront 上启用了无缝模式。

检查是否在 Linux VDA 上启用了无缝模式的命令：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg list -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix" | grep "SeamlessEnabled"
2 <!--NeedCopy-->
```

如果它显示 “SeamlessEnabled = 0x00000000”，则无缝模式处于禁用状态。要启用它，请运行以下命令：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix" -v "SeamlessEnabled" -d "0
   x00000001"
2 <!--NeedCopy-->
```

已知问题

在发布应用程序期间发现了以下已知问题：

- 当无缝模式在 StoreFront 上处于禁用状态，但在 Linux VDA 上仍处于启用状态时，已发布的非无缝应用程序将无法启动。同时在 Linux VDA 和 StoreFront 上启用/禁用无缝模式。
- 不支持非长方形窗口。窗口的边角可能会显示服务器端背景。
- 不支持从已发布的应用程序预览窗口的内容。
- 目前，无缝模式支持以下窗口管理器：Mutter (CentOS7.3\RHEL7.3\SUSE12.2)、Metacity (CentOS6.6\RHEL6.6\SUSE 11.4) 和 Compiz (Ubuntu 16.04)。Kwin 和其他窗口管理器不受支持。请确保您的窗口管理器属于受支持的窗口管理器。
- 运行多个 LibreOffice 应用程序时，只有第一个启动的应用程序显示在 Citrix Studio 上，因为这些应用程序共享进程。
- “Dolphin” 之类的基于 Qt5 的已发布应用程序可能不显示图标。要解决此问题，请参阅网址为 <https://wiki.archlinux.org/index.php/Qt> 的文章。
- 同一 ICA 会话中运行的已发布应用程序的所有任务栏按钮都组合在同一个组中。要解决此问题，请将任务栏属性设置为不组合任务栏按钮。

打印

November 8, 2021

本文提供有关打印最佳实践的信息。

安装

Linux VDA 要求同时启用 **cups** 和 **foomatic** 过滤器。请根据您的 Linux 发行版运行以下命令：

RHEL 7 打印支持：

```
1 sudo yum -y install cups
2
3 sudo yum -y install foomatic-filters
4 <!--NeedCopy-->
```

RHEL 6 打印支持:

```
1 sudo yum -y install cups
2
3 sudo yum -y install foomatic
4 <!--NeedCopy-->
```

使用情况

可以从已发布的桌面和已发布的应用程序打印。仅客户端默认打印机会映射到 Linux VDA 会话。对于桌面和应用程序，打印机名称必须不同。请注意以下事项：

- 对于发布的桌面：
`CitrixUniversalPrinter:$CLIENT_NAME:dsk$SESSION_ID`
- 对于发布的应用程序：
`CitrixUniversalPrinter:$CLIENT_NAME:app$SESSION_ID`

注意：

如果同一用户同时打开了已发布的桌面和已发布的应用程序，会话可以访问两种打印机。无法在已发布的应用程序会话中打印至桌面打印机，也无法在已发布的桌面会话中打印至应用程序打印机。

故障排除

无法打印

打印不正常时要检查若干项目。打印守护程序是一个按会话进程，必须在会话期间内运行。确认打印守护程序是否正在运行。

```
1 ps -ef | grep ctxlpmngt
2 <!--NeedCopy-->
```

如果 **ctxlpmngt** 进程未运行，请从命令行手动启动 **ctxlpmngt**。如果仍无法打印，请检查 CUPS 框架。**ctxcups** 服务用于打印机管理，并与 Linux CUPS 框架通信。此进程在每个计算机上有一个，可通过以下方式检查：

```
1 service ctxcups status
2 <!--NeedCopy-->
```

打印 **CUPS** 时的额外日志

用于获取打印组件（作为 Linux VDA 的组件之一）的日志的方法与用于其他组件的方法类似。

对于 RHEL，必须执行一些额外步骤以配置 CUPS 服务文件。否则，无法在 **hdx.lo** 中记录某些日志：

```
1 sudo service cups stop
2
3 sudo vi /etc/systemd/system/printer.target.wants/cups.service
4
5 PrivateTmp=false
6
7 sudo service cups start
8
9 sudo systemctl daemon-reload
10 <!--NeedCopy-->
```

注意：

此配置仅用于在出现问题时收集完整的打印日志。一般情况下不建议做此配置，因为这会损害 CUPS 安全性。

打印输出为乱码

打印机驱动程序不兼容可能会导致输出乱码。系统中为每个用户提供了驱动程序配置，该配置可通过编辑 **~/.CtulpProfile\$CLIENT_NAME** 配置文件进行配置。

```
1 [DEFAULT_PRINTER]
2
3 printername=
4
5 model=
6
7 ppdpath=
8
9 drivertype=
10 <!--NeedCopy-->
```

重要

:

printername 字段包含的是当前客户端默认打印机的名称。它是一个只读值。请勿编辑。

不能同时设置字段 **ppdpath**、**model** 和 **drivertype**，因为映射的打印机只能使用其中一个字段。

如果通用打印机驱动程序与客户端打印机不兼容，请使用 **model=** 选项配置本机打印机驱动程序的型号。可以使用 **lpinfo** 命令查找打印机的当前型号名称：

```
1 lpinfo - m
2
3 ...
```

```

4
5 xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
6
7 xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
8
9 xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
10 <!--NeedCopy-->

```

然后可以设置型号以与打印机匹配：

```

1 Model=xerox/ph3115.ppd.gz
2 <!--NeedCopy-->

```

如果通用打印机驱动程序与客户端打印机不兼容，请配置本机打印机驱动程序的 PPD 文件路径。**ppdpath** 值是本机打印机驱动程序文件的绝对路径。

例如，/home/tester/NATIVE_PRINTER_DRIVER.ppd 下存在一个 **ppd** 驱动程序：

```

1 ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
2 <!--NeedCopy-->

```

Citrix 提供了三种类型的通用打印机驱动程序（postscript、pcl5 和 pcl6）。如果没有本机打印机驱动程序，可以配置驱动程序类型。

例如，如果客户端默认打印机驱动程序类型为 PCL5：

```

1 drivertype=pcl5
2 <!--NeedCopy-->

```

输出大小为零

尝试使用其他类型的打印机。并尝试使用 CutePDF 和 PDFCreator 之类的虚拟打印机以确定此问题是否与打印机驱动程序有关。

打印作业取决于客户端默认打印机的打印机驱动程序。务必确定当前活动驱动程序类型。如果客户端打印机使用的是 PCL5 驱动程序，而 Linux VDA 选择的是 Postscript 驱动程序，则会出现问题。

如果打印机驱动程序类型正确，可以执行以下步骤来确定问题：

要确定问题，请执行以下操作：

1. 登录 ICA 会话桌面。
2. vi ~/.CtxlProfile\$CLIENT_NAME
3. 将以下字段添加到 Linux VDA 上的保存池文件：

```

1 deletespoolfile=no
2 <!--NeedCopy-->

```

4. 注销并重新登录以加载配置更改。

5. 打印文档以重现问题。打印后,将有一个 spool 文件保存在 `/var/spool/cups-ctx/$logon_user/$spool_file` 下。
6. 确认 spool 是否为空。如果 spool 文件大小为零,表示有问题。请联系 Citrix 支持(并提供打印日志)以获取更多指导。
7. 如果 spool 大小不为零,则将该文件复制到客户端。spool 文件内容取决于客户端默认打印机的打印机驱动程序类型。如果映射的打印机(本机)驱动程序是 postscript,可以直接在 Linux 操作系统上打开 spool 文件。确认该内容是否正确。

如果 spool 文件是 PCL,或者客户端操作系统是 Windows,则将 spool 文件复制到客户端,并使用客户端打印机打印该文件。完成该步骤后,使用其他打印机驱动程序对其进行测试。

8. 要将映射的打印机更改为其他第三方打印机驱动程序,请使用 postscript 客户端打印机,例如:
 - a) 登录活动会话,在客户端桌面上打开浏览器。
 - b) 打开打印管理门户:

```
1 localhost:631
2 <!--NeedCopy-->
```

- c) 选择映射的打印机 **CitrixUniversalPrinter:\$ClientName:app/dek\$SESSION_ID** 和 **Modify Printer** (修改打印机)。此操作要求使用管理员权限。
- d) 保持 cups-ctx 连接,然后单击“Continue”(继续)以更改打印机驱动程序。
- e) 在“Make and Model”(品牌和型号)页面,选择其他 postscript 驱动程序,而不是 Citrix UPD 驱动程序(例如,Citrix Universal Driver Postscript)。例如,如果安装了 CUPS-PDF 虚拟打印机,可以选择“Generic CUPS-PDF Printer”(通用 CUPS-PDF 打印机)。保存修改。
- f) 如果此过程成功,则会在 **.CtxlpProfile\$CLIENT_NAME** 中配置驱动程序的 PPD 文件路径,以允许映射的打印机使用此第三方驱动程序。

已知问题

下面是已确定的在 Linux VDA 上打印时存在的问题:

CTXPS 驱动程序与部分 PLC 打印机不兼容

如果发生打印输出损坏,请将打印机驱动程序设置为制造商提供的本机打印机驱动程序。

打印大文档时打印速度较慢

在本地客户端打印机上打印大文档时,文档会通过服务器连接进行传输。如果连接的速度很慢,传输可能需要很长时间。

在其他会话中看到打印机和打印作业通知

Linux 的会话概念与 Windows 操作系统不同。因此，所有用户都会获得系统范围的通知。您可以禁用这些通知，方法是更改 CUPS 配置文件：**`/etc/cups/cupsd.conf`**。

找到文件中配置的当前策略名称：

DefaultPolicy default

如果策略名称为 *default*，则将以下行添加到默认策略 XML 块中：

```
1 <Policy default>
2
3     # Job/subscription privacy...
4
5     JobPrivateAccess default
6
7     JobPrivateValues default
8
9     SubscriptionPrivateAccess default
10
11    SubscriptionPrivateValues default
12
13    ... ..
14
15    <Limit Create-Printer-Subscription>
16
17        Require user @OWNER
18
19        Order deny,allow
20
21    </Limit>
22
23    <Limit All>
24
25        Order deny,allow
26
27    </Limit>
28
29 </Policy>
30 <!--NeedCopy-->
```

PDF 打印

April 7, 2021

使用支持 PDF 打印的 Citrix Workspace 应用程序版本，可以打印从 Linux VDA 会话内部转换的 PDF。会话打印作业将被发送到安装了 Citrix Workspace 应用程序的本地计算机。在本地计算机上，可以使用所选 PDF 查看器打开 PDF，并在所选打印机上进行打印。

Linux VDA 支持在以下版本的 Citrix Workspace 应用程序上进行 PDF 打印：

- Citrix Receiver for HTML5 版本 2.4 到 2.6.9、适用于 HTML5 的 Citrix Workspace 应用程序 1808 及更高版本
- Citrix Receiver for Chrome 版本 2.4 到 2.6.9、适用于 Chrome 的 Citrix Workspace 应用程序 1808 及更高版本
- 适用于 Windows 的 Citrix Workspace 应用程序 1905 及更高版本

配置

除了使用支持 PDF 打印的 Citrix Workspace 应用程序版本外，还要在 Citrix Studio 中启用以下策略：

- 客户端打印机重定向（默认启用）
- 自动创建 **PDF** 通用打印机（默认禁用）

启用这些策略后，当您在已启动的会话中单击打印时，打印预览将显示在本地计算机上，以便您选择打印机。有关设置默认打印机的信息，请参阅 [Citrix Workspace 应用程序文档](#)。

配置图形

November 30, 2022

本文指导如何完成 Linux VDA 显卡配置和微调。

有关详细信息，请参阅[系统要求](#)和[安装概述](#)部分。

配置参数

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\Thinwire 下面有几个与图形相关的配置参数可以通过 **ctxreg** 实用程序进行调节。

如何启用 **Thinwire Plus**

对于标准 VDA 和 3D Pro，默认启用 Thinwire Plus。

如何启用 **H.264**

除了操作系统要求外，H.264 还对 Citrix Workspace 应用程序（以前称为 Citrix Receiver）版本有最低要求。如果客户端不满足要求，会转而使用 Thinwire Plus。

操作系统	H.264 最低要求
Windows	3.4 或更高版本
Mac OS X	11.8 或更高版本
Linux	13.0 或更高版本
Android	3.5
iOS	5.9
Chrome OS	1.4

Citrix Workspace 应用程序的最新功能列表可在 <https://docs.citrix.com/zh-cn/citrix-workspace-app/citrix-workspace-app-feature-matrix.html> 上找到。

可以运行以下命令在 VDA 上播发 H.264 编码：

```
1 sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "AdvertiseH264" -d "0x00000001" --force
2 <!--NeedCopy-->
```

如何在 **HDX 3D Pro** 中启用硬件编码

对于 HDX 3D Pro, **AdvertiseH264** 设置只能启用软件 H.264 编码。

运行以下命令可启用硬件编码：

```
1 sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "HardwareEncoding" -d "0x00000001" --force
2 <!--NeedCopy-->
```

注意：

如果您收到“ctxreg command can't be found”错误，请使用带完整路径的 ctxreg 命令。例如，请使用 `sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "AdvertiseH264" -d "0x00000001" -force` 而非 `sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "AdvertiseH264" -d "0x00000001" -force`。

如何为较低带宽调节 **Thinwire Plus**

- MaxColorDepth

```
1 Default 0x20, type DWORD
2 <!--NeedCopy-->
```

此选项指定通过 Thinwire 协议传输到客户端的图形的颜色深度。

为了节省带宽，将其设置为 0x10（表示适用于简单图形的首选颜色深度）或 0x8（实验低带宽模式）。

- 质量

视觉质量

```
1 Default: 0x1(medium), type: DWORD, valid values: 0x0(low), 0x1(
  medium), 0x2(high), 0x3(build to lossless), 0x4 always
  lossless.
2 <!--NeedCopy-->
```

为了节省带宽，将“质量”设置为 0x0(low)。

- 更多参数

- TargetFPS

目标帧速率

```
1 Default: 0x1e (30), Type: DWORD
2 <!--NeedCopy-->
```

- MinFPS

目标最低帧速率

```
1 Default: 0xa (10), Type: DWORD
2 <!--NeedCopy-->
```

- MaxScreenNum

客户端可以具有的最大监视器数

```
1 Default: 0x2, Type: DWORD
2 <!--NeedCopy-->
```

对于标准 VDA，可以将最大值设置为 10。对于 3D Pro，允许的最大值是 4。

故障排除

检查正在使用哪种编码

运行以下命令可检查是否正在使用 H.264 编码（**1** 表示 H.264；**0** 表示 TW+）：

```
1 sudo ctxreg dump | grep H264
2 <!--NeedCopy-->
```

结果类似于：

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000001"--force

create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-t "
REG_DWORD"-v "AdvertiseH264"-d "0x00000001"--force
```

检查是否在为 **3D Pro** 使用硬件编码

运行以下命令（**0** 表示未使用；**1** 表示正在使用）：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
2 <!--NeedCopy-->
```

结果类似于：

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000001"--force
```

另一个方法是使用 **nvidia-smi** 命令。如果正在使用硬件编码，输出将类似于以下内容：

```
1 Tue Apr 12 10:42:03 2016
2 +-----+
3 | NVIDIA-SMI 361.28      Driver Version: 361.28      |
4 |-----+-----+-----+-----+
5 | GPU   Name           Persistence-M| Bus-Id        Disp.A | Volatile
6 | Fan  Temp  Perf    Pwr:Usage/Cap|      Memory-Usage | GPU-Util
7 |-----+-----+-----+-----+
8 |    0  GRID K1              Off   | 0000:00:05.0   Off   |
9 | N/A   42C    P0      14W / 31W   | 207MiB / 4095MiB |      8%
10 |-----+-----+-----+-----+
11
12 +-----+
13 | Processes:                                             GPU
14 | GPU           PID    Type   Process name
15 |-----+-----+-----+-----+
16 |    0           2164  C+G   /usr/local/bin/ctxgfx
17 |    0           2187   G     Xorg
18 |    0           2187   G     Xorg
19 |    0           2187   G     Xorg
20 |-----+-----+-----+-----+
```

```
18 +-----+
19 <!--NeedCopy-->
```

确认 **NVIDIA GRID** 图形驱动程序是否已正确安装

要确认 NVIDIA GRID 图形驱动程序是否已正确安装，请运行 **nvidia-smi**。结果类似于：

```
1 +-----+
2 | NVIDIA-SMI 352.70      Driver Version: 352.70      |
3 |-----+-----+-----+-----+-----+-----+
4 | GPU   Name           Persistence-M| Bus-Id        Disp.A | Volatile
   Uncorr. ECC |
5 | Fan  Temp  Perf    Pwr:Usage/Cap|      Memory-Usage | GPU-Util
   Compute M. |
6 |=====+=====+=====+=====+=====+=====+
7 |    0   Tesla M60                Off | 0000:00:05.0    Off |
   N/A   20C    P0      37W / 150W |      19MiB /  8191MiB |      0%
   Default |
9 +-----+-----+-----+-----+-----+-----+
10
11 +-----+-----+-----+-----+-----+-----+
12 | Processes:                                                       GPU
   Memory |
13 | GPU       PID  Type  Process name
   Usage   |
14 |=====+=====+=====+=====+=====+=====+
15 | No running processes found
16 +-----+-----+-----+-----+-----+-----+
17 <!--NeedCopy-->
```

为显卡设置正确的配置：

```
etc/X11/ctx-nvidia.sh
```

HDX 3D Pro 多监视器重绘问题

如果在非主监视器屏幕上发生重绘问题，请检查 NVIDIA GRID 许可证是否可用。

检查 **Xorg** 错误日志

Xorg 的日志文件命名类似于 **Xorg.{DISPLAY}.log**，位于 **/var/log/** 文件夹中。

已知问题及限制

对于 **vGPU**，**XenServer** 本地控制台显示 **ICA** 桌面会话屏幕

解决方法：通过运行以下命令禁用 VM 的本地 VGA 控制台：

```
1 xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"  
2 <!--NeedCopy-->
```

8Q 以外的 **vGPU** 配置文件不支持 **NVENC API**

8Q 以外的 NVIDIA Tesla M60 卡 vGPU 配置文件不支持 cuda，因此 NVENC API 和 Citrix 3D Pro 硬件编码不可用。

NVIDIA K2 显卡不支持在直通模式下进行 **YUV444** 硬件编码

这是 NVIDIA K2 图形卡的限制。

登录时 **Gnome 3** 桌面显示很慢

这是 Gnome 3 桌面会话启动的限制。

在调整 **Citrix Receiver** 窗口大小时，有些 **OpenGL/WebGL** 应用程序无法很好地呈现

调整 Citrix Receiver 窗口大小会改变屏幕分辨率。NVIDIA 专用驱动程序会更改某些内部状态，并可能要求应用程序做出相应的响应。例如，WebGL 库元素 **lightgl.js** 可能会生成错误，指示 **Rendering to this texture is not supported (incomplete frame buffer)**。

非 **GRID 3D** 图形

March 11, 2024

概述

通过此功能增强，Linux VDA 不仅支持 NVIDIA GRID 3D 卡，而且还支持非 GRID 3D 卡。

安装

要使用非 GRID 3D 图形功能，您必须：

- 安装 XDamage 作为必备条件。通常情况下，XDamage 是作为 XServer 的扩展程序。
- 在安装 Linux VDA 时将 `CTX_XDL_HDX_3D_PRO` 设置为 `Y`。有关环境变量的信息，请参阅[步骤 3: 设置运行时环境以完成安装](#)。

配置

Xorg 配置文件

如果您的 3D 卡驱动程序是 NVIDIA，则会自动安装和设置配置文件。

其他类型的 3D 卡

如果您的 3D 卡驱动程序不是 NVIDIA，则必须修改安装在 `/etc/X11/` 下面的四个模板配置文件：

- `ctx-driver_name-1.conf`
- `ctx-driver_name-2.conf`
- `ctx-driver_name-3.conf`
- `ctx-driver_name-4.conf`

以 `ctx-driver_name-1.conf` 为例，执行以下操作来修改模板配置文件：

1. 将 **`driver_name`** 替换为实际的驱动程序名称。

例如，如果您的驱动程序名称为 `intel`，可以将配置文件名称更改为 `ctx-intel-1.conf`。

2. 添加视频驱动程序信息。

每个模板配置文件都一个包含名为“Device”的部分，这部分被注释掉。本节介绍视频驱动程序信息。请在添加您的视频驱动程序信息之前先完成本节内容。要启用本部分内容，请执行以下操作：

- a) 请参阅制造商提供的 3D 卡指南了解配置信息。可以生成本机配置文件。确认在未使用 Linux VDA ICA 会话时，您的 3D 卡在使用本机配置文件的本地环境中是否能正常使用。
 - b) 将本机配置文件的“Device”部分复制到 `ctx-driver_name-1.conf`。
3. 运行以下命令来设置注册表项，以使 Linux VDA 能够识别在步骤 1 中设置的配置文件名称。

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
  CurrentControlSet\Control\Citrix\XDamage" -t "REG_SZ" -v "
  DriverName" -d "intel" --force
2 <!--NeedCopy-->
```

启用非 **GRID 3D** 图形功能

默认情况下，非 GRID 3D 图形功能处于禁用状态。可以运行以下命令将 XDamageEnabled 设置为 1 来启用它。

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
  CurrentControlSet\Control\Citrix\XDamage" -t "REG_DWORD" -v "
  XDamageEnabled" -d "0x00000001" --force
2 <!--NeedCopy-->
```

故障排除

无图形输出或图形输出为乱码

如果您可以在本地运行 3D 应用程序，且所有配置均正确，则丢失图形输出或图形输出为乱码是因为缺陷。请使用 `/opt/Citrix/VDA/bin/setlog` 并将 `GFX_X11` 设置为 “verbose” 来收集跟踪信息以进行调试。

不能进行硬件编码

此功能仅支持软件编码。

配置策略

November 8, 2021

安装

按照安装文章来准备 Linux VDA。

依赖项

请务必在安装 Linux VDA 软件包之前安装这些依赖项。

RHEL/CentOS:

```
1 sudo yum -y install openldap
2
3 sudo yum -y install libxml2
4
5 sudo yum -y install cyrus-sasl
6
7 sudo yum -y install cyrus-sasl-gssapi
8 <!--NeedCopy-->
```

SLES/SELD:

```
1 sudo zypper install openldap2
2
3 sudo zypper install libxml2
4
5 sudo zypper install cyrus-sasl
6
7 sudo zypper install cyrus-sasl-gssapi
8 <!--NeedCopy-->
```

Ubuntu:

```
1 sudo apt-get install -y libldap-2.4-2
2
3 sudo apt-get install -y libsasl2-2
4
5 sudo apt-get install -y libsasl2-modules-gssapi-mit
6 <!--NeedCopy-->
```

配置

Citrix Studio 中的策略设置

要在 Citrix Studio 中设置策略，请执行以下操作：

1. 打开 **Citrix Studio**。
2. 选择策略面板。
3. 单击创建策略。
4. 根据[策略支持列表](#)设置策略。

VDA 上的 **LDAP** 服务器设置

对于单域环境，VDA 上的 LDAP 服务器设置是可选的，但对于多域和多级林环境，该设置是必需的。策略服务需要此设置才能在這些环境中执行 LDAP 搜索。

安装 Linux VDA 软件包后，运行以下命令：

```
1 /opt/Citrix/VDA/sbin/ctxsetup.sh
2 <!--NeedCopy-->
```

按建议的格式键入所有 LDAP 服务器：由空格分隔的 LDAP 完全限定域名 (FQDN) (带有 LDAP 端口) 列表 (例如 ad1.mycompany.com:389 ad2.mycompany.com:389)。

```
Checking CTX_XDL_LDAP_LIST... value not set.
The Virtual Delivery Agent by default queries DNS to discover LDAP servers, however if DNS is unable to provide
LDAP service records, you may provide a space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with
LDAP port (e.g. ad1.mycompany.com:389).
If required, please provide the FQDN:port of at least one LDAP server. [<none>]: █
```

还可以通过运行 **ctxreg** 命令将此设置直接写入注册表：

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
  VirtualDesktopAgent" -t "REG_SZ" -v "ListOfLDAPServers" -d "ad1.
  mycompany.com:389 ad2.mycompany.com:389" --force
2 <!--NeedCopy-->
```

以下策略仅适用于 Linux VDA，并且只能在 Citrix Studio 7.12 版及更高版本进行配置：

- ClipboardSelectionUpdateMode
- PrimarySelectionUpdateMode
- MaxSpeexQuality

[策略支持列表](#)中说明了这些策略。如果您使用的是 Citrix Studio 7.11 或更低版本，则必须使用 **ctxreg** 命令在 Linux VDA 上本地配置这些策略。

注意：

这些值限于一定的范围。有关详细说明，请参阅[策略支持列表](#)。

策略支持列表

November 8, 2021

Linux VDA 策略支持列表

Studio 策略	注册表项名称	类型	模块	默认值
ICA 保持活动状态	SendICAKeepAlives	计算机	ICA\保持活动状态	不发送 ICA 保持活动状态消息 (0)

Studio 策略	注册表项名称	类型	模块	默认值
ICA 保持活动状态超时	ICAKeepAliveTimeout	计算机	ICA\保持活动状态	60 秒
ICA 侦听器端口号	IcaListenerPortNumber	计算机	ICA	1494
音频重定向带宽限制	LimitAudioBw	用户	音频	0 Kbps
客户端音频重定向	AllowAudioRedirection	用户	音频	允许 (1)
客户端打印机重定向	AllowPrinterRedir	用户	打印	允许 (1)
客户端剪贴板重定向	AllowClipboardRedir	用户	剪贴板	允许 (1)
客户端 USB 设备重定向	AllowUSBRedir	用户	USB	禁止 (0)
客户端 USB 设备重定向规则	USBDeviceRules	用户	USB	"\0"
移动图像压缩	MovingImageCompressionConfiguration	用户	Thinwire	已启用 (1)
目标最低帧速率	TargetedMinimumFramesPerSecond	用户	Thinwire	10 fps
目标帧速率	FramesPerSecond	用户	Thinwire	30 fps
视觉质量	VisualQuality	用户	Thinwire	中 (3)
使用视频编解码器进行压缩	VideoCodec	用户	Thinwire	首选时使用 (3)
使用视频编解码器的硬件编码	UseHardwareEncodingForVideoCodec	用户	Thinwire	已启用 (1)
简单图形的首选颜色深度	PreferredColorDepth	用户	Thinwire	24 位/像素 (1)
音频质量	SoundQuality	用户	音频	高 - 高清晰度音频 (2)
客户端麦克风重定向	AllowMicrophoneRedirection	用户	音频	允许 (1)
最大会话数	MaximumNumberOfSessions	计算机	负载管理	250
并发登录数容差	ConcurrentLogonsToComputer	计算机	负载管理	2
启用控制器自动更新	EnableAutoUpdateOfControllers	计算机	Virtual Delivery Agent 设置	允许 (1)
剪贴板选择更新模式	ClipboardSelectionUpdateMode	用户	剪贴板	3
主选定内容更新模式	PrimarySelectionUpdateMode	用户	剪贴板	3
最高 Speex 质量	MaxSpeexQuality	用户	音频	5
自动连接客户端驱动器	AutoConnectDrives	用户	ICA\文件重定向	已启用 (1)

Studio 策略	注册表项名称	类型	模块	默认值
客户端光盘驱动器	AllowCdromDrives	用户	ICA\文件重定向	允许 (1)
客户端固定驱动器	AllowFixedDrives	用户	ICA\文件重定向	允许 (1)
客户端软盘驱动器	AllowFloppyDrives	用户	ICA\文件重定向	允许 (1)
客户端网络驱动器	AllowNetworkDrives	用户	ICA\文件重定向	允许 (1)
客户端可移动驱动器	AllowRemoveableDrives	用户	ICA\文件重定向	允许 (1)
客户端驱动器重定向	AllowDriveRedir	用户	ICA\文件重定向	允许 (1)
只读客户端驱动器访问	ReadOnlyMappedDrives	用户	ICA\文件重定向	已禁用 (0)

可以在 Citrix Studio 7.12 版及更高版本中配置以下策略。

- MaxSpeexQuality

值 (整数): [0-10]

默认值: 5

详细信息:

音频质量为中低时, 音频重定向采用 Speex 编解码器对音频数据进行编码 (请参阅音频质量策略)。Speex 是一种有损编解码器, 这意味着它会牺牲输入语音信号保真度来进行压缩。与其他一些语音编解码器不同, 这可以控制在质量和比特率之间所做的权衡。大多数时候 Speex 编码过程通过范围在 0 到 10 之间的质量参数控制。质量越高, 比特率越高。

最高 Speex 质量根据音频质量和带宽限制 (请参阅音频重定向带宽限制策略) 选择最佳 Speex 质量对音频数据编码。如果音频质量为中, 编码器将处于宽带模式, 这意味着采样率较高。如果音频质量为低, 编码器将处于窄带模式, 这意味着采样率较低。相同的 Speex 质量在不同的模式下有不同的比特率。最佳 Speex 质量出现在最大值满足以下条件时:

- 不高于最高 Speex 质量。
- 其比特率等于或小于带宽限制。

相关设置: 音频质量、音频重定向带宽限制

- PrimarySelectionUpdateMode

值 (枚举): [0, 1, 2, 3]

默认值: 3

详细信息:

选择数据并通过按下鼠标中键粘贴数据时, 将使用主选定内容。

此设置控制 Linux VDA 和客户端上的主选定内容变更是否可以在对方的剪贴板上更新。有四个值选项：

Primary selection update mode

Value: Selection changes are not updated on neither client nor host

Use

▼ Application
 Virtual Desktop OS, 7.1 Desktop OS, 7.5 Server OS, 7.5 Desktop OS, 7.8 Server OS, 7.8 Desktop OS, 7.9 Server OS, 7.9 Desktop OS, 7.11 Server OS, 7.11 Desktop OS, 7.12 Server OS, 7.12 Desktop OS, 7.13 Server OS, 7.13 Desktop OS, 7.14 Server OS, 7.14 Desktop OS, 7.15 Server OS, 7.15 Desktop OS, 7.16 Server OS, 7.16 Desktop OS, 7.17 Server OS, 7.17 Desktop OS, 7.18 Server OS, 7.18 Desktop OS, 7.19 Server OS, 7.19 Desktop OS

▼ Description
 This setting is supported only by Linux VDA version 1.4 onwards.

PRIMARY selection is used for explicit copy/paste actions such as mouse selection and middle mouse button paste. This setting controls whether PRIMARY selection changes on the Linux VDA can be updated on the client's clipboard (and vice versa). It can include one of the following selection changes:

Selection changes are not updated on the client or the host. PRIMARY selection changes do not update a client's clipboard. Client clipboard changes do not update PRIMARY selection.

Host selection changes are not updated on the client. PRIMARY selection changes do not update a client's clipboard. Client clipboard changes update the PRIMARY selection.

Client selection changes are not updated on the host. PRIMARY selection changes update the client's clipboard. Client clipboard changes do not update the PRIMARY selection.

Selection changes are updated on both the client and host. PRIMARY selection change updates the client's clipboard. Client clipboard changes update the PRIMARY selection.

▼ Related settings
 Clipboard selection update mode

- 选定内容变更既不在客户端上也不在主机上更新
Linux VDA 上的主选定内容变更不更新客户端上的剪贴板。客户端上的主选定内容变更不更新 Linux VDA 上的剪贴板。
- 主机选定内容变更不更新到客户端
Linux VDA 上的主选定内容变更不更新客户端上的剪贴板。客户端上的主选定内容变更更新 Linux VDA 上的剪贴板。
- 客户端选定内容变更不更新到主机
Linux VDA 上的主选定内容变更更新客户端上的剪贴板。客户端上的主选定内容变更不更新 Linux VDA 上的剪贴板。
- 选定内容变更同时在客户端和主机上更新

Linux VDA 上的主选定内容变更更新客户端上的剪贴板。客户端上的主选定内容变更更新 Linux VDA 上的剪贴板。此选项为默认值。

相关设置：剪贴板选定内容更新模式

- ClipboardSelectionUpdateMode

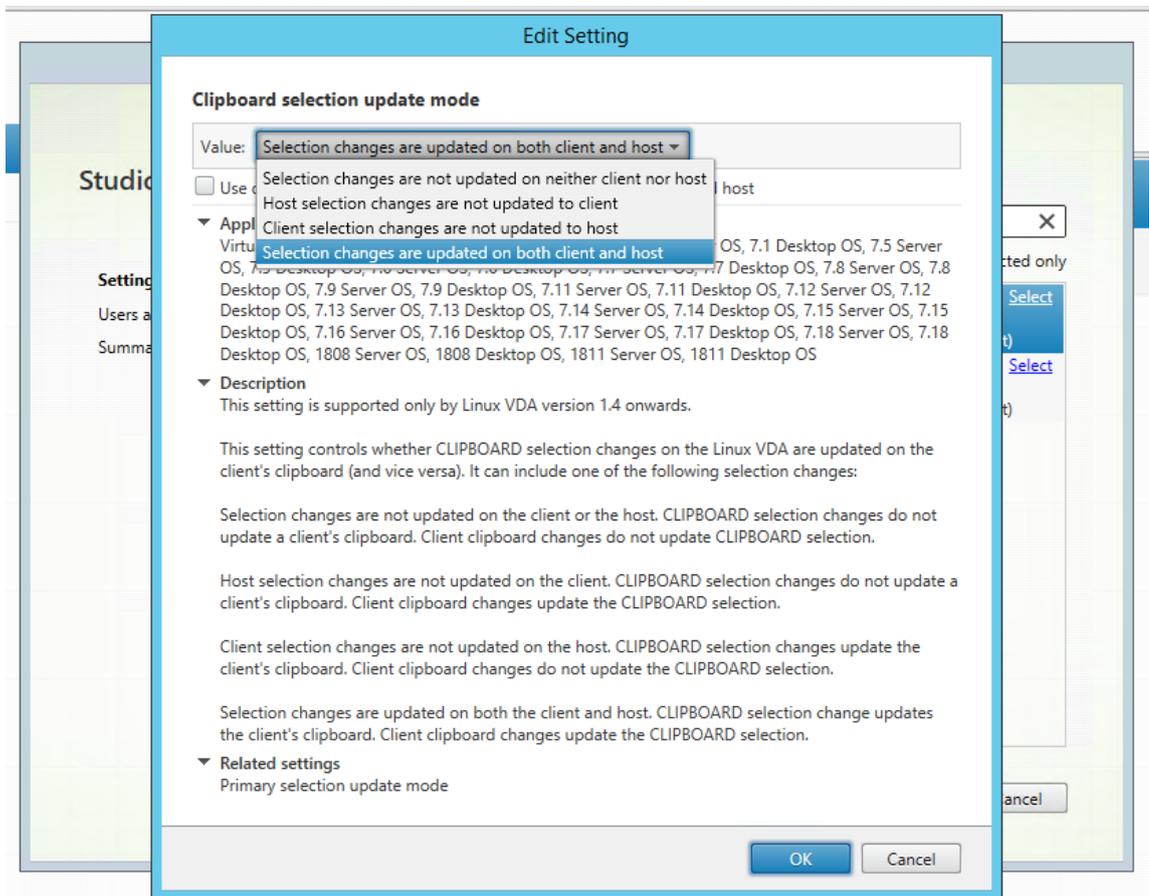
值（枚举）：[0, 1, 2, 3]

默认值：3

详细信息：

当您选择某些数据并明确请求将其“复制”到剪贴板时使用剪贴板选定内容，例如通过从快捷菜单中选择“复制”。剪贴板选定内容主要用于 Microsoft Windows 剪贴板操作，而主选定内容对 Linux 而言是唯一的。

此策略控制 Linux VDA 和客户端上的剪贴板选定内容变更是否可以在对方的剪贴板上更新。有四个值选项：



- 选定内容变更既不在客户端上也不在主机上更新
Linux VDA 上的剪贴板选定内容变更不更新客户端上的剪贴板。客户端上的剪贴板选定内容变更不更新 Linux VDA 上的剪贴板。
- 主机选定内容变更不更新到客户端
Linux VDA 上的剪贴板选定内容变更不更新客户端上的剪贴板。客户端上的剪贴板选定内容变更更新

Linux VDA 上的剪贴板。

- 客户端选定内容变更不更新到主机

Linux VDA 上的剪贴板选定内容变更更新客户端上的剪贴板。客户端上的剪贴板选定内容变更不更新 Linux VDA 上的剪贴板。

- 选定内容变更同时在客户端和主机上更新

Linux VDA 上的剪贴板选定内容变更更新客户端上的剪贴板。客户端上的剪贴板选定内容变更更新 Linux VDA 上的剪贴板。此选项为默认值。

相关设置：主选定内容更新模式

注意：

Linux VDA 支持剪贴板选定内容和主选定内容。要控制 Linux VDA 与客户端之间的复制和粘贴行为，我们建议您同时将剪贴板选定内容更新模式和主选定内容更新模式设置为相同的值。

配置 IPv6

November 8, 2021

Linux VDA 支持 IPv6 以便与 XenApp 和 XenDesktop 保持一致。使用此功能时，请注意以下事项：

- 对于双堆栈环境，除非显式启用 IPv6，否则使用 IPv4。
- 如果在 IPv4 环境中启用了 IPv6，Linux VDA 将无法运行。

重要

:

- 整个网络环境必须为 IPv6，而非仅针对 Linux VDA。
- Centrify 不支持纯 IPv6。

安装 Linux VDA 时，不需要对 IPv6 执行任何特殊的设置任务。

为 Linux VDA 配置 IPv6

更改 Linux VDA 的配置之前，请确保您的 Linux 虚拟机以前在 IPv6 网络中运行。有两个与 IPv6 配置有关的注册表项：

```
1 "HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD"  
  -v "OnlyUseIPv6ControllerRegistration"  
2  
3 "HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD"  
  -v "ControllerRegistrationIPv6Netmask"  
4 <!--NeedCopy-->
```

必须将 **OnlyUseIPv6ControllerRegistration** 设置为 1 才能在 Linux VDA 上启用 IPv6:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\  
Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "  
OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force  
2 <!--NeedCopy-->
```

如果 Linux VDA 有多个网络接口, 则可以使用 **ControllerRegistrationIPv6Netmask** 指定用于 Linux VDA 注册的网络接口:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\  
Citrix\VirtualDesktopAgent" -t "REG_SZ" -v "  
ControllerRegistrationIPv6Netmask " -d "{  
2 IPv6 netmask }  
3 " --force  
4 <!--NeedCopy-->
```

请将 **{IPv6 netmask}** 替换为真实的网络掩码 (例如 2000::/64)。

有关 XenApp 和 XenDesktop 中的 IPv6 部署的详细信息, 请参阅 [IPv4/IPv6 支持](#)。

故障排除

检查基础 IPv6 网络环境并使用 ping6 检查 AD 和 Delivery Controller 是否可访问。

配置 Citrix 客户体验改善计划 (CEIP)

February 11, 2021

参与 CEIP 时, 系统会向 Citrix 发送匿名统计数据和使用情况信息以提高 Citrix 产品的质量和性能。

注册表设置

默认情况下, 您在安装 Linux VDA 时会自动参与 CEIP。大约在您安装 Linux VDA 七天后第一次上载数据。可以在注册表中更改此默认设置。

- **CEIPSwitch**

启用或禁用 CEIP 的注册表设置 (默认值 = 0):

位置: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

名称: CEIPSwitch

值: 1 = 禁用, 0 = 启用

未指定时，CEIP 处于启用状态。

可以在客户端上运行以下命令来禁用 CEIP：

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\  
Citrix\CEIP" -v "CEIPSwitch" -d "1"  
2 <!--NeedCopy-->
```

• DataPersistPath

控制数据保留路径的注册表设置（默认值 = /var/xdl/ceip）：

位置：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

名称：DataPersistPath

值：字符串

可以运行以下命令来设置此路径：

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\  
Citrix\CEIP" -v "DataPersistPath" -d "your_path"  
2 <!--NeedCopy-->
```

如果配置的路径不存在或无法访问，数据将保存在默认路径中。

从 Linux VDA 收集的 CEIP 数据

下表提供了收集的匿名信息的类型示例。数据中不包含任何识别出您是客户的详细信息。

数据点	注册表项名称	说明
计算机 GUID	machine_guid	标识从其获取数据的计算机
AD 解决方案	ad_solution	表示计算机的域加入方法的文本字符串
Linux 内核版本	kernel_version	表示计算机的内核版本的文本字符串
LVDA 版本	vda_version	表示安装的 Linux VDA 版本的文本字符串。
LVDA 更新或全新安装	update_or_fresh_install	表示正在全新安装或更新当前 Linux VDA 软件包的文本字符串
LVDA 安装方法	install_method	表示通过使用 MCS、PVS、轻松安装或手动安装安装了当前 Linux VDA 软件包的文本字符串。
是否启用 HDX 3D pro	hdx_3d_pro	表示是否在计算机上启用 HDX 3D Pro 的文本字符串
是否启用 VDI 模式	vdi_mode	表示是否启用 VDI 模式的文本字符串

数据点	注册表项名称	说明
LVDA 主要服务上次重新启动时间	ctxhdx ctxvda	ctxhdx 和 ctxvda 服务的上次重新启动时间，格式为 dd-hh:mm:ss，例如 10-17:22:19
GPU 类型	gpu_type	表示计算机的 GPU 类型
CPU 内核	cpu_cores	表示计算机的 CPU 内核数的整数
CPU 频率	cpu_frequency	表示 CPU 频率的浮点数（以 MHz 为单位）
物理内存大小	memory_size	表示物理内存大小的整数（以 KB 为单位）
活动会话数	active_session_number	表示我们收集此数据点时计算机上活动会话数的整数
Linux 操作系统名称和版本	os_name_version	表示计算机的 Linux 操作系统名称和版本的文本字符串
会话密钥	session_key	标识从其获取数据的会话
重新连接所用时间	econnect_time_cost	用于保存会话的重新连接所用时间。数组的大小为 5，用于跟踪此数据点的当前值、最小值、最大值、运行总和以及更新计数。
活动会话时间	active_session_time	用于保存会话的活动时间。一个会话可以有多个活动时间，因为会话可以断开连接/重新连接。
会话持续时间	session_duration_time	用于保存从登录到注销的会话持续时间
Receiver 客户端类型	receiver_type	表示用于启动会话的 Citrix Receiver 类型的整数
Receiver 客户端版本	receiver_version	表示用于启动会话的 Citrix Receiver 版本的文本字符串
打印计数	printing_count	表示会话使用打印功能的次数的整数
USB 重定向计数	usb_redirecting_count	表示会话使用 USB 设备的次数的整数

配置 **USB** 重定向

November 8, 2021

USB 设备在 Citrix Receiver 与 Linux VDA 桌面之间共享。将 USB 设备重定向到桌面后，用户就可以像使用本地连接的 USB 设备那样使用它。

USB 重定向包含三个主要方面的功能：

- 开源项目实施 (VHCI)
- VHCI 服务
- USB 服务

开源 **VHCI**：

这部分 USB 重定向功能发展了通过 IP 网络的通用 USB 设备共享系统。它由 Linux 内核驱动程序和一些用户模式库组成，这些库使您可以与内核驱动程序通信以获取所有 USB 数据。在 Linux VDA 实现中，Citrix 重用 VHCI 的内核驱动程序。但是，Linux VDA 与 Citrix Receiver 之间的所有 USB 数据传输都封装在 Citrix ICA 协议软件包中。

VHCI 服务：

VHCI 服务是 Citrix 提供用来与 VHCI 内核模块通信的开源服务。此服务充当 VHCI 与 Citrix USB 服务之间的网关。

USB 服务：

USB 服务相当于管理 USB 设备上的所有虚拟化和数据传输的 Citrix 模块。

USB 重定向的工作方式

通常情况下，如果 USB 设备成功重定向至 Linux VDA，会在系统 `/dev` 路径中创建一个或多个设备节点。但是，重定向的设备有时不可用于活动的 Linux VDA 会话。USB 设备依赖于驱动程序才能正常使用，且有些设备需要特殊的驱动程序。如果并未提供驱动程序，活动 Linux VDA 会话无法使用重定向的 USB 设备。为确保 USB 设备的连接性，请安装驱动程序并正确配置系统。

Linux VDA 支持一组成功重定向至客户端和从客户端重定向的 USB 设备。此外，正确装载设备（尤其是 USB 磁盘）后，用户就可以访问磁盘，而无需进行任何其他配置。

支持的 **USB** 设备

下列设备已确认支持此 Linux VDA 版本。可以随意使用其他设备，但会有意外结果：

注意：

Linux VDA 仅支持 USB 2.0 协议。

USB 大容量存储设备	VID:PID	文件系统
Netac Technology Co., Ltd	0dd8:173c	FAT32
Kingston Datatraveler 101 II	0951:1625	FAT32

USB 大容量存储设备	VID:PID	文件系统
Kingston Datatraveler GT101 G2	1567:8902	FAT32
SanDisk SDCZ80 闪存驱动器	0781:5580	FAT32
WD HDD	1058:10B8	FAT32

USB 3D 鼠标	VID:PID
3DConnexion SpaceMouse Pro	046d: c62b

USB 扫描仪	VID:PID
Epson Perfection V330 照片	04B8: 0142

配置 **USB** 重定向

有一个 Citrix 策略控制是否启用或禁用 USB 设备重定向。此外，还可以使用 Delivery Controller 策略指定设备类型。为 Linux VDA 配置 USB 重定向时，请配置以下策略和规则：

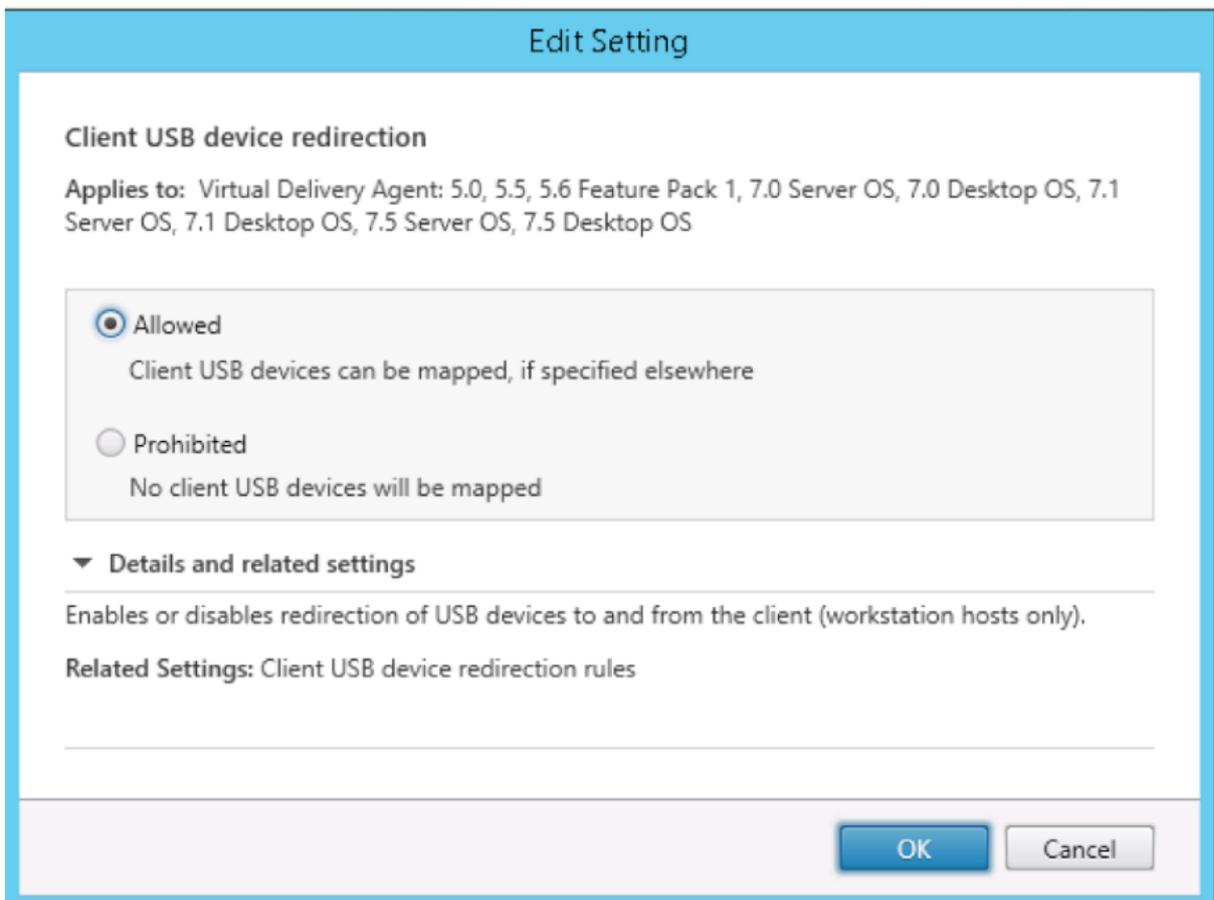
- 客户端 USB 设备重定向策略
- 客户端 USB 设备重定向规则

启用 **USB** 重定向策略

在 Citrix Studio 中，启用（或禁用）与客户端之间的 USB 设备重定向（仅限工作站主机）。

在编辑设置对话框中：

1. 选择允许。
2. 单击确定。

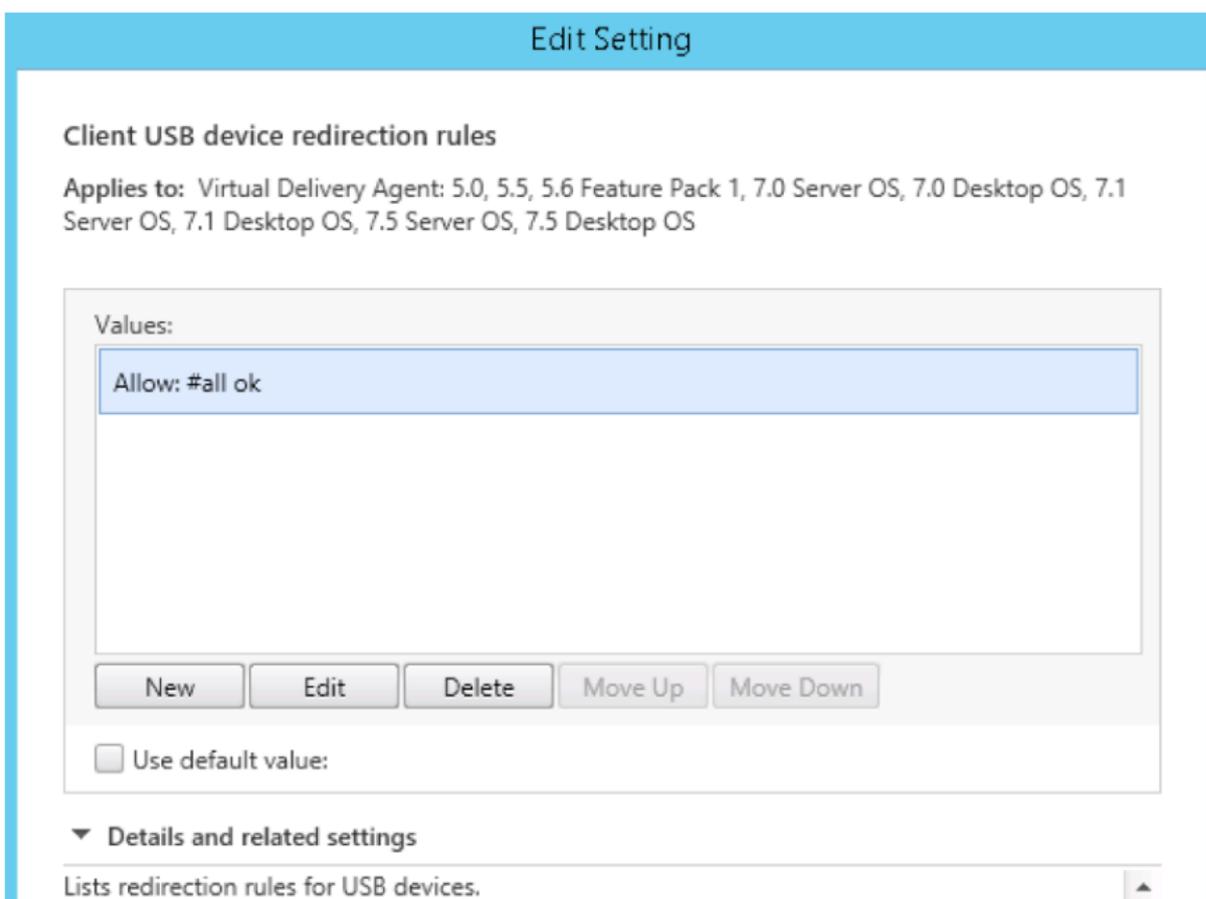


设置 **USB** 重定向规则

启用 USB 重定向策略后，使用 Citrix Studio 设置重定向规则，方法是指定允许（或拒绝）在 Linux VDA 上使用哪些设备。

在“客户端 USB 设备重定向规则”对话框中：

1. 单击新建添加重定向规则，或单击编辑检查现有规则。
2. 创建（或编辑）规则后，单击确定。



有关如何配置通用 USB 重定向的详细信息，请参阅 [Citrix Generic USB Redirection Configuration Guide](#) (《Citrix 通用 USB 重定向配置指南》)。

构建 **VHCI** 内核模块

USB 重定向依赖于 VHCI 内核模块 (**usb-vhci-hcd.ko** 和 **usb-vhci-iocif.ko**)。这些模块包含在 Linux VDA 发行版中 (作为 RPM 软件包的一部分)。它们根据正式的 Linux 发行版内核进行编译，请见下表：

支持的 Linux 发行版	内核版本
RHEL 7.3	3.10.0-514.el7.x86_64
RHEL 6.6	2.6.32-504.el6.x86_64
SUSE 12.2	4.4.49-92.11 - 默认
SUSE 11.4	3.0.101-0.47.55-default
Ubuntu 16.04	4.4.0-45-generic

重要

:

如果您的计算机的内核与 Citrix 为 Linux VDA 构建的驱动程序不兼容，USB 服务可能无法启动。在这种情况下，仅当您构建自己的 VHCI 内核模块时，才能使用 USB 重定向功能。

确认您的内核与 **Citrix** 构建的模块是否一致

在命令行上，运行以下命令来确认内核是否一致：

```
1 insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
2 <!--NeedCopy-->
```

如果命令运行成功，则内核模块已成功加载，且版本与 Citrix 安装的模块一致。

如果命令运行后显示错误，则内核与 Citrix 模块不一致，必须重新构建。

重新构建 **VHCI** 内核模块

如果您的内核模块与 Citrix 的版本不一致，请执行以下操作：

1. 从 [Citrix 下载站点](#) 下载 LVDA 源代码。选择 **Linux Virtual Delivery Agent (sources)** 部分中包含的文件。
2. 还原 citrix-linux-vda-sources.zip 文件中的文件；可以获取 **linux-vda-souces/vhci-hcd-1.15.tar.bz2** 中的 VHCI 源文件；可以使用 **tar xvf vhci-hcd-1.15.tar.bz2** 还原 VHCI 文件。
3. 基于头文件和 **Module.symvers** 文件构建内核模块。按照以下步骤安装内核头文件并根据相应的 Linux 发行版创建 **Module.symvers**：

RHEL 7.3/RHEL 6.9/RHEL 6.6:

```
1 yum install kernel-devel
2 <!--NeedCopy-->
```

SUSE 12.2:

```
1 zypper install kernel-devel
2
3 zypper install kernel-source
4 <!--NeedCopy-->
```

SUSE 11.4:

```
1 zypper install kernel-source
2 <!--NeedCopy-->
```

Ubuntu 16.04:

```
1 apt-get install linux-headers
2 <!--NeedCopy-->
```

提示：

如果安装成功，将会有类似如下文件夹的内核文件夹：

```
/usr/src/kernels/3.10.0-327.10.1.el7.x86_64
```

4. 在 `/usr/src/kernels/3.10.0-327.10.1.el7.x86_64` 文件夹中，确认是否存在 **Module.symvers** 文件。如果该文件夹中没有此文件，请构建内核以获取此文件（例如 `make oldconfig`、`make prepare`、`make modules`、`make`）或者从 `/usr/src/kernels/3.10.0-327.10.1.el7.x86_64-obj/x86_64/defaults/module.*` 复制此文件。
5. 在 `vhci-hcd-1.15/Makefile` 文件中，更改 VCHI 的 Makefile，并将 KDIR 设置为内核目录：

```
1 #KDIR = $(BUILD_PREFIX)/lib/modules/$(KVERSION)/build
2
3 KDIR = /usr/src/kernels/3.10.0-327.10.1.el7.x86_64
4 <!--NeedCopy-->
```

6. 在文件夹 `vhci-hcd-1.15/` 中，运行 `make` 以构建 VHCI 内核。

注意：

如果构建成功，则会在文件夹 `vhci-hcd-1.15/` 中创建 `usb-vhci-hcd.ko` 和 `usb-vhci-iocifc.ko`。

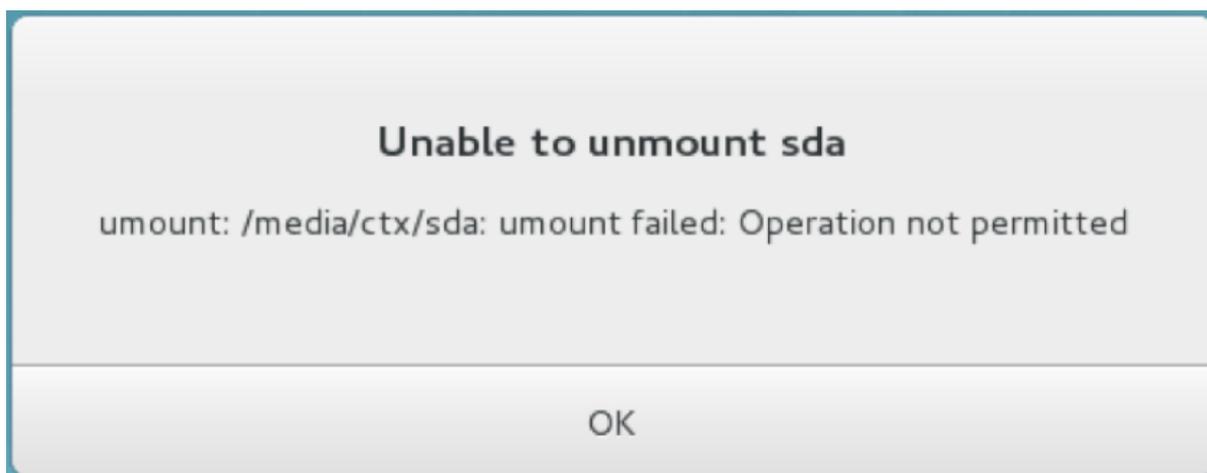
7. 将内核模块替换为新构建的模块：`cp -f usb-vhci-*.ko /opt/Citrix/VDA/lib64/`
8. 重新启动 USB 服务：`service ctxusbsd restart`
9. 注销并重新登录会话。检查 USB 重定向是否正常。

解决 USB 重定向问题

请根据本节中的信息解决您在使用 Linux VDA 时可能遇到的各种问题。

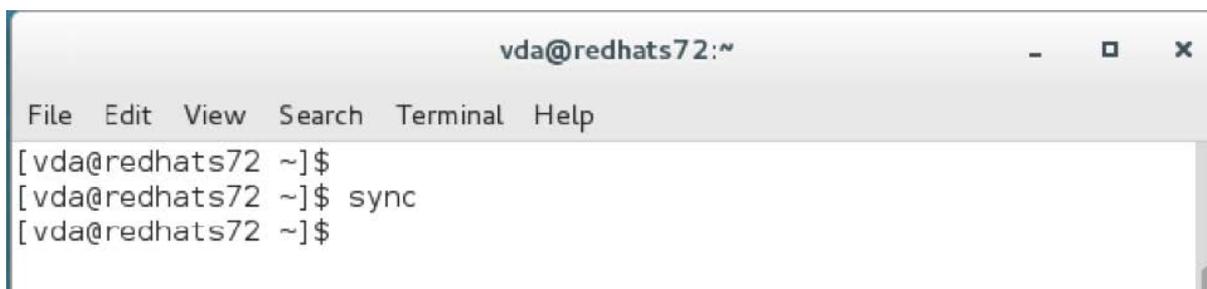
无法卸载重定向的 USB 磁盘

为了对从 Citrix Receiver 重定向的所有 USB 磁盘进行访问控制，Linux VDA 采用管理权限管理所有这些设备，确保只有所有者才能访问重定向的设备。因此，没有管理权限的用户不能卸载设备。



停止重定向 **USB** 磁盘时文件丢失

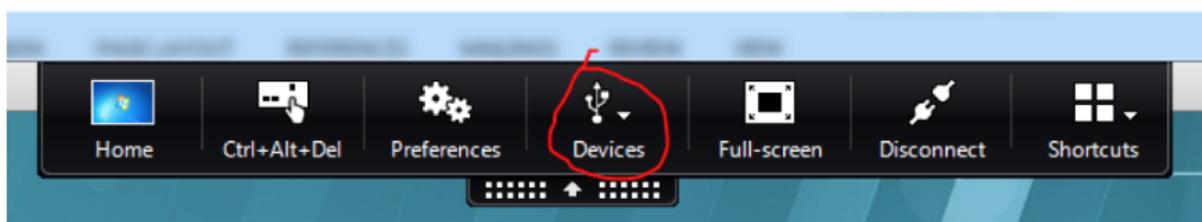
如果将 USB 磁盘重定向到会话并尝试修改该磁盘（例如，在磁盘上创建一些文件），然后立即使用 Citrix Receiver 工具栏停止重定向，您修改或创建的文件可能会丢失。出现此问题是因为您将数据写入文件系统时，系统在文件系统中装载内存缓存。数据并未写入磁盘本身。如果使用 Citrix Receiver 工具栏停止重定向，则没有时间将数据刷新至磁盘，从而导致数据丢失。为了解决此问题，请先在终端使用同步命令将数据刷新至磁盘，然后再停止 USB 重定向。



Citrix Receiver 的工具栏中无设备

有时，您可能会看到 Citrix Receiver 的工具栏中没有列出设备，这表示没有进行 USB 重定向。如果遇到该问题，请确认以下事项：

- 策略已配置为允许 USB 重定向
- 内核模块与您的内核兼容



注意：

设备选项卡在 Citrix Receiver for Linux 中不可用。

当 **USB** 设备在 **Citrix Receiver** 工具栏中显示，但这些设备都标有受策略限制时，重定向失败

此问题是由于设备的策略配置所致。在此类情况下，请执行以下操作：

- 配置 Linux VDA 策略以启用重定向
- 检查是否在 Citrix Receiver 注册表中配置了任何其他策略限制。Citrix Receiver 的注册表设置可能会阻止设备。检查注册表路径中的 **DeviceRules** 以确保此设置未导致出现访问设备被拒绝的情况：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB
```

有关详细信息，请参阅 Citrix 支持站点上的 [How to Configure Automatic Redirection of USB Devices](#)（如何配置 USB 设备的自动重定向）。

USB 设备已成功重定向，但无法在会话中使用

通常情况下，只能重定向受支持的 **USB 设备**。但是，有时其他种类的设备可能会重定向到活动 Linux VDA 会话。在这些情况下，对于每个重定向的设备，都会在系统 **/dev** 路径中创建用户拥有的节点。但是，用户是否可以成功使用设备由驱动程序和配置决定。如果您发现拥有（已插入）的某个设备无法访问，请将该设备添加到不受限制策略。

注意：

如果是 USB 驱动器，Linux VDA 会配置和装载磁盘。用户（且仅限安装它的所有者）无需执行任何其他配置即可访问该磁盘。未包含在受支持设备列表中的设备可能不是这种情况。

客户端输入法编辑器 (IME)

November 21, 2020

概述

必须通过 IME 输入双字节字符，例如中文、日语和朝鲜语字符。通过与客户端上的 Citrix Workspace 应用程序兼容的任何 IME（例如 Windows 本机 CJK IME）键入此类字符。

安装

在安装 Linux VDA 时，会自动安装此功能。

使用情况

正常打开 XenDesktop 或 XenApp 会话。

根据需要在客户端上更改您的输入法以开始使用客户端 IME。

已知问题

- 必须先双击 Google 电子表格中的单元格，才能使用客户端 IME 功能在单元格中键入字符。
- 不会在“密码”字段中自动禁用客户端 IME。
- IME 用户界面不在输入区域中跟随光标。
- SUSE 11 发行版不支持客户端 IME。

HDX Insight

February 9, 2024

概述

HDX Insight 是 Citrix Application Delivery Management (ADM) 的一部分，基于行业通用标准 AppFlow。通过 HDX Insight，IT 可以提供对通过 NetScaler 或 Citrix SD-WAN 应用程序网络结构传送的 Citrix ICA 通信前所未有的端到端可见性，从而实现卓越的用户体验。

在此版本中，Linux VDA 部分支持 HDX Insight 功能。由于尚未实现最终用户体验管理 (EUEM) 功能，与持续时间相关的数据点不可用。

安装

没有依赖软件包需要安装。

使用情况

HDX Insight 将分析通过 Citrix Workspace 应用程序和 Linux VDA 之间的 NetScaler 传递的 ICA 消息。

必须使用 Linux VDA 设置 NetScaler Insight Center 部署，然后启用 HDX Insight 功能。可以将您的 NetScaler Insight Center 部署迁移到 Citrix ADM，而不会丢失现有的配置、设置或数据。有关详细信息，请参阅[从 NetScaler Insight Center 迁移到 Citrix ADM](#)。

故障排除

不显示任何数据点

可能有两个原因：

- HDX Insight 未正确配置。
例如，在 NetScaler 上未启用 AppFlow 或在 Insight Center 上配置了不正确的 NetScaler 实例。
- 在 Linux VDA 上未启动 ICA 控制虚拟通道。

```
ps aux | grep -i ctxctl
```

如果 `ctxctl` 未运行，请与管理员联系以向 Citrix 报告缺陷。

不显示任何应用程序数据点

请确认是否启用了无缝虚拟通道且无缝应用程序启动了一段时间。

已知问题

无法显示与持续时间有关的数据点。由于未实现 EUEM 功能，与持续时间（例如，ICA RTT）有关的数据点不可用，并显示为“不适用”。

启用跟踪

August 10, 2021

概述

收集日志并重现问题减慢了诊断速度，并且降低了用户体验。“启用跟踪”功能可以简化此类工作。跟踪功能默认对 Linux VDA 启用。

配置

`ctxlogd` 守护程序和 `setlog` 实用程序现在包括在 Linux VDA 版本软件包中。默认情况下，`ctxlogd` 守护程序在您安装并配置 Linux VDA 后启动。

ctxlogd 守护程序

跟踪的所有其他服务都基于 `ctxlogd` 守护程序。如果不希望跟踪 Linux VDA，可以停止 `ctxlogd` 守护程序。

setlog 实用程序

“启用跟踪”功能是使用 `setlog` 实用程序配置的，该程序位于 `/opt/Citrix/VDA/bin/` 路径下。只有 root 用户有权运行该程序。可以使用 GUI 或运行命令来查看和更改配置。请运行以下命令以获取使用 `setlog` 实用程序的帮助信息：

```
1 setlog help
2 <!--NeedCopy-->
```

值 默认情况下，**Log Output Path**（日志输出路径）设置为 `/var/log/xdl/hdx.log`，**Max Log Size**（最大日志大小）设置为 200 MB，您最多可以在 **Log Output Path**（日志输出路径）下保存两个旧日志文件。

查看当前的 `setlog` 值：

```
1 setlog values
2
3 log_path (Log Output Path) = /var/log/xdl/hdx.log
4
5 log_size (Max Log Size (MiB)) = 200
6
7 log_count (Max Old Log Files) = 2
8 <!--NeedCopy-->
```

查看或设置单个 `setlog` 值：

```
1 setlog value <name> [<value>]
2 <!--NeedCopy-->
```

例如：

```
1 setlog value log_size 100
2 <!--NeedCopy-->
```

级别 默认情况下，日志级别设置为警告。

查看为不同组件设置的日志级别：

```
1 setlog levels
2 <!--NeedCopy-->
```

可以通过以下命令设置所有日志级别（包括禁用、已继承、详细、信息、警告、错误和致命错误）：

```
1 setlog level <class> [<level>]
2 <!--NeedCopy-->
```

<class> 变量指定 Linux VDA 的一个组件。要涵盖所有组件，请将其设置为 **all**：

```
1 setlog level all error
2
3 Setting log class ALL to ERROR.
4 <!--NeedCopy-->
```

标志 默认情况下，标志设置如下：

```
1 setlog flags
2
3 DATE = true
4
5 TIME = true
6
7 NAME = true
8
9 PID = true
10
11 TID = false
12
13 SID = true
14
15 UID = false
16
17 GID = false
18
19 CLASS = false
20
21 LEVEL = false
22
23 FUNC = true
24
25 FILE = false
26 <!--NeedCopy-->
```

查看当前标志：

```
1 setlog flags
2 <!--NeedCopy-->
```

查看或设置单个日志标志：

```
1 setlog flag <flag> [<state>]
2 <!--NeedCopy-->
```

还原默认值 将所有级别、标志和值还原到默认设置：

```
1 setlog default
2 <!--NeedCopy-->
```

重要

:

`ctxlogd` 服务是使用 `/var/xdl.ctxlog` 文件配置的，只有 `root` 用户能够创建该文件。其他用户对该文件没有写入权限。Citrix 建议 `root` 用户不要向其他用户授予写入权限。否则会导致对 `ctxlogd` 进行任意配置或恶意配置，这样会影响服务器性能，进而影响用户体验。

故障排除

`/var/xdl.ctxlog` 文件丢失（例如，意外删除）时，`ctxlogd` 守护程序失败，您将无法重新启动 `ctxlogd` 服务。

`/var/log/messages`:

```
1 Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]:Failed to open logging
   configuration file.
2
3 Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited, code
   =exited, status=1/FAILURE
4
5 Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.
6
7 Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
8 <!--NeedCopy-->
```

要解决此问题，请以 `root` 用户身份运行 `setlog` 以重新创建 `/var/xdl.ctxlog` 文件。然后重新启动其他服务所基于的 `ctxlogd` 服务。

配置未经身份验证的会话

April 18, 2024

按照本文信息配置未经身份验证的会话。安装 Linux VDA 以使用此功能时无需特殊设置。

注意：

配置未经身份验证的会话时，请考虑会话预启动并不受支持。会话预启动在 Citrix Receiver for Android 上也不受支持。

创建未经身份验证的应用商店

要在 Linux VDA 上支持未经身份验证的会话，请使用 StoreFront [创建未经身份验证的应用商店](#)。

在交付组中启用未经身份验证的用户

在创建未经身份验证的应用商店后，在交付组中启用未经身份验证的用户以支持未经身份验证的会话。要在交付组中启用未经身份验证的用户，请按照 [XenApp](#) 和 [XenDesktop](#) 文档中的说明进行操作。

设置未经身份验证的会话空闲时间

未经身份验证的会话的默认空闲超时时间是 10 分钟。此值是通过注册表设置 **AnonymousUserIdleTime** 进行配置。可以使用 **ctxreg** 工具更改此值。例如，将此注册表设置为 5 分钟：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix" -v AnonymousUserIdleTime -d 0
  x00000005
2 <!--NeedCopy-->
```

设置未经身份验证的用户的最大数量

要设置未经身份验证的用户的最大数量，请使用注册表项 **MaxAnonymousUserNumber**。此设置限制单个 Linux VDA 上同时运行的未经身份验证的会话数。可以使用 **ctxreg** 工具配置此注册表设置。例如，将该值设置为 32：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber -d 0
  x00000020
2 <!--NeedCopy-->
```

重要：

限制未经身份验证的会话数。如果同时启动太多会话，VDA 可能会出现一些问题，其中包括耗尽可用内存。

故障排除

配置未经身份验证的会话时，请考虑以下事项：

- 无法登录到未经身份验证的会话。

确认注册表是否已更新包含了以下内容（设置为 0）：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg read -k "HKLM\System\CurrentControlSet
  \Control\Citrix" -v MaxAnonymousUserNumber
2 <!--NeedCopy-->
```

确认 **nscd** 服务是否正在运行，且已配置为启用 **passwd** 缓存：

```
1 ps uax | grep nscd
2 cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
3 <!--NeedCopy-->
```

如果已启用，请将 **Passwd** 缓存变量设置为 **no**，然后重新启动 **ncsd** 服务。更改此配置后您可能需要重新安装 Linux VDA。

- 使用 **KDE** 时未经身份验证的会话中显示锁屏按钮。

默认情况下未经身份验证的会话中禁用锁屏按钮和菜单。但是，它们仍可显示在 KDE 中。在 KDE 中，要对特定用户禁用锁屏按钮和菜单，请将以下行添加到配置文件 **\$Home/.kde/share/config/kdeglobals** 中。例如：

```
1 [KDE Action Restrictions]
2 action/lock_screen=false
3 <!--NeedCopy-->
```

但是，如果在全局范围的 **kdeglobals** 文件(例如 **/usr/share/kde-settings/kde-profile/default/share/config/kdeglobals**) 中 **KDE Action Restrictions** 参数已配置为不可变，用户配置没有效果。

为了解决这个问题，请修改系统范围的 **kdeglobals** 文件，删除 **[KDE Action Restrictions]** 部分的 ****\\${i}** 标记，也可以直接使用系统范围的配置来禁用锁屏按钮和菜单。有关 KDE 配置的详细信息，请参阅 [\[KDE System Administration/Kiosk/Keys page\]](#) (KDE 系统管理/Kiosk/键页面)。

配置 LDAPS

November 8, 2021

安全 LDAP (LDAPS) 允许您为 Active Directory 管理的域启用安全轻型目录访问协议以提供通过 SSL (Secure Socket Layer, 安全套接字层) /TLS (Transport Layer Security, 传输层安全性) 进行通信的功能。

默认不加密客户端与服务器应用程序之间的 LDAP 通信。通过使用 SSL/TLS 的 LDAP (LDAPS)，可以保护 Linux VDA 与 LDAP 服务器之间的 LDAP 查询内容。

以下 Linux VDA 组件在 LDAPS 上都具有依赖项：

- Broker 代理：Linux VDA 注册到 Delivery Controller 中
- 策略服务：策略评估

配置 LDAPS 涉及以下过程：

- 在 Active Directory (AD)/LDAP 服务器上启用 LDAPS
- 导出根 CA 以供客户端使用
- 在 Linux VDA 上启用/禁用 LDAPS
- 为第三方平台配置 LDAPS
- 配置 SSSD
- 配置 Winbind
- 配置 Centrify
- 配置 Quest

在 **AD/LDAP** 服务器上启用 **LDAPS**

可以通过安装 Microsoft 证书颁发机构 (CA) 或非 Microsoft CA 提供的格式正确的证书来启用通过 SSL 的 LDAP (LDAPS)。

提示：

在域控制器上安装企业根 CA 时将自动启用通过 SSL/TLS 的 LDAP (LDAPS)。

有关如何安装证书并验证 LDAPS 连接的详细信息，请参阅 Microsoft 支持站点上的 [How to enable LDAP over SSL with a third-party certification authority](#) (如何借助第三方证书颁发机构启用通过 SSL 的 LDAP)。

当您有一个多层 (例如，两层或三层) 证书颁发机构层次结构时，您在域控制器上不会自动拥有用于 LDAPS 身份验证的合适证书。

有关如何使用多层证书颁发机构层次结构为域控制器启用 LDAPS 的信息，请参阅 Microsoft TechNet 站点上的 [LDAP over SSL \(LDAPS\) Certificate](#) (通过 SSL 的 LDAP (LDAPS) 证书) 一文。

启用根证书颁发机构以供客户端使用

客户端必须使用 LDAP 服务器信任的 CA 颁发的证书。要为客户端启用 LDAPS 身份验证，请导入根 CA 证书以信任密钥库。

有关如何导出根 CA 的详细信息，请参阅 Microsoft 支持 Web 站点上的 [How to export Root Certification Authority Certificate](#) (如何导出根证书颁发机构)。

在 **Linux VDA** 上启用或禁用 **LDAPS**

要为 Linux VDA 启用或禁用 LDAPS，请运行以下脚本 (在以管理员身份登录时)：

此命令的语法包括以下内容：

- 通过提供的根 CA 证书启用通过 SSL/TLS 的 LDAP：

```
1 /opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
2 <!--NeedCopy-->
```

- 回退到未启用 SSL/TLS 的 LDAP

```
1 /opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
2 <!--NeedCopy-->
```

专用于 LDAPS 的 Java 密钥库位于 **/etc/xdm/.keystore**。受影响的注册表项包括：

```
1 HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers
2
```

```
3 HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy
4
5 HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS
6
7 HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore
8 <!--NeedCopy-->
```

为第三方平台配置 LDAPS

除 Linux VDA 组件外，还有多个附着于可能也需要安全 LDAP 的 VDA 的第三方软件组件，例如 SSSD、Winbind、Centrify 和 Quest。以下各部分介绍了如何通过 LDAPS、STARTTLS 或 SASL 签名和封装配置安全 LDAP。

提示：

并非所有这些软件组件都优先使用 SSL 端口 636 来确保安全 LDAP。并且大多数时间 LDAPS（端口 636 上通过 SSL 的 LDAP）不能与 389 上的 STARTTLS 共存。

SSSD

根据选项在端口 636 或 389 上配置 SSSD 安全 LDAP 流量。有关详细信息，请参阅 [SSSD LDAP Linux 手册页](#)。

Winbind

Winbind LDAP 查询使用 ADS 方法。Winbind 在端口 389 上仅支持 StartTLS 方法。受影响的配置文件为 **ldap.conf** 和 **smb.conf**。按如下所示更改这些文件：

```
1 ldap.conf:
2
3 TLS_REQCERT never
4
5 smb.conf:
6
7 ldap ssl = start tls
8
9 ldap ssl ads = yes
10
11 client ldap sasl wrapping = plain
12 <!--NeedCopy-->
```

或者，安全 LDAP 可以通过 SASL GSSAPI 签名和封装进行配置，但不能与 TLS/SSL 共存。要使用 SASL 加密，请更改 **smb.conf** 配置：

```
1 smb.conf:
2
3 ldap ssl = off
4
```

```
5 ldap ssl ads = no
6
7 client ldap sasl wrapping = seal
8 <!--NeedCopy-->
```

Centrify

Centrify 在端口 636 上不支持 LDAPS。但它在端口 389 上提供安全加密。有关详细信息，请参阅 [Centrify 站点](#)。

Quest

Quest Authentication Service 在端口 636 上支持 LDAPS，但在端口 389 上使用其他方法提供安全加密。

故障排除

使用此功能时可能会引发以下问题：

- **LDAPS 服务可用性**

请确认 LDAPS 连接是否在 AD/LDAP 服务器上可用。默认情况下，端口为 636。

- 启用了 **LDAPS** 时 **Linux VDA** 注册失败

验证 LDAP 服务器和端口是否已正确配置。请先检查根 CA 证书，确保其与 AD/LDAP 服务器匹配。

- 意外错误地更改注册表项

如果在未使用 **enable_ldaps.sh** 的情况下意外更新 LDAPS 相关的注册表项，则可能会破坏 LDAPS 组件的依赖项。

- **LDAP** 流量不通过 **SSL/TLS** 从 **Wireshark** 或任何其他网络监视工具加密

默认禁用 LDAPS。请运行 **/opt/Citrix/VDA/sbin/enable_ldaps.sh** 强制执行。

- 没有来自 **Wireshark** 或任何其他网络连接监视工具的 **LDAPS** 流量

发生 Linux VDA 注册和组策略评估时会出现 LDAP/LDAPS 流量。

- 无法通过在 **AD** 服务器上运行 **ldp connect** 验证 **LDAPS** 可用性

使用 AD FQDN 而非 IP 地址。

- 无法通过运行 **/opt/Citrix/VDA/sbin/enable_ldaps.sh** 脚本导入根 **CA** 证书

请提供 CA 证书的完整路径，并确认根 CA 证书的类型是否正确。一般来说，它应与受支持的大多数 Java Keytool 类型兼容。如果它未在支持列表中列出，您可以先转换类型。如果遇到证书格式问题，Citrix 建议您使用 base64 编码的 PEM 格式。

- 无法通过 **Keytool -list** 显示根 **CA** 证书

通过运行 **/opt/Citrix/VDA/sbin/enable_ldaps.sh** 启用 LDAPS 时，证书将被导入到 **/etc/xdm/.keystore** 中，并设置密码以保护密钥库。如果忘记了密码，可以重新运行该脚本以创建密钥库。

配置 Xauthority

November 8, 2021

Linux VDA 支持使用 X11 显示功能（包括 **xterm** 和 **gvim**）进行交互式远程处理的环境。此功能提供必需的安全机制以确保 XClient 与 XServer 之间的通信安全。

可以通过两种方法确保此安全通信的权限安全：

- **Xhost**。默认情况下，Xhost 仅允许本地主机 XClient 与 XServer 进行通信。如果选择允许远程 XClient 访问 XServer，则必须运行 Xhost 命令授予对特定计算机的权限。或者，也可以使用 **xhost +** 以允许任意 XClient 连接到 XServer。
- **Xauthority**。可以在每个用户的主目录中找到 **.Xauthority** 文件。它用于将凭据存储在 xauth 使用的 cookie 中以用于对 XServer 进行身份验证。启动 XServer 实例 (Xorg) 后，该 cookie 将用于对与该特定显示的连接进行身份验证。

工作原理

Xorg 启动时，**.Xauthority** 文件将被传递到 Xorg。此 **.Xauthority** 文件包含以下元素：

- 显示数量
- 远程请求协议
- cookie 数量

可以使用 **xauth** 命令浏览此文件。例如：

```
1 # xauth -f ~/.Xauthority
2
3 # > list
4
5 # > us01msip06:107 MIT-MAGIC-COOKIE-1
   fb228d1b695729242616c5908f11624b
6 <!--NeedCopy-->
```

如果 XClient 远程连接到 Xorg，则必须满足两个必备条件：

- 设置远程 XServer 的 **DISPLAY** 环境变量。
- 获取包含 Xorg 中的其中一个 cookie 数量的 **.Xauthority** 文件。

配置 Xauthority

要在 Linux VDA 上启用 Xauthority 以进行远程 X11 显示，必须创建下面两个注册表项：

```

1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "
   XauthEnabled" -d "0x00000001" --force
2
3 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "ListenTCP"
   -d "0x00000001" --force
4 <!--NeedCopy-->

```

启用 Xauthority 后，手动或通过挂载共享主目录将 `.Xauthority` 文件传递到 XClient：

- 手动将 `.Xauthority` 文件传递给 XClient

启动 ICA 会话后，Linux VDA 将为 XClient 生成 `.Xauthority` 文件，并将该文件存储在登录用户的主目录中。可以将此 `.Xauthority` 文件复制到远程 XClient 计算机，并设置 `DISPLAY` 和 `XAUTHORITY` 环境变量。`DISPLAY` 是存储在 `.Xauthority` 文件中的显示数量，`XAUTHORITY` 是 Xauthority 的文件路径。例如，请查看以下命令：

```

1 export DISPLAY={
2   Display number stored in the Xauthority file }
3
4
5 export XAUTHORITY={
6   the file path of .Xauthority }
7
8 <!--NeedCopy-->

```

注意：

如果未设置 `XAUTHORITY` 环境变量，则默认使用 `~/.Xauthority` 文件。

- 通过挂载共享主目录将 `.Xauthority` 文件传递到 XClient

最便捷的方式是为登录用户挂载共享主目录。当 Linux VDA 启动 ICA 会话时，将在登录用户的主目录下创建 `.Xauthority` 文件。如果此主目录与 XClient 共享，用户不需要手动将此 `.Xauthority` 文件传输到 XClient。正确设置 `DISPLAY` 和 `XAUTHORITY` 环境变量后，将自动在 XServer 桌面中显示 GUI。

故障排除

如果 Xauthority 不起作用，请按照故障排除步骤进行操作：

1. 以具有 root 权限的管理员身份获取所有 Xorg cookie：

```

1 ps aux | grep -i xorg
2 <!--NeedCopy-->

```

此命令将显示启动过程中传递到 Xorg 的 Xorg 进程和参数。另一个参数显示使用的 `.Xauthority` 文件。例如：

```
1 /var/xdl/xauth/.Xauthority110
2 <!--NeedCopy-->
```

使用 **Xauth** 命令显示 cookie：

```
1 Xauth -f /var/xdl/xauth/.Xauthority110
2 <!--NeedCopy-->
```

2. 使用 **Xauth** 命令显示 `~/Xauthority` 中包含的 cookie。如果显示编号相同，则显示的 cookie 必须与 Xorg 和 XClient 的 `.Xauthority` 文件中的 cookie 相同。
3. 如果 cookie 相同，请检查是否能够使用 Linux VDA 的 IP 地址（例如 10.158.11.11）访问远程显示端口，并检查已发布桌面显示数量（例如 160）。

在 XClient 计算机上运行以下命令：

```
1 telnet 10.158.11.11 6160
2 <!--NeedCopy-->
```

端口号为 $6000 + \langle \text{显示数量} \rangle$ 的总和。

如果此 Telnet 操作失败，防火墙可能在阻止请求。



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).