



Linux Virtual Delivery Agent 1912 LTSR

Contents

新增功能	4
累积更新 9 (CU9)	4
累积更新 8 (CU8)	5
累积更新 7 (CU7)	6
1912 LTSR CU7 修补程序 1 (19.12.7001) 中已修复的问题	6
累积更新 6 (CU6)	7
累积更新 5 (CU5)	7
1912 LTSR CU5 中已修复的问题	8
累积更新 4 (CU4)	8
1912 LTSR CU4 中已修复的问题	9
累积更新 3 (CU3)	9
1912 LTSR CU3 中已修复的问题	10
累积更新 2 (CU2)	10
1912 LTSR CU2 中已修复的问题	11
累积更新 1 (CU1)	11
1912 LTSR CU1 中已修复的问题	12
关于此版本	12
1912 LTSR 中已修复的问题	13
已知问题	14
第三方声明	15
弃用	16
系统要求	16
安装概述	20

使用轻松安装进行快速安装（推荐）	20
手动安装 Linux Virtual Delivery Agent for RHEL/CentOS	36
手动安装 Linux Virtual Delivery Agent for SUSE	65
手动安装 Linux Virtual Delivery Agent for Ubuntu	86
使用 Machine Creation Services (MCS) 创建 Linux VM	114
配置 Delivery Controller	139
配置 Linux VDA	140
将 NIS 与 Active Directory 集成	141
发布应用程序	146
Remote PC Access	147
打印	156
文件传输	162
PDF 打印	166
配置图形	167
Thinwire 渐进式显示	175
非 GRID 3D 图形	177
配置策略	179
策略支持列表	180
配置 IPv6	187
配置 Citrix 客户体验改善计划 (CEIP)	188
配置 USB 重定向	191
配置会话可靠性	200
软键盘	202
客户端输入法编辑器 (IME)	205

支持多语言输入	205
动态键盘布局同步	207
客户端 IME 用户界面同步	209
HDX Insight	211
自适应传输	212
启用跟踪	214
重影会话	217
支持适用于 HTML5 的 Citrix Workspace 应用程序	222
监视 Citrix Director 中的 Linux 会话	222
监视服务守护程序	223
使用 TLS 保护用户会话安全	225
使用 DTLS 的安全用户会话	229
支持智能卡	230
双跃点单点登录身份验证	240
配置未经身份验证的会话	242
配置 LDAPS	244
配置 Xauthority	248
联合身份验证服务	250

新增功能

May 30, 2024

累积更新 9 (CU9) 是 Linux Virtual Delivery Agent 1912 LTSR 的最新版本。CU9 不包含任何已修复的问题。

注意：

自 CU3 版本起，请先安装 .NET Core 运行时 3.1 作为必备项，然后再安装 Linux VDA。

累积更新 9 (CU9)

May 30, 2024

发布日期：2024 年 4 月 30 日

关于此版本

累积更新 9 (CU9) 是 Linux Virtual Delivery Agent 1912 LTSR 的最新版本。CU9 不包含任何已修复的问题。

新增功能

增强的 **CPB/WCF** 可扩展性

现在包括 Linux VDA CPB/WCF 可扩展性增强功能，并且每个 Citrix Cloud Connector 可以支持 3000 个 Linux VDA。您可以在每个站点位置中部署两个 Cloud Connector 以实现高可用性，还可以在每个站点位置中最多部署 3000 个 Linux VDA。

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 8 \(CU8\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 7 \(CU7\) 修补程序 1 \(19.12.7001\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 7 \(CU7\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 6 \(CU6\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 5 \(CU5\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 4 \(CU4\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 3 \(CU3\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 1 \(CU1\)](#)

[Linux Virtual Delivery Agent 1912 LTSR \(初始版本\)](#)

[此版本中的已知问题](#)

[弃用和删除](#)

[Citrix 产品专享升级服务资格日期](#)

累积更新 **8 (CU8)**

May 30, 2024

发布日期: 2023 年 9 月 11 日

关于此版本

累积更新 8 (CU8) 是 Linux Virtual Delivery Agent 1912 LTSR 的最新版本。CU8 解决了有助于改进整体性能、安全性和稳定性的多个问题。

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 7 \(CU7\) 修补程序 1 \(19.12.7001\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 7 \(CU7\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 6 \(CU6\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 5 \(CU5\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 4 \(CU4\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 3 \(CU3\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 1 \(CU1\)](#)

[Linux Virtual Delivery Agent 1912 LTSR \(初始版本\)](#)

[此版本中的已知问题](#)

[弃用和删除](#)

[Citrix 产品专享升级服务资格日期](#)

累积更新 **7 (CU7)**

July 14, 2023

发布日期：2023 年 3 月 15 日

关于此版本

累积更新 7 (CU7) 修补程序 1 (19.12.7001) 是 Linux Virtual Delivery Agent 1912 LTSR 的最新版本。此修补程序修复了自 1912 LTSR CU7 发布以来报告的一个[问题](#)。

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 7 \(CU7\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 6 \(CU6\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 5 \(CU5\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 4 \(CU4\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 3 \(CU3\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 1 \(CU1\)](#)

[Linux Virtual Delivery Agent 1912 LTSR \(初始版本\)](#)

[此版本中的已知问题](#)

[弃用和删除](#)

[Citrix 产品专享升级服务资格日期](#)

1912 LTSR CU7 修补程序 1 (19.12.7001) 中已修复的问题

July 14, 2023

自 Linux Virtual Delivery Agent 1912 LTSR CU7 起，以下问题已修复：

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

1912 LTSR CU7 中已修复的问题

自 Linux Virtual Delivery Agent 1912 LTSR CU6 起，以下问题已修复：

- 当您从运行 Microsoft Windows 的便携式计算机连接到 Linux VDA 会话，并且该便携式计算机的合盖操作设置为不执行任何操作、休眠或睡眠时，可能会将随机密钥注入到 VDA 会话中。[CVADHELP-18438]
- 当您某些便携式计算机连接到 Linux VDA 并按 **Fn** 键时，它可能起到 **Delete** 键的作用。[CVADHELP-21630]

累积更新 6 (CU6)

November 4, 2022

发布日期：2022 年 10 月 31 日

关于此版本

CU6 不包含任何已修复的问题。

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 5 \(CU5\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 4 \(CU4\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 3 \(CU3\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 1 \(CU1\)](#)

[Linux Virtual Delivery Agent 1912 LTSR \(初始版本\)](#)

[此版本中的已知问题](#)

[弃用和删除](#)

[Citrix 产品专享升级服务资格日期](#)

累积更新 5 (CU5)

March 16, 2022

发布日期：2022 年 3 月 9 日

关于此版本

Linux Virtual Delivery Agent 1912 LTSR 累积更新 5 (CU5) 修复了自 1912 LTSR CU4 发布以来报告的两个[问题](#)。

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 4 \(CU4\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 3 \(CU3\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 1 \(CU1\)](#)

[Linux Virtual Delivery Agent 1912 LTSR \(初始版本\)](#)

[此版本中的已知问题](#)

[弃用和删除](#)

[Citrix 产品专享升级服务资格日期](#)

1912 LTSR CU5 中已修复的问题

March 16, 2022

自 Linux Virtual Delivery Agent 1912 LTSR CU4 起，以下问题已修复：

- Linux VDA 桌面可能无法响应键盘和鼠标输入。[CVADHELP-18498]
- 在具有多个域控制器的环境中关闭一个域控制器可能会导致在 Linux VDA 上启动会话失败。[CVADHELP-18900]

累积更新 4 (CU4)

January 26, 2022

发布日期：2021 年 11 月 3 日

关于此版本

Linux Virtual Delivery Agent 1912 LTSR 累积更新 4 (CU4) 修复了自 1912 LTSR CU3 发布以来报告的三个[问题](#)。

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 3 \(CU3\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 1 \(CU1\)](#)

[Linux Virtual Delivery Agent 1912 LTSR \(初始版本\)](#)

[此版本中的已知问题](#)

[弃用和删除](#)

[Citrix 产品专享升级服务资格日期](#)

1912 LTSR CU4 中已修复的问题

January 26, 2022

自 Linux Virtual Delivery Agent 1912 LTSR CU3 起，以下问题已修复：

- 在使用适用于 Mac 或 Linux 的 Citrix Workspace 应用程序连接的 Linux VDA 上，按 Shift + Tab 键可能会注册为双击 **Shift** 键。[CVADHELP-16831]
- 如果使用 Machine Creation Services 在 Azure 中创建 Linux VM，尝试在 RHEL 上启动 Linux VDA 会话可能会失败。[CVADHELP-17244]
- 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]

累积更新 3 (CU3)

January 26, 2022

发布日期：May 12, 2021

关于此版本

Linux Virtual Delivery Agent 1912 LTSR 累积更新 3 (CU3) 修复了自 1912 LTSR CU2 发布以来报告的九个[问题](#)。

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 2 \(CU2\)](#)

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 1 \(CU1\)](#)

[Linux Virtual Delivery Agent 1912 LTSR \(初始版本\)](#)

[此版本中的已知问题](#)

[弃用和删除](#)

[Citrix 产品专享升级服务资格日期](#)

1912 LTSR CU3 中已修复的问题

January 26, 2022

自 Linux Virtual Delivery Agent 1912 LTSR CU2 起，以下问题已修复：

- 升级 64 位 Linux VDA 后，用户尝试启动应用程序可能会失败。用户看到一条消息，指示应用程序正在启动，然后消息消失。因此，VDA 上仍有多个过时的会话。[CVADHELP-15899]
- 执行扫描后，`ctxmonitorservice` 进程可能会意外退出，并出现 SIGABRT 错误。[CVADHELP-15969]
- 在小米 Mi 10 手机上尝试选择图片传输协议 (PTP) 和媒体传输协议 (MTP) USB 选项可能会失败。[CVADHELP-16188]
- 当 Citrix Desktop Viewer (CDViewer.exe) 窗口消失时，尝试重新连接到 Linux VDA 可能会失败。[CVADHELP-16239]
- 在 Linux VDA 中，某些应用程序可能无法识别出现在设备选项中的网络摄像机设备。[CVADHELP-16247]
- 在 Linux VDA 会话中为网络摄像机使用 USB 重定向时，`ctxusbdsd` 进程可能会意外退出，并提示 `segfault` 错误。[CVADHELP-16366]
- `ctxcmd` 进程可能无法在正确的 SELinux 安全上下文中运行。[CVADHELP-16381]
- 配置到 Linux VDA 时，智能卡可能无法正常工作。[CVADHELP-16488]
- 出现在 Linux VDA 会话中的文本可能会变形且模糊不清。[CVADHELP-17199]

累积更新 2 (CU2)

January 26, 2022

发布日期：2020 年 11 月 19 日

关于此版本

Linux Virtual Delivery Agent 1912 LTSR 累积更新 2 (CU2) 修复了自 1912 LTSR CU1 发布以来报告的五个问题。

[Linux Virtual Delivery Agent 1912 LTSR 累积更新 1 \(CU1\)](#)

[Linux Virtual Delivery Agent 1912 LTSR \(初始版本\)](#)

[此版本中的已知问题](#)

[弃用和删除](#)

1912 LTSR CU2 中已修复的问题

January 26, 2022

自 Linux Virtual Delivery Agent 1912 LTSR CU1 起，以下问题已修复：

- 启用 LDAP 签名后，尝试向 Delivery Controller 注册 Linux VDA 可能会失败。[CVADHELP-14481]
- 尝试启动 VDA 可能会导致灰屏。此问题是 HDX 用户策略验证超时的结果。当存在许多 LDAP 服务器并且 VDA 无法访问一个或多个服务器时，可能会发生超时。[CVADHELP-14746]
- Linux VDA 可能只识别客户端 **USB** 设备重定向规则，这是 HDX 策略设置中最顶层的规则。其他规则将被放弃。[CVADHELP-14971]
- 在无缝模式下启动已发布的应用程序时，已发布的应用程序始终位于顶部，显示在本地应用程序上。仅当最小化已发布的应用程序时，才能将本地应用程序置于前台。[CVADHELP-15134]
- 登录到 Machine Creation Services (MCS) 创建的 Ubuntu 虚拟机时，某些文件（例如.bashrc 和.profile）可能不会按预期自动复制到主文件夹。[CVADHELP-15306]
- 在运行 Ubuntu 的 Linux VDA 上安装了 NVIDIA GRID 图形卡后，尝试调整会话大小时，会话可能会意外退出。[CVADHELP-15664]
- 将区域设置更改为非英语语言可能会导致性能计数器无法将字符串值转换为数字值，并在 VDA 日志中生成以下错误。
[PerfCounter] [Error] SysStat.ReadUpTime: Converting element '29363.68' resulted in a NumberFormatException. Error: Input string was not in a correct format.（错误：输入字符串的格式不正确。）
[CVADHELP-15767]

累积更新 1 (CU1)

November 21, 2020

发布日期：May 7, 2020

关于此版本

Linux Virtual Delivery Agent 1912 LTSR 累积更新 1 (CU1) 修复了自首次发布 1912 LTSR 以来报告的八个以上的问题。

[Linux Virtual Delivery Agent \(初始版本\)](#)

[此版本中的已知问题](#)

[弃用和删除](#)

[Citrix 产品专享升级服务资格日期](#)

1912 LTSR CU1 中已修复的问题

January 26, 2022

自 Linux Virtual Delivery Agent 1912 LTSR 初始版本起，以下问题已修复：

- Linux VDA 可能无法显示已登录用户的列表。[CVADHELP-13659]
- 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]
- 将 Linux VDA 更新到版本 1909 或 1912 后，可能需要很长时间才能初始化。[CVADHELP-13802]
- 使用 Quest Authentication Services 的 Linux VDA 可能无法向 Delivery Controller 注册。使用 Linux VDA 版本 1909、1912 LTSR 初始版本和 2003 时会出现此问题。[CVADHELP-14027]
- Linux VDA 可能无法达到 **Target frame rate** (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]
- 重新启动系统后，**ctxjproxy** 服务可能找不到 LDAP 服务器。[CVADHELP-14269]
- Linux VDA 可能无法向 Delivery Controller 注册。当 Linux VDA 与 Delivery Controller 通信时使用的端口不是 80 时会出现此问题。[CVADHELP-14270]
- 安装 Linux VDA 时，可能无法验证 .NET Core 运行时脚本以进行身份验证。[CVADHELP-14424]

关于此版本

May 12, 2020

新增功能

1912 LTSR 中的新增功能

Linux VDA 1912 版包括以下新增功能和增强功能：

在 **AWS** 平台上支持 **MCS**

可以使用 Machine Creation Services (MCS) 在 AWS 平台上创建 Linux VM。有关详细信息，请参阅[使用 MCS 创建 Linux VM](#)。

当前正在运行的 **VDA** 可用作模板

使用 MCS 创建 Linux VM 时，可以使用当前正在运行的 VDA 作为模板，并继承其所有的现有配置。此正在运行的 VDA 可以手动安装，也可以使用轻松安装功能。有关详细信息，请参阅[使用 MCS 创建 Linux VM](#)。

客户端驱动器映射：支持大型文件传输

客户端驱动器映射现在支持在 Linux VDA 与客户端设备之间传输大小为 4 GB 及更大的文件。此增强功能要求您的客户端运行适用于 Windows 的 Citrix Workspace 应用程序 1808 或更高版本。

注意：

此版本将所有支持的发行版上的 OpenJDK 更新到版本 1.8.0。

1912 LTSR 中已修复的问题

January 26, 2022

自 Linux Virtual Delivery Agent 1909 起，以下问题已修复：

- 在 4K 显示器上，您可能会遇到与击键和刷新率相关的 GPU 性能问题。[CVADHELP-12661]
- 如果鼠标和键盘的焦点不在同一窗口上或者鼠标无法更改焦点，Linux VDI 会话可能会变得无响应。[CVADHELP-12768]
- 使用仅使用 IPv6 地址的虚拟机 (VM) 时，Linux VDA 注册可能会失败。[CVADHELP-13103]
- 将策略设置为默认时，Linux VDA 可能不会更新数据库。出现此问题是因为较高优先级的策略不能重置设置为默认的较低优先级的策略。[CVADHELP-13107]

- 启用本地键盘布局功能后，键盘布局同步可能无法在客户端匈牙利语言环境中运行。使用 **DE** 作为本地设置启动应用程序时，语言将同步，但不适用于匈牙利语布局。[CVADHELP-13199]
- 配置 **Xauthority** 以保护 XClient 与 XServer 之间的通信安全时，将仅添加 IPv4 地址。不会添加 IPv6 地址。[CVADHELP-13255]
- 在 Ubuntu 18.04 上，尝试使用 Machine Creation Services (MCS) 创建或更新计算机目录可能会失败。[CVADHELP-13178]

已知问题

July 14, 2023

在本版本中确定了以下问题：

- 已发布的非无缝应用程序可能会在启动后不久退出。Mutter 升级高于 mutter-3.28.3-4 的版本后会出现此问题。要解决此问题，请使用 mutter-3.28.3-4 或更早版本。[LNXVDA-6967]
- 当您使用 NVIDIA GRID 3D 卡但不启用 HDX 3D Pro 时，Linux VDA 不按预期运行。RHEL 7.5 及更早版本、SUSE 12.3 及更早版本和 Ubuntu 16.04 上会出现此问题。原因是多个 OpenGL 库不能在这些 Linux 发行版的图形系统中共存。
- 文件下载过程中出现意外窗口。该窗口不会影响文件下载功能，并且在一段时间后会自动消失。[LNXVDA-5646]
- PulseAudio 的默认设置会导致正常运行的服务器程序在处于不活动状态 20 秒后退出。当 PulseAudio 退出时，音频将不起作用。要解决此问题，请在 /etc/pulse/daemon.conf 文件中设置 exit-idle-time=-1。[LNXVDA-5464]
- SUSE 12.3 中的 **libtcmalloc** 4.3.0 可能会导致进程意外退出。
- 在 Ubuntu 16.04 和 SUSE 12.3 VDA 上，**ctxhdx** 服务可能会意外退出。此问题会在 GNU C 库 (**glibc**) 2.22 到 2.24 版中出现。该问题已在 **glibc** 2.25 中修复。如果要使用 SUSE 12.3 发行版，可以安装 SUSE 提供的 **修补程序** 以修复此问题。发布 Linux VDA 7.17 时，没有适用于 Ubuntu 16.04 的修补程序。[LNXVDA-4481]
- 启用了 SSL 加密并且禁用了会话可靠性时，无法在适用于 Linux 的 Citrix Workspace 应用程序中启动会话。[RFLNX-1557]
- **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。
- 适用于 Android 的 Citrix Workspace 应用程序的 CapsLock 键状态可能会在会话漫游期间反转。漫游与适用于 Android 的 Citrix Workspace 应用程序的现有连接时，Caps Lock 键状态可能会丢失。解决方法：使用扩展键盘上的 Shift 键在大写与小写之间切换。
- 使用适用于 Mac 的 Citrix Workspace 应用程序连接至 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，适用于 Mac 的 Citrix Workspace 应用程序都会发送 AltGr。您可以在 Citrix Workspace 应用程序设置中修改此行为，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。
- 适用于 Windows 的 Citrix Workspace 应用程序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 Delivery Agent 1912 LTSR](#) (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。

弃用

November 8, 2021

本文声明旨在提前通知您正在逐渐淘汰的平台、Citrix 产品和功能，以便您能够及时制定业务决策。Citrix 将监视客户使用情况和反馈以确定其退出时间。在后续版本中声明可能会有更改，可能不会包括每个弃用的特性或功能。有关产品生命周期支持的详细信息，请参阅 [Product Lifecycle Support Policy](#)（产品生命周期支持策略）一文。

弃用和删除

下表显示了已弃用或删除的平台、Citrix 产品和功能。

已弃用的项目不会立即删除。Citrix 在此版本中继续支持这些项目，但将在未来的当前版本中将其删除。在 Linux VDA 中，已删除的项目已被删除或不再受支持。

项目	宣布弃用的版本	删除版本
支持 RHEL 6.9	1909	1909
支持 RHEL7.5、CentOS 7.5	1903	1903
支持 RHEL7.4、CentOS 7.4	1811	1811
支持 RHEL 6.8	1811	1811
支持 RHEL 7.3、CentOS 7.3	7.18	7.18
支持 RHEL 6.6	7.16	7.16
SUSE 11.4	7.16	7.16

系统要求

January 26, 2022

Linux 发行版

注意：

本档中未涉及的组件（例如 Citrix Workspace 应用程序）的系统要求在其各自的文档集中进行说明。

自 CU3 版本起，请先安装 .NET Core 运行时 3.1 作为必备项，然后再安装 Linux VDA。有关详细信息，请参阅

<https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>。

Linux VDA 不支持使用 SecureICA 进行加密。在 Linux VDA 上启用 SecureICA 会导致会话启动失败。

有关在长期服务版本 (LTSR) 环境中使用当前版本 (CR) 以及其他常见问题解答的信息，请参阅[知识中心文章](#)。

Linux VDA 支持以下 Linux 发行版：

重要提示：

当操作系统供应商提供的支持过期时，Citrix 解决问题的能力可能会受到限制。

对于已弃用或已删除的平台，请参阅[弃用](#)。

- SUSE Linux Enterprise:
 - Desktop 12 Service Pack 3
 - Server 12 Service Pack 3
- Red Hat Enterprise Linux
 - Workstation 7.7
 - Workstation 6.10
 - Server 7.7
 - Server 6.10
- CentOS Linux
 - CentOS 7.7
 - CentOS 6.10
- Ubuntu Linux
 - Ubuntu Desktop 18.04
 - Ubuntu Server 18.04
 - Ubuntu Live Server 18.04
 - Ubuntu Desktop 16.04
 - Ubuntu Server 16.04
- Pardus Linux
 - Pardus 17 (有关受支持功能范围的信息，请参阅[知识中心文章 CTX238492](#)。)

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 7.7、CentOS 7.7	1.20

Linux 发行版	Xorg 版本
RHEL 6.10、CentOS 6.10	1.17
Ubuntu 18.04	1.19
Ubuntu 16.04	1.18
SUSE 12.3	1.18
Pardus 17	1.19

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：

- 如果您在 CentOS 7.4 上安装了 Linux VDA 1912 LTSR 累积更新 2 (CU2)，并希望将其与 Citrix Virtual Apps and Desktops 服务一起使用，请务必先安装以下组件，然后再安装 VDA：
 - Xorg 1.20.4
 - SELinux policy 3.13.1-268
 - .NET Core Runtime 2.1
 - GNOME 3.28.3 or later
- Gnome 和 KDE 桌面在 SUSE、RHEL 和 CentOS 中受支持。只有 Ubuntu 16.04 支持 Unity 桌面。Gnome 桌面在 Ubuntu 18.04 中受支持。至少必须安装一种桌面。

Citrix Virtual Desktops

Linux VDA 与当前所有受支持的 Citrix Virtual Desktops 版本兼容。要获取有关 Citrix Virtual Desktops 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。

支持的主机平台和虚拟化环境

- 裸机服务器
- Citrix Hypervisor
- VMware ESX 和 ESXi
- Microsoft Hyper-V
- Nutanix AHV
- Microsoft Azure Resource Manager

- Amazon Web Services (AWS)
- Google 云端平台 (GCP)

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
- PBIS (与 RHEL 7 和 Ubuntu 兼容)

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

借助 Citrix Virtual Apps and Desktops 中的 HDX 3D Pro 功能，您可以交付使用图形处理器 (GPU) 进行硬件加速实现最佳性能的桌面和应用程序。

虚拟机管理程序

对于 Linux VDA，HDX 3D Pro 与以下虚拟机管理程序提供的 GPU 直通和 GPU 虚拟化技术兼容：

- Citrix Hypervisor
- VMware ESX 和 ESXi
- Nutanix AHV

注意

：虚拟机管理程序与某些 Linux 发行版兼容。

GPU

要了解您的 Linux 发行版支持的 NVIDIA GPU 卡，请转到 [NVIDIA 产品支持列表](#)，然后查看虚拟机管理程序或裸机操作系统、软件产品部署、硬件支持和来宾操作系统支持列。确保为 GPU 卡安装了最新的 vGPU 驱动程序。有关详细信息，请参阅 [NVIDIA 虚拟 GPU 软件支持的 GPU](#)。

下面是我们针对 GPU 直通和 GPU 虚拟化支持测试过的 GPU 卡。

我们已针对 GPU 直通测试过的 GPU:

- NVIDIA GRID - Tesla T4
- NVIDIA GTX750Ti
- NVIDIA GRID - Tesla M60
- NVIDIA GRID - K2
- NVIDIA GRID - Tesla P40
- NVIDIA GRID - Tesla P4
- NVIDIA GRID - Tesla P100

我们已针对 vGPU 测试过的 GPU:

- NVIDIA GRID - Tesla T4
- NVIDIA GRID - Tesla V100
- NVIDIA GRID - Tesla M60
- NVIDIA GRID - Tesla M10
- NVIDIA GRID - Tesla P40
- NVIDIA GRID - Tesla P4
- NVIDIA GRID - Tesla P100

安装概述

September 30, 2021

此部分将指导您完成以下过程:

- 使用轻松安装进行快速安装 (推荐, 适用于全新安装)
- 基于各种 Linux 发行版的手动安装
- 使用 MCS 创建 Linux VM
- 为 XenDesktop 7.6 及早期版本配置 Delivery Controller

使用轻松安装进行快速安装 (推荐)

March 9, 2023

重要提示：

对于全新安装，建议您参阅本文以进行快速安装。本文将分步介绍如何使用轻松安装来安装和配置 Linux VDA。轻松安装省时又省力，与手动安装相比，更不易于出错。它可以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	PBIS
RHEL 7.7	是	是	是	是
RHEL 6.10	是	是	是	否
CentOS 7.7	是	是	是	是
CentOS 6.10	是	是	是	否
Ubuntu 18.04	是	是	是	是
Ubuntu 16.04	是	是	是	是
SUSE 12.3	是	否	是	否

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 Virtual Apps and Desktops 下载页面](#)。展开适当版本的 Citrix Virtual Apps and Desktops。单击组件下载与您的 Linux 发行版匹配的 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
- 域的完全限定域名 (FQDN)

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。

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=<your workgroup>” 行添加到文件中并保存您所做的更改。
- 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。

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 Centrify 及其配置独有的。要解决此问题，请执行以下操作:

- a. 在域控制器上打开管理工具。
 - b. 选择 **Active Directory** 站点和服务。
 - c. 为子网添加正确的子网地址。
- 自 Linux VDA 7.16 起，轻松安装支持纯 IPv6。以下先决条件和限制适用：
 - 必须配置您的 Linux 存储库，以确保您的计算机可以通过纯 IPv6 网络下载所需软件包。
 - 在纯 IPv6 网络中不支持 Centrify。

注意:

如果您的网络是纯 IPv6，并且所有输入均采用恰当的 IPv6 格式，VDA 将通过 IPv6 向 Delivery Controller 注册。如果您的网络具有混合 IPv4 和 IPv6 配置，第一个 DNS IP 地址的类型将决定是使用 IPv4 还是使用 IPv6 来注册。

- 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 URL：
RHEL: wget http://edge.centrixy.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.centriify.com/products/centriify-suite/2016-update-1/installers/centriify-suite-2016.1-rhel4-x86_64.tgz?_ga=1.186648044.558673738.1478847956`

SUSE: `wget http://edge.centriify.com/products/centriify-suite/2016-update-1/installers/centriify-suite-2016.1-suse10-x86_64.tgz?_ga=1.10831088.558673738.1478847956`

Ubuntu: `wget http://edge.centriify.com/products/centriify-suite/2016-update-1/installers/centriify-suite-2016.1-deb7-x86_64.tgz?_ga=1.178323680.558673738.1478847956`

- 从本地目录中提取 Centriify 软件包。要指定 Centriify 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
        centriifyda-3.3.1-rhel4-x86_64.rpm
6      33492 -r--r--r--. 1 root root 34292673 May 13 2016
        centriifydc-5.3.1-rhel4-x86_64.rpm
7      4 -rw-rw-r--. 1 root root 1168 Dec 1 2015
        centriifydc-install.cfg
8      756 -r--r--r--. 1 root root 770991 May 13 2016
        centriifydc-ldaproxy-5.3.1-rhel4-x86_64.rpm
9      268 -r--r--r--. 1 root root 271296 May 13 2016
        centriifydc-nis-5.3.1-rhel4-x86_64.rpm
10     1888 -r--r--r--. 1 root root 1930084 Apr 12 2016
        centriifydc-openssh-7.2p2-5.3.1-rhel4-x86_64.rpm
11     124 -rw-rw-r--. 1 root root 124543 Apr 19 2016
        centriify-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-->
```

- 如果选择 PBIS 作为加入域的方法，`ctxinstall.sh` 脚本需要 PBIS 软件包。`ctxinstall.sh` 获取 PBIS 软件包的方法有两种：

- 轻松安装可帮助自动从 Internet 下载 PBIS 软件包。下面是每个发行版的 URL：

RHEL 7/CentOS 7: `wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh`

Ubuntu: `wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh`

- 从 Internet 获取 PBIS 软件包的特定版本。为此，请更改 `/opt/Citrix/VDA/sbin/ctxinstall.sh` 文件中的行 “`pbisDownloadPath`”，以指定 PBIS 软件包的 URL。

有关示例，请参阅以下屏幕截图：

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 Hypervisor 上的时间同步问题

启用了 Citrix Hypervisor 时间同步功能时，在每个半虚拟化 Linux VM 中，您会发现 NTP 和 Citrix Hypervisor 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 Citrix VM Tools，您可以检查 Citrix Hypervisor 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/independent_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 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 Citrix Hypervisor 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：安装必备软件 **.NET Core Runtime**

在安装 Linux VDA 之前，请按照 <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers> 上的说明安装 .NET Core Runtime。

- 对于 1912 LTSR 初始版本 CU1 和 CU2，请安装 .NET Core Runtime 2.1。

- 对于 CU3 及更高版本，请安装 .NET Core Runtime 3.1。

安装 .NET Core Runtime 后，请运行 `which dotnet` 命令以找到您的运行时路径。

根据命令输出，设置 .NET Core Runtime 二进制文件路径。例如，如果命令输出为 `/aa/bb/dotnet`，请使用 `/aa/bb` 作为 .NET 二进制文件路径。

步骤 4：下载 **Linux VDA** 软件包

转至 [Citrix Virtual Apps and Desktops 下载页面](#)。展开相应版本的 Citrix Virtual Apps and Desktops，然后单击组件以下载与 Linux 发行版匹配的 Linux VDA 包。

步骤 5：安装 **Linux VDA** 软件包

要为 Linux VDA 设置环境，请运行以下命令。

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 6：安装 **NVIDIA GRID** 驱动程序

启用 HDX 3D Pro 要求您在虚拟机管理程序和 VDA 计算机上安装 NVIDIA GRID 驱动程序。

要在特定虚拟机管理程序上安装和配置 NVIDIA GRID 虚拟 GPU 管理器（主机驱动程序），请参阅以下指南：

- [Citrix Hypervisor](#)
- [VMware ESX](#)

要安装和配置 NVIDIA GRID 来宾 VM 驱动程序，请执行下面的常规步骤：

1. 确保来宾 VM 已关闭。
2. 在虚拟机管理程序控制面板中，为 VM 分配一个 GPU。
3. 启动 VM。
4. 在 VM 上安装来宾 VM 驱动程序。

步骤 7：设置运行时环境以完成安装

注意：

在设置运行时环境之前，请确保已在操作系统中安装了 `en_US.UTF-8` 区域设置。如果该区域设置在您的操作系统中不可用，请运行 `sudo locale-gen en_US.UTF-8` 命令。

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。

注意：

下载 .NET Core Runtime（该运行时大小超过 27 MB）时，轻松安装可能看起来没有响应。检查 `/var/log/ctx-install.log` 中的下载进度。

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-ntp** - 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 | pbis** - 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。

`ctxsetup.sh` 脚本使用以下变量：

- **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 VDA 服务。
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** - Linux VDA 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 VDA 打开所需端口（默认端口 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_FAS_LIST=' list-fas-servers'** - 联合身份验证服务 (FAS) 服务器是通过 AD 组策略配置的。Linux VDA 不支持 AD 组策略，但您可以改为提供以分号分隔的 FAS 服务器的列表。顺序必须与在 AD 组策略中配置的顺序相同。如果删除了任何服务器地址，请使用 **<none>** 文本字符串填充其空白，并且不要修改服务器地址的顺序。
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** - 安装 .NET Core Runtime 支持新的 Broker 代理服务 (ctxvda) 的路径。默认路径为 /usr/bin。
- **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。通过环境变量设置了所有参数时，ctxinstall.sh 脚本仍会提示用户输入安装 .NET Core Runtime 的路径。

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 |
    pbis
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_FAS_LIST='list-fas-servers' | '<none>'
40
41 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
42
43 export CTX_XDL_START_SERVICE=Y | N
44
45 sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh
46 <!--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。我们建议您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_FAS_LIST='list-fas-servers' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_START_SERVICE=Y|N \
28
29 /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--NeedCopy-->
```

步骤 8: 运行 XDPing

我们提供了一个命令行实用程序，即 Linux XDPing 工具，用于检查 Linux VDA 环境中的常见配置问题。可以在运行受支持的 Linux 发行版的任何计算机上安装 XDPing 软件包。XDPing 不需要在计算机上安装 Linux VDA 软件包。有关该工具的详细信息，请参阅知识中心文章 [CTX202015](#)。

步骤 9: 运行 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-->
```

注意:

在停止 `ctxvda` 和 `ctxhdx` 服务之前，请运行 `service ctxmonitorservice stop` 命令以停止监视服务守护程序。否则，监视服务守护程序将重新启动您停止的服务。

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 10：在 **Citrix Virtual Apps** 或 **Citrix Virtual Desktops** 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：
 - 多会话操作系统选项（对于托管共享桌面交付模型）。
 - 单会话操作系统选项（对于 VDI 专用桌面交付模型）。
- 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 11：在 **Citrix Virtual Apps** 或 **Citrix Virtual Desktops** 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：

- 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。

有关如何创建计算机目录和交付组的信息，请参阅 [Citrix Virtual Apps and Desktops 7 1912 LTSR](#)。

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，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，尝试启动 **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-->

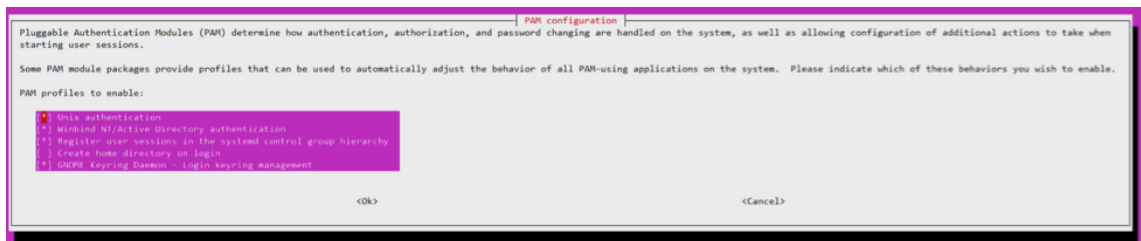
```

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. 在生成的对话框中，确认是否已选中 **Create home directory login**（创建主目录登录信息）。



会话不启动，也不快速结束并显示 **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，我们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。

手动安装 **Linux Virtual Delivery Agent for RHEL/CentOS**

June 21, 2022

重要提示：

对于全新安装，建议您使用[轻松安装](#)以进行快速安装。轻松安装省时又省力，与本文中详述的手动安装相比，更不易于出错。

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

确保已连接并正确配置网络。例如，必须在 Linux VDA 上配置 DNS 服务器。

步骤 1b: 设置主机名

要确保正确报告计算机的主机名，请更改 `/etc/hostname` 文件（适用于 RHEL 7 和 CentOS 7）或 `/etc/sysconfig/network` 文件（适用于 RHEL 6 和 CentOS 6），以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 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。

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：

```
1 sudo yum info java-1.8.0-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：

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

打开新的 shell，然后确认 Java 版本：

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

提示：

为避免在 Delivery Controller 中注册失败，请务必仅安装 OpenJDK 1.8.0。从系统中删除所有其他版本的 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 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 Hypervisor 上的时间同步问题

启用了 Citrix Hypervisor 时间同步功能时，在每个半虚拟化 Linux VM 中，您会发现 NTP 和 Citrix Hypervisor 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 Citrix VM Tools，您可以检查 Citrix Hypervisor 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/independent_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 Citrix Hypervisor 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 Services](#)

- [Centrify DirectControl](#)
- [SSSD](#)
- [PBIS](#) (仅与 RHEL 7 兼容)

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：

```
--enablekrb5kdc dns --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。

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，请验证系统 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，请使用以前未使用的域用户帐户登录 Linux VDA。

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

验证 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 6：安装 Linux VDA](#)。

Quest Authentication Services

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 是否能够通过 PAM 对域用户进行身份验证, 请使用以前未使用的域用户帐户登录 Linux VDA。

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

验证是否为 `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-->
```

验证 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 6: 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 adinfo
3 <!--NeedCopy-->
```

验证 `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 adinfo -diag
3 <!--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 6: 安装 Linux VDA](#)。

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. 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[LDAP 提供程序配置 Active Directory](#) 中提供的说明进行操作。

使用本文中包含的说明时，以下环境已通过测试和验证：

- RHEL 7.7 及更高版本
- CentOS 7.7 及更高版本

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` 或 `Samba`。

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

安装或更新所需软件包：

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

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：

```
--enablekrb5kdc dns --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** 是拥有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/sss/sss.conf
chmod 0600 /etc/sss/sss.conf
restorecon /etc/sss/sss.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 验证系统 **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, 请使用以前未使用的域用户帐户登录 Linux VDA。

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

验证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-->
```

验证用户的 Kerberos 凭据缓存中的票据是否有效且未过期。

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

在进行域加入验证后继续执行 [步骤 6: 安装 Linux VDA](#)。

PBIS

下载所需的 **PBIS** 软件包 例如:

```
1 wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/
   pbis-open-8.8.0.506.linux.x86_64.rpm.sh
2 <!--NeedCopy-->
```

使 **PBIS** 安装脚本可执行 例如:

```
1 chmod +x pbis-open-8.8.0.506.linux.x86_64.rpm.sh
2 <!--NeedCopy-->
```

运行 **PBIS** 安装脚本 例如:

```
1 sh pbis-open-8.8.0.506.linux.x86_64.rpm.sh
2 <!--NeedCopy-->
```

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 /opt/pbis/bin/domainjoin-cli join domain-name user
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。

注意：要将 Bash 设置为默认 shell，请运行 **/opt/pbis/bin/config LoginShellTemplate/bin/bash** 命令。

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。验证加入了 PBIS 的 Linux 计算机是否位于域中：

```
1 /opt/pbis/bin/domainjoin-cli query
2 <!--NeedCopy-->
```

如果计算机已加入某个域，此命令将返回有关当前加入的 AD 域和 OU 的信息。否则，仅显示主机名。

验证用户身份验证 要验证 PBIS 是否能够通过 PAM 对域用户进行身份验证，请使用以前未使用的域用户帐户登录 Linux VDA。

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

验证是否为 **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-->
```

退出会话。

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

在进行域加入验证后继续执行 [步骤 6: 安装 Linux VDA](#)。

步骤 4: 安装必备软件.NET Core Runtime

在安装 Linux VDA 之前，请按照 <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers> 上的说明安装 .NET Core Runtime。

- 对于 1912 LTSR 初始版本 CU1 和 CU2，请安装 .NET Core Runtime 2.1。
- 对于 CU3 及更高版本，请安装 .NET Core Runtime 3.1。

安装 .NET Core Runtime 后，请运行 **which dotnet** 命令以找到您的运行时路径。

根据命令输出，设置 .NET Core Runtime 二进制文件路径。例如，如果命令输出为 `/aa/bb/dotnet`，请使用 `/aa/bb` 作为 .NET 二进制文件路径。

步骤 5：下载 **Linux VDA** 软件包

转至 [Citrix Virtual Apps and Desktops 下载页面](#)。展开相应版本的 Citrix Virtual Apps and Desktops，然后单击组件以下载与 Linux 发行版匹配的 Linux VDA 包。

步骤 6：安装 **Linux VDA**

可以执行全新安装或从先前的两个版本和 LTSR 版本升级现有安装。

执行全新安装

1. (可选) 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。

a) 停止 Linux VDA 服务：

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

注意：

在停止 `ctxvda` 和 `ctxhdx` 服务之前，请运行 `service ctxmonitorservice stop` 命令以停止监视服务守护程序。否则，监视服务守护程序将重新启动您停止的服务。

b) 卸载软件包：

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

注意：

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。

2. 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-19.12.0.50-1.el7_x.x86_64.  
rpm  
2 <!--NeedCopy-->
```

对于 **RHEL 6/CentOS 6**:

```
1 sudo yum install -y XenDesktopVDA-19.12.0.50-1.el6_x.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-19.12.0.50-1.el7_x.x86_64.rpm  
2 <!--NeedCopy-->
```

对于 **RHEL 6/CentOS 6**:

```
1 sudo rpm -i XenDesktopVDA-19.12.0.50-1.el6_x.x86_64.rpm  
2 <!--NeedCopy-->
```

RHEL 7/CentOS 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 rpmlib(FileDigests) <= 4.6.0-1
58
59 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
60
61 rpmlib(CompressedFileNames) <= 3.0.4-1
62
63 rpmlib(PayloadIsXz) <= 5.2-1
64 <!--NeedCopy-->
```

注意：

有关此版本的 Linux VDA 支持的 Linux 发行版和 Xorg 版本的列表，请参阅[系统要求](#)。

RHEL 6/CentOS 6 的 RPM 依赖项列表：

```
1 postgresql-jdbc >= 8.4
2
3 postgresql-server >= 8.4
4
5 java-1.8.0-openjdk >= 1.8.0
6
7 ImageMagick >= 6.5.4.7
8
9 GConf2 >= 2.28.0
10
11 system-config-firewall-base >= 1.2.27
```

```
12
13  polycoreutils-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  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-->
```

注意：

在 RHEL 7.x 上安装 Linux VDA 后，运行 `sudo yum install -y python-websocketify x11vnc` 命令。目的是手动安装 `python-websocketify` 和 `x11vnc` 以使用会话重影功能。有关详细信息，请参阅[重影会话](#)。

升级现有安装

可以从之前的两个版本和 LTSR 版本升级现有安装。

- 要使用 Yum 升级您的软件，请执行以下操作：

对于 **RHEL 7/CentOS 7**：

```
1  sudo yum install -y XenDesktopVDA-19.12.0.50-1.el7_x.x86_64.rpm
2  <!--NeedCopy-->
```

对于 **RHEL 6/CentOS 6**：

```
1  sudo yum install -y XenDesktopVDA-19.12.0.50-1.el6_x.x86_64.rpm
2  <!--NeedCopy-->
```

- 要使用 RPM 软件包管理器升级您的软件，请执行以下操作：

对于 **RHEL 7/CentOS 7**：

```
1  sudo rpm -U XenDesktopVDA-19.12.0.50-1.el7_x.x86_64.rpm
2  <!--NeedCopy-->
```

对于 **RHEL 6/CentOS 6**：

```
1  sudo rpm -U XenDesktopVDA-19.12.0.50-1.el6_x.x86_64.rpm
2  <!--NeedCopy-->
```

重要：

升级软件后重新启动 Linux VDA 计算机。

步骤 7：安装 NVIDIA GRID 驱动程序

启用 HDX 3D Pro 要求您在虚拟机管理程序和 VDA 计算机上安装 NVIDIA GRID 驱动程序。

要在特定虚拟机管理程序上安装和配置 NVIDIA GRID 虚拟 GPU 管理器（主机驱动程序），请参阅以下指南：

- [Citrix Hypervisor](#)
- [VMware ESX](#)

要安装和配置 NVIDIA GRID 来宾 VM 驱动程序，请执行以下步骤：

1. 确保来宾 VM 已关闭。
2. 在 XenCenter 中，为 VM 分配一个 GPU。
3. 启动 VM。
4. 为 NVIDIA GRID 驱动程序准备 VM：

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

5. 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 8: 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 | 5** -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 Services
 - 3 - Centrify DirectControl
 - 4 - SSSD
 - 5 -PBIS
- **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_FAS_LIST= 'list-fas-servers'** -联合身份验证服务 (FAS) 服务器是通过 AD 组策略配置的。由于 Linux VDA 不支持 AD 组策略, 您可以改为提供以分号分隔的 FAS 服务器的列表。顺序必须与在 AD 组策略中配置的顺序相同。如果删除了任何服务器地址, 则使用 **<none>** 文本字符串填充空白处, 并使服务器地址的顺序保持不变。
 - **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** - 安装 .NET Core Runtime 支持新的 Broker 代理服务 (ctxvda) 的路径。默认路径为 /usr/bin。
 - **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|5
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-site-name | '<none>'

```

```
18
19 export CTX_XDL_LDAP_LIST= 'list-ldap-servers' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST= 'list-fas-servers' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_START_SERVICE=Y|N
28
29 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--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|5 \
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_FAS_LIST= 'list-fas-servers' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_START_SERVICE=Y|N \
28
29 /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--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 9：运行 XDPing

我们提供了一个命令行实用程序，即 Linux XDPing 工具，用于检查 Linux VDA 环境中的常见配置问题。您可以在运行受支持的 Linux 发行版的任何计算机上安装 XDPing 软件包。XDPing 不要求在计算机上安装 Linux VDA 软件包。有关该工具的详细信息，请参阅知识中心文章 [CTX202015](#)。

步骤 10：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-->
```

注意：

在停止 `ctxvda` 和 `ctxhdx` 服务之前，请运行 `service ctxmonitorservice stop` 命令以停止监视服务守护程序。否则，监视服务守护程序将重新启动您停止的服务。

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 11：在 Citrix Virtual Apps 或 Citrix Virtual Desktops 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：
 - 多会话操作系统选项（对于托管共享桌面交付模型）。
 - 单会话操作系统选项（对于 VDI 专用桌面交付模型）。
- 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 12：在 **Citrix Virtual Apps** 或 **Citrix Virtual Desktops** 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：

- 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。

有关如何创建计算机目录和交付组的信息，请参阅 [Citrix Virtual Apps and Desktops 7 1912 LTSR](#)。

手动安装 **Linux Virtual Delivery Agent for SUSE**

June 21, 2022

重要提示：

对于全新安装，建议您使用[轻松安装](#)以进行快速安装。轻松安装省时又省力，与本文中详述的手动安装相比，更不易于出错。

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）验证 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 12: 9.3 版或更高版本
- OpenJDK 1.8.0
- Open Motif Runtime Environment 2.3.1 或更高版本
- Cups
 - SLED/SLES 12: 1.6.0 版或更高版本
- Foomatic 过滤器
 - SLED/SLES 12: 1.0.0 版或更高版本
- ImageMagick
 - 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 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 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-SP3-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 1.8.0。

提示：

为避免在 Delivery Controller 中注册失败，请务必仅安装 OpenJDK 1.8.0。从系统中删除所有其他版本的 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_8_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_8_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_8_0-openjdk
2 <!--NeedCopy-->
```

2. 检查 Java 版本：

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

安装 **PostgreSQL** 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 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/sdk
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 Hypervisor** 上的时间同步问题

如果启用了 Citrix Hypervisor 时间同步功能，则在每个半虚拟化 Linux VM 中，您会发现 NTP 和 Citrix Hypervisor 都在尝试管理系统时钟。为避免时钟与其他服务器不同步，请将每个 Linux 来宾中的系统时钟与 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 Citrix VM Tools，您可以检查 Citrix Hypervisor 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/independent_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 reboot
2 <!--NeedCopy-->
```

重新启动后，验证此设置是否正确：

```
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，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 Citrix Hypervisor 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 Services](#)
- [Centrify DirectControl](#)

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

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. 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）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，请验证系统 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，请使用以前未使用的域用户帐户登录 Linux VDA。

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

验证是否为 `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-->
```

验证用户的 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 6: 安装 Linux VDA](#)。

Quest Authentication Services

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) 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 是否能够通过 PAM 对域用户进行身份验证, 请使用以前未使用的域用户帐户登录 Linux VDA。

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

验证是否为 `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-->
```

验证 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 6: 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 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-->
```

验证 **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 6: 安装 Linux VDA](#)。

步骤 4: 安装必备软件.NET Core Runtime

在安装 Linux VDA 之前，请按照 <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers> 上的说明安装.NET Core Runtime。

- 对于 1912 LTSR 初始版本 CU1 和 CU2，请安装.NET Core Runtime 2.1。
- 对于 CU3 及更高版本，请安装.NET Core Runtime 3.1。

安装.NET Core Runtime 后，请运行 `which dotnet` 命令以找到您的运行时路径。

根据命令输出，设置 .NET Core Runtime 二进制文件路径。例如，如果命令输出为 /aa/bb/dotnet，请使用 /aa/bb 作为 .NET 二进制文件路径。

步骤 5：下载 **Linux VDA** 软件包

转至 [Citrix Virtual Apps and Desktops 下载页面](#)。展开相应版本的 Citrix Virtual Apps and Desktops，然后单击组件以下载与 Linux 发行版匹配的 Linux VDA 包。

步骤 6：安装 **Linux VDA**

步骤 6a：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-->
```

注意：

在停止 `ctxvda` 和 `ctxhdx` 服务之前，请运行 `service ctxmonitorservice stop` 命令以停止监视服务守护程序。否则，监视服务守护程序将重新启动您停止的服务。

2. 卸载软件包：

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

重要：

支持从最新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 6b：安装 **Linux VDA**

使用 Zypper 安装 Linux VDA 软件：

对于 **SUSE 12**：

```
1 sudo zypper install XenDesktopVDA-19.12.0.50-1.sle12_x.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-19.12.0.50-1.sle12_x.x86_64.rpm
2 <!--NeedCopy-->
```

步骤 **6c**：升级 **Linux VDA**（可选）

可以从先前的两个版本和 LTSR 版本升级现有安装。

对于 **SUSE 12**：

```
1 sudo rpm -U XenDesktopVDA-19.12.0.50-1.sle12_x.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-1.8.0-openjdk >= 1.8.0
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
51 libtcmalloc4 >= 2.5
52
53 libcap-progs >= 2.22
54
55 xorg-x11-server >= 7.6_1.18.3-76.15
56
57 ibus >= 1.5
58 <!--NeedCopy-->
```

重要：

在升级后重新启动 Linux VDA 计算机。

步骤 7：安装 **NVIDIA GRID** 驱动程序

启用 HDX 3D Pro 要求您在虚拟机管理程序和 VDA 计算机上安装 NVIDIA GRID 驱动程序。

要在特定虚拟机管理程序上安装和配置 NVIDIA GRID 虚拟 GPU 管理器（主机驱动程序），请参阅以下指南：

- [Citrix Hypervisor](#)
- [VMware ESX](#)

要安装和配置 NVIDIA GRID 来宾 VM 驱动程序，请执行下面的常规步骤：

1. 确保来宾 VM 已关闭。
2. 在虚拟机管理程序控制面板中，为 VM 分配一个 GPU。
3. 启动 VM。
4. 在 VM 上安装来宾 VM 驱动程序。

步骤 8: 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 Services
 - 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 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_FAS_LIST= 'list-fas-servers'** -联合身份验证服务 (FAS) 服务器是通过 AD 组策略配置的。由于 Linux VDA 不支持 AD 组策略，您可以改为提供以分号分隔的 FAS 服务器的列表。顺序必须与在 AD 组策略中配置的顺序相同。如果删除了任何服务器地址，则使用 **<none>** 文本字符串填充空白处，并使服务器地址的顺序保持不变。
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** - 安装 .NET Core Runtime 支持新的 Broker 代理服务 (ctxvda) 的路径。默认路径为 /usr/bin。
- **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-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST= 'list-ldap-servers' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22

```

```
23 export CTX_XDL_FAS_LIST= 'list-fas-servers' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_START_SERVICE=Y|N
28
29 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--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。我们建议您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_FAS_LIST= 'list-fas-servers' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_START_SERVICE=Y|N \
28
29 /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--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：

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 9：运行 **XDPIing**

我们提供了一个命令行实用程序，即 Linux **XDPIing** 工具，用于检查 Linux VDA 环境中的常见配置问题。您可以在运行受支持的 Linux 发行版的任何计算机上安装 **XDPIing** 软件包。**XDPIing** 不要求在计算机上安装 Linux VDA 软件包。有关该工具的详细信息，请参阅知识中心文章 [CTX202015](#)。

步骤 10：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-->
```

注意：

在停止 `ctxvda` 和 `ctxhdx` 服务之前，请运行 `service ctxmonitorservice stop` 命令以停止监视服务守护程序。否则，监视服务守护程序将重新启动您停止的服务。

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 11： 在 **Citrix Virtual Apps** 或 **Citrix Virtual Desktops** 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：
 - 多会话操作系统选项（对于托管共享桌面交付模型）。
 - 单会话操作系统选项（对于 VDI 专用桌面交付模型）。
- 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 12：在 **Citrix Virtual Apps** 或 **Citrix Virtual Desktops** 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：

- 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。

有关如何创建计算机目录和交付组的信息，请参阅 [Citrix Virtual Apps and Desktops 7 1912 LTSR](#)。

手动安装 **Linux Virtual Delivery Agent for Ubuntu**

June 21, 2022

重要提示：

对于全新安装，建议您使用[轻松安装](#)以进行快速安装。轻松安装省时又省力，与本文中详述的手动安装相比，更不易于出错。

步骤 1：为 **VDA** 安装准备 **Ubuntu**

步骤 1a：验证网络配置

确保已连接并正确配置网络。例如，必须在 Linux VDA 上配置 DNS 服务器。

如果您使用的是 Ubuntu 18.04 Live Server，请在设置主机名之前在 **/etc/cloud/cloud.cfg** 配置文件中做以下更改：

```
preserve_hostname: true
```

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

确保计算机的 DNS 域名和完全限定域名 (FQDN) 正确地返回报告。方法是更改 `/etc/hosts` 文件的以下行以包含 FQDN 和主机名作为前两个条目:

```
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。

在 Ubuntu 16.04 上, 使用以下方法安装 OpenJDK:

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

在 Ubuntu 18.04 上，使用以下方法安装 OpenJDK:

```
1 sudo apt-get install -y openjdk-8-jdk
2 <!--NeedCopy-->
```

步骤 1i: 安装 PostgreSQL

Linux VDA 要求在 Ubuntu 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 1l: 安装以下软件包 (仅限 Ubuntu 18.04)

```
1 sudo apt-get install -y libgtk2.0-0
2 <!--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 Hypervisor 上的时间同步问题

启用了 Citrix Hypervisor 时间同步功能时，在每个半虚拟化 Linux VM 中，您会发现 NTP 和 Citrix Hypervisor 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 Citrix VM Tools，您可以检查 Citrix Hypervisor 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/independent_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 Citrix Hypervisor 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 Services](#)
- [Centrify DirectControl](#)
- [SSSD](#)
- [PBIS](#)

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 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，请验证系统 **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，请使用以前未使用的域用户帐户登录 Linux VDA。

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

注意：

要成功运行 SSH 命令，请确保 SSH 已启用并正常运行。

验证是否为 **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-->
```

验证用户的 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 6：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 Services

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 是否能够通过 PAM 对域用户进行身份验证，请使用以前未使用的域用户帐户登录 Linux VDA。

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

验证是否为 **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-->
```

验证 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 6: 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** 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-->
```

验证 **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-->
```

## 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。

- 如果使用 `adcli` 加入域名，请完成以下步骤：

#### 1. 安装 `adcli`。

```

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

```

#### 2. 使用 `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** 是有权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）。

#### 3. 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。

- 如果使用 `Samba` 加入域名，请完成以下步骤：

### 1. 安装软件包。

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

### 2. 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。

### 3. 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** 是有权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 install --only-upgrade 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
 than 14 days
20
21 krb5_renewable_lifetime = 14d
22
23 # Set krb5_renew_interval to lower value if TGT ticket lifetime is
 shorter than 2 hours
24
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/sss/sss.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。

- 如果使用 `adcli` 验证域成员身份，请运行 `sudo adcli info domain-dns-name` 命令以显示域信息。
- 如果使用 Samba 验证域成员身份，请运行 `sudo net ads testjoin` 命令验证计算机是否已加入到域，运行 `sudo net ads info` 命令验证额外的域和计算机对象信息。

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，请验证系统 `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-->
```

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, 请使用以前未使用的域用户帐户登录 Linux VDA。

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

验证 **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, 验证是否已为前面的 **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 6: 安装 Linux VDA](#)。

## PBIS

下载所需的 **PBIS** 软件包 例如:

```
1 sudo wget https://github.com/BeyondTrust/pbis-open/releases/download
 /8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh
2 <!--NeedCopy-->
```

使 **PBIS** 安装脚本可执行 例如:

```
1 sudo chmod +x pbis-open-8.8.0.506.linux.x86_64.deb.sh
2 <!--NeedCopy-->
```

运行 **PBIS** 安装脚本 例如:



```
1 sudo sh pbis-open-8.8.0.506.linux.x86_64.deb.sh
2 <!--NeedCopy-->
```

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 /opt/pbis/bin/domainjoin-cli join domain-name user
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。

注意：要将 Bash 设置为默认 shell，请运行 **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash** 命令。

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。验证加入了 PBIS 的 Linux 计算机是否位于域中：

```
1 /opt/pbis/bin/domainjoin-cli query
2 <!--NeedCopy-->
```

如果计算机已加入某个域，此命令将返回有关当前加入的 AD 域和 OU 的信息。否则，仅显示主机名。

验证用户身份验证 要验证 PBIS 是否能够通过 PAM 对域用户进行身份验证，请使用以前未使用的域用户帐户登录 Linux VDA。

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

验证是否为 **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-->
```

退出会话。

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

在进行域加入验证后继续执行 [步骤 6: 安装 Linux VDA](#)。

#### 步骤 4: 安装必备软件.NET Core Runtime

在安装 Linux VDA 之前, 请按照 <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers> 上的说明安装.NET Core Runtime。

- 对于 1912 LTSR 初始版本 CU1 和 CU2, 请安装.NET Core Runtime 2.1。
- 对于 CU3 及更高版本, 请安装.NET Core Runtime 3.1。

安装.NET Core Runtime 后, 请运行 `which dotnet` 命令以找到您的运行时路径。

根据命令输出, 设置.NET Core Runtime 二进制文件路径。例如, 如果命令输出为 `/aa/bb/dotnet`, 请使用 `/aa/bb` 作为.NET 二进制文件路径。

#### 步骤 5: 下载 Linux VDA 软件包

转至 [Citrix Virtual Apps and Desktops 下载页面](#)。展开相应版本的 Citrix Virtual Apps and Desktops, 然后单击组件以下载与 Linux 发行版匹配的 Linux VDA 包。

#### 步骤 6: 安装 Linux VDA

##### 步骤 6a: 安装 Linux VDA

使用 Debian 软件包管理器安装 Linux VDA 软件:

对于 **Ubuntu 18.04**:

```
1 sudo dpkg -i xendesktopvda_19.12.0.50-1.ubuntu18.04_amd64.deb
2 <!--NeedCopy-->
```

对于 **Ubuntu 16.04**:

```
1 sudo dpkg -i xendesktopvda_19.12.0.50-1.ubuntu16.04_amd64.deb
2 <!--NeedCopy-->
```

Ubuntu 18.04 的 Debian 依赖项列表:

```
1 postgresql >= 9.5
2
3 libpostgresql-jdbc-java >= 9.2
4
5 openjdk-8-jdk >= 1.8.0
6
7 gtk3-nocsd >=3
8
9 imagemagick >= 8:6.8.9.9
10
11 ufw >= 0.35
```

```
12
13 ubuntu-desktop >= 1.361
14
15 libxrandr2 >= 2:1.5.0
16
17 libxtst6 >= 2:1.2.2
18
19 libxm4 >= 2.3.4
20
21 util-linux >= 2.27.1
22
23 bash >= 4.3
24
25 findutils >= 4.6.0
26
27 sed >= 4.2.2
28
29 cups >= 2.1
30
31 libldap-2.4-2 >= 2.4.42
32
33 libsasl2-modules-gssapi-mit >= 2.1.~
34
35 python-requests >= 2.9.1
36
37 libgoogle-perftools4 >= 2.4~
38
39 xserver-xorg-core >= 2:1.18
40
41 xserver-xorg-core << 2:1.19
42
43 x11vnc>=0.9.13
44
45 python-websocketify >= 0.6.1
46 <!--NeedCopy-->
```

Ubuntu 16.04 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
37 xserver-xorg-core >= 2:1.18
38
39 xserver-xorg-core << 2:1.19
40
41 x11vnc>=0.9.13
42
43 python-websockify >= 0.6.1
44 <!--NeedCopy-->
```

**注意：**

有关此版本的 Linux VDA 支持的 Linux 发行版和 Xorg 版本的列表，请参阅[系统要求](#)。

**步骤 6b：升级 Linux VDA (可选)**

可以从先前的两个版本和 LTSR 版本升级现有安装。

```
1 sudo dpkg -i <PATH>/<Linux VDA deb>
2 <!--NeedCopy-->
```

**步骤 7：安装 NVIDIA GRID 驱动程序**

启用 HDX 3D Pro 要求您在虚拟机管理程序和 VDA 计算机上安装 NVIDIA GRID 驱动程序。

要在特定虚拟机管理程序上安装和配置 NVIDIA GRID 虚拟 GPU 管理器（主机驱动程序），请参阅以下指南：

- [Citrix Hypervisor](#)
- [VMware ESX](#)

要安装和配置 NVIDIA GRID 来宾 VM 驱动程序，请执行下面的常规步骤：

1. 确保来宾 VM 已关闭。
2. 在虚拟机管理程序控制面板中，为 VM 分配一个 GPU。
3. 启动 VM。
4. 在 VM 上安装来宾 VM 驱动程序。

## 步骤 8：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 | 5** -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 Services
  - 3 - Centrify DirectControl
  - 4 - SSSD
  - 5 -PBIS
- **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\_FAS\_LIST=' list-fas-servers'** -联合身份验证服务 (FAS) 服务器是通过 AD 组策略配置的。由于 Linux VDA 不支持 AD 组策略, 您可以改为提供以分号分隔的 FAS 服务器的列表。顺序必须与在 AD 组策略中配置的顺序相同。如果删除了任何服务器地址, 则使用 **<none>** 文本字符串填充空白处, 并使服务器地址的顺序保持不变。
- **CTX\_XDL\_DOTNET\_RUNTIME\_PATH=path-to-install-dotnet-runtime** - 安装 .NET Core Runtime 支持新的 Broker 代理服务 (ctxvda) 的路径。默认路径为 /usr/bin。
- **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|5
```

```
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-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST= 'list-ldap-servers' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST= 'list-fas-servers' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_START_SERVICE=Y|N
28
29 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--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|5 \
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_FAS_LIST= 'list-fas-servers' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_START_SERVICE=Y|N \
28
```

```
29 /opt/Citrix/VDA/sbin/ctxsetup.sh
30 <!--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。

#### 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 9：运行 XDPing

我们提供了一个命令行实用程序，即 Linux XDPing 工具，用于检查 Linux VDA 环境中的常见配置问题。您可以在运行受支持的 Linux 发行版的任何计算机上安装 XDPing 软件包。XDPing 不要求在计算机上安装 Linux VDA 软件包。有关该工具的详细信息，请参阅知识中心文章 [CTX202015](#)。

### 步骤 10：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-->
```

**注意：**

在停止 `ctxvda` 和 `ctxhdx` 服务之前，请运行 `service ctxmonitorservice stop` 命令以停止监视服务守护程序。否则，监视服务守护程序将重新启动您停止的服务。

**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 11：在 Citrix Virtual Apps 或 Citrix Virtual Desktops 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：
  - 多会话操作系统选项（对于托管共享桌面交付模型）。
  - 单会话操作系统选项（对于 VDI 专用桌面交付模型）。
- 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 12：在 Citrix Virtual Apps 或 Citrix Virtual Desktops 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：

- 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。

有关如何创建计算机目录和交付组的信息，请参阅 [Citrix Virtual Apps and Desktops 7 1912 LTSR](#)。

## 使用 **Machine Creation Services (MCS)** 创建 **Linux VM**

May 8, 2023

从 7.18 版起，您可以使用 MCS 创建 Linux VM。

受支持的虚拟机管理程序

- AWS
- Citrix Hypervisor
- Microsoft Azure
- VMware vSphere

如果您尝试在受支持的虚拟机管理程序以外的其他虚拟机管理程序上准备主映像，可能会出现意外结果。

### 使用 **MCS** 在 **Citrix Hypervisor** 上创建 **Linux VM**

步骤 **1**: 准备主映像

主映像包含操作系统、非虚拟化应用程序、VDA 和其他软件。要准备主映像，请执行以下操作：

步骤 **1a**: 安装 **Citrix VM Tools** 必须在模板 VM 上安装 Citrix VM Tools, 每个 VM 才能使用 xe CLI 或 XenCenter。除非安装这些工具，否则 VM 性能会较低。如果没有这些工具，无法执行以下任何操作：

- 彻底关闭、重新启动或挂起 VM。
- 在 XenCenter 中查看 VM 性能数据。
- 迁移正在运行的 VM（通过 XenMotion）。
- 创建快照或带有内存（检查点）的快照，以及还原到快照。
- 在正在运行的 Linux VM 上调整 vCPU 数。

1. 运行以下命令装载名为 `guest-tools.iso` 的 Citrix VM Tools。

```
1 sudo mount /dev/cdrom /mnt
2 <!--NeedCopy-->
```

2. 根据您的 Linux 发行版，运行以下命令安装 `xe-guest-utilities` 软件包。

对于 **RHEL/CentOS**:

```
1 sudo rpm -i /mnt/Linux/xe-guest-utilities_{
2 package-version }
3 _all.rpm
4 <!--NeedCopy-->
```

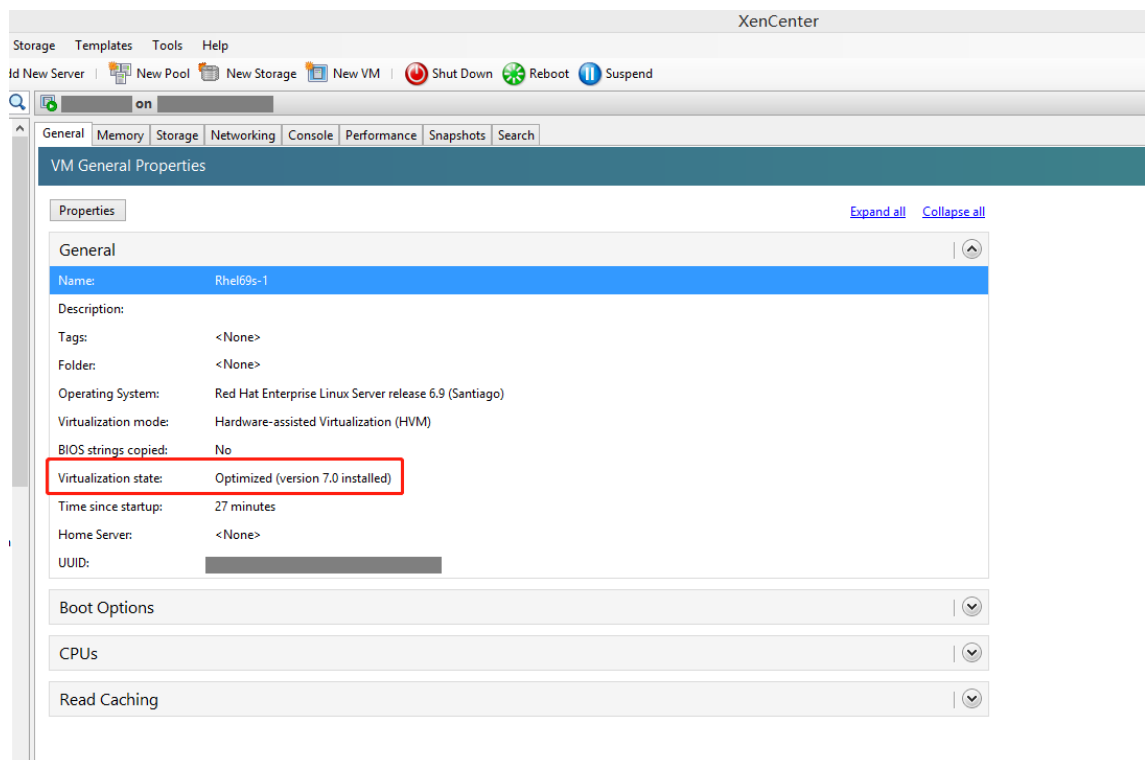
对于 **Ubuntu**:

```
1 sudo dpkg -i /mnt/Linux/xe-guest-utilities_{
2 package-version }
3 _all.deb
4 <!--NeedCopy-->
```

对于 **SUSE 12**:

```
1 sudo rpm -i /mnt/Linux/xe-guest-utilities_{
2 package-version }
3 _all.rpm
4 <!--NeedCopy-->
```

3. 在 XenCenter 中的常规选项卡上检查模板 VM 的虚拟化状态。如果正确安装了 Citrix VM Tools，则虚拟化状态为已优化:



**步骤 1b:** 在模板 VM 上安装 **Linux VDA** 软件包

注意:

要使用当前运行的 VDA 作为模板 VM，请省略此步骤。

在模板 VM 上安装 Linux VDA 软件包之前，请安装 .NET Core Runtime 3.1。有关详细信息，请参阅[安装概述](#)。

根据您的 Linux 发行版，运行以下命令为 Linux VDA 设置环境：

对于 **RHEL/CentOS**：

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

对于 **Ubuntu**：

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

对于 **SUSE 12**：

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

步骤 **1c**：启用存储库以安装 **tdb-tools** 软件包 对于 **RHEL 7** 服务器：

```
1 subscription-manager repos --enable=rhel-7-server-optional-rpms
2 <!--NeedCopy-->
```

对于 **RHEL 7** 工作站：

```
1 subscription-manager repos --enable=rhel-7-workstation-optional-rpms
2 <!--NeedCopy-->
```

步骤 **1d**：安装包含 **ntfs-3g** 的 **EPEL** 存储库 在 RHEL 6/CentOS 6、RHEL 7/CentOS 7 上安装 EPEL 存储库，以便稍后运行 `deploymcs.sh` 会安装其中包含的 **ntfs-3g** 软件包。

步骤 **1e**：在 **SUSE 12** 上手动安装 **ntfs-3g** 在 SUSE 12 平台上，没有提供 **ntfs-3g** 的存储库。下载源代码，编译并手动安装 **ntfs-3g**：

1. 安装 GNU Compiler Collection (GCC) 编译器系统并将软件包设置为：

```
1 sudo zypper install gcc
2 sudo zypper install make
3 <!--NeedCopy-->
```

2. 下载 **ntfs-3g** 软件包。

3. 解压缩 **ntfs-3g** 软件包：

```
1 sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
2 <!--NeedCopy-->
```

4. 输入 ntfs-3g 软件包的路径:

```
1 sudo cd ntfs-3g_ntfsprogs-<package version>
2 <!--NeedCopy-->
```

5. 安装 ntfs-3g:

```
1 ./configure
2 make
3 make install
4 <!--NeedCopy-->
```

**步骤 1f:** 设置运行时环境 运行 **deploymcs.sh** 之前, 请执行以下操作:

- 更改 **/etc/xdl/mcs/mcs.conf** 中的变量。 **mcs.conf** 配置文件中包含用于设置 MCS 和 Linux VDA 的变量。 以下是您可以根据需要设置的变量:
  - **Use\_Existing\_Configurations\_Of\_Current\_VDA:** 确定是否使用当前正在运行的 VDA 的现有配置。如果设置为 Y, MCS 创建的计算机上的配置文件将与当前正在运行的 VDA 上的等效文件相同。但是, 您仍然必须配置 **dns** 和 **AD\_INTEGRATION** 变量。默认值为 N, 这意味着 MCS 创建的计算机上的配置文件由主映像上的配置模板确定。
  - **dns:** 设置 DNS IP 地址。
  - **AD\_INTEGRATION:** 设置 Winbind 或 SSSD。
  - **WORKGROUP:** 设置工作组名称, 如果已在 AD 中配置, 则为 NetBIOS 名称 (区分大小写)。否则, 工作组名称默认为域名。
- 在模板计算机上, 将命令行添加到 **/etc/xdl/mcs/mcs\_local\_setting.reg** 文件以根据需要写入或更新注册表值。此操作可防止数据和设置在 MCS 预配的计算机每次重新启动时丢失。

**/etc/xdl/mcs/mcs\_local\_setting.reg** 文件中的每一行就是用于设置或更新注册表值的一个命令。

例如, 您可以将以下命令行添加到 **/etc/xdl/mcs/mcs\_local\_setting.reg** 文件中, 以分别写入或更新注册表值:

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
 VirtualChannels\Clipboard\ClipboardSelection" -t "REG_DWORD" -
 v "Flags" -d "0x00000003" --force
2 <!--NeedCopy-->
```

```
1 update -k "HKLM\System\CurrentControlSet\Control\Citrix\
 VirtualChannels\Clipboard\ClipboardSelection" -v "Flags" -d "0
 x00000003"
2 <!--NeedCopy-->
```

### 步骤 1g: 创建主映像

1. 运行 `/opt/Citrix/VDA/sbin/deploymcs.sh`。
2. (可选)在模板 VM 上,更新配置模板以自定义创建的所有 VM 上的相关 `/etc/krb5.conf`、`/etc/samba/smb.conf` 和 `/etc/sss/sss.conf` 文件。

对于 Winbind 用户,请更新 `/etc/xdl/mcs/winbind_krb5.conf.tmpl` 和 `/etc/xdl/mcs/winbind_smb.conf.tmpl` 模板。

对于 SSSD 用户,请更新 `/etc/xdl/mcs/sss.conf.tmpl`、`/etc/xdl/mcs/sss_krb5.conf.tmpl` 和 `/etc/xdl/mcs/sss_smb.conf.tmpl` 模板。

注意:请保留模板文件中使用的现有格式并使用变量,例如 `$WORKGROUP`、`$REALM`、`$realm` 和 `$AD_FQDN`。

3. 在 Citrix Hypervisor 上,关闭模板 VM。创建并命名主映像的快照。

### 步骤 2: 创建计算机目录

在 Citrix Studio 中,创建计算机目录并指定要在目录中创建的 VM 数量。根据需要执行其他配置任务。有关详细信息,请参阅[使用 Studio 创建计算机目录](#)。

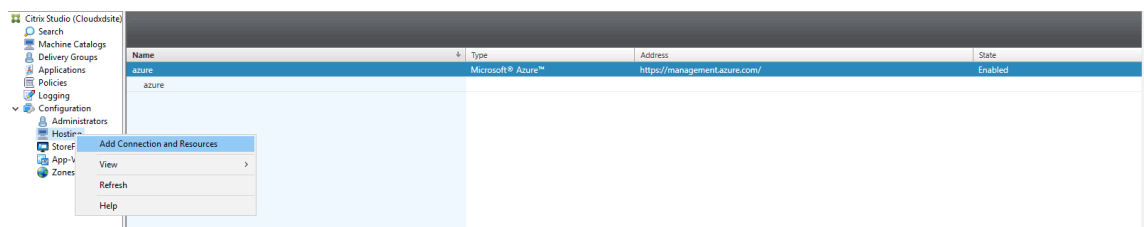
### 步骤 3: 创建交付组

交付组是从一个或多个计算机目录中选择的计算机的集合。它指定哪些用户可以使用这些计算机,以及可供这些用户使用的应用程序和桌面。有关详细信息,请参阅[创建交付组](#)。

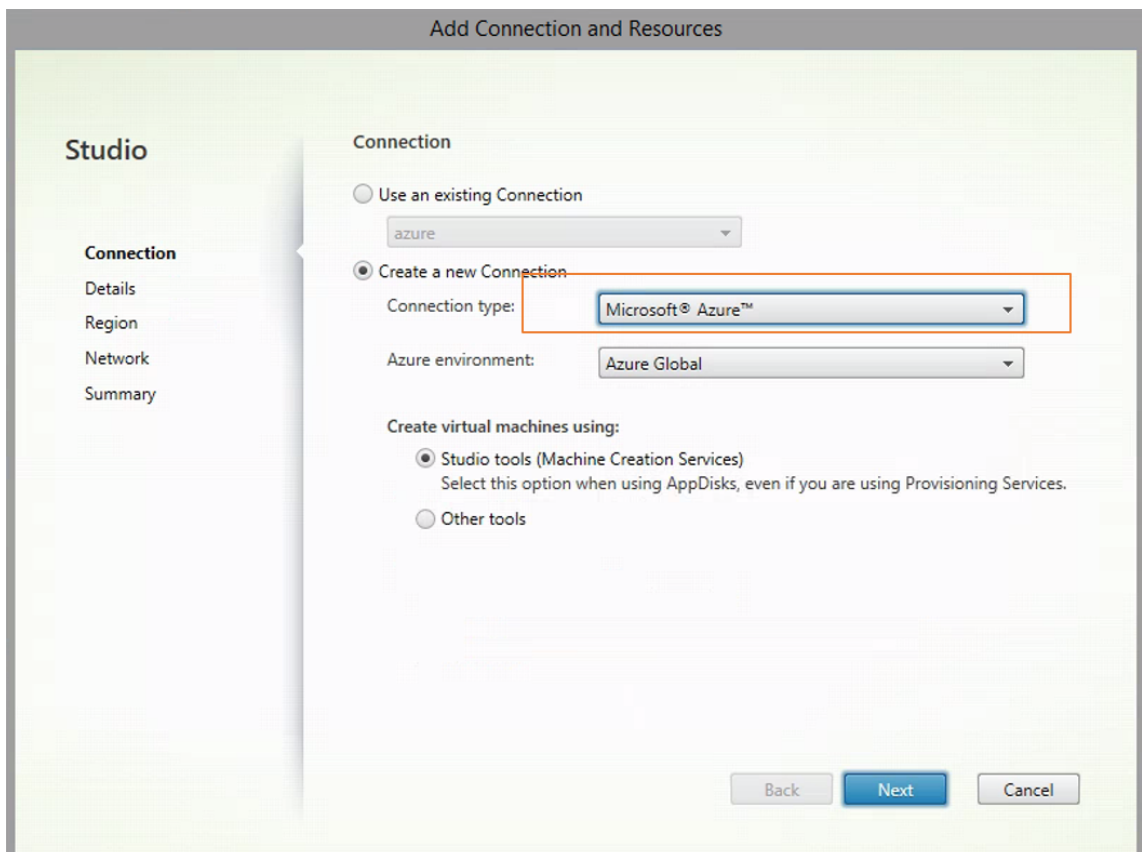
## 使用 MCS 在 Azure 上创建 Linux VM

### 步骤 1: 在 Citrix Studio 中创建与 Azure 的托管连接

1. 在 Citrix Studio 中,选择配置 > 托管 > 添加连接和资源以创建与 Azure 的连接。

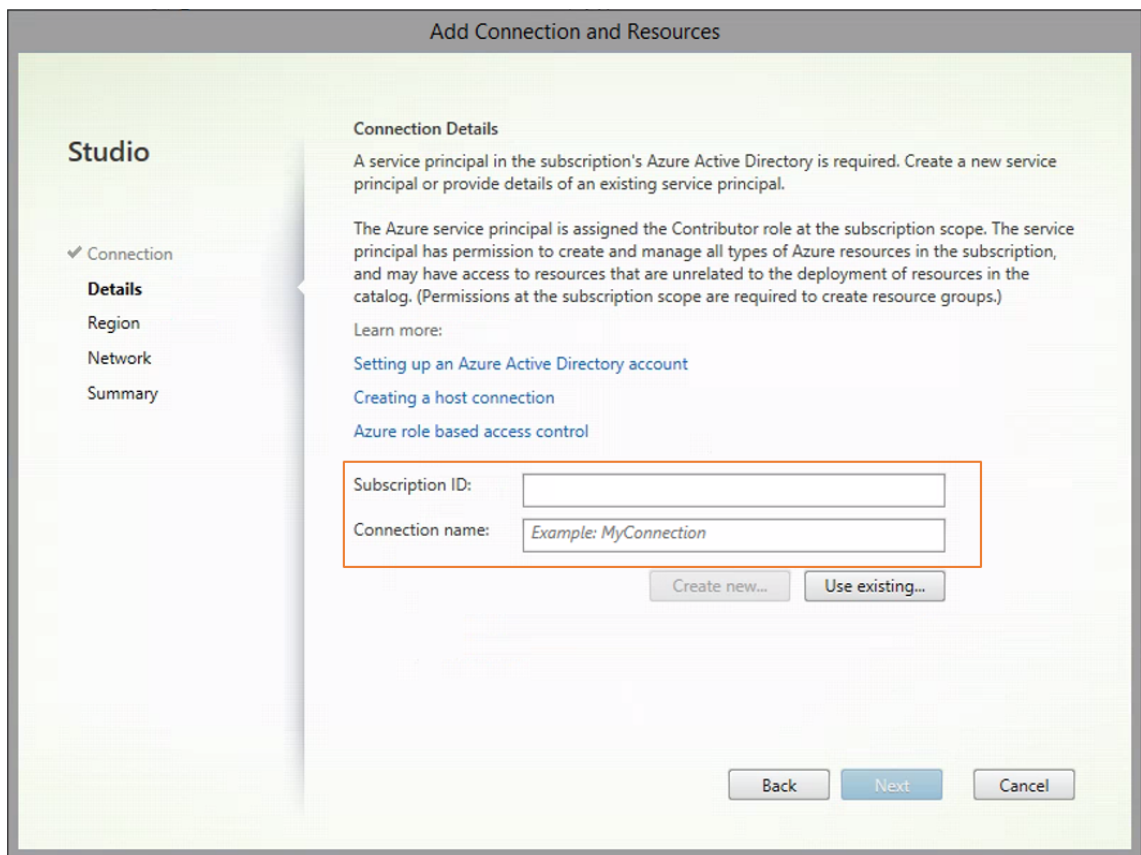


2. 选择连接类型 Microsoft Azure。

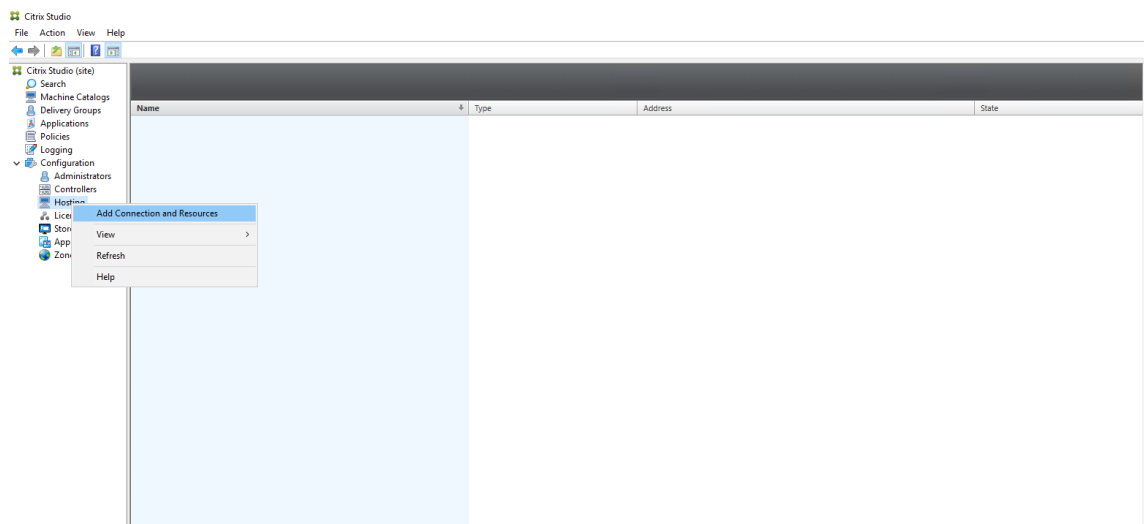


3. 键入您的 Azure 帐户的订阅 ID，然后键入您的连接名称。





将在托管窗格中显示一个新连接。



**步骤 2:** 在模板 **VM** 上准备主映像

主映像包含操作系统、非虚拟化应用程序、VDA 和其他软件。要准备主映像，请执行以下操作：

步骤 **2a**: 为 **Ubuntu 18.04** 配置 **cloud-init** 要确保在重新启动或停止 VM 时 VDA 主机名仍然存在, 请运行以下命令。

```
1 echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99_hostname.
 cfg
2 <!--NeedCopy-->
```

确保在 /etc/cloud/cloud.cfg 文件中的 **system\_info** 部分下存在以下行:

```
1 system_info:
2 network:
3 renderers: ['netplan', 'eni', 'sysconfig']
4 <!--NeedCopy-->
```

步骤 **2b**: 在模板 **VM** 上安装 **Linux VDA** 软件包

注意:

要使用当前运行的 VDA 作为模板 VM, 请省略此步骤。

在模板 VM 上安装 Linux VDA 软件包之前, 请安装 .NET Core Runtime 3.1。有关详细信息, 请参阅[安装概述](#)。

根据您的 Linux 发行版, 运行以下命令为 Linux VDA 设置环境:

对于 **RHEL/CentOS**:

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

对于 **Ubuntu**:

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

对于 **SUSE 12**:

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

步骤 **2c**: 启用存储库以安装 **tdb-tools** 软件包 对于 **RHEL 7** 服务器:

```
1 subscription-manager repos --enable=rhel-7-server-optional-rpms
2 <!--NeedCopy-->
```

对于 **RHEL 7** 工作站:

```
1 subscription-manager repos --enable=rhel-7-workstation-optional-rpms
2 <!--NeedCopy-->
```

步骤 **2d**: 安装包含 **ntfs-3g** 的 **EPEL** 存储库 在 RHEL 6/CentOS 6、RHEL 7/CentOS 7 上安装 EPEL 存储库, 以便稍后运行 `deploymcs.sh` 会安装其中包含的 `ntfs-3g` 软件包。

步骤 **2e**: 在 **SUSE 12** 上手动安装 **ntfs-3g** 在 SUSE 12 平台上, 没有提供 `ntfs-3g` 的存储库。下载源代码, 编译并手动安装 `ntfs-3g`:

1. 安装 GNU Compiler Collection (GCC) 编译器系统并将软件包设置为:

```
1 sudo zypper install gcc
2 sudo zypper install make
3 <!--NeedCopy-->
```

2. 下载 `ntfs-3g` 软件包。

3. 解压缩 `ntfs-3g` 软件包:

```
1 sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
2 <!--NeedCopy-->
```

4. 输入 `ntfs-3g` 软件包的路径:

```
1 sudo cd ntfs-3g_ntfsprogs-<package version>
2 <!--NeedCopy-->
```

5. 安装 `ntfs-3g`:

```
1 ./configure
2 make
3 make install
4 <!--NeedCopy-->
```

步骤 **2f**: 设置运行时环境 运行 `deploymcs.sh` 之前, 请执行以下操作:

- 更改 `/etc/xdl/mcs/mcs.conf` 中的变量。 `mcs.conf` 配置文件中包含用于设置 MCS 和 Linux VDA 的变量。下面是一些变量, 其中必须设置 `dns` 和 `AD_INTEGRATION`:

注意: 如果为一个变量设置多个值, 请将这些值放置在单引号内并用空格分隔。例如, `LDAP_LIST='aaa.lab:389 bbb.lab:389.'`

- `Use_Existing_Configurations_Of_Current_VDA`: 确定是否使用当前正在运行的 VDA 的现有配置。如果设置为 Y, MCS 创建的计算机上的配置文件将与当前正在运行的 VDA 上的等效文件相同。但是, 您仍然必须配置 `dns` 和 `AD_INTEGRATION` 变量。默认值为 N, 这意味着 MCS 创建的计算机上的配置文件由主映像上的配置模板确定。
- `dns`: 设置 DNS IP 地址。
- `AD_INTEGRATION`: 设置 Winbind 或 SSSD (SUSE 不支持 SSSD)。
- `WORKGROUP`: 设置工作组名称, 如果已在 AD 中配置, 则为 NetBIOS 名称 (区分大小写)。否则, 工作组名称默认为域名。

- 在模板计算机上，将命令行添加到 `/etc/xdl/mcs/mcs_local_setting.reg` 文件以根据需要写入或更新注册表值。此操作可防止数据和设置在 MCS 预配的计算机每次重新启动时丢失。

`/etc/xdl/mcs/mcs_local_setting.reg` 文件中的每一行就是用于设置或更新注册表值的一个命令。

例如，您可以将以下命令行添加到 `/etc/xdl/mcs/mcs_local_setting.reg` 文件中，以分别写入或更新注册表值：

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
 VirtualChannels\Clipboard\ClipboardSelection" -t "REG_DWORD" -
 v "Flags" -d "0x00000003" --force
2 <!--NeedCopy-->
```

```
1 update -k "HKLM\System\CurrentControlSet\Control\Citrix\
 VirtualChannels\Clipboard\ClipboardSelection" -v "Flags" -d "0
 x00000003"
2 <!--NeedCopy-->
```

## 步骤 2g: 创建主映像

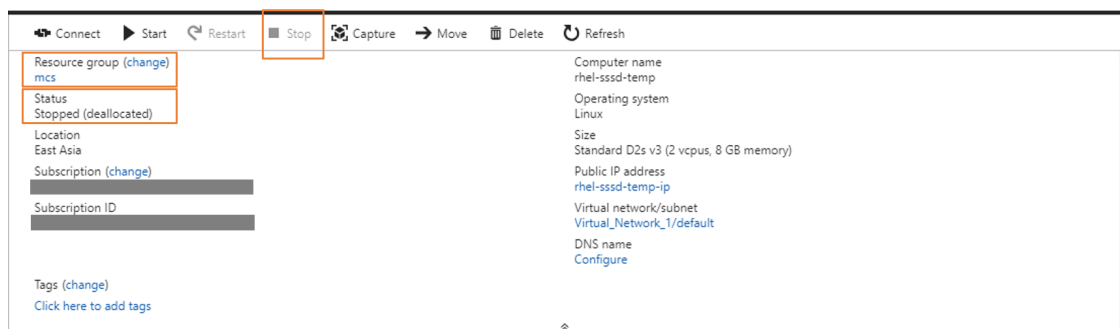
- 运行 `/opt/Citrix/VDA/sbin/deploymcs.sh`。
- (可选)在模板 VM 上,更新配置模板以自定义创建的所有 VM 上的相关 `/etc/krb5.conf`、`/etc/samba/smb.conf` 和 `/etc/sss/sss.conf` 文件。

对于 Winbind 用户，请更新 `/etc/xdl/mcs/winbind_krb5.conf.tpl` 和 `/etc/xdl/mcs/winbind_smb.conf.tpl` 模板。

对于 SSSD 用户，请更新 `/etc/xdl/mcs/sss.conf.tpl`、`/etc/xdl/mcs/sss_krb5.conf.tpl` 和 `/etc/xdl/mcs/sss_smb.conf.tpl` 模板。

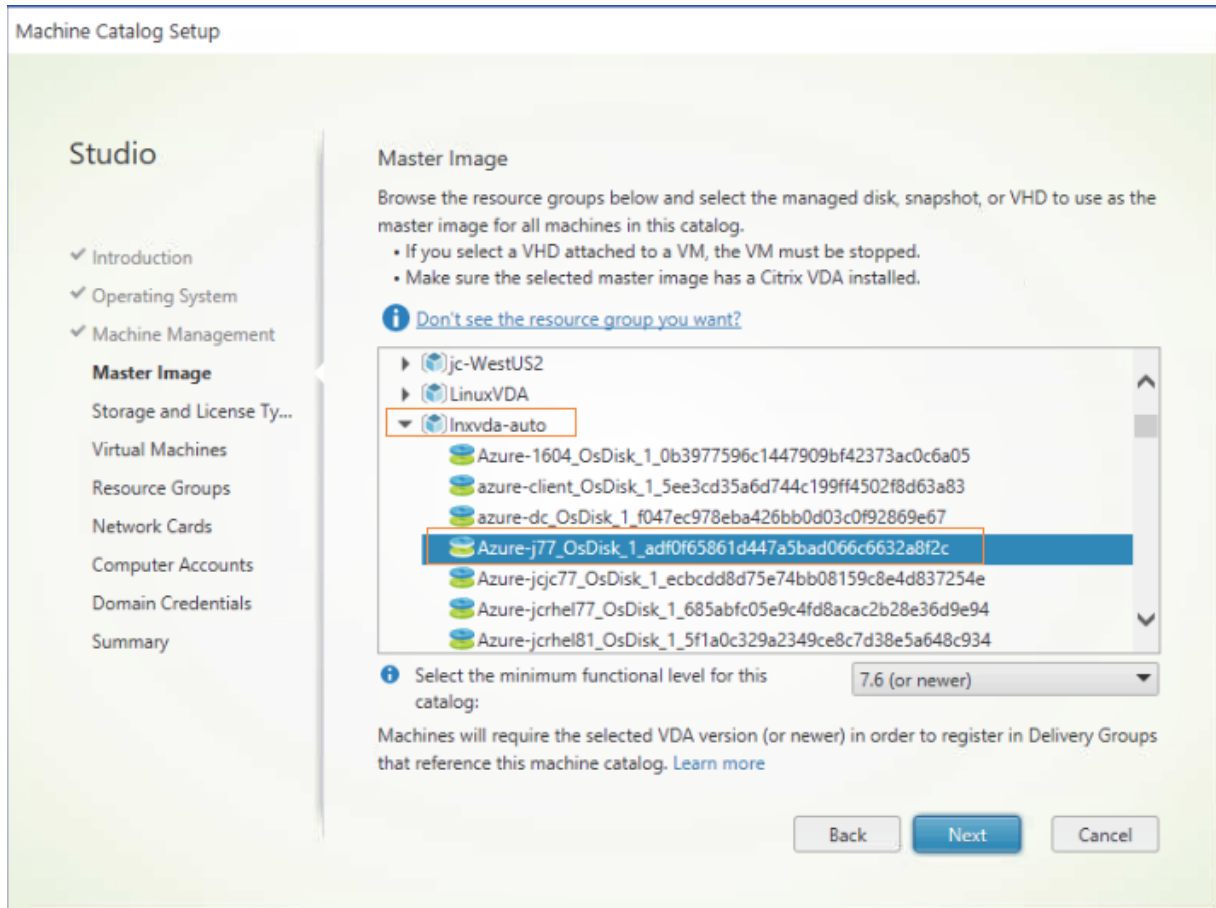
注意：请保留模板文件中使用的现有格式并使用变量，例如 `$WORKGROUP`、`$REALM`、`$realm` 和 `$AD_FQDN`。

- 在模板 VM 上安装应用程序后，从 Azure 门户关闭模板 VM。确保模板 VM 的电源状态为 **Stopped (deallocated)** (已停止 (已取消分配))。记住此处的资源组名称。在 Azure 上查找您的主映像时需要该名称。



### 步骤 3：创建计算机目录

在 Citrix Studio 中，创建计算机目录并指定要在目录中创建的 VM 数量。创建计算机目录时，从模板 VM 所属的资源组中选择主映像，并查找模板 VM 的 VHD。请参阅以下屏幕截图。



根据需要执行其他配置任务。有关详细信息，请参阅[使用 Studio 创建计算机目录](#)。

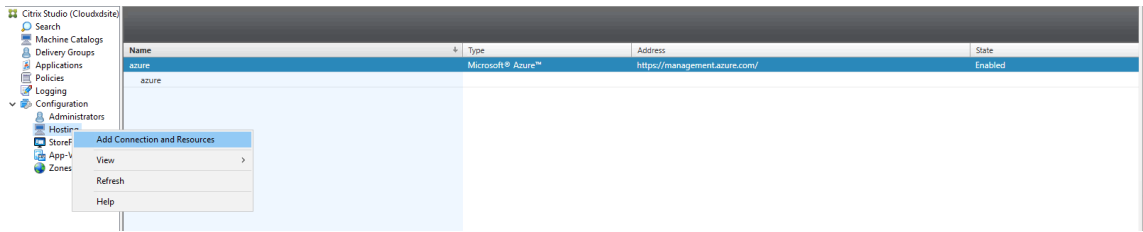
### 步骤 4：创建交付组

交付组是从一个或多个计算机目录中选择的计算机的集合。它指定哪些用户可以使用这些计算机，以及可供这些用户使用的应用程序和桌面。有关详细信息，请参阅[创建交付组](#)。

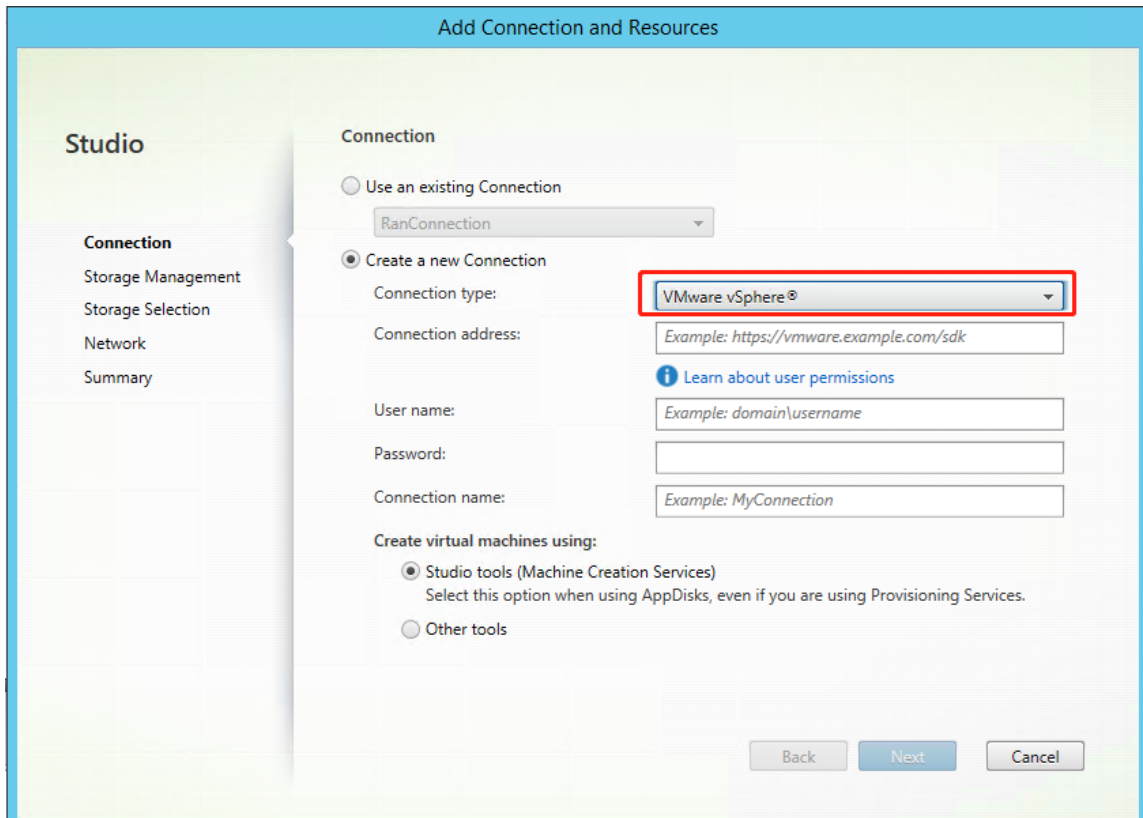
## 使用 MCS 在 VMware vSphere 上创建 Linux VM

步骤 1：在 Citrix Studio 中创建与 VMware 的托管连接

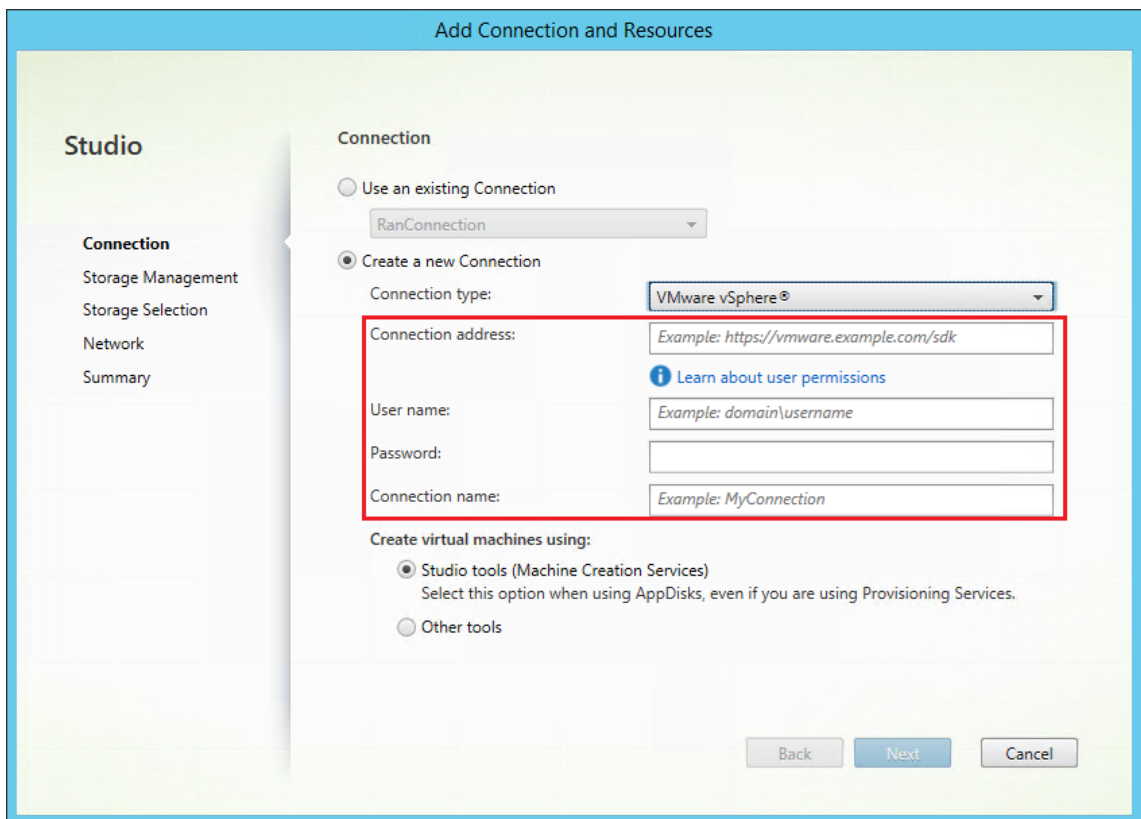
1. 在 vSphere 环境中安装 vCenter Server。有关详细信息，请参阅[VMware vSphere](#)。
2. 在 Citrix Studio 中，选择配置 > 托管 > 添加连接和资源以创建与 VMware vSphere 的连接。



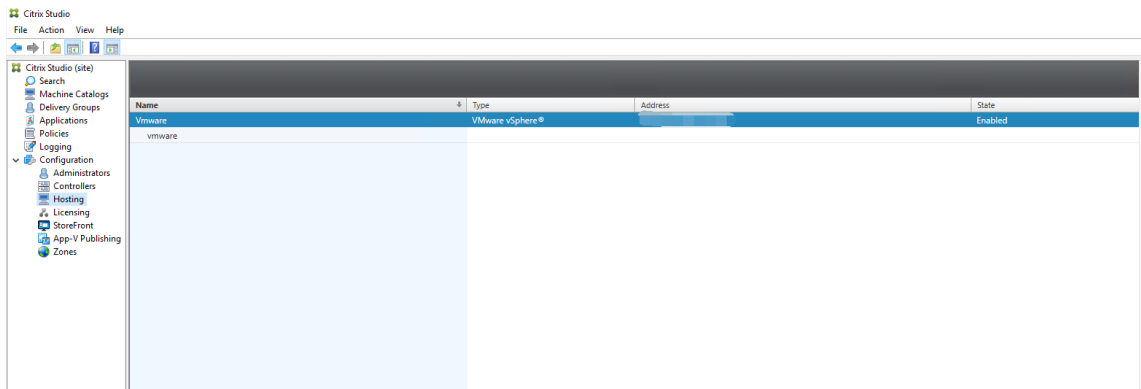
3. 选择 VMware vSphere 作为连接类型。



4. 键入 VMware 帐户的连接地址 (vCenter Server URL)、您的用户名和密码以及连接名称。



将在托管窗格中显示一个新连接。



## 步骤 2：准备主映像

主映像包含操作系统、非虚拟化应用程序、VDA 和其他软件。要准备主映像，请执行以下操作：

### 步骤 2a：在模板 VM 上安装 Linux VDA 软件包

注意：

要使用当前运行的 VDA 作为模板 VM，请省略此步骤。

在模板 VM 上安装 Linux VDA 软件包之前，请安装 .NET Core Runtime 3.1。有关详细信息，请参阅[安装概述](#)。

根据您的 Linux 发行版，运行以下命令为 Linux VDA 设置环境：

对于 **RHEL/CentOS**：

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

对于 **Ubuntu**：

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

对于 **SUSE 12**：

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

步骤 **2b**：启用存储库以安装 **tdb-tools** 软件包 对于 **RHEL 7** 服务器：

```
1 subscription-manager repos --enable=rhel-7-server-optional-rpms
2 <!--NeedCopy-->
```

对于 **RHEL 7** 工作站：

```
1 subscription-manager repos --enable=rhel-7-workstation-optional-rpms
2 <!--NeedCopy-->
```

步骤 **2c**：安装包含 **ntfs-3g** 的 **EPEL** 存储库 在 RHEL 6/CentOS 6、RHEL 7/CentOS 7 上安装 EPEL 存储库，以便稍后运行 `deploymcs.sh` 会安装其中包含的 **ntfs-3g** 软件包。

步骤 **2d**：在 **SUSE 12** 上手动安装 **ntfs-3g** 在 SUSE 12 平台上，没有提供 **ntfs-3g** 的存储库。下载源代码，编译并手动安装 **ntfs-3g**：

1. 安装 GNU Compiler Collection (GCC) 编译器系统并将软件包设置为：

```
1 sudo zypper install gcc
2 sudo zypper install make
3 <!--NeedCopy-->
```

2. 下载 **ntfs-3g** 软件包。

3. 解压缩 **ntfs-3g** 软件包：



```
1 sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
2 <!--NeedCopy-->
```

#### 4. 输入 ntfs-3g 软件包的路径:

```
1 sudo cd ntfs-3g_ntfsprogs-<package version>
2 <!--NeedCopy-->
```

#### 5. 安装 ntfs-3g:

```
1 ./configure
2 make
3 make install
4 <!--NeedCopy-->
```

步骤 **2e**: 设置运行时环境 运行 **deploymcs.sh** 之前, 请执行以下操作:

- 更改 **/etc/xdl/mcs/mcs.conf** 中的变量。 **mcs.conf** 配置文件中包含用于设置 MCS 和 Linux VDA 的变量。下面是一些变量, 其中必须设置 **dns** 和 **AD\_INTEGRATION**:

注意: 如果为一个变量设置多个值, 请将这些值放置在单引号内并用空格分隔。例如, `LDAP_LIST='aaa.lab:389 bbb.lab:389.'`

- **Use\_Existing\_Configurations\_Of\_Current\_VDA**: 确定是否使用当前正在运行的 VDA 的现有配置。如果设置为 Y, MCS 创建的计算机上的配置文件将与当前正在运行的 VDA 上的等效文件相同。但是, 您仍然必须配置 **dns** 和 **AD\_INTEGRATION** 变量。默认值为 N, 这意味着 MCS 创建的计算机上的配置文件由主映像上的配置模板确定。
- **dns**: 设置 DNS IP 地址。
- **AD\_INTEGRATION**: 设置 Winbind 或 SSSD (SUSE 不支持 SSSD)。
- **WORKGROUP**: 设置工作组名称, 如果已在 AD 中配置, 则为 NetBIOS 名称 (区分大小写)。否则, 工作组名称默认为域名。
- 在模板计算机上, 将命令行添加到 **/etc/xdl/mcs/mcs\_local\_setting.reg** 文件以根据需要写入或更新注册表值。此操作可防止数据和设置在 MCS 预配的计算机每次重新启动时丢失。

**/etc/xdl/mcs/mcs\_local\_setting.reg** 文件中的每一行就是用于设置或更新注册表值的一个命令。

例如, 您可以将以下命令行添加到 **/etc/xdl/mcs/mcs\_local\_setting.reg** 文件中, 以分别写入或更新注册表值:

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
 VirtualChannels\Clipboard\ClipboardSelection" -t "REG_DWORD" -
 v "Flags" -d "0x00000003" --force
2 <!--NeedCopy-->
```

```
1 update -k "HKLM\System\CurrentControlSet\Control\Citrix\
 VirtualChannels\Clipboard\ClipboardSelection" -v "Flags" -d "0
 x00000003"
```

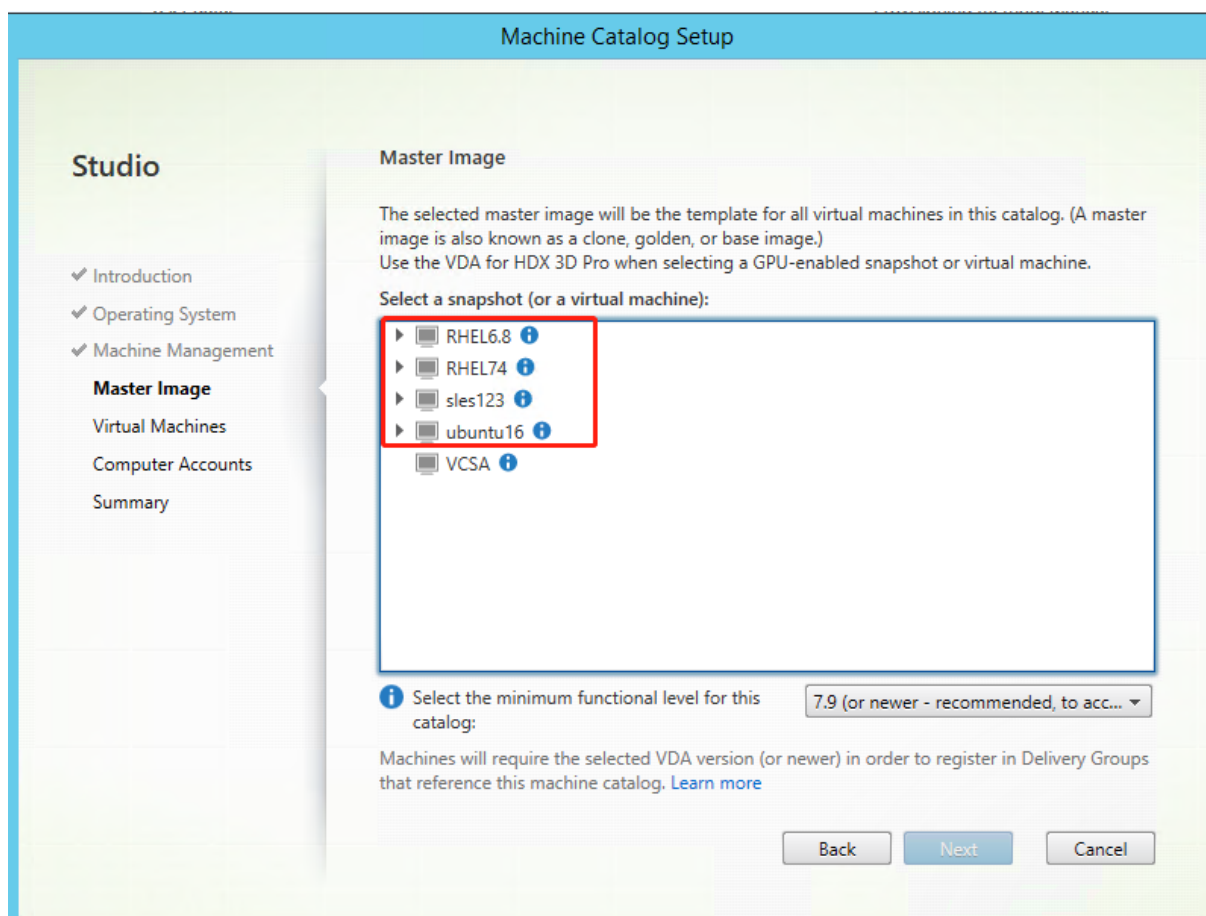
2 <!--NeedCopy-->

**步骤 2f:** 创建主映像

1. 运行 `/opt/Citrix/VDA/sbin/deploymcs.sh`。
2. (可选)在模板 VM 上,更新配置模板以自定义创建的所有 VM 上的相关 `/etc/krb5.conf`、`/etc/samba/smb.conf` 和 `/etc/sss/sss.conf` 文件。  
  
对于 Winbind 用户,请更新 `/etc/xdl/mcs/winbind_krb5.conf.templ` 和 `/etc/xdl/mcs/winbind_smb.conf.templ` 模板。  
  
对于 SSSD 用户,请更新 `/etc/xdl/mcs/sss.conf.templ`、`/etc/xdl/mcs/sss_krb5.conf.templ` 和 `/etc/xdl/mcs/sss_smb.conf.templ` 模板。  
  
注意:请保留模板文件中使用的现有格式并使用变量,例如 `$WORKGROUP`、`$REALM`、`$realm` 和 `$AD_FQDN`。
3. 在模板 VM 上安装应用程序后,从 VMware 门户关闭模板 VM。创建模板 VM 的快照。

**步骤 3:** 创建计算机目录

在 Citrix Studio 中,创建计算机目录并指定要在目录中创建的 VM 数量。创建计算机目录时,请从快照列表中选择主映像。



根据需要执行其他配置任务。有关详细信息，请参阅[使用 Studio 创建计算机目录](#)。

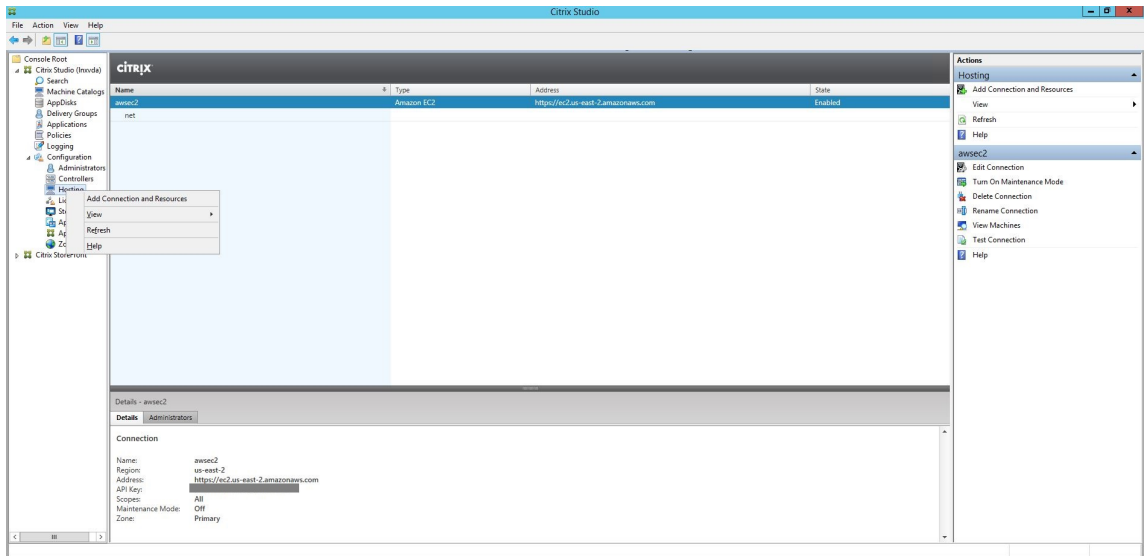
#### 步骤 4：创建交付组

交付组是从一个或多个计算机目录中选择的计算机的集合。交付组指定哪些用户可以使用这些计算机，以及可供这些用户使用的应用程序和桌面。有关详细信息，请参阅[创建交付组](#)。

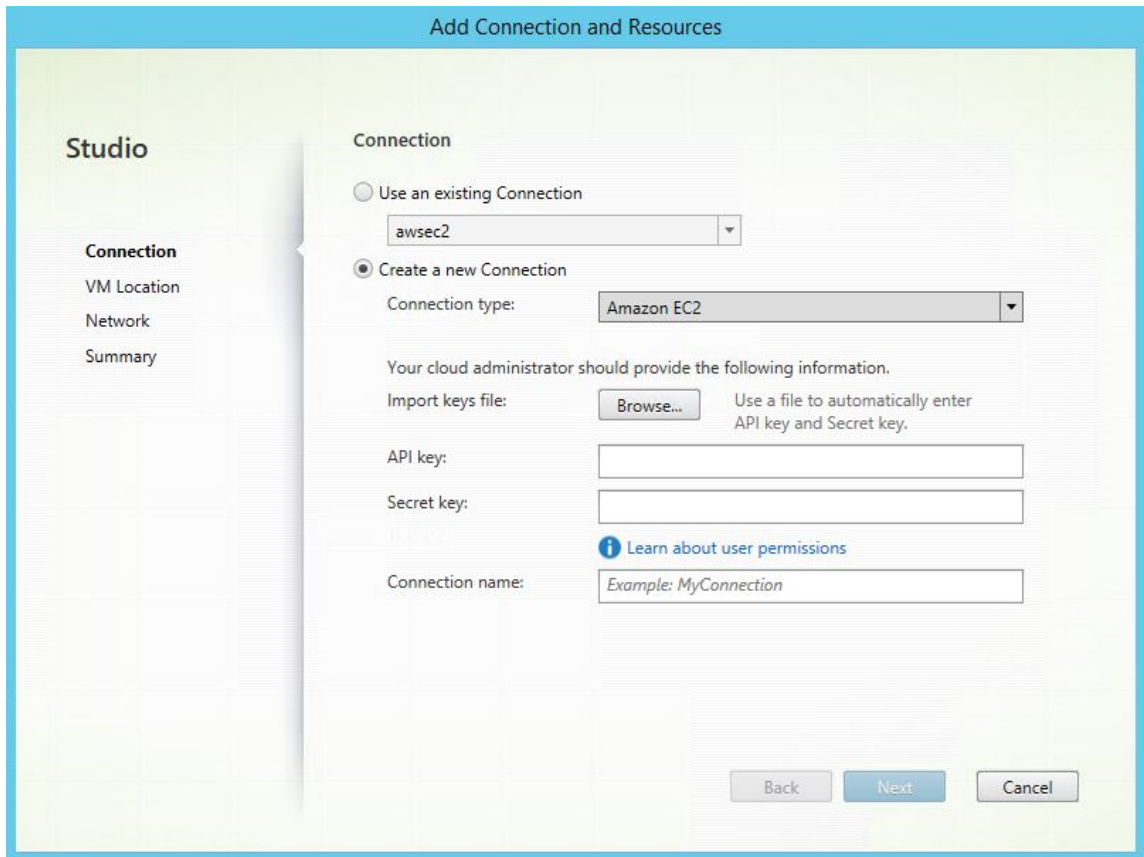
### 在 AWS 上使用 MCS 创建 Linux VM

步骤 1：在 Citrix Studio 中创建与 AWS 的托管连接

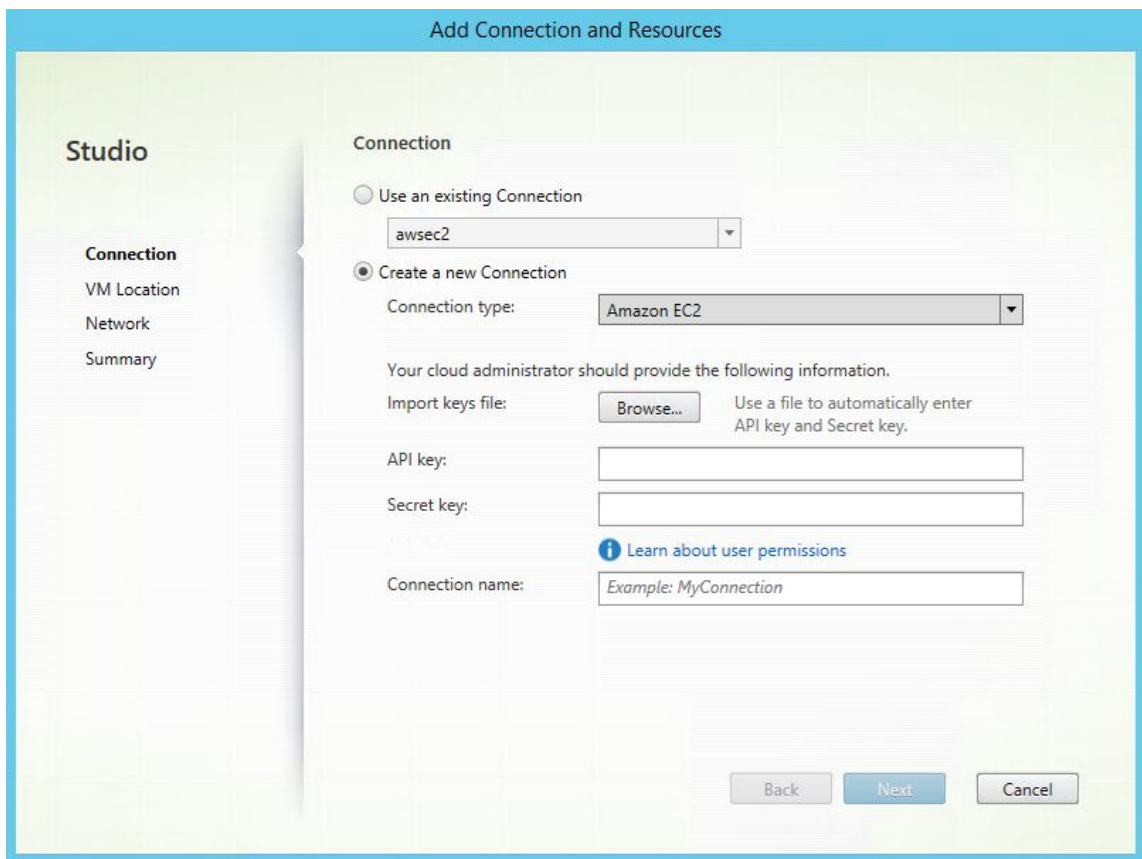
1. 在 Citrix Studio 中，选择配置 > 托管 > 添加连接和资源以创建与 AWS 的连接。



2. 选择 **Amazon EC2** 作为连接类型。



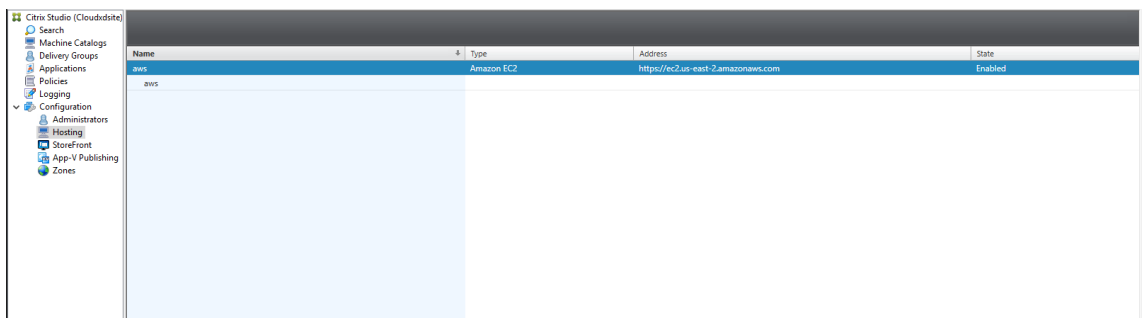
3. 键入 AWS 帐户的 API 密钥和密钥，然后键入您的连接名称。



**API 密钥**是您的访问密钥 ID，**密钥**是您的秘密访问密钥。这些密钥被视为访问密钥对。如果您丢失了秘密访问密钥，则可以删除该访问密钥并创建一个新访问密钥。要创建访问密钥，请执行以下操作：

- a) 登录 AWS 服务。
- b) 导航到身份和访问管理 (IAM) 控制台。
- c) 在左侧导航窗格中，选择用户。
- d) 选择目标用户并向下滚动以选择安全凭据选项卡。
- e) 向下滚动并单击创建访问密钥。此时将显示一个新窗口。
- f) 单击下载 **.csv** 文件并将访问密钥保存到一个安全的位置。

将在托管窗格中显示一个新连接。



## 步骤 2: 准备主映像

主映像包含操作系统、非虚拟化应用程序、VDA 和其他软件。要准备主映像，请执行以下操作：

### 步骤 2a: 配置 cloud-init

1. 要确保在重新启动或停止 EC2 实例时 VDA 主机名仍然存在，请运行以下命令以保留 VDA 主机名。

```
1 echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99
 _hostname.cfg
2 <!--NeedCopy-->
```

对于 Ubuntu 18.04，请确保在 /etc/cloud/cloud.cfg 文件中的 system\_info 部分下存在以下行：

```
1 system_info:
2 network:
3 renderers: ['netplan', 'eni', 'sysconfig']
4 <!--NeedCopy-->
```

2. 要使用 SSH 远程访问 AWS 上 MCS 创建的 VM，请启用密码身份验证，因为这些 VM 没有附加的密钥名称。根据需要执行以下操作。

- 编辑 cloud-init 配置文件 /etc/cloud/cloud.cfg。确保 **ssh\_pwauth: true** 行存在。删除或注释 **set-password** 行和以下行（如果存在）。

```
1 users:
2 - default
3 <!--NeedCopy-->
```

- 如果您计划使用通过 cloud-init 创建的默认用户 `ec2-user` 或 `ubuntu`，则可以使用 `passwd` 命令更改用户密码。请记住新密码，以便以后用于登录 MCS 创建的 VM。
- 编辑 /etc/ssh/sshd\_config 文件以确保存在以下行：

```
1 PasswordAuthentication yes
2 <!--NeedCopy-->
```

保存该文件并运行 `sudo service sshd restart` 命令。

### 步骤 2b: 在模板 VM 上安装 Linux VDA 软件包

注意：

要使用当前运行的 VDA 作为模板 VM，请省略此步骤。

在模板 VM 上安装 Linux VDA 软件包之前，请安装 .NET Core Runtime 3.1。有关详细信息，请参阅 [安装概述](#)。

根据您的 Linux 发行版，运行以下命令为 Linux VDA 设置环境：

对于 **RHEL/CentOS**：

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

对于 **Ubuntu**:

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

对于 **SUSE 12**:

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

步骤 **2c**: 启用存储库以安装 **tdb-tools** 软件包 对于 **RHEL 7** 服务器:

```
1 subscription-manager repos --enable=rhel-7-server-optional-rpms
2 <!--NeedCopy-->
```

对于 **RHEL 7** 工作站:

```
1 subscription-manager repos --enable=rhel-7-workstation-optional-rpms
2 <!--NeedCopy-->
```

步骤 **2d**: 安装包含 **ntfs-3g** 的 **EPEL** 存储库 在 RHEL 6/CentOS 6、RHEL 7/CentOS 7 上安装 EPEL 存储库，以便稍后运行 `deploymcs.sh` 会安装其中包含的 **ntfs-3g** 软件包。

步骤 **2e**: 在 **SUSE 12** 上手动安装 **ntfs-3g** 在 SUSE 12 平台上，没有提供 **ntfs-3g** 的存储库。下载源代码，编译并手动安装 **ntfs-3g**:

1. 安装 GNU Compiler Collection (GCC) 编译器系统并将软件包设置为:

```
1 sudo zypper install gcc
2 sudo zypper install make
3 <!--NeedCopy-->
```

2. 下载 **ntfs-3g** 软件包。
3. 解压缩 **ntfs-3g** 软件包:

```
1 sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
2 <!--NeedCopy-->
```

4. 输入 **ntfs-3g** 软件包的路径:

```
1 sudo cd ntfs-3g_ntfsprogs-<package version>
2 <!--NeedCopy-->
```

## 5. 安装 ntf3-3g:

```
1 ./configure
2 make
3 make install
4 <!--NeedCopy-->
```

步骤 **2f**: 设置运行时环境 运行 **deploymcs.sh** 之前, 请执行以下操作:

- 更改 **/etc/xdl/mcs/mcs.conf** 中的变量。 **mcs.conf** 配置文件中包含用于设置 MCS 和 Linux VDA 的变量。下面是一些变量, 其中必须设置 **dns** 和 **AD\_INTEGRATION**:

注意: 如果为一个变量设置多个值, 请将这些值放置在单引号内并用空格分隔。例如, `LDAP_LIST='aaa.lab:389 bbb.lab:389.'`

- **Use\_Existing\_Configurations\_Of\_Current\_VDA**: 确定是否使用当前正在运行的 VDA 的现有配置。如果设置为 Y, MCS 创建的计算机上的配置文件将与当前正在运行的 VDA 上的等效文件相同。但是, 您仍然必须配置 **dns** 和 **AD\_INTEGRATION** 变量。默认值为 N, 这意味着 MCS 创建的计算机上的配置文件由主映像上的配置模板确定。
- **dns**: 设置 DNS IP 地址。
- **AD\_INTEGRATION**: 设置 Winbind 或 SSSD (SUSE 不支持 SSSD)。
- **WORKGROUP**: 设置工作组名称, 如果已在 AD 中配置, 则为 NetBIOS 名称 (区分大小写)。否则, 工作组名称默认为域名。
- 在模板计算机上, 将命令行添加到 **/etc/xdl/mcs/mcs\_local\_setting.reg** 文件以根据需要写入或更新注册表值。此操作可防止数据和设置在 MCS 预配的计算机每次重新启动时丢失。

**/etc/xdl/mcs/mcs\_local\_setting.reg** 文件中的每一行就是用于设置或更新注册表值的一个命令。

例如, 您可以将以下命令行添加到 **/etc/xdl/mcs/mcs\_local\_setting.reg** 文件中, 以分别写入或更新注册表值:

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
 VirtualChannels\Clipboard\ClipboardSelection" -t "REG_DWORD" -
 v "Flags" -d "0x00000003" --force
2 <!--NeedCopy-->
```

```
1 update -k "HKLM\System\CurrentControlSet\Control\Citrix\
 VirtualChannels\Clipboard\ClipboardSelection" -v "Flags" -d "0
 x00000003"
2 <!--NeedCopy-->
```

步骤 **2g**: 创建主映像

1. 运行 **/opt/Citrix/VDA/sbin/deploymcs.sh**。



2. (可选)在模板 VM 上,更新配置模板以自定义创建的所有 VM 上的相关 `/etc/krb5.conf`、`/etc/samba/smb.conf` 和 `/etc/sss/sss.conf` 文件。

对于 Winbind 用户,请更新 `/etc/xdl/mcs/winbind_krb5.conf.templ` 和 `/etc/xdl/mcs/winbind_smb.conf.templ` 模板。

对于 SSSD 用户,请更新 `/etc/xdl/mcs/sss.conf.templ`、`/etc/xdl/mcs/sss_krb5.conf.templ` 和 `/etc/xdl/mcs/sss_smb.conf.templ` 模板。

注意:请保留模板文件中使用的现有格式并使用变量,例如 `$WORKGROUP`、`$REALM`、`$realm` 和 `$AD_FQDN`。

3. 在模板 VM 上安装应用程序后,从 AWS EC2 门户关闭模板 VM。确保模板 VM 的电源状态为已停止。
4. 右键单击模板 VM,然后选择映像 > 创建映像。键入信息并根据需要进行设置。单击创建映像。

**Create Image**
✕

Instance ID ⓘ i-011e...

Image name ⓘ

Image description ⓘ

No reboot ⓘ

**Instance Volumes**

| Volume Type ⓘ | Device ⓘ  | Snapshot ⓘ | Size (GiB) ⓘ | Volume Type ⓘ             | IOPS ⓘ     | Throughput (MB/s) ⓘ | Delete on Termination ⓘ             | Encrypted ⓘ   |
|---------------|-----------|------------|--------------|---------------------------|------------|---------------------|-------------------------------------|---------------|
| Root          | /dev/sda1 | snap-02    | 40           | General Purpose SSD (gp2) | 120 / 3000 | N/A                 | <input checked="" type="checkbox"/> | Not Encrypted |

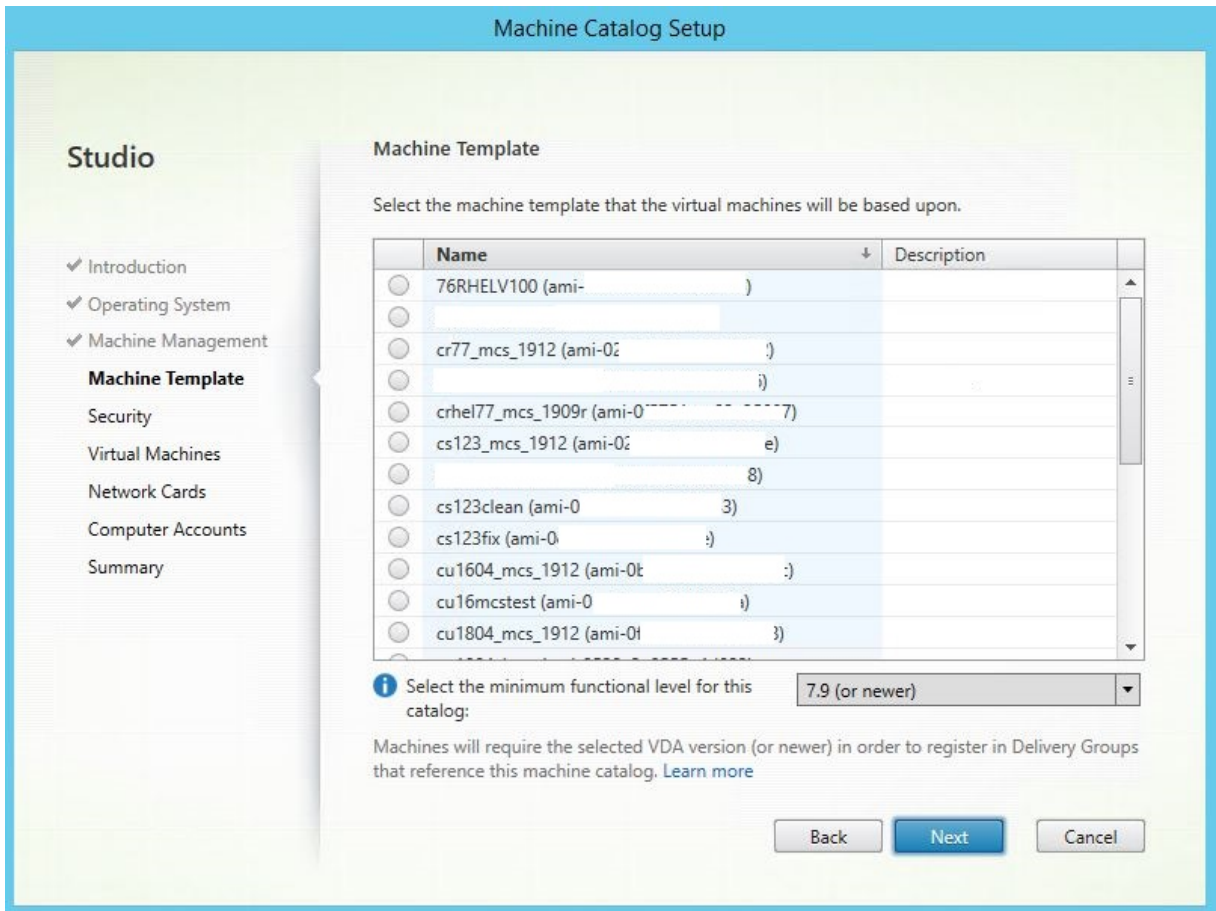
[Add New Volume](#)

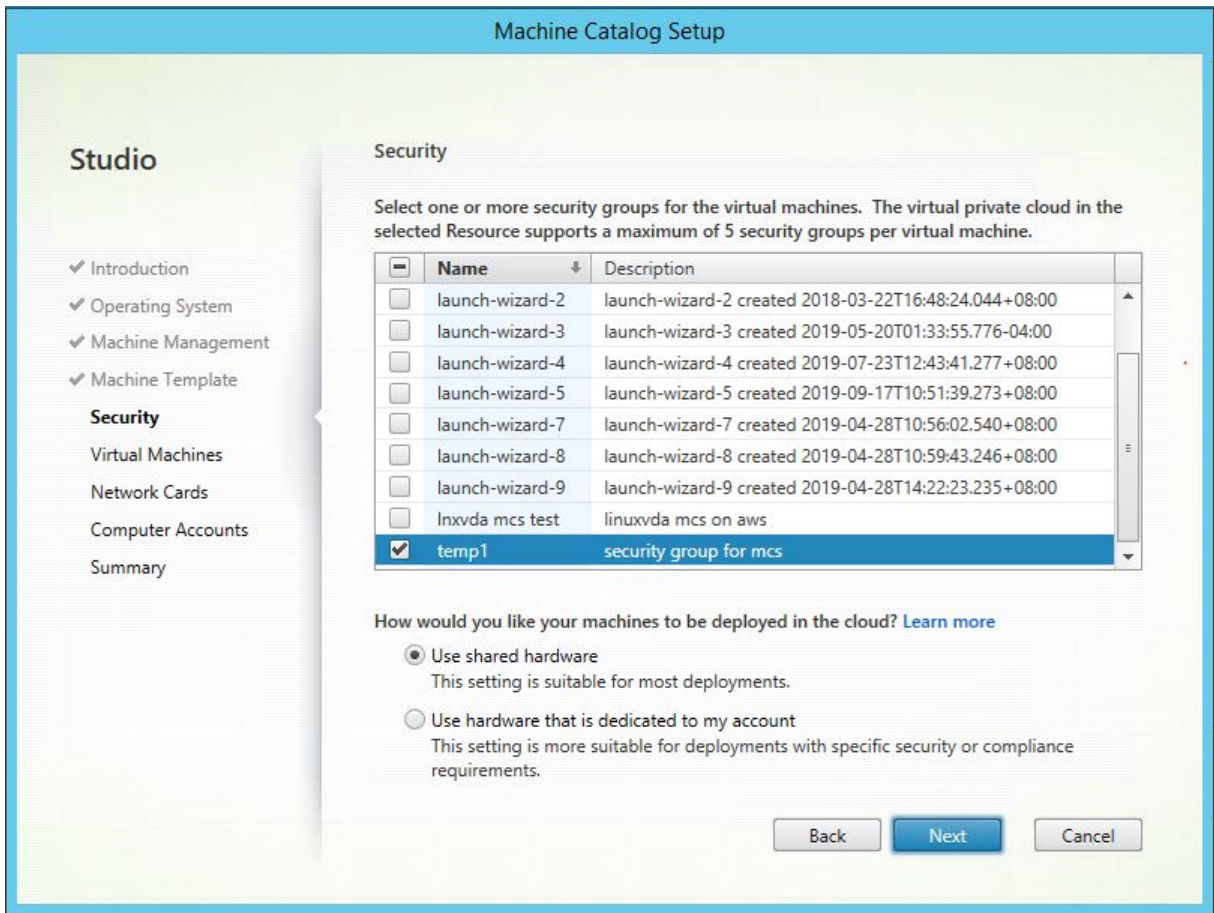
Total size of EBS Volumes: 40 GiB  
When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

Cancel
Create Image

### 步骤 3: 创建计算机目录

在 Citrix Studio 中,创建计算机目录并指定要在目录中创建的 VM 数量。创建计算机目录时,请选择您的计算机模板(之前创建的主映像),然后选择一个或多个安全组。





根据需要执行其他配置任务。有关详细信息，请参阅[使用 Studio 创建计算机目录](#)。

#### 步骤 4：创建交付组

交付组是从一个或多个计算机目录中选择的计算机的集合。它指定哪些用户可以使用这些计算机，以及可供这些用户使用的应用程序和桌面。有关详细信息，请参阅[创建交付组](#)。

#### 使用 MCS 升级您的 Linux VDA

要使用 MCS 来升级 Linux VDA，请执行以下操作：

1. 在模板计算机上升级 Linux VDA：

对于 **RHEL 7/CentOS 7**：

```
1 sudo rpm -U XenDesktopVDA-19.12.0.50-1.el7_x.x86_64.rpm
2 <!--NeedCopy-->
```

对于 **RHEL 6/CentOS 6**：

```
1 sudo rpm -U XenDesktopVDA-19.12.0.50-1.el6_x.x86_64.rpm
2 <!--NeedCopy-->
```

对于 **SUSE 12**:

```
1 sudo rpm -U XenDesktopVDA-19.12.0.50-1.sle12_x.x86_64.rpm
2 <!--NeedCopy-->
```

对于 **Ubuntu 16.04**:

```
1 sudo dpkg -i xendesktopvda_19.12.0.50-1.ubuntu16.04_amd64.deb
2 <!--NeedCopy-->
```

对于 **Ubuntu 18.04**:

```
1 sudo dpkg -i xendesktopvda_19.12.0.50-1.ubuntu18.04_amd64.deb
2 <!--NeedCopy-->
```

2. 编辑 `/etc/xdl/mcs/mcs.conf` 和 `/etc/xdl/mcs/mcs_local_setting.reg`。
3. 生成新快照。
4. 在 Citrix Studio 中，选择用于更新计算机目录的新快照。在每台计算机重新启动之前，等待一段时间。请勿手动重新启动计算机。

## 配置 Delivery Controller

May 12, 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。

注意：

Linux VDA 不支持使用 Secure ICA 进行加密。在 Linux VDA 上启用 Secure ICA 会导致会话启动失败。

## 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-->
```

## 配置 Linux VDA

November 21, 2020

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

提示：

用于收集日志的 `xdlcollect` Bash 脚本将集成到 Linux VDA 软件中并位于 `/opt/Citrix/VDA/bin` 下。安装 Linux VDA 后，可以运行 `bash /opt/Citrix/VDA/bin/xdlcollect.sh` 命令来收集日志。

日志收集完成后，压缩的日志文件将在与脚本相同的文件夹中生成。`xdlcollect` 可以询问您是否将压缩的日志文件上载到 Citrix Insight Services (CIS)。如果您同意，`xdlcollect` 将在上载完成后返回 `upload_ID`。上载不会从您的本地计算机中删除压缩的日志文件。其他用户可以使用 `upload_ID` 访问 CIS 中的日志文件。

## 将 NIS 与 Active Directory 集成

November 8, 2021

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 Virtual Apps and Desktops 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 是什么？

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。

使用本文中包含的说明时，以下环境已通过测试和验证：

- RHEL 7.7 及更高版本
- CentOS 7.7 及更高版本

## 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 [NIS/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** **sssd.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>[^\w]+)\((?P<name>.+)$))|((?P<name>[^\w]+)@
10 (?P<domain>.+$))|(^(?P<name>[^\w]+)$))
11 id_provider = proxy
12 proxy_lib_name = nis
13 auth_provider = ad
14 access_provider = ad
15 # Should be specified as the long version of the Active Directory
16 domain.
17 ad_domain = EXAMPLE.COM
18 # Kerberos settings
19 krb5_ccachedir = /tmp
20 krb5_ccname_template = FILE:%d/krb5cc_%U
21
22 # Uncomment if service discovery is not working
23 # ad_server = server.ad.example.com
24
25 # Comment out if the users have the shell and home dir set on the AD
26 side
27 default_shell = /bin/bash
28 fallback_homedir = /home/%d/%u
29
30 # Uncomment and adjust if the default principal SHORTNAME$@REALM is not
31 available
32 # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
33 <!--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/sss/sss.conf
chmod 0600 /etc/sss/sss.conf
restorecon /etc/sss/sss.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** 脚本中的额外解决方案, 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 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：

```
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。要解决这个问题，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。

### 限制

Linux VDA 不支持单个用户启动同一应用程序的多个并发实例。

### 已知问题

在发布应用程序期间发现了以下已知问题：

- 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、Metacity 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/title/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。

## Remote PC Access

March 16, 2022

## 概述

Remote PC Access 是 Citrix Virtual Apps and Desktops 的扩展程序。它使组织能够轻松地允许员工以安全的方式远程访问其物理办公室 PC。如果用户可以访问其办公室 PC，他们可以访问完成工作所需的所有应用程序、数据和资源。

Remote PC Access 使用交付虚拟桌面和应用程序的相同 Citrix Virtual Apps and Desktops 组件。部署和配置 Remote PC Access 的要求和流程与部署 Citrix Virtual Apps and Desktops 以交付虚拟资源所需的要求和流程相同。这种统一性提供了一致且统一的管理体验。用户通过使用 Citrix HDX 交付其远程办公室 PC 会话，获得最佳用户体验。

有关详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的 [Remote PC Access](#)。

## 配置

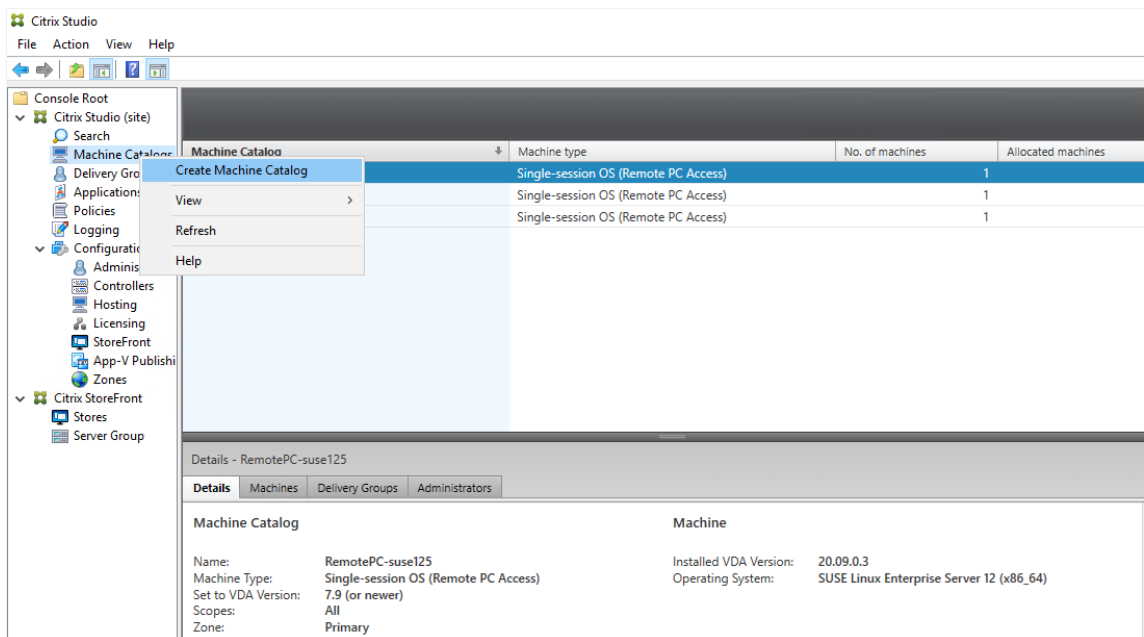
要交付 Linux PC 会话，请在目标 PC 上安装 Linux VDA，创建 **Remote PC Access** 类型的计算机目录，然后创建交付组，以使计算机目录中的 PC 可供请求访问的用户使用。以下部分详细介绍了该过程：

### 步骤 1 - 在目标 PC 上安装 Linux VDA

建议您使用[轻松安装](#)来安装 Linux VDA。在安装过程中，将 `CTX_XDL_VDI_MODE` 变量的值设置为 Y。

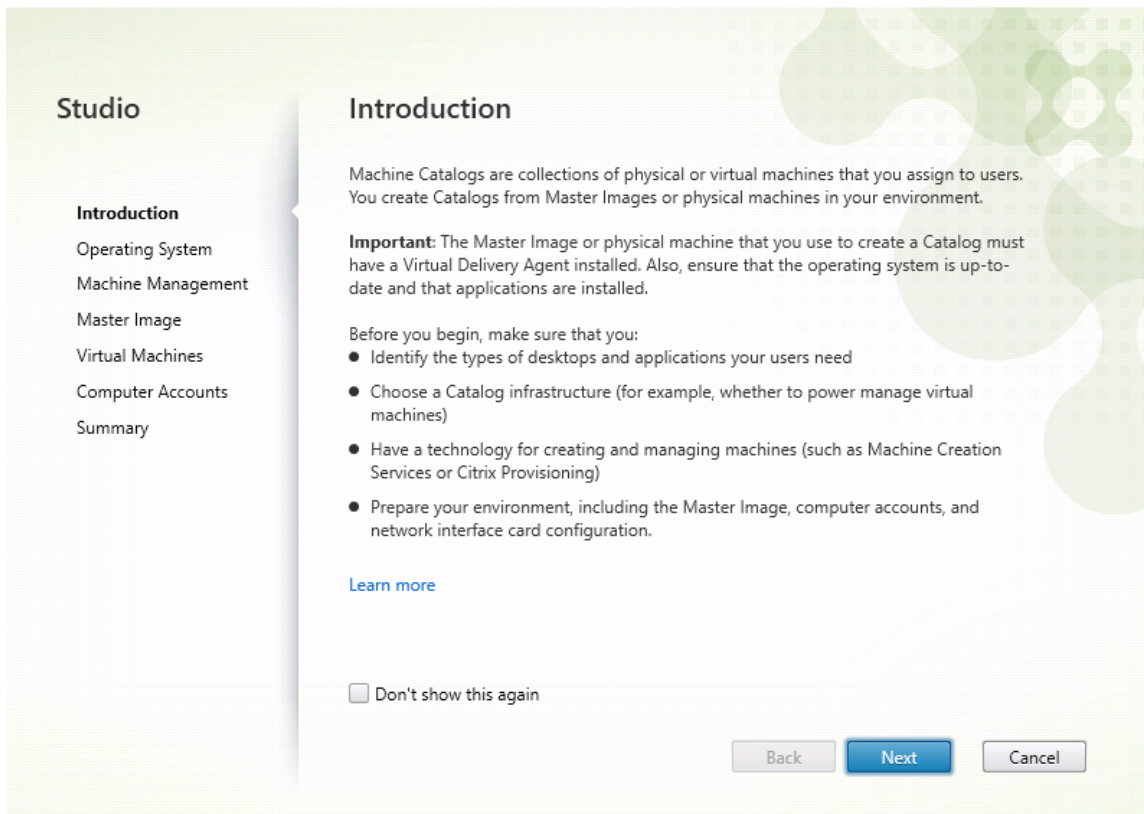
### 步骤 2 - 创建 **Remote PC Access** 类型的计算机目录

1. 在 Citrix Studio 中，右键单击计算机目录，然后从快捷菜单中选择创建计算机目录。



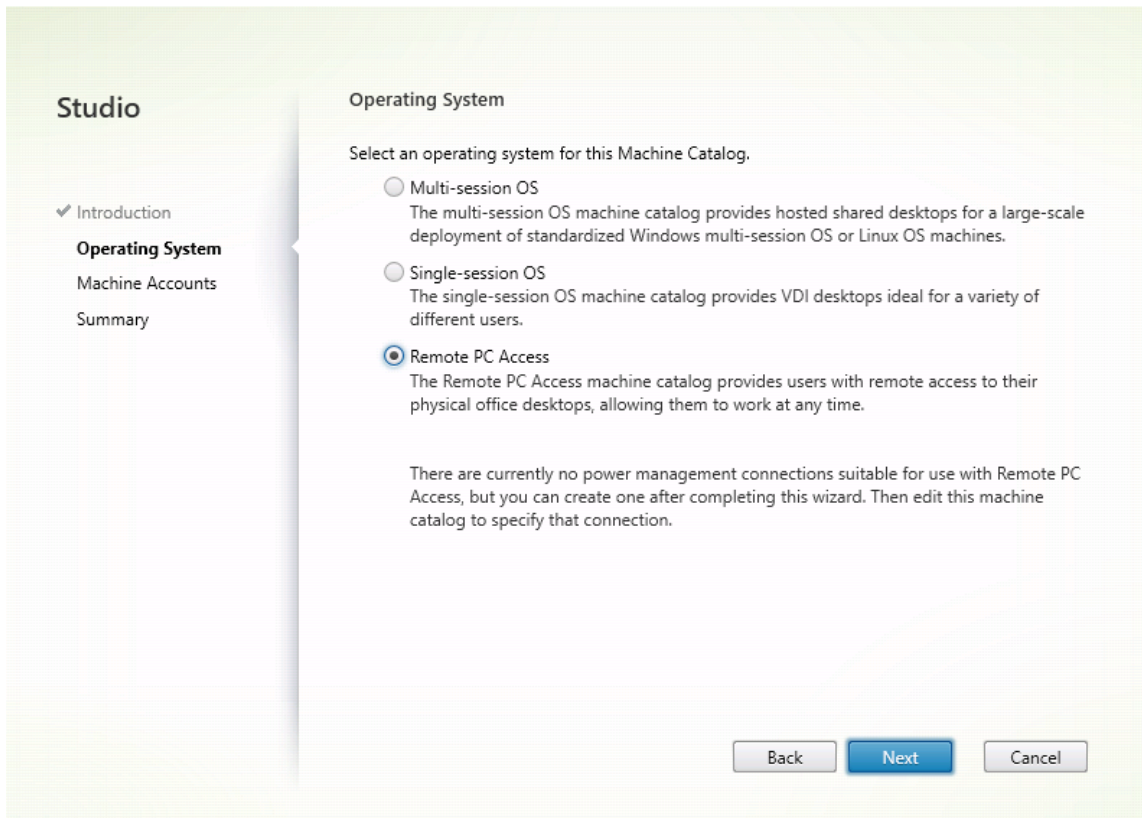
2. 单击简介页面上的下一步。

Machine Catalog Setup



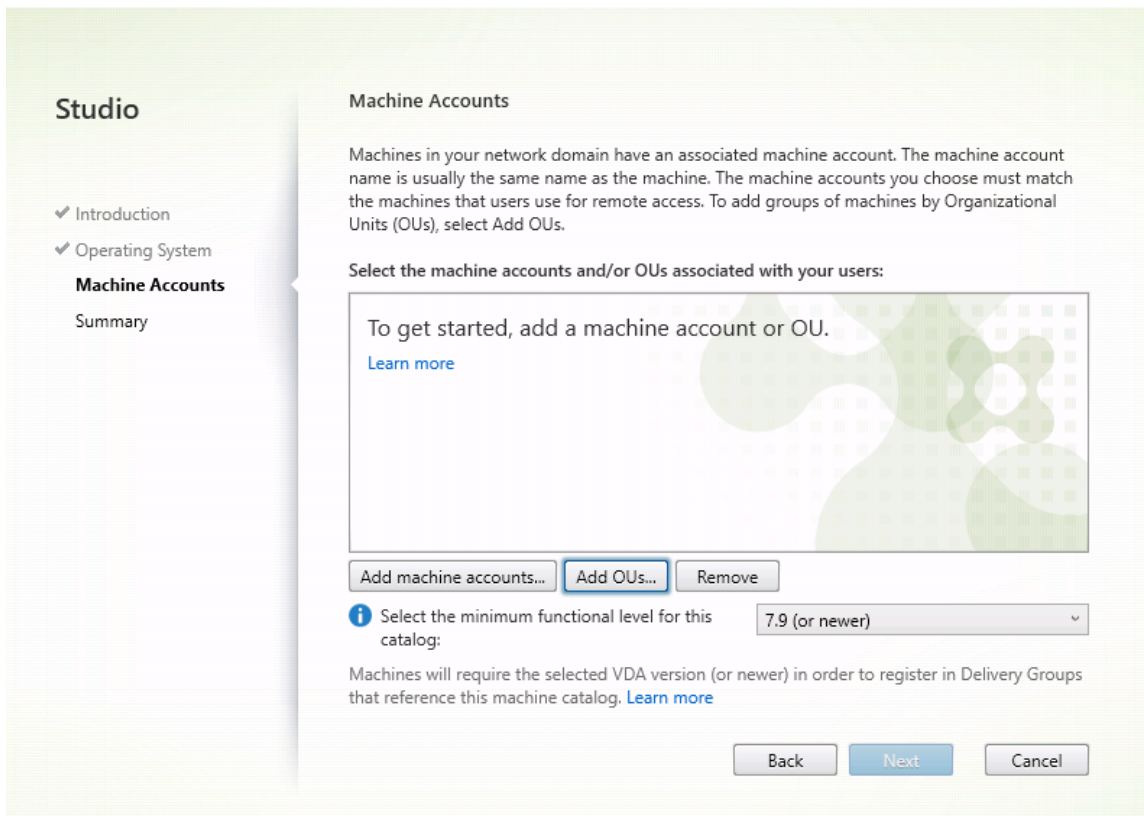
3. 在操作系统页面上选择 **Remote PC Access**。

Machine Catalog Setup



4. 单击添加 **OU** 以选择包含目标 PC 的 OU，或者单击添加计算机帐户将单个计算机添加到计算机目录中。

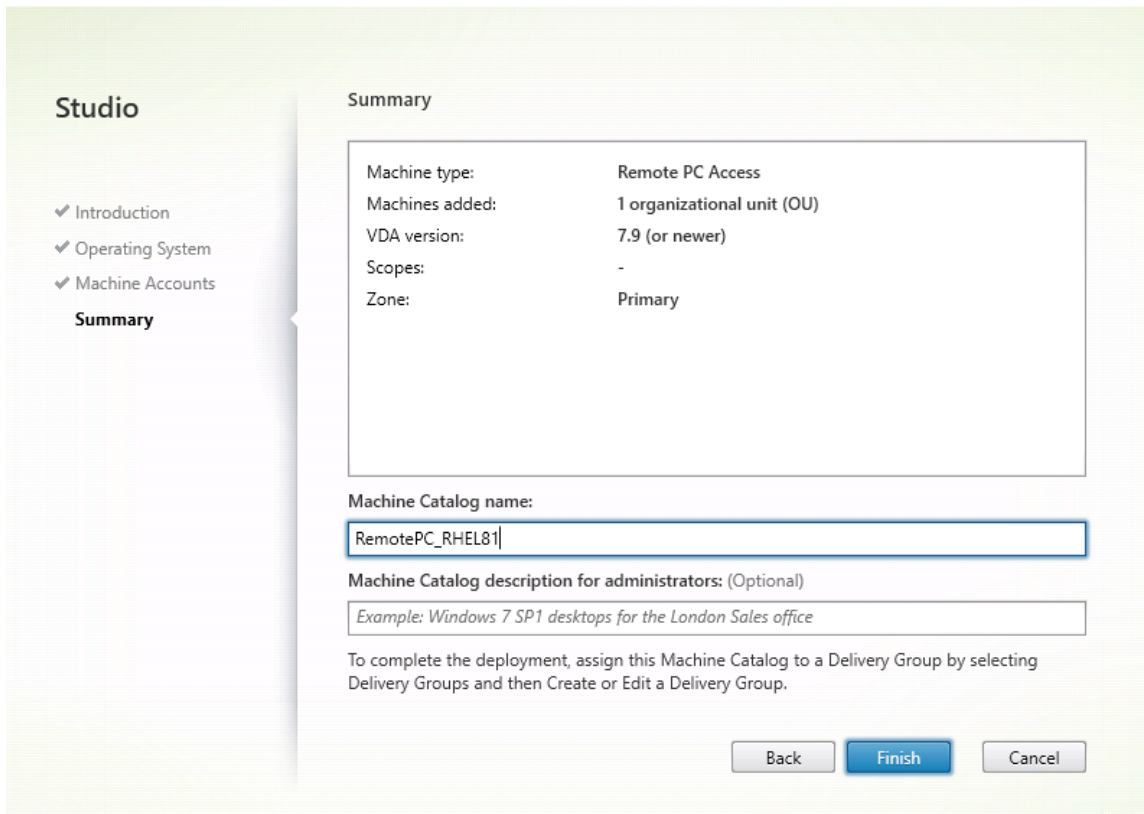
Machine Catalog Setup



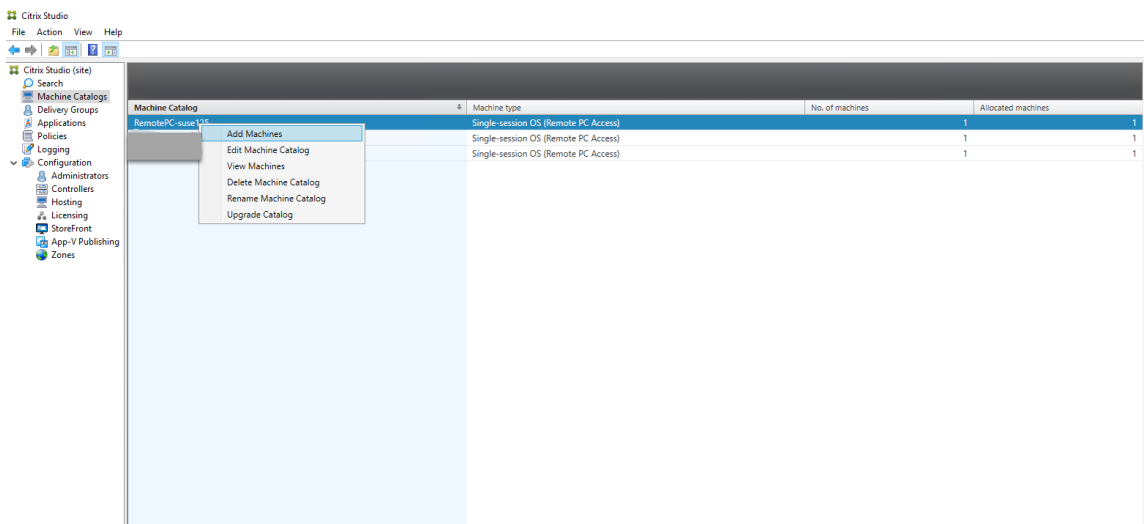
5. 命名计算机目录。



Machine Catalog Setup

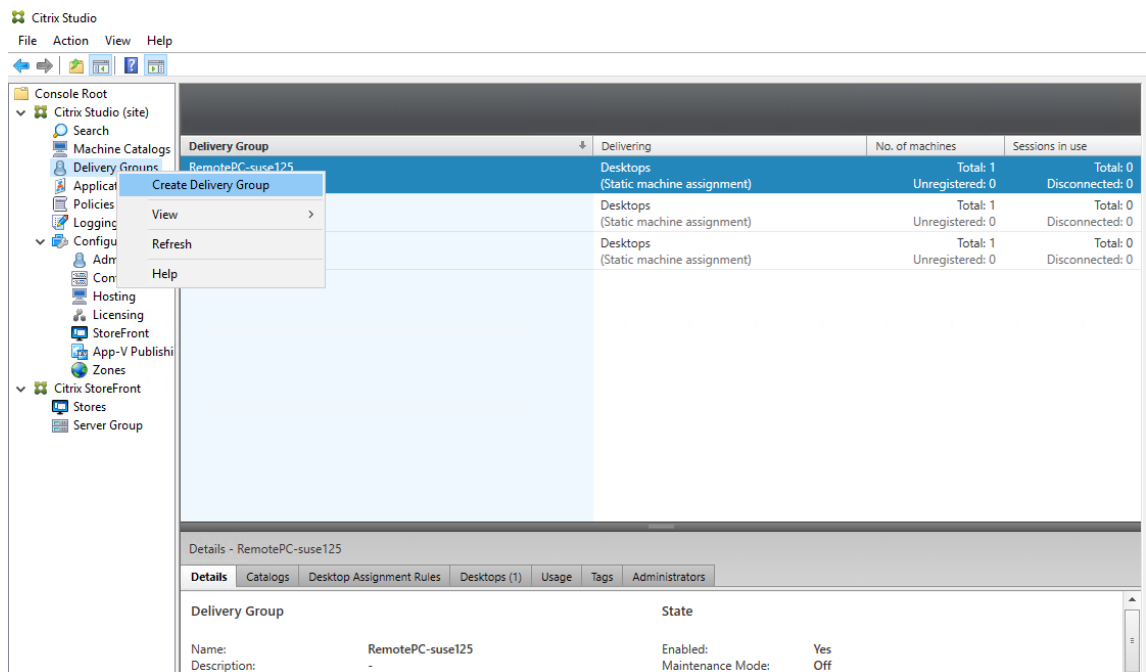


6. (可选) 右键单击计算机目录以执行相关操作。

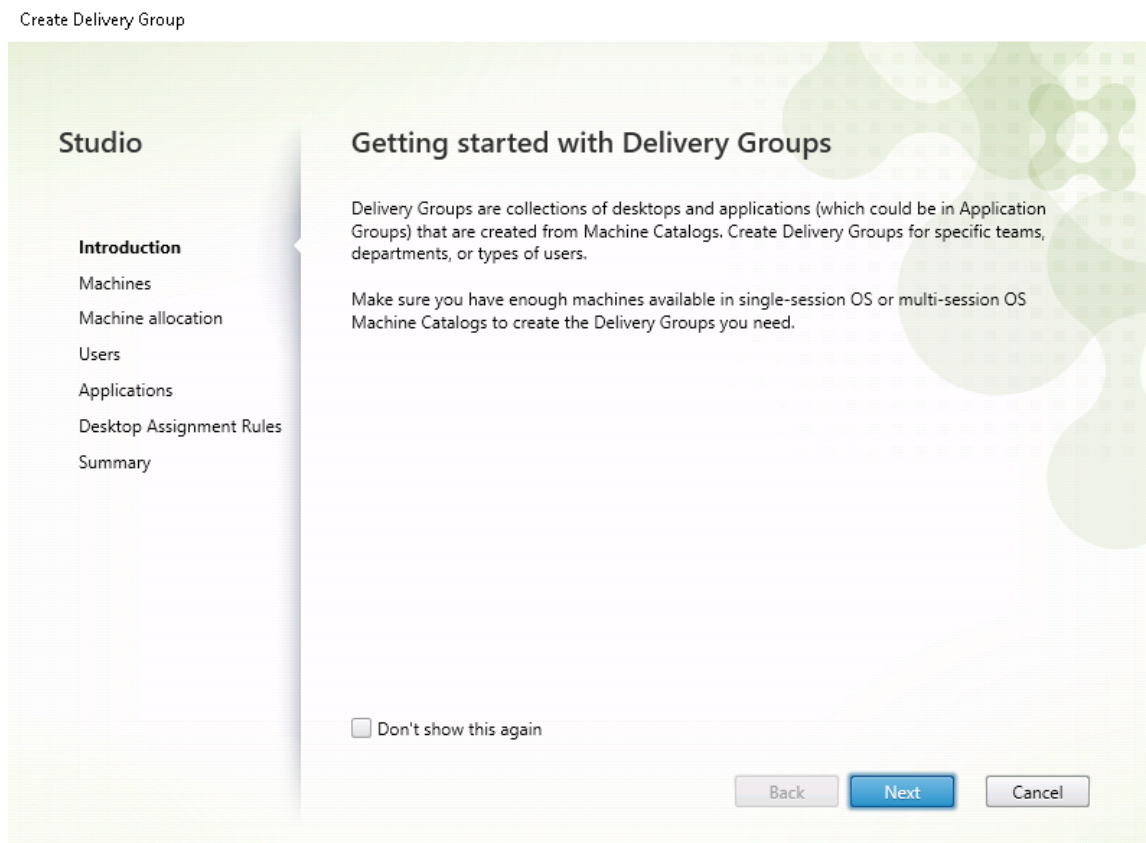


步骤 3 - 创建交付组，以使计算机目录中的 PC 可供请求访问权限的用户使用

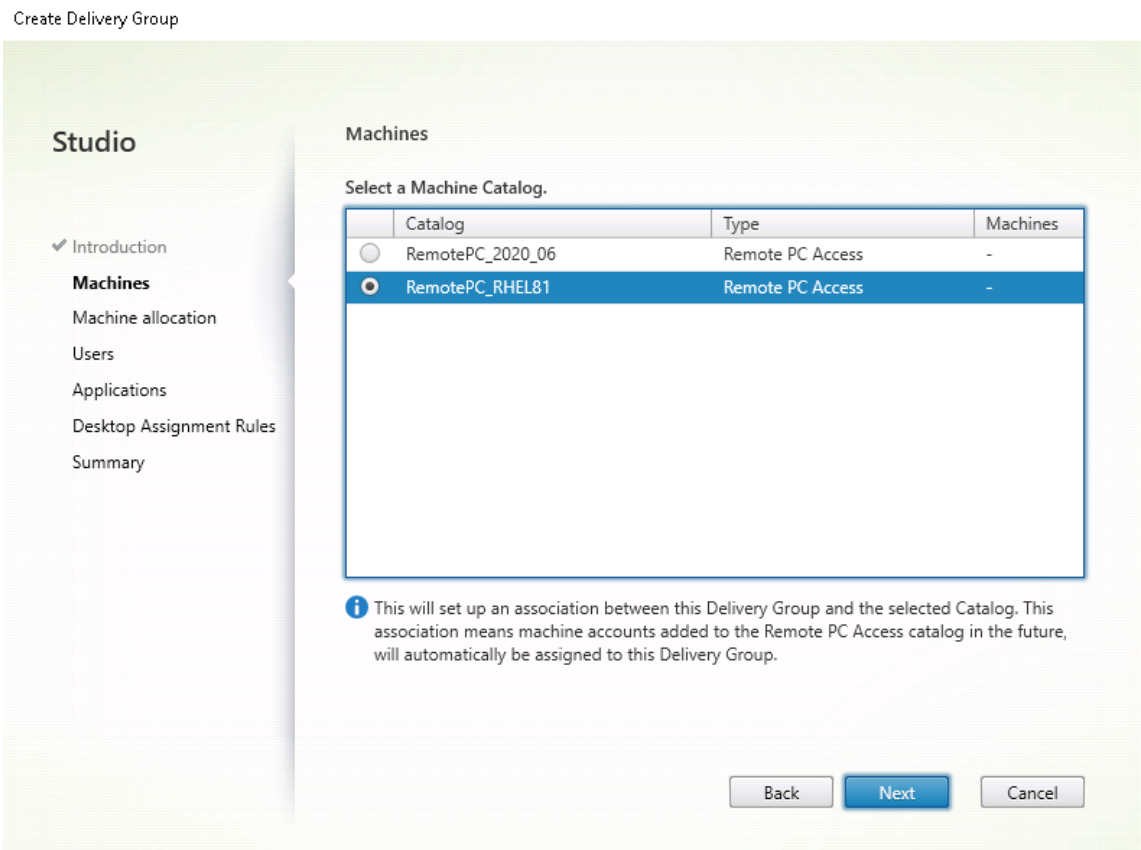
1. 在 Citrix Studio 中，右键单击交付组，然后从快捷菜单中选择创建交付组。



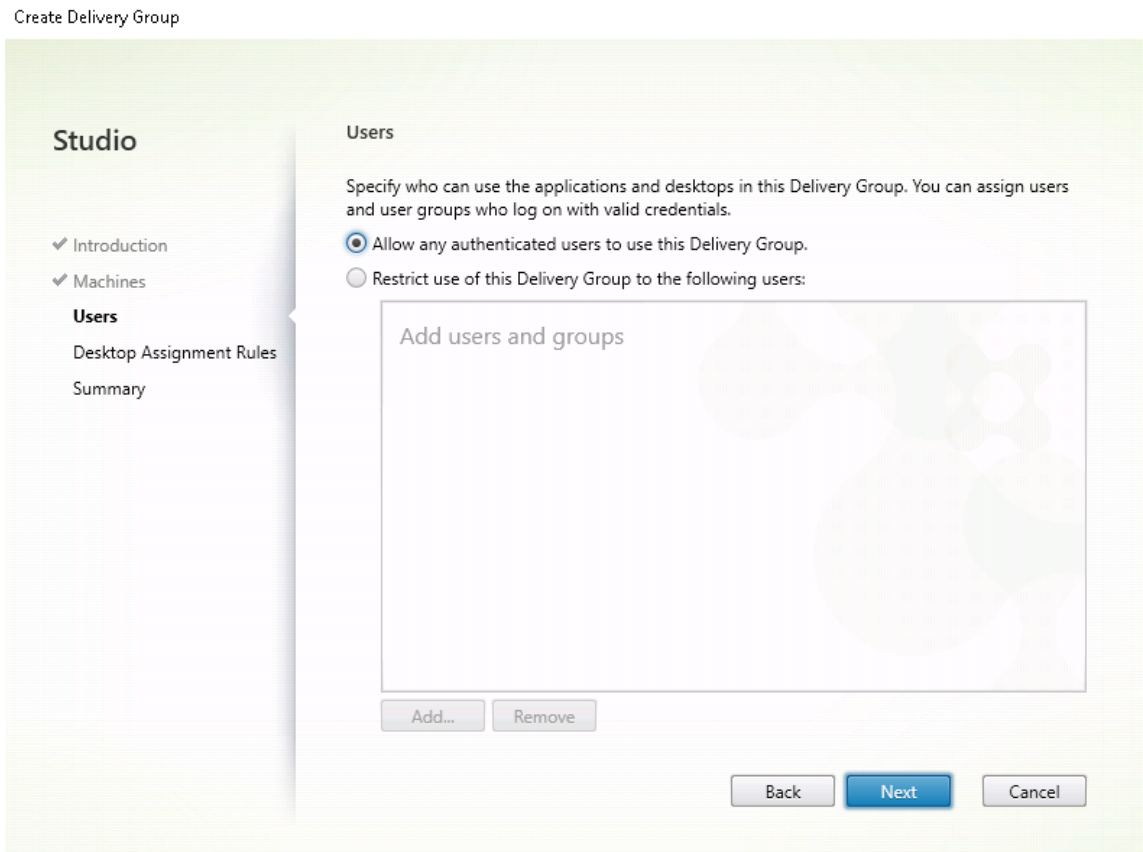
2. 单击交付组入门页面上的下一步。



3. 选择在步骤 2 中创建的计算机目录，以将其与交付组关联。



4. 添加可以访问计算机目录中 PC 的用户。添加的用户可以使用客户端设备上的 Citrix Workspace 应用程序远程访问 PC。



## 注意事项

这些注意事项是 Linux VDA 特有的：

- 请仅在非 3D 模式下在物理机上使用 Linux VDA。由于 NVIDIA 驱动程序的限制，当启用了 HDX 3D 模式时，PC 的本地屏幕无法停止，并显示会话的活动。显示此屏幕存在安全风险。
- 请对物理 Linux 计算机使用单会话操作系统类型的计算机目录。
- 集成的局域网唤醒功能不适用于 Linux 计算机。
- 自动用户分配不适用于 Linux 计算机。通过自动用户分配，用户在本地登录 PC 时会自动将其分配给各自的计算机。在没有管理员干预的情况下执行此登录。通过在客户端设备上运行的 Citrix Workspace 应用程序，用户可以在 Remote PC Access 桌面会话中访问办公室 PC 上的应用程序和数据。
- 如果用户已在本地登录到其 PC，尝试从 StoreFront 启动 PC 将失败。
- 节能选项不适用于 Linux 计算机。

## 更多资源

下面是 Remote PC Access 的其他资源：

- 解决方案设计指南：[Remote PC Access 设计决策](#)。
- Remote PC Access 体系结构的示例：[Citrix Remote PC Access 解决方案的参考体系结构](#)。

## 打印

March 16, 2022

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。在安装 VDA 时安装过滤器。还可以根据分发情况手动安装过滤器。例如：

在 **RHEL 7** 上：

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

在 **RHEL 6**：

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

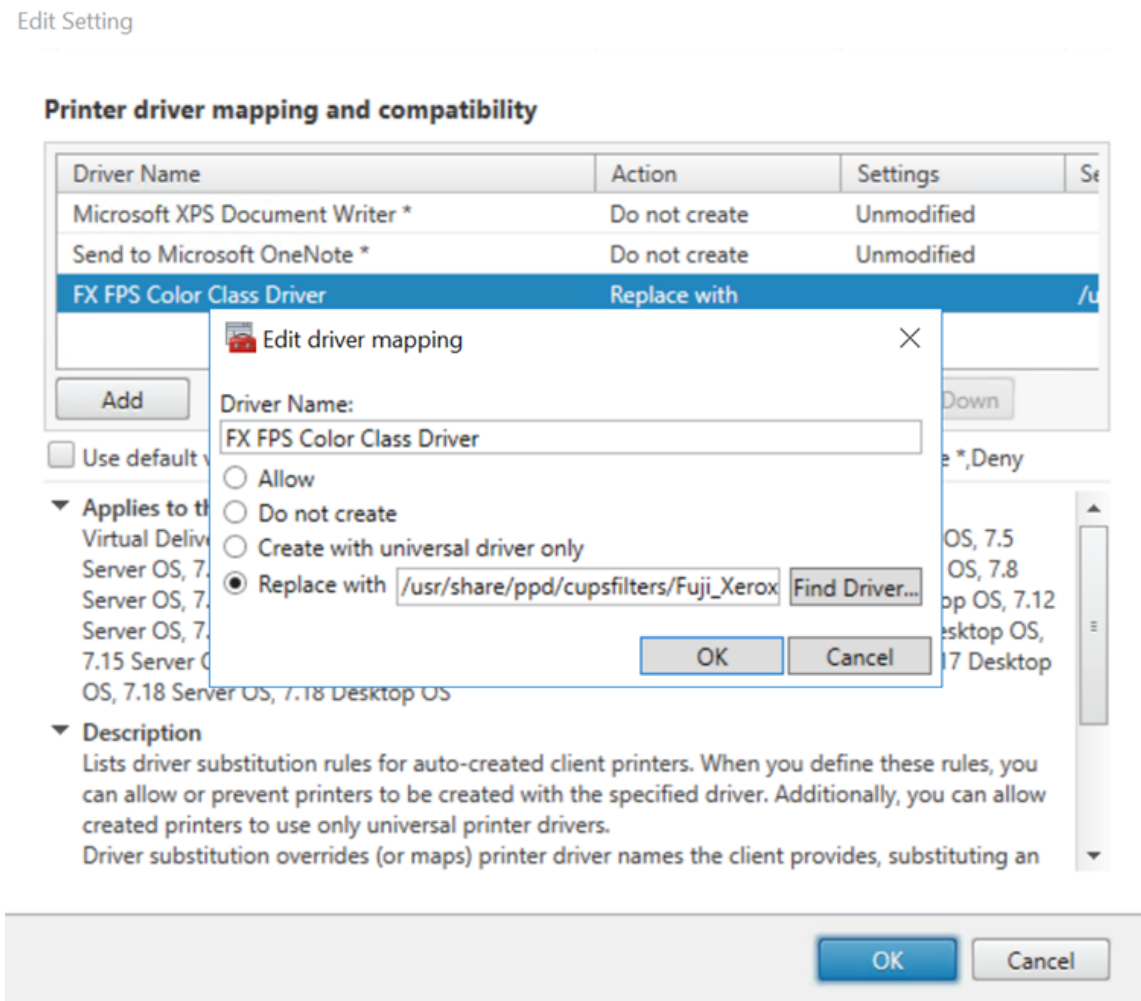
## 配置

Citrix 提供了三种类型的通用打印机驱动程序（postscript、pcl5 和 pcl6）。但是，通用打印机驱动程序可能与您的客户端打印机不兼容。在这种情况下，早期版本中的唯一选择为编辑 `~/.CitrixProfile$CLIENT_NAME` 配置文件。自版本 1906 起，可以选择改为在 Citrix Studio 中配置打印机驱动程序映射和兼容性策略。

要在 Citrix Studio 中配置打印机驱动程序映射和兼容性策略，请执行以下操作：

1. 选择打印机驱动程序映射和兼容性策略。
2. 单击添加。
3. 使用客户端打印机的驱动程序名称填写驱动程序名称。如果使用适用于 Linux 的 Citrix Workspace 应用程序，请改为填写打印机名称。

4. 选择替换为并键入 VDA 上的驱动程序文件的绝对路径。



注意：

- 仅支持 PPD 驱动程序文件。
- 不支持打印机驱动程序映射和兼容性策略的其他选项。只有替换为生效。

#### 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，打印机名称不同。

- 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的桌面打印机上打印，也无法在已发布的桌面会话中的应用程序打印机上打印。

## 故障排除

### 无法打印

打印无法正常工作时，请检查打印守护程序 **ctxlpmngt** 和 CUPS 框架。

打印守护程序 **ctxlpmngt** 是一个按会话进程，必须在会话期间内运行。运行以下命令以确认打印守护程序是否正在运行。如果 **ctxlpmngt** 未运行，请从命令行中手动启动 **ctxlpmngt**。

```
1 ps -ef | grep ctxlpmngt
2 <!--NeedCopy-->
```

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，可通过运行以下命令进行检查：

```
1 service cxcups status
2 <!--NeedCopy-->
```

### 收集 **CUPS** 日志的额外步骤

要收集 CUPS 日志，请运行以下命令以配置 CUPS 服务文件。否则，CUPS 日志无法记录在 **hdx.log** 中：

```
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：

此配置仅在出现问题时收集完整的打印日志时设置。在正常情况下，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 `~/.CtxlpProfile$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 xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
9
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）。可以根据打印机属性配置驱动程序类型。



例如，如果客户端默认打印机驱动程序类型为 PCL5，请将 **drivertype** 设置为：

```
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：

1. 登录到已发布的桌面会话。
2. 运行 **vi ~/.CtxlpProfile\$CLIENT\_NAME** 命令。
3. 添加以下字段以在 Linux VDA 上保存后台打印文件：

```
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. 检查后台打印是否为空。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。检查内容是否正确。  
  
如果后台打印文件是 PCL，或者客户端操作系统是 Windows，则将后台打印文件复制到客户端，并使用不同的打印机驱动程序在客户端打印机上打印该文件。
8. 将映射的打印机更改为使用不同的打印机驱动程序。下例以 PostScript 客户端打印机为例：
  - 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/dsk\$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**（制造商）和 **Model**（型号）字段中，从 Citrix UPD 驱动程序中选择不同的打印机驱动程序。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）驱动程序。保存更改。
- 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新选择的驱动程序。

## 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：

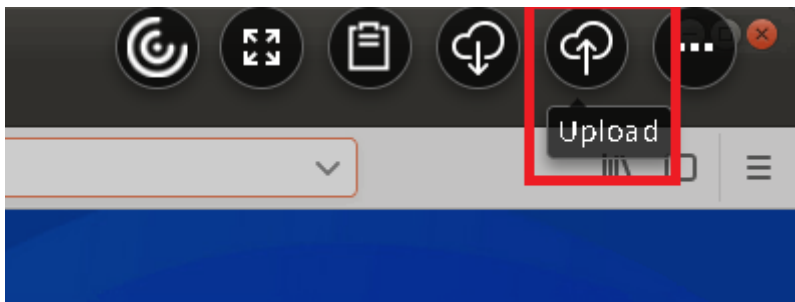
```
1 <Policy default>
2
3 # Job/subscription privacy...
4
5 JobPrivateAccess default
6
7 JobPrivateValues default
8
9 SubscriptionPrivateAccess default
10
11 SubscriptionPrivateValues default
12
```

```
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-->
```

## 文件传输

March 16, 2022

支持在 Linux VDA 和客户端设备之间进行文件传输。当客户端设备运行支持 HTML5 沙盒属性的 Web 浏览器时，可以使用此功能。HTML5 沙盒属性允许用户使用适用于 HTML5 和 Chrome 的 Citrix Workspace 应用程序访问虚拟桌面和应用程序。在已发布的会话中，您可以使用 Citrix Workspace 应用程序的工具栏在 Linux VDA 和客户端设备之间上载和下载文件。例如，可以单击工具栏上的上载图标，选择客户端设备上的某个文件，然后将该文件上载到 Linux VDA。

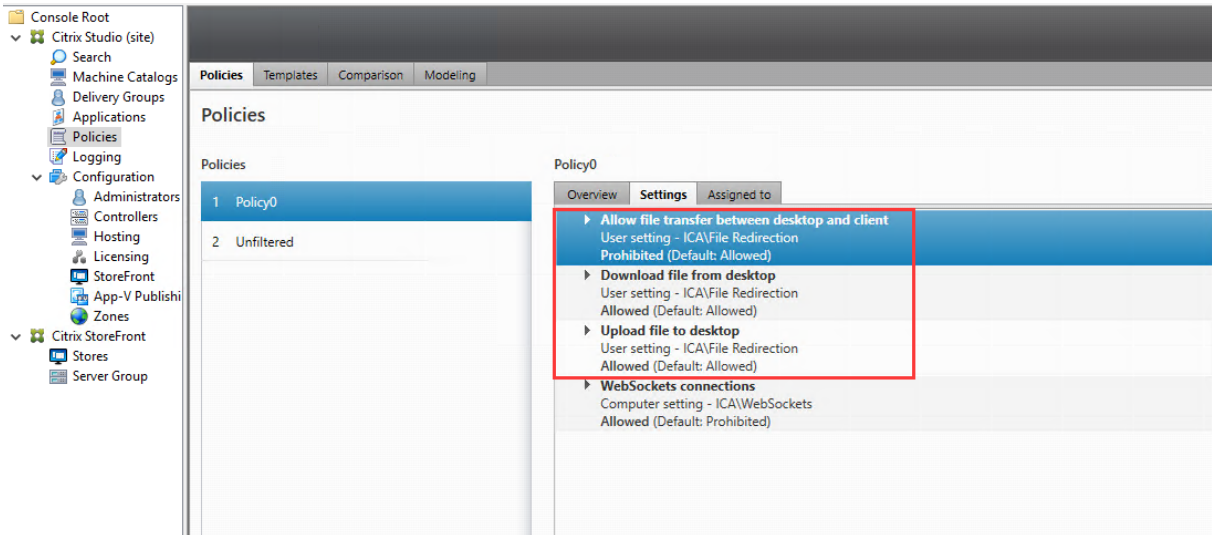


### 注意：

此功能适用于 RedHat7.7、CentOS7.6、SUSE12.3、Ubuntu16.04 和 Ubuntu18.04。  
要使用此功能，请确保启用 Citrix Workspace 应用程序的工具栏。

## 文件传输策略

可以使用 Citrix Studio 设置文件传输策略。默认启用文件传输。



### 策略说明：

- 允许在桌面与客户端之间传输文件。允许或阻止用户在 Citrix Virtual Apps and Desktops 会话与其设备之间传输文件。
- 从桌面下载文件。允许或阻止用户将文件从 Citrix Virtual Apps and Desktops 会话下载到其设备。
- 将文件上传到桌面。允许或阻止用户将文件从其设备上载到 Citrix Virtual Apps and Desktops 会话。

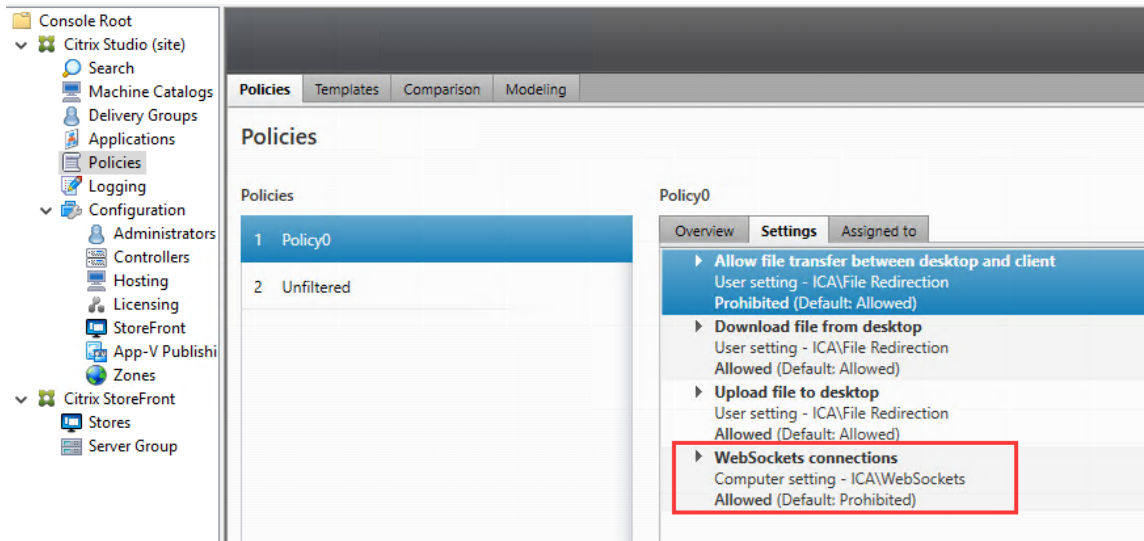
### 注意：

为确保从桌面下载文件和将文件上传到桌面策略生效，请将允许在桌面与客户端之间传输文件策略设置为允许。

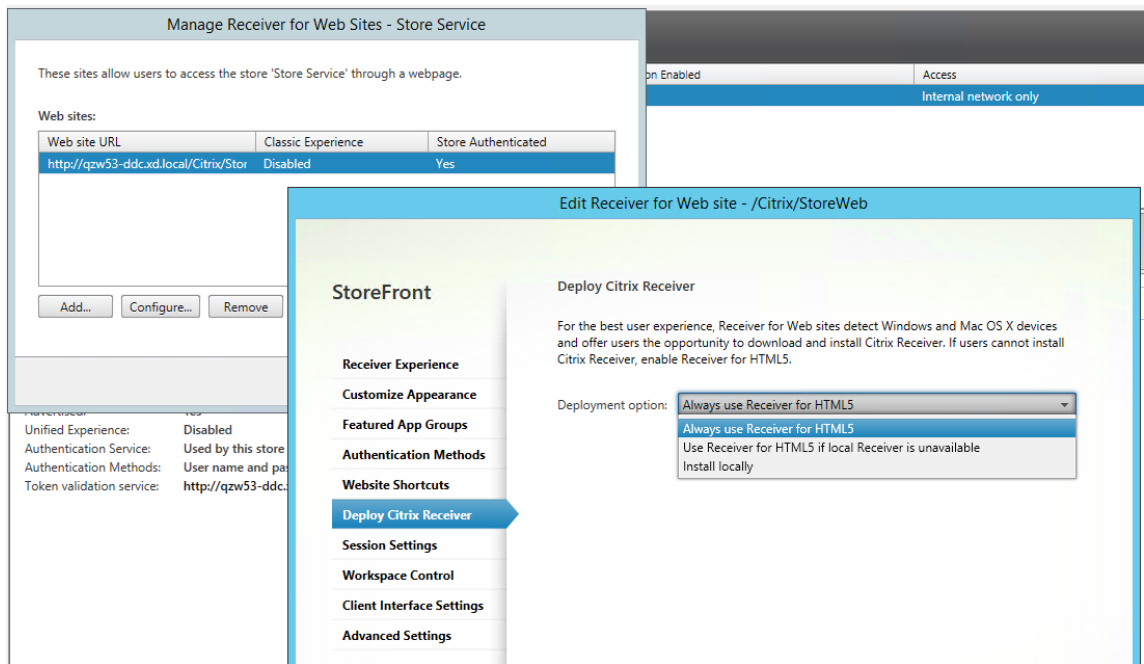
### 使用情况

要通过适用于 HTML5 的 Citrix Workspace 应用程序使用文件传输功能，请执行以下操作：

1. 在 Citrix Studio 中，将 **WebSocket** 连接策略设置为允许。



2. 在 Citrix Studio 中，通过上述文件传输策略启用文件传输功能。
3. 在 Citrix StoreFront 管理控制台中，单击应用商店，选择管理 **Receiver for Web** 站点节点，然后通过选择始终使用 **Receiver for HTML5** 选项来启用 Citrix Receiver for HTML5。



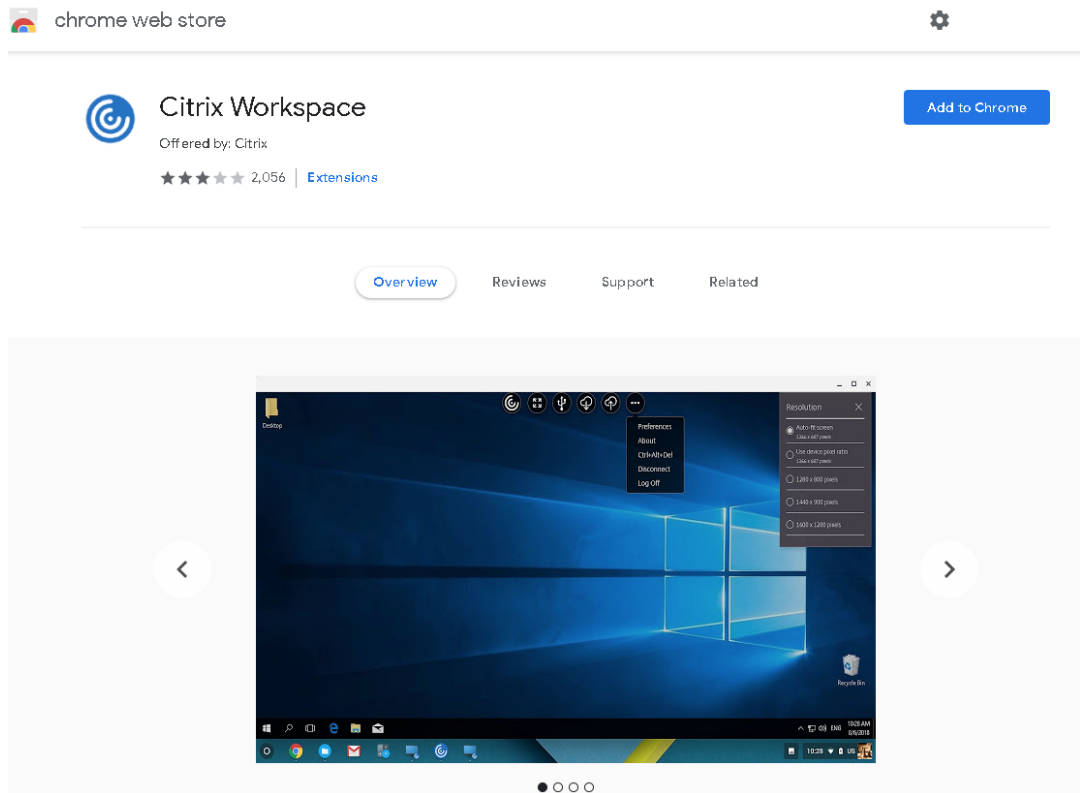
4. 启动虚拟桌面或 Web 浏览器应用程序会话。在 Linux VDA 和客户端设备之间上传和下载文件。

要通过适用于 Chrome 的 Citrix Workspace 应用程序使用文件传输功能，请执行以下操作：

1. 通过上述文件传输策略启用文件传输功能。
2. 从 Chrome 网上应用店中获取 Citrix Workspace 应用程序。

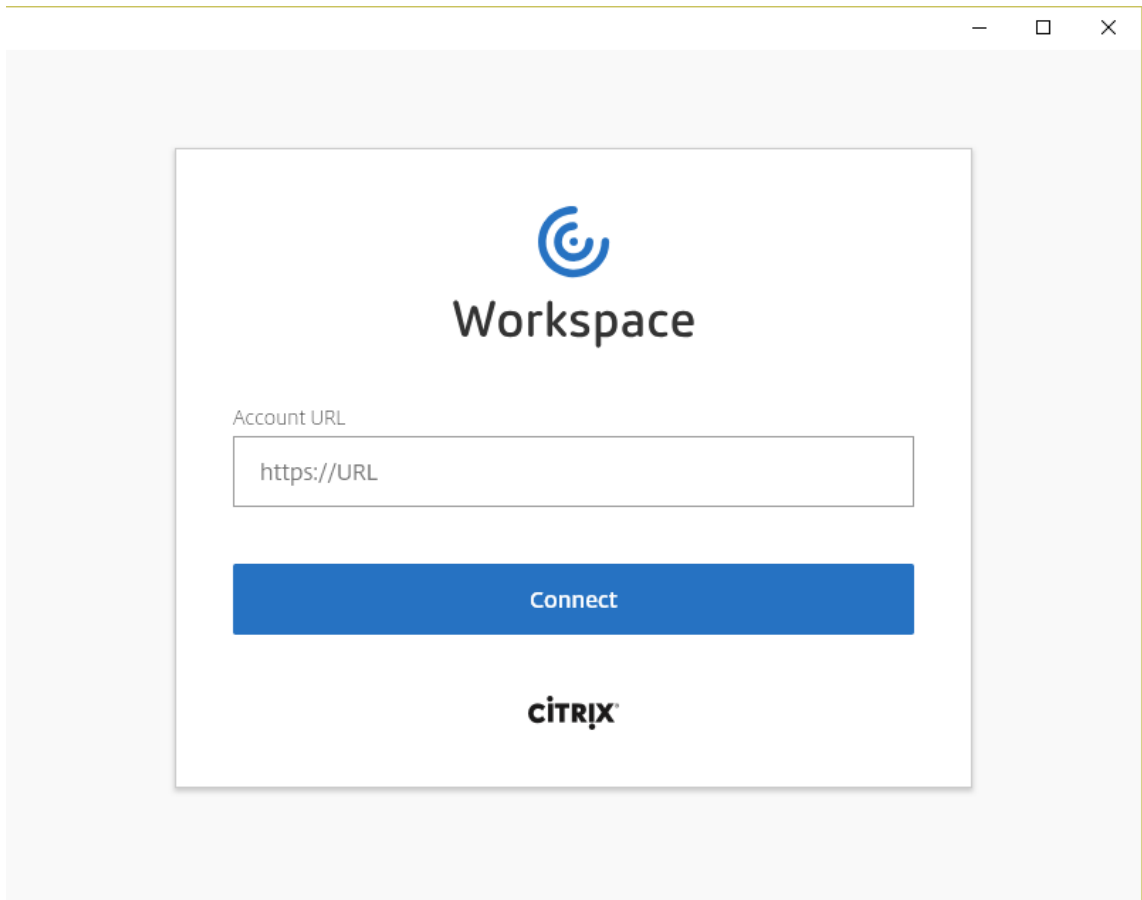
如果您已将适用于 Chrome 的 Citrix Workspace 应用程序添加到“Chrome 应用程序”页面，请跳过此步骤。

- a) 在 Google Chrome 的搜索框中键入适用于 **Chrome** 的 **Citrix Workspace**。单击搜索图标。
- b) 在搜索结果中，单击指向 Chrome 网上应用店（提供 Citrix Workspace 应用程序）的 URL。



- c) 单击添加到 **Chrome** 以将 Citrix Workspace 应用程序添加到 Google Chrome 中。
3. 在“Chrome 应用程序”页面上单击“适用于 Chrome 的 Citrix Workspace 应用程序”。
4. 键入要连接的 StoreFront 应用商店的 URL。

如果您之前键入了该 URL，请跳过此步骤。



5. 启动虚拟桌面或 Web 浏览器应用程序会话。在 Linux VDA 和客户端设备之间上传和下载文件。

## PDF 打印

May 12, 2020

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

April 18, 2024

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。

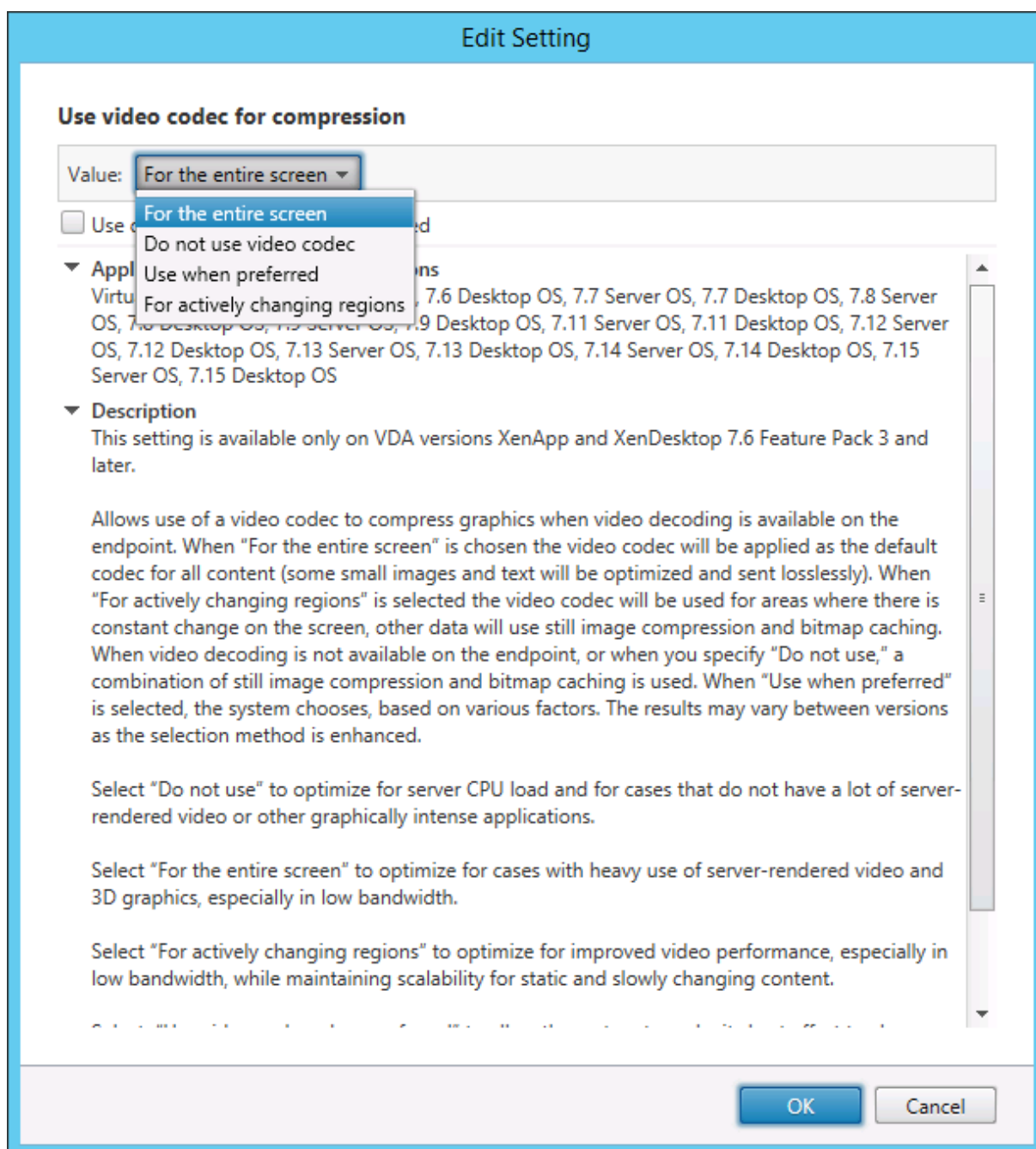
### 配置

Thinwire 是 Linux VDA 中使用的显示内容远程处理技术。该技术允许一台计算机上生成的图形传输（通常跨网络）到另一台计算机上进行显示。

[使用视频编解码器进行压缩](#)图形策略设置默认图形模式，并针对不同的用例提供以下选项：

- 偏好时使用。这是默认设置。无需执行其他配置。保持此设置可确保为所有 Citrix 连接选择 Thinwire，且 Thinwire 已针对典型桌面工作负载在可扩展性、带宽和卓越图像质量方面经过优化。
- 针对整个屏幕。为 Thinwire 提供全屏 H.264 或 H.265，以针对改进用户体验和带宽使用情况进行优化，尤其是在大量使用 3D 图形的情况下。
- 针对主动变化的区域。Thinwire 中的自适应显示技术识别移动图像（视频、动态 3D），并只在图像移动的屏幕部分使用 H.264。选择性使用 **H.264** 视频编解码器支持 HDX Thinwire 检测屏幕的频繁更新部分（例如视频内容），并使用 H.264 视频编解码器对其进行编码。对于屏幕的其余部分（包括文本和摄影图片），仍继续使用图像压缩（JPEG、RLE）和位图缓存。用户可获得以下益处：使用较低带宽、提高视频内容质量以及在其他位置获得无损文本或高质量图像。要启用此功能，请将策略设置使用视频编解码器进行压缩更改为偏好时使用（默认设置）或针对主动变化的区域。有关详细信息，请参阅[图形策略设置](#)。





一些其他策略设置（包括以下视频显示策略设置）可以用于对显示远程处理技术的性能进行完善：

- 简单图形的首选颜色深度
- 目标帧速率
- 视觉质量

在 **Thinwire** 中将 **H.264** 用于“无损构建”

默认情况下，现在对于移动图像，视觉质量策略设置的无损构建首选项为 H.264 而不是 JPEG。

H.264 编码可提供卓越的图像质量。使用视频编解码器进行压缩策略控制该首选项，默认设置为偏好时使用。要强制无损构建使用 JPEG，请将使用视频编解码器进行压缩策略设置为不使用视频编解码器。如果客户端不支持选择性 H.264，无论策略设置是什么，无损构建都将回退到 JPEG。Citrix Receiver for Windows 4.9 到 4.12、Citrix Receiver for Linux 13.5 到 13.10、适用于 Windows 的 Citrix Workspace 应用程序 1808 及更高版本，以及适用于 Linux 的 Citrix Workspace 应用程序 1808 及更高版本支持选择性 H.264。有关视觉质量和使用视频编解码器进行压缩策略设置的详细信息，请参阅[视觉显示策略设置](#)和[图形策略设置](#)。

支持 **H.265** 视频编解码器

从 7.18 版起，Linux VDA 支持使用 H.265 视频编解码器对远程图形和视频进行硬件加速。您可以在 Citrix Receiver for Windows 4.10 到 4.12 和适用于 Windows 的 Citrix Workspace 应用程序 1808 及更高版本上使用此功能。要从此功能受益，请在 Linux VDA 和客户端上启用此功能。如果客户端的 GPU 不支持使用 DXVA 接口进行 H.265 解码，“图形的 H.265 解码”策略设置将被忽略，会话将回退到使用 H.264 视频编解码器。有关详细信息，请参阅[H.265 视频编码](#)。

要在 VDA 上启用 H.265 硬件编码，请执行以下操作：

1. 启用使用视频编解码器的硬件编码策略。
2. 启用针对 **3D** 图形工作负载优化策略。
3. 确保使用视频编解码器进行压缩策略采用默认设置，或设置为针对整个屏幕。
4. 确保视觉质量策略未设置为无损构建或始终无损。

要在客户端上启用 H.265 硬件编码，请参阅[H.265 视频编码](#)。

支持 **YUV444** 软件编码

Linux VDA 支持 YUV444 软件编码。YUV 编码方案会向每个像素分配亮度和颜色值。在 YUV 中，**Y** 表示亮度或 luma 值，**UV** 表示颜色或 chroma 值。您可以在 Citrix Receiver for Windows 4.10 到 4.12 和适用于 Windows 的 Citrix Workspace 应用程序 1808 及更高版本上使用 Linux VDA 的这一功能。

每个唯一的 Y、U 和 V 值均包含 8 位数或一个字节。YUV444 数据格式以 24 位/像素的速度传输。YUV422 数据格式可在两个像素之间共享 U 和 V 值，从而导致平均传输速率为 16 位/像素。下表显示了 YUV444 和 YUV420 之间的直观比较。

YUV444

|   | A      | B      | C      |
|---|--------|--------|--------|
| 1 | Citrix | Citrix | Citrix |
| 2 | Citrix | Citrix | Citrix |
| 3 | Citrix | Citrix | Citrix |
| 4 | Citrix | Citrix | Citrix |
| 5 | Citrix | Citrix | Citrix |
| 6 | Citrix | Citrix | Citrix |

YUV420

|   | A      | B      | C      |
|---|--------|--------|--------|
| 1 | Citrix | Citrix | Citrix |
| 2 | Citrix | Citrix | Citrix |
| 3 | Citrix | Citrix | Citrix |
| 4 | Citrix | Citrix | Citrix |
| 5 | Citrix | Citrix | Citrix |
| 6 | Citrix | Citrix | Citrix |

要在 VDA 上启用 YUV444 软件编码，请执行以下操作：

1. 确保将使用视频编解码器进行压缩策略设置为针对整个屏幕。
2. 确保将视觉质量策略设置为始终无损或无损构建。

根据带宽估算值调整平均位速率

通过根据带宽估算值调整平均位速率，Citrix 增强了 HDX 3D Pro 硬件编码。

使用 HDX 3D Pro 硬件编码时，VDA 可以间歇性地估计网络带宽并根据带宽估算值调整已编码的帧的位速率。这一新增功能提供了一种平衡清晰度和流畅度的机制。

默认情况下启用此功能。要禁用此功能，请运行以下命令：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
 CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
 DisableReconfigureEncoder" -d "0x00000001" --force
2 <!--NeedCopy-->
```

除了使用此功能之外，您还可以运行以下命令来调整清晰度和流畅度。**AverageBitRatePercent** 和 **MaxBitRatePercent** 参数将设置带宽使用情况的百分比。设置的值越高，图形就越清晰，但流畅度越低。建议的设置范围为 50 到 100。

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
 CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
 AverageBitRatePercent" -d "90" --force
2
3 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
 CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
 MaxBitRatePercent" -d "100" --force
4 <!--NeedCopy-->
```

在调整平均位速率时，如果您的屏幕画面保持不变，则最近的帧将处于低质量状态，因为未发送任何新的帧。通过重新配置并即时发送最高质量的最新帧，锐化支持可以解决此问题。

有关 Linux VDA Thinwire 支持的策略的完整列表，请参阅[策略支持列表](#)。

有关 Linux VDA 上的多监视器支持配置的信息，请参阅 [CTX220128](#)。

## 故障排除

检查正在使用哪种图形模式

运行以下命令来检查正在使用哪种图形模式（**0** 表示 TW+；**1** 表示全屏视频编解码器）：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
2 <!--NeedCopy-->
```

结果类似于：

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000000"--force
```

检查是否正在使用 **H.264**

运行以下命令来检查是否正在使用 H.264（**0** 表示未在使用；**1** 表示正在使用）：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
2 <!--NeedCopy-->
```

结果类似于：

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000000"--force
```

检查是否正在使用 **H.265**

运行以下命令来检查是否正在使用全屏 H.265（**0** 表示未使用；**1** 表示正在使用）：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
2 <!--NeedCopy-->
```

结果类似于：

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H265"-d "0x00000000"--force
```

检查正在使用哪种 **YUV** 编码方案

运行以下命令来检查正在使用哪种 YUV 编码方案（**0** 表示 YUV420；**1** 表示 YUV422；**2** 表示 YUV444）：

注意：仅当正在使用视频编解码器时，YUVFormat 的值才有意义。

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
2 <!--NeedCopy-->
```

结果类似于:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000000"--force
```

检查是否正在使用 **YUV444** 软件编码

运行以下命令来检查是否正在使用 YUV444 软件编码:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
2 <!--NeedCopy-->
```

当 YUV444 处于运行状态时, 结果类似于:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000001"--force
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000001"--force
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000000"--force
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000002"--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
 | Uncorr. ECC | | |
 +-----+-----+-----+-----+
```

```

6 | Fan Temp Perf Pwr:Usage/Cap | Memory-Usage | GPU-Util
 | Compute M. |
7 | =====+=====+=====+
8 | 0 GRID K1 Off | 0000:00:05.0 Off |
 | N/A |
9 | N/A 42C P0 14W / 31W | 207MiB / 4095MiB | 8%
 | Default |
10 +-----+-----+-----+
11
12 +-----+-----+-----+
13 | Processes: GPU
 | Memory |
14 | GPU PID Type Process name
 | Usage |
15 | =====+=====+=====+
16 | 0 2164 C+G /usr/local/bin/ctxgfx
 | 106MiB |
17 | 0 2187 G Xorg
 | 85MiB |
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 |
 | Off |
8 | N/A 20C P0 37W / 150W | 19MiB / 8191MiB | 0%
 | Default |
9 | +-----+-----+-----+
10
11 +-----+-----+-----+
12 | Processes: GPU
 | Memory |

```

```
13 | GPU PID Type Process name
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**，**Citrix Hypervisor** 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：

对于 Citrix Hypervisor 8.1 及更高版本：

```
1 [root@xenserver ~]# xe vgpu-param-set uuid=vgpu-uuid extra_args=
 disable_vnc=1
2 <!--NeedCopy-->
```

对于 8.1 之前的 Citrix Hypervisor：

```
1 xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
2 <!--NeedCopy-->
```

### NVIDIA K2 显卡不支持在直通模式下进行 YUV444 硬件编码

通过策略设置启用了无损构建时，在使用 NVIDIA K2 显卡的情况下，用户启动应用程序/桌面会话时会出现黑屏或灰屏。出现该问题是因为 NVIDIA K2 显卡不支持在直通模式下进行 YUV444 硬件编码。有关详细信息，请参阅[视频编码和解码 GPU 支持列表](#)。

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 Workspace** 应用程序窗口大小时，有些 **OpenGL/WebGL** 应用程序无法很好地呈现

调整 Citrix Workspace 应用程序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)**。

## Thinwire 渐进式显示

November 8, 2021

会话交互性在低带宽或高延迟连接中会降级。例如，对于带宽小于 2 Mbps 或延迟超过 200 毫秒的连接，在 Web 页面上滚动可能会变得缓慢、无响应或不稳定。键盘和鼠标操作可能会滞后于图形更新。

在 7.17 版中，能够使用策略设置来降低带宽占用量，方法是将会话配置为低视觉质量，或者设置较低的颜色深度（16 位或 8 位图形）。但是，您必须知道用户是在使用弱连接。HDX Thinwire 不会根据网络状况动态调整静态图像质量。

从 7.18 版起，当可用带宽低于 2 Mbps 或网络延迟超过 200 毫秒时，HDX Thinwire 会默认切换到渐进式更新模式。在此模式下：

- 所有静态图像都将深度压缩。
- 文本质量降低。

例如，在下图中，渐进式更新模式处于活动状态，字母 **F** 和 **e** 具有蓝色虚像，图像已深度压缩。此方法可显著降低带宽占用量，从而提高图像和文本的接收速度，并改进会话交互性。

## Features



用户停止与会话交互后，降级的图像和文本将逐渐锐化到无损效果。例如，在下图中，字母不再包含蓝色虚像，图像以源质量显示。



## Features



对于图像，锐化使用随机块状方法。对于文本，锐化各个字母或单词的各个部分。锐化过程是在多个帧上进行。此方法可避免在处理单个大型锐化帧时出现延迟。

瞬变影像（视频）仍通过自适应显示或选择性 H.264 进行管理。

### 如何使用渐进式模式

默认情况下，渐进式模式对视觉质量策略设置高、中（默认设置）和低而言处于随时准备使用状态。

在以下情况下强制关闭（不使用）渐进式模式：

- 视觉质量 = 始终无损或无损构建
- 简单图形的首选颜色深度 = 8 位
- 使用视频编解码器进行压缩 = 针对整个屏幕（需要全屏 H.264 时）

渐进式模式处于随时准备使用状态时，如果出现以下情况之一，则默认启用此模式：

- 可用带宽低于 2 Mbps
- 网络延迟超过 200 毫秒

发生模式切换后，在该模式中最短将花费 10 秒钟时间，即使网络条件暂时不利亦如此。

### 更改渐进式模式行为

可以通过运行以下命令更改渐进式模式的行为：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
 CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
 ProgressiveDisplay" -d "<value>" --force
2 <!--NeedCopy-->
```

其中 <value>：

0 = 始终关闭（在任何情况下都不使用）

1 = 自动（根据网络状况切换，默认值）

2 = 始终开启

处于自动模式 (1) 时，可以运行以下命令之一更改切换渐进式模式时的阈值：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
 CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
 ProgressiveDisplayBandwidthThreshold" -d "<value>" --force
2 <!--NeedCopy-->
```

其中 <value> 为 < 阈值，以 Kbps 为单位 >（默认值 = 2048）

示例：4096 = 在带宽低于 4 Mbps 时开启渐进式模式

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE
 \CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
 ProgressiveDisplayLatencyThreshold" -d "<value>" --force
2 <!--NeedCopy-->
```

其中 <value> 为 < 阈值，以毫秒为单位 >（默认值 = 200）

示例：100 = 在网络延迟低于 100 毫秒时开启渐进式模式。

## 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 7: 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-->
```

## 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                  |
|--------------------|-----------------------------|-----|----------------|----------------------|
| 使用客户端本地时间          | UseLocalTimeOfClient        | 用户  | ICA\时区控制       | 使用服务器时区              |
| ICA 往返行程计算         | IcaRoundTripCheckEnabled    | 计算机 | ICA\最终用户监视     | 已启用 (1)              |
| ICA 往返行程计算间隔       | IcaRoundTripCheckPeriod     | 计算机 | ICA\最终用户监视     | 15                   |
| 空闲连接的 ICA 往返行程计算   | IcaRoundTripCheckWhenIdle   | 计算机 | ICA\最终用户监视     | 已禁用 (0)              |
| 总会话带宽限制            | LimitOverallBw              | 用户  | ICA\带宽         | 0                    |
| 音频重定向带宽限制          | LimitAudioBw                | 用户  | ICA\带宽         | 0                    |
| 音频重定向带宽限制百分比       | LimitAudioBwPercent         | 用户  | ICA\带宽         | 0                    |
| 客户端 USB 设备重定向带宽限制  | LimitUSBBw                  | 用户  | ICA\带宽         | 0                    |
| 客户端 USB 设备重定向带宽百分比 | LimitUSBBwPercent           | 用户  | ICA\带宽         | 0                    |
| 剪贴板重定向带宽限制         | LimitClipbdBW               | 用户  | ICA\带宽         | 0                    |
| 剪贴板重定向带宽限制百分比      | LimitClipbdBWPercent        | 用户  | ICA\带宽         | 0                    |
| 文件重定向带宽限制          | LimitCdmBw                  | 用户  | ICA\带宽         | 0                    |
| 文件重定向带宽限制百分比       | LimitCdmBwPercent           | 用户  | ICA\带宽         | 0                    |
| 打印机重定向带宽限制         | LimitPrinterBw              | 用户  | ICA\带宽         | 0                    |
| 打印机重定向带宽限制百分比      | LimitPrinterBwPercent       | 用户  | ICA\带宽         | 0                    |
| WebSocket 连接       | AcceptWebSocketsConnections | 计算机 | ICA\WebSockets | 禁止                   |
| WebSocket 端口号      | WebSocketsPort              | 计算机 | ICA\WebSockets | 8008                 |
| WebSocket 可信源服务器列表 | WSTrustedOriginServers      | 计算机 | ICA\WebSockets | *                    |
| 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) |
| 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                 |
| HDX 自适应传输          | HDXoverUDP                  | 计算机 | ICA            | Preferred(2)         |

| Studio 策略       | 注册表项名称                              | 类型  | 模块            | 默认值                                                                       |
|-----------------|-------------------------------------|-----|---------------|---------------------------------------------------------------------------|
| 会话可靠性连接         | AcceptSessionReliabilityConnections | 计算机 | ICA\会话可靠性     | 允许 (1)                                                                    |
| 重新连接 UI 透明度级别   | ReconnectionUiTransparencyLevel     | 计算机 | ICA\客户端自动重新连接 | 80%                                                                       |
| 会话可靠性端口号        | SessionReliabilityPort              | 计算机 | ICA\会话可靠性     | 2598                                                                      |
| 会话可靠性超时         | SessionReliabilityTimeout           | 计算机 | ICA\会话可靠性     | 180 秒                                                                     |
| 客户端自动重新连接       | AllowAutoClientReconnect            | 用户  | ICA\客户端自动重新连接 | 允许 (1)                                                                    |
| 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       | AllowPrinterRedirection             | 用户  | 打印            | 允许 (1)                                                                    |
| 自动创建 PDF 通用打印机  | AutoCreatePDFPrinter                | 用户  | 打印            | 已禁用 (0)                                                                   |
| 打印机驱动程序映射和兼容性   | DriverMappingList                   | 用户  | 打印            | "Microsoft XPS Document Writer *, Deny;Send to Microsoft OneNote *, Deny" |
| 客户端剪贴板重定向       | AllowClipboardRedirection           | 用户  | 剪贴板           | 允许 (1)                                                                    |
| 客户端 USB 设备重定向   | AllowUSBRedirection                 | 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)                                                                   |
| 额外颜色压缩          | ExtraColorCompression               | 用户  | Thinwire      | 已禁用 (0)                                                                   |
| 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)                                                                   |
| 允许视觉无损压缩        | AllowVisuallyLosslessCompression    | 用户  | Thinwire      | 已禁用 (0)                                                                   |

| Studio 策略       | 注册表项名称                        | 类型  | 模块                        | 默认值            |
|-----------------|-------------------------------|-----|---------------------------|----------------|
| 针对 3D 图形工作负载优化  | OptimizeFor3dWorkload         | 用户  | Thinwire                  | 已禁用 (0)        |
| 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       | 系统  | 负载管理                      | 250            |
| 并发登录数容差         | ConcurrentLogonsToThisMachine | 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  | 文件重定向/CDM                 | 已启用 (1)        |
| 客户端光盘驱动器        | AllowCdromDrives              | 用户  | 文件重定向/CDM                 | 允许 (1)         |
| 客户端固定驱动器        | AllowFixedDrives              | 用户  | 文件重定向/CDM                 | 允许 (1)         |
| 客户端软盘驱动器        | AllowFloppyDrives             | 用户  | 文件重定向/CDM                 | 允许 (1)         |
| 客户端网络驱动器        | AllowNetworkDrives            | 用户  | 文件重定向/CDM                 | 允许 (1)         |
| 客户端驱动器重定向       | AllowDriveRedir               | 用户  | 文件重定向/CDM                 | 允许 (1)         |
| 只读客户端驱动器访问      | ReadOnlyMappedDrives          | 用户  | 文件重定向/CDM                 | 已禁用 (0)        |
| 自动显示键盘          | AllowAutoKeyboardPopup        | 用户  | MRVC                      | 已禁用 (0)        |
| 允许在桌面与客户端之间传输文件 | AllowFileTransfer             | 用户  | 文件传输                      | 允许             |
| 从桌面下载文件         | AllowFileDownload             | 用户  | 文件传输                      | 允许             |
| 将文件上载到桌面        | AllowFileUpload               | 用户  | 文件传输                      | 允许             |

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 Selection changes are not updated on neither client nor host

Host selection changes are not updated to client

Client selection changes are not updated to host

Selection changes are updated on both client and host

S, 7.1 Desktop OS, 7.5 Server OS, 7.1 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

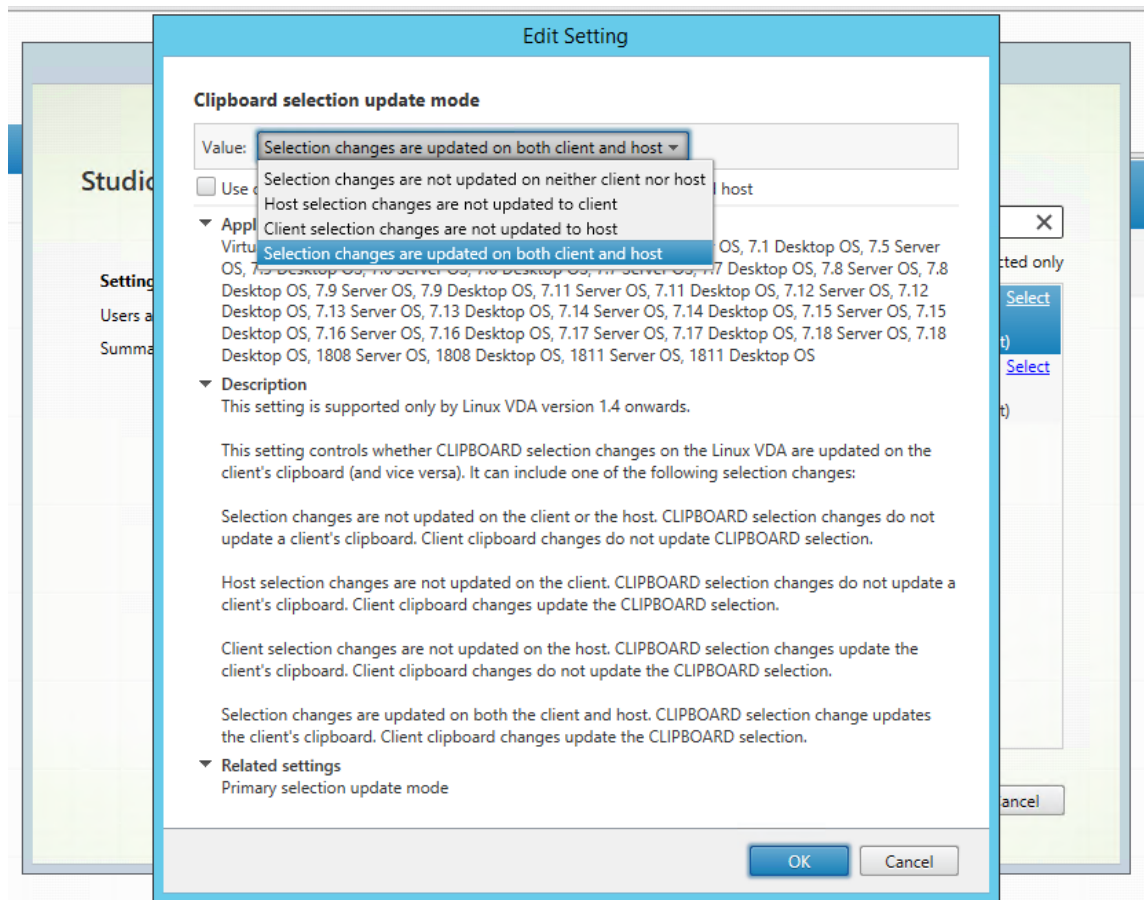
值（枚举）：[0, 1, 2, 3]

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，Citrix 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

May 12, 2020

Linux VDA 支持 IPv6 以便与 Citrix Virtual Apps and Desktops 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 "HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD"
 -v "ControllerRegistrationIPv6Netmask"
3 <!--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 Citrix Virtual Apps and Desktops 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。此外，匿名数据的副本将被发送到 Google Analytics (GA) 以进行快速、高效地分析。

### 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 七天后第一次上传数据。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-->
```

#### • GASwitch

启用或禁用 GA 的注册表设置（默认值 = 0）：

位置：HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CEIP

名称：GASwitch

值：1 = 禁用，0 = 启用

未指定时，GA 处于启用状态。

可以在客户端上运行以下命令来禁用 GA：

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
Citrix\CEIP" -v "GASwitch" -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                                                                        |
| 系统区域设置            | system_locale           | 表示此计算机的区域设置的文本字符串                                                                          |
| LVDA 主要服务上次重新启动时间 | ctxhdx ctxvda           | <a href="#">ctxhdx</a> 和 <a href="#">ctxvda</a> 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）                                                                      |
| 启动的会话数            | session_launch          | 表示我们收集此数据点时计算机上启动（登录或重新连接）的会话数的整数                                                          |
| 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                                                                                |
| 资源类型              | resource_type           | 表示启动的会话的资源类型的文本字符串：桌面或 <appname>                                                           |
| 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                                                  |

| 数据点            | 注册表项名称                  | 说明                                       |
|----------------|-------------------------|------------------------------------------|
| 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 Workspace 应用程序的类型的整数    |
| Receiver 客户端版本 | receiver_version        | 表示用于启动会话的 Citrix Workspace 应用程序的版本的文本字符串 |
| 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                      |
| Gfx 提供程序类型     | gfx_provider_type       | 表示会话的图形提供程序类型的文本字符串                      |
| 重影计数           | shadow_count            | 表示会话被重影的次数的整数                            |
| 用户选择的语言        | ctxism_select           | 包含用户选择的所有语言的组合长字符串                       |
| 智能卡重定向计数       | scard_redirecting_count | 表示智能卡重定向用于会话中应用程序的会话登录和用户身份验证的次数的整数      |

## 配置 **USB** 重定向

March 11, 2022

USB 设备在 Citrix Workspace 应用程序与 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 Workspace 应用程序之间的所有 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 |
| 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：

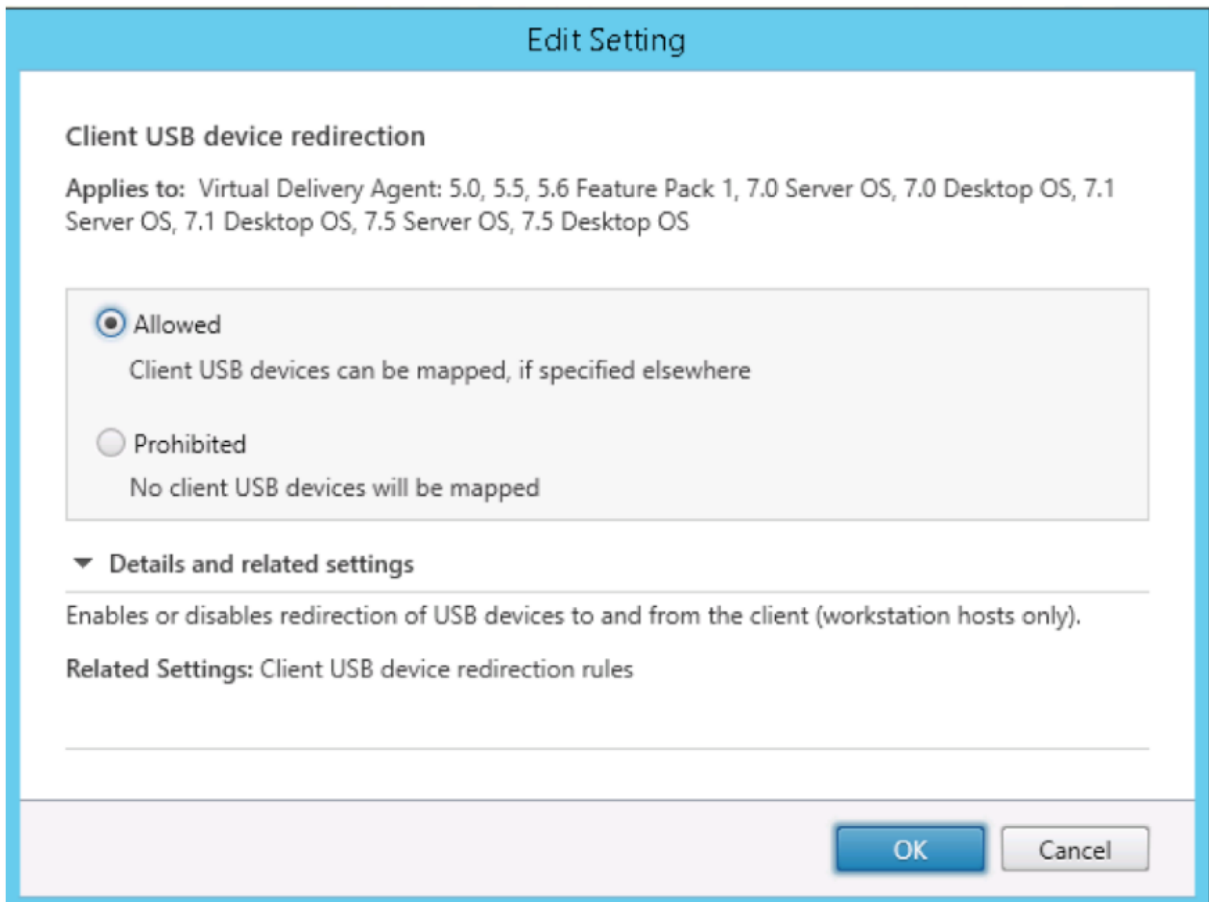
- 客户端 USB 设备重定向策略
- 客户端 USB 设备重定向规则

### 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。

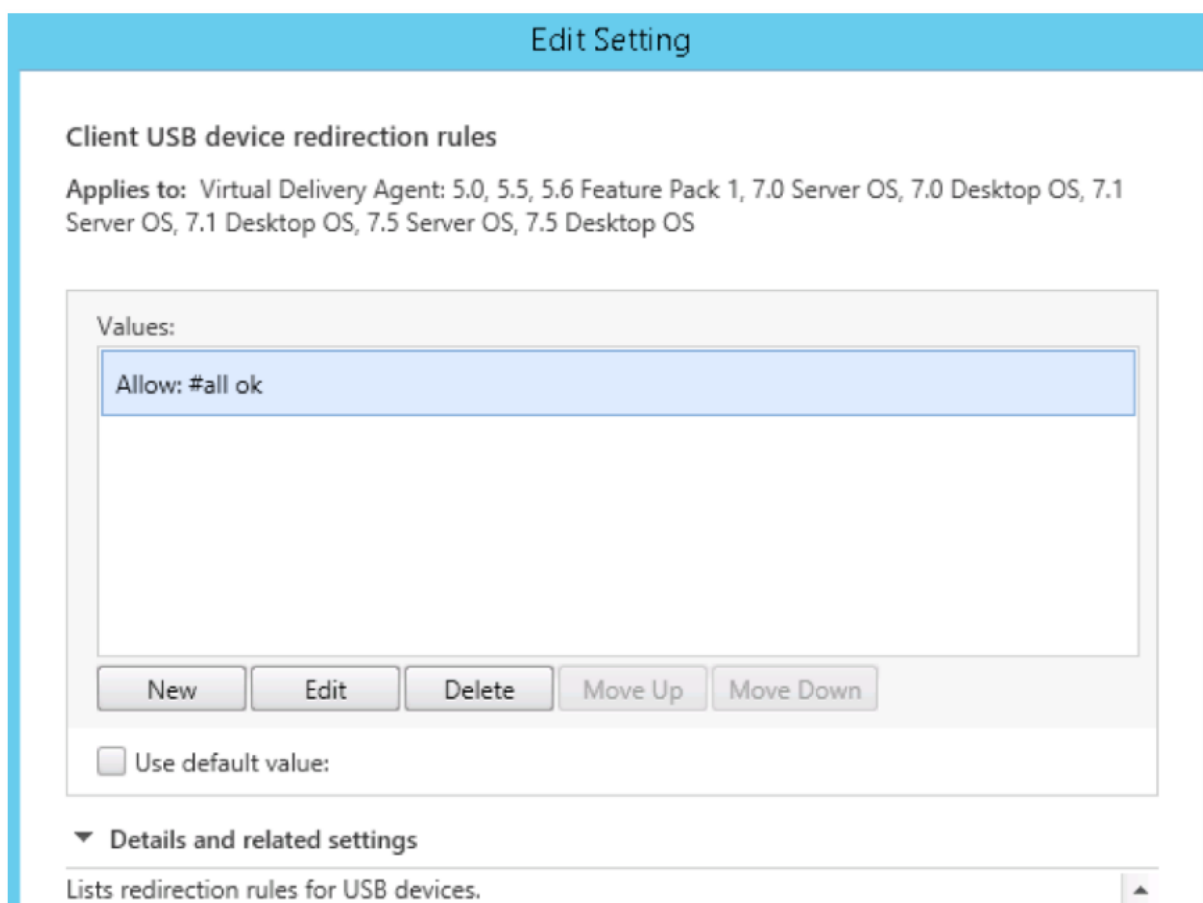


### 设置 **USB** 重定向规则

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 7.7、CentOS 7.7 | 3.10.0-1062       |
| SUSE 12.3           | 4.4.73-5-default  |
| Ubuntu 18.04        | 4.15.0-45-generic |
| Ubuntu 16.04        | 4.4.0-142-generic |

### 重要:

如果您的计算机的内核与为 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. 解压缩 **citrix-linux-vda-sources.zip** 文件。导航到 **linux-vda-sources/vhci-hcd-1.15.tar.bz2**，并使用 **tar xvf vhci-hcd-1.15.tar.bz2** 解压 VHCI 源文件。
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/CentOS:**

```
1 yum install kernel-devel
2 <!--NeedCopy-->
```

#### **SUSE 12:**

```
1 zypper install kernel-devel
2
3 zypper install kernel-source
4 <!--NeedCopy-->
```

#### **Ubuntu:**

```
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
```

- 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（通过按顺序运行以下命令：`make oldconfig`、`make prepare`、`make modules`、`make`）构建内核以获取此文件，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。
- 运行以下命令以安装开发工具。

**RHEL/CentOS:**

```
1 yum groupinstall 'Development Tools'
2 <!--NeedCopy-->
```

**Ubuntu 18.04:**

```
1 apt install build-essential
2 apt install libelf-dev
3 <!--NeedCopy-->
```

**Ubuntu 16.04:**

```
1 apt install build-essential
2 <!--NeedCopy-->
```

- 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-->
```

- 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`。

- 将内核模块替换为新构建的模块：`cp -f usb-vhci-*.ko /opt/Citrix/VDA/lib64/`
- 重新启动 USB 服务：

```
1 service ctxusbds restart
2 <!--NeedCopy-->
```

- 注销并重新登录会话。检查 USB 重定向是否正常。

### 解决内核构建问题

- 对于 **Ubuntu 16** 的特定内核，可能会出现内核构建错误。错误为 `implicit declaration of function 'copy_to_user'`，请参见下面的屏幕截图。

```
usb-vhci-iocifc.c:216:5: error: implicit declaration of function 'copy_to_user'
```

该错误是由于内核中的头文件发生变化所致。解决方法：将 `#include <linux/uaccess.h>` 行添加到 `vhci-hcd-1.15/usb-vhci-iocifc.c` 文件中。

```
#include <linux/fs.h>
#include <linux/uaccess.h>
#include "usb-vhci-hcd.h"
```

- 对于 **Ubuntu 16** 的内核 **4.15.0-29-generic**，可能会出现内核构建错误。错误为 `'driver_attr_debug_output' undeclared`，请参见下面的屏幕截图。

```
error: 'driver_attr_debug_output' undeclared (first use in this function)
```

当内核缺少符号时，将出现错误。解决方法：禁用 `vhci-hcd-1.15/usb-vhci-iocifc.c` 和 `vhci-hcd-1.15/usb-vhci-hcd.c` 文件中 `DEBUG` 的宏定义。

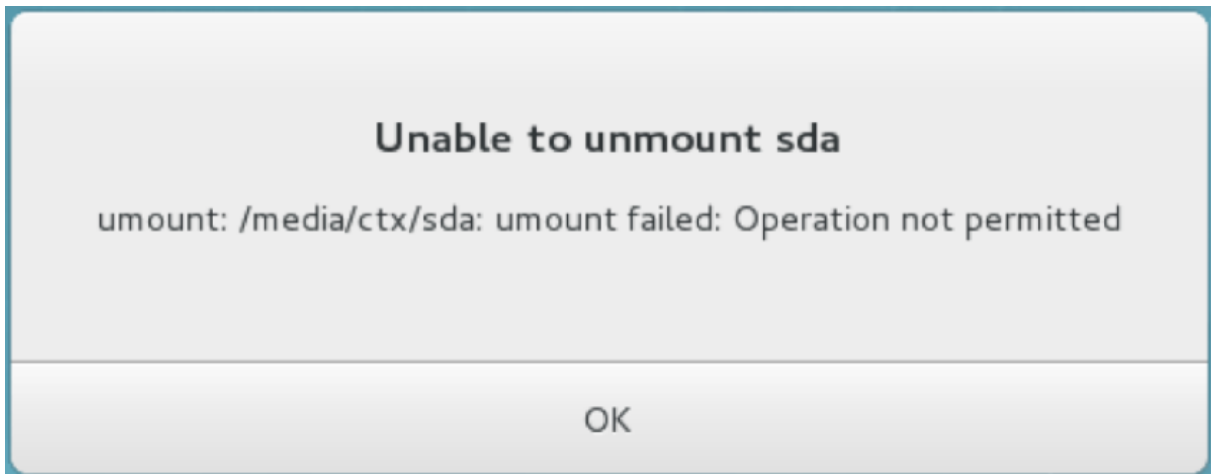
```
22
23 // #define DEBUG
24
25 #include <linux/module.h>
```

### 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。

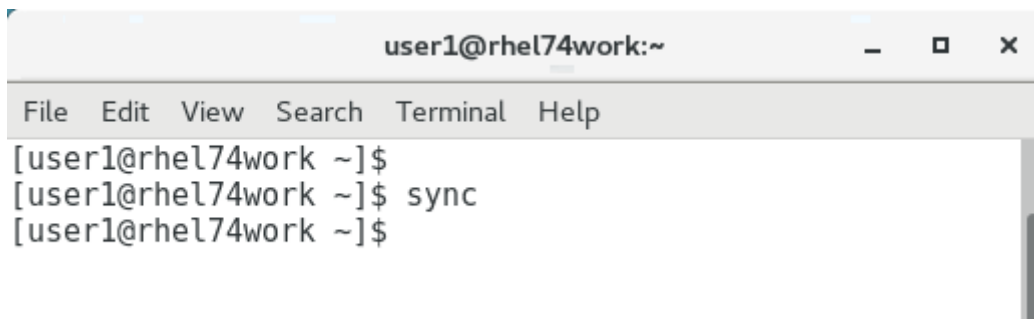
#### 无法卸载重定向的 **USB** 磁盘 \*\*

为了对从 Citrix Workspace 应用程序重定向的所有 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 Workspace 应用程序的工具栏停止重定向，则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 Workspace 应用程序的工具栏停止重定向，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。

A terminal window titled "user1@rhel74work:~" with standard window controls. The terminal shows a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The command prompt shows three lines: "[user1@rhel74work ~]\$", "[user1@rhel74work ~]\$ sync", and "[user1@rhel74work ~]\$".

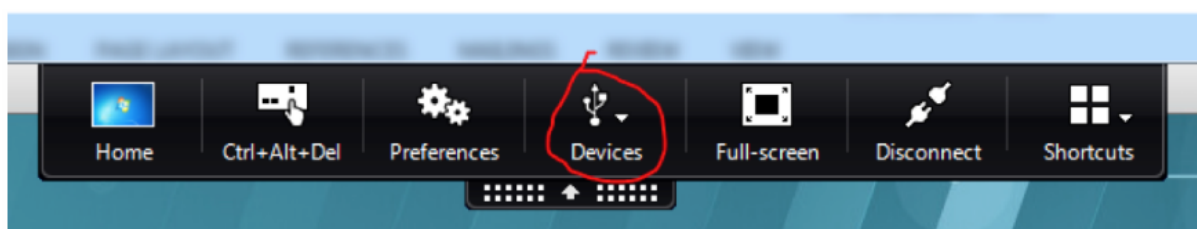
```
user1@rhel74work:~
File Edit View Search Terminal Help
[user1@rhel74work ~]$
[user1@rhel74work ~]$ sync
[user1@rhel74work ~]$
```

#### **Citrix Workspace** 应用程序的工具栏中无设备

有时，您可能会看到 Citrix Workspace 应用程序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：

设备选项卡在适用于 Linux 的 Citrix Workspace 应用程序中不可用。

当 **USB** 设备在 **Citrix Workspace** 应用程序的工具栏中显示，但这些设备都标有受策略限制时，重定向失败

出现此问题时，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 Workspace 应用程序的注册表中配置了任何其他策略限制。请检查注册表路径中的 **DeviceRules**，以确保此设置未拒绝访问该设备：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB
```

有关详细信息，请参阅知识中心

文章 [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。其他设备可能也会重定向到活动 Linux VDA 会话。在此示例中，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。

## 配置会话可靠性

November 21, 2020

Citrix 将会话可靠性功能引入所有支持的 Linux 平台。会话可靠性在默认情况下处于启用状态。

会话可靠性将在网络中断时无缝重新连接 ICA 会话。有关会话可靠性的详细信息，请参阅[客户端自动重新连接和会话可靠性](#)。

注意：默认情况下，通过会话可靠性连接传输的数据是纯文本数据。出于安全考虑，我们建议您启用 TLS 加密。有关 TLS 加密的详细信息，请参阅[使用 TLS 保护用户会话安全](#)。

### 配置

#### Citrix Studio 中的策略设置

可以在 Citrix Studio 中为会话可靠性设置以下策略：

- 会话可靠性连接
- 会话可靠性超时
- 会话可靠性端口号
- 重新连接 UI 透明度级别

有关详细信息，请参阅[会话可靠性策略设置](#)和[客户端自动重新连接策略设置](#)。

注意：设置会话可靠性连接或会话可靠性端口号策略后，请按此顺序重新启动 VDA 服务和 HDX 服务，以使设置生效。

#### Linux VDA 上的设置

- 启用/禁用会话可靠性 **TCP** 侦听器

默认情况下，在端口 2598 上启用和侦听会话可靠性 TCP 侦听器。要禁用该侦听器，请运行以下命令。

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
 CurrentControlSet\Control\Citrix\WinStations\cgp" -v "
 fEnableWinStation" -d "0x00000000"
2 <!--NeedCopy-->
```

注意：请重新启动 HDX 服务以使设置生效。禁用 TCP 侦听器不会禁用会话可靠性。仍可通过其他侦听器（例如 SSL）获得会话可靠性，前提是通过会话可靠性连接策略启用了该功能。

- 会话可靠性端口号

还可以使用以下命令设置会话可靠性端口号（以端口号 2599 为例）。

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
 CurrentControlSet\Control\Citrix\WinStations\cgp" -v "PortNumber"
 -d "2599"
2 <!--NeedCopy-->
```

注意：请重新启动 HDX 服务以使设置生效。如果在 Citrix Studio 中通过策略设置设置了端口号，则将忽略 Linux VDA 上的设置。确保 VDA 上的防火墙配置为不禁止通过设置端口传输网络流量。

- 服务器到客户端保持活动状态时间间隔

会话中没有活动（例如，没有鼠标移动、没有屏幕更新）时，在 Linux VDA 和 ICA 客户端之间发送会话可靠性保持活动状态消息。保持活动状态消息用于检测客户端是否仍可响应。如果客户端没有响应，则挂起会话，直到客户端重新连接。此设置指定相邻保持活动状态消息之间间隔的秒数。默认情况下未配置此设置。要对其进行配置，请运行以下命令（以 10 秒为例）。

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XTEConfig" -t "REG_DWORD" -v "CgpServerToClientKeepAlive" -d "10" --force
```

- 客户端到服务器保持活动状态时间间隔

此设置指定从 ICA 客户端发送到 Linux VDA 的相邻保持活动状态消息之间间隔的秒数。默认情况下未配置此设置。要对其进行配置，请运行以下命令（以 10 秒为例）。

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XTEConfig" -t "REG_DWORD" -v "CgpClientToServerKeepAlive" -d "10" --force
2 <!--NeedCopy-->
```

### 故障排除

通过策略设置启用会话可靠性后，无法启动会话。

要解决此问题，请执行以下操作：

1. 在 Citrix Studio 中通过策略设置启用会话可靠性后，请务必按此顺序重新启动 VDA 服务和 HDX 服务。
2. 在 VDA 上，运行以下命令以验证会话可靠性 TCP 侦听器是否正在运行（以端口 2598 为例）。

```
1 netstat -an | grep 2598
2 <!--NeedCopy-->
```

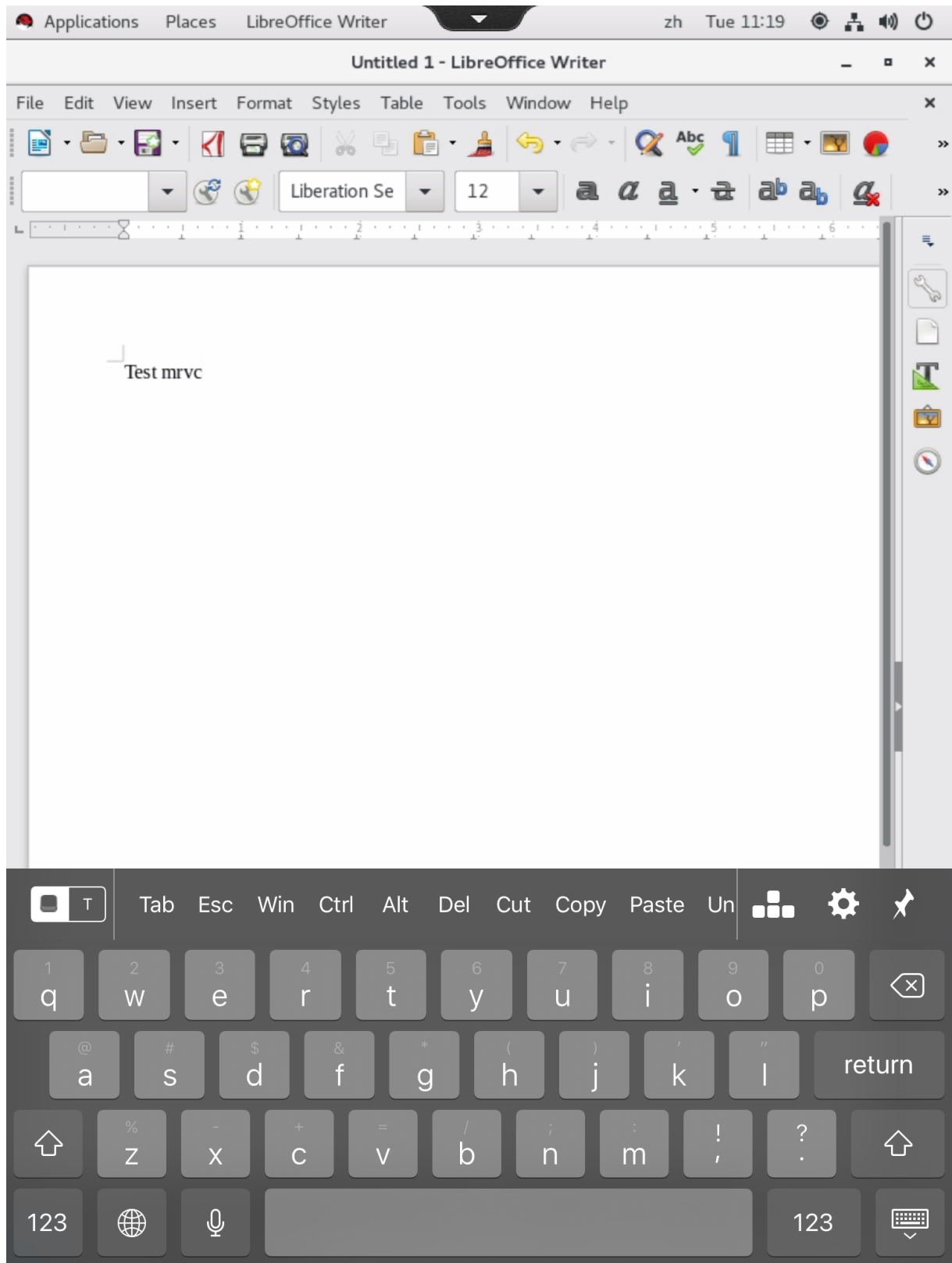
如果会话可靠性端口上没有 TCP 侦听器，请运行以下命令启用该侦听器。

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations\cgp" -v "fEnableWinStation" -d "0x00000001"
2 <!--NeedCopy-->
```

### 软键盘

November 8, 2021

可以在 Linux 虚拟桌面或应用程序会话中使用软键盘功能。软键盘会在您输入或离开输入字段时显示或隐藏。



**注意：**

此功能适用于 RHEL 7.7、CentOS 7.6、SUSE 12.3、Ubuntu 16.04 和 Ubuntu 18.04。适用于 iOS 和 Android 的 Citrix Workspace 应用程序支持该功能。

### 启用和禁用该功能

默认情况下，该功能处于禁用状态。可以使用 **ctxreg** 实用程序启用或禁用该功能。给定 Linux VDA 上的功能配置应用于该 VDA 上发布的所有会话。

要启用此功能，请执行以下操作：

1. 运行以下命令：

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
 CurrentControlSet\Control\Citrix\VirtualChannels\MrVc" -v "
 Enabled" -d "0x00000001"
2 <!--NeedCopy-->
```

2. 在 Citrix Studio 中，将自动显示键盘策略设置为允许。

3. (可选) 对于 RHEL 7 和 CentOS 7，运行以下命令将智能输入总线 (IBus) 配置为默认 IM 服务：

```
1 echo "GTK_IM_MODULE=ibus" >>/etc/bashrc
2 <!--NeedCopy-->
```

要禁用该功能，请运行以下命令：

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
 Control\Citrix\VirtualChannels\MrVc" -v "Enabled" -d "0x00000000"
2 <!--NeedCopy-->
```

**注意：**

之前的设置将在您登录到新会话或注销后返回到当前会话时生效。

### 限制

- 该功能在 Google Chrome、LibreOffice 和其他应用程序中可能无法正常运行。
- 要在手动隐藏软键盘后再次显示它，请单击非输入字段，然后再次单击当前输入字段。
- 在 Web 浏览器中从一个输入字段切换到单击另一个输入字段时，软键盘可能不显示。要解决此问题，请单击非输入字段，然后单击目标输入字段。
- 此功能不支持 Unicode 字符和双字节字符（例如，中文、日语和韩语字符）。
- 软键盘不适用于密码输入字段。

- 软键盘可能会与当前输入字段重叠。在这种情况下，请移动应用程序窗口或向上滚动屏幕以将输入字段移到可访问的位置。
- 由于 Citrix Workspace 应用程序和 Huawei 平板电脑之间存在兼容性问题，因此即使连接了物理键盘，软键盘也会显示在 Huawei 平板电脑上。

## 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

照常打开 Citrix Virtual Apps 或 Citrix Virtual Desktops 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 功能。

### 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 功能。
- IME 用户界面不在输入区域中跟随光标。

## 支持多语言输入

November 8, 2021

自 Linux VDA 版本 1.4 起，Citrix 添加了对已发布的应用程序的支持。用户可以在没有 Linux 桌面环境的情况下访问所需的 Linux 应用程序。

但是，由于语言栏与 Linux 桌面环境高度集成，因此，Linux VDA 上的本地语言栏对于已发布的应用程序不可用。因此，用户无法以需要 IME 的语言（例如，中文、日语或韩语）输入文本。此外，在应用程序会话期间，用户也不能在键盘布局之间切换。

为了解决这些问题，此功能为接受文本输入的已发布应用程序提供语言栏。通过语言栏，用户可以在应用程序会话期间选择服务器端 IME 以及在键盘布局之间切换。

### 配置

您可以使用 **ctxreg** 实用程序启用或禁用此功能（默认情况下禁用）。给定 Linux VDA 服务器上的功能配置应用于在该 VDA 上发布的所有应用程序。

配置注册表项为“HKEY\_LOCAL\_MACHINE \SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar”，类型为 DWORD。

要启用此功能，请运行以下命令：

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

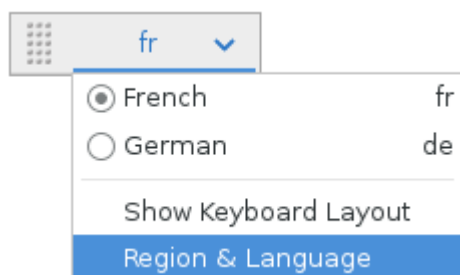
要禁用此功能，请运行以下命令：

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE \SYSTEM\
 CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0
 x00000000"
2 <!--NeedCopy-->
```

### 使用情况

用法很简单。

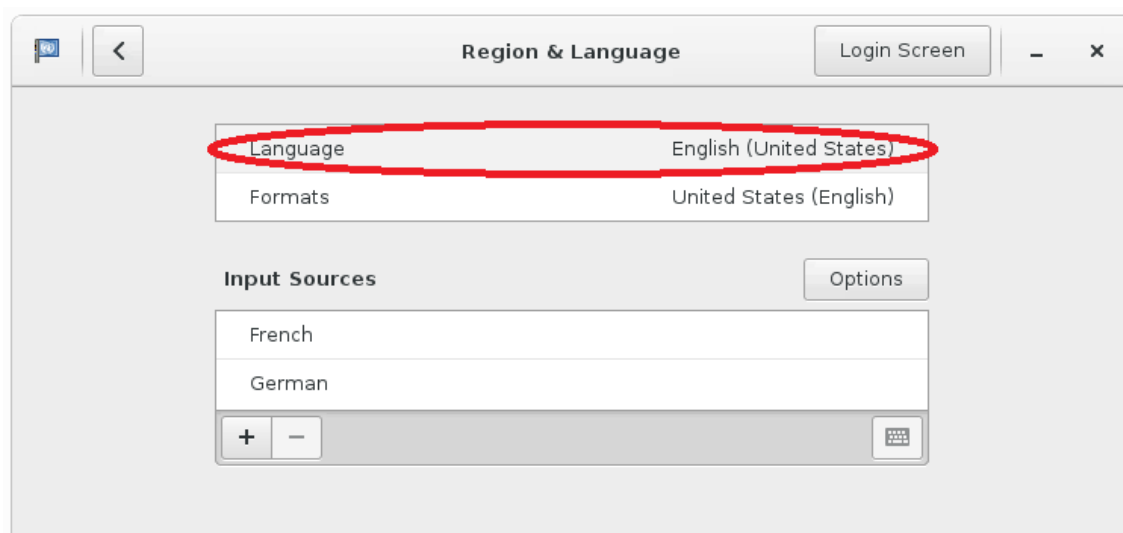
1. 启用功能。
2. 访问可以接受文本输入的已发布的应用程序。在会话中应用程序旁边会显示语言栏。
3. 从下拉菜单中选择区域和语言以添加所需的语言（输入源）。



4. 从下拉菜单中选择 IME 或键盘布局。
5. 使用所选的 IME 或键盘布局键入语言。

注意：

- 在 VDA 端语言栏上更改键盘布局时，请确保在运行 Citrix Workspace 应用程序的客户端上使用相同的键盘布局。
- 必须将 **accountsservice** 软件包升级到版本 0.6.37 或更高版本，才能在区域和语言对话框中执行设置。



## 动态键盘布局同步

November 8, 2021

以前，Linux VDA 和客户端设备上的键盘布局必须相同。例如，如果客户端设备上的键盘布局从“英语”更改为“法语”，但在 VDA 上未更改，会发生键映射问题并持续存在，直至 VDA 也更改为“法语”。

Citrix 通过自动将 VDA 的键盘布局与客户端设备的键盘布局同步来解决此问题。无论何时客户端设备上的键盘布局发生变化，VDA 随后都会做出恰当的调整。



提示:

适用于 Windows 的 Citrix Workspace 应用程序支持此功能，并且此功能与已发布的应用程序和桌面兼容。

## 配置

默认情况下，此功能处于禁用状态。请使用 **ctxreg** 实用程序启用或禁用此功能。给定 Linux VDA 上的功能配置应用于该 VDA 上发布的所有会话。

配置注册表项为“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\SyncKeyboardLayout”，类型为 DWORD。

要启用此功能，请运行以下命令：

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

要禁用此功能，请运行以下命令：

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
 CurrentControlSet\Control\Citrix\LanguageBar" -v "SyncKeyboardLayout"
 -d "0x00000000"
2 <!--NeedCopy-->
```

## 使用情况

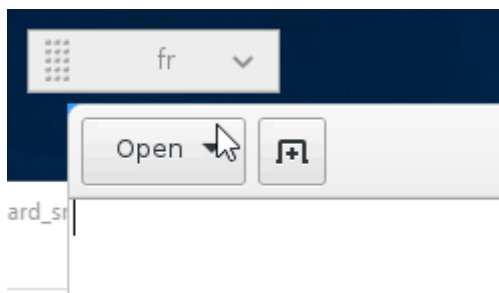
启用此功能后，如果会话过程中客户端设备上的键盘布局发生变化，会话的键盘布局也将相应地发生变化。

例如，如果将客户端设备上的键盘布局更改为“法语 (FR)”：



Linux VDA 会话的键盘布局随后也将更改为“fr”。

在应用程序会话中，如果启用了语言栏，则可以看到这一自动变化情形：



在桌面会话中，可以在任务栏中看到这一自动发生的变化：

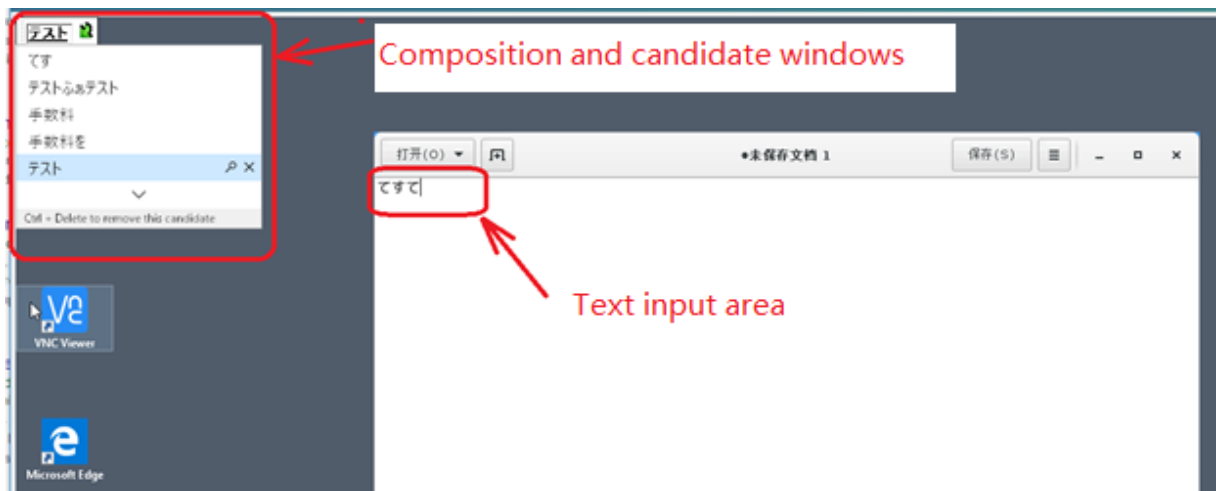


## 客户端 **IME** 用户界面同步

November 8, 2021

### 概述

迄今为止，客户端 IME 用户界面（包括撰写窗口和候选窗口）置于屏幕左上角。以前不跟随光标，有时距离文本输入区域中的光标较远：



Citrix 增强了可用性，并进一步提高了客户端 IME 的无缝体验，如下所示：



#### 注意:

该功能不适用于 RHEL 7.x、CentOS 7.x、Ubuntu 16.04、Ubuntu 18.04 和 SUSE 12.x。它在适用于 Windows 和 Mac 的 Citrix Workspace 应用程序上受支持。

要在 RHEL 7.x 桌面会话中使用该功能，必须启用 IBus。例如，将用户界面语言设置为需要 IME 输入的语言，或者将 **GTK\_IM\_MODULE=ibus** 添加到 **`\${HOME}/.config/imsettings/xinputrc** 文件中。

该功能是自动安装的，但您必须启用该功能，才能使用它。

#### 启用和禁用该功能

默认情况下，该功能处于禁用状态。可以使用 **ctxreg** 实用程序启用或禁用该功能。给定 Linux VDA 上的功能配置应用于该 VDA 上发布的所有会话。

要启用该功能，请运行以下命令：

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

要禁用该功能，请运行以下命令：

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
 CurrentControlSet\Control\Citrix\LanguageBar" -v "SyncClientIME" -d
 "0x00000000"
2 <!--NeedCopy-->
```

## 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 Citrix ADC 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。

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，某些与持续时间有关的数据点不可用。

### 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 Citrix ADC 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，未在 Citrix ADC 上启用 AppFlow，或者在 Citrix ADM 上配置了不正确的 Citrix ADC 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。

## 自适应传输

March 16, 2022

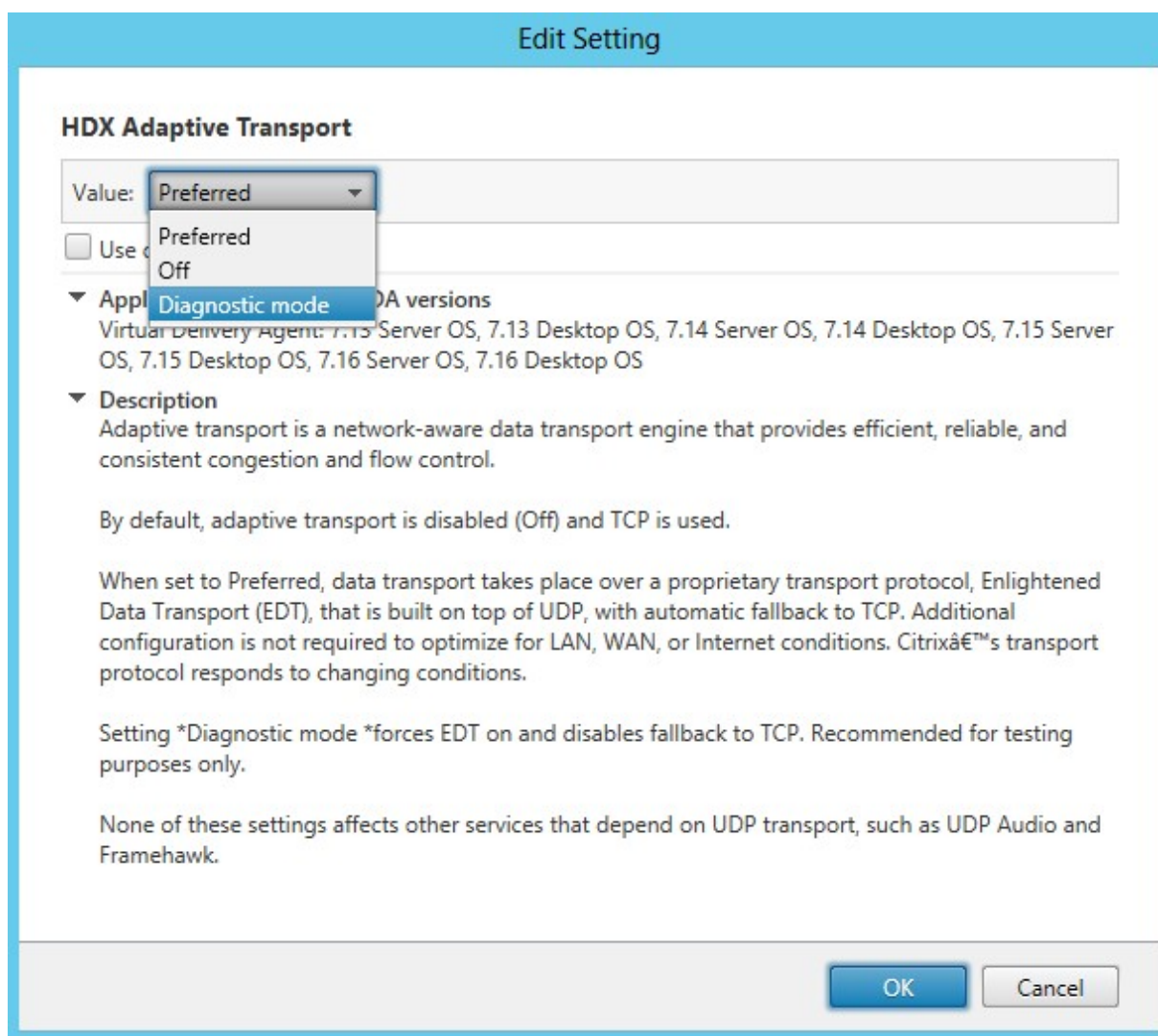
以前作为实验性功能提供的自适应传输功能在本版本中完全受支持。

自适应传输是 Citrix Virtual Apps and Desktops 的数据传输机制。此传输速度更快，更具可扩展性，改进了应用程序的交互性，并且在具有挑战性的远距离 WAN 和 Internet 连接中互动性更强。有关详细信息，请参阅[自适应传输](#)。

### 启用自适应传输

在 Citrix Studio 中，验证 **HDX** 自适应传输策略设置为首选还是诊断模式。首选默认处于选中状态。

- 首选：尽可能使用基于 Enlightened Data Transport (EDT) 的自适应传输，并回退到 TCP。
- 诊断 模式：强制启用 EDT，并禁用回退到 TCP。



## 禁用自适应传输

要禁用自适应传输，请在 Citrix Studio 中将 **HDX** 自适应传输策略设置为关。

## 故障排除

检查是否启用了自适应传输

要检查 UDP 侦听器是否正在运行，请运行以下命令。

```
1 netstat -an | grep "1494|2598"
2 <!--NeedCopy-->
```

在正常情况下，输出类似于如下所示。

```
1 udp 0 0 0.0.0.0:2598 0.0.0.0:*
2
3 udp 0 0 :::1494 :::*
4 <!--NeedCopy-->
```

## 启用跟踪

November 8, 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，日志级别将设置为警告（不区分大小写）。

要查看为不同组件设置的日志级别，请运行以下命令：

```

1 setlog levels
2 <!--NeedCopy-->

```

要设置日志级别（包括“已禁用”、“已继承”、“详细”、“信息”、“警告”、“错误”和“致命错误”），请运行以下命令：

```

1 setlog level <class> [<level>]
2 <!--NeedCopy-->

```

| 日志级别 | 命令参数（不区分大小写） |
|------|--------------|
| 已禁用  | 无            |
| 已继承  | 继承           |
| 详细   | 详细           |
| 信息   | 信息           |
| 警告   | 警告           |
| 错误   | 错误           |
| 致命错误 | 致命           |

`<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“全部”。例如：

```

1 setlog level all error

```



```
2 <!--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。

### 重影会话

November 8, 2021

通过会话重影功能，域管理员可以在 Intranet 中查看用户的 ICA 会话。该功能使用 noVNC 连接到 ICA 会话，仅 RHEL 7.x 和 Ubuntu 16.04 支持该功能。

注意：

Citrix Director 的版本必须为 7.16 或更高版本，才能使用会话重影功能。

### 安装和配置

#### 依赖项

会话重影需要两个新的依赖关系 `python-websockify` 和 `x11vnc`。在 Ubuntu 16.04 上安装 Linux VDA 时，会自动安装 `python-websockify` 和 `x11vnc` 依赖项。在 RHEL 7.x 上，必须在安装 Linux VDA 之后手动安装 `python-websockify` 和 `x11vnc`。

在 RHEL 7.x 上运行以下命令以安装 `python-websockify` 和 `x11vnc` (`x11vnc` 版本 0.9.13 或更高版本)。

```
1 sudo yum install -y python-websockify x11vnc
2 <!--NeedCopy-->
```

要解决 `python-websockify` 和 `x11vnc`，请在 RHEL 7.x 上启用以下存储库：

- 适用于 Enterprise Linux (EPEL) 的额外软件包

`python-websockify` 和 `x11vnc` 都需要 EPEL 存储库。运行以下命令以启用 EPEL 存储库：

```
1 sudo yum install https://dl.fedoraproject.org/pub/epel/epel-
 release-latest-$(rpm -E '%{
2 rhel }
3 ').noarch.rpm
4 <!--NeedCopy-->
```

- 可选 RPM

要启用可选的 RPM 存储库以安装 `x11vnc` 的一些依赖项软件包，请运行以下任一命令：

对于工作站：

```
1 subscription-manager repos --enable=rhel-7-workstation-optional-
 rpms
2 <!--NeedCopy-->
```

对于服务器：

```
1 subscription-manager repos --enable=rhel-7-server-optional-rpms
2 <!--NeedCopy-->
```

## 端口

会话重影功能会自动选择 6001-6099 内的可用端口来建立从 Linux VDA 到 Citrix Director 的连接。因此，可以并行重影的 ICA 会话数不应超过 99 个。请确保有足够的端口可用来满足您的要求，尤其是多会话重影。

## 注册表

下表列出了相关注册表：

| 注册表                    | 说明                                        | 默认值    |
|------------------------|-------------------------------------------|--------|
| EnableSessionShadowing | 启用或禁用会话重影功能                               | 1 (启用) |
| ShadowingUseSSL        | 确定是否对 Linux VDA 和 Citrix Director 之间的连接加密 | 0 (禁用) |

可在 Linux VDA 上运行 `ctxreg` 命令来更改注册表值。例如，要禁用会话影子处理，请运行以下命令：

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
VirtualDesktopAgent" -v "EnableSessionShadowing" -d 0x00000000
```

## SSL

Linux VDA 和 Citrix Director 之间的 noVNC 连接使用 WebSocket 协议。对于会话重影，由前面提及的“ShadowingUseSSL”注册表确定选择 `ws://` 或 `wss://`。默认情况下，选择 `ws://`。但是，出于安全原因，Citrix 建议您使用 `wss://`，并在每个 Citrix Director 客户端和每台 Linux VDA 服务器上安装证书。Citrix 拒绝承担使用 `ws://` 进行 Linux VDA 会话重影的任何安全责任。

获取服务器证书和根 **SSL** 证书 证书必须由可信证书颁发机构 (CA) 签发。

对于要在其中配置 SSL 的每台 Linux VDA 服务器来说，都需要一份单独的服务器证书（包括密钥）。服务器证书标识特定的计算机，因此您必须知道每台服务器的完全限定的域名 (FQDN)。为了方便起见，您可以对整个域使用通配符证书。在这种情况下，您必须至少知道域名。

除了每台服务器上安装一份服务器证书之外，还必须在与 Linux VDA 服务器通信的每个 Citrix Director 客户端上安装从同一 CA 获取的根证书。根证书可从颁发服务器证书的同一 CA 获得。您可以安装来自以下 CA 的服务器证书和客户端证书：与您的操作系统捆绑的 CA，企业 CA（组织授予您访问权限的 CA），或没有与您的操作系统捆绑的 CA。请咨询您组织的安全团队，了解他们需要哪种方法来获取证书。

重要：

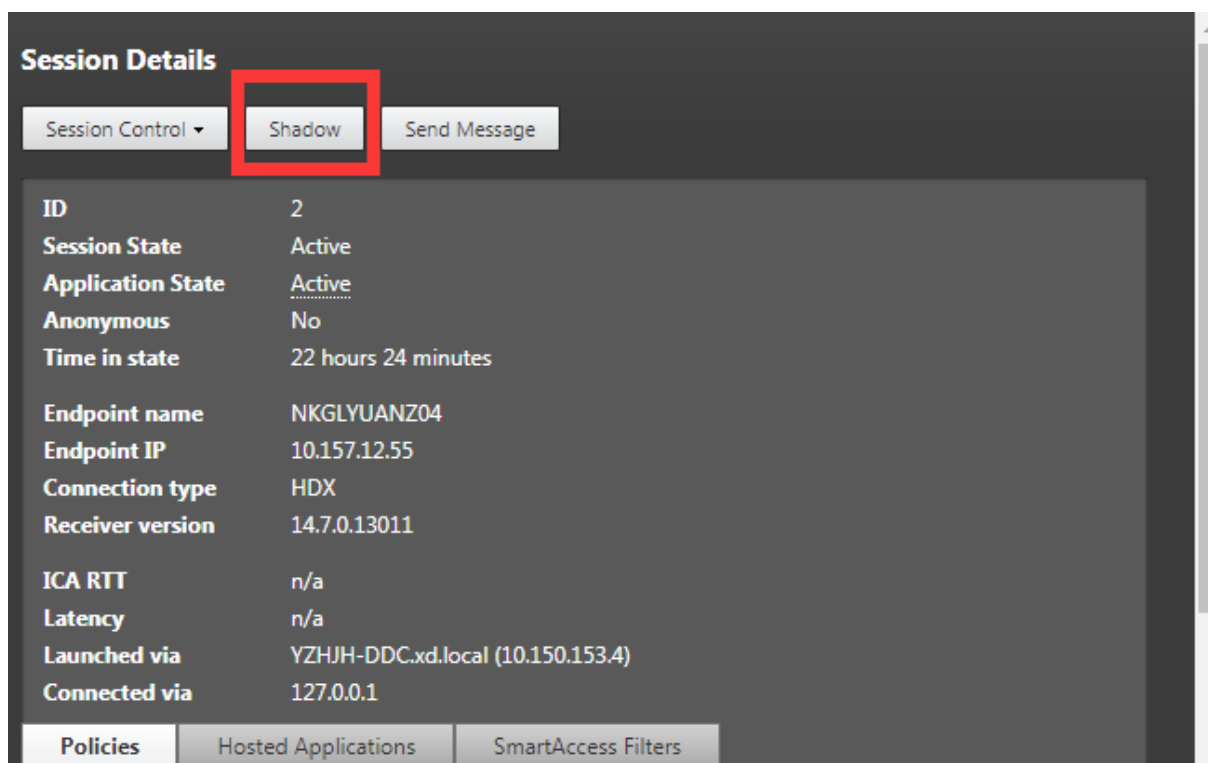
- 服务器证书的公用名必须是 Linux VDA 服务器的确切 FQDN 或至少是正确的通配符加域字符。例如 `vda1.basedomain.com` 或 `*.basedomain.com`。
- 哈希算法（包括 SHA1 和 MD5）对于数字证书中的签名而言太弱，某些浏览器不支持。因此，SHA-256 指定为最低标准。

在每个 **Citrix Director** 客户端上安装根证书 会话重影与 IIS 使用相同的基于注册表的证书存储，因此您可以使用 IIS 或 Microsoft 管理控制台 (MMC) 证书管理单元安装根证书。收到 CA 的证书后，可在 IIS 中重新启动 Web 服务器证书向导，然后此向导将安装该证书。另外，您可以在使用 MMC 并将证书作为独立的管理单元添加的计算机上，查看并导入证书。默认情况下，Internet Explorer 和 Google Chrome 会导入安装在操作系统上的证书。对于 Mozilla Firefox，必须在证书管理器的 **Authorities**（颁发机构）选项卡上导入您的根 SSL 证书。

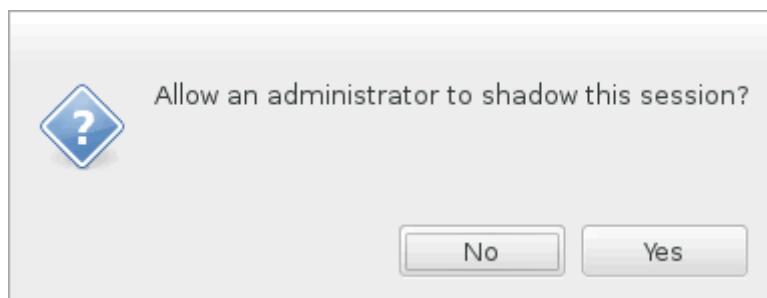
在每台 **Linux VDA** 服务器上安装服务器证书及其密钥 将服务器证书命名为“`shadowingcert.*`”，并将密钥文件命名为“`shadowingkey.*`”（\* 可以指示格式，例如 `shadowingcert.csr` 和 `shadowingkey.key`）。将服务器证书和密钥文件放在路径 `/etc/xdl/shadowingssl` 下，并使用受限权限适当地对其进行保护。如果名称或路径不正确，Linux VDA 将无法找到特定的证书或密钥文件，从而导致与 Citrix Director 的连接失败。

## 使用情况

在 Citrix Director 中，找到目标会话，然后单击会话详细信息视图中的重影以向 Linux VDA 发送重影请求。



连接初始化后，ICA 会话客户端（不是 Citrix Director 客户端）上会显示一条确认消息，要求用户允许对会话进行重影。



如果用户单击是，则 Citrix Director 端将显示一个窗口，指示正在重影 ICA 会话。

有关用法的详细信息，请参阅 [Citrix Director 文档](#)。

## 限制

- 会话重影仅适用于 Intranet。它不适用于外部网络，即使通过 Citrix Gateway 连接也是如此。Citrix 拒绝承担在外部网络中进行 Linux VDA 会话重影的任何责任。
- 启用了会话重影后，域管理员只能查看 ICA 会话，但无权对其写入或控制。

- 管理员在 Citrix Director 中单击重影后，系统会显示一条确认消息，要求用户允许对会话进行重影。只有在会话用户允许后才能对会话进行重影。
- 前面提及的确认消息有超时限制，即 20 秒。超时后，重影请求将失败。
- 在一个 Citrix Director 窗口中，一个 ICA 会话只能由一位管理员重影。如果某个 ICA 会话已由管理员 A 重影，此时，管理员 B 发送重影请求，则会在用户设备上重新出现要求用户允许的确认消息。如果用户同意，则管理员 A 的重影连接将停止，并为管理员 B 创建一个新的重影连接。如果同一位管理员发送另一个针对同一 ICA 会话的重影请求，也是同样情况。
- 要使用会话重影，请安装 Citrix Director 7.16 或更高版本。
- Citrix Director 客户端使用 FQDN 而不是 IP 地址来连接到目标 Linux VDA 服务器。因此，Citrix Director 客户端必须能够解析 Linux VDA 服务器的 FQDN。

## 故障排除

如果会话重影失败，请在 Citrix Director 客户端和 Linux VDA 上执行调试。

### 在 **Citrix Director** 客户端上

通过浏览器的开发人员工具，在控制台选项卡上检查输出日志。或者在网络选项卡上检查 ShadowLinuxSession API 的响应。如果出现了要求用户允许的确认消息，但无法建立连接，请手动 ping Linux VDA 的 FQDN 以验证 Citrix Director 是否可以解析 FQDN。如果 `wss://` 连接出现问题，请检查您的证书。

### 在 **Linux VDA** 上

确认在出现重影请求时，是否显示要求用户允许的确认消息。如果没有，请检查 `vda.log` 和 `hdx.log` 文件以获取相关线索。要获取 `vda.log` 文件，请执行以下操作：

1. 找到 `/etc/xdl/ctx-vda.conf` 文件。取消注释以下行以启用 `vda.log` 配置：

```
Log4jConfig="/etc/xdl/log4j.xml"
```

2. 打开 `/etc/xdl/log4j.xml`，找到 `com.citrix.dmc` 部分，并将“info”更改为“trace”，如下所示：

```
1 <!-- Broker Agent Plugin - Director VDA plugin Logger -->
2
3 <logger name="com.citrix.dmc">
4
5 <level value="trace"/>
6
7 </logger>
8 <!--NeedCopy-->
```

3. 运行 `service ctxvda restart` 命令以重新启动 `ctxvda` 服务。

如果在建立连接期间出现错误：

1. 检查是否有任何防火墙限制阻止会话重影打开端口。
2. 在使用 SSL 的情况下，确认证书和密钥文件是否正确命名，并放在正确的路径下。
3. 确认 6001-6099 之间是否有足够的端口用于新的重影请求。

## 支持适用于 **HTML5** 的 **Citrix Workspace** 应用程序

November 8, 2021

从此版本开始，您可以使用适用于 HTML5 的 Citrix Workspace 应用程序来直接访问 Linux 虚拟应用程序和桌面，而无需将客户端连接到 Citrix Gateway。有关适用于 HTML5 的 Citrix Workspace 应用程序的信息，请参阅 [Citrix 文档](#)。

### 启用此功能

默认情况下，此功能处于禁用状态。要启用该功能，请执行以下操作：

1. 在 Citrix StoreFront 中，启用适用于 HTML5 的 Citrix Workspace 应用程序。

有关详细过程，请参阅知识中心文章 [CTX208163](#) 的“步骤 1”。

2. 启用 WebSocket 连接。

- a) 在 Citrix Studio 中，将 **WebSocket** 连接策略设置为允许。

您还可以设置其他 WebSocket 策略。有关 WebSocket 策略的完整列表，请参阅 [WebSockets 策略设置](#)。

- b) 在 VDA 上，请按此顺序重新启动 `ctxvda` 服务和 `ctxhdx` 服务，以使设置生效。

- c) 在 VDA 上，运行以下命令来检查 WebSocket 侦听器是否正在运行。

```
netstat -an | grep 8008
```

WebSocket 侦听器处于运行状态时，命令输出将如下所示：

```
tcp 0 0 :::8008 :::* LISTEN
```

注意：您还可以启用 TLS 加密以保护 WebSocket 连接的安全。有关启用 TLS 加密的信息，请参阅 [使用 TLS 保护用户会话安全](#)。

## 监视 **Citrix Director** 中的 **Linux** 会话

June 16, 2023

以下衡量指标可用于 Citrix Director 中的 Linux 会话。要查看衡量指标，请在 Citrix Director 中查找目标会话并检查会话详细信息面板。

- ICA RTT

自 Linux VDA 1903 版起，可以查看 ICA RTT 衡量指标。要查看 ICA RTT 衡量指标，请使用 Citrix Director 1903 或更高版本并在 Citrix Studio 中创建 **ICA** 往返行程计算和 **ICA** 往返行程计算时间间隔策略。有关创建策略的信息，请参阅[使用 Studio 创建策略](#)。

- 协议

自 Linux VDA 1909 版起，可以查看协议信息。Linux 会话的传输协议将在会话详细信息控制板中显示为 **UDP** 或 **TCP**。

## 监视服务守护程序

November 8, 2021

监视服务守护程序通过执行定期扫描来监视关键服务。检测到异常时，该守护程序会重新启动或停止服务进程，并清除进程残留以释放资源。检测到的异常记录在 `/var/log/xdl/ms.log` 文件中。

### 配置

当您启动 VDA 时，监视服务守护程序将自动启动。

可以使用管理员权限通过 **scanningpolicy.conf**、**rulesets.conf** 和 **whitelist.conf** 文件配置该功能。配置文件位于 `/opt/Citrix/VDA/sbin` 下。

要使 **scanningpolicy.conf**、**rulesets.conf** 和 **whitelist.conf** 文件中的更改生效，请运行以下命令以重新启动监视服务守护程序。

```
1 service ctxmonitorservice restart
2 <!--NeedCopy-->
```

- **scanningpolicy.conf**

此配置文件启用或禁用监视服务守护程序。它设置服务检测时间间隔，并指定是否修复检测到的异常。

- MonitorEnable: true/false (默认值为 true)
- DetectTime: 20 (单位: 秒, 默认值: 20, 最小值: 5)
- AutoRepair: true/false (默认值为 true)
- MultBalance: false



- ReportAlarm: false

- **rulesets.conf**

此配置文件指定要监视的目标服务。默认情况下有四种受监视的服务，如下面的屏幕截图所示。

```
MonitorUser: all
MonitorType: 3
ProcessName: ctxhdx
Operation: 4
DBRecord: false
MonitorUser: all
MonitorType: 3
ProcessName: ctxvda
Operation: 4
DBRecord: false
MonitorUser: all
MonitorType: 3
ProcessName: ctxpolicyd
Operation: 4
DBRecord: false
MonitorUser: all
MonitorType: 3
ProcessName: Xorg
Operation: 8
DBRecord: false
```

要配置要监视的每个服务，请设置以下字段。

- MonitorUser: all
- MonitorType: 3
- ProcessName: <> (进程名称不能留空，必须完全匹配。)
- Operation: 1/2/4/8 (1 = 检测到异常时停止服务。2 = 检测到异常时终止服务。4 = 重新启动服务。8 = 清理 Xorg 进程残留。)
- DBRecord: false

- **whitelist.conf**

在 **rulesets.conf** 文件中指定的目标服务也必须在 **whitelist.conf** 文件中配置。白名单配置是安全性的辅助筛选器。

要配置白名单，请在 **whitelist.conf** 文件中仅包含进程名称 (必须完全匹配)。有关示例，请参阅下面的屏幕截图。

```
ctxcdmd
ctxcdmmount
ctxcdmstat
ctxceip
ctxclipboard
ctxconnect
ctxcredentialctl
ctxctl
ctxcupsd
ctxdisconnect
ctxeuem
ctxfiletransfer
ctxgfx
ctxhdx
ctxism
ctxlogd
ctxlogin
ctxmonitorservice
ctxmrvc
ctxpolicyd
ctxscardsd
ctxvhcid
ctxvda
Xorg
```

注意：

在停止 `ctxvda`、`ctxhdx` 和 `ctxpolicyd` 服务之前，请运行 `service ctxmonitorservice stop` 命令以停止监视服务守护程序。否则，监视服务守护程序将重新启动您停止的服务。

## 使用 TLS 保护用户会话安全

March 1, 2022

自版本 7.16 起，Linux VDA 支持用于保护用户会话安全的 TLS 加密。默认情况下，TLS 加密处于禁用状态。

### 启用 TLS 加密

要启用用于保护用户会话安全的 TLS 加密，请在 Linux VDA 和 Delivery Controller (Controller) 上获取证书并启用 TLS 加密。

#### 获取证书

从可信证书颁发机构 (CA) 获取 PEM 格式的服务器证书和 CRT 格式的根证书。服务器证书包含以下部分：

- 证书
- 未加密的私钥
- 中间证书（可选）

服务器证书示例：



## 启用 TLS 加密

在 **Linux VDA** 上启用 **TLS** 加密 在 Linux VDA 上，使用 **enable\_vdassl.sh** 工具启用（或禁用）TLS 加密。该工具位于 **/opt/Citrix/VDA/sbin** 目录中。有关该工具中可用选项的信息，请运行 **/opt/Citrix/VDA/sbin/enable\_vdassl.sh -help** 命令。

提示：必须在每台 Linux VDA 服务器上安装服务器证书，以及必须在每台 Linux VDA 服务器和客户机上安装根证书。

## 在 **Controller** 上启用 **TLS** 加密

### 注意：

只能对整个交付组启用 TLS 加密。不能为特定应用程序启用 TLS 加密。

在 **Controller** 上的 PowerShell 窗口中，按顺序运行以下命令以对目标交付组启用 TLS 加密。

1. `Add-PSSnapin citrix.*`
2. `Get-BrokerAccessPolicyRule -DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true`

### 注意：

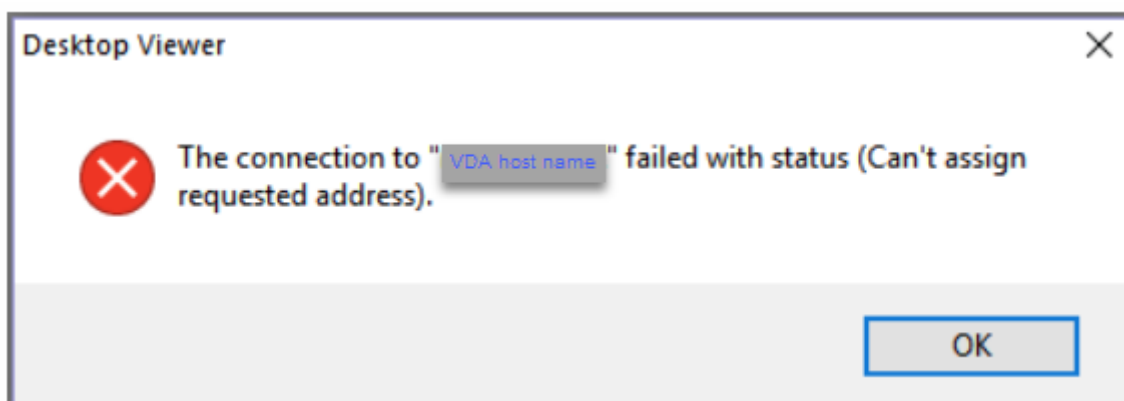
要确保 ICA 会话文件中仅包含 VDA FQDN，还可以运行 **Set-BrokerSite -DnsResolutionEnabled \$true** 命令。该命令将启用 DNS 解析。如果禁用了 DNS 解析，ICA 会话文件会显示 VDA IP 地址，并仅为与 TLS 相关的项目（例如 `SSLProxyHost` 和 `UDPDTLSport`）提供 FQDN。

要在 **Controller** 上禁用 TLS 加密，请按顺序运行以下命令：

1. `Add-PSSnapin citrix.*`
2. `Get-BrokerAccessPolicyRule -DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule -HdxSslEnabled $false`
3. `Set-BrokerSite -DnsResolutionEnabled $false`

## 故障排除

尝试访问已发布的桌面会话时，适用于 Windows 的 Citrix Workspace 应用程序中可能会出现下面的“无法分配请求的地址”错误：



解决方法：向 **hosts** 文件添加一个条目，类似于：

<IP address of the Linux VDA>            <FQDN of the Linux VDA>

在 Windows 计算机上，**hosts** 文件通常位于 `C:\Windows\System32\drivers\etc\hosts` 中。

## 使用 **DTLS** 的安全用户会话

November 8, 2021

从 7.18 版本起，DTLS 加密是一项完全受支持的功能。默认情况下，此功能在 VDA 上处于启用状态。有关详细信息，请参阅[传输层安全性](#)。

### 启用 **DTLS** 加密

验证自适应传输是否已启用

在 Citrix Studio 中，验证 **HDX** 自适应传输策略设置为首选还是诊断模式。

在 **Linux VDA** 上启用 **SSL** 加密

在 Linux VDA 上，使用 **enable\_vdassl.sh** 工具启用（或禁用）SSL 加密。该工具位于 `/opt/Citrix/VDA/sbin`。有关该工具中可用选项的信息，请运行 `/opt/Citrix/VDA/sbin/enable_vdassl.sh -h` 命令。

注意：

当前，Linux VDA 支持 DTLS 1.0 和 DTLS 1.2。DTLS 1.2 需要 Citrix Receiver for Windows 4.12 或适用于 Windows 的 Citrix Workspace 应用程序 1808 或更高版本。如果您的客户端仅支持 DTLS 1.0（例如 Citrix

Receiver for Windows 4.11)，请使用 `enable_vdassl.sh` 工具将 `SSLMinVersion` 设置为 `TLS_1.0`，将 `SSLCipherSuite` 设置为 `COM` 或 `ALL`。

## 支持智能卡

April 18, 2024

登录 Linux Virtual Desktop 会话时，可以使用连接到客户端设备的智能卡进行身份验证。此功能是通过 ICA 智能卡虚拟通道进行的智能卡重定向实现的。还可以在会话中使用智能卡。用例包括向文档中添加数字签名、加密或解密电子邮件或向要求智能卡身份验证的 Web 站点进行身份验证。

对于此功能，Linux VDA 使用与 Windows VDA 相同的配置。有关详细信息，请参阅本文中的[配置智能卡环境](#)部分。

使用智能卡进行直通身份验证的可用性取决于以下条件：

- Linux VDA 安装在 RHEL 7.7 上。
- 使用 CoolKey 支持智能卡。
- 使用 Citrix Workspace for Windows 的应用程序。

注意：

官方不支持在 Linux VDA 会话中使用映射的智能卡登录 Citrix Gateway。

## 在 RHEL 7.7 上安装 Linux VDA 软件

使用 RPM 软件包管理器或[轻松安装](#)功能安装 Linux VDA 软件，请参阅[安装概述](#)部分。

VDA 安装完成后，请验证 VDA 是否能够在 Delivery Controller 中注册，以及已发布的 Linux 桌面会话是否能够使用密码身份验证成功启动。

## 确保 CoolKey 支持智能卡

CoolKey 是 RHEL 上广泛使用的智能卡驱动程序。CoolKey 支持四种类型的智能卡，即 CoolKey 卡、CAC、PIV 和 PKCS#15。但正式支持并通过验证的卡的数量仍有限；请参阅[Smart Card Support in Red Hat Enterprise Linux](#) (Red Hat Enterprise Linux 中的智能卡支持)。

在本文中，YubiKey 4 智能卡用作阐明配置的示例。YubiKey 4 是一个通用 USB CCID PIV 设备，可以很容易地从 Amazon 或其他零售供应商处购买。CoolKey 驱动程序支持 YubiKey 4。



如果贵组织需要某些其他更高级的智能卡，请准备一台安装了 RHEL 7.7 和 CoolKey 软件包的物理机。有关 CoolKey 安装的信息，请参阅[安装智能卡驱动程序](#)。插入智能卡，然后运行以下命令以确认 CoolKey 是否支持智能卡：

```
1 pkcs11-tool --module libcoolkeypk11.so --list-slots
2 <!--NeedCopy-->
```

如果 CoolKey 支持智能卡，命令输出将与下面包含插槽信息的内容类似。

```
[root@rhphy ~]# pkcs11-tool --module libcoolkeypk11.so --list-slots
Available slots:
Slot 0 (0x1): Yubico Yubikey 4 CCID 00 00
 token label : user1
 token manufacturer :
 token model :
 token flags : login required, token initialized, PIN initialized, readonly
 hardware version : 0.0
 firmware version : 0.0
 serial num :
[root@rhphy ~]#
```

## 配置

### 准备根证书

根证书用于验证智能卡上的证书。请执行以下操作以下载并安装根证书。

1. 获取 PEM 格式的根证书，通常从 CA 服务器中获取。

可以运行类似如下的命令以将 DER 文件 (\*.crt、\*.cer、\*.der) 转换为 PEM。在下面的命令示例中，**certnew.cer** 为 DER 文件。

```
1 openssl x509 -inform der -in certnew.cer -out certnew.pem
2 <!--NeedCopy-->
```

2. 在 `openssl` 目录中安装根证书。**certnew.pem** 文件用作示例。



```
1 cp certnew.pem <path where you install the root certificate>
2 <!--NeedCopy-->
```

要创建安装根证书的路径，请运行 `sudo mkdir -p <path where you install the root certificate>`。

### 配置 NSS 数据库

Linux VDA 登录模块依赖 NSS 数据库来访问智能卡和证书。请执行以下操作以配置 NSS 数据库。

1. 将前面提及的根证书添加到 NSS 数据库中。

```
1 certutil -A -n "My Corp Root" -t "CT,C,C" -a -d /etc/pki/nssdb -i
 /etc/pki/CA/certs/certnew.pem
2 <!--NeedCopy-->
```

2. 运行以下命令以验证根证书是否已成功添加到 NSS 数据库中。

```
1 certutil -L -d /etc/pki/nssdb
2 <!--NeedCopy-->
```

如果已成功添加根证书，命令输出将如下所示。

```
[root@rh73ws LVDA]# certutil -L -d /etc/pki/nssdb

Certificate Nickname Trust Attributes
 SSL,S/MIME,JAR/XPI

My Corp Root CT,C,C
```

3. 检查 CoolKey 是否已安装在 NSS PKCS#11 库中。

```
1 modutil -list -dbdir /etc/pki/nssdb
2 <!--NeedCopy-->
```

如果已安装 CoolKey 模块，命令输出将如下所示。

```
[root@rh73demo ~]# modutil -list -dbdir /etc/pki/nssdb

Listing of PKCS #11 Modules

1. NSS Internal PKCS #11 Module
 slots: 2 slots attached
 status: loaded

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

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

2. CoolKey PKCS #11 Module
 library name: libcoolkeypk11.so
 slots: There are no slots attached to this module
 status: loaded

```

如果未安装 CoolKey 模块，请运行以下命令以手动安装该模块，然后重新检查安装。

```
1 modutil -add "CoolKey PKCS #11 Module" -libfile libcoolkeypk11.so
 -dbdir /etc/pki/nssdb
2 <!--NeedCopy-->
```

#### 4. 配置 pam\_pkcs11 模块。

pam\_pkcs11 模块依赖本地 VDA 配置来验证用户证书。pam\_pkcs11 使用的默认根证书位于 **/etc/pam\_pkcs11/cacerts/**。此路径中的每个根证书都有一个哈希链接。请运行以下命令以安装准备好的根证书并配置 pam\_pkcs11。

```
1 yum install pam_pkcs11
2
3 mkdir /etc/pam_pkcs11/cacerts/
4
5 cp certnew.pem /etc/pam_pkcs11/cacerts/
6
7 cacertdir_rehash /etc/pam_pkcs11/cacerts
8 <!--NeedCopy-->
```

#### 配置智能卡环境

可以使用 ctxsmartlogon.sh 脚本配置智能卡环境或手动执行配置。

- 使用 ctxsmartlogon.sh 脚本配置智能卡环境

注意：

ctxsmartlogon.sh 脚本将 PKINIT 信息添加到默认领域。可以通过 **/etc/krb5.conf** 配置文件更改此

设置。

首次使用智能卡之前，请运行 `ctxsmartlogon.sh` 脚本以配置智能卡环境。

提示：

如果已使用 SSSD 加入域，请在运行 `ctxsmartlogon.sh` 后重新启动该 SSSD 服务。

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

结果类似于以下内容：

```

ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
includes automatic installation of the necessary packages and changes to
the configuration files.
#
Note:
The ctxsmartlogon.sh adds pkinit information to the default realm. You can
change this setting through the /etc/krb5.conf configuration file.

Step 1:Enable smart card logon.
Do you want enable smart card logon? (y/n)[y] y
Step 2:Select the Active Directory integration method.
Please select which Active Directory integration method to use:
1: Winbind
2: SSSD
3: Centrify
Select one of the above options (1-3)[1] 1
Step 3:Install dependent packages.
Installing, please wait...
[krb5-pkinit][pam_krb5] already installed.
[pcsc-lite][pcsc-lite-ccid][pcsc-lite-libs][coolkey] already installed.
Packages installed. [Success]
Step 4:Configure krb5.conf.
Specify the path to the root CA (e.g., /etc/pki/CA/certs/root.pem):/etc/pki/CA/certs/root.pem
/etc/krb5.conf configure successfully.
Step 5:Configure PAM files.
Specify the path to the smart card PKCS11 driver (e.g., /usr/lib64/pkcs11/libcoolkeypk11.so):/usr/lib64/pkcs11/libcoolkeypk11.so
/etc/pam.d/ctxfsc configure successfully.
/etc/pam.d/smartcard-auth configure successfully.
ctxsmartlogon.sh executed successfully. SmartCard is ready.
```

此外，您还可以通过运行 `ctxsmartlogon.sh` 脚本来禁用智能卡：

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

结果类似于以下内容：

```

ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
includes automatic installation of the necessary packages and changes to
the configuration files.
#
Note:
The ctxsmartlogon.sh adds pkinit information to the default realm. You can
change this setting through the /etc/krb5.conf configuration file.

Step 1:Enable smart card logon.
Do you want enable smart card logon? (y/n)[y] n
ctxsmartlogon.sh exit.
```

- 手动配置智能卡环境

Linux VDA 使用与 Windows VDA 相同的智能卡环境。在该环境中，必须配置多个组件，包括域控制器、Microsoft 证书颁发机构 (CA)、Internet Information Services、Citrix StoreFront 和 Citrix Workspace 应用程序。有关基于 YubiKey 4 智能卡的配置信息，请参阅知识中心文章 [CTX206156](#)。

继续执行下个步骤之前，请确保所有组件都已正确配置，私钥和用户证书都已下载到智能卡，并且您能够使用智能卡成功登录 Windows VDA。

### 安装 **PC/SC Lite** 软件包

PCSC Lite 是个人计算机/智能卡 (PC/SC) 规范在 Linux 中的实现。它提供与智能卡和读卡器进行通信的 Windows 智能卡接口。Linux VDA 中的智能卡重定向是在 PC/SC 级别实现的。

运行以下命令可安装 PC/SC Lite 软件包。

```
1 yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
2 <!--NeedCopy-->
```

### 安装智能卡读卡器

CoolKey 是 RHEL 上广泛使用的智能卡驱动程序。如果未安装 CoolKey，请运行以下命令以进行安装。

```
1 yum install coolkey
2 <!--NeedCopy-->
```

### 安装用于智能卡身份验证的 **PAM** 模块

运行以下命令可安装 pam\_krb5 和 krb5-pkinit 模块。

```
1 yum install pam_krb5 krb5-pkinit
2 <!--NeedCopy-->
```

pam\_krb5 模块是可插入身份验证模块，可识别 PAM 的应用程序可以使用它来检查密码以及从密钥发行中心 (KDC) 获取票据授予票据。krb5-pkinit 模块包含允许客户端使用私钥和证书从 KDC 获取初始凭据的 PKINIT 插件。

### 配置 **pam\_krb5** 模块

pam\_krb5 模块与 KDC 交互以使用智能卡中的证书获取 Kerberos 票据。要在 PAM 中启用 pam\_krb5 身份验证，请运行以下命令：

```
1 authconfig --enablekrb5 --update
2 <!--NeedCopy-->
```

在 `/etc/krb5.conf` 配置文件中，根据实际的领域添加 PKINIT 信息。

注意：

**pkinit\_cert\_match** 选项指定客户端证书在用于尝试 PKINIT 身份验证之前必须匹配的规则。匹配规则的语法为：

`[relation-operator] component-rule ...`

其中 **relation-operator** 可以为 `&&`，表示所有组件规则必须匹配，也可以为 `||`，表示只有一条组件规则必须匹配。

西面是一个通用 `krb5.conf` 文件的示例：

```

1 EXAMPLE.COM = {
2
3
4 kdc = KDC. EXAMPLE.COM
5
6 auth_to_local = RULE:[1:$1@$0]
7
8 pkinit_anchors = FILE:<path where you install the root certificate
9 >/certnew.pem
10
11 pkinit_kdc_hostname = KDC.EXAMPLE.COM
12
13 pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
14
15 pkinit_eku_checking = kpServerAuth
16 }
17
18 <!--NeedCopy-->

```

添加 PKINIT 信息后，该配置文件将如下所示。

```

XD.LOCAL = {
 kdc = ██████████
 auth_to_local = RULE:[1:$1@$0]
 pkinit_anchors = FILE:/etc/pki/CA/certs/certnew.pem
 pkinit_kdc_hostname = SZCXC-DOMAINC.XD.LOCAL
 pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
 pkinit_eku_checking = kpServerAuth
}

```

### 配置 PAM 身份验证

PAM 配置文件指示用于 PAM 身份验证的模块。要添加 `pam_krb5` 作为身份验证模块，请向 `/etc/pam.d/smartcard-auth` 文件中添加以下行：

```
auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:/usr/lib64/pkcs11/libcoolkeypk11.so
```

如果使用 SSSD，则修改后该配置文件将如下所示。

```

#%PAM-1.0
This file is auto-generated.
User changes will be destroyed the next time authconfig is run.
auth required pam_env.so
auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:/usr/lib64/pkcs11/libcoolkeypk11.so
auth sufficient pam_permit.so
auth required pam_deny.so

account required pam_unix.so
account sufficient pam_localuser.so
account sufficient pam_succeed_if.so uid < 1000 quiet
account [default=bad success=ok user_unknown=ignore] pam_sss.so
account [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore] pam_krb5.so
account required pam_permit.so

password required pam_pkcs11.so

session optional pam_keyinit.so revoke
session required pam_limits.so
-session optional pam_systemd.so
#session optional pam_oddjob_mkhomedir.so umask=0077
session optional pam_mkhomedir.so umask=0077
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session required pam_unix.so
session optional pam_sss.so
session optional pam_krb5.so

```

如果使用 Winbind，则修改后该配置文件将如下所示。

```

#%PAM-1.0
This file is auto-generated.
User changes will be destroyed the next time authconfig is run.
auth required pam_env.so
auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:/usr/lib64/pkcs11/libcoolkeypk11.so
auth sufficient pam_permit.so
auth required pam_deny.so

account required pam_unix.so broken_shadow
account sufficient pam_localuser.so
account sufficient pam_succeed_if.so uid < 1000 quiet
account [default=bad success=ok user_unknown=ignore] pam_winbind.so
account [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore] pam_krb5.so
account required pam_permit.so

password required pam_pkcs11.so

session optional pam_keyinit.so revoke
session required pam_limits.so
-session optional pam_systemd.so
#session optional pam_oddjob_mkhomedir.so umask=0077
session optional pam_mkhomedir.so umask=0077
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session required pam_unix.so
session optional pam_winbind.so
session optional pam_krb5.so

```

如果使用 Centrify，则修改后该配置文件将如下所示。

```

#%PAM-1.0
This file is auto-generated.
User changes will be destroyed the next time authconfig is run.
auth required pam_env.so
auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:/usr/lib64/pkcs11/libcoolkeypk11.so
auth sufficient pam_permit.so
auth required pam_deny.so

account required pam_nologin.so
account required pam_krb5.so
account required pam_permit.so

password required pam_pkcs11.so

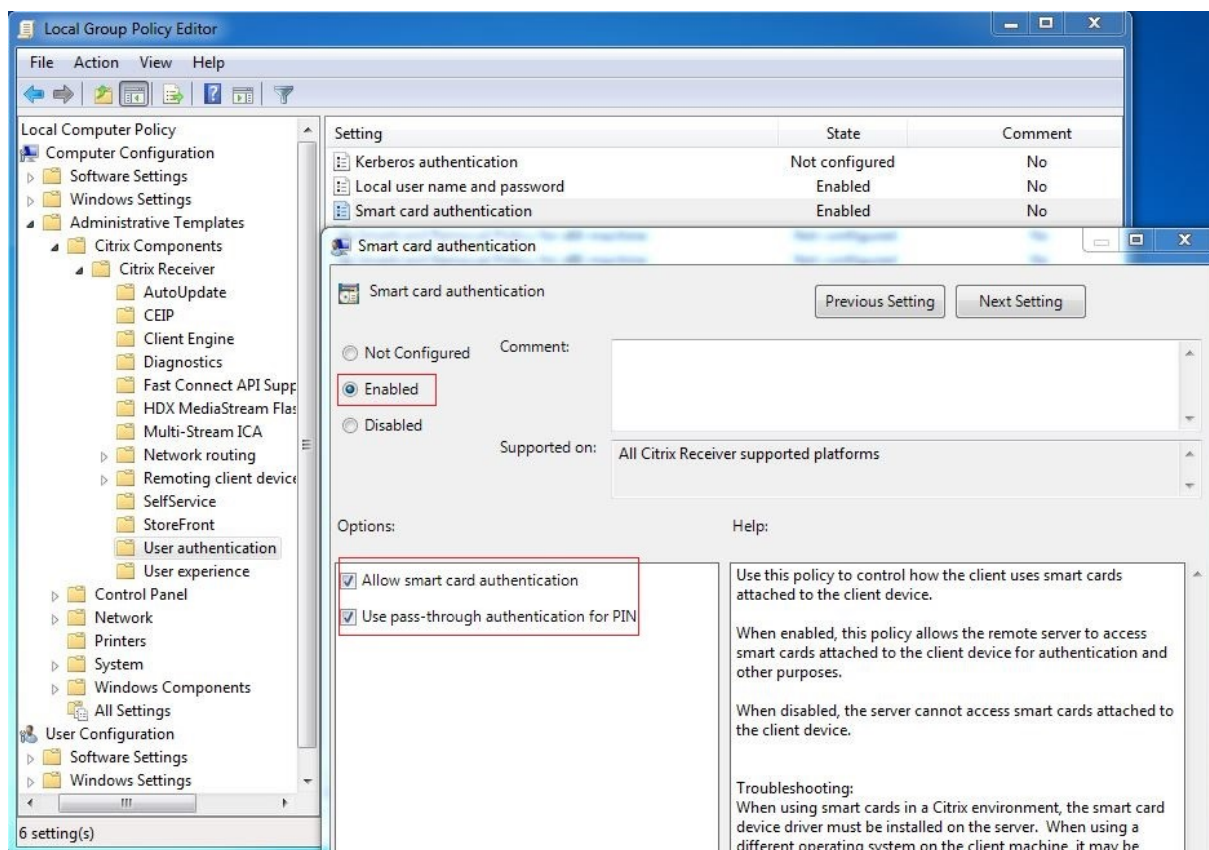
session optional pam_keyinit.so revoke
session required pam_limits.so
-session optional pam_systemd.so
session optional pam_mkhomedir.so umask=0077
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session required pam_unix.so
session optional pam_krb5.so

```

(可选) 使用智能卡进行单点登录

单点登录 (SSO) 是一项 Citrix 功能，用于实现对虚拟桌面和应用程序启动的直通身份验证。此功能降低了用户键入其 PIN 码的次数。要将 SSO 与 Linux VDA 结合使用，请配置 Citrix Workspace 应用程序。该配置与 Windows VDA 相同。有关详细信息，请参阅知识中心文章 [CTX133982](#)。

在 Citrix Workspace 应用程序中配置组策略时，请按如下所示启用智能卡身份验证。



### 快速智能卡登录

快速智能卡是对现有基于 HDX PC/SC 的智能卡重定向的改进。在高延迟 WAN 环境中使用智能卡时，可以提高性能。有关详细信息，请参阅[智能卡](#)。

Linux VDA 支持在以下版本的 Citrix Workspace 应用程序中使用快速智能卡：

- Citrix Receiver for Windows 4.12
- 适用于 Windows 的 Citrix Workspace 应用程序 1808 及更高版本

在客户端上启用快速智能卡登录 默认情况下，快速智能卡登录功能在 VDA 上处于启用状态，在客户端上处于禁用状态。在客户端，要启用快速智能卡登录，请将以下参数包含在关联 StoreFront 站点的 default.ica 文件中：

```
1 [WFClient]
2 SmartCardCryptographicRedirection=On
3 <!--NeedCopy-->
```

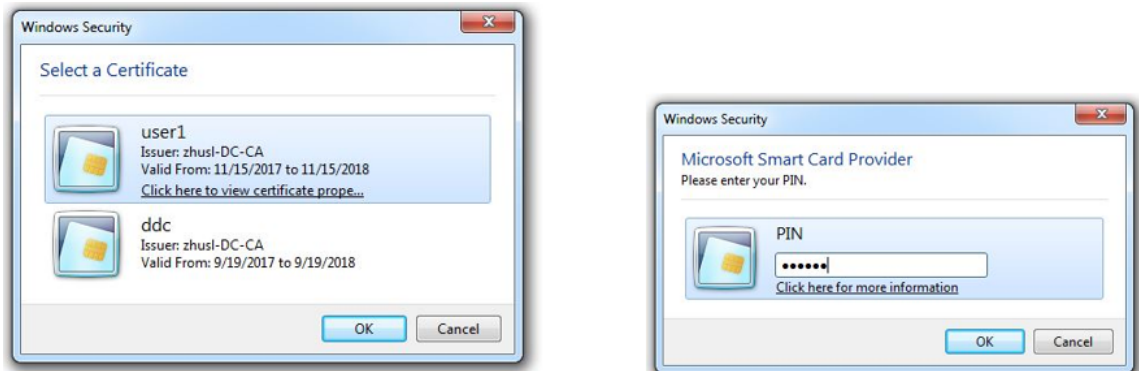
在客户端上禁用快速智能卡登录 要在客户端上禁用快速智能卡登录，请从关联的 StoreFront 站点的 default.ica 文件中删除 **SmartCardCryptographicRedirection** 参数。

## 使用情况

### 使用智能卡登录 Linux VDA

可以在 SSO 和非 SSO 场景中使用智能卡登录 Linux VDA。

- 在 SSO 场景中，您将使用缓存的智能卡证书和 PIN 码自动登录 StoreFront。在 StoreFront 中启动 Linux Virtual Desktop 会话时，PIN 码将传递到 Linux VDA 以进行智能卡身份验证。
- 在非 SSO 场景中，系统将提示您选择证书并键入 PIN 码以登录 StoreFront。



在 StoreFront 中启动 Linux Virtual Desktop 会话时，将显示 Linux VDA 登录对话框，如下所示。用户名是从智能卡中的证书中提取的，必须重新键入 PIN 码以进行登录身份验证。

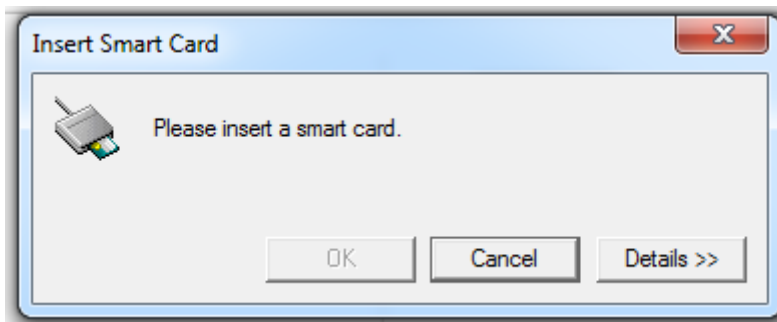
此行为与 Windows VDA 相同。

### 使用智能卡重新连接到会话

请务必将智能卡连接到客户端设备，才能重新连接到会话。否则，Linux VDA 端将显示一个灰色缓存窗口，并快速退出，因为重新身份验证在未连接智能卡的情况下失败。在这种情况下，系统不提供任何其他提示以提醒您连接智能卡。

但是，在 StoreFront 端，如果尝试重新连接到会话时未连接智能卡，StoreFront Web 可能会按如下所示提供警报。





## 限制

### 智能卡移除策略

Linux VDA 对智能卡移除仅使用默认行为。成功登录 Linux VDA 后移除智能卡时，会话仍保持连接，并且会话屏幕不锁定。

### 支持其他智能卡和 **PKCS#11** 库

虽然我们的支持列表中仅列出了 CoolKey 智能卡，但是您可以尝试使用其他智能卡和 PKCS#11 库，因为 Citrix 会提供通用智能卡重定向解决方案。要切换到特定的智能卡或 PKCS#11 库，请执行以下操作：

1. 使用 PKCS#11 库替换所有 `libcoolkeypk11.so` 实例。
2. 要将 PKCS#11 库的路径设置为注册表，请运行以下命令：

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
 CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v "
 PKCS11LibPath" -d "PATH"
2 <!--NeedCopy-->
```

其中 **PATH** 指向您的 PKCS#11 库，例如 `/usr/lib64/pkcs11/libcoolkeypk11.so`

3. 在客户端上禁用快速智能卡登录。

## 双跃点单点登录身份验证

November 8, 2021

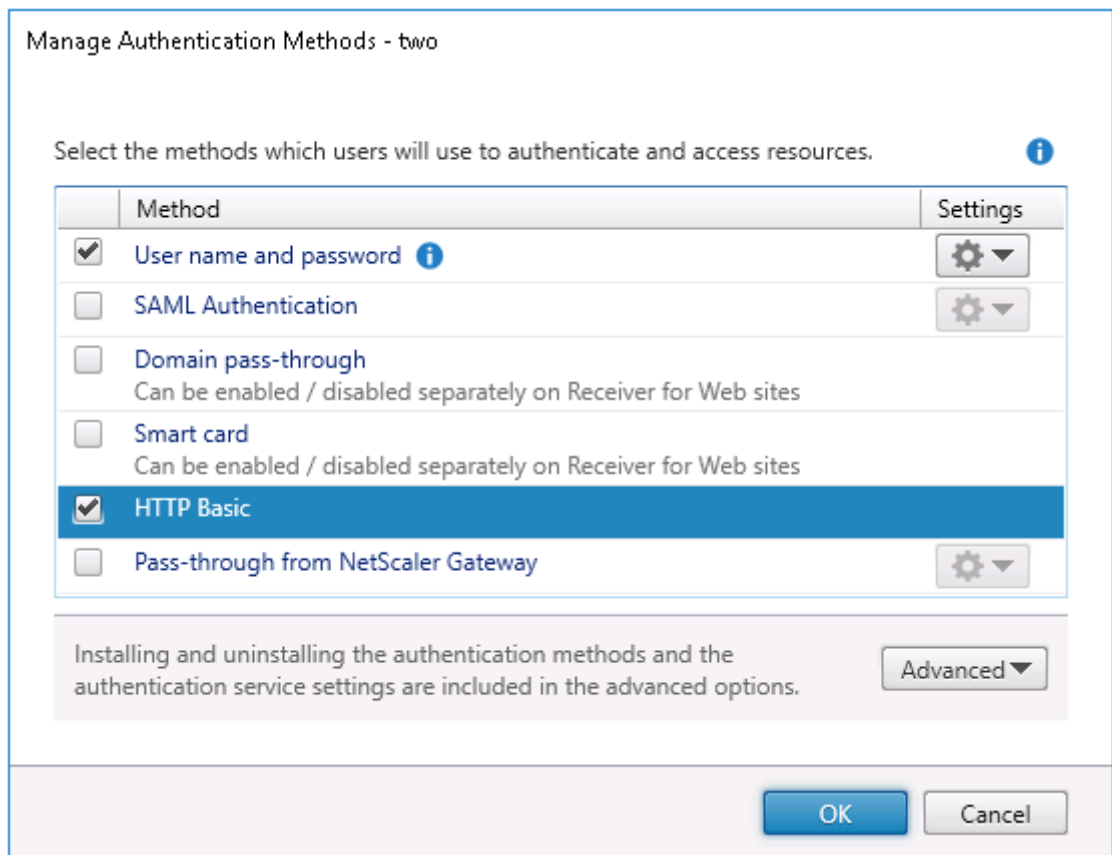
此功能可将访问 StoreFront 应用商店需要输入的用户凭据注入到适用于 Linux 的 Citrix Workspace 应用程序和 Citrix Receiver for Linux 13.10 的 AuthManager 模块。注入后，您可以使用该客户端访问 Linux 虚拟桌面会话中的虚拟桌面和应用程序，而无需再次输入用户凭据。

注意：

适用于 Linux 的 Citrix Workspace 应用程序和 Citrix Receiver for Linux 13.10 支持此功能。

要启用此功能，请执行以下操作：

1. 在 Linux VDA 上，安装适用于 Linux 的 Citrix Workspace 应用程序或 Citrix Receiver for Linux 13.10。  
从 Citrix Workspace 应用程序或 Citrix Receiver 的 [Citrix 下载页面](#) 下载相应应用程序。  
默认安装路径为 `/opt/Citrix/ICAClient/`。如果要应用程序安装在其他路径中，请将 `ICAROOT` 环境变量设置为指向实际安装路径。
2. 在 Citrix StoreFront 管理控制台中，为目标应用商店添加 **HTTP** 基本身份验证方法。



3. 将以下注册表项添加到 AuthManager 配置文件 (`$ICAROOT/config/AuthManConfig.xml`) 以允许进行 HTTP 基本身份验证：

```

1 <Protocols>
2 <HTTPBasic>
3 <Enabled>True</Enabled>
4 </HTTPBasic>
5 </Protocols>
6 <!--NeedCopy-->

```

4. 请运行以下命令以在指定目录中安装根证书。

```
1 cp rootcert.pem $ICAROOT/keystore/cacerts/
2 $ICAROOT/util/ctx_rehash $ICAROOT/keystore/cacerts/
3 <!--NeedCopy-->
```

5. 运行以下命令以启用该功能：

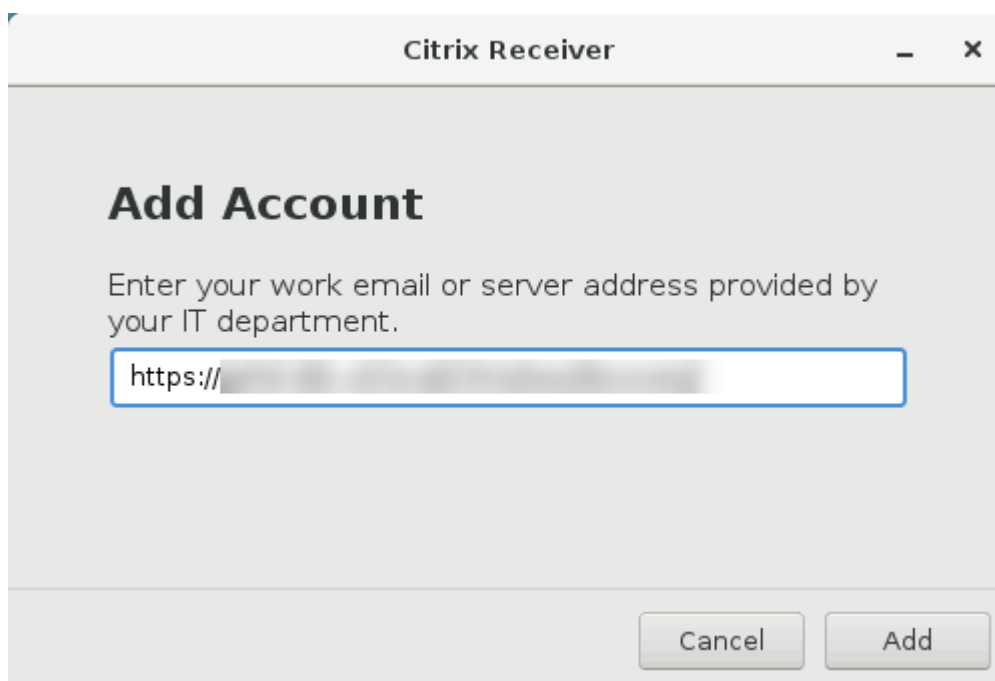
```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d "0
x00000001"
2 <!--NeedCopy-->
```

6. 启动 Linux 虚拟桌面会话和该会话中的适用于 Linux 的 Citrix Workspace 应用程序或 Citrix Receiver for Linux 13.10。

首次启动 Linux 虚拟桌面会话中的适用于 Linux 的 Citrix Workspace 应用程序或 Citrix Receiver for Linux 13.10 时，系统会提示您登录应用商店帐户。以后您可以自动登录到之前指定的应用商店。

注意：

输入 HTTPS URL 作为您的应用商店帐户。



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。会话预启动在适用于 Android 的 Citrix Workspace 应用程序上也不受支持。

### 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 [Citrix Virtual Apps and Desktops 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 **nscd** 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，可以尝试修改系统范围的 **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，请将根 CA 证书导入到受信任的密钥库。

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/xdl/.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 **/etc/samba/smb.conf** 和 **/etc/openldap/ldap.conf**（对于 RHEL）或 **/etc/ldap/ldap.conf**（对于 Ubuntu）。按如下所示更改这些文件：

- smb.conf

```
ldap ssl = start tls
ldap ssl ads = yes
client ldap sasl wrapping = plain
```

- ldap.conf

```
TLS_REQCERT never
```

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：

```
ldap ssl = off
ldap ssl ads = no
client ldap sasl wrapping = seal
```

## 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。

- 通过装载共享主目录将 `.Xauthority` 文件传递到 XClient

最便捷的方式是为登录用户装载共享主目录。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 + \< 显示数量\>` 的总和。

如果此 Telnet 操作失败，防火墙可能在阻止请求。

## 联合身份验证服务

June 16, 2023

### 概述

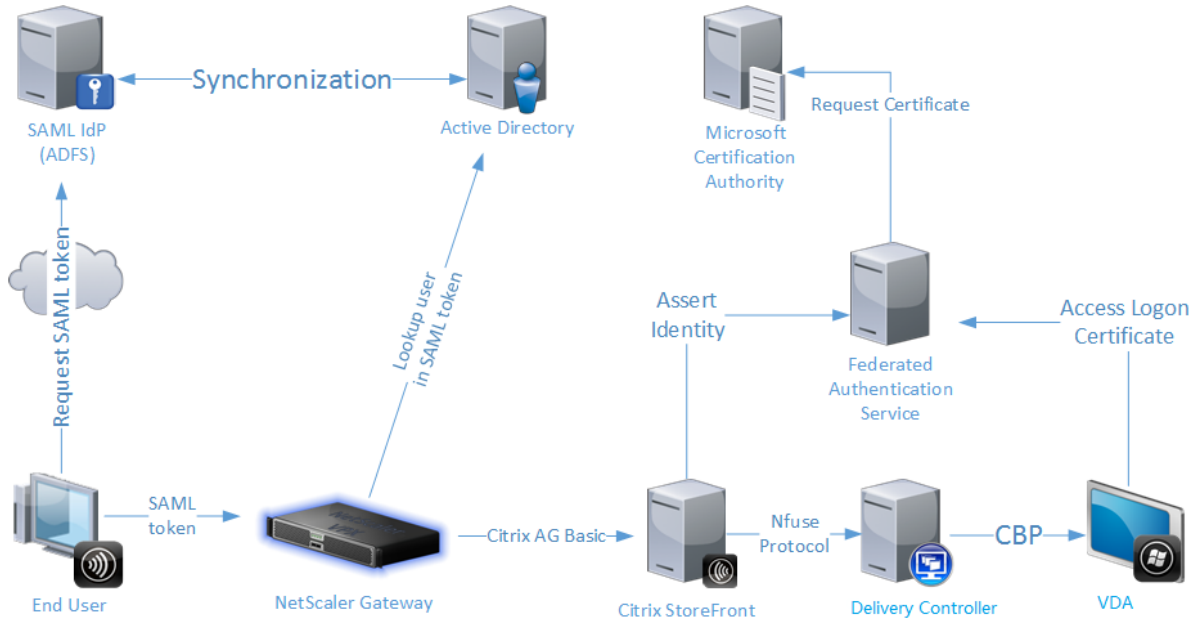
Citrix 联合身份验证服务 (FAS) 是一个特权组件，可与 Active Directory 证书服务集成。它动态地为用户颁发证书，以使用户能够登录到 Active Directory 环境，就如同他们具有智能卡一样。此功能使得 StoreFront 能够使用范围更广的身份验证选项，例如安全声明标记语言 (SAML) 声明。SAML 常用于替代 Internet 上的传统 Windows 用户帐户。

注意：

要使用 SAML 身份验证，请在 VDA 上正确配置 FAS。

从 CU3 开始，Linux VDA 会使用短连接与 FAS 服务器传输数据。

下图显示了 FAS 与 Microsoft 证书颁发机构的集成，并为 StoreFront 和 VDA 提供支持服务。



当用户请求访问 Citrix 环境时，可信 StoreFront 服务器会联系 FAS。FAS 将授予一个票据，允许单个 Citrix Virtual Apps 或 Citrix Virtual Desktops 会话使用该会话的证书进行身份验证。当 VDA 需要对用户进行身份验证时，它会连接到 FAS 并找回票据。仅 FAS 有权访问用户证书的私钥。VDA 必须向 FAS 发送需要执行的每个签名和解密操作以及证书。

## 要求

在 Windows Server 2008 R2 及更高版本上支持 FAS。

- 我们建议在不包含其他 Citrix 组件的服务器上安装 FAS。
- 必须确保 Windows Server 访问注册颁发机构证书和私钥的安全，才能自动为域用户颁发证书以及颁发用于访问这些用户证书和私钥的证书。

在 Citrix Virtual Apps 或 Citrix Virtual Desktops 站点中：

- Delivery Controller 的版本必须至少为 7.9。
- StoreFront 服务器的版本必须至少为 3.6（随 XenApp 和 XenDesktop 7.9 ISO 提供的版本）。
- Linux VDA 的版本必须至少为 7.18。在以通常方式创建计算机目录之前，验证已向 VDA 正确应用联合身份验证服务组策略配置。有关详细信息，请参阅本文中的配置组策略部分。

参考：

- Active Directory 证书服务  
<https://social.technet.microsoft.com/wiki/contents/articles/1137.active-directory-certificate-services-ad-cs-introduction.aspx>
- 配置 Windows 的登录证书  
<http://support.citrix.com/article/CTX206156>
- 安装联合身份验证服务  
[联合身份验证服务](#)

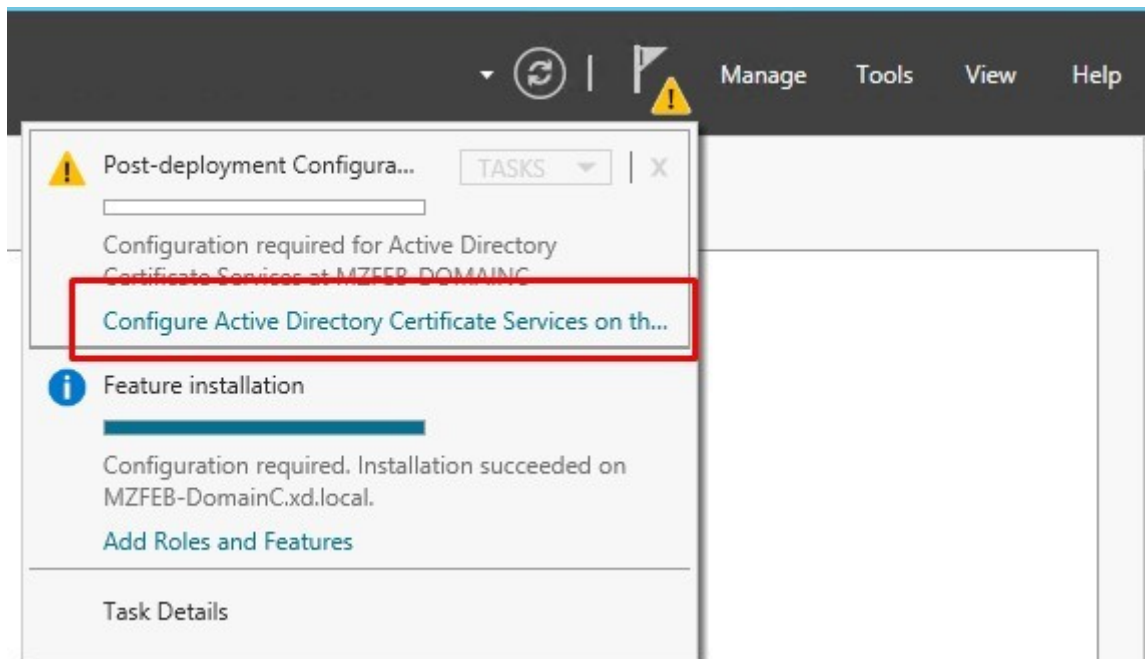
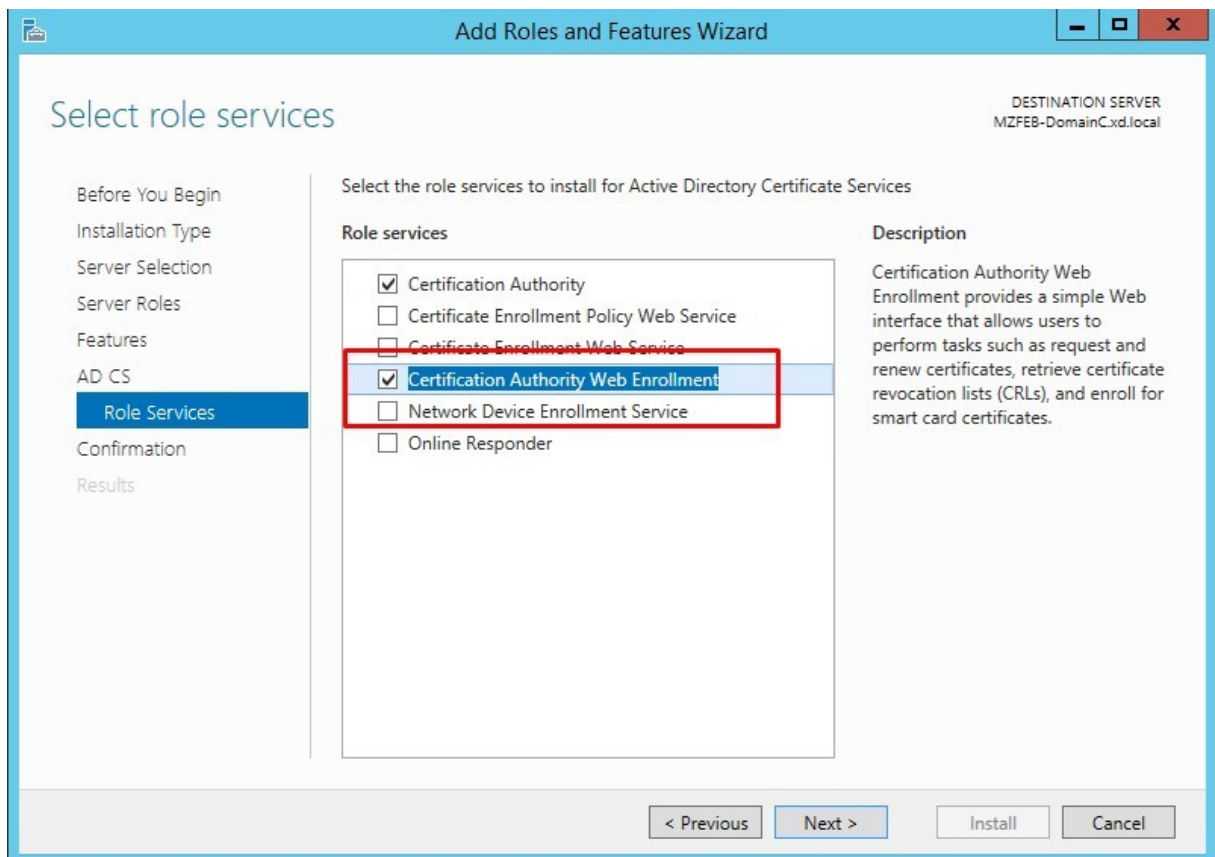
### 配置 **Windows** 进行证书登录

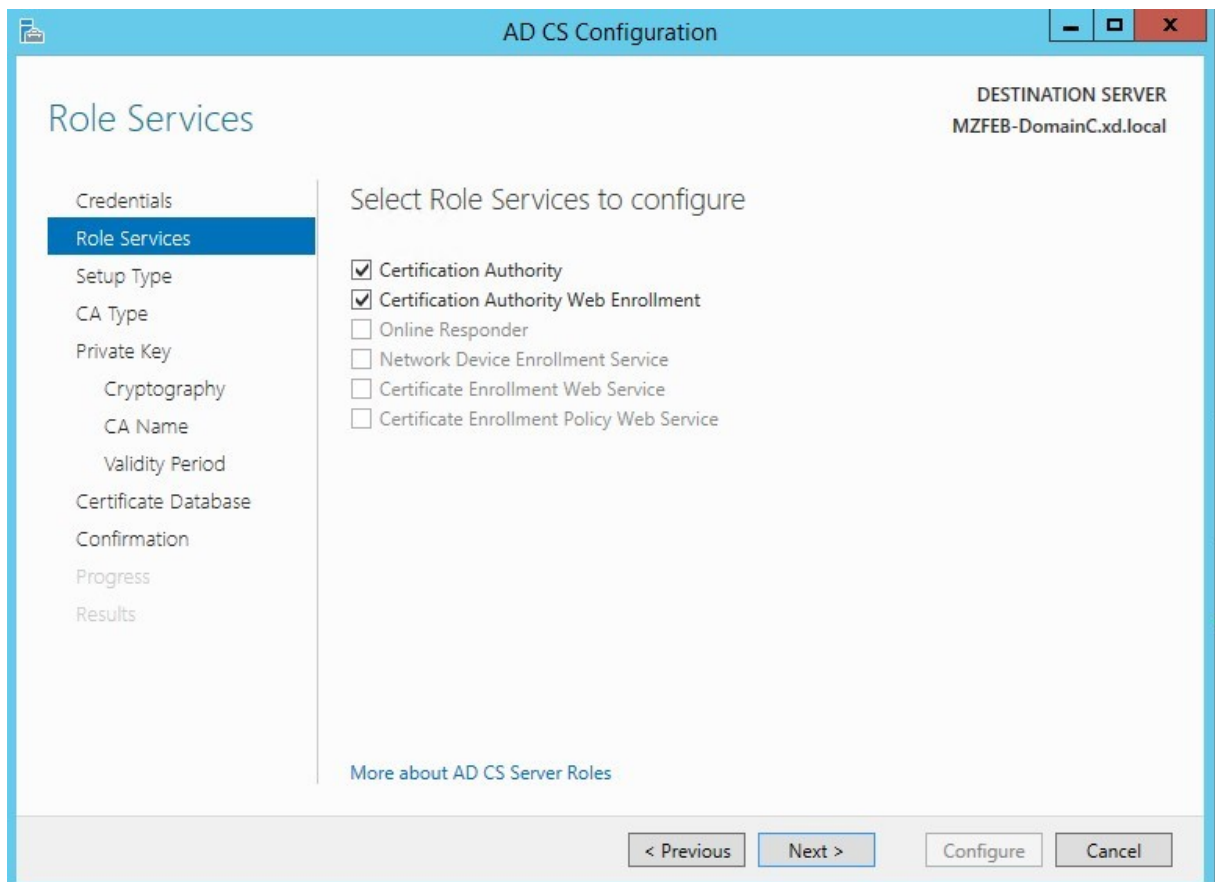
有关配置 Windows 进行证书登录的信息,请打开知识中心文章 [CTX206156](#) 以下载并阅读 **Smart\_card\_config\_Citrix\_Env.pdf** 文件 (下文称为“PDF 文件”)。请根据该 PDF 文件执行以下步骤,同时注意每个步骤中列出的差异或补充内容。应特别注意执行操作的目标计算机,例如 AD、Delivery Controller 或 StoreFront。

### 设置 **Windows** 域 (在 **AD** 上)

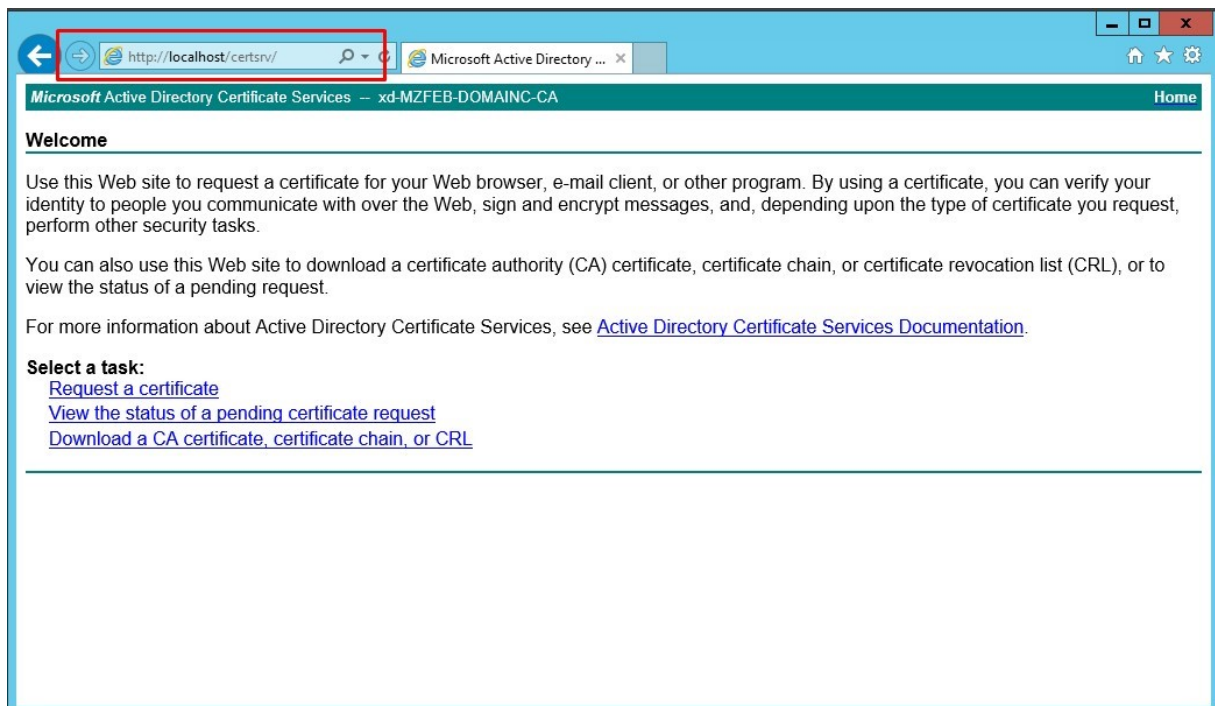
安装域控制器角色 请参阅该 PDF 文件中的 **Installing Domain Controller Roles** (安装域控制器角色) 部分。

在安装 Active Directory 证书服务期间,请务必选择以下选项:





打开 <http://localhost/certsrv/> 以检查是否显示以下欢迎页面。如果显示，则已成功安装 Active Directory 证书服务。



准备证书颁发机构以使用智能卡 无补充内容。请参阅该 PDF 文件中的 **Preparing the Certificate Authority for Smart card usage**（准备证书颁发机构以使用智能卡）部分。

颁发域控制器证书 无补充内容。请参阅该 PDF 文件中的 **Issuing a Domain Controller Certificate**（颁发域控制器证书）部分。

为 **Microsoft IIS** 配置 **HTTPS**（在 **StoreFront** 上）

在 **Microsoft IIS** 中配置 **HTTPS** 无补充内容。请参阅该 PDF 文件中的 **Configuring HTTPS on Microsoft IIS**（在 Microsoft IIS 中配置 HTTPS）部分。

未加入域的计算机

请参阅该 PDF 文件中的 **Non-Domain Joined Computers**（未加入域的计算机）部分。

从 **Microsoft CA** 检索 **CA** 证书（在 **AD** 上） 无补充内容。请参阅该 PDF 文件中的 **Retrieving the CA Certificate from the Microsoft CA**（从 Microsoft CA 中获取 CA 证书）部分。

在 **Windows** 上安装可信的 **CA** 证书 无补充内容。请参阅该 PDF 文件中的 **Installing the Trusted CA Certificate on Windows**（在 Windows 上安装可信的 CA 证书）部分。

配置 **Citrix StoreFront**（在 **StoreFront** 上）

创建应用商店 请参阅该 PDF 文件中的 **Creating the Store**（创建应用商店）部分。

完成前面的 IIS 配置后，常用应用商店的基本 URL 强制设置为 <https://> 而非 <http://>。由于 FAS 不与智能卡共享应用商店，因此 FAS 需要新的应用商店。Linux VDA FAS 与任何 StoreFront 身份验证方法都兼容。例如，FAS 应用商店可以配置为使用密码或 SAML，但不能同时使用两者。选择了 SAML 时，StoreFront 的 URL 将自动重定向到 IdP，且忽略密码身份验证方法。



Create Store

## StoreFront

- ✓ Getting Started
- Store Name**
- Delivery Controllers
- Remote Access
- Authentication Methods
- XenApp Services URL
- Summary

### Store name and access

Enter a name that helps users identify the store. The store name appears in Citrix Receiver as part of the user's account.

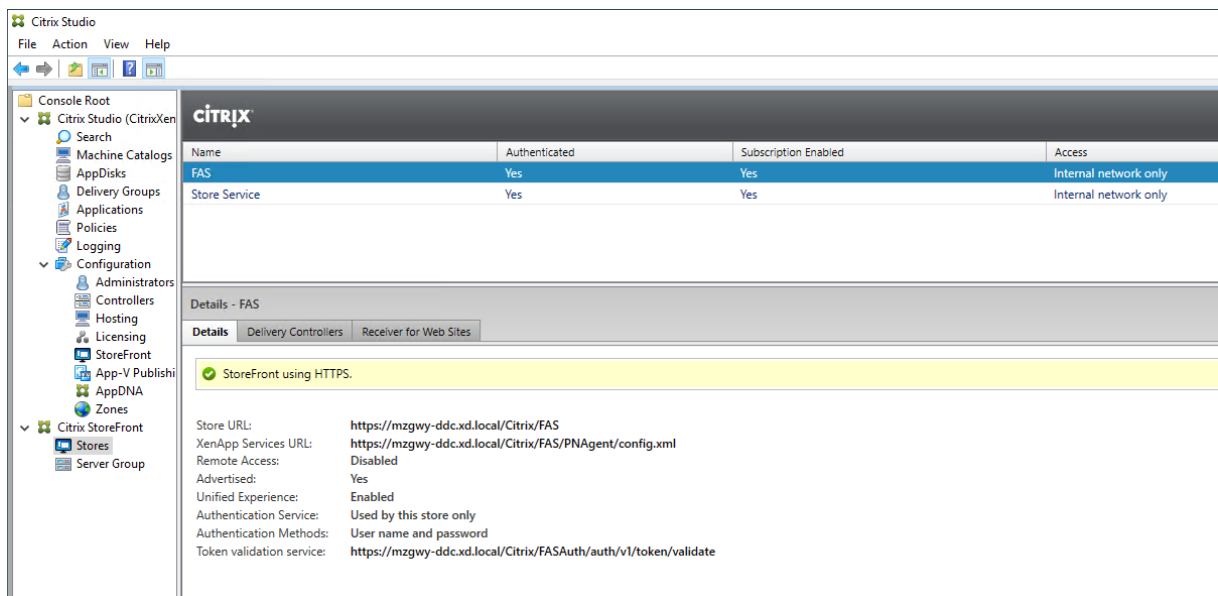
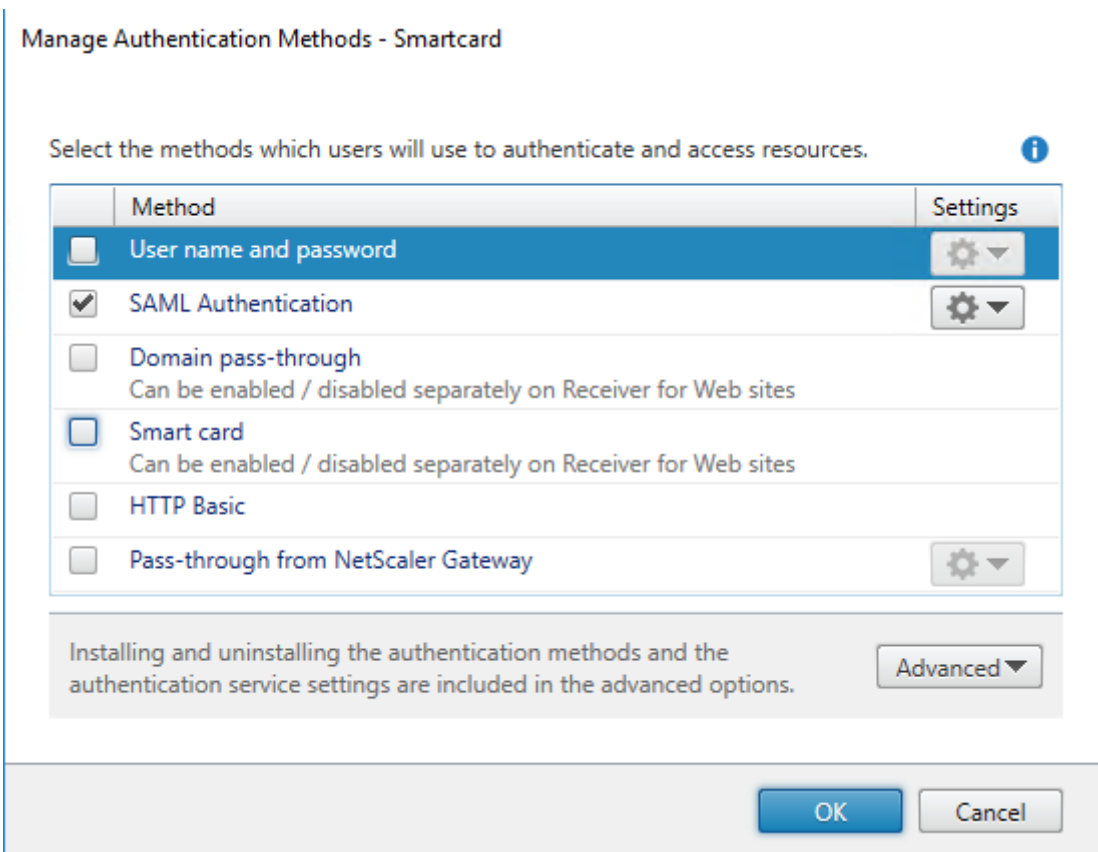
**i** Store name and access type cannot be changed, once the store is created.

Store Name:

Allow only unauthenticated (anonymous) users to access this store  
Unauthenticated users can access the store without presenting credentials.

### Receiver for Web Site Settings

Set this Receiver for Web site as IIS default  
When this is checked, the Receiver for Web site created with the store will be set as the default IIS website. This setting will override any previous defaults configured for the IIS sites.



启动 Internet Explorer 并打开 FAS 应用商店的 URL (例如 <https://mzgwgy-ddc.xd.local/Citrix/FASWeb>)。

注意：FAS 应用商店的 URL 必须附加 **Web**。

## 安装和设置 **FAS**

安装和设置过程包括以下步骤：

1. 安装联合身份验证服务
2. 在 StoreFront 服务器上启用“联合身份验证服务”插件
3. 配置组策略
4. 使用“联合身份验证服务”管理控制台执行以下操作：(a) 部署所提供的模板，(b) 设置证书颁发机构，以及 (c) 授权联合身份验证服务使用您的证书颁发机构
5. 配置用户规则

有关每个步骤的说明，请参阅[联合身份验证服务](#)。请注意每个步骤中的以下差异或补充内容。应特别注意执行操作的目标计算机，例如 AD、Delivery Controller、StoreFront 或 FAS 服务器。

安装联合身份验证服务（在 **FAS** 服务器上）

出于安全考虑，请将 FAS 安装在专用服务器上，并且此服务器应受到与域控制器或证书颁发机构类似的保护。

在 **StoreFront** 应用商店上启用联合身份验证服务插件（在 **StoreFront** 上）

请确保以下命令使用在配置 StoreFront 时键入的同一 FAS 应用商店名称。例如，在此示例中，FAS 是应用商店名称：

```
$StoreVirtualPath = "/Citrix/FAS"
```

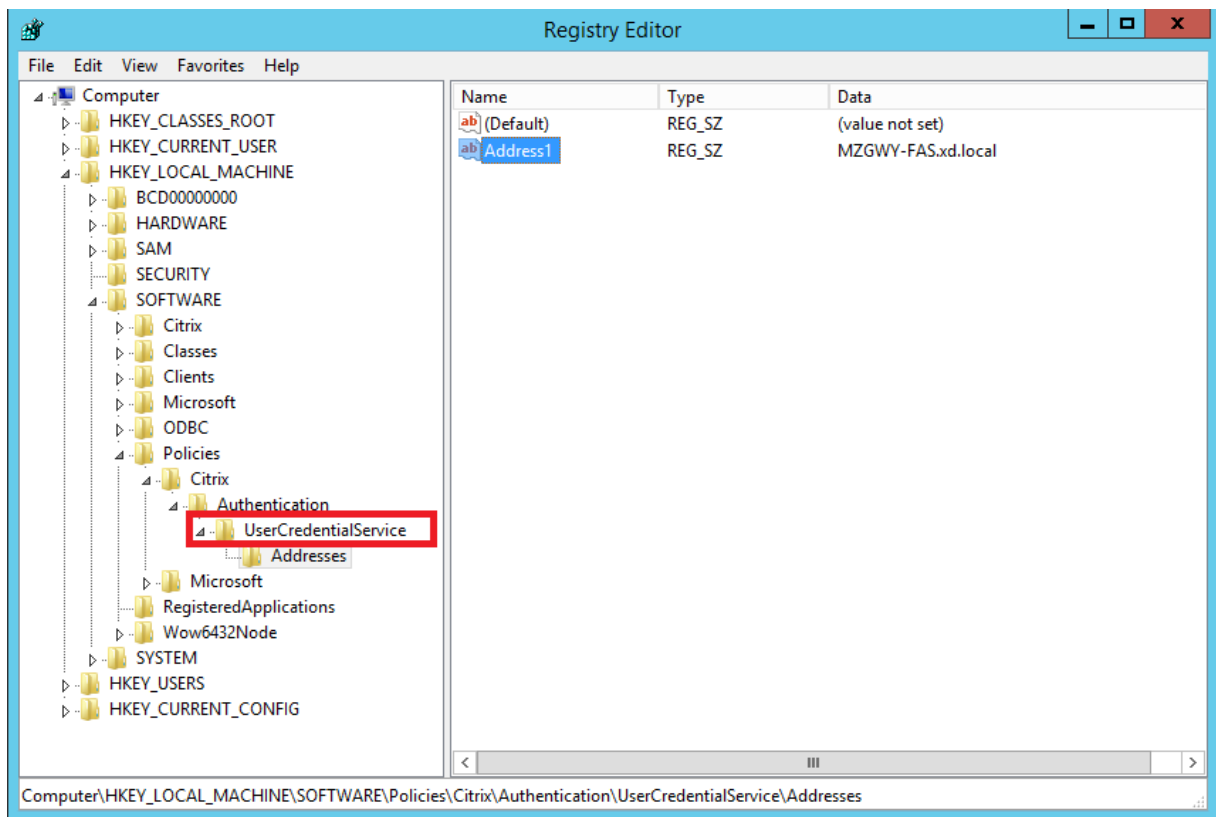
配置 **Delivery Controller**（在 **Delivery Controller** 上）

要使用联合身份验证服务，请配置 Delivery Controller 以信任可与其连接的 StoreFront 服务器：运行 **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** PowerShell cmdlet。有时，您可能需要先运行 `Add-PSSnapin citrix.*`。

配置组策略（在 **FAS** 服务器上 and **AD** 上）

您必须是管理员，才能执行此部分中的步骤 1-7。步骤 1 必须在 FAS 服务器上完成，步骤 2-7 必须在 AD 上完成。

完成步骤 1-7 后，在 FAS 服务器的注册表编辑器中检查以确认是否设置了 FAS 策略。



启用会话中证书支持 Linux VDA 不支持会话中证书。

使用联合身份验证服务管理控制台（在 **FAS** 服务器上）

无补充内容。请参阅[联合身份验证服务](#)一文。

部署证书模板（在 **FAS** 服务器上）

无补充内容。请参阅[联合身份验证服务](#)一文。

设置 **Active Directory** 证书服务（在 **FAS** 服务器上）

无补充内容。请参阅[联合身份验证服务](#)一文。

授权联合身份验证服务（在 **FAS** 服务器上）

无补充内容。请参阅[联合身份验证服务](#)一文。

配置用户规则（在 **FAS** 服务器上）

无补充内容。请参阅[联合身份验证服务](#)一文。

有关详细信息，另请参阅[联合身份验证服务](#)一文的安全注意事项部分中的委派注册代理和访问控制列表配置部分。

联合身份验证服务 **ADFS** 部署

有关如何为联合身份验证服务部署 ADFS IdP 的信息，请参阅[联合身份验证服务 ADFS 部署](#)。

## 配置 Linux VDA

设置 **FAS** 服务器

如果是全新安装 Linux VDA，要使用 FAS，请在执行 `ctxinstall.sh` 或 `ctxsetup.sh` 过程中看到要求提供 `CTX_XDL_FAS_LIST` 时，键入每个 FAS 服务器的 FQDN。由于 Linux VDA 不支持 AD 组策略，您可以改为提供以分号分隔的 FAS 服务器的列表。如果删除了任何服务器地址，则使用 **<none>** 文本字符串填充空白处，并使服务器地址的顺序保持不变。

如果是升级现有的 Linux VDA 安装，可以重新运行 `ctxsetup.sh` 来设置 FAS 服务器。或者，也可以运行以下命令来设置 FAS 服务器，并重新启动 `ctxvda` 服务以使设置生效。

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
VirtualDesktopAgent\Authentication\UserCredentialService" -t "REG_SZ"
" -v "Addresses" -d "<Your-FAS-Server-List>" --force
2
3 service ctxvda restart
4 <!--NeedCopy-->
```

要通过 `ctxreg` 更新 FAS 服务器，请运行以下命令：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
VirtualDesktopAgent\Authentication\UserCredentialService" -v "
Addresses" -d "<Your-FAS-Server-List>"
2
3 service ctxvda restart
4 <!--NeedCopy-->
```

安装根 **CA** 证书

要验证用户证书，请在 VDA 上安装根 CA 证书。从前面的从 **Microsoft CA** 中获取 **CA** 证书（在 **AD** 中）步骤中获取 AD 根证书，也可以从根 CA 服务器 <http://CA-SERVER/certsrv> 下载 DER 格式的该证书。

注意：

以下命令也适用于配置中间证书。

运行类似如下的命令将 DER 文件（.crt、.cer、.der）转换为 PEM：

```
1 sudo openssl x509 -inform der -in root.cer -out root.pem
2 <!--NeedCopy-->
```

然后，运行类似如下的命令将根 CA 证书安装到 openssl 目录：

```
1 sudo cp root.pem /etc/pki/CA/certs/
2 <!--NeedCopy-->
```

注意：

请勿将根 CA 证书置于 **/root** 路径下。否则，FAS 无权读取根 CA 证书。

## 配置 FAS

运行以下脚本以配置 FAS：

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

注意：

上述脚本仅处理使用单个根 CA 证书的场景。

如果您的环境中存在中间证书，请将中间证书的路径添加到 `/etc/krb5.conf`，如下所示：

```
[realms]
EXAMPLE.COM = {
...
pkinit_anchors = FILE:/etc/pki/CA/certs/root.pem
pkinit_pool = FILE:/etc/pki/CA/certs/intermediate.pem
...
}
```

添加两个环境变量，以便 `ctxfascfg.sh` 可以在静默模式下运行：

- **CTX\_FAS\_ADINTEGRATIONWAY=winbind|sssd|centrify** -表示 Active Directory 集成方法，相当于在指定 `CTX_EASYINSTALL_ADINTEGRATIONWAY` 时使用 `CTX_EASYINSTALL_ADINTEGRATIONWAY`。如果未指定 `CTX_EASYINSTALL_ADINTEGRATIONWAY`，`CTX_FAS_ADINTEGRATIONWAY` 将使用自己的值设置。
- **CTX\_FAS\_ROOT\_CA\_PATH=<root\_CA\_certificate>** -指定根 CA 证书的完整路径。

选择正确的 Active Directory 集成方法，然后键入正确的根 CA 证书路径（例如 `/etc/pki/CA/certs/root.pem`）。

脚本随后安装 `krb5-pkinit` 和 `pam_krb5` 软件包，并设置相关的配置文件。

### 限制

- FAS 支持有限的平台和 AD 集成方法，请参阅下表：

|                      | Winbind | SSSD | Centrify |
|----------------------|---------|------|----------|
| RHEL 7.7 /CentOS 7.7 | √       | √    | √        |
| Ubuntu 18.04         | √       | ×    | √        |
| Ubuntu 16.04         | √       | ×    | √        |
| SLES 12.3            | √       | ×    | √        |

- FAS 尚不支持锁屏界面。如果在会话中单击锁定按钮，则无法使用 FAS 重新登录该会话。
- 此版本仅支持[联合身份验证服务体系结构概述](#)一文中概括的常见 FAS 部署，不包括 **Windows 10 Azure AD** 联接。

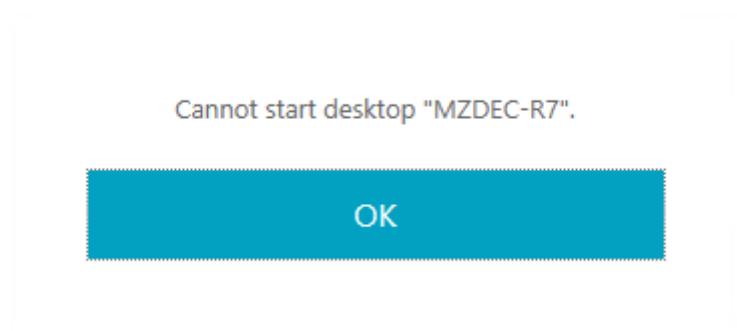
### 故障排除

在对 FAS 进行故障排除之前，请确保已安装并正确配置 Linux VDA，以便可以使用密码身份验证在常用应用商店中成功启动非 FAS 会话。

如果非 FAS 会话正常运行，请将登录类别的 HDX 日志级别设置为“VERBOSE”，将 VDA 日志级别设置为“TRACE”。有关如何为 Linux VDA 启用跟踪日志记录的信息，请参阅知识中心文章 [CTX220130](#)。

### FAS 服务器配置错误

从 FAS 应用商店启动会话失败。有关示例，请参见以下屏幕截图：



检查 `/var/log/xdl/hdx.log` 并查找类似如下内容的错误日志：

```
1 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: query2fas: failed
 to retrieve data: No such file or directory.
2
3 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin:
 sayhello2fas_internal: Failed to query.
4
5 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin:
 sayhello2fas_convertcredential: exit.
6
7 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: LoginFasValidate:
 Failed to start FAS.
8
9 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: receive_data:
 LoginFASValidate - parameters check error.
10
11 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: receive_data: Exit
 FAILURE
12
13 2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: main: EXITING
 login process..., FAILURE
14 <!--NeedCopy-->
```

**解决方案** 运行以下命令以确认 Citrix 注册表值“HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent\Auther”是否设置为 <Your-FAS-Server-List>。

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
2 <!--NeedCopy-->
```

如果现有设置不正确，请按照前面的[设置 FAS 服务器](#)步骤操作以重新设置。

根 **CA** 证书配置错误

从 FAS 应用商店启动会话失败。将显示一个灰色窗口，并且几秒钟后消失。



检查 `/var/log/xdl/hdx.log` 并查找类似如下内容的错误日志：



```
1 2018-03-27 10:15:52.227 <P9099:S3> citrix-ctxlogin: validate_user:
 pam_authenticate err,can retry for user user1@CTXFAS.LAB
2
3 2018-03-27 10:15:52.228 <P9099:S3> citrix-ctxlogin: logout_user:
 closing session and pam transaction
4
5 2018-03-27 10:15:52.228 <P9099:S3> citrix-ctxlogin: validate_user: Exit
 (user=user1@CTXFAS.LAB)=INVALID_PASSWORD
6
7 2018-03-27 10:15:52.228 <P9099:S3> citrix-ctxlogin: LoginBoxValidate:
 failed validation of user 'user1@CTXFAS.LAB', INVALID_PASSWORD
8
9 2018-03-27 10:15:52.228 <P9099:S3> citrix-ctxlogin: Audit_login_failure
 : Not yet implemented
10 <!--NeedCopy-->
```

解决方案 确认是否在 /etc/krb5.conf 中正确设置了根 CA 证书的完整路径。完整路径如下所示：

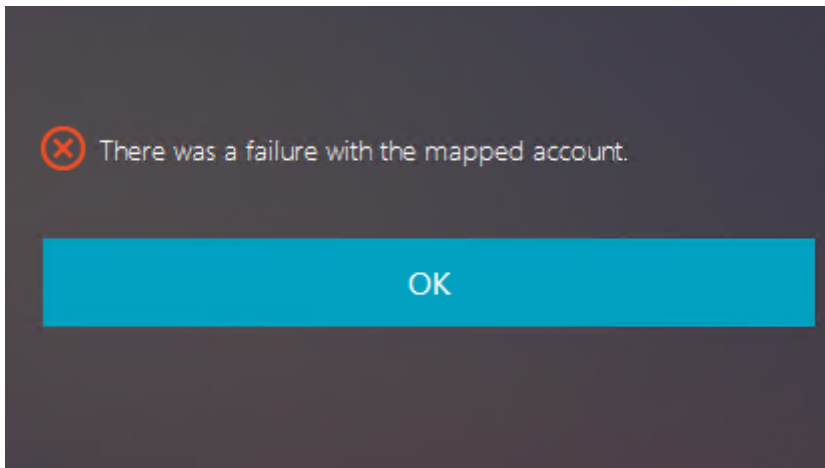
```
1 [realms]
2
3 EXAMPLE.COM = {
4
5
6
7
8 pkinit_anchors = FILE:/etc/pki/CA/certs/root.pem
9
10
11
12 }
13
14 <!--NeedCopy-->
```

如果现有设置不正确，请按照前面的[安装根 CA 证书](#)步骤操作以重新设置。

或者，检查根 CA 证书是否有效。

重影帐户映射错误

FAS 配置了 SAML 身份验证。ADFS 用户在 ADFS 登录页面上输入用户名和密码后，可能会出现以下错误。

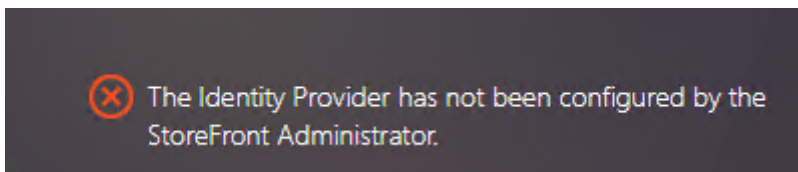


此错误表明已成功验证 ADFS 用户，但在 AD 上没有配置任何重影用户。

**解决方案** 在 AD 上设置重影帐户。

#### 未配置 ADFS

尝试登录 FAS 应用商店过程中出现以下错误：



这是因为 FAS 应用商店配置为使用 SAML 身份验证，但缺少 ADFS 部署。

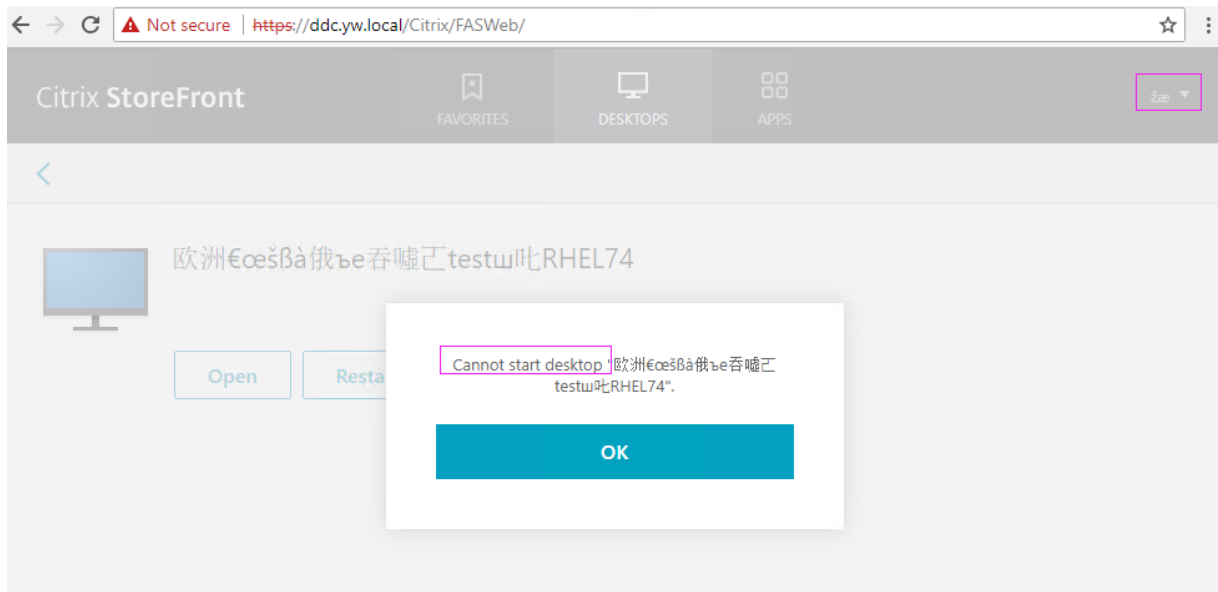
**解决方案** 为联合身份验证服务部署 ADFS IdP。有关详细信息，请参阅[联合身份验证服务 ADFS 部署](#)。

#### 相关信息

- 通用 FAS 部署在[联合身份验证服务体系结构概述](#)一文中加以概括。
- [联合身份验证服务高级配置](#)一章中引入了“操作方法”文章。

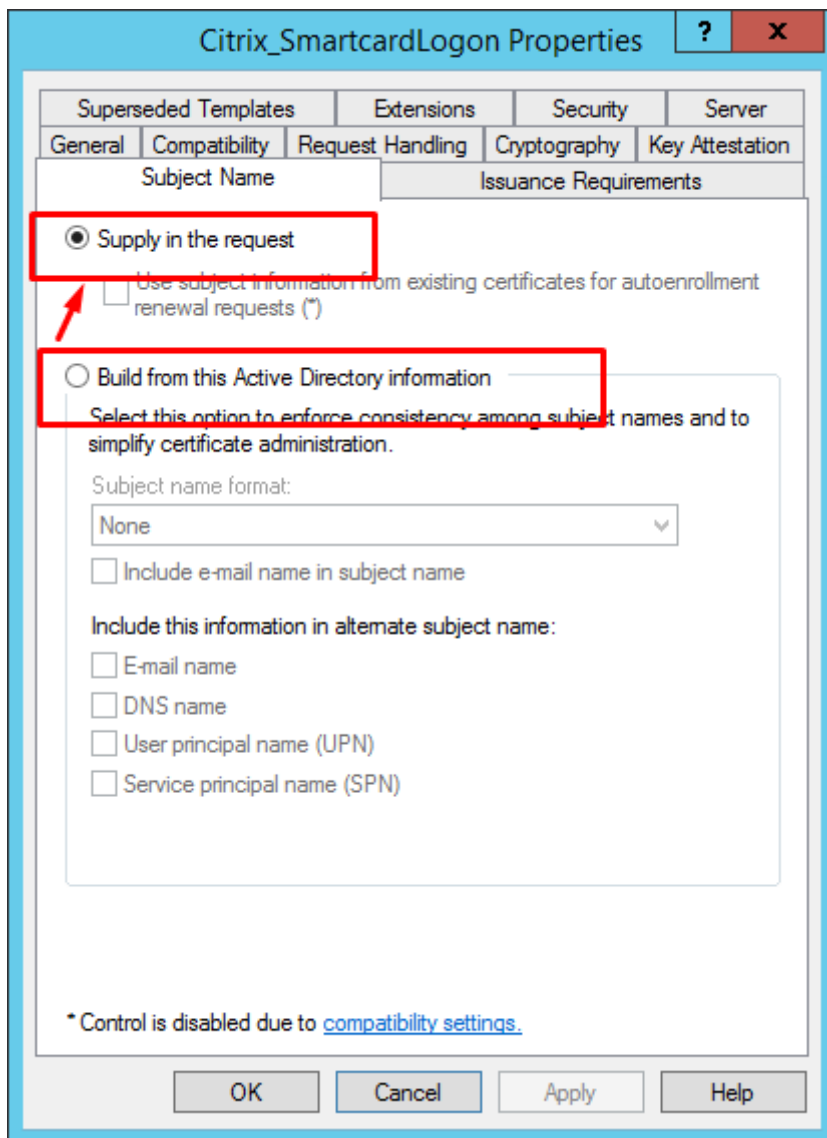
#### 已知问题

如果正在使用 FAS，则尝试启动包含非英语字符的已发布桌面或应用程序会话时，可能会失败。



#### 解决方法

在 CA 工具中右键单击 **Manage Templates**（管理模板）以将 **Citrix\_SmartcardLogon** 模板从 **Build from this Active Directory information**（基于此 Active Directory 信息构建）更改为 **Supply in the request**（在请求中提供）：





© 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).