# Linux Virtual Delivery Agent 2209

# Contents



# Linux Virtual Delivery Agent 2209

October 31, 2022

> 重要：
>
> 生命周期里程碑中介绍了当前版本 (CR) 和长期服务版本 (LTSR) 的产品生命周期策略。

Linux Virtual Delivery Agent (VDA) 支持在任何位置从安装了 Citrix Workspace 应用程序的任何设备访问 Linux 虚拟应用程序和桌面。

您可以根据受支持的 Linux 发行版交付虚拟应用程序和桌面。在您的 Linux 虚拟机上安装 VDA 软件，配置 Delivery Controller，然后使用 Citrix Studio 向用户提供这些应用程序和桌面。

## 新增功能

October 31, 2022

### 2209 中的新增功能

Linux VDA 2209 版包括以下新增功能和增强功能：

#### 支持 RHEL 8.6、Rocky Linux 8.6 和 Ubuntu 22.04

我们添加了 RHEL 8.6、Rocky Linux 8.6 和 Ubuntu 22.04 作为支持的发行版。

#### 加入了 SSSD 和 PBIS 的 Ubuntu 和 SUSE VDA 支持联合身份验证

我们已将联合身份验证服务 (FAS) 的支持扩展到以下类型的 VDA：

- 使用 SSSD 和 PBIS 加入域的 Ubuntu VDA
- 使用 SSSD 加入域的 SUSE VDA。

现在，您可以使用 FAS 对登录这些 VDA 的用户进行身份验证。有关详细信息，请参阅联合身份验证服务。

#### 按会话用户划分的自定义桌面环境

会话用户现在可以自定义其桌面环境。必须提前在 VDA 上安装桌面环境，才能启用此功能。有关详细信息，请参阅按会话用户划分的自定义桌面环境。

#### GPG 签名

我们已经使用 GPG 对 Linux VDA 软件包进行了签名，因此，您可以使用公钥验证 Linux VDA 软件包的完整性。

要获取公钥，请执行以下操作：

1. 转至 Citrix Virtual Apps and Desktops 下载页面。
2. 展开适当版本的 Citrix Virtual Apps and Desktops。
3. 单击组件查找并下载公钥。

要使用公钥验证 Linux VDA 软件包的完整性，请执行以下操作：

- 对于 RPM 软件包，请将公钥导入到 RPM 数据库中并运行以下命令：

```
rpmkeys --import <path to the public key>
rpm --checksig --verbose <path to the Linux VDA package>
<!--NeedCopy-->
```

- 对于 DEB 软件包，请将公钥导入到 DEB 数据库中并运行以下命令：

```
sudo apt-get install dpkg-sig
gpg --import <path to the public key>
dpkg-sig --verify <path to the Linux VDA package>
<!--NeedCopy-->
```

#### 早期版本中的新增功能

有关在 1912 LTSR 到 2207 CR 之后提供的发行版中包含的新增功能，请参阅新增功能历史记录。

## 已修复的问题

October 31, 2022

自 Linux Virtual Delivery Agent 2207 起，以下问题已修复：

- 用户启动 Linux 虚拟应用程序或桌面会话后，**PATH** 环境变量可能不包含 **/usr/local/bin** 路径。[CVADHELP-20683]
- **ctxgfx** 进程中出现的 **segfault** 错误可能会导致 Linux 虚拟应用程序和桌面意外退出。[CVADHELP-18646]

## 已知问题

July 14, 2023

在本版本中确定了以下问题：

- 当您重新启动 Cloud Connector 或 Delivery Controller 时，Linux VDA 可能会取消注册。[CVADHELP-21256]
- 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。
- 在 GNOME 桌面会话中，尝试更改键盘布局可能会失败。[CVADHELP-15639]
- 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]
- 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]
- 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]
- 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：

```
klist -li 0x3e4 purge
<!--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

November 4, 2022

Linux Virtual Delivery Agent 2209（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

October 31, 2022

本文中的声明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 | 已在其中宣布弃用的版本 | 已在其中删除的版本 |
| --- | --- | --- |
| 支持 Debian 10.9 | 2206 | 2210 |
| 支持 SUSE 15.2 | 2206 | 2209 |
| 支持 RHEL 8.2 | 2206 | 2209 |

| 项目 | 已在其中宣布弃用的版本 | 已在其中删除的版本 |
| --- | --- | --- |
| 支持 RHEL 8.1、RHEL 8.3 | 2203 | 2206 |
| 支持 RHEL 7.8、CentOS 7.8 | 2203 | 2204 |
| 支持 CentOS 8.x | 2110 | 2201 |
| 支持 SUSE 12.5 | 2109 | 2204 |
| 支持 Ubuntu 16.04 | 2109 | 2203 |
| 支持 RHEL 7.7、CentOS 7.7 | 2006 | 2009 |
| 支持 SUSE 12.3 | 2006 | 2006 |
| 支持 RHEL 6.10、CentOS 6.10 | 2003 | 2003 |
| 支持 RHEL 6.9、CentOS 6.9 | 1909 | 1909 |
| 支持 RHEL 7.5、CentOS 7.5 | 1903 | 1903 |
| 支持 RHEL 7.4、CentOS 7.4 | 1811 | 1811 |
| 支持 RHEL 6.8、CentOS 6.8 | 1811 | 1811 |
| 支持 RHEL 7.3、CentOS 7.3 | 7.18 | 7.18 |
| 支持 RHEL 6.6、CentOS 6.6 | 7.16 | 7.16 |
| SUSE 11.4 | 7.16 | 7.16 |

## 系统要求

October 31, 2022

Linux VDA 的当前版本与 Citrix Virtual Apps and Desktops 保持一致。它还向后兼容尚未结束其生命周期的 Citrix Virtual Apps and Desktops 的早期版本。要获取有关 Citrix 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。所有 Delivery Controller 场都能为 Windows 和 Linux 桌面提供代理服务。

本文档中未涉及的组件（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。

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 发行版

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。

- Amazon Linux
  - Amazon Linux 2
- CentOS Linux
  - CentOS 7.9
- Debian Linux
  - Debian 11.3
  - Debian 10.9
- Red Hat Enterprise Linux
  - 工作站 8.6
  - Workstation 8.4
  - 工作站 7.9
  - Server 8.6
  - Server 8.4
  - Server 7.9
- Rocky Linux 8.6
- SUSE Linux Enterprise：
  - Server 15 Service Pack 3
- Ubuntu Linux
  - Ubuntu Desktop 22.04
  - Ubuntu Server 22.04
  - Ubuntu Desktop 20.04
  - Ubuntu Server 20.04
  - Ubuntu Desktop 18.04
  - Ubuntu Server 18.04
  - Ubuntu Live Server 18.04

> 注意：
>
> CentOS 项目将关注的焦点切换到 CentOS Stream。作为 RHEL 8 的重建，CentOS Linux 8 将于 2021 年底终止提供。之后，CentOS Stream 将继续用作 Red Hat Enterprise Linux 的上游(开发)分支。有关详细信息，请参阅 https://www.redhat.com/en/blog/centos-stream-building-innovative-future-enterprise-linux。

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 | 支持的桌面 |
| --- | --- | --- |
| Amazon Linux 2 | 1.20 | MATE、GNOME、GNOME Classic |
| Debian 11.3、Debian 10.9 | 1.20 | MATE、GNOME、GNOME Classic、KDE |
| RHEL 8.6、RHEL 8.4 | 1.20 | MATE、GNOME、GNOME Classic |
| RHEL 7.9、CentOS 7.9 | 1.20 | MATE、GNOME、GNOME Classic、KDE |
| Rocky Linux 8.6 | 1.20 | MATE、GNOME、GNOME Classic、KDE |
| SUSE 15.3 | 1.20 | MATE、GNOME、GNOME Classic |
| Ubuntu 22.04 | 1.21 | MATE、GNOME、GNOME Classic、KDE |
| Ubuntu 20.04 | 1.20 | MATE、GNOME、GNOME Classic、KDE |
| Ubuntu 18.04 | 1.19 | MATE、GNOME、GNOME Classic、KDE |

> 提示：
>
> 请勿在 Ubuntu 上使用 `HWE kernel` 或 `HWE Xorg`。
>
> 必须至少安装一个桌面。可以通过 ctxinstall.sh 或 ctxsetup.sh 脚本指定要在会话中使用的 GNOME 或 MATE 桌面环境。
> 您的用户名格式必须符合当前显示管理器的 `systemd` 语法规则。有关 `systemd` 用户名语法的详细信息，请参阅用户/组名称语法。

支持的主机平台和虚拟化环境

- 裸机服务器
- Amazon Web Services (AWS)
- Citrix Hypervisor

- Google 云端平台 (GCP)
- 基于内核的虚拟机 (KVM)
- Microsoft Azure
- Microsoft Hyper-V
- VMware vSphere Hypervisor
- Nutanix AHV

> 注意：
>
> 在所有情况下，受支持的处理器架构均为 x86-64。
>
> 自 Citrix Virtual Apps and Desktops 7 2003 到 2112，只有 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）支持在 Microsoft Azure、AWS 和 GCP 上托管 Linux VDA。自 2203 版起，您可以在这些公有云上为 Citrix DaaS 和 Citrix Virtual Apps and Desktops 托管 Linux VDA。要将这些公有云主机连接添加到 Citrix Virtual Apps and Desktops 部署，您需要混合权限许可证。有关混合权限许可证的信息，请参阅使用混合权限转换和升级换购 (TTU)。

### **Active Directory** 集成软件包

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

| | Winbind | SSSD | Centrify | PBIS | Quest |
|---|---|---|---|---|---|
| Amazon Linux 2 | 是 | 是 | 是 | 是 | 否 |
| Debian 11.3、Debian 10.9 | 是 | 是 | 是 | 是 | 否 |
| RHEL 8.6、RHEL 8.4 | 是 | 是 | 是 | 是 | 否 |
| RHEL 7.9、CentOS 7.9 | 是 | 是 | 是 | 是 | 是（Quest v4.1 及更高版本） |
| Rocky Linux 8.6 | 是 | 是 | 否 | 否 | 否 |
| SUSE 15.3 | 是 | 是 | 是 | 是 | 否 |
| Ubuntu 22.04、Ubuntu 20.04、Ubuntu 18.04 | 是 | 是 | 是 | 是 | 是（Quest v4.1 及更高版本） |

### HDX 3D Pro

借助 Citrix Virtual Apps and Desktops 的 HDX 3D Pro，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兼容：

- Citrix Hypervisor
- VMware vSphere Hypervisor
- Nutanix AHV
- Microsoft Azure
- Amazon Web Services (AWS)
- Google 云端平台 (GCP)

> 注意：
>
> 虚拟机管理程序与某些 Linux 发行版兼容。
> 要对 Amazon Linux 2 使用 HDX 3D Pro，我们建议您安装 NVIDIA 驱动程序 470。

#### 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。目前，Linux VDA 最高支持 vGPU 13。有关详细信息，请参阅 NVIDIA 虚拟 GPU 软件支持的 GPU。

## 安装概述

October 31, 2022

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
- 在 Citrix DaaS Standard for Azure（以前称为“适用于 Azure 的 Citrix Virtual Apps and Desktops Standard”）中创建已加入域和未加入域的 Linux VDA
- 使用 Citrix Provisioning 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）

November 4, 2022

> 重要：
>
> - 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。
> - 必须使用 Machine Creation Services (MCS)，才能创建未加入域的 VDA。有关详细信息，请参阅使用 Machine Creation Services (MCS) 创建 Linux VM。
> - 要了解适用于未加入域的 VDA 的功能，请转到未加入域的 VDA。

### 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：

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

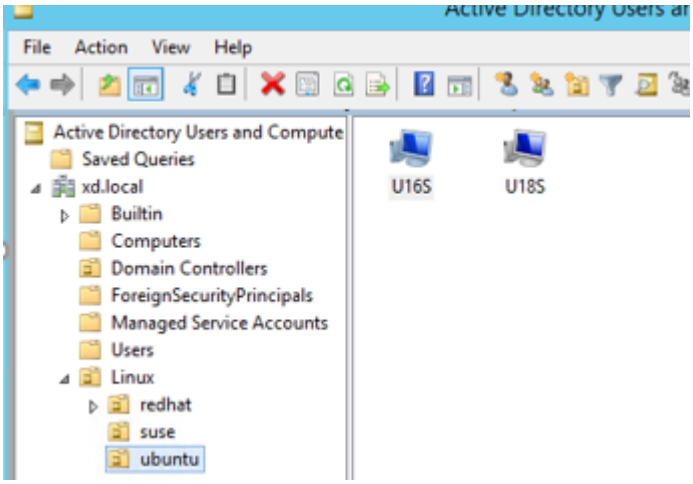
此问题是 Centrify 及其配置独有的。要解决此问题，请执行以下操作：

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。

- 要将 VDA 连接到特定 OU，请执行以下操作：

  1. 确保域控制器上存在特定的 OU。

     有关示例 OU，请参阅下面的屏幕截图。

  2. 在 VDA 上创建 /tmp/ctxinstall.conf 文件。
  3. 将 ou=<your ou> 行添加到 /tmp/ctxinstall.conf 文件中。

     OU 值因 AD 方法的不同而异。请参见下表。

| 操作系统 | Winbind | SSSD | Centrify | PBIS |
| --- | --- | --- | --- | --- |
| Amazon Linux 2 | `ou="Linux/amazon"` | `ou="Linux/amazon"` | `ou="XD.LOCAL/Linux/amazon"` | `ou="Linux/amazon"` |
| Debian | `ou="Linux/debian"` | `ou="Linux/debian"` | `ou="XD.LOCAL/Linux/debian"` | `ou="Linux/debian"` |

| 操作系统 | Winbind | SSSD | Centrify | PBIS |
| --- | --- | --- | --- | --- |
| RHEL 8、Rocky Linux 8 | `ou="OU=redhat,OU=Linux"` | `ou="OU=redhat,OU=Linux"` | `ou="XD.LOCAL/Linux/redhat"` | `ou="Linux/redhat"` |
| RHEL 7 | `ou="Linux/redhat"` | `ou="Linux/redhat"` | `ou="XD.LOCAL/Linux/redhat"` | `ou="Linux/redhat"` |
| SUSE | `ou="Linux/suse"` | `ou="Linux/suse"` | `ou="XD.LOCAL/Linux/suse"` | `ou="Linux/suse"` |
| Ubuntu | `ou="Linux/ubuntu"` | `ou="Linux/ubuntu"` | `ou="XD.LOCAL/Linux/ubuntu"` | `ou="Linux/ubuntu"` |

- 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.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-rhel4-x86_64.tgz?_ga=1.178323680.558673738.1478847956

    CentOS：wget http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-rhel4-x86_64.tgz?_ga=1.186648044.558673738.1478847956

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

    Ubuntu/Debian：wget https://downloads.centrify.com/products/infrastructure-services/19.9/centrify-infrastructure-services-19.9-deb8-x86_64.tgz?_ga=2.151462329.1042350071.1592881996-604509155.1572850145

- 从本地目录中提取 Centrify 软件包。要指定 Centrify 软件包的目录，请执行以下操作：

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

  例如：

```
cat /tmp/ctxinstall.conf
set "centrifypkgpath=/home/mydir"
ls  -ls  /home/mydir
    9548 -r-xr-xr-x. 1 root root  9776688 May 13  2016
       adcheck-rhel4-x86_64
    4140 -r--r--r--. 1 root root  4236714 Apr 21  2016
   centrifyda-3.3.1-rhel4-x86_64.rpm
    33492 -r--r--r--. 1 root root 34292673 May 13  2016
   centrifydc-5.3.1-rhel4-x86_64.rpm
    4 -rw-rw-r--. 1 root root     1168 Dec  1  2015
   centrifydc-install.cfg
    756 -r--r--r--. 1 root root   770991 May 13  2016
   centrifydc-ldapproxy-5.3.1-rhel4-x86_64.rpm
    268 -r--r--r--. 1 root root   271296 May 13  2016
   centrifydc-nis-5.3.1-rhel4-x86_64.rpm
    1888 -r--r--r--. 1 root root  1930084 Apr 12  2016
   centrifydc-openssh-7.2p2-5.3.1-rhel4-x86_64.rpm
    124 -rw-rw-r--. 1 root root   124543 Apr 19  2016
   centrify-suite.cfg
    0 lrwxrwxrwx. 1 root root       10 Jul  9  2012 install-
   express.sh -> install.sh
    332 -r-xr-xr--. 1 root root   338292 Apr 10  2016 install
   .sh
    12 -r--r--r--. 1 root root    11166 Apr  9  2015 release-
   notes-agent-rhel4-x86_64.txt
    4 -r--r--r--. 1 root root     3732 Aug 24  2015 release-
   notes-da-rhel4-x86_64.txt
    4 -r--r--r--. 1 root root     2749 Apr  7  2015 release-
   notes-nis-rhel4-x86_64.txt
    12 -r--r--r--. 1 root root     9133 Mar 21  2016 release-
   notes-openssh-rhel4-x86_64.txt
<!--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。例如，下面是每个发行版的 URL：

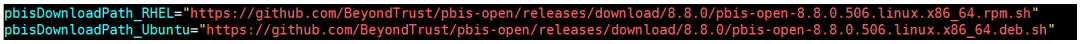
    Amazon Linux 2、CentOS 7、RHEL 8、RHEL 7、SUSE 15.3: `wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh`

    Debian、Ubuntu: `wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.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 pbisDownloadRelease 和 pbisDownloadExpectedSHA256 行。

  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。根据正在使用的虚拟机管理程序平台做出以下更改。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，在每个半虚拟化的 Linux VM 中，您都会遇到 NTP 和 Citrix Hypervisor 的问题。两者都试图管理系统时钟。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。

如果您正在运行半虚拟化的 Linux 内核，并且安装了 Citrix VM Tools，则可以检查 Citrix Hypervisor 时间同步功能是否存在，以及是否已在 Linux VM 中启用：

```
su -

cat /proc/sys/xen/independent_wallclock
<!--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：

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

```
su -

cat /proc/sys/xen/independent_wallclock
<!--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 VMware 时间同步功能后，在每个半虚拟化的 Linux VM 中，您都会遇到 NTP 和虚拟机管理程序的问题。两者都试图同步系统时钟。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 Runtime 6.0**

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 Runtime 6.0。

安装.NET Runtime 6.0 后，运行 **which dotnet** 命令查找您的运行时路径。

根据命令输出，设置.NET 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

1. 转至 Citrix Virtual Apps and Desktops 下载页面。
2. 展开适当版本的 Citrix Virtual Apps and Desktops。
3. 单击组件下载与您的 Linux 发行版匹配的 Linux VDA 软件包以及可用于验证 Linux VDA 软件包的完整性的 GPG 公钥。

   要使用公钥验证 Linux VDA 软件包的完整性，请执行以下操作：

   - 对于 RPM 软件包，请将公钥导入到 RPM 数据库中并运行以下命令：

     ```
     rpmkeys --import <path to the public key>
     rpm --checksig --verbose <path to the Linux VDA package>
     <!--NeedCopy-->
     ```

   - 对于 DEB 软件包，请将公钥导入到 DEB 数据库中并运行以下命令：

     ```
     sudo apt-get install dpkg-sig
     gpg --import <path to the public key>
     dpkg-sig --verify <path to the Linux VDA package>
     <!--NeedCopy-->
     ```

### 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、CentOS 和 Rocky Linux 发行版：

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

> 注意：
>
> 对于 RHEL 和 CentOS，请先安装 EPEL 存储库，然后才能成功安装 Linux VDA。有关如何安装 EPEL 的信息，请参阅 https://docs.fedoraproject.org/en-US/epel/ 上提供的说明。

对于 Ubuntu/Debian 发行版：

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

> 注意：
>
> - 要为 Debian 11.3 发行版安装必要的依赖项，请将 `deb http://deb.debian.org/debian / bullseye main` 行添加到 /etc/apt/sources.list 文件。
> - 要为 Debian 10.9 发行版安装必要的依赖项，请将 `deb http://deb.debian.org/debian`

> / oldstable main 行添加到 /etc/apt/sources.list 文件。

对于 SUSE 发行版：

```
zypper -i install <PATH>/<Linux VDA RPM>
<!--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
- Nutanix AHV

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

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。

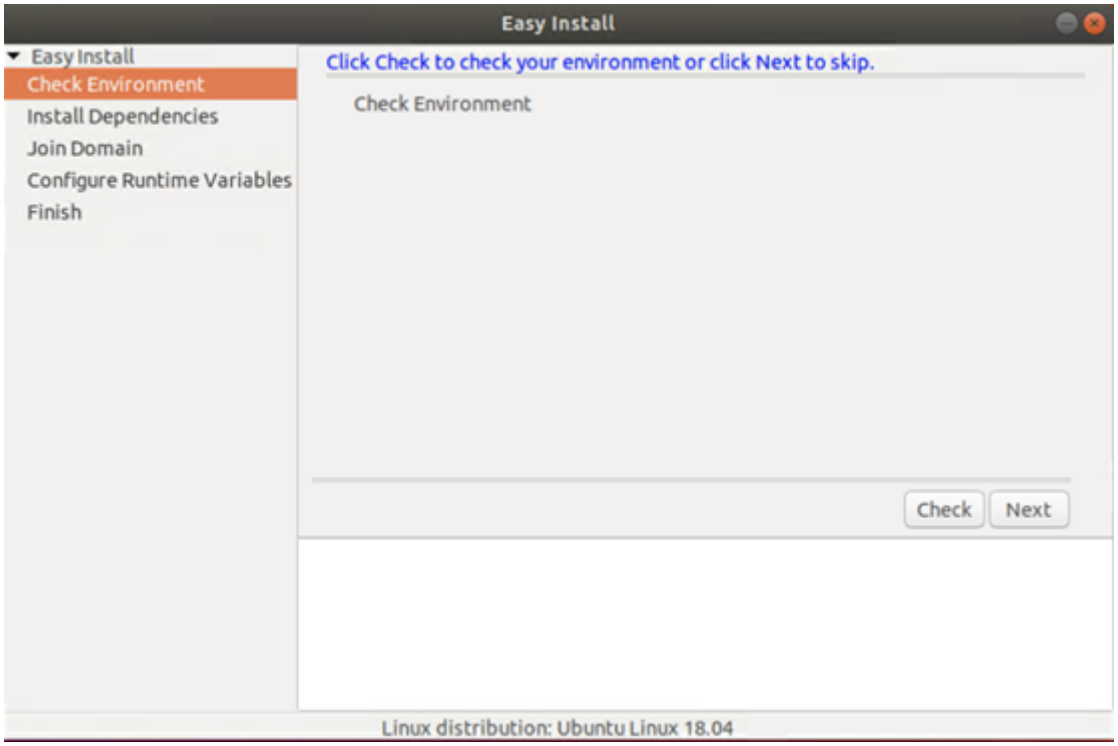
> 注意：
>
> 在设置运行时环境之前，请确保已在您的操作系统中安装了 en_US.UTF-8 区域设置。如果该区域设置在您的操作系统中不可用，请运行 sudo locale-gen en_US.UTF-8 命令。对于 Debian，请通过取消批注 # en_US.UTF-8 UTF-8 行来编辑 /etc/locale.gen 文件，然后运行 sudo locale-gen 命令。

交互模式：

在交互模式下使用轻松安装有两种方法：

- 运行 sudo /opt/Citrix/VDA/sbin/ctxinstall.sh 命令，然后在命令行界面中的每个提示符下键入相关参数。
- 在 VDA 的桌面环境中运行 /opt/Citrix/VDA/bin/easyinstall 命令，然后按照轻松安装 GUI 上的说明进行操作。




轻松安装 GUI 将引导您完成以下操作：

- 检查系统环境
- 安装依赖项
- 将 VDA 加入指定域
- 配置运行时环境

无提示模式：

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

- **CTX_EASYINSTALL_HOSTNAME=host-name** - 表示 Linux VDA 服务器的主机名。
- **CTX_EASYINSTALL_DNS=ip-address-of-dns** - DNS 的 IP 地址。
- **CTX_EASYINSTALL_NTPS=address-of-ntps** - NTP 服务器的 IP 地址或字符串名称。
- **CTX_EASYINSTALL_DOMAIN=domain-name** - 域的 NetBIOS 名称。
- **CTX_EASYINSTALL_REALM=realm-name** - Kerberos 领域名称。
- **CTX_EASYINSTALL_FQDN=ad-fqdn-name**
- **CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify | 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 Virtual Desktop 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 Virtual Desktop 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 ad2.mycompany.com:3268 ad3.mycompany.com:3268。如果将 LDAP 端口号指定为 389，Linux VDA 将在轮询模式下查询指定域中的每个 LDAP 服务器。如果有 x 个策略和 y 个 LDAP 服务器，Linux VDA 总共将执行 X 乘以 Y 次查询。如果轮询时间超过阈值，会话登录可能会失败。要启用更快的 LDAP 查询，请在域控制器上启用全局编录，并将相关的 LDAP 端口号指定为 3268。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）。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。要与 FAS 服务器正确通信，请确保附加的端口号与在 FAS 服务器上指定的端口号一致，例如 CTX_XDL_FAS_LIST=' fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number' 。
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** - 安装.NET Runtime 6.0 以支持新的 Broker 代理服务 (`ctxvda`) 的路径。默认路径为 /usr/bin。
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/mate** –指定要在会话中使用的 GNOME 、GNOME Classic 或 MATE 桌面环境。如果未指定变量，则使用 VDA 上当前安装的桌面。但是，如果当前安装的桌面为 MATE，则必须将变量值设置为 **mate**。

还可以通过完成以下步骤来更改目标会话用户的桌面环境：

1. 在 VDA 上的 **$HOME/<username>** 目录下创建一个 `.xsession` 或 `.Xclients` 文件。如果您使用的是 Amazon Linux 2，请创建 `.Xclients` 文件。如果您正在使用其他发行版，请创建一个 `.xsession` 文件。
2. 编辑 `.xsession` 或 `.Xclients` 文件以根据发行版指定桌面环境。
   - 对于 **MATE** 桌面

     ```
     MSESSION="$(type -p mate-session)"
     if [ -n "$MSESSION" ]; then
       exec mate-session
     fi
     ```

   - 适用于 **GNOME Classic** 桌面

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     export GNOME_SHELL_SESSION_MODE=classic
     exec gnome-session --session=gnome-classic
     fi
     ```

   - 对于 **GNOME** 桌面

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     exec gnome-session
     fi
     ```

3. 与目标会话用户共享 700 文件权限。

自版本 2209 起，会话用户可以自定义其桌面环境。必须提前在 VDA 上安装可切换的桌面环境，才能启用此功能。有关详细信息，请参阅按会话用户划分的自定义桌面环境。

- **CTX_XDL_START_SERVICE=Y | N** - 在完成配置后，是否启动 Linux VDA 服务。
- **CTX_XDL_TELEMETRY_SOCKET_PORT** - 用于侦听 Citrix Scout 的套接字端口。默认端口为 7503。
- **CTX_XDL_TELEMETRY_PORT** - 用于与 Citrix Scout 通信的端口。默认端口为 7502。

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 Runtime 6.0 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。

```
export CTX_EASYINSTALL_HOSTNAME=host-name

export CTX_EASYINSTALL_DNS=ip-address-of-dns

export CTX_EASYINSTALL_NTPS=address-of-ntps

```

```
export CTX_EASYINSTALL_DOMAIN=domain-name

export CTX_EASYINSTALL_REALM=realm-name

export CTX_EASYINSTALL_FQDN=ad-fqdn-name

export CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify |
   pbis

export CTX_EASYINSTALL_USERNAME=domain-user-name

export CTX_EASYINSTALL_PASSWORD=password

export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y | N

export CTX_XDL_ADD_FIREWALL_RULES=Y | N

export CTX_XDL_HDX_3D_PRO=Y | N

export CTX_XDL_VDI_MODE=Y | N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
   none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y | N

sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh
<!--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。

另外，您可以使用单个命令指定所有参数：

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

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

### 步骤 **8**：运行 **XDPing**

请运行 `sudo /opt/Citrix/VDA/bin/xdping` 以检查 Linux VDA 环境存在的常见配置问题。有关详细信息，请参阅 XDPing。

### 步骤 **9**：运行 **Linux VDA**

启动 **Linux VDA**:

启动 Linux VDA 服务：

```
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 AD 用户和组已正确配置，能够登录到 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 2206。

## 故障排除

请利用此部分中的信息对可能因使用轻松安装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)'.
```

```
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))
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')
Check the following:- The system clock is in sync between this machine
    and the delivery controller.
-  The Active Directory provider (e.g. winbind daemon) service is
    running and correctly configured.
-  Kerberos is correctly configured on this machine.
If the problem persists, please refer to Citrix Knowledge Base article
    CTX117248 for further information.
Error Details:
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'.
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.
Ensure that the system clock is in sync between this machine and the
    delivery controller.
Verify the NTP daemon is running on this machine and is correctly
    configured.
2016-11-04 02:11:52.364 [ERROR] - Could not register with any
    controllers. Waiting to try again in 120000 ms. Multi-forest - false
2016-11-04 02:11:52.365 [INFO ] - The Citrix Desktop Service failed to
    register with any controllers in the last 470 minutes.
<!--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

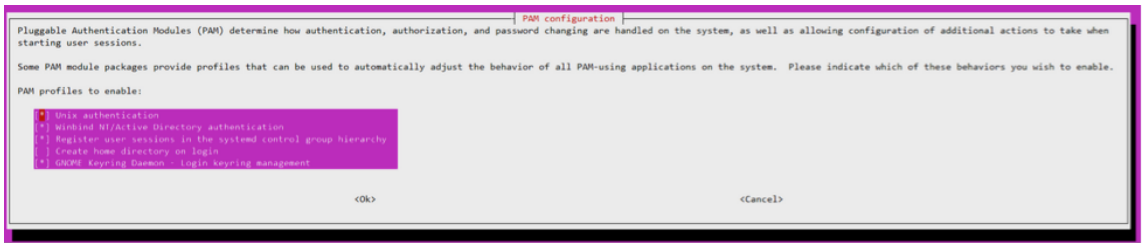
/var/log/xdl/hdx.log:

```
2016-11-02 13:21:19.015 <P22492:S1> citrix-ctxlogin: StartUserSession:
    failed to change to directory(/home/CITRIXLAB/ctxadmin) errno(2)

2016-11-02 13:21:19.017 <P22227> citrix-ctxhdx: logSessionEvent:
    Session started for user ctxadmin.

2016-11-02 13:21:19.023 <P22492:S1> citrix-ctxlogin: ChildPipeCallback:
     Login Process died: normal.

2016-11-02 13:21:59.217 <P22449:S1> citrix-ctxgfx: main: Exiting
    normally.
<!--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）：

```
Oct 27 04:17:16 CentOS7 citrix-ctxhdx[8978]: Session started for user
    CITRIXLAB\ctxadmin.

Oct 27 04:17:18 CentOS7 kernel: traps: gnome-session[19146] trap int3
    ip:7f89b3bde8d3 sp:7fff8c3409d0 error:0

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...

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)

Oct 27 04:17:18 CentOS7 gnome-session: aborting...

Oct 27 04:17:18 CentOS7 citrix-ctxgfx[18981]: Exiting normally.

Oct 27 04:17:18 CentOS7 citrix-ctxhdx[8978]: Session stopped for user
    CITRIXLAB\ctxadmin.
<!--NeedCopy-->
```

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

```
Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] pid.c:
    Stale PID file, overwriting.

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.

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.

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.

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
```

```
        # grep sshd /var/log/audit/audit.log | audit2allow -M mypol

# semodule -i mypol.pp
<!--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。

## 手动安装适用于 **Amazon Linux 2**、**CentOS**、**RHEL** 和 **Rocky Linux** 的 **Linux Virtual Delivery Agent**

September 25, 2023

> 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 **Linux** 发行版以安装 **VDA**

#### 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

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

```
hostname
```

#### 步骤 **1c**：为主机名分配环回地址

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

```
127.0.0.1 hostname-fqdn hostname localhost 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。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：

```
hostname
<!--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：

```
hostname -f
<!--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：

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--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 8 或 RHEL 7 默认环境使用 Chrony 守护程序 (`chronyd`) 进行时钟同步。

配置 **Chrony** 服务　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：

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

server peer2-fqdn-or-ip-address iburst
<!--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服务器条目，包括环回 IP 地址、localhost 以及公共服务器 ***.pool.ntp.org** 条目。

保存更改并重新启动 Chrony 守护程序：

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

步骤 **1g**：安装 **OpenJDK 11**

Linux VDA 要求存在 OpenJDK 11。

- 如果使用的是 CentOS、RHEL 或 Rocky Linux，则当您安装 Linux VDA 时，OpenJDK 11 会自动作为依赖项进行安装。
- 如果使用的是 Amazon Linux 2，请运行以下命令以启用并安装 OpenJDK 11：

  ```
  amazon-linux-extras install java-openjdk11
  <!--NeedCopy-->
  ```

确认版本是否正确：

```
sudo yum info java-11-openjdk
<!--NeedCopy-->
```

预先封装的 OpenJDK 可能为早期版本。更新到 OpenJDK 11：

```
sudo yum -y update java-11-openjdk
<!--NeedCopy-->
```

步骤 **1h**：安装 **PostgreSQL**

Linux VDA 需要 PostgreSQL。以下命令从 Linux VDA 软件包安装 PostgreSQL（适用于 Amazon Linux 2、RHEL 7 和 CentOS 7 的 PostgreSQL 9 以及适用于 RHEL 8 和 Rocky Linux 8 的 PostgreSQL 10）。

```
sudo yum -y install postgresql-server

sudo yum -y install postgresql-jdbc
<!--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。

```
sudo postgresql-setup initdb
<!--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：

```
sudo systemctl enable postgresql

sudo systemctl start postgresql
<!--NeedCopy-->
```

使用以下命令检查 PostgreSQL 版本：

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

（仅限 RHEL 7）使用 **psql** 命令行实用程序确认数据目录已设置：

```
sudo -u postgres psql -c 'show data_directory'
<!--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。根据正在使用的虚拟机管理程序平台做出以下更改。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，在每个半虚拟化的 Linux VM 中，您都会遇到 NTP 和 Citrix Hypervisor 的问题。两者都试图管理系统时钟。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。

如果您正在运行半虚拟化的 Linux 内核，并且安装了 Citrix VM Tools，则可以检查 Citrix Hypervisor 时间同步功能是否存在，以及是否已在 Linux VM 中启用：

```
su -

cat /proc/sys/xen/independent_wallclock
<!--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：

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

```
su -

cat /proc/sys/xen/independent_wallclock
<!--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 VMware 时间同步功能后，在每个半虚拟化的 Linux VM 中，您都会遇到 NTP 和虚拟机管理程序的问题。两者都试图同步系统时钟。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：

对于 RHEL 8 和 Rocky Linux 8：

```
sudo yum -y install samba-winbind samba-winbind-clients krb5-
    workstation oddjob-mkhomedir realmd authselect
<!--NeedCopy-->
```

对于 Amazon Linux 2、CentOS 7 和 RHEL 7：

```
sudo yum -y install samba-winbind samba-winbind-clients krb5-
    workstation authconfig oddjob-mkhomedir
<!--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：

```
sudo /sbin/chkconfig winbind on
<!--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. 运行以下命令。

   对于 RHEL 8 和 Rocky Linux 8：

   ```
   sudo authselect select winbind with-mkhomedir --force
   <!--NeedCopy-->
   ```

   对于 Amazon Linux 2、CentOS 7 和 RHEL 7：

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

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

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

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

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

2. 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
   winbind offline logon = no
   ```

3. （仅限 RHEL 8 和 Rocky Linux 8）打开 **/etc/krb5.conf** 并在 `[libdefaults]`、`[realms]` 和 `[domain_realm]` 部分下添加条目：

   在 `[libdefaults]` 部分下：

   ```
   default_ccache_name = FILE:/tmp/krb5cc_%{ uid }
   default_realm = REALM
   dns_lookup_kdc = true
   ```

   在 `[realms]` 部分下：

```
REALM = {
kdc = fqdn-of-domain-controller
}
```

在 [domain_realm] 部分下：

```
realm = REALM
.realm = REALM
```

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：

对于 RHEL 8 和 Rocky Linux 8：

```
sudo realm join -U user --client-software=winbind REALM
<!--NeedCopy-->
```

对于 Amazon Linux 2 和 RHEL 7：

```
sudo net ads join REALM -U user
<!--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：

```
sudo /sbin/service winbind restart
<!--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 VDA）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：

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

运行以下命令验证额外的域和计算机对象信息：

```
sudo net ads info
<!--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：

```
sudo klist -ke
<!--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：

```
sudo kinit -k MACHINE$@REALM
<!--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：

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

使用以下命令检查计算机的帐户详细信息：

```
sudo net ads status
<!--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：

```
wbinfo --krb5auth=domain\username%password
<!--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。

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

验证 Kerberos 凭据缓存中的票据是否有效且未过期：

```
klist
<!--NeedCopy-->
```

退出会话。

```
exit
<!--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：

```
reboot
<!--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。

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval 32400

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth false
<!--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：

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

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

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

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

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

```
sudo /opt/quest/bin/vastool info domain
<!--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。

```
ssh localhost -l domain\username
id -u
<!--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：

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

验证 Kerberos 凭据缓存中的票据是否有效且未过期：

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

退出会话。

```
exit
<!--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：

```
su -
adjoin -w -V -u user domain-name
<!--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 VDA）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：

```
su -
adinfo
<!--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：

```
adinfo --sysinfo all
adinfo  - diag
<!--NeedCopy-->
```

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

```
adinfo --test
<!--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. 启用 SSSD
4. 验证 Kerberos 配置
5. 验证用户身份验证

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**。

本部分内容介绍了适用于 Amazon Linux 2 和 RHEL 7 的 **Samba** 方法以及适用于 RHEL 8 的 `adcli` 方法。对于 **realmd**，请参阅 RHEL 或 CentOS 文档。必须在配置 SSSD 之前执行这些步骤。

- **Samba**（**Amazon Linux 2** 和 **RHEL 7**）：

  安装或更新所需软件包：

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

  在正确配置了以下文件的 Linux 客户端上：

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

  将计算机配置为进行 **Samba** 和 Kerberos 身份验证：

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

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

> 注意：
>
> 本文中的设置适用于单域、单林模型。根据您的 AD 基础结构配置 Kerberos。

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
winbind offline logon = no
```

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。

```
sudo net ads join REALM -U user
<!--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。

- **Adcli**（**RHEL 8** 和 **Rocky Linux 8**）：

  安装或更新所需软件包：

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

  将计算机配置为进行 **Samba** 和 Kerberos 身份验证：

```
sudo authselect select sssd with-mkhomedir --force
<!--NeedCopy-->
```

  打开 **/etc/krb5.conf** 并在 [realms] 和 [domain_realm] 部分下添加条目：

  在 [realms] 部分下：

```
REALM = {
kdc = fqdn-of-domain-controller
}
```

  在 [domain_realm] 部分下：

```
realm = REALM
.realm = REALM
```

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。

```
sudo realm join REALM -U user
<!--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：

- 通过运行 `sudo yum -y install sssd` 命令在 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。

RHEL 7 的 **sssd.conf** 配置示例（可以根据需要添加额外的选项）：

```
[sssd]
config_file_version = 2
domains = ad.example.com
services = nss, pam

[domain/ad.example.com]
# Uncomment if you need offline logins
# cache_credentials = true

id_provider = ad
auth_provider = ad
access_provider = ad
ldap_id_mapping = true
ldap_schema = ad

# Should be specified as the lower-case version of the long version of the Active Directory domain.
ad_domain = ad.example.com

# Kerberos settings
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U

# Uncomment if service discovery is not working
# ad_server = server.ad.example.com

# Comment out if the users have the shell and home dir set on the AD side
default_shell = /bin/bash
fallback_homedir = /home/%d/%u

# Uncomment and adjust if the default principal SHORTNAME$@REALM is not available
# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
```

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。

（仅限 RHEL 8）
打开 **/etc/sssd/sssd.conf** 并在 [domain/ad.example.com] 部分下添加以下条目：

```
ad_gpo_access_control = permissive
full_name_format = %2$s\\%1$s
fallback_homedir = /home/%d/%u
# Kerberos settings
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U
```

对 sssd.conf 设置文件所有权和权限：

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

启用 **SSSD**　对于 **RHEL 8** 和 **Rocky Linux 8**：

运行以下命令以启用 SSSD：

```
sudo systemctl restart sssd
sudo systemctl enable sssd.service
sudo chkconfig sssd on
<!--NeedCopy-->
```

对于 **Amazon Linux 2**、**CentOS 7** 和 **RHEL 7**：

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

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

sudo service sssd start

sudo chkconfig sssd on
<!--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：

```
sudo klist -ke
<!--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：

```
sudo kinit  -k MACHINE$@REALM
<!--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：

```
sudo klist
<!--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：

```
sudo getent passwd DOMAIN\username
<!--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。

```
sudo ssh localhost  - l DOMAIN\username

id -u
<!--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：

```
ls /tmp/krb5cc_{
 uid }

<!--NeedCopy-->
```

验证用户的 Kerberos 凭据缓存中的票据是否有效且未过期。

```
klist
<!--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

```
wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/
    pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```

使 **PBIS** 安装脚本可执行

```
chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```

运行 **PBIS** 安装脚本

```
sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--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：

```
/opt/pbis/bin/domainjoin-cli join domain-name user
<!--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 VDA）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：

```
/opt/pbis/bin/domainjoin-cli query
<!--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。

```
ssh localhost -l domain\user

id -u
<!--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：

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

退出会话。

```
exit
<!--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 Runtime 6.0**

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 Runtime 6.0。

安装.NET Runtime 6.0 后，运行 **which dotnet** 命令查找您的运行时路径。

根据命令输出，设置.NET 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

1. 转至 Citrix Virtual Apps and Desktops 下载页面。
2. 展开适当版本的 Citrix Virtual Apps and Desktops。
3. 单击组件下载与您的 Linux 发行版匹配的 Linux VDA 软件包以及可用于验证 Linux VDA 软件包的完整性的 GPG 公钥。

   要验证 Linux VDA 软件包的完整性，请将公钥导入到 RPM 数据库中并运行以下命令：

   ```
   ```
   rpmkeys --import <path to the public key>
   rpm --checksig --verbose <path to the Linux VDA package>
   <!--NeedCopy--> ```
   ```

### 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：

   ```
   sudo /sbin/service ctxvda stop

   sudo /sbin/service ctxhdx stop
   <!--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：

```
sudo rpm -e XenDesktopVDA
<!--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. 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。

3. 安装 Linux VDA

   > 注意：
   >
   > 对于 RHEL 和 CentOS，请先安装 EPEL 存储库，然后才能成功安装 Linux VDA。有关如何安装 EPEL 的信息，请参阅 https://docs.fedoraproject.org/en-US/epel/ 上提供的说明。

   - 使用 Yum 安装 Linux VDA 软件：

     对于 **Amazon Linux 2**：

     ```
     sudo yum install -y XenDesktopVDA-<version>.amzn2.x86_64.rpm
     <!--NeedCopy-->
     ```

     对于 **RHEL 8** 和 **Rocky Linux 8**：

     ```
     sudo yum install -y XenDesktopVDA-<version>.el8_x.x86_64.rpm
     <!--NeedCopy-->
     ```

     对于 **CentOS 7** 和 **RHEL 7**：

     ```
     sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
     <!--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 **Amazon Linux 2**：

     ```
     sudo rpm -i XenDesktopVDA-<version>.amzn2.x86_64.rpm
     <!--NeedCopy-->
     ```

     对于 **RHEL 8** 和 **Rocky Linux 8**：

```
sudo rpm -i XenDesktopVDA-<version>.el8_x.x86_64.rpm
<!--NeedCopy-->
```

对于 **CentOS 7** 和 **RHEL 7**：

```
sudo rpm -i XenDesktopVDA-<version>.el7_x.x86_64.rpm
<!--NeedCopy-->
```

**RHEL 8** 和 **Rocky Linux 8** 的 **RPM** 依赖项列表：

```
postgresql-server >= 10.5

postgresql-jdbc >= 42.2.3

java-11-openjdk >= 11

icoutils >= 0.32

firewalld >= 0.6.3

policycoreutils-python >= 2.8.9

policycoreutils-python-utils >= 2.8

python3-policycoreutils >= 2.8

dbus >= 1.12.8

dbus-common >= 1.12.8

dbus-daemon >= 1.12.8

dbus-tools >= 1.12.8

dbus-x11 >= 1.12.8

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.4

libXpm >= 3.5.12

libXrandr >= 1.5.1

libXtst >= 1.2.3

pam >= 1.3.1

util-linux >= 2.32.1

util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5
```

```
44
45  bash >= 4.3
46
47  findutils >= 4.6
48
49  gawk >= 4.2
50
51  sed >= 4.5
52
53  cups >= 1.6.0
54
55  foomatic-filters >= 4.0.9
56
57  cups-filters >= 1.20.0
58
59  ghostscript >= 9.25
60
61  libxml2 >= 2.9
62
63  libmspack >= 0.7
64
65  krb5-workstation >= 1.13
66
67  ibus >= 1.5
68
69  nss-tools >= 3.44.0
70
71  gperftools-libs >= 2.4
72
73  cyrus-sasl-gssapi >= 2.1
74
75  python3 >= 3.6~
76
77  qt5-qtbase >= 5.5~
78
79  qt5-qtbase-gui >= 5.5~
80
81  qrencode-libs >= 3.4.4
82
83  imlib2 >= 1.4.9
84  <!--NeedCopy-->
```

**CentOS 7** 和 **RHEL 7** 的 **RPM** 依赖项列表：

```
1  postgresql-server >= 9.2
2
3  postgresql-jdbc >= 9.2
4
5  java-11-openjdk >= 11
6
7  ImageMagick >= 6.7.8.9
8
9  firewalld >= 0.3.9
```

```
policycoreutils-python >= 2.0.83

dbus >= 1.6.12

dbus-x11 >= 1.6.12

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.2

xorg-x11-server-Xorg >= 1.20.4

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

pam >= 1.1.8

util-linux >= 2.23.2

bash >= 4.2

findutils >= 4.5

gawk >= 4.0

sed >= 4.2

cups >= 1.6.0

foomatic-filters >= 4.0.9

libxml2 >= 2.9

libmspack >= 0.5

ibus >= 1.5

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~

gperftools-libs >= 2.4

nss-tools >= 3.44.0

qt5-qtbase >= 5.5~

qt5-qtbase >= 5.5~

```

```
imlib2 >= 1.4.5
<!--NeedCopy-->
```

**Amazon Linux 2** 的 **RPM** 依赖项列表：

```
postgresql-server >= 9.2

postgresql-jdbc >= 9.2

java-11-openjdk >= 11

ImageMagick >= 6.7.8.9

firewalld >= 0.3.9

policycoreutils-python >= 2.0.83

dbus >= 1.6.12

dbus-x11 >= 1.6.12

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.2

xorg-x11-server-Xorg >= 1.20.4

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

pam >= 1.1.8

util-linux >= 2.23.2

bash >= 4.2

findutils >= 4.5

gawk >= 4.0

sed >= 4.2

cups >= 1.6.0

foomatic-filters >= 4.0.9

libxml2 >= 2.9

libmspack >= 0.5

```

```
ibus >= 1.5

cyrus-sasl-gssapi >= 2.1

gperftools-libs >= 2.4

nss-tools >= 3.44.0

qt5-qtbase >= 5.5~

qrencode-libs >= 3.4.1

imlib2 >= 1.4.5
<!--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。
>
> 在 RHEL 7.x 上安装 Linux VDA 后，运行 `sudo yum install -y python-websockify x11vnc` 命令。目的是手动安装 `python-websockify` 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

可以从先前的两个版本和 LTSR 版本升级现有安装。

> 注意：
>
> 升级现有安装将覆盖 /etc/xdl 下的配置文件。在进行升级之前，请务必备份这些文件。

- 要使用 Yum 升级您的软件，请执行以下操作：

  对于 **Amazon Linux 2**：

  ```
  sudo yum install -y XenDesktopVDA-<version>.amzn2.x86_64.rpm
  <!--NeedCopy-->
  ```

  对于 **RHEL 8** 和 **Rocky Linux 8**：

  ```
  sudo yum install -y XenDesktopVDA-<version>.el8_x.x86_64.rpm
  <!--NeedCopy-->
  ```

  对于 **CentOS 7** 和 **RHEL 7**：

  ```
  sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
  <!--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 **Amazon Linux 2**：

```
sudo rpm -U XenDesktopVDA-<version>.amzn2.x86_64.rpm
<!--NeedCopy-->
```

对于 **RHEL 8**：

```
sudo rpm -U XenDesktopVDA-<version>.el8_x.x86_64.rpm
<!--NeedCopy-->
```

对于 **CentOS 7** 和 **RHEL 7**：

```
sudo rpm -U XenDesktopVDA-<version>.el7_x.x86_64.rpm
<!--NeedCopy-->
```

> 注意：
>
> 如果您使用的是 RHEL 7，请务必在运行上述升级命令后完成以下步骤：
>
> 1. 运行 `/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent"-t "REG_SZ"-v "DotNetRuntimePath"-d "/opt/rh/rh-dotnet31/root/usr/bin/"--force` 以设置正确的.NET Runtime 路径。
> 2. 重新启动 `ctxvda` 服务。
>
> 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。

> 注意：
>
> 要对 Amazon Linux 2 使用 HDX 3D Pro，我们建议您安装 NVIDIA 驱动程序 470。有关详细信息，请参阅系统要求。

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
- Nutanix AHV

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：

```
yum install gcc

yum install "kernel-devel-$(uname -r)"

systemctl set-default multi-user.target
<!--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                                                 |
+-----------------------------------------------------------------------------+
```

为显卡设置正确的配置：

```
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响应自动运行脚本。继续操作前，请查看该脚本的帮助信息：

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

提示配置

运行会提示各种问题的手动配置：

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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 VDA 服务。默认情况下，该值设置为 Y。
- **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 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，旨在优化图形密集型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 ad2.mycompany.com:3268 ad3.mycompany.com:3268。如果将 LDAP 端口号指定为 389，Linux VDA 将在轮询模式下查询指定域中的每个 LDAP 服务器。如果有 x 个策略和 y 个 LDAP 服务器，Linux VDA 总共将执行 X 乘以 Y 次查询。如果轮询时间超过阈值，会话登录可能会失败。要启用更快的 LDAP 查询，请在域控制器上启用全局目录，并将相关的 LDAP 端口号指定为 3268。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。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。要与 FAS 服务器正确通信，请确保附加的端口号与在 FAS 服务器上指定的端口号一致，例如 CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'。
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** - 安装.NET Runtime 6.0 以支持新的 Broker 代理服务 (`ctxvda`) 的路径。默认路径为 /usr/bin。
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** –指定要在会话中使用的 GNOME、GNOME Classic 或 MATE 桌面环境。如果未指定变量，则使用 VDA 上当前安装的桌面。但是，如果当前安装的桌面为 MATE，则必须将变量值设置为 **mate**。

  还可以通过完成以下步骤来更改目标会话用户的桌面环境：

  1. 在 VDA 上的 **$HOME/<username>** 目录下创建一个 `.xsession` 或 `.Xclients` 文件。如果您使用的是 Amazon Linux 2，请创建 `.Xclients` 文件。如果您正在使用其他发行版，请创建一个 `.xsession` 文件。
  2. 编辑 `.xsession` 或 `.Xclients` 文件以指定桌面环境。
     - 对于 **MATE** 桌面

       ```
       1  MSESSION="$(type -p mate-session)"
       ```

```
if [ -n "$MSESSION" ]; then
  exec mate-session
fi
```

- 适用于 **GNOME Classic** 桌面

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
export GNOME_SHELL_SESSION_MODE=classic
exec gnome-session --session=gnome-classic
fi
```

- 对于 **GNOME** 桌面

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
exec gnome-session
fi
```

3. 与目标会话用户共享 700 文件权限。

自版本 2209 起，会话用户可以自定义其桌面环境。必须提前在 VDA 上安装可切换的桌面环境，才能启用此功能。有关详细信息，请参阅按会话用户划分的自定义桌面环境。

- **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。
- **CTX_XDL_TELEMETRY_SOCKET_PORT** - 用于侦听 Citrix Scout 的套接字端口。默认端口为 7503。
- **CTX_XDL_TELEMETRY_PORT** - 用于与 Citrix Scout 通信的端口。默认端口为 7502。

设置环境变量并运行配置脚本：

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4|5

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

```

```
export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
    none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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：

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

```

```
CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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：

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

删除配置更改：

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
<!--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**

请运行 `sudo /opt/Citrix/VDA/bin/xdping` 以检查 Linux VDA 环境存在的常见配置问题。有关详细信息，请参阅 XDPing。

### 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：

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

停止 **Linux VDA**：

停止 Linux VDA 服务：

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--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：

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start
<!--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：

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
<!--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：
>
> 当您将已删除的计算机重新加入到 Active Directory 域时，请从中删除该计算机并将其重新添加到其计算机目录中。

### 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 AD 用户和组已正确配置，能够登录到 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 2209。

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

February 9, 2024

> 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：

```
su -

yast
<!--NeedCopy-->
```

要启动基于 UI 的 YaST 工具，请执行以下操作：

```
su -

yast2 &
<!--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。

配置主机名和域名系统 **(DNS)**

1. 启动基于 UI 的 YaST 工具。
2. 选择系统，然后选择网络设置。
3. 打开 **Hostname/DNS**（主机名/DNS）选项卡。
4. 为 **Set Hostname via DHCP**（通过 DHCP 设置主机名）选择 **no**（否）选项。
5. 为修改 **DNS** 配置选择使用自定义策略选项。
6. 编辑以下内容，以反映所作的网络设置：
   - 静态主机名 - 添加计算机的 DNS 主机名。
   - 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。
7. 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 <FQDN of the VDA> <hostname of the VDA> localhost`

> 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。

检查主机名　验证主机名设置是否正确无误：

```
hostname
<!--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：

```
hostname -f
<!--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：

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--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。

对于 **SUSE 15.3**：

1. 启动基于 UI 的 YaST 工具。
2. 选择网络服务，然后选择 **NTP** 配置。
3. 在 **Start NTP Daemon**（启动 NTP 守护程序）部分，选择 **Now and on Boot**（现在及引导时）。
4. 为配置源选择动态。

5. 根据需要添加 NTP 服务器。NTP 服务通常托管在 Active Directory 域控制器上。
6. 在 /etc/chrony.conf 中删除或注释以下行（如果存在）。

   ```
   include /etc/chrony.d/*.conf
   ```

   编辑 chrony.conf 后，重新启动 `chronyd` 服务。

   ```
   sudo systemctl restart chronyd.service
   <!--NeedCopy-->
   ```

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：

- Postgresql13-server 13 或更高版本
- OpenJDK 11
- Open Motif Runtime Environment 2.3.1 或更高版本
- Cups 1.6.0 或更高版本
- ImageMagick 6.8 或更高版本

添加存储库　除了 ImageMagick 之外，您还可以从官方存储库中获取大多数必需的软件包。要获取 ImageMagick 软件包，请使用 YaST 或以下命令启用 `sle-module-desktop-applications` 存储库：

```
SUSEConnect -p sle-module-desktop-applications/<version number>/
x86_64
```

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：

```
sudo zypper install krb5-client
<!--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 11**　Linux VDA 要求存在 OpenJDK 11。

要安装 OpenJDK 11，请运行以下命令：

```
sudo zypper install java-11-openjdk
<!--NeedCopy-->
```

安装 **PostgreSQL**　要安装 `Postgresql`，请运行以下命令：

```
sudo zypper install postgresql-server

sudo zypper install postgresql-jdbc
<!--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：

```
sudo systemctl enable postgresql

sudo systemctl restart postgresql
<!--NeedCopy-->
```

数据库文件位于 /var/lib/pgsql/data。

### 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。根据正在使用的虚拟机管理程序平台做出以下更改。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，在每个半虚拟化的 Linux VM 中，您都会遇到 NTP 和 Citrix Hypervisor 的问题。两者都试图管理系统时钟。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。

如果您正在运行半虚拟化的 Linux 内核，并且安装了 Citrix VM Tools，则可以检查 Citrix Hypervisor 时间同步功能是否存在，以及是否已在 Linux VM 中启用：

```
su -

cat /proc/sys/xen/independent_wallclock
<!--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：

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

```
reboot
<!--NeedCopy-->
```

重新启动后，验证此设置是否正确：

```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

此命令返回值 1。

#### 修复 **Microsoft Hyper-V** 上的时间同步问题

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

从管理操作系统中：

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

> 注意：
>
> 此方法与 VMware 和 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，在每个半虚拟化的 Linux VM 中，您都会遇到 NTP 和虚拟机管理程序的问题。两者都试图同步系统时钟。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。

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

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

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

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

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

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

1. 启动 YaST，选择网络服务，然后选择 **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 **Use SMB information for Linux Authentication**（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。如果系统提示您安装某些软件包，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. 手动重新启动服务或重新启动计算机。我们建议您重新启动计算机：

```
su -
reboot
<!--NeedCopy-->
```

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

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

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

运行以下命令验证额外的域和计算机对象信息：

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

验证 **Kerberos** 配置　确保系统 keytab 文件是否已创建并且包含有效密钥：

```
sudo klist  -ke
<!--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：

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

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

请使用以下命令验证计算机帐户的 TGT 票据已缓存：

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

请使用以下命令检查计算机帐户详细信息：

```
sudo net ads status
<!--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：

```
wbinfo --krb5auth=domain\username%password
<!--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。

验证 Winbind PAM 模块的配置是否正确。为此，请使用以前未使用过的域用户帐户登录到 Linux VDA。

```
ssh localhost -l domain\username
id -u
<!--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：

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

验证用户的 Kerberos 凭据缓存中的票据是否有效且未过期：

```
klist
<!--NeedCopy-->
```

退出会话。

```
exit
<!--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 Service

**在域控制器上配置 Quest** 假定您已在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：

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
    interval 32400

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
    auth false
<!--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），请手动配置 PAM 和 NSS：

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

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

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

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

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

```
sudo /opt/quest/bin/vastool info domain
<!--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　验证 Quest 是否可以通过 PAM 对域用户进行身份验证。为此，请使用以前未使用过的域用户帐户登录到 Linux VDA。

```
ssh localhost -l domain\username
id -u
<!--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：

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

验证 Kerberos 凭据缓存中的票据是否有效且未过期：

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

退出会话。

```
exit
<!--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：

```
sudo adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

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

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

```
sudo adinfo
<!--NeedCopy-->
```

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

请使用以下命令可获得更全面的系统和诊断信息：

```
adinfo --sysinfo all

adinfo  - diag
<!--NeedCopy-->
```

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

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

在进行域加入验证后继续执行步骤 6：安装 Linux VDA。

### SSSD

如果您在 SUSE 上使用 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 SUSE 上设置 SSSD，请完成以下步骤：

1. 加入域并创建主机 keytab
2. 为 SSSD 配置 PAM
3. 设置 SSSD
4. 启用 SSSD
5. 验证域成员身份
6. 验证 Kerberos 配置
7. 验证用户身份验证

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 **Samba** 方法。在配置 SSSD 之前，请完成以下步骤。

1. 停止并禁用 Name Service Cache Daemon (NSCD) 守护进程。

```
sudo systemctl stop nscd
sudo systemctl disable nscd
<!--NeedCopy-->
```

2. 检查主机名和 Chrony 时间同步。

```
hostname
hostname -f
chronyc traking
<!--NeedCopy-->
```

3. 安装或更新所需软件包：

```
sudo zypper install samba-client sssd-ad
<!--NeedCopy-->
```

4. 以 root 用户身份编辑 `/etc/krb5.conf` 文件，以允许 **kinit** 实用程序与目标域进行通信。在 **[libdefaults]**、**[realms]** 和 **[domain_realm]** 部分下添加以下条目：

> 注意：
>
> 根据您的 AD 基础结构配置 Kerberos。以下设置适用于单域、单林模型。

```
[libdefaults]

    dns_canonicalize_hostname = false

    rdns = false

    default_realm = REALM

    forwardable = true

[realms]

    REALM = {
```

```
14
15
16          kdc = fqdn-of-domain-controller
17
18          default_domain = realm
19
20          admin_server = fqdn-of-domain-controller
21       }
22
23  [domain_realm]
24
25      .realm = REALM
26  <!--NeedCopy-->
```

**realm** 是 Kerberos 领域的名称，例如 example.com。**REALM** 是大写的 Kerberos 领域名称，例如 EXAMPLE.COM。

5. 以 root 用户身份编辑 /etc/samba/smb.conf，以允许 **net** 实用程序与目标域进行通信。将以下条目添加到 **[global]** 部分：

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

**domain** 是 Active Directory 域的简短 NetBIOS 名称，例如 EXAMPLE。

6. 修改 /etc/nsswitch.conf 文件中的 **passwd** 和 **group** 条目以在解析用户和组时引用 SSSD。

```
1  passwd: compat sss
2
3  group: compat sss
4  <!--NeedCopy-->
```

7. 使用已配置的 Kerberos 客户端以管理员身份向目标域进行身份验证。

```
1  kinit administrator
2  <!--NeedCopy-->
```

8. 使用 **net** 实用程序将系统加入域并生成系统 Keytab 文件。

```
1  net ads join osname="SUSE Linux Enterprise Server" osVersion=15 -U
       administrator
2  <!--NeedCopy-->
```

为 **SSSD** 配置 **PAM**　在为 SSSD 配置 PAM 之前，请安装或更新所需的软件包：

```
sudo zypper install sssd sssd-ad
<!--NeedCopy-->
```

将 PAM 模块配置为通过 SSSD 进行用户身份验证，并为用户登录创建主目录。

```
sudo pam-config --add  --sss
sudo pam-config --add --mkhomedir
<!--NeedCopy-->
```

设置 **SSSD**

1. 以 root 用户身份编辑 /etc/sssd/sssd.conf，以允许 SSSD 守护程序与目标域进行通信。sssd.conf 配置示例（可以根据需要添加额外的选项）：

```
[sssd]
    config_file_version = 2
    services = nss,pam
    domains = domain-dns-name

[domain/domain-dns-name]
    id_provider = ad
    auth_provider = ad
    access_provider = ad
    ad_domain = domain-dns-name
    ad_server = fqdn-of-domain-controller
    ldap_id_mapping = true
    ldap_schema = ad

# Kerberos settings
    krb5_ccachedir = /tmp
    krb5_ccname_template = FILE:%d/krb5cc_%U

# Comment out if the users have the shell and home dir set on the
   AD side

    fallback_homedir = /home/%d/%u
    default_shell = /bin/bash

# Uncomment and adjust if the default principal SHORTNAME$@REALM
   is not available

# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM

    ad_gpo_access_control = permissive

<!--NeedCopy-->
```

**domain-dns-name** 是 DNS 域名，例如 example.com。

> 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。将 **ad_gpo_access_control** 设置为 **permissive** 以防止 Linux 会话出现无效登录错误。请参阅 `sssd.conf` 和 `sssd-ad` 的手册页。

2. 对 `sssd.conf` 设置文件所有权和权限：

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

启用 **SSSD**　请运行以下命令以在系统启动时启用并启动 SSSD 守护程序：

```
sudo systemctl enable sssd
sudo systemctl start sssd
<!--NeedCopy-->
```

验证域成员身份

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

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

2. 运行以下命令验证额外的域和计算机对象信息：

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

验证 **Kerberos** 配置　确保系统 keytab 文件是否已创建并且包含有效密钥：

```
sudo klist -ke
<!--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：

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

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

请使用以下命令验证计算机帐户的 TGT 票据已缓存：

```
sudo klist
<!--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。

```
ssh localhost -l domain\username

id -u

klist

exit
<!--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：

```
ls /tmp/krb5cc_uid
<!--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。

### PBIS

下载所需的 **PBIS** 软件包　例如：

```
wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/
    pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```

使 **PBIS** 安装脚本可执行　例如：

```
chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```

运行 **PBIS** 安装脚本　例如：

```
sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```

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

```
/opt/pbis/bin/domainjoin-cli join domain-name user
<!--NeedCopy-->
```

**user** 为有权将计算机添加到 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 VDA）都要在 Active Directory 中有一个计算机对象。要验证加入了 PBIS 的 Linux 计算机是否位于域中，请执行以下操作：

```
/opt/pbis/bin/domainjoin-cli query
<!--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　验证 PBIS 是否能够通过 PAM 对域用户进行身份验证。为此，请使用以前未使用过的域用户帐户登录到 Linux VDA。

```
ssh localhost -l domain\user

id -u
<!--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：

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

退出会话。

```
exit
<!--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 Runtime 6.0**

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 Runtime 6.0。

安装.NET Runtime 6.0 后，运行 **which dotnet** 命令查找您的运行时路径。

根据命令输出，设置.NET 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

1. 转至 Citrix Virtual Apps and Desktops 下载页面。

2. 展开适当版本的 Citrix Virtual Apps and Desktops。
3. 单击组件下载与您的 Linux 发行版匹配的 Linux VDA 软件包以及可用于验证 Linux VDA 软件包的完整性的 GPG 公钥。

   要使用公钥验证 Linux VDA 软件包的完整性，请将公钥导入到 RPM 数据库中并运行以下命令：

```
rpmkeys --import <path to the public key>
rpm --checksig --verbose <path to the Linux VDA package>
<!--NeedCopy-->
```

### 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：

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--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：

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

> 重要提示：
>
> 支持从最新的两个版本进行升级。
>
> 注意：
>
> 您可以在 **/opt/Citrix/vda/** 下找到已安装的组件。
>
> 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：

```
sudo zypper install XenDesktopVDA-<version>.sle15_x.x86_64.rpm
<!--NeedCopy-->
```

使用 RPM 软件包管理器安装 Linux VDA 软件：

```
sudo rpm -i XenDesktopVDA-<version>.sle15_x.x86_64.rpm
<!--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。

> 注意：
>
> 升级现有安装将覆盖 /etc/xdl 下的配置文件。在进行升级之前，请务必备份这些文件。

```
sudo rpm -U XenDesktopVDA-<version>.sle15_x.x86_64.rpm
<!--NeedCopy-->
```

**SUSE 15** 的 **RPM** 依赖项列表：

```
postgresql >= 13

postgresql-server >= 13

postgresql-jdbc >= 9.4

java-11-openjdk >= 11

ImageMagick >= 7.0

dbus-1 >= 1.12.2

dbus-1-x11 >= 1.12.2

xorg-x11 >= 7.6_1

libXpm4 >= 3.5.12

libXrandr2 >= 1.5.1

libXtst6 >= 1.2.3

pam >= 1.3.0

bash >= 4.4

findutils >= 4.6

gawk >= 4.2
```

```
30
31  sed >= 4.4
32
33  cups >= 2.2
34
35  cups-filters >= 1.25
36
37  libxml2-2 >= 2.9
38
39  libmspack0 >= 0.6
40
41  ibus >= 1.5
42
43  libtcmalloc4 >= 2.5
44
45  libcap-progs >= 2.26
46
47  mozilla-nss-tools >= 3.53.1
48
49  libpython3_6m1_0 >= 3.6~
50
51  libQt5Widgets5 >= 5.12
52
53  libqrencode4 >= 4.0.0
54
55  libImlib2-1 >= 1.4.10
56  <!--NeedCopy-->
```

> 重要提示：
>
> 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
- Nutanix AHV

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。脚本做出任何更改之前，都会验证环境，并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：

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

#### 提示配置

运行会提示各种问题的手动配置：

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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 VDA 服务。默认情况下，该值设置为 Y。
- **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 打开所需的端口（默认为端口 80 和 1494）。默认情况下设置为 Y。
- **CTX_XDL_AD_INTEGRATION=1 | 2 | 3 | 4** –Linux VDA 要求使用 Kerberos 配置设置向 Delivery Controller 进行身份验证。Kerberos 配置根据系统上已安装和已配置的 Active Directory 集成工具确定。指定要使用且受支持的 Active Directory 集成方法：
  - 1 –Samba Winbind
  - 2 –Quest Authentication Service
  - 3 - Centrify DirectControl
  - 4 - SSSD

- **CTX_XDL_HDX_3D_PRO=Y | N** - Linux VDA 支持 HDX 3D Pro，这是一组 GPU 加速技术，旨在优化富图形应用程序的虚拟化水平。如果选择了 HDX 3D Pro，则要为 VDI 桌面（单会话）模式配置 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 ad2.mycompany.com:3268 ad3.mycompany.com:3268。如果将 LDAP 端口号指定为 389，Linux VDA 将在轮询模式下查询指定域中的每个 LDAP 服务器。如果有 x 个策略和 y 个 LDAP 服务器，Linux VDA 总共将执行 X 乘以 Y 次查询。如果轮询时间超过阈值，会话登录可能会失败。要启用更快的 LDAP 查询，请在域控制器上启用全局目录，并将相关的 LDAP 端口号指定为 3268。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。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。要与 FAS 服务器正确通信，请确保附加的端口号与在 FAS 服务器上指定的端口号一致，例如 CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'。
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** - 安装.NET Runtime 6.0 以支持新的 Broker 代理服务 (`ctxvda`) 的路径。默认路径为 /usr/bin。
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** –指定要在会话中使用的 GNOME、GNOME Classic 或 MATE 桌面环境。如果未指定变量，则使用 VDA 上当前安装的桌面。但是，如果当前安装的桌面为 MATE，则必须将变量值设置为 **mate**。

  还可以通过完成以下步骤来更改目标会话用户的桌面环境：

  1. 在 VDA 上的 **$HOME/<username>** 目录下创建一个 `.xsession` 文件。
  2. 编辑 `.xsession` 文件以指定桌面环境。
     - 适用于 **SUSE 15** 上的 **MATE** 桌面

```
MSESSION="$(type -p mate-session)"
if [ -n "$MSESSION" ]; then
  exec mate-session
fi
```

- 适用于 **SUSE 15** 上的 **GNOME Classic** 桌面

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
export GNOME_SHELL_SESSION_MODE=classic
exec gnome-session --session=gnome-classic
fi
```

- 适用于 **SUSE 15** 上的 **GNOME** 桌面

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
exec gnome-session
fi
```

3. 与目标会话用户共享 700 文件权限。

自版本 2209 起，会话用户可以自定义其桌面环境。必须提前在 VDA 上安装可切换的桌面环境，才能启用此功能。有关详细信息，请参阅按会话用户划分的自定义桌面环境。

- **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。
- **CTX_XDL_TELEMETRY_SOCKET_PORT** - 用于侦听 Citrix Scout 的套接字端口。默认端口为 7503。
- **CTX_XDL_TELEMETRY_PORT** - 用于与 Citrix Scout 通信的端口。默认端口为 7502。

设置环境变量并运行配置脚本：

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

```

```
export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
    none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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：

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

```

```
/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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：

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

删除配置更改：

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

> 重要提示：
>
> 此脚本会从数据库删除所有配置数据，从而使 Linux VDA 无法使用。

配置日志

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

`/tmp/xdl.configure.log`

重新启动 Linux VDA 服务，确保更改生效。

### 步骤 **9**：运行 **XDPing**

请运行 `sudo /opt/Citrix/VDA/bin/xdping` 以检查 Linux VDA 环境存在的常见配置问题。有关详细信息，请参阅 XDPing。

### 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：

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

停止 **Linux VDA**：

要停止 Linux VDA 服务，请执行以下操作：

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--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：

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start
<!--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：

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
<!--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。

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

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 2206。

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

November 4, 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：

```
hostname
<!--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：

```
hostname -f
<!--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：

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--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：

```
apt-get install chrony
<!--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：

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

步骤 **1h**：安装 **OpenJDK 11**

Linux VDA 要求存在 OpenJDK 11。

在 Ubuntu 20.04 和 Ubuntu 18.04 上，使用以下命令安装 OpenJDK 11：

```
sudo apt-get install -y openjdk-11-jdk
<!--NeedCopy-->
```

步骤 **1i**：安装 **PostgreSQL**

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

```
sudo apt-get install -y postgresql

sudo apt-get install -y libpostgresql-jdbc-java
<!--NeedCopy-->
```

步骤 **1j**：安装 **Motif**

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

步骤 **1k**：安装其他软件包

对于 Ubuntu 22.04：

```
sudo apt-get install -y libsasl2-2
sudo apt-get install -y libsasl2-modules-gssapi-mit
sudo apt-get install -y libldap-2.5-0
sudo apt-get install -y krb5-user
sudo apt-get install -y libgtk2.0-0
<!--NeedCopy-->
```

对于 Ubuntu 20.04、Ubuntu 18.04：

```
sudo apt-get install -y libsasl2-2
sudo apt-get install -y libsasl2-modules-gssapi-mit
sudo apt-get install -y libldap-2.4-2
sudo apt-get install -y krb5-user
sudo apt-get install -y libgtk2.0-0
<!--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。根据正在使用的虚拟机管理程序平台做出以下更改。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，在每个半虚拟化的 Linux VM 中，您都会遇到 NTP 和 Citrix Hypervisor 的问题。两者都试图管理系统时钟。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。

如果您正在运行半虚拟化的 Linux 内核，并且安装了 Citrix VM Tools，则可以检查 Citrix Hypervisor 时间同步功能是否存在，以及是否已在 Linux VM 中启用：

```
su -

cat /proc/sys/xen/independent_wallclock
<!--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：

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

```
su -

cat /proc/sys/xen/independent_wallclock
<!--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，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

启用 VMware 时间同步功能后，在每个半虚拟化的 Linux VM 中，您都会遇到 NTP 和虚拟机管理程序的问题。两者都试图同步系统时钟。为避免时钟与其他服务器不同步，请确保每个 Linux 客户机中的系统时钟都与 NTP 同步。这种情况要求禁用主机时间同步。

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

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

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

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

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

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
<!--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：

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

> 注意：
>
> 确保 `winbind` 脚本位于 `/etc/init.d` 下。

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

> 注意：
>
> 根据您的 AD 基础结构配置 Kerberos。以下设置适用于单域、单林模型。

```
[libdefaults]
default_realm = REALM
dns_lookup_kdc = false
[realms]
REALM = {
admin_server = domain-controller-fqdn
kdc = domain-controller-fqdn
}
[domain_realm]
domain-dns-name = REALM
.domain-dns-name = REALM
```

此上下文中的 **domain-dns-name** 参数为 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：

```
[global]
```

```
workgroup = WORKGROUP
security = ADS
realm = REALM
encrypt passwords = yes
idmap config *:range = 16777216-33554431
winbind trusted domains only = no
kerberos method = secrets and keytab
winbind refresh tickets = yes
template shell = /bin/bash
```

**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：

```
sudo net ads join REALM -U user
<!--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**

```
sudo systemctl restart winbind
<!--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：

```
sudo pam-auth-update
<!--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：

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

运行以下命令验证额外的域和计算机对象信息：

```
sudo net ads info
<!--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：

```
sudo klist -ke
<!--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：

```
sudo kinit -k MACHINE$@REALM
<!--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：

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

使用以下命令检查计算机的帐户详细信息：

```
sudo net ads status
<!--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：

```
wbinfo --krb5auth=domain\username%password
<!--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。

```
ssh localhost -l domain\username

id -u
<!--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：

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

验证用户的 Kerberos 凭据缓存中的票据是否有效且未过期：

```
klist
<!--NeedCopy-->
```

退出会话。

```
exit
<!--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 Service

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

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

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

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

在 **Linux VDA** 上配置 **Quest**

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

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

```
SELINUX=disabled
```

此更改要求重新启动计算机：

```
reboot
<!--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：

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
    interval 32400

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
    auth false
<!--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：

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

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

```
sudo /opt/quest/bin/vastool -u user join domain-name
<!--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：

```
sudo /opt/quest/bin/vastool info domain
<!--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。

```
ssh localhost -l domain\username

id -u
<!--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：

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

验证 Kerberos 凭据缓存中的票据是否有效且未过期：

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

退出会话。

```
exit
<!--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：

```
su -
adjoin -w -V -u user domain-name
<!--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：

```
su  -

adinfo
<!--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：

```
adinfo --sysinfo all

adinfo --diag
<!--NeedCopy-->
```

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

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

在进行域加入验证后继续执行步骤 6：安装 Linux VDA。

### SSSD

配置 **Kerberos**　运行以下命令以安装 Kerberos：

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

要配置 Kerberos，请以 root 用户身份打开 **/etc/krb5.conf** 并配置以下参数：

> 注意：
>
> 根据您的 AD 基础结构配置 Kerberos。以下设置适用于单域、单林模型。

```
[libdefaults]

default_realm = REALM

dns_lookup_kdc = false

[realms]

REALM = {

admin_server = domain-controller-fqdn

kdc = domain-controller-fqdn
```

```
}
[domain_realm]
domain-dns-name = REALM
.domain-dns-name = REALM
```

此上下文中的 `domain-dns-name` 参数为 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：

- 如果您使用 **adcli** 加入域，请完成以下步骤：

1. 安装 **adcli**。

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

2. 通过 **adcli** 加入域。

   使用以下命令删除旧系统 keytab 文件并加入域：

   ```
   su -

   rm -rf /etc/krb5.keytab

   adcli join domain-dns-name -U user -H hostname-fqdn
   <!--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. 验证域成员身份。

   对于 Ubuntu 22.04 和 Ubuntu 20.04 计算机，请运行 `adcli testjoin` 命令来测试这些计算机是否已加入域。

   对于 Ubuntu 18.04 计算机，请运行 `sudo klist -ket` 命令。**adcli** 工具的功能有限。该工具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。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，请完成以下步骤：

1. 安装软件包。

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

2. 配置 **Samba**。

   打开 **/etc/samba/smb.conf** 并配置以下设置：

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
client signing = yes
client use spnego = yes
kerberos method = secrets and keytab
```

   **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。

```
sudo net ads join REALM -U user
<!--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：

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

如果已安装软件包，则建议进行更新：

```
sudo apt-get install --only-upgrade sssd
<!--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/sssd/sssd.conf** 配置文件，必须手动创建。以 root 用户身份创建或打开 **/etc/sssd/sssd.conf** 并配置以下设置：

```
[sssd]
services = nss, pam
config_file_version = 2
domains = domain-dns-name
[domain/domain-dns-name]
id_provider = ad
access_provider = ad
auth_provider = krb5
krb5_realm = REALM
# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer
than 14 days
krb5_renewable_lifetime = 14d
# Set krb5_renew_interval to lower value if TGT ticket lifetime is
shorter than 2 hours
krb5_renew_interval = 1h
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U
# This ldap_id_mapping setting is also the default value
ldap_id_mapping = true
override_homedir = /home/%d/%u
default_shell = /bin/bash
ad_gpo_map_remote_interactive = +ctxhdx
```

> 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** 参数为 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。
>
> 有关配置设置的信息，请参阅 sssd.conf 和 `sssd-ad` 的手册页。

SSSD 守护程序要求配置文件必须仅具有所有者读取权限：

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

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

```
sudo systemctl start sssd

sudo systemctl enable sssd
<!--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：

```
sudo pam-auth-update
<!--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：

```
sudo klist -ke
<!--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：

```
sudo kinit -k MACHINE$@REALM
<!--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 已缓存：

```
sudo klist
<!--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。

```
ssh localhost -l domain\username

id -u

klist

exit
<!--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：

```
ls /tmp/krb5cc_uid
<!--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

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

使 **PBIS** 安装脚本可执行

```
sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

运行 **PBIS** 安装脚本

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--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：

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
<!--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：

```
/opt/pbis/bin/domainjoin-cli query
<!--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。

```
sudo ssh localhost -l domain\user

id -u
<!--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：

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

退出会话。

```
exit
<!--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 Runtime 6.0**

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 Runtime 6.0。

安装.NET Runtime 6.0 后，运行 **which dotnet** 命令查找您的运行时路径。

根据命令输出，设置.NET 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

1. 转至 Citrix Virtual Apps and Desktops 下载页面。
2. 展开适当版本的 Citrix Virtual Apps and Desktops。
3. 单击组件下载与您的 Linux 发行版匹配的 Linux VDA 软件包以及可用于验证 Linux VDA 软件包的完整性的 GPG 公钥。

   要使用公钥验证 Linux VDA 软件包的完整性，请将公钥导入到 DEB 数据库中并运行以下命令：

```
```
sudo apt-get install dpkg-sig
gpg --import <path to the public key>
dpkg-sig --verify <path to the Linux VDA package>
<!--NeedCopy--> ```
```

### 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 22.04**：

```
sudo dpkg -i xendesktopvda_<version>.ubuntu22.04_amd64.deb
<!--NeedCopy-->
```

对于 **Ubuntu 20.04**：

```
sudo dpkg -i xendesktopvda_<version>.ubuntu20.04_amd64.deb
<!--NeedCopy-->
```

对于 **Ubuntu 18.04**：

```
sudo dpkg -i xendesktopvda_<version>.ubuntu18.04_amd64.deb
<!--NeedCopy-->
```

**Ubuntu 22.04** 的 **Debian** 依赖项列表：

```
postgresql >= 14

libpostgresql-jdbc-java >= 42.3

openjdk-11-jdk >= 11

imagemagick >= 8:6.9.11

libgtkmm-3.0-1v5 >= 3.24.5

ufw >= 0.36

ubuntu-desktop >= 1.481

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.37
```

 
```

```
gtk3-nocsd >= 3

bash >= 5.1

findutils >= 4.8.0

sed >= 4.8

cups >= 2.4

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.9~

libpython3.10 >= 3.10~

libsasl2-modules-gssapi-mit >= 2.1.~

libnss3-tools >= 2:3.68

libqt5widgets5 >= 5.15~

libqrencode4 >= 4.1.1

libimlib2 >= 1.7.4
<!--NeedCopy-->
```

**Ubuntu 20.04** 的 **Debian** 依赖项列表：

```
postgresql >= 12

libpostgresql-jdbc-java >= 42.2

openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

libgtkmm-3.0-1v5 >= 3.24.2

ufw >= 0.36

ubuntu-desktop >= 1.450

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.34
```

```
gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.7.0

sed >= 4.7

cups >= 2.3

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.7~

libpython3.8 >= 3.8~

libsasl2-modules-gssapi-mit >= 2.1.~

libnss3-tools >= 2:3.49

libqt5widgets5 >= 5.7~

libqrencode4 >= 4.0.0

libimlib2 >= 1.6.1
<!--NeedCopy-->
```

**Ubuntu 18.04** 的 **Debian** 依赖项列表：

```
postgresql >= 9.5

libpostgresql-jdbc-java >= 9.2

openjdk-11-jdk >= 11

imagemagick >= 8:6.8.9.9

ufw >= 0.35

libgtkmm-3.0-1v5 >= 3.22.2

ubuntu-desktop >= 1.361

libxrandr2 >= 2:1.5.0

libxtst6 >= 2:1.2.2

libxm4 >= 2.3.4

util-linux >= 2.27.1
```

```
gtk3-nocsd >= 3

bash >= 4.3

findutils >= 4.6.0

sed >= 4.2.2

cups >= 2.1

libmspack0 >= 0.6

ibus >= 1.5

libsasl2-modules-gssapi-mit >= 2.1.~

libgoogle-perftools4 >= 2.4~

libpython3.6 >= 3.6~

libnss3-tools >= 2:3.35

libqt5widgets5 >= 5.7~

libqrencode3 >= 3.4.4

libimlib2 >= 1.4.10
<!--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。

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

> 注意：
>
> 升级现有安装将覆盖 /etc/xdl 下的配置文件。在进行升级之前，请务必备份这些文件。

#### 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
- Nutanix AHV

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：

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

#### 提示配置

运行会提示各种问题的手动配置：

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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 VDA 服务。默认情况下设置为 Y。

- **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 打开所需的端口（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 Service
  - 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 ad2.mycompany.com:3268 ad3.mycompany.com:3268。如果将 LDAP 端口号指定为 389，Linux VDA 将在轮询模式下查询指定域中的每个 LDAP 服务器。如果有 x 个策略和 y 个 LDAP 服务器，Linux VDA 总共将执行 X 乘以 Y 次查询。如果轮询时间超过阈值，会话登录可能会失败。要启用更快的 LDAP 查询，请在域控制器上启用全局编录，并将相关的 LDAP 端口号指定为 3268。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。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。要与 FAS 服务器正确通信，请确保附加的端口号与在 FAS 服务器上指定的端口号一致，例如 CTX_XDL_FAS_LIST=’ fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number’ 。
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** - 安装.NET Runtime 6.0 以支持新的 Broker 代理服务 (`ctxvda`) 的路径。默认路径为 /usr/bin。

- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** –指定要在会话中使用的 GNOME 、GNOME Classic 或 MATE 桌面环境。如果未指定变量，则使用 VDA 上当前安装的桌面。但是，如果当前安装的桌面为 MATE，则必须将变量值设置为 **mate**。

  还可以通过完成以下步骤来更改目标会话用户的桌面环境：

  1. 在 VDA 上的 **$HOME/<username>** 目录下创建一个 `.xsession` 文件。
  2. 编辑 `.xsession` 文件以根据发行版指定桌面环境。
     - 对于 **MATE** 桌面

       ```
       MSESSION="$(type -p mate-session)"
       if [ -n "$MSESSION" ]; then
         exec mate-session
       fi
       ```

     - 适用于 **GNOME Classic** 桌面

       ```
       GSESSION="$(type -p gnome-session)"
       if [ -n "$GSESSION" ]; then
       export GNOME_SHELL_SESSION_MODE=classic
       exec gnome-session --session=gnome-classic
       fi
       ```

     - 对于 **GNOME** 桌面

       ```
       GSESSION="$(type -p gnome-session)"
       if [ -n "$GSESSION" ]; then
       exec gnome-session
       fi
       ```

  3. 与目标会话用户共享 700 文件权限。

  自版本 2209 起，会话用户可以自定义其桌面环境。必须提前在 VDA 上安装可切换的桌面环境，才能启用此功能。有关详细信息，请参阅按会话用户划分的自定义桌面环境。

- **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。
- **CTX_XDL_TELEMETRY_SOCKET_PORT** - 用于侦听 Citrix Scout 的套接字端口。默认端口为 7503。
- **CTX_XDL_TELEMETRY_PORT** - 用于与 Citrix Scout 通信的端口。默认端口为 7502。

设置环境变量并运行配置脚本：

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

```

```
export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4|5

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
    none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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。

另外，您可以使用单个命令指定所有参数：

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

```

```
CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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：

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

删除配置更改：

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
<!--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：

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

查看更多详细信息：

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

要卸载 Linux VDA 软件，请执行以下操作：

```
dpkg -r xendesktopvda
<!--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**

请运行 `sudo /opt/Citrix/VDA/bin/xdping` 以检查 Linux VDA 环境存在的常见配置问题。有关详细信息，请参阅 XDPing。

### 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：

```
sudo systemctl start ctxhdx

sudo systemctl start ctxvda
<!--NeedCopy-->
```

停止 **Linux VDA**：

停止 Linux VDA 服务：

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
<!--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：

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

sudo systemctl restart ctxvda
<!--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：

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
<!--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 AD 用户和组已正确配置，能够登录到 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 2209。

## 手动安装 **Linux Virtual Delivery Agent for Debian**

November 4, 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 **Debian** 以便进行 **VDA** 安装

##### 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

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。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：

```
hostname
<!--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：

```
hostname -f
<!--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** 并更改以下行：

```
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：

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--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：

```
apt-get install chrony
<!--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：

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

步骤 **1h**：安装软件包

```
sudo apt-get install -y libsasl2-2

sudo apt-get install -y libgtk2.0-0
<!--NeedCopy-->
```

步骤 **1i**：添加存储库以安装必要的依赖项

对于 Debian 11.3，请将 `deb http://deb.debian.org/debian/ bullseye main` 行添加到 /etc/apt/sources.list 文件中。

对于 Debian 10.9，请将 `deb http://deb.debian.org/debian/ oldstable main` 行添加到 /etc/apt/sources.list 文件中。

步骤 **1j**：安装 **PostgreSQL**

Linux VDA 要求在 Debian 上安装 PostgreSQL：

```
sudo apt-get install -y postgresql

sudo apt-get install -y libpostgresql-jdbc-java
<!--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。根据正在使用的虚拟机管理程序平台做出以下更改。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，在每个半虚拟化的 Linux VM 中，您都会遇到 NTP 和 Citrix Hypervisor 的问题。两者都试图管理系统时钟。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。

如果您正在运行半虚拟化的 Linux 内核，并且安装了 Citrix VM Tools，则可以检查 Citrix Hypervisor 时间同步功能是否存在，以及是否已在 Linux VM 中启用：

```
su -
cat /proc/sys/xen/independent_wallclock
<!--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：

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

```
su -
cat /proc/sys/xen/independent_wallclock
<!--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，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

启用 VMware 时间同步功能后，在每个半虚拟化的 Linux VM 中，您都会遇到 NTP 和虚拟机管理程序的问题。两者都试图同步系统时钟。为避免时钟与其他服务器不同步，请确保每个 Linux 客户机中的系统时钟都与 NTP 同步。这种情况要求禁用主机时间同步。

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

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

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

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

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

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
<!--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：

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

> 注意：
>
> 确保 `winbind` 脚本位于 `/etc/init.d` 下。

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

> 注意：
>
> 根据您的 AD 基础结构配置 Kerberos。以下设置适用于单域、单林模型。

```
[libdefaults]
default_realm = REALM
dns_lookup_kdc = false
[realms]
REALM = {
admin_server = domain-controller-fqdn
```

```
kdc = domain-controller-fqdn
}
[domain_realm]
domain-dns-name = REALM
.domain-dns-name = REALM
```

此上下文中的 **domain-dns-name** 参数为 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　打开 **/etc/samba/smb.conf** 并配置以下设置：

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
encrypt passwords = yes
idmap config *:range = 16777216-33554431
winbind trusted domains only = no
kerberos method = secrets and keytab
winbind refresh tickets = yes
template shell = /bin/bash
```

**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: systemd winbind
group: systemd 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：

```
sudo net ads join REALM -U user
<!--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**

```
sudo systemctl restart winbind
<!--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：

```
sudo pam-auth-update
<!--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：

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

运行以下命令验证额外的域和计算机对象信息：

```
sudo net ads info
<!--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：

```
sudo klist -ke
<!--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：

```
sudo kinit -k MACHINE$@REALM
<!--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：

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

使用以下命令检查计算机的帐户详细信息：

```
sudo net ads status
<!--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：

```
wbinfo --krb5auth=domain\username%password
<!--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。

```
ssh localhost -l domain\username

id -u
<!--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：

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

验证用户的 Kerberos 凭据缓存中的票据是否有效且未过期：

```
klist
<!--NeedCopy-->
```

退出会话。

```
exit
<!--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，然后重试。

### Quest Authentication Service

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

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

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

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

### 在 **Linux VDA** 上配置 **Quest**

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

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

```
SELINUX=disabled
```

此更改要求重新启动计算机：

```
reboot
<!--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：

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
    interval 32400

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
    auth false
<!--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：

```
sudo /opt/quest/bin/vastool configure pam
sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

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

```
sudo /opt/quest/bin/vastool -u user join domain-name
<!--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：

```
sudo /opt/quest/bin/vastool info domain
<!--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。

```
ssh localhost -l domain\username

id -u
<!--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：

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

验证 Kerberos 凭据缓存中的票据是否有效且未过期：

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

退出会话。

```
exit
```

```
<!--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：

```
su -
adjoin -w -V -u user domain-name
<!--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：

```
su -

adinfo
<!--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：

```
adinfo --sysinfo all

adinfo --diag
<!--NeedCopy-->
```

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

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

在进行域加入验证后继续执行步骤 6：安装 Linux VDA。

### SSSD

配置 **Kerberos**　运行以下命令以安装 Kerberos：

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

要配置 Kerberos，请以 root 用户身份打开 **/etc/krb5.conf** 并配置以下参数：

> 注意：
>
> 根据您的 AD 基础结构配置 Kerberos。以下设置适用于单域、单林模型。

```
[libdefaults]
default_realm = REALM
dns_lookup_kdc = false
[realms]
REALM = {
admin_server = domain-controller-fqdn
kdc = domain-controller-fqdn
}
[domain_realm]
domain-dns-name = REALM
.domain-dns-name = REALM
```

此上下文中的 domain-dns-name 参数为 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：

- 如果您使用 **adcli** 加入域，请完成以下步骤：

1. 安装 **adcli**。

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

2. 通过 **adcli** 加入域。

   使用以下命令删除旧系统 keytab 文件并加入域：

```
su -

rm -rf /etc/krb5.keytab

```

```
adcli join domain-dns-name -U user -H hostname-fqdn
<!--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。

   运行 `sudo klist -ket` 命令以确保系统 keytab 文件已创建。

   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，请完成以下步骤：

1. 安装软件包。

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

2. 配置 **Samba**。

   打开 **/etc/samba/smb.conf** 并配置以下设置：

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
client signing = yes
client use spnego = yes
kerberos method = secrets and keytab
```

   **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。

```
sudo net ads join REALM -U user
<!--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：

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

如果已安装软件包，则建议进行更新：

```
sudo apt-get install --only-upgrade sssd
<!--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/sssd/sssd.conf** 配置文件，必须手动创建。以 root 用户身份创建或打开 **/etc/sssd/sssd.conf** 并配置以下设置：

```
[sssd]
services = nss, pam
config_file_version = 2
domains = domain-dns-name
[domain/domain-dns-name]
id_provider = ad
access_provider = ad
auth_provider = krb5
krb5_realm = REALM
# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer
than 14 days
krb5_renewable_lifetime = 14d
# Set krb5_renew_interval to lower value if TGT ticket lifetime is
shorter than 2 hours
krb5_renew_interval = 1h
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U
# This ldap_id_mapping setting is also the default value
ldap_id_mapping = true
override_homedir = /home/%d/%u
```

```
default_shell = /bin/bash

ad_gpo_map_remote_interactive = +ctxhdx
```

> 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。PAM 服务 ctxhdx 已添加到 ad_gpo_map_remote_interactive。
>
> 此上下文中的 **domain-dns-name** 参数为 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。
>
> 有关配置设置的信息，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：

```
sudo chmod 0600 /etc/sssd/sssd.conf
<!--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：

```
sudo systemctl start sssd

sudo systemctl enable sssd
<!--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：

```
sudo pam-auth-update
<!--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：

```
sudo klist -ke
<!--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：

```
sudo kinit -k MACHINE$@REALM
<!--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 已缓存：

```
sudo klist
<!--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。

```
ssh localhost -l domain\username

id -u

klist

exit
<!--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：

```
ls /tmp/krb5cc_uid
<!--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

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download
    /9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

使 **PBIS** 安装脚本可执行

```
sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

运行 **PBIS** 安装脚本

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--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：

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
<!--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：

```
/opt/pbis/bin/domainjoin-cli query
<!--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。

```
sudo ssh localhost -l domain\user

id -u
<!--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：

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

退出会话。

```
exit
<!--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 Runtime 6.0**

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 Runtime 6.0。

安装.NET Runtime 6.0 后，运行 **which dotnet** 命令查找您的运行时路径。

根据命令输出，设置.NET 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

1. 转至 Citrix Virtual Apps and Desktops 下载页面。
2. 展开适当版本的 Citrix Virtual Apps and Desktops。
3. 单击组件下载与您的 Linux 发行版匹配的 Linux VDA 软件包以及可用于验证 Linux VDA 软件包的完整性的 GPG 公钥。

   要验证 Linux VDA 软件包的完整性，请将公钥导入到 DEB 数据库中并运行以下命令：

   ```
   ```
   sudo apt-get install dpkg-sig
   gpg --import <path to the public key>
   dpkg-sig --verify <path to the Linux VDA package>
   <!--NeedCopy--> ```
   ```

### 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：

```
sudo dpkg -i xendesktopvda_<version>.debian10_amd64.deb
<!--NeedCopy-->
```

**Debian 11.3** 的依赖项列表：

```
postgresql >= 13

libpostgresql-jdbc-java >= 42.2

openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

ufw >= 0.36

```

 
```

```
desktop-base >= 10.0.2

libxrandr2 >= 2:1.5.1

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.33

gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.6.0

sed >= 4.7

cups >= 2.2

ghostscript >= 9.53~

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.7~

libpython3.9 >= 3.9~

libsasl2-modules-gssapi-mit >= 2.1.~

libqt5widgets5 >= 5.5~

mutter >= 3.38.6~

libqrencode4 >= 4.0.0

libimlib2 >= 1.5.1
<!--NeedCopy-->
```

**Debian 10.9** 的依赖项列表：

```
postgresql >= 11

libpostgresql-jdbc-java >= 42.2

openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

libgtkmm-3.0-1v5 >= 3.24.0

```

```
ufw >= 0.36

desktop-base >= 10.0.2

libxrandr2 >= 2:1.5.1

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.33

gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.6.0

sed >= 4.7

cups >= 2.2

ghostscript >= 9.27~

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.7~

libpython3.7 >= 3.7~

libsasl2-modules-gssapi-mit >= 2.1.~

libqt5widgets5 >= 5.5~

libqrencode4 >= 4.0.0

libimlib2 >= 1.5.1
<!--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。

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

> 注意：
>
> 升级现有安装将覆盖 /etc/xdl 下的配置文件。在进行升级之前，请务必备份这些文件。

### 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
- Nutanix AHV

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：

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

#### 提示配置

运行会提示各种问题的手动配置：

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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 VDA 服务。默认情况下设置为 Y。
- **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 打开所需的端口（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 Service
  - 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 ad2.mycompany.com:3268 ad3.mycompany.com:3268。如果将 LDAP 端口号指定为 389，Linux VDA 将在轮询模式下查询指定域中的每个 LDAP 服务器。如果有 x 个策略和 y 个 LDAP 服务器，Linux VDA 总共将执行 X 乘以 Y 次查询。如果轮询时间超过阈值，会话登录可能会失败。要启用更快的 LDAP 查询，请在域控制器上启用全局编录，并将相关的 LDAP 端口号指定为 3268。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。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。要与 FAS 服务器正确通信，请确保附加的端口号与在 FAS 服务器上指定的端口号一致，例如 CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'。
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** - 安装.NET Runtime 6.0 以支持新的 Broker 代理服务 (`ctxvda`) 的路径。默认路径为 /usr/bin。
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** –指定要在会话中使用的 GNOME 、GNOME Classic 或 MATE 桌面环境。如果未指定变量，则使用 VDA 上当前安装的桌面。但是，如果当前安装的桌面为 MATE，则必须将变量值设置为 **mate**。

  还可以通过完成以下步骤来更改目标会话用户的桌面环境：

  1. 在 VDA 上的 **$HOME/<username>** 目录下创建一个 `.xsession` 文件。
  2. 编辑 `.xsession` 文件以根据发行版指定桌面环境。
     - 对于 **MATE** 桌面

       ```
       MSESSION="$(type -p mate-session)"
       if [ -n "$MSESSION" ]; then
         exec mate-session
       fi
       ```

     - 适用于 **GNOME Classic** 桌面

       ```
       GSESSION="$(type -p gnome-session)"
       if [ -n "$GSESSION" ]; then
       export GNOME_SHELL_SESSION_MODE=classic
       exec gnome-session --session=gnome-classic
       fi
       ```

     - 对于 **GNOME** 桌面

       ```
       GSESSION="$(type -p gnome-session)"
       if [ -n "$GSESSION" ]; then
       exec gnome-session
       fi
       ```

  3. 与目标会话用户共享 700 文件权限。

  自版本 2209 起，会话用户可以自定义其桌面环境。必须提前在 VDA 上安装可切换的桌面环境，才能启用此功能。有关详细信息，请参阅按会话用户划分的自定义桌面环境。
- **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。
- **CTX_XDL_TELEMETRY_SOCKET_PORT** - 用于侦听 Citrix Scout 的套接字端口。默认端口为 7503。

- **CTX_XDL_TELEMETRY_PORT** - 用于与 Citrix Scout 通信的端口。默认端口为 7502。

设置环境变量并运行配置脚本：

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4|5

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
    none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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。

另外，您可以使用单个命令指定所有参数：

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

```

```
CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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：

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

删除配置更改：

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
<!--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：

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

查看更多详细信息：

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

要卸载 Linux VDA 软件，请执行以下操作：

```
dpkg -r xendesktopvda
<!--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**

请运行 `sudo /opt/Citrix/VDA/bin/xdping` 以检查 Linux VDA 环境存在的常见配置问题。有关详细信息，请参阅 XDPing。

### 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：

```
sudo systemctl start ctxhdx

sudo systemctl start ctxvda
<!--NeedCopy-->
```

停止 **Linux VDA**：

停止 Linux VDA 服务：

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
<!--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：

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

sudo systemctl restart ctxvda
<!--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：

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
<!--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 AD 用户和组已正确配置，能够登录到 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 2206。

## 在 **Citrix DaaS Standard for Azure** 中创建 **Linux VDA**

June 16, 2023

可以在 Citrix DaaS Standard for Azure（以前称为“适用于 Azure 的 Citrix Virtual Apps and Desktops Standard”）中创建已加入域和未加入域的 Linux VDA，以将虚拟应用程序和桌面从 Microsoft Azure 交付到任何设备。有关详细信息，请参阅 Citrix DaaS Standard for Azure。

### 支持的 **Linux** 发行版

以下 Linux 发行版支持此功能：

- RHEL 8.6
- RHEL 8.4
- Rocky Linux 8.6
- Ubuntu 22.04

- Ubuntu 20.04
- Ubuntu 18.04

步骤

要在 Citrix DaaS Standard for Azure 中创建 Linux VDA，请完成以下步骤：

1. 在 Azure 中准备主映像：

   > 注意：
   >
   > 此外，您还可以使用 Linux VDA 自助更新功能来计划软件自动更新。要实现此目标，请在主映像上的 etc/xdl/mcs/mcs_local_setting.reg 文件中添加命令行。
   > 例如，可以添加以下命令行：

   ```
   create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0x00000001" -force

   create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "Immediately" -force

   create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-Container-Url>" -force

   create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local-Certificate-Path-of-PortalAzureCom>" --force
   <!--NeedCopy-->
   ```

   a) 在 Azure 中，创建支持的发行版的 Linux VM。

   b) 如有必要，请在 Linux VM 上安装桌面环境。

   c) 在 VM 上，根据 https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers 上的说明安装.NET Runtime 6.0。

   d)（仅限 Ubuntu）在 `/etc/network/interfaces` 文件中添加 `source /etc/network/interfaces.d/*` 行。

   e)（仅限 Ubuntu）请将 `/etc/resolv.conf` 指向 `/run/systemd/resolve/resolv.conf`，而非将其指向 `/run/systemd/resolve/stub-resolv.conf`：

   ```
   unlink /etc/resolv.conf

   ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
   <!--NeedCopy-->
   ```

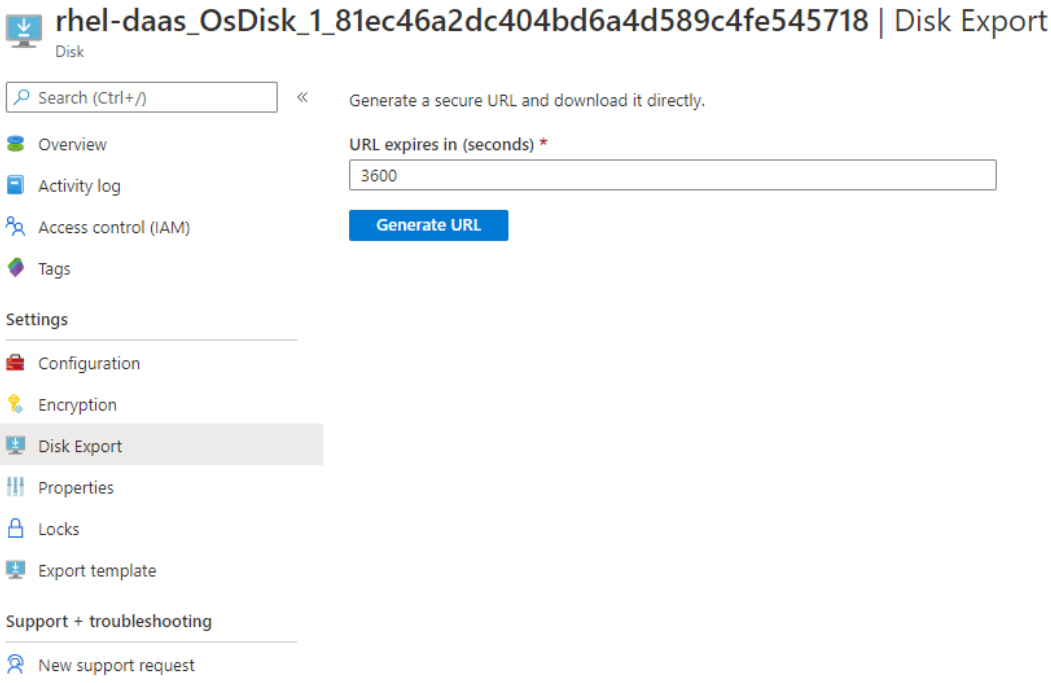
f) 安装 Linux VDA 软件包。

g) 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。

> 注意：
>
> 请将 dns 变量保留为未指定。
> 如果在创建计算机目录时选择静态或随机类型，请设置 `VDI_MODE=Y`。

h) 运行 `/opt/Citrix/VDA/sbin/deploymcs.sh`。

i) 在 Azure 中，停止（或取消分配）VM。单击磁盘导出为虚拟硬盘 (VHD) 文件生成 SAS URL，您可以将该文件用作主映像来创建其他 VM。




j)（可选）在主映像上配置组策略设置。您可以使用 `ctxreg` 工具来配置组策略设置。例如，以下命令将为 PDF 打印启用自动创建 **PDF** 通用打印机策略。

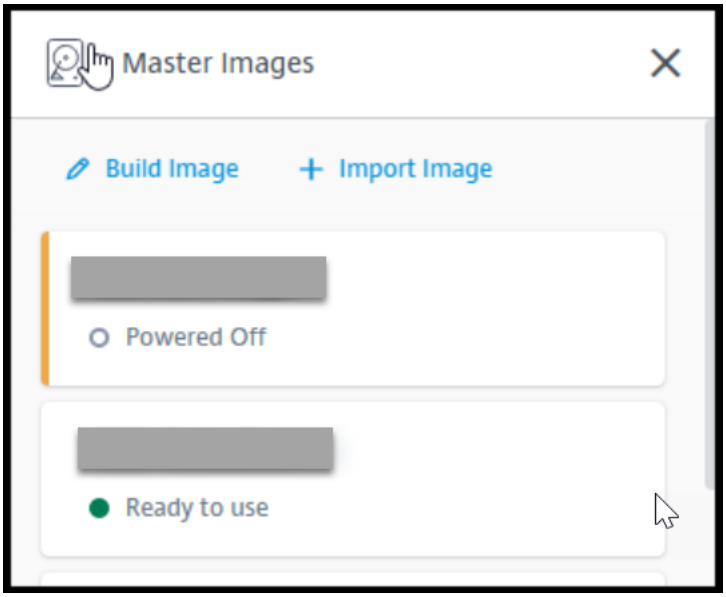
```
1    /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
        GroupPolicy\Defaults\PrintingPolicies" -t "REG_DWORD" -v
         "AutoCreatePDFPrinter" -d "0x00000001"  - force
2    <!--NeedCopy-->
```

2. 从 Azure 导入主映像。

a) 在管理控制板中，展开右侧的主映像。显示内容将列出 Citrix 提供的主映像以及您创建和导入的映像。

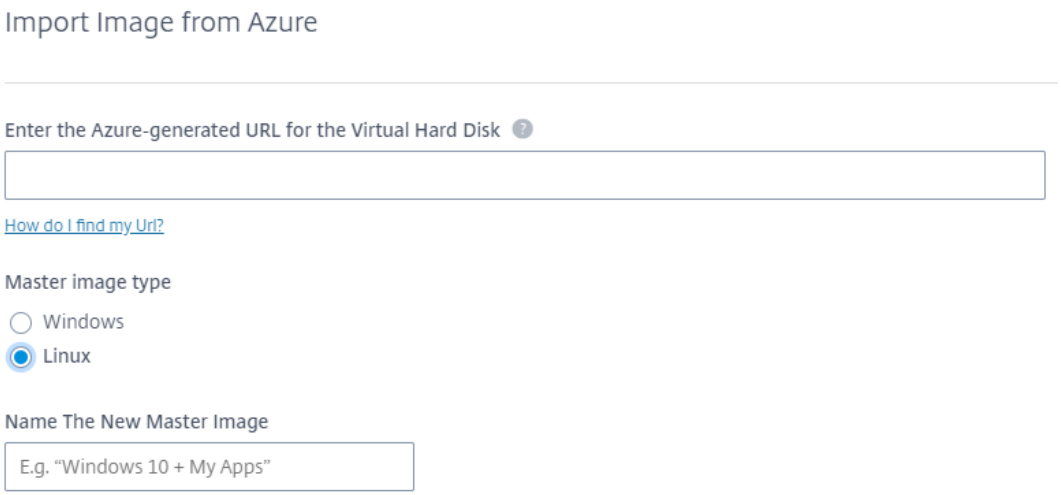
提示：此服务的大多数管理员活动都通过管理和监视控制板进行管理。创建第一个目录后，管理控制板将在登录到 Citrix Cloud 并选择 **Managed Desktops**（托管桌面）服务后自动启动。




b) 单击导入映像。

c) 输入您在 Azure 中生成的 VHD 文件的 SAS URL。选择 **Linux** 作为主映像类型。




d) 按照向导中的说明完成导入主映像的操作。

3. 创建计算机目录。

访问管理控制板，然后单击创建目录。创建计算机目录时，请选择之前创建的主映像。

> 注意：
>
> 用作主映像的 VM 无法通过 SSH 或 RDP 访问。要访问 VM，请使用 Azure 门户中的串行控制台。

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

January 4, 2024

支持的发行版

| | Winbind | SSSD | Centrify | PBIS |
|---|---|---|---|---|
| Debian 11.3、Debian 10.9 | 是 | 是 | 否 | 是 |
| RHEL 8.6、RHEL 8.4 | 是 | 否 | 是 | 是 |
| Rocky Linux 8.6 | 是 | 否 | 否 | 否 |
| RHEL 7.9、CentOS 7.9 | 是 | 是 | 是 | 是 |
| SUSE 15.3 | 是 | 是 | 否 | 是 |
| Ubuntu 22.04、Ubuntu 20.04、Ubuntu 18.04 | 是 | 是 | 否 | 是 |

受支持的虚拟机管理程序

- AWS
- Citrix Hypervisor
- GCP
- Microsoft Azure
- Nutanix AHV
- 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** 创建 **Linux VM**

> 注意：
>
> 自 Citrix Virtual Apps and Desktops 7 2003 到 Citrix Virtual Apps and Desktops 7 2112，只有 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）支持在 Microsoft Azure、AWS 和 GCP 上托管 Linux VDA。自 2203 版起，您可以在这些公有云上为 Citrix DaaS 和 Citrix Virtual Apps and Desktops 托

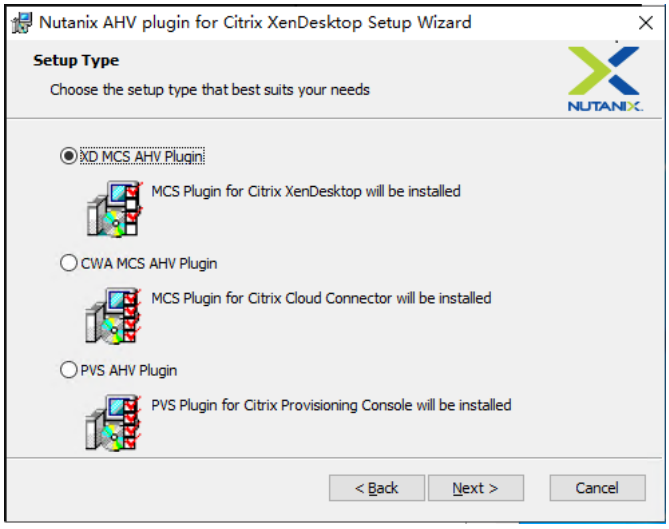
 

> 管 Linux VDA。要将这些公有云主机连接添加到 Citrix Virtual Apps and Desktops 部署，您需要混合权限许可证。有关混合权限许可证的信息，请参阅使用混合权限转换和升级换购 (TTU)。
>
> 不支持将裸机服务器与 MCS 结合使用以创建虚拟机。
>
> 如果您使用 PBIS 或 Centrify 将 MCS 创建的计算机加入到 Windows 域，请完成以下任务：
>
> - 在模板计算机上，在 `/etc/xdl/mcs/mcs.conf` 文件中配置 PBIS 或 Centrify 软件包下载路径或直接安装 PBIS 或 Centrify 软件包。
> - 在运行 `/opt/Citrix/VDA/sbin/deploymcs.sh` 之前，请创建一个组织单位 (OU)，该组织单位对其所有从属 MCS 创建的计算机具有写入和密码重置权限。
> - 在 `/opt/Citrix/VDA/sbin/deploymcs.sh` 完成运行后重新启动 MCS 创建的计算机之前，请根据您的部署在 Delivery Controller 或 Citrix Cloud Connector 上运行 `klist -li 0x3e4 purge`。

（仅限 **Nutanix**）步骤 **1**：安装并注册 **Nutanix AHV** 插件

从 Nutanix 中获取 Nutanix AHV 插件包。在您的 Citrix Virtual Apps and Desktops 环境中安装并注册该插件。有关详细信息，请参阅 Nutanix 支持门户中提供的《Nutanix Acropolis MCS Plugin Installation Guide》（Nutanix Acropolis MCS 插件安装指南）。

步骤 **1a**：为本地 **Delivery Controller** 安装并注册 **Nutanix AHV** 插件　安装 Citrix Virtual Apps and Desktops 后，选择并在 Delivery Controller 上安装 **XD MCS AHV** 插件。




步骤 **1b**：为云端 **Delivery Controller** 安装并注册 **Nutanix AHV** 插件　选择并安装适用于 Citrix Cloud Connector 的 **CWA MCS AHV** 插件。在向 Citrix Cloud 租户注册的所有 Citrix Cloud Connector 上安装插件。即使 Citrix Cloud Connector 在没有 AHV 的情况下提供资源位置，也必须注册 Citrix Cloud Connector。

步骤 **1c**：安装插件后完成以下步骤

- 验证是否在`C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreati\v1.0.0.0`中创建了 Nutanix Acropolis 文件夹。
- 运行`"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe"-PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"`命令。
- 在本地 Delivery Controller 上重新启动 Citrix Host Service、Citrix Broker Service 和 Citrix Machine Creation Service，或者在 Citrix Cloud Connector 上重新启动 Citrix RemoteHCLServer Service。

  > 提示：
  >
  > 我们建议您在安装或更新 Nutanix AHV 插件时停止并重新启动 Citrix Host Service、Citrix Broker Service 和 Machine Creation Service。

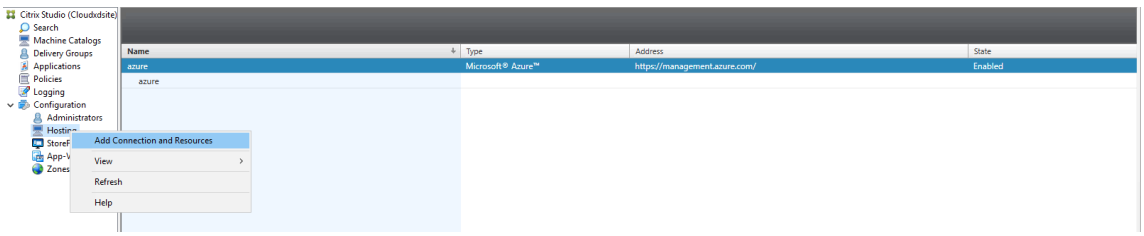
步骤 **2**：创建主机连接

本部分内容将指导您创建与 Azure、AWS、GCP、Nutanix AHV 和 VMware vSphere 的托管连接：

- 在 Citrix Studio 中创建与 Azure 的托管连接
- 在 Citrix Studio 中创建与 AWS 的托管连接
- 在 Citrix Studio 中创建与 GCP 的托管连接
- 在 Citrix Studio 中创建与 Nutanix 的托管连接
- 在 Citrix Studio 中创建与 VMware 的托管连接

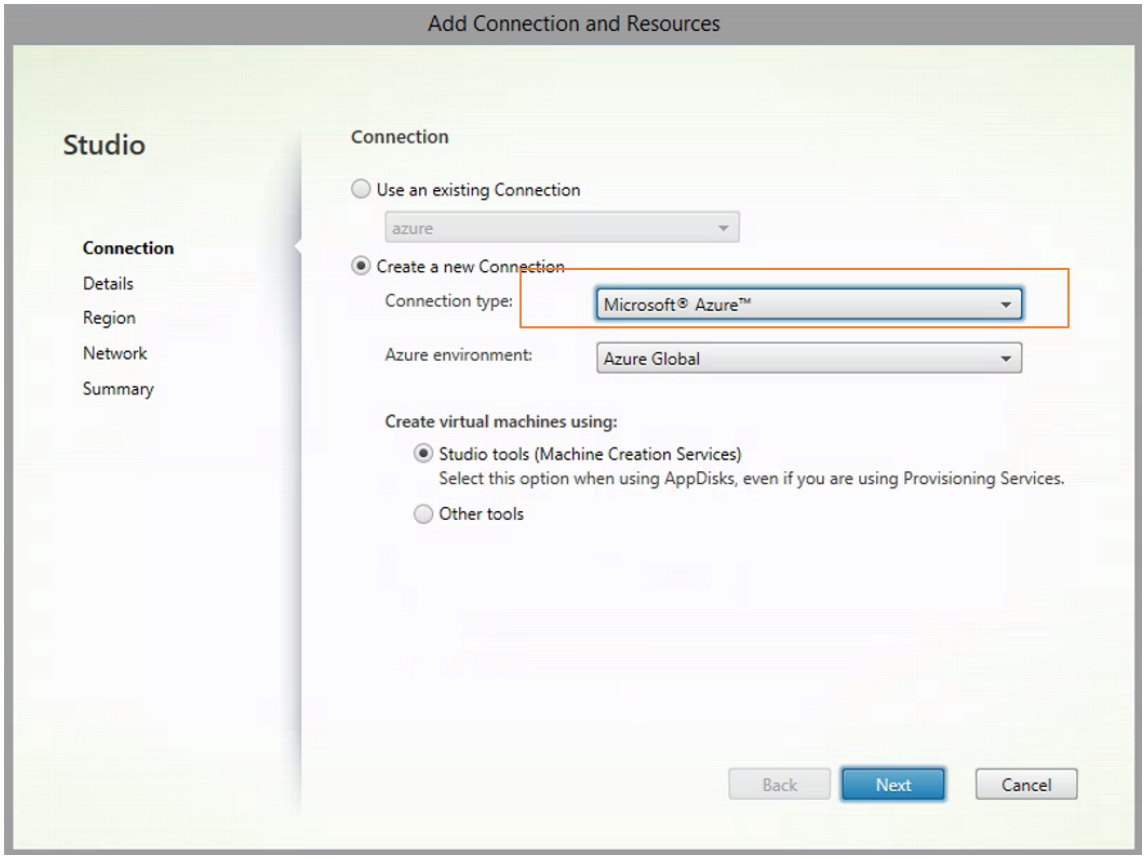
在 **Citrix Studio** 中创建与 **Azure** 的托管连接

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



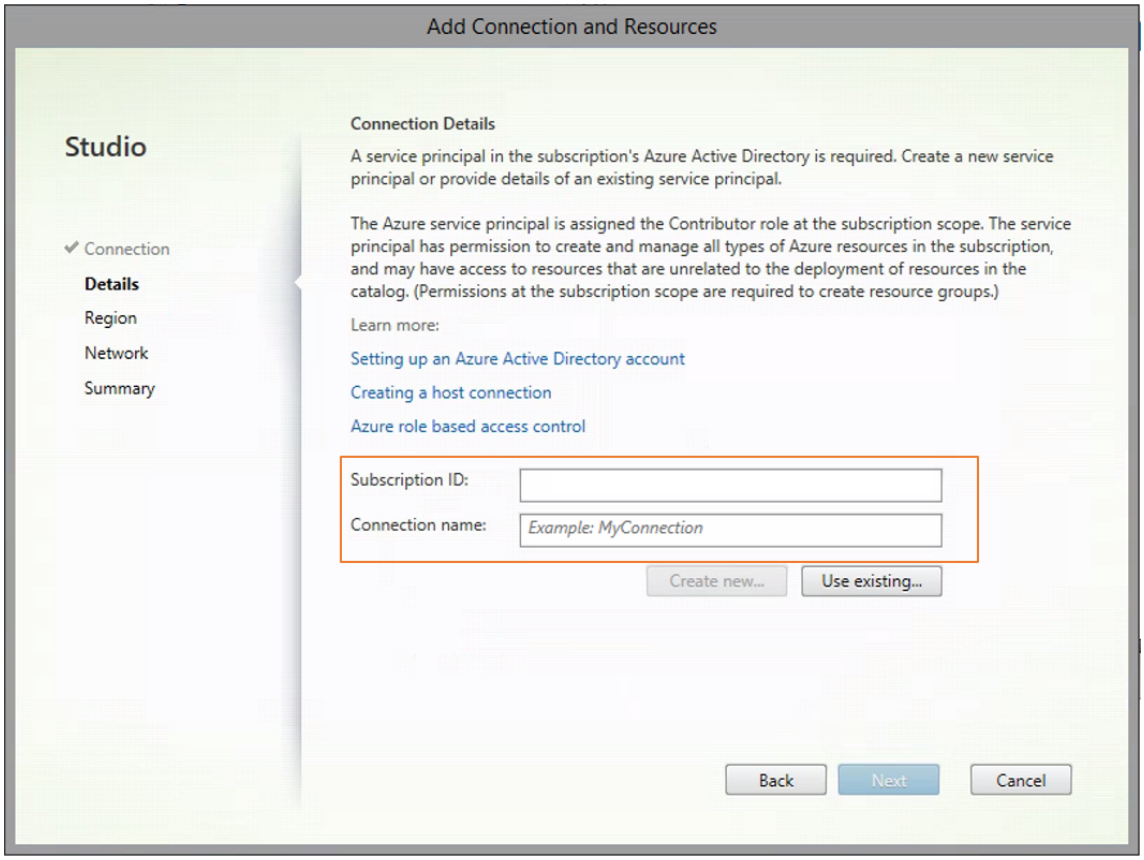

2. 选择连接类型 Microsoft Azure。

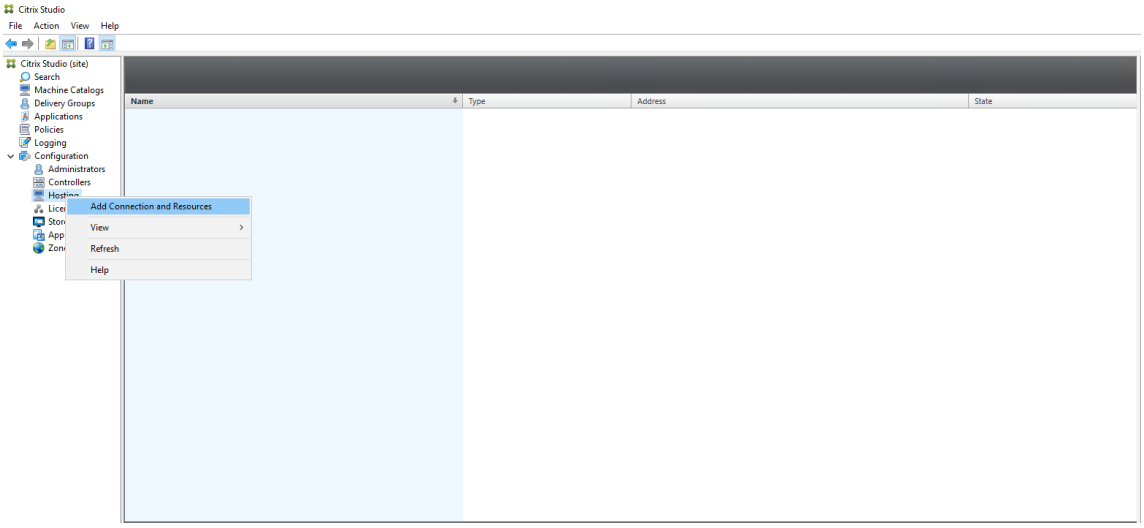



3. 键入您的 Azure 帐户的订阅 ID，然后键入您的连接名称。



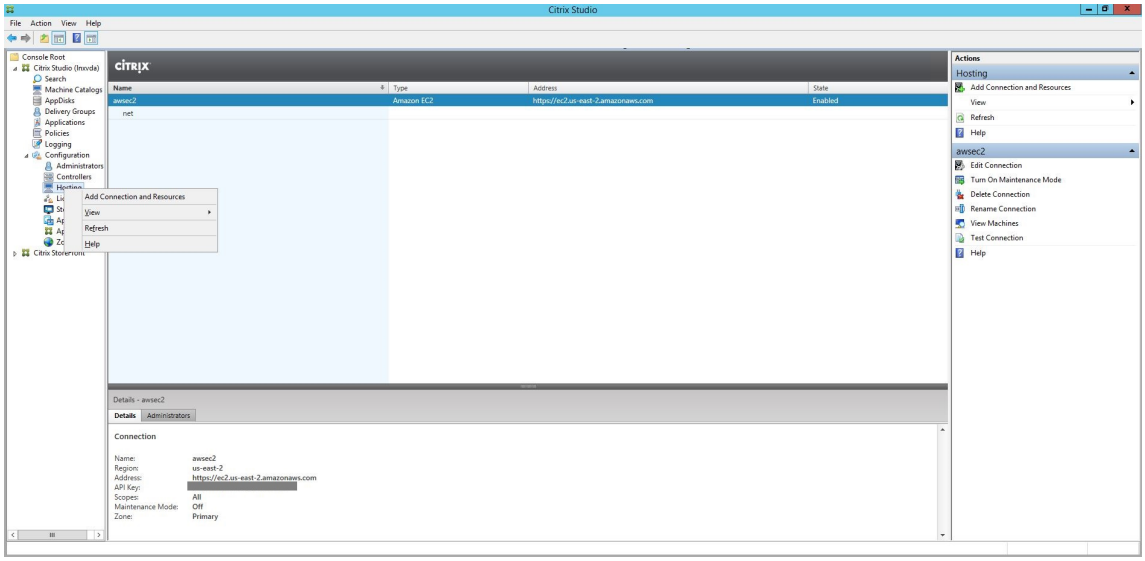

将在托管窗格中显示一个新连接。



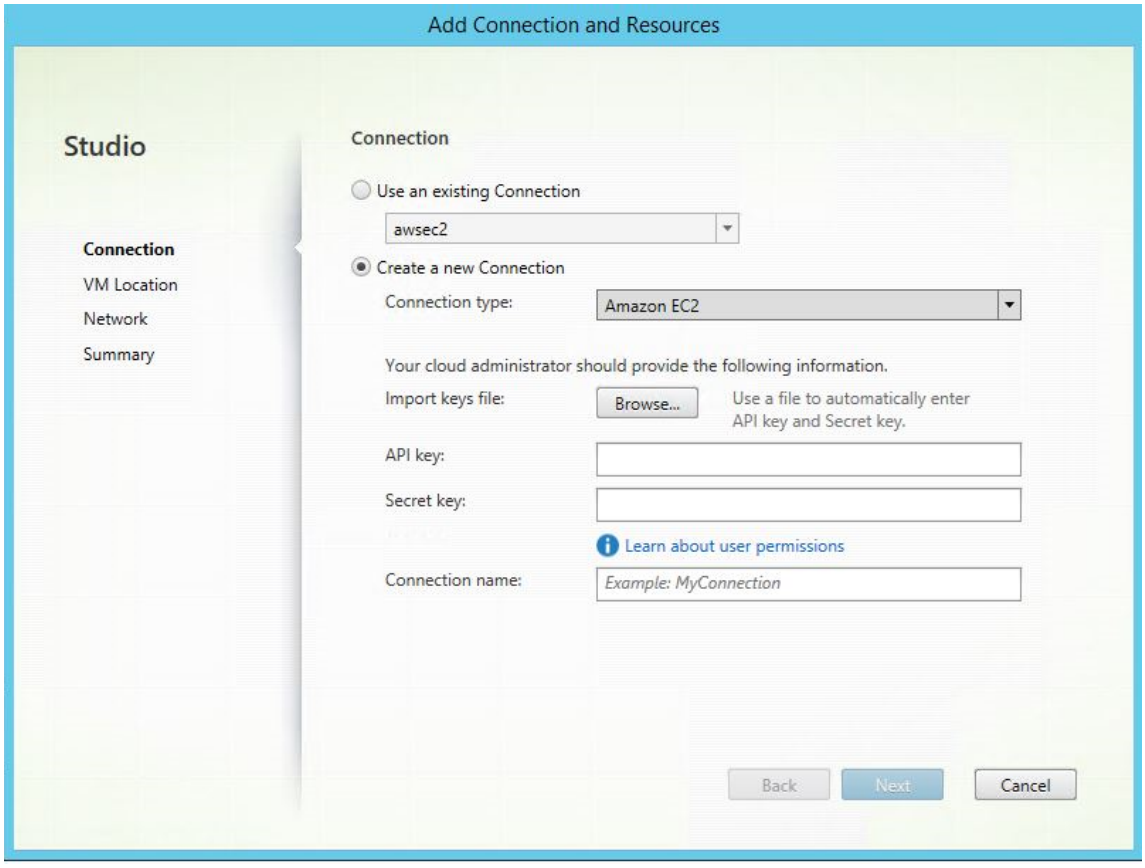

在 **Citrix Studio** 中创建与 **AWS** 的托管连接

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

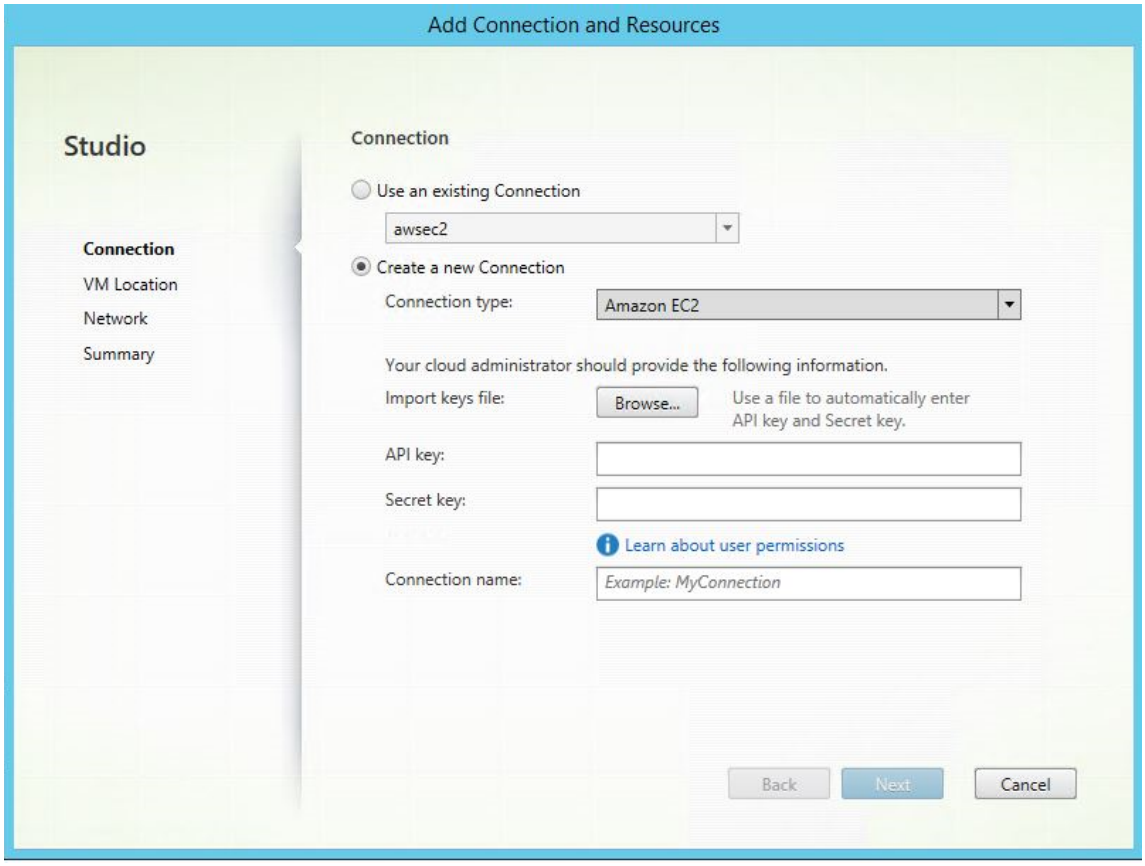



2. 选择 **Amazon EC2** 作为连接类型。




3. 键入 AWS 帐户的 API 密钥和密钥，然后键入您的连接名称。

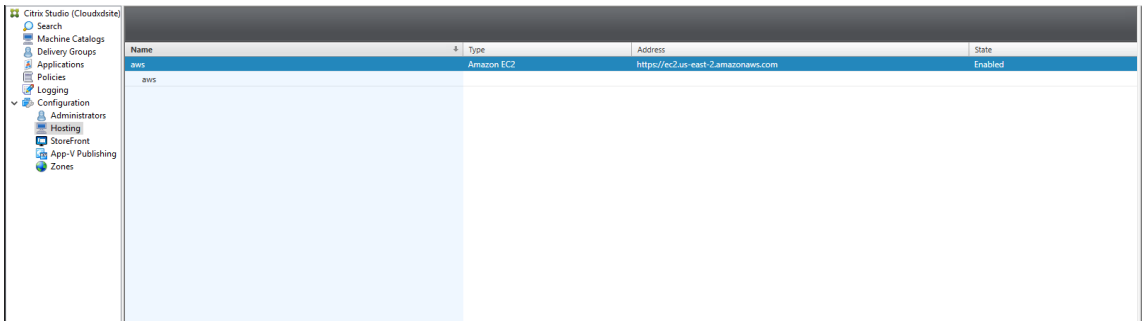
 




**API** 密钥是您的访问密钥 ID，密钥是您的秘密访问密钥。这些密钥被视为访问密钥对。如果您丢失了秘密访问密钥，则可以删除该访问密钥并创建另一个访问密钥。要创建访问密钥，请执行以下操作：

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。

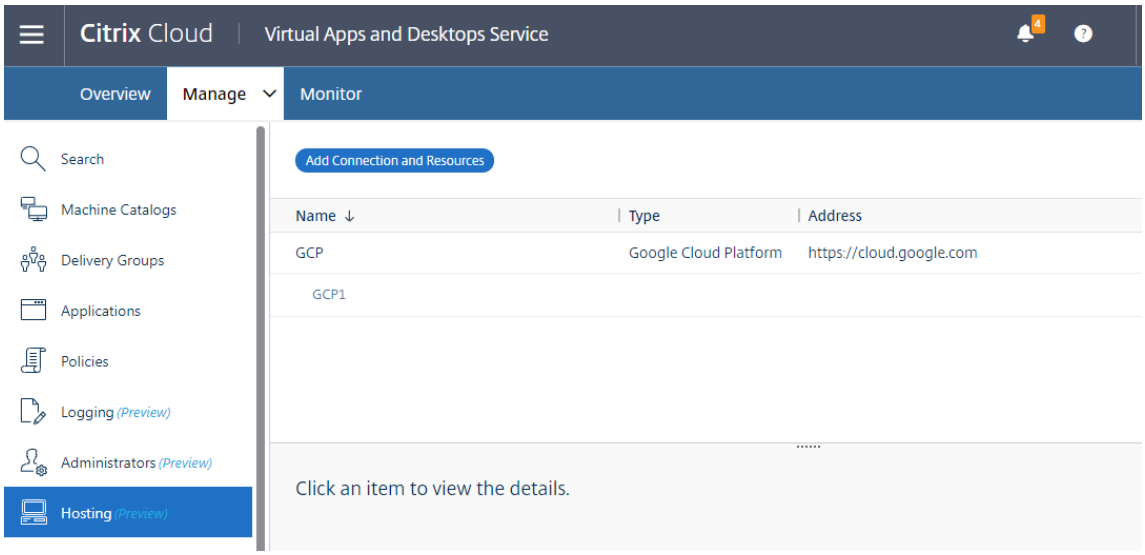
将在托管窗格中显示一个新连接。



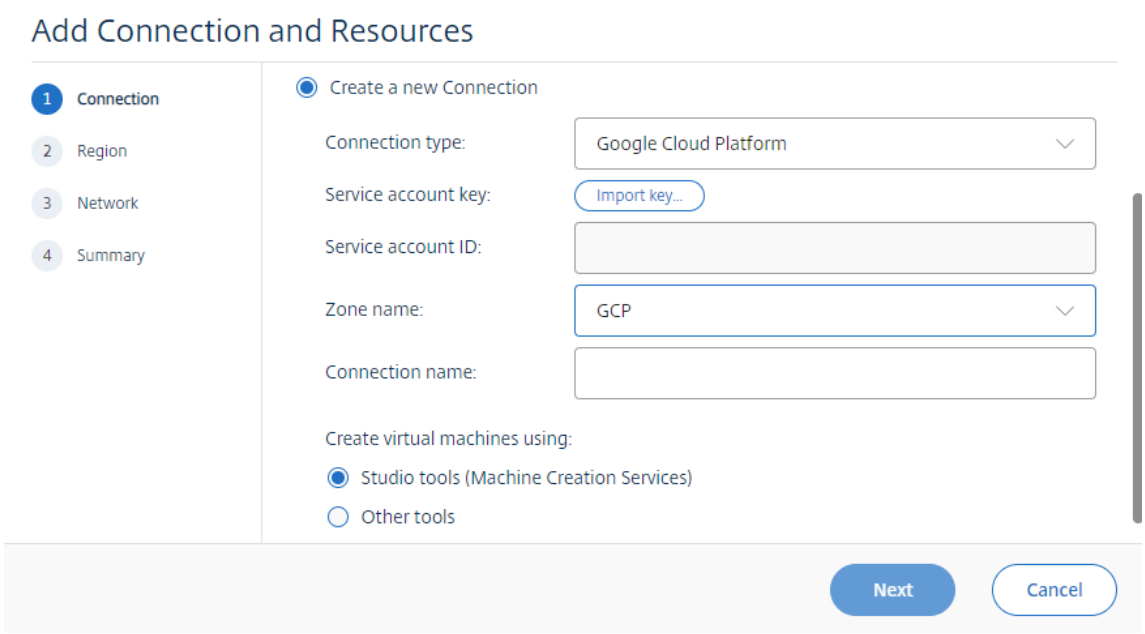

 

在 **Citrix Studio** 中创建与 **GCP** 的托管连接　根据 Google 云端平台虚拟化环境设置您的 GCP 环境，然后完成以下步骤以创建与 GCP 的托管连接。

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

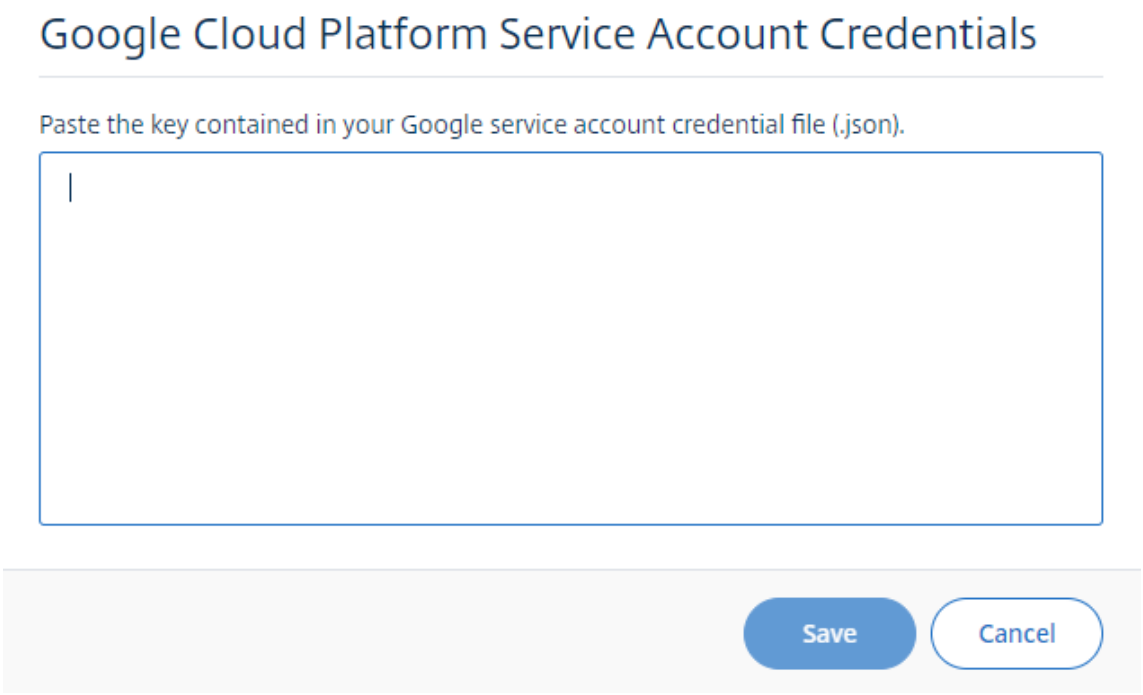



2. 选择 **Google Cloud Platform**（Google 云端平台）作为连接类型。

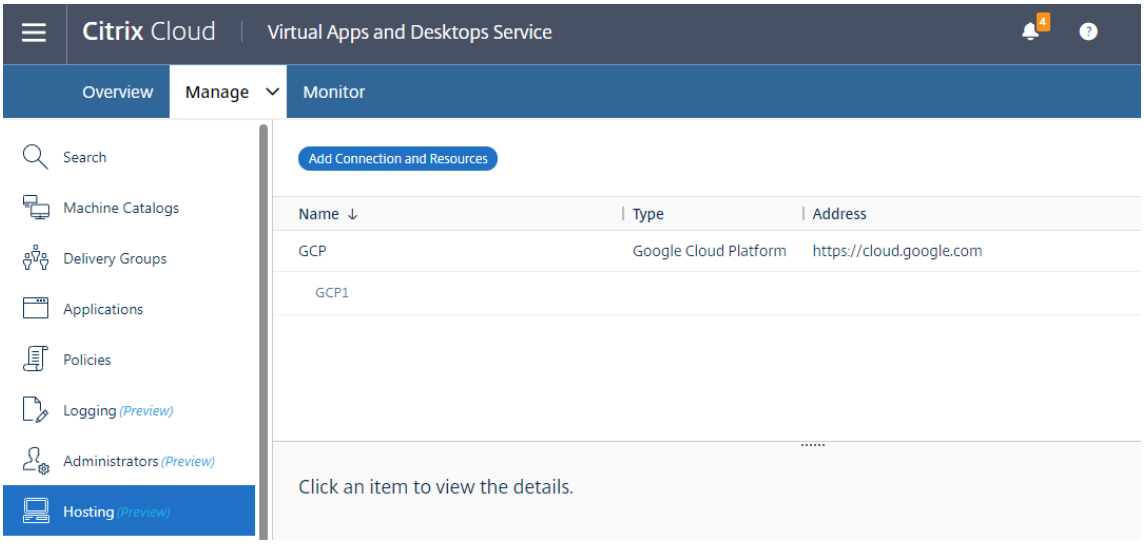



3. 导入 GCP 帐户的服务帐号密钥并键入连接名称。




将在托管窗格中显示一个新连接。

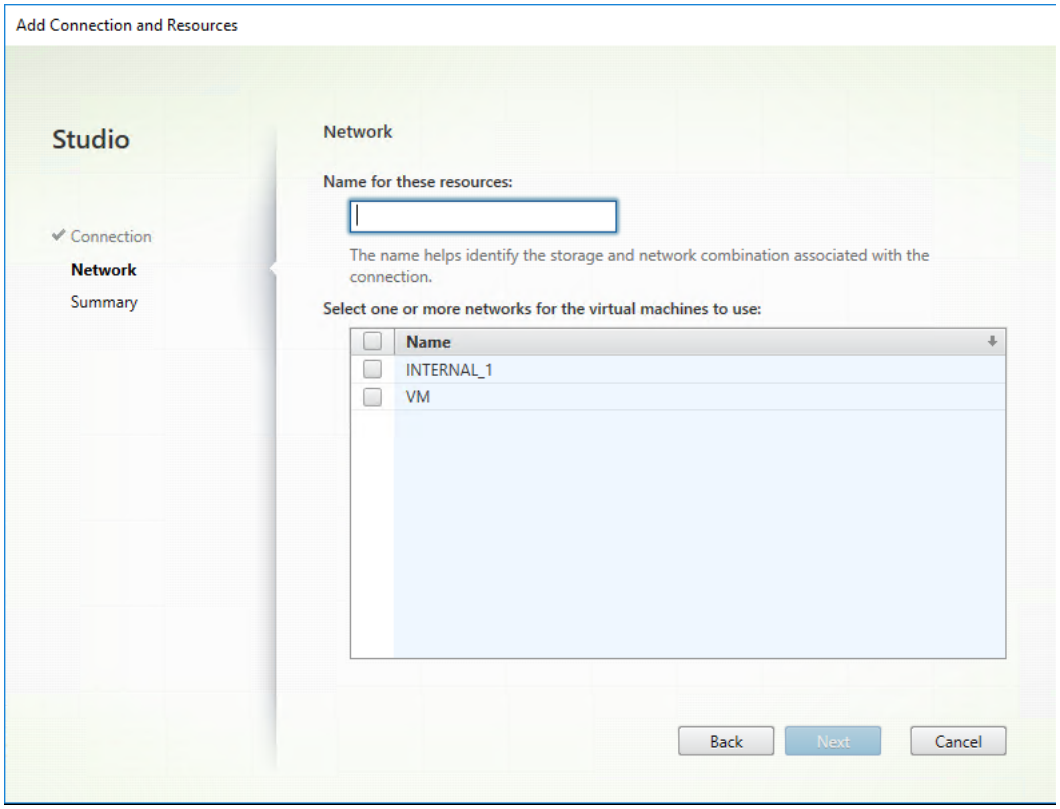



在 **Citrix Studio** 中创建与 **Nutanix** 的托管连接

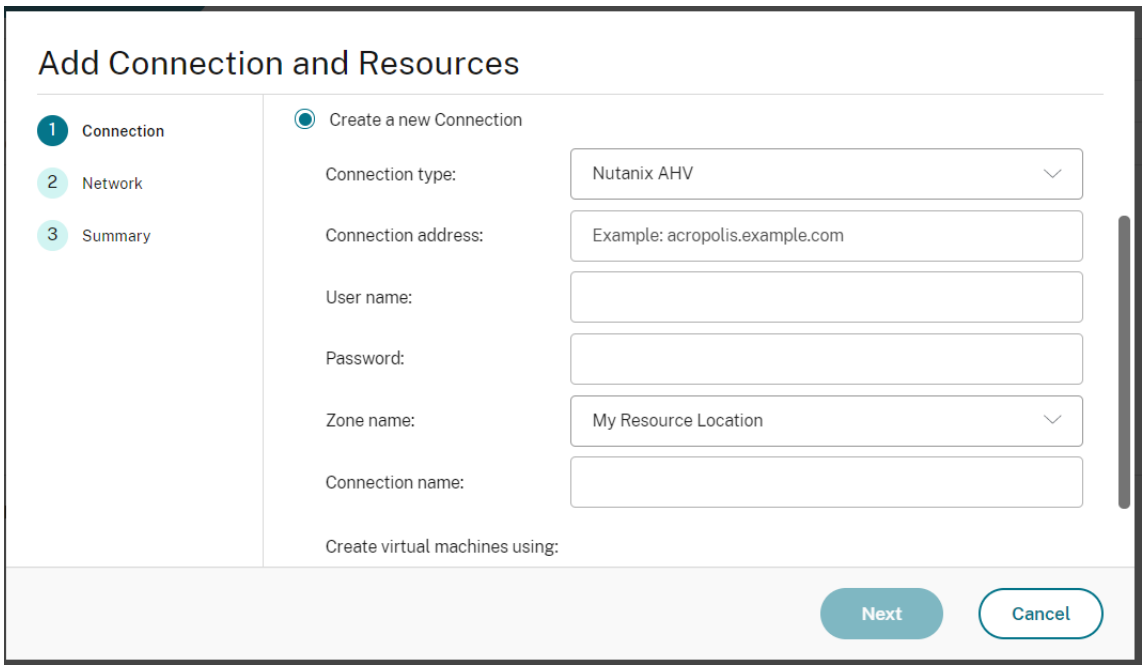
1. 对于本地 Delivery Controller，请在本地 Citrix Studio 中选择配置 **>** 托管 **>** 添加连接和资源。对于云 Delivery Controller，请在 Citrix Cloud 上的基于 Web 的 Studio 控制台中选择管理 **>** 托管 **>** 添加连接和资源，以创建与 Nutanix 虚拟机管理程序的连接。
2. 在添加连接和资源向导中的连接页面上选择 Nutanix AHV 作为连接类型，然后指定虚拟机管理程序地址、凭据以及连接名称。在网络页面上，选择用于托管单元的网络。

例如，在本地 Citrix Studio 中：




例如，在 Citrix Cloud 上的基于 Web 的 Studio 控制台中：

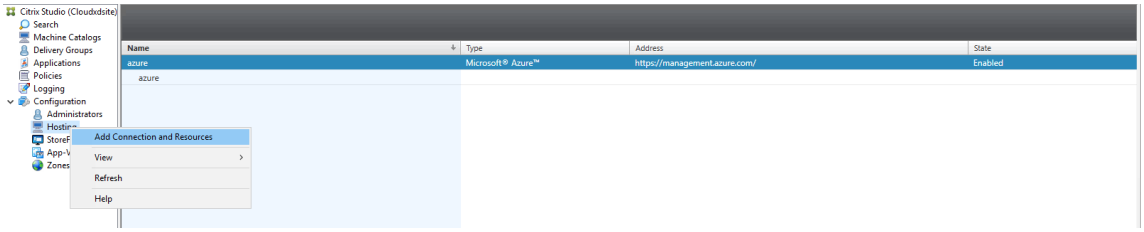



3. 在网络页面上，选择用于托管单元的网络。

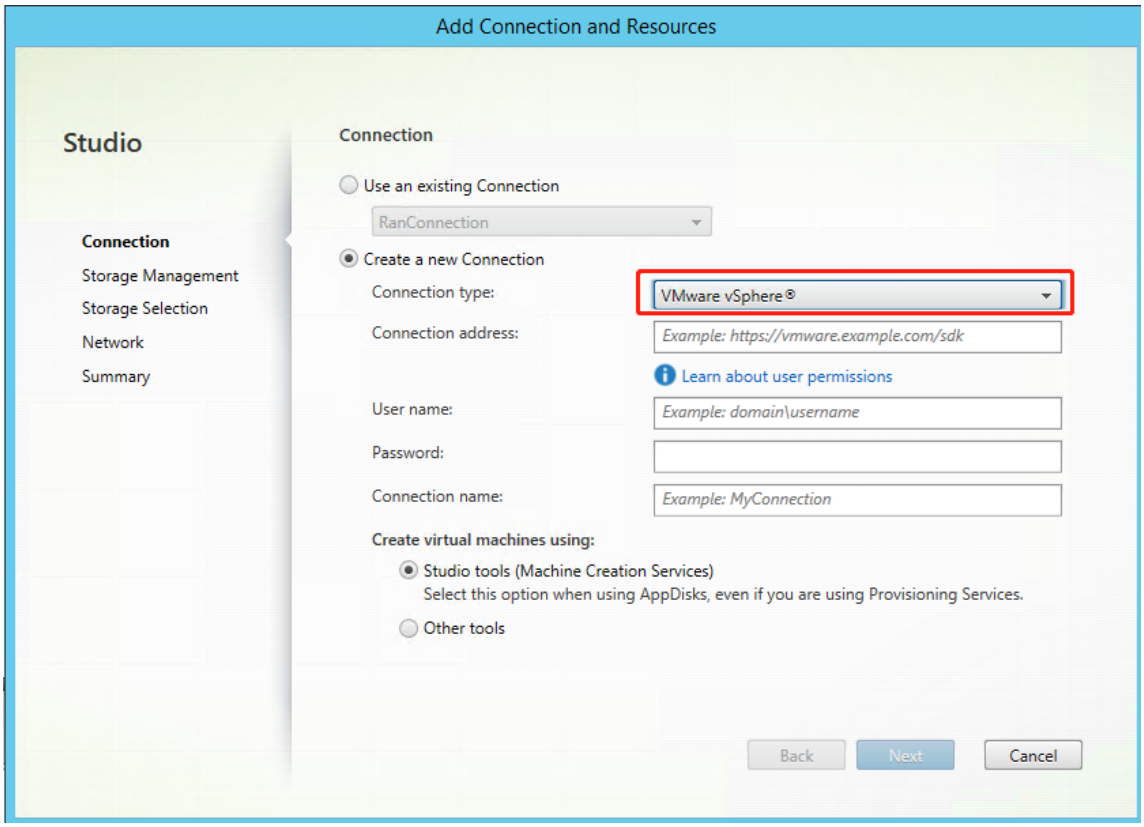
 

在 **Citrix Studio** 中创建与 **VMware** 的托管连接

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。

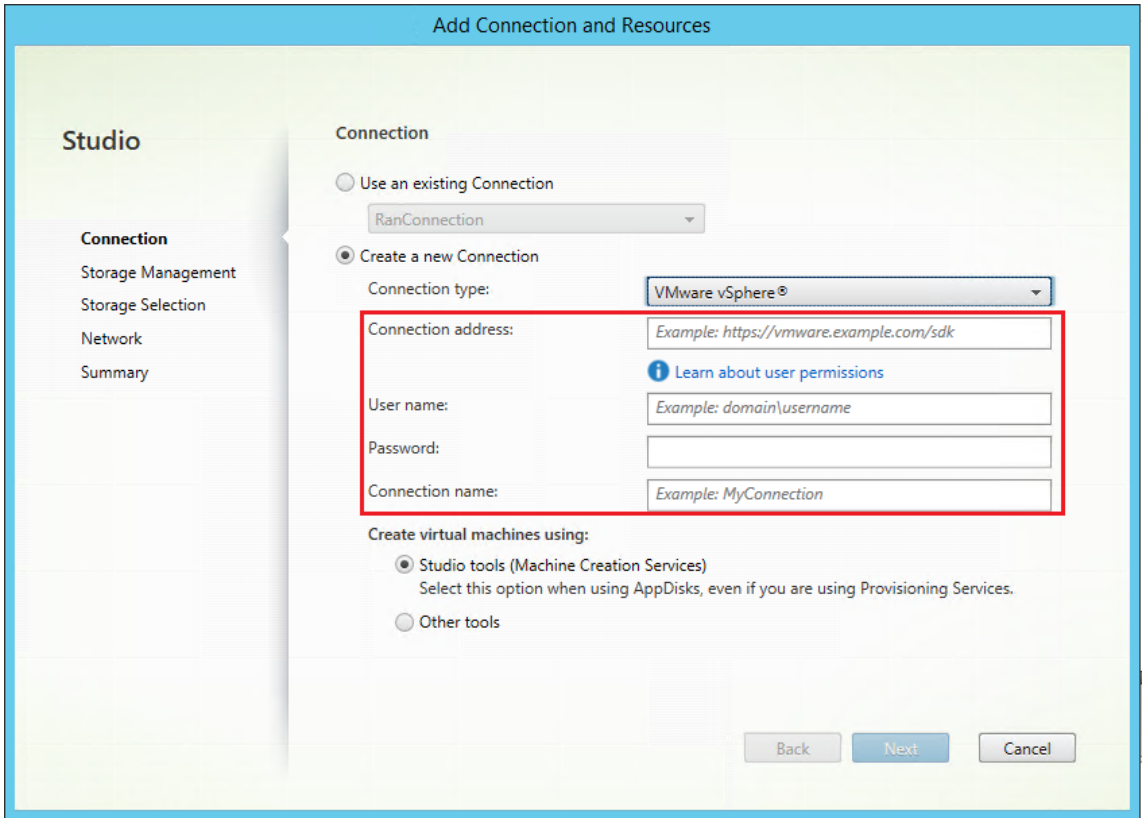



3. 选择 VMware vSphere 作为连接类型。

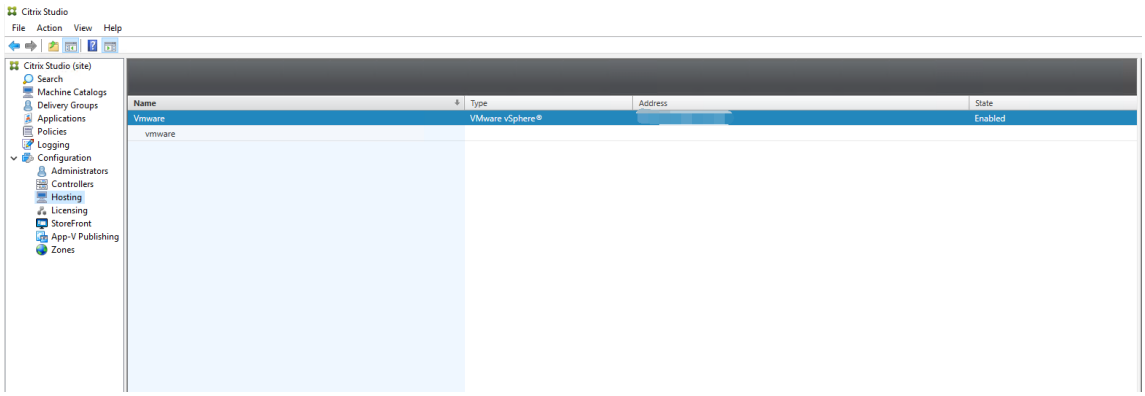



4. 键入 VMware 帐户的连接地址 (vCenter Server URL)、您的用户名和密码以及连接名称。




将在托管窗格中显示一个新连接。




步骤 **3**：准备主映像

（仅限 **Citrix Hypervisor**）步骤 **3a**：安装 **Citrix VM Tools**　在模板 VM 上安装 Citrix VM Tools，以使每个 VM 都使用 xe CLI 或 XenCenter。除非安装这些工具，否则 VM 的性能可能会很慢。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。

```
sudo mount /dev/cdrom /mnt
<!--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/Rocky Linux**:

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

   对于 **Ubuntu/Debian**:

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

   对于 **SUSE**:

```
sudo rpm -i /mnt/Linux/xe-guest-utilities_{
 package-version }
 _all.rpm
<!--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。

（适用于 **Azure**、**AWS** 和 **GCP**）步骤 **3b**：为 **Ubuntu 18.04** 配置 **cloud-init**

1. 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：

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

   确认在 /etc/cloud/cloud.cfg 文件中的 **system_info** 部分下存在以下行：

```
system_info:
   network:
       renderers: ['netplan', 'eni', 'sysconfig']
<!--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）。

```
users:
- default
<!--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：

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

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

步骤 **3c**：在模板 **VM** 上安装 **Linux VDA** 软件包

> 注意：
>
> 要使用当前正在运行的 VDA 作为模板 VM，请跳过此步骤。
>
> 在模板 VM 上安装 Linux VDA 软件包之前，请安装.NET Runtime 6.0。

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/Rocky Linux**：

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

> 注意：
>
> 对于 RHEL 和 CentOS，请先安装 EPEL 存储库，然后才能成功安装 Linux VDA 并运行 `deploymcs.sh`。有关如何安装 EPEL 的信息，请参阅 https://docs.fedoraproject.org/en-US/epel/ 上提供的说明。

对于 **Ubuntu/Debian**：

```
sudo dpkg -i <PATH>/<Linux VDA DEB>

apt-get install -f
<!--NeedCopy-->
```

对于 **SUSE**：

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

步骤 **3d**：启用存储库以安装 **tdb-tools** 软件包　对于 **RHEL 7** 服务器：

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

对于 **RHEL 7** 工作站：

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

步骤 **3e**：（在 **SUSE** 上）手动安装 **ntfs-3g**　在 SUSE 平台上，所有存储库都不提供 ntfs-3g。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：

   ```
   sudo zypper install gcc
   sudo zypper install make
   <!--NeedCopy-->
   ```

2. 下载 ntfs-3g 软件包。

3. 解压缩 ntfs-3g 软件包：

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

4. 输入 ntfs-3g 软件包的路径：

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

5. 安装 ntfs-3g：

   ```
   ./configure
   make
   make install
   <!--NeedCopy-->
   ```

步骤 **3f**：编辑 **MCS** 配置文件

1. 更改 `/etc/xdl/mcs/mcs.conf` 中的变量。

   - 适用于未加入域的场景

     对于未加入域的场景，可以将 `/etc/xdl/mcs/mcs.conf` 中的变量保留为未指定或者根据需要更改以下变量：

     `DOTNET_RUNTIME_PATH`=**path-to-install-dotnet-runtime **
     `DESKTOP_ENVIRONMENT`= **gnome | mate **

```
VDA_PORT=port-number
REGISTER_SERVICE=Y | N
ADD_FIREWALL_RULES=Y | N
HDX_3D_PRO=Y | N
VDI_MODE=Y | N
SITE_NAME=dns-site-name | '<none>'
SEARCH_BASE=search-base-set | '<none>'
START_SERVICE=Y | N
TELEMETRY_SOCKET_PORT=port-number
TELEMETRY_PORT=port-number
```

- 适用于已加入域的场景

  更改 /etc/xdl/mcs/mcs.conf 中的变量。mcs.conf 配置文件提供用于设置 MCS 和 Linux VDA 的变量。下面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 AD 相关配置文件(/etc/krb5.conf、/etc/sssd.conf 和 /etc/samba/smb.conf)。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，这意味着主映像上的配置模板负责确定 MCS 创建的计算机上的配置文件。
  - dns：设置每个 DNS 服务器的 IP 地址。您最多可以设置四个 DNS 服务器。
  - NTP_SERVER：设置 NTP 服务器的 IP 地址。除非另行说明，否则该地址是您的域控制器的 IP 地址。
  - WORKGROUP：将工作组名称设置为您在 AD 中配置的 NetBIOS 名称（区分大小写）。否则，MCS 将使用域名中紧随计算机主机名之后的部分作为工作组名称。例如，如果计算机帐户为 **user1.lvda.citrix.com**，MCS 将使用 **lvda** 作为工作组名称，而 **citrix** 是正确的选择。请务必正确设置工作组名称。
  - AD_INTEGRATION：设置 Winbind、SSSD、PBIS 或 Centrify。有关 MSC 支持的 Linux 发行版和域加入方法的列表，请参阅本文中的支持的发行版。
  - CENTRIFY_DOWNLOAD_PATH：设置下载 Server Suite Free（以前称为 Centrify Express）软件包的路径。只有将 AD_INTEGRATION 变量设置为 Centrify 时，该值才会生效。
  - CENTRIFY_SAMBA_DOWNLOAD_PATH：设置下载 Centrify Samba 软件包的路径。只有将 AD_INTEGRATION 变量设置为 Centrify 时，该值才会生效。
  - PBIS_DOWNLOAD_PATH：设置下载 PBIS 软件包的路径。只有将 AD_INTEGRATION 变量设置为 PBIS 时，该值才会生效。
  - UPDATE_MACHINE_PW：启用或禁用自动更新计算机帐户密码。有关详细信息，请参阅自动更新计算机帐户密码。

- 下列 Linux VDA 配置变量：

  DOTNET_RUNTIME_PATH=**path-to-install-dotnet-runtime **
  DESKTOP_ENVIRONMENT= **gnome | mate **
  SUPPORT_DDC_AS_CNAME=**Y | N**
  VDA_PORT=**port-number**
  REGISTER_SERVICE=**Y | N**
  ADD_FIREWALL_RULES=**Y | N**
  HDX_3D_PRO=**Y | N**
  VDI_MODE=**Y | N**
  SITE_NAME=**dns-site-name |** '**<none>**'
  LDAP_LIST= '**list-ldap-servers**' | '**<none>**'
  SEARCH_BASE=**search-base-set |** '**<none>**'
  FAS_LIST= '**list-fas-servers**' | '**<none>**'
  START_SERVICE=**Y | N**
  TELEMETRY_SOCKET_PORT=**port-number**
  TELEMETRY_PORT=**port-number**

有关 `mcs.conf` 的示例，请参见下面的屏幕截图。

```
#!/bin/bash

#============================================================================
#
# Citrix Virtual Apps & Desktops For Linux Script: Machine Creation Service
# Copyright (c) Citrix Systems, Inc. All Rights Reserved.
#
# This is the configuration file for mcs scripts.


#########################Template machine check#################################
# If unspecified, the value is N by default, meaning that mcs configuration templates will overwrite configuration items
# If you choose Y, MCS created VMs will use the existing configurations of the current VDA that must running correctly
Use_Existing_Configurations_Of_Current_VDA=N

#########################DNS Configuration######################################
# Provide DNS information
# You can provide 4 DNS servers at most.
# Leave empty if you do not have 4 servers. You may also leave all of them empty
# and configure dns manually.
# Format:
# dns1="xx.xx.xx.xx"
# dns2="xx.xx.xx.xx"
# dns3=
# dns4=
dns1="192.1681.5"
dns2="192.168.3.4"
dns3=
dns4=

#########################NTP Configuration######################################
# Provide NTP server information.
# If not set here, the default value will be the address of domain controller.
# Format:
# NTP_SERVER="xx.xx.xx.xx"
NTP_SERVER="192.168.4.5"

#########################WORKGROUP Configuration################################
# Provide Workgroup information.
# Usually workgroup is the same with domain name and you do not need to configure it here.
# If that is not the case, please config it according to the correct format:
# WORKGROUP="workgroup_name"
WORKGROUP="example"

#########################Domain Join Configuration##############################
# Provide Domain Join method.
# Winbind: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# SSSD: support RHEL7/CentOS7, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, SUSE12, SUSE15
# Centrify: support RHEL7/CentOS7
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, Debian 10
# AD_INTEGRATION="winbind" or AD_INTEGRATION="sssd" or AD_INTEGRATION="centrify" or AD_INTEGRATION="pbis"
AD_INTEGRATION="winbind"

#########################Centrify download path Configuration###################
# When choose Centrify as AD_INTEGRATION, provide Centrify download path with related distribution if Centrify is not installed.
# To find out the correct download url for your os, you may go here:
# https://www.centrify.com/express/linux/download-files/#accordion-download-express-02
CENTRIFY_DOWNLOAD_PATH=


#########################Centrify Samba download path Configuration##############
# When choose Centrify as AD_INTEGRATION, provide Centrify Samba download path with related distribution if Centrify is not installed.
# CENTRIFY_SAMBA_DOWNLOAD_PATH="http://edge.centrify.com/products/opensource/samba-4.5.9/centrify-samba-4.5.9-rhel3-x86_64.tgz
CENTRIFY_SAMBA_DOWNLOAD_PATH=


#########################PBIS download path Configuration########################
# When choose PBIS as AD_INTEGRATION, provide PBIS download path if PBIS is not installed.
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12/SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# RHEL7 and SUSE12: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
# RHEL8: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# Ubuntu: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh"
# SUSE15: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# PBIS_DOWNLOAD_PATH="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
PBIS_DOWNLOAD_PATH=


#########################Machine Password Automate Update########################
# Machine password will expire after 30 days(default), so we have a mechnisum to update
# this password regularly.
# You can set this value to enabled to enable this feature.
UPDATE_MACHINE_PW="disabled"

#########################Linux VDA Configuration################################
# Provide Linux VDA configuration information.
# Please refer to Linux VDA Documentation for these settings.
DOTNET_RUNTIME_PATH=/opt/dotnet
DESKTOP_ENVIRONMENT=gnome
SUPPORT_DDC_AS_CNAME=N
VDA_PORT=80
REGISTER_SERVICE=Y
ADD_FIREWALL_RULES=Y
HDX_3D_PRO=N
VDI_MODE=Y
SITE_NAME='<none>'
LDAP_LIST="dc1.example.com"
SEARCH_BASE="DC=example,DC=com"
FAS_LIST='<none>'
START_SERVICE=Y
TELEMETRY_SOCKET_PORT=7503
TELEMETRY_PORT=7502
```

2. 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：

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

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

步骤 **3g**：创建主映像

1. 运行 /opt/Citrix/VDA/sbin/deploymcs.sh。
2. （如果使用当前正在运行的 VDA 作为模板 VM，请跳过此步骤。）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/sssd/sssd.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/sssd.conf.tmpl、/etc/xdl/mcs/sssd_krb5.conf.tmpl 和 /etc/xdl/mcs/sssd_smb.conf.tmpl 模板。

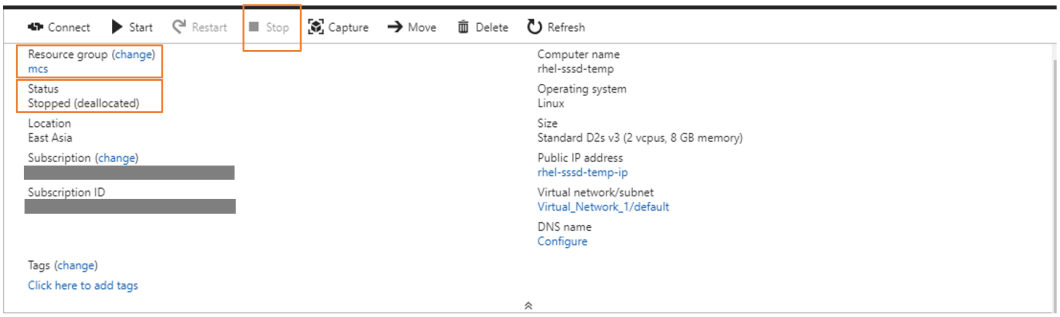
   对于 Centrify 用户，请更新 /etc/xdl/mcs/centrify_krb5.conf.tmpl 和 /etc/xdl/mcs/centrify_smb.conf.tmpl 模板。

   > 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、$realm、${new_hostname} 和 $AD_FQDN。

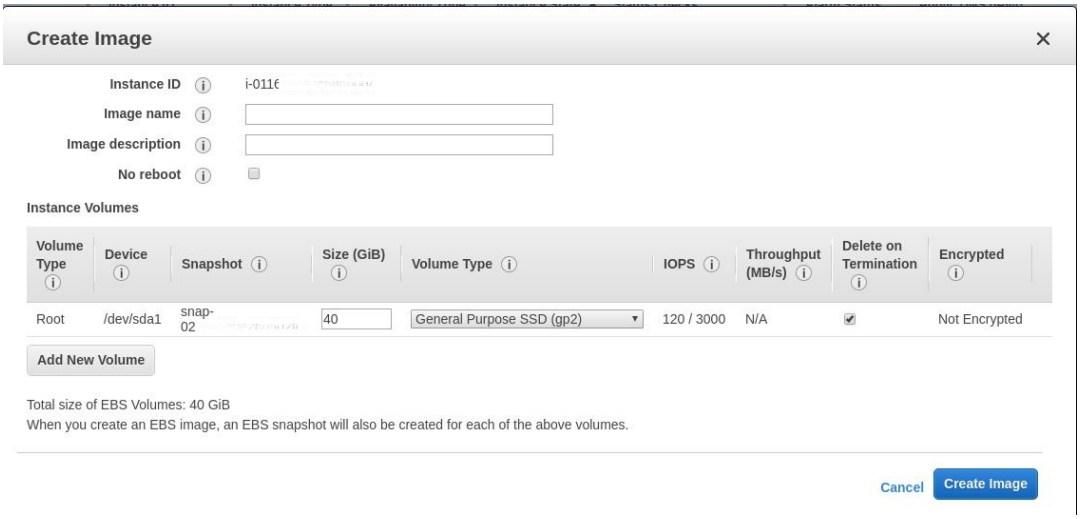
3. 根据您使用的公有云创建主映像的快照并命名。

   - （适用于 **Citrix Hypervisor**、**GCP** 和 **VMware vSphere**）在模板 VM 上安装应用程序并关闭模板 VM。创建并命名主映像的快照。
   - （适用于 **Azure**）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。




- （适用于 **AWS**）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。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。



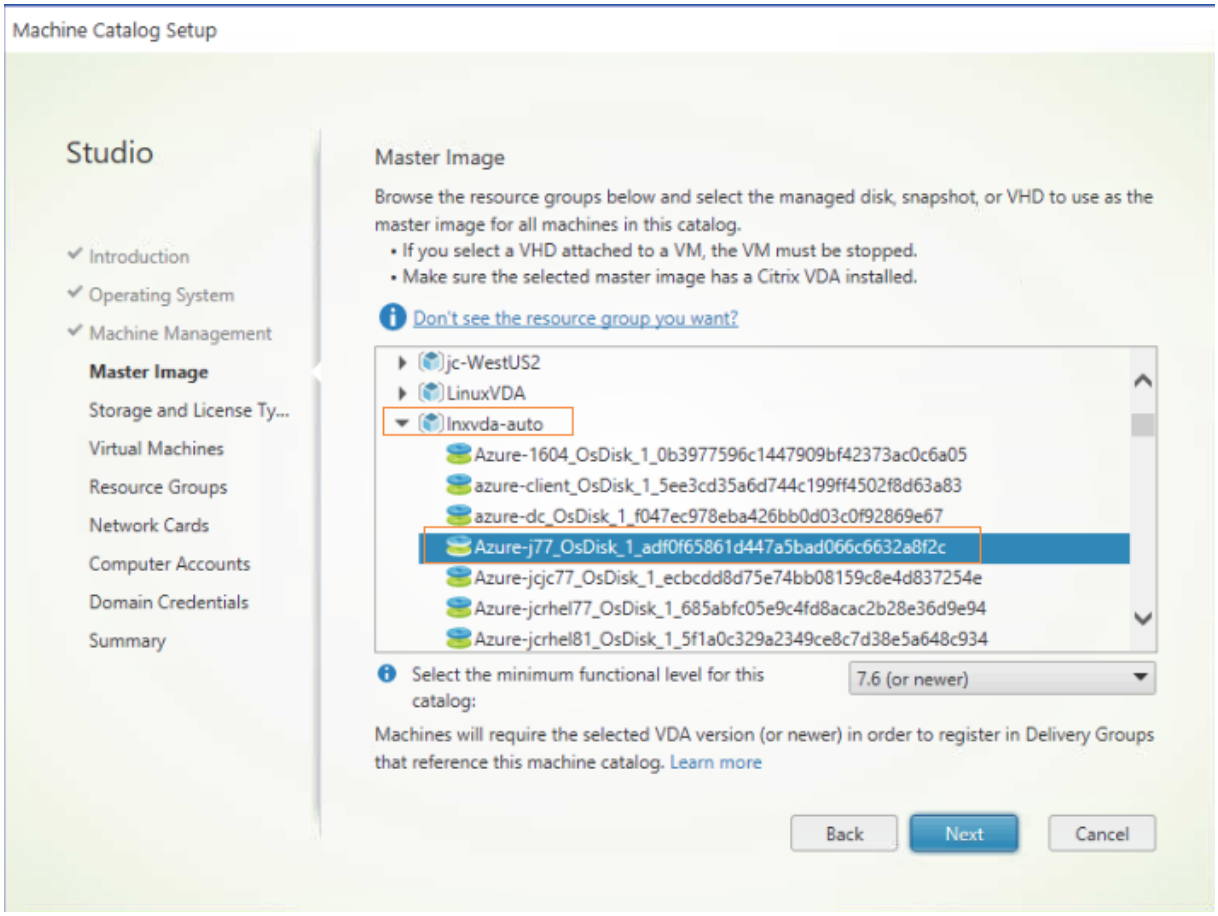

- （适用于 **Nutanix**）在 Nutanix AHV 上，关闭模板 VM。创建并命名主映像的快照。

> 注意：
>
> 必须在 Acropolis 快照名称前加上前缀 XD_ 才能在 Citrix Virtual Apps and Desktops 中使用。根据需要使用 Acropolis 控制台重命名快照。重命名快照后，重新启动创建目录向导以获取刷新后的列表。

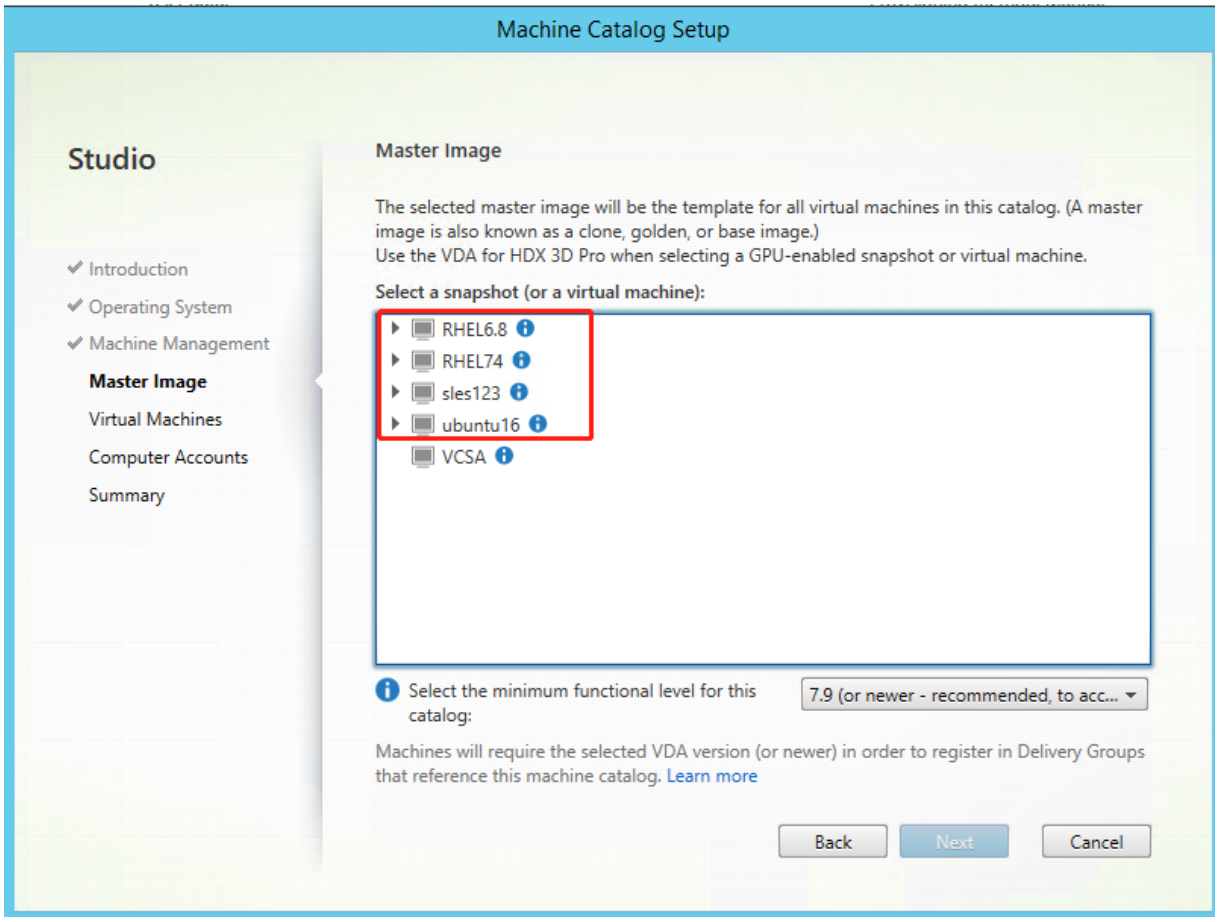
步骤 **4**：创建计算机目录

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，请选择您的主映像。下面是几个示例：






在 Nutanix 独有的 **Container**（容器）页面上，选择您之前为模板 VM 指定的容器。在主映像页面上，选择映像快照。在虚拟机页面上，检查虚拟 CPU 的数量以及每个 vCPU 的核心数。

> 注意：
>
> 如果 Delivery Controller 上的计算机目录创建过程需要大量时间，请转至 Nutanix Prism 并手动打开前缀为 **Preparation** 的计算机的电源。这种方法有助于继续执行创建过程。

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 **5**：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** 更新您的 **Linux VDA**

要使用 MCS 更新您的 Linux VDA，请执行以下操作：

1. 在将 Linux VDA 更新到当前版本之前，请确保已安装.NET Runtime 6.0。
2. 在模板计算机上更新 Linux VDA：

> 注意：
>
> 此外，您还可以使用 Linux VDA 自助更新功能来计划软件自动更新。要实现此目标，请在模板计算机上的 etc/xdl/mcs/mcs_local_setting.reg 文件中添加命令行。
> 例如，可以添加以下命令行：

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0x00000001" -force

create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "Immediately" -force

create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-Container-Url>" -force

create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local-Certificate-Path-of-PortalAzureCom>" --force
<!--NeedCopy-->
```

对于 **RHEL 7** 和 **CentOS 7**：

```
sudo rpm -U XenDesktopVDA-<version>.el7_x.x86_64.rpm
<!--NeedCopy-->
```

对于 **RHEL 8** 和 **Rocky Linux 8**：

```
sudo rpm -U XenDesktopVDA-<version>.el8_x.x86_64.rpm
<!--NeedCopy-->
```

对于 **SUSE**：

```
sudo rpm -U XenDesktopVDA-<version>.sle12_x.x86_64.rpm
<!--NeedCopy-->
```

对于 **Ubuntu 18.04**：

```
sudo dpkg -i xendesktopvda_<version>.ubuntu18.04_amd64.deb
<!--NeedCopy-->
```

对于 **Ubuntu 20.04**：

```
sudo dpkg -i xendesktopvda_<version>.ubuntu20.04_amd64.deb
<!--NeedCopy-->
```

对于 **Ubuntu 22.04**：

```
sudo dpkg -i xendesktopvda_<version>.ubuntu22.04_amd64.deb
<!--NeedCopy-->
```

3. 编辑 /etc/xdl/mcs/mcs.conf 和 /etc/xdl/mcs/mcs_local_setting.reg。
4. 生成新快照。
5. 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。

### 自动更新计算机帐户密码

默认情况下，计算机帐户密码在创建计算机目录后 30 天过期。要防止密码过期以及自动更新计算机帐户密码，请执行以下操作：

1. 在运行 /opt/Citrix/VDA/sbin/deploymcs.sh 之前，将以下条目添加到 /etc/xdl/mcs/mcs.conf 中。

   ```
   UPDATE_MACHINE_PW="enabled"
   ```

2. 运行 /opt/Citrix/VDA/sbin/deploymcs.sh 后，打开 /etc/cron.d/mcs_update_password_cronjob 以设置更新时间和频率。默认设置每周星期日凌晨 2:30 更新计算机帐户密码。

每次更新计算机帐户密码后，Delivery Controller 上的票证缓存将变为无效，并且在 /var/log/xdl/jproxy.log 中可能会出现以下错误：

```
[ERROR] - AgentKerberosServiceAction.Run: GSSException occurred.
 Error: Failure unspecified at GSS-API level (Mechanism level:
Checksum failed)
```

要消除错误，请定期清除票证缓存。可以在所有 Delivery Controller 或域控制器上安排缓存清理任务。

### 在 **MCS** 创建的 **VM** 上启用 **FAS**

可以在以下发行版上运行的 MCS 创建的虚拟机上启用 FAS：

| | Winbind | SSSD | Centrify | PBIS |
|---|---|---|---|---|
| RHEL 8 | 是 | 否 | 否 | 是 |
| Rocky Linux 8 | 是 | 否 | 否 | 否 |
| RHEL 7、CentOS 7 | 是 | 是 | 否 | 是 |
| Ubuntu 22.04、Ubuntu 20.04、Ubuntu 18.04 | 是 | 否 | 否 | 否 |

| | Winbind | SSSD | Centrify | PBIS |
|---|---|---|---|---|
| Debian 11.3、Debian 10.9 | 是 | 否 | 否 | 否 |
| SUSE 15.3 | 是 | 否 | 否 | 否 |

#### 在模板 **VM** 上准备主映像时启用 **FAS**

1. 导入根 CA 证书。

```
sudo cp root.pem /etc/pki/CA/certs/
<!--NeedCopy-->
```

2. 运行 ctxfascfg.sh。有关详细信息，请参阅运行 ctxfascfg.sh。
3. 在 /etc/xdl/mcs/mcs.conf 中设置变量。

> 注意：
>
> 必须在 /etc/xdl/mcs/mcs.conf 中设置所有必需的变量，因为这些变量是在 VM 启动时调用的。

   a) 将 Use_Existing_Configurations_Of_Current_VDA 的值设置为 Y。
   b) 将 FAS_LIST 变量设置为您的 FAS 服务器地址或多个 FAS 服务器地址。用分号分隔多个地址，并用单引号将一个或多个地址括起来，例如 FAS_LIST='<FAS_SERVER_FQDN>;<FAS_SERVER_FQDN>'。
   c) 根据需要设置其他变量，例如 VDI_MODE。

4. 运行脚本 /opt/Citrix/VDA/sbin/deploymcs.sh。

#### 在 **MCS** 创建的 **VM** 上启用 **FAS**

如果未如上文所述在模板计算机上启用 FAS，则可以在每个 MCS 创建的 VM 上启用 FAS。

要在 MCS 创建的 VM 上启用 FAS，请执行以下操作：

1. 在 /etc/xdl/mcs/mcs.conf 中设置变量。

> 注意：
>
> 必须在 /etc/xdl/mcs/mcs.conf 中设置所有必需的变量，因为这些变量是在 VM 启动时调用的。

   a) 将 Use_Existing_Configurations_Of_Current_VDA 的值设置为 Y。
   b) 将 FAS_LIST 变量设置为 FAS 服务器地址。
   c) 根据需要设置其他变量，例如 VDI_MODE。

2. 导入根 CA 证书。

```
sudo cp root.pem /etc/pki/CA/certs/
<!--NeedCopy-->
```

3. 运行脚本 /opt/Citrix/VDA/sbin/ctxfascfg.sh。有关详细信息，请参阅运行 ctxfascfg.sh。

## 使用 Citrix Provisioning 创建 Linux VM

October 31, 2022

本文提供有关通过流技术推送 Linux 目标设备的信息。使用此功能，您可以直接在 Citrix Virtual Apps and Desktops 环境中预配 Linux 虚拟桌面。

支持以下 Linux 发行版：

- Ubuntu 20.04
- Ubuntu 18.04
- RHEL 8.4
- RHEL 7.9
- SUSE 15.3

> 重要：
>
> - 我们建议您使用 Citrix Provisioning 的最新安装包。请根据您的 Linux 发行版使用该软件包。要使用 Linux 流技术推送代理 2109 及更高版本，需要安装 Citrix Provisioning 服务器 2109 或更高版本。
> - 使用 Citrix Provisioning 通过流技术推送 Linux 目标设备时，请对单个共享磁盘映像创建单独的启动分区，以便预配的设备能够正常启动。
> - 请避免使用 **btrfs** 格式化任何分区。GRUB2 在查找 **btrfs** 分区时出现内部问题。**GRUB** 代表 **GRand Unified Bootloader**。

有关详细信息，请参阅 Citrix Provisioning 文档中的通过流技术推送 Linux 目标设备。

## 为 XenDesktop 7.6 及早期版本配置 Delivery Controller

October 31, 2022

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

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：

```
.\Update-BrokerServiceConfig.ps1
<!--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：
>
> ```
> Set-ExecutionPolicy Unrestricted
> <!--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 场可同时无缝管理和代理 Windows 和 Linux VDA 的会话。

### 验证 **Delivery Controller** 配置

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

在 Windows 命令提示窗口中，以本地管理员身份登录进行检查：

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

# 策略和 LDAP 服务器设置

November 4, 2022

## 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。

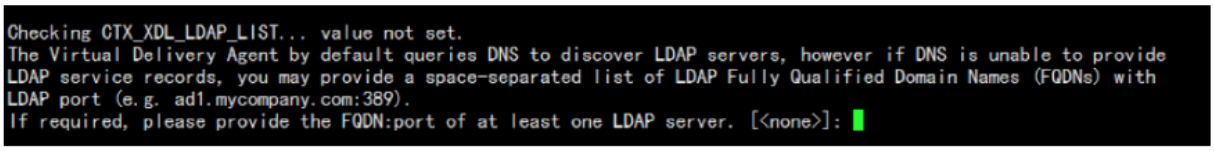
## VDA 上的 LDAP 服务器设置

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这些环境中执行 LDAP 搜索。

安装 Linux VDA 软件包后，运行以下命令：

```
/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--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.mycomany.com:389）。




还可以通过运行 **ctxreg** 命令将此设置直接写入注册表：

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
   VirtualDesktopAgent" -t "REG_SZ" -v "ListOfLDAPServers" -d "ad1.
   mycompany.com:389 ad2.mycomany.com:389" --force
<!--NeedCopy-->
```

# 配置

October 31, 2022

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

## 管理

November 4, 2022

本部分内容包含以下主题：

- CEIP
- HDX Insight
- 与 Citrix Telemetry Service 集成
- 面向 Citrix DaaS Standard for Azure 的 Linux VDA 自我更新
- Linux VM 和 Linux 会话指标
- 日志收集
- 会话影子处理
- 监视服务守护程序
- 工具和实用程序
- 其他
  - 适用于 HTML5 的 Citrix Workspace 应用程序支持
  - 创建 Python3 虚拟环境
  - 将 NIS 与 Active Directory 集成
  - IPv6
  - LDAPS
  - **Xauthority**

## Citrix 客户体验改善计划 (CEIP)

October 31, 2022

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。默认情况下，GA 处于禁用状态。

注册表设置

默认情况下，您在安装 Linux VDA 时会自动参与 CEIP。大约在您安装 Linux VDA 七天后第一次上载数据。可以在注册表中更改此默认设置。

- **CEIPSwitch**

启用或禁用 CEIP 的注册表设置（默认值 = 0）：

位置：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

名称：**CEIPSwitch**

值：1 = 禁用，0 = 启用

未指定时，CEIP 处于启用状态。

可以在客户端上运行以下命令来禁用 CEIP：

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
     Citrix\CEIP" -v "CEIPSwitch" -d "1"
2 <!--NeedCopy-->
```

- **GASwitch**

启用或禁用 GA 的注册表设置（默认值 = 1）：

位置：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

名称：**GASwitch**

值：1 = 禁用，0 = 启用

未指定时，GA 处于禁用状态。

可以在客户端上运行以下命令来启用 GA：

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
     Citrix\CEIP" -v "GASwitch" -d "0"
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：

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
   Citrix\CEIP" -v "DataPersistPath" -d "your_path"
<!--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** | `ctxhdx` 和 `ctxvda` 服务的上次重新启动时间，格式为 dd-hh:mm:ss，例如 10-17:22:19 |
| GPU 类型 | **gpu_type** | 表示计算机的 GPU 类型 |
| CPU 内核 | **cpu_cores** | 表示计算机的 CPU 内核数的整数 |
| CPU 频率 | **cpu_frequency** | 表示 CPU 频率的浮点数（以 MHz 为单位） |
| 物理内存大小 | **memory_size** | 表示物理内存大小的整数（以 KB 为单位） |
| 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 |

| 数据点 | 注册表项名称 | 说明 |
| --- | --- | --- |
| 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 |
| 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 |

## HDX Insight

April 18, 2024

概述

Linux VDA 部分支持 HDX Insight 功能。

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。所有 HDX Insight 数据均来自 NSAP 虚拟通道并以未压缩方式发送。NSAP 虚拟通道默认处于启用状态。

以下命令分别禁用和启用 NSAP 虚拟通道：

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000000"
     --force
2 <!--NeedCopy-->
```

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000001"
     --force
2 <!--NeedCopy-->
```

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

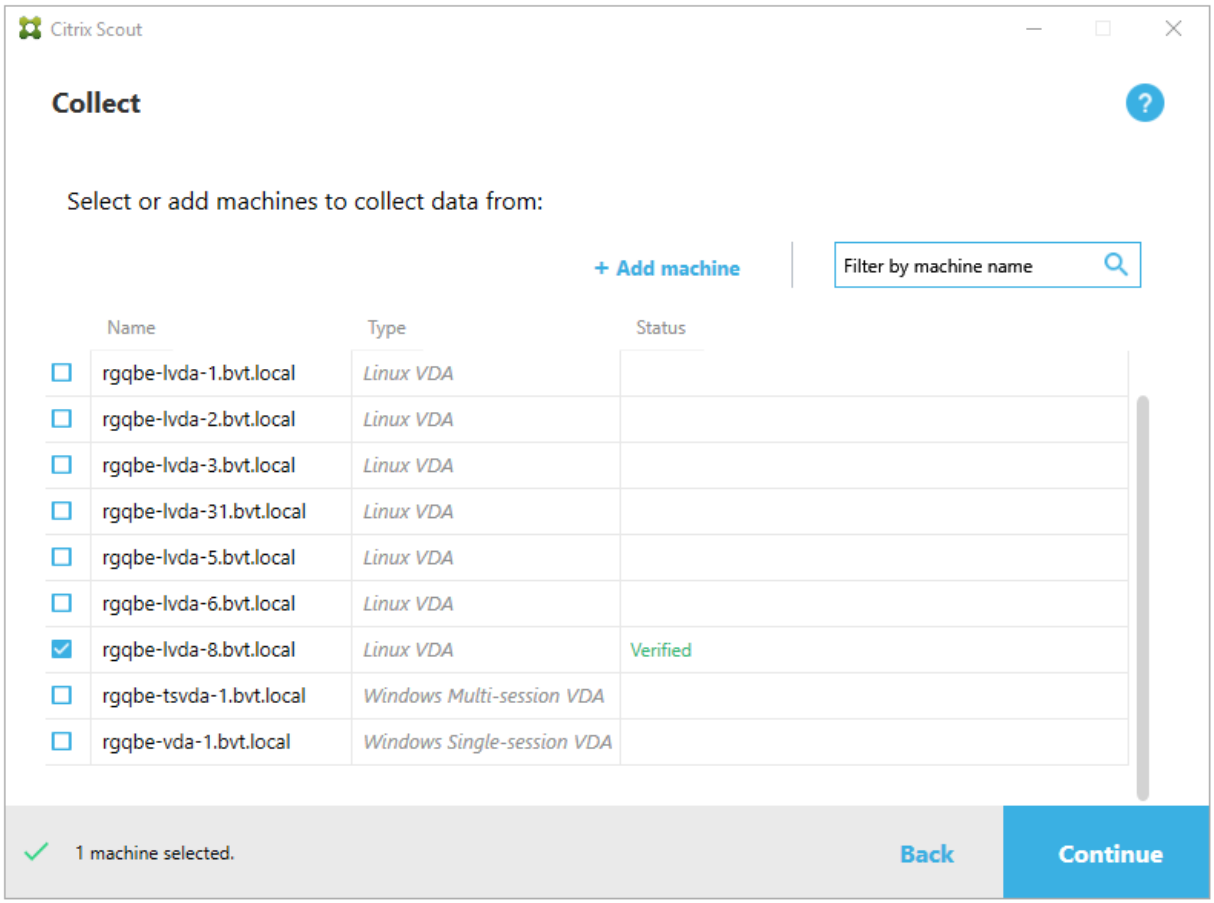
请确认是否启用了无缝虚拟通道且无缝应用程序正在运行。

## 与 **Citrix Telemetry Service** 集成

November 4, 2022

通过与 Linux VDA 软件集成的 Citrix Telemetry Service (`ctxtelemetry`)，您可以运行 Citrix Scout，然后使用 /opt/Citrix/VDA/bin/xdlcollect.sh 脚本来收集有关 Linux VDA 的日志。




> 注意：
>
> 从 Linux VDA 1912 及更早版本升级后，必须重新运行 /opt/Citrix/VDA/sbin/ctxsetup.sh 以配置 Citrix Telemetry Service (`ctxtelemetry`) 的变量。有关这些变量的详细信息，请参阅轻松安装。

### 启用和禁用 **Citrix Telemetry Service**

- 要启用该服务，请运行 **sudo systemctl enable ctxtelemetry.socket** 命令。
- 要禁用该服务，请运行 **sudo systemctl disable ctxtelemetry.socket**。

#### 端口

默认情况下，Citrix Telemetry Service (`ctxtelemetry`) 使用 TCP/IP 端口 7503 侦听 Citrix Scout。它使用 Delivery Controller 上的 TCP/IP 端口 7502 与 Citrix Scout 进行通信。

在安装 Linux VDA 时，可以使用默认端口或者通过以下变量更改端口。

- **CTX_XDL_TELEMETRY_SOCKET_PORT** - 用于侦听 Citrix Scout 的套接字端口。默认端口为 7503。
- **CTX_XDL_TELEMETRY_PORT** - 用于与 Citrix Scout 通信的端口。默认端口为 7502。

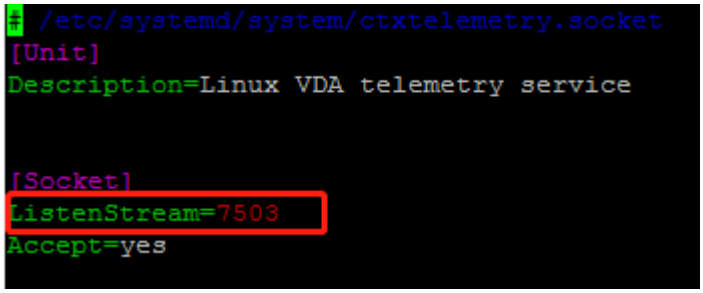
要在安装 VDA 后更改端口，请执行以下操作：

1. 要更改用于与 Scout 通信的端口，请运行以下命令。

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
    VirtualDesktopAgent" -v "TelemetryServicePort" -d <port number>
     -t REG_DWORD
<!--NeedCopy-->
```

2. 要更改侦听 Scout 的套接字端口，请运行以下命令以打开并编辑 ctxtelemetry.socket 文件。

```
sudo vi /etc/systemd/system/ctxtelemetry.socket
<!--NeedCopy-->
```




3. 运行以下命令以重新启动套接字端口。

```
sudo systemctl daemon-reload
sudo systemctl stop ctxtelemetry.socket
sudo systemctl start ctxtelemetry.socket
<!--NeedCopy-->
```

4. 在防火墙配置中启用新端口。

   例如，如果您使用的是 Ubuntu，请运行 **sudo ufw allow 7503** 命令以启用端口 7503。

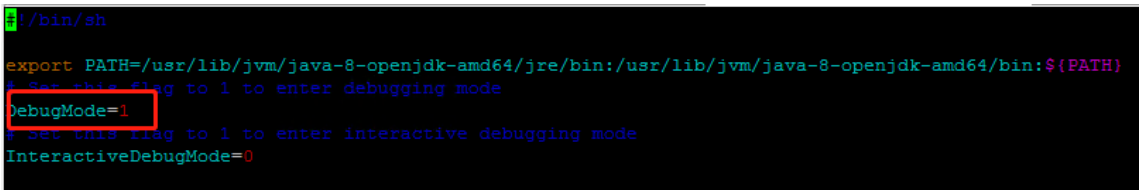
### 调试模式

如果 Citrix Telemetry Service 无法按预期方式运行，则可以启用调试模式来确定原因。

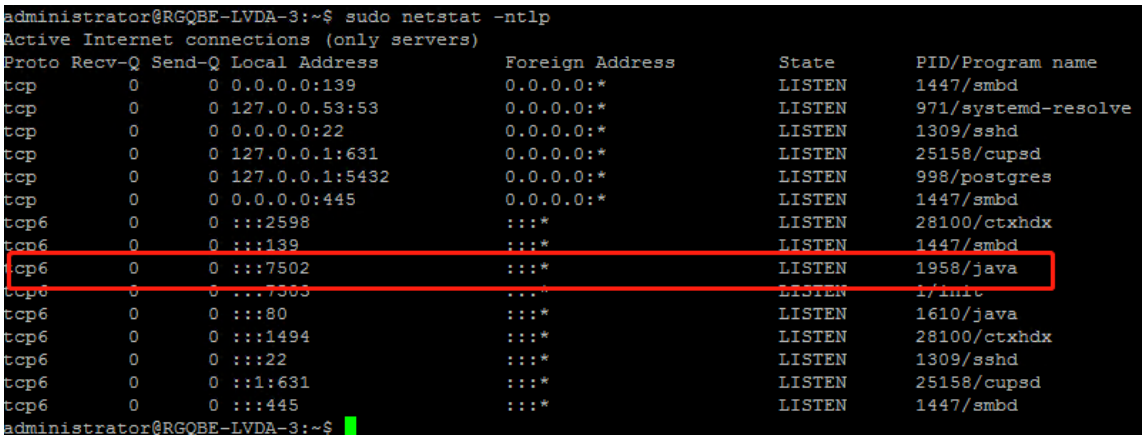
1. 要启用调试模式，请运行以下命令以打开 `ctxtelemetry` 文件，然后将 DebugMode 值更改为 1。

```
sudo vi /opt/Citrix/VDA/sbin/ctxtelemetry
<!--NeedCopy-->
```




2. 手动停止 Citrix Telemetry Service，或者等待 15 分钟以使服务自动停止。




在此示例中，可以运行以下命令来停止 Citrix Telemetry Service。

```
sudo netstat -ntlp
Kill -9 1958
<!--NeedCopy-->
```

3. 要重新启动 Citrix Telemetry Service，请在 Scout 上选择您的 Linux VDA 并在 /var/log/xdl/ 中查找 telemetry-debug.log。

### 服务等待时间

打开套接字端口的 `systemd` 守护程序默认启动并使用少量资源。Citrix Telemetry Service 默认处于停止状态，并仅在从 Delivery Controller 发出日志收集请求时启动。日志收集完成后，服务会等待新的收集请求，持续时间为 15 分钟，如果没有任何收集请求，则会再次停止。可以通过以下命令配置等待时间。最小值为 10 分钟。如果设置的值小于 10 分钟，则最小值 10 分钟将生效。设置等待时间后，停止并重新启动服务。

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent" -v "TelemetryServiceIdleTimeoutInMinutes" -d <
    number> -t REG_DWORD
<!--NeedCopy-->
```

### 验证测试

在开始收集信息之前，验证测试将针对选定的每台计算机自动运行。这些测试将确保满足这些要求。如果某台计算机的测试失败，Scout 将显示一条消息，提供建议的更正措施。有关验证测试的详细信息，请参阅 Citrix Scout 文档中的验

证测试部分。

## 通过 **Azure** 进行 **Linux VDA** 自助更新

May 30, 2024

此功能有助于立即或在计划的时间自动更新 Linux VDA 软件。当您在 Citrix DaaS Standard for Azure（以前称为“适用于 Azure 的 Citrix Virtual Apps and Desktops Standard”）中创建 Linux VDA 时非常有用。您在 Azure 中不需要 VM 的任何管理员权限。有关详细信息，请参阅在 Citrix DaaS Standard for Azure 中创建 Linux VDA。

### 配置

要使用此功能，请完成以下步骤：

#### 步骤 **1**：将更新信息和新 **VDA** 包上载到 **Azure** 容器

步骤 1a：在 Azure 存储帐户下创建一个容器并将容器访问级别设置为 **Blob (Anonymous read access for blobs only)**（Blob (仅限 blob 的匿名读取访问权限)）。

> 注意：
>
> Azure 容器和 blob 专门由客户持有和管理。Citrix 对其任何安全问题不承担责任。为了确保数据安全性和成本效率，请在每次自我更新后将容器访问级别设置为 **Private (no anonymous access)**（私密 (无匿名访问权限)）。

Step1b：将 VDA 更新信息合并到名为 UpdateInfo.json 的 JSON 文件中。有关文件格式的示例，请参阅以下块：

```
{

 "Version": "21.04.200.4",
"Distributions":[
{

"TargetOS": "RHEL7_9",
"PackageName": "",
"PackageHash": ""
 }
 ,
{

"TargetOS": "UBUNTU18_04",
"PackageName": "xendesktopvda_21.04.200.4-1.ubuntu18.04_amd64.deb",
"PackageHash": "4148
   cc3f25d3717e3cbc19bd953b42c72bd38ee3fcd7f7034c2cd6f2b15b3c5a"
 }
```

```
 ,
{

"TargetOS": "UBUNTU20_04",
"PackageName": "",
"PackageHash": ""
 }

]
 }

<!--NeedCopy-->
```

其中，“**Version**”表示新的 VDA 版本，“**Distributions**”是一组更新对象。每个对象包含三个项目：

- “**TargetOS**”：必须是“RHEL7_9”（适用于 RHEL 7、CentOS 7 和 Amazon Linux 2）、”UBUNTU18_04”或“UBUNTU20_04”。`ctxmonitorservice` 无法识别任何其他发行版。
- “**PackageName**”：指定版本的 VDA 软件包的全名。
- “**PackageHash**”：使用 `shasum -a 256 <pkgname>` 命令计算的 SHA-256 值。

Step1c：将 JSON 文件和 Linux VDA 软件包的新版本上载到您的 Azure 容器。

步骤 **2**：在主映像或每个 **VDA** 上启用自助更新功能

默认情况下，自我更新处于禁用状态。如果在 Citrix DaaS Standard for Azure 中创建 Linux VDA，必须在主映像上执行功能启用。否则，请直接在每个目标 VDA 上启用该功能。

要启用自我更新，请运行类似于以下内容的命令，以编辑 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\ 下的注册表项。

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Control\Citrix\SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0
   x00000001" --force

/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Control\Citrix\SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "
   Immediately" --force

/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Control\Citrix\SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-
   Container-Url>" --force

/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Control\Citrix\SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local
   -Certificate-Path-of-PortalAzureCom>" --force
<!--NeedCopy-->
```

下表介绍了注册表设置。

| 注册表设置 | 说明 |
| --- | --- |
| fEnabled | 此设置为必填项。默认情况下，该值为 0，表示自我更新已禁用。可以将其设置为 1 以启用自我更新。 |
| Url | 此设置为必填项。它设置 Azure 容器的 URL 以获取更新信息和新的 VDA 软件包。 |
| ScheduledTime | 此设置为必填项。可以将其设置为 **Immediately** 或 **NextStart**。**Immediately** 意味着下载 VDA 软件包后立即运行更新。当下载速度很高且您的更新非常紧急时，此选项适用。但是，如果下载软件包时有任何实时会话，则可能会中断用户体验。**NextStart** 意味着在下次启动 `ctxmonitorservice` 时运行更新。当下载速度不高且您的更新不紧急时，此选项适用。 |
| CaCertificate | 此设置为可选设置。它设置 PEM 证书的完整路径以验证 Azure 容器的 URL。对于 Azure blob，它可以是从浏览器中检索并转换为 PEM 的 portal.azure.com 的证书。为了安全起见，我们建议您添加此注册表设置，但仅在 Ubuntu 上受支持。在 RHEL 上，它没有链接 `curl` 命令的一些 NSS 库。确保设置证书的最低权限。 |

重新启动 `ctxmonitorservice` 时，它首先查询 **Url** 以获取 UpdateInfo.json 文件，然后从 JSON 文件中检索更新版本。然后 `ctxmonitorservice` 会将更新版本与当前版本进行比较。如果当前版本较早，该服务将从 Azure 下载新版本的 VDA 软件包并将其保存在本地。之后，它根据 **ScheduledTime** 的设置运行更新。对于本地部署，您可以直接重新启动 `ctxmonitorservice` 以触发更新。但是，在 Citrix DaaS Standard for Azure 中，您对 VM 没有管理员权限，只能在重新启动 VDA 计算机后重新启动 `ctxmonitorservice`。如果更新失败，您的 VDA 将回滚到现有版本。

> 注意：
>
> - 无法更改在主映像上配置的注册表设置。
> - 如果环境中的所有 VM 同时下载软件包，本地网络可能会拥塞。
> - 如果更新和回滚均失败，用户数据将丢失。
> - 如果更新失败但回滚成功，同一网络中的用户可能拥有不同版本的 Linux VDA。这种情况不是最佳情况。
> - 更新通常需要几分钟时间才能完成。Citrix Studio 中没有状态指示器。

## Linux VM 和 Linux 会话指标

November 4, 2022

下表列出了一些适用于 Linux VM 和 Linux 会话的指标。

| 指标 | 所需的最低 VDA 版本 | 说明 | 备注 |
| --- | --- | --- | --- |
| 登录持续时间 | 2109 | 它是登录过程的一种度量，该过程是指用户从 Citrix Workspace 应用程序开始连接到能够使用会话的这段时间。要查看会话的指标，请转到 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）的监视选项卡。Monitor 将以 Director 控制台的方式提供，以监视 Citrix Virtual Apps and Desktops 当前版本和 LTSR 部署并对其进行故障排除。在监视选项卡上，单击平均登录持续时间部分中的查看历史趋势。在登录性能页面上，设置过滤条件并单击应用以可视化指标。 | 仅在监视器中可用。 |
| 会话自动重新连接计数 | 2109 | 要查看会话中的自动重新连接次数，请访问趋势视图。设置条件并单击应用以缩小搜索结果范围。会话自动重新连接计数列将显示会话的自动重新连接次数。会话可靠性或客户端自动重新连接策略生效时，将启用“自动重新连接”。有关会话重新连接的详细信息，请参阅会话。有关策略的详细信息，请参阅客户端自动重新连接策略设置和会话可靠性策略设置。 | 在 Citrix Director 和监视器中均可用。 |
| 空闲时间 | 2103 | 要访问此指标，请通过选择过滤器 **>** 会话 **>** 所有会话打开所有会话页面。 | 在 Citrix Director 和监视器中均可用。 |

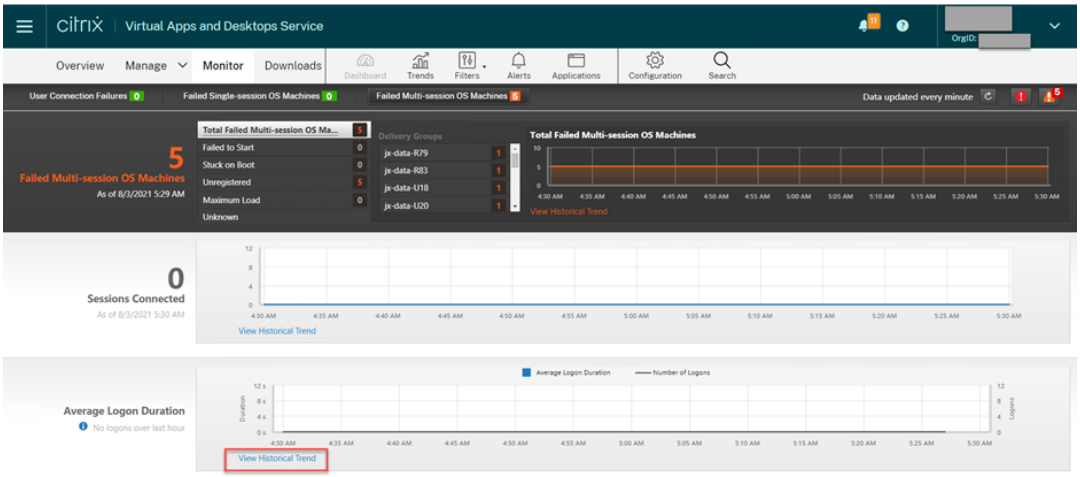
 

| 指标 | 所需的最低 VDA 版本 | 说明 | 备注 |
| --- | --- | --- | --- |
| Linux VM 的衡量指标 | 2103 | Linux VM 的以下衡量指标可用：CPU 核心数、内存大小、硬盘容量以及当前和历史 CPU 和内存利用率 | 在 Citrix Director 和监视器中均可用。 |
| 协议 | 1909 | Linux 会话的传输协议将在会话详细信息控制板中显示为 UDP 或 TCP。 | 在 Citrix Director 和监视器中均可用。 |
| ICA RTT | 1903 | ICA 往返时间 (RTT) 是从您按下某个键直到响应出现在终端上所经过的时间。要获取 ICA RTT 指标，请在 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。 | 在 Citrix Director 和监视器中均可用。 |

如何访问 **Citrix Director** 和监视器中的各种指标的示例

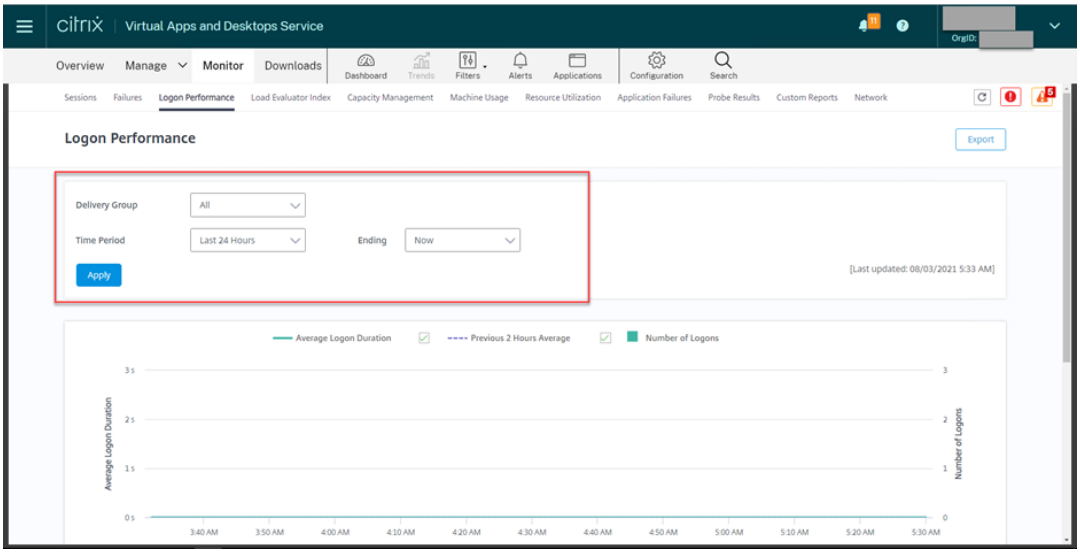
- 登录持续时间

1. 在 Citrix DaaS 的监视选项卡上，单击平均登录持续时间部分中的查看历史趋势。

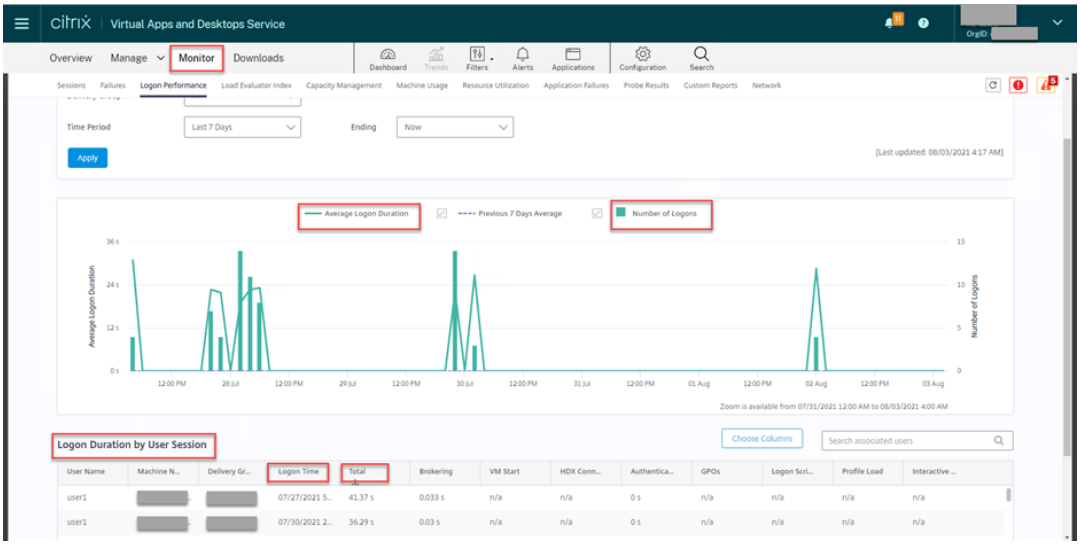



2. 在登录性能页面上，设置过滤条件。




3. 单击应用以可视化登录持续时间指标。




- CPU 核心数、内存大小、硬盘容量，以及 Linux VM 的当前和历史 CPU 及内存利用率

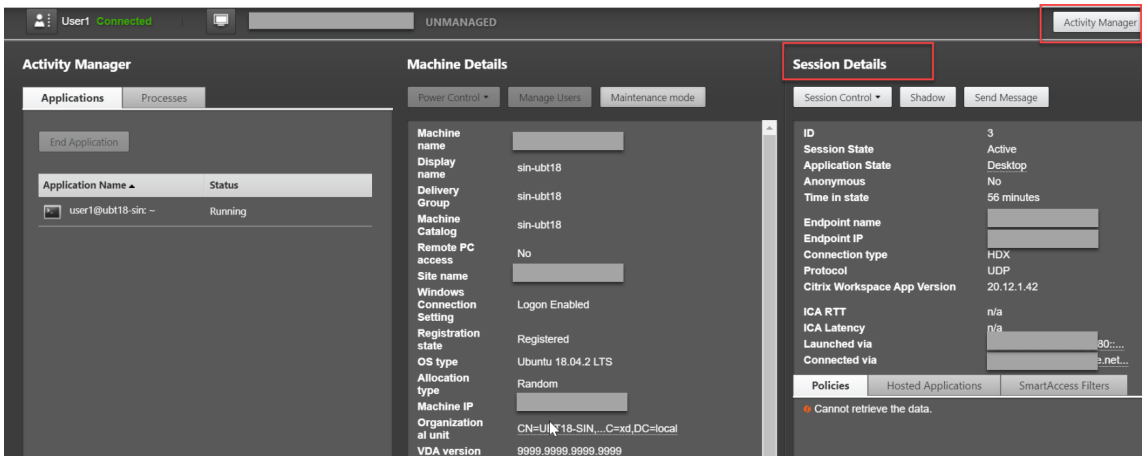
  要访问 Linux VM 的这些指标，请在 Citrix Director 或监视器中找到该 VM，然后查看计算机详细信息面板。例如：


- ICA RTT、协议

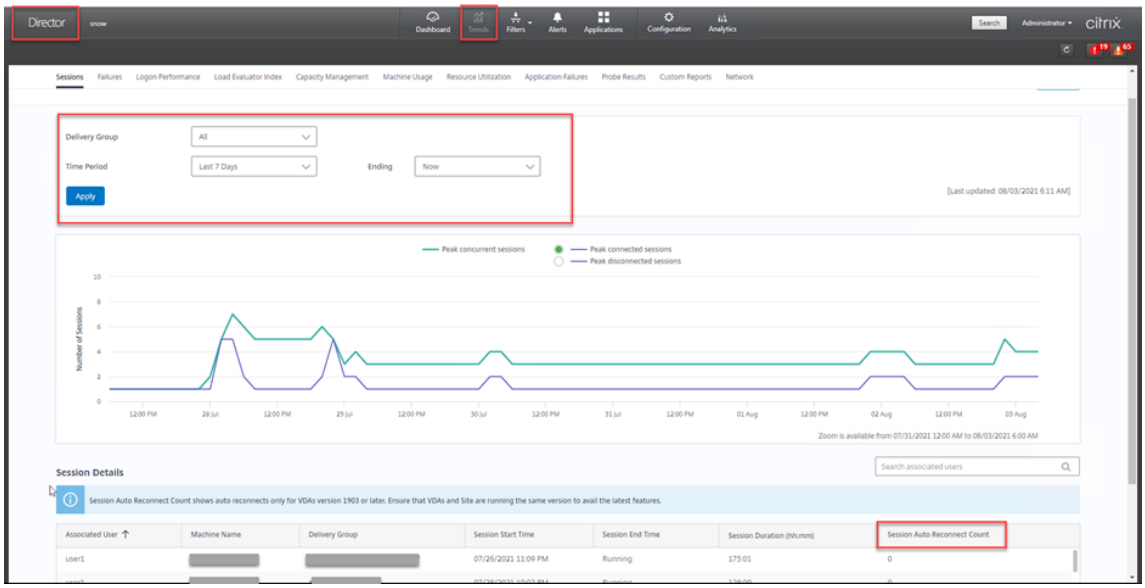
要查看 Linux 会话的指标，请通过选择过滤器 **>** 会话 **>** 所有会话打开所有会话页面，或者访问会话详细信息面板。要访问会话详细信息面板，请打开所有会话页面，然后单击目标会话以访问其活动管理器视图。例如：




- 会话自动重新连接计数

  要查看会话中的自动重新连接次数，请访问趋势视图。设置条件并单击应用以缩小搜索结果范围。

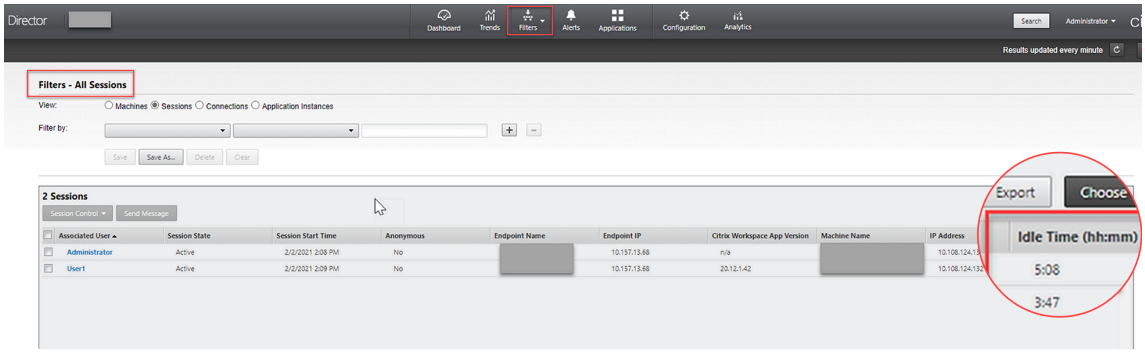
  会话自动重新连接计数列将显示会话的自动重新连接次数。例如：




- 空闲时间

  例如：




## 日志收集

October 31, 2022

### 概述

默认情况下，Linux VDA 的日志收集功能处于启用状态。

### 配置

`ctxlogd` 守护程序和 `setlog` 实用程序包括在 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** 守护进程

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

日志收集功能是使用 `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：

```
setlog help
<!--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：

```
setlog values

log_path (Log Output Path) = /var/log/xdl/hdx.log

log_size (Max Log Size (MiB)) = 200

log_count (Max Old Log Files) = 2
<!--NeedCopy-->
```

查看或设置单个 `setlog` 值：

```
setlog value <name> [<value>]
<!--NeedCopy-->
```

例如：

```
setlog value log_size 100
<!--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：

```
setlog levels
<!--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：

```
setlog level <class> [<level>]
<!--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：

```
setlog level all error
<!--NeedCopy-->
```

标志　默认情况下，标志设置如下：

```
setlog flags

DATE = true

TIME = true

NAME = true

PID = true

TID = false

SID = true

UID = false

GID = false

CLASS = false

LEVEL = false

FUNC = true

FILE = false
<!--NeedCopy-->
```

查看当前标志：

```
setlog flags
<!--NeedCopy-->
```

查看或设置单个日志标志：

```
setlog flag <flag> [<state>]
<!--NeedCopy-->
```

还原默认值　将所有级别、标志和值还原到默认设置：

```
setlog default
<!--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。我们建议 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:

```
Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging
   configuration file.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited, code
   =exited, status=1/FAILURE

Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
<!--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。

## 会话影子处理

April 18, 2024

通过重影会话功能，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。

> 注意：
>
> 要使用该功能，请使用 Citrix Director 7.16 或更高版本。

#### 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。在安装 Linux VDA 后手动安装 python-websockify 和 x11vnc。

对于 **RHEL 7.x** 和 **Amazon Linux2**：

请运行以下命令以安装 python-websockify 和 x11vnc（x11vnc 版本 0.9.13 或更高版本）：

```
sudo pip3 install websockify
sudo yum install x11vnc
<!--NeedCopy-->
```

要解决 python-websockify 和 x11vnc，请在 RHEL 7.x 上启用 Extra Packages for Enterprise Linux (EPEL) 和可选的 RPM 存储库：

- EPEL

  x11vnc 需要 EPEL 存储库。请运行以下命令以启用 EPEL 存储库：

  ```
  yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
  <!--NeedCopy-->
  ```

- 可选 RPM

  要启用可选的 RPMs 存储库以安装 x11vnc 的一些依赖项软件包，请运行以下命令：

  ```
  subscription-manager repos --enable rhel-7-server-optional-rpms --enable rhel-7-server-extras-rpms
  <!--NeedCopy-->
  ```

对于 **RHEL 8.x** 和 **Rocky Linux 8**：

请运行以下命令以安装 python-websockify 和 x11vnc（x11vnc 版本 0.9.13 或更高版本）。

```
sudo pip3 install websockify
sudo yum install x11vnc
<!--NeedCopy-->
```

要解析 x11vnc，请启用 EPEL 和 CodeReady Linux Builder 存储库：

```
dnf install -y --nogpgcheck https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm

subscription-manager repos --enable "codeready-builder  -for-rhel-8-x86_64-rpms"
<!--NeedCopy-->
```

对于 **Ubuntu**：

请运行以下命令以安装 python-websockify 和 x11vnc（x11vnc 版本 0.9.13 或更高版本）：

```
sudo pip3 install websockify
sudo apt-get install x11vnc
<!--NeedCopy-->
```

对于 **SUSE**：

请运行以下命令以安装 python-websockify 和 x11vnc（x11vnc 版本 0.9.13 或更高版本）：

```
sudo pip3 install websockify
sudo zypper install x11vnc
<!--NeedCopy-->
```

对于 **Debian**：

请运行以下命令以安装 python-websockify 和 x11vnc（x11vnc 版本 0.9.13 或更高版本）：

```
sudo pip3 install websockify
sudo apt-get install x11vnc
<!--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：

```
/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，将根据前面提及的“ShadowingUseSSL”注册表来选择 ws://（或 wss://）。默认情况下，选择 ws://。但是，出于安全原因，我们建议您使用 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)。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。

与 Linux VDA 通信的每个 Citrix Director 客户端也需要根证书。根证书可从颁发服务器证书的同一 CA 获得。

可以从以下 CA 安装服务器和客户端证书：

- 与您的操作系统捆绑在一起的 CA
- 企业 CA（贵组织允许您访问的 CA）
- 未与操作系统捆绑在一起的 CA

请咨询您组织的安全团队，了解他们需要使用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 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。

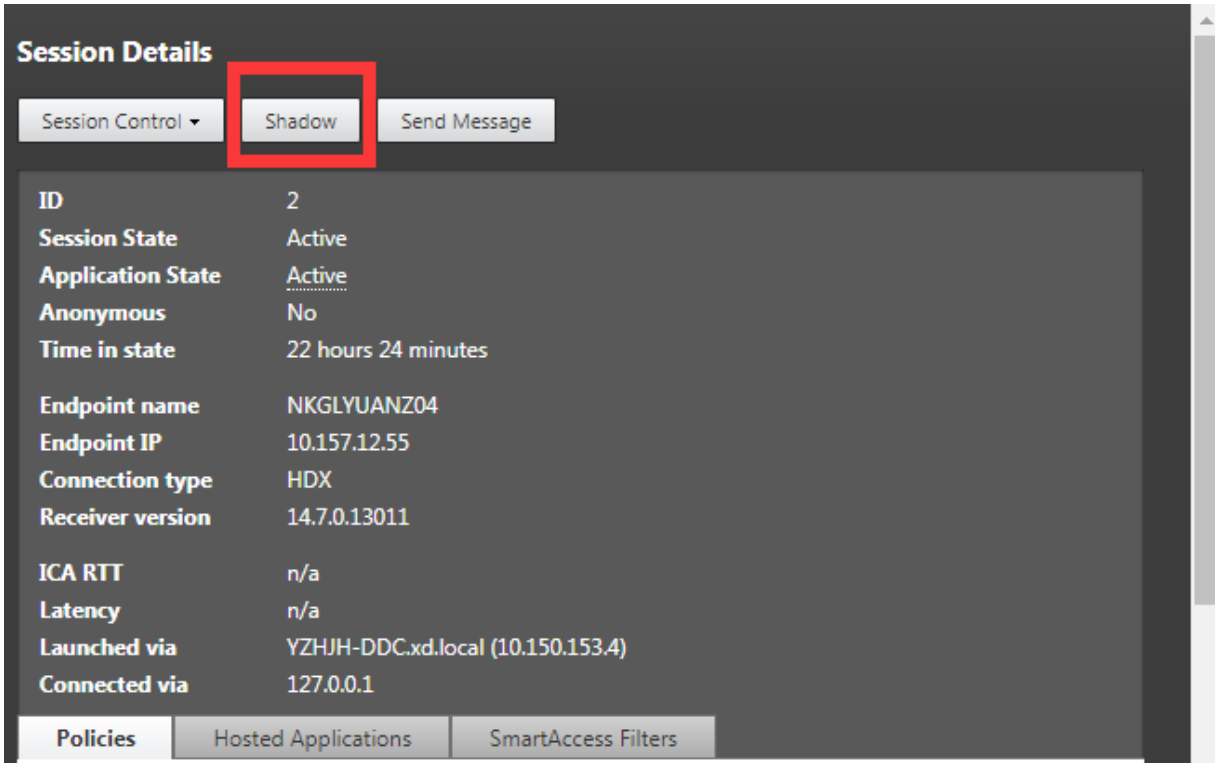
在每个 **Citrix Director** 客户端上安装根证书　会话重影与 IIS 使用相同的基于注册表的证书存储，因此您可以使用 IIS 或 Microsoft 管理控制台 (MMC) 证书管理单元安装根证书。收到 CA 的证书后，可在 IIS 中重新启动 Web 服务器证书向导，然后此向导将安装该证书。另外，您可以在使用 MMC 并将证书作为独立的管理单元添加的计算机上，查看并导入证书。默认情况下，Internet Explorer 和 Google Chrome 会导入安装在操作系统上的证书。对于 Mozilla Firefox，必须在证书管理器的 **Authorities**（颁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

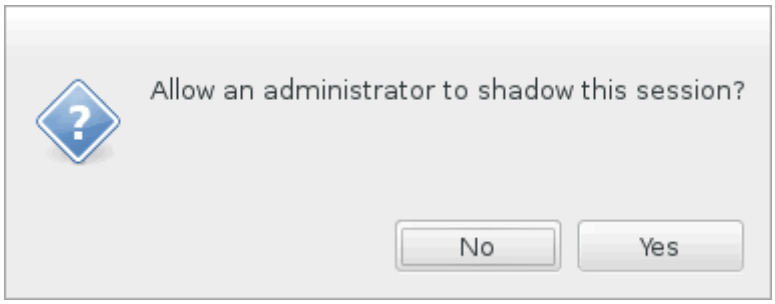
使用情况

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。

- 一个会话只能由一位管理员进行重影。例如，如果管理员 B 向会话管理员 A 发送重影请求，获取用户权限的确认信息会重新出现在用户设备上。如果用户同意，管理员 A 的重影连接将停止，并为管理员 B 构建新的重影连接。如果管理员为同一会话发送另一个重影请求，还可以构建新的重影连接。
- 要使用会话重影功能，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 上进行调试。

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。如果显示获取用户权限的确认信息，但连接建立失败，请手动 ping VDA 的 FQDN 以验证 Citrix Director 是否能够解析 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：

   ```
   <!-- Broker Agent Plugin - Director VDA plugin Logger -->

    <logger name="com.citrix.dmc">

      <level value="trace"/>

    </logger>
   <!--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，确认您已正确命名证书和密钥文件，并将其置于正确的路径下。
3. 确认 6001-6099 之间是否有足够的端口用于新的重影请求。

# 监视服务守护程序

November 4, 2022

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 **/opt/Citrix/VDA/sbin** 下的 **scanningpolicy.conf**、**rulesets.conf** 和 **whitelist.conf** 文件配置该功能。

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。

```
service ctxmonitorservice restart
<!--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。

## 工具和实用程序

May 8, 2023

### 会话数据查询实用程序

我们提供的实用程序 `ctxsdcutil` 可用于查询每个 Linux VDA 上的会话数据。要查询 VDA 上托管的所有会话或特定会话的以下数据，请运行 `/opt/Citrix/VDA/bin/ctxsdcutil -q <all | SessionID> [-c]` 命令。`[-c]` 参数表示每秒钟查询一次数据。

- 输入会话带宽
- 输出会话带宽、
- 输出会话线速度

- 延迟 - 上次记录
- 往返行程时间
- 输出 **ThinWire** 带宽
- 输出音频带宽
- 输出打印机带宽
- 输入驱动器带宽
- 输出驱动器带宽

### xdlcollect Bash 脚本

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，将在与脚本相同的文件夹中生成一个压缩的日志文件。`xdlcollect` Bash 脚本可能会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。

### XDPing

Linux **XDPing** 工具是一个命令行应用程序。它可以自动执行检查 Linux VDA 环境中的常见配置问题的过程。

Linux **XDPing** 工具在系统中执行 150 多个单独的测试，这些测试大致分类如下：

- 检查是否满足 Linux VDA 系统要求
- 识别和显示计算机信息，包括 Linux 发行版
- 检查 Linux 内核的兼容性
- 检查是否存在任何可能影响 Linux VDA 操作的已知 Linux 发行版问题
- 检查安全增强型 Linux (SELinux) 模式和兼容性
- 识别网络接口并检查网络设置
- 检查存储分区和可用的磁盘空间
- 检查计算机主机和域名配置
- 检查 DNS 配置并执行查找测试
- 识别基本虚拟机管理程序并检查虚拟机配置。支持：
  - Citrix Hypervisor
  - Microsoft HyperV
  - VMware vSphere
- 检查时间设置并检查网络时间同步是否可以运行
- 检查 PostgreSQL 服务是否正确配置和运行

- 检查防火墙是否已启用且所需端口是否已打开
- 检查 Kerberos 配置并执行身份验证测试
- 检查 LDAP 搜索环境中的组策略服务引擎
- 检查 Active Directory 集成是否已正确设置，以及当前计算机是否已加入域。支持：
  - Samba Winbind
  - Dell Quest Authentication Services
  - Centrify DirectControl
  - SSSD
- 检查 Active Directory 中 Linux 计算机对象的完整性
- 检查可插拔身份验证模块 (PAM) 配置
- 检查核心转储模式
- 检查是否安装了 Linux VDA 所需的软件包
- 识别 Linux VDA 软件包并检查安装的完整性
- 检查 PostgreSQL 注册表数据库的完整性
- 检查 Linux VDA 服务是否已正确配置和运行
- 检查 VDA 和 HDX 配置的完整性
- 探测配置的每个 Delivery Controller，以测试 Broker Service 是否可访问、运行且响应迅速
- 检查计算机是否已在 Delivery Controller 场中注册
- 检查每个活动或断开连接的 HDX 会话的状态
- 扫描日志文件中是否存在与 Linux VDA 相关的错误和警告
- 检查 Xorg 的版本是否适合

### 使用 **Linux XDPing** 工具

> 注意：
>
> 运行 ctxsetup.sh 不会安装 **XDPing**。可以运行 `sudo /opt/Citrix/VDA/bin/xdping` 来安装 **XDPing**。
> 此命令还会创建一个 **XDPing** 所需的 Python3 虚拟环境。如果此命令无法创建 Python3 虚拟环境，请按照创建 Python3 虚拟环境中的说明手动创建该环境。
>
> 要解决在使用 pip 工具时可能会遇到的 SSL 连接错误，请考虑将以下可信主机添加到 /etc/pip.conf 文件中：
>
> ```
> [global]
> trusted-host =
> pypi.org
> files.pythonhosted.org
> ```

**XDPing** 附带从命令 shell 运行的名为 `xdping` 的单个可执行文件。

要显示命令行选项，请使用 `-h` 选项：

```
sudo /opt/Citrix/VDA/bin/xdping -h
<!--NeedCopy-->
```

要运行全套测试，请在不使用任何命令行选项的情况下运行 `xdping`：

```
sudo /opt/Citrix/VDA/bin/xdping
<!--NeedCopy-->
```

要在安装 Linux VDA 软件包之前检查环境，请运行 `pre-flight` 测试：

```
sudo /opt/Citrix/VDA/bin/xdping --preflight
<!--NeedCopy-->
```

要仅运行特定的测试类别（例如，时间测试和 Kerberos 测试），请使用 `-T` 选项：

```
sudo /opt/Citrix/VDA/bin/xdping -T time,kerberos
<!--NeedCopy-->
```

要探测特定的 XenDesktop 控制器，请执行以下操作：

```
sudo /opt/Citrix/VDA/bin/xdping -d myddc.domain.net
<!--NeedCopy-->
```

示例输出　下面是运行 Kerberos 测试的示例输出：

```
sudo xdping -T kerberos

Root User -------------------------------------------------------------------
    User:         root
    EUID:         0
      Verify user is root                                                [Pass]

Kerberos --------------------------------------------------------------------
    Kerberos version: 5
      Verify Kerberos available                                          [Pass]
      Verify Kerberos version 5                                          [Pass]
    KRB5CCNAME:   [Not set]
                  Distro default FILE:/tmp/krb5cc_%{uid}
    KRB5CCNAME type: [Supported]
    KRB5CCNAME format: [Default]
      Verify KRB5CCNAME cache type                                       [Pass]
      Verify KRB5CCNAME format                                           [Pass]
    Configuration file: /etc/krb5.conf [Exists]
```

```
  Verify Kerberos configuration file found                              [Pass]
Keytab file:  /etc/krb5.keytab [Exists]
Default realm: XD2.LOCAL
Default realm KDCs: [NONE SPECIFIED]
Default realm domains: [NONE SPECIFIED]
DNS lookup realm: [Enabled]
DNS lookup KDC: [Enabled]
Weak crypto:  [Disabled]
Clock skew limit:  300 s
  Verify system keytab file exists                                      [Pass]
  Verify default realm set                                              [Pass]
  Verify default realm in upper-case                                    [Pass]
  Verify default realm not EXAMPLE.COM                                  [Pass]
  Verify default realm domain mappings                                  [Pass]
  Verify default realm master KDC configured                            [Pass]
  Verify Kerberos weak crypto disabled                                  [Pass]
  Verify Kerberos clock skew setting                                    [Pass]
Default ccache: [Not set]
               Distro default FILE:/tmp/krb5cc_%{uid}
Default ccache type: [Supported]
Default ccache format: [Default]
  Verify default credential cache cache type                            [Pass]
  Verify default credential cache format                                [Pass]
UPN system key [MYVDA1$@          ]: [MISSING]
SPN system key [host/m                  l]: [Exists]
  Verify Kerberos system keys for UPN exist                            [ERROR]
  No system keys were found for the user principal name (UPN) of
  the machine account. For the Linux VDA to mutually authenticate
  with the Delivery Controller, the system keytab file must
  contain keys for both the UPN and host-based SPN of the machine
  account.

      Verify Kerberos system keys for SPN exist                          [Pass]
    Kerberos login: [FAILED AUTHENTICATION]
                    Keytab contains no suitable keys for MYVDA1$@
                    while getting initial credentials
      Verify KDC authentication                                         [ERROR]
      Failed to authenticate and obtain a Ticket Granting Ticket (TGT)
      from the KDC authentication service for the machine account UPN
      MYVDA1$@          . Check that the Kerberos configuration is
      valid and the keys in the system keytab are current.


Summary ------------------------------------------------------------------------
  The following tests did not pass:
      Verify Kerberos system keys for UPN exist                         [ERROR]
      Verify KDC authentication                                         [ERROR]
```

## 其他

November 4, 2022

本部分内容包含以下主题：

- 适用于 HTML5 的 Citrix Workspace 应用程序支持
- 创建 Python3 虚拟环境
- 将 NIS 与 Active Directory 集成
- IPv6
- LDAPS
- **Xauthority**

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

November 4, 2022

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。

## 创建 **Python3** 虚拟环境

November 27, 2023

如果要连接到网络，运行 `sudo /opt/Citrix/VDA/bin/xdping` 或 `/opt/Citrix/VDA/sbin/enable_ldaps.sh` 命令可以创建 Python3 虚拟环境。但是，如果这些命令无法创建 Python3 虚拟环境，则即使没有网络连接，也可以手动创建。本文详细介绍了创建没有网络连接的 Python3 虚拟环境的必备条件和步骤。
/opt/Citrix/VDA/sbin/enable_ldaps.sh

### 必备条件

- 必须具有管理权限才能访问 `/opt/Citrix/VDA/sbin/ctxpython3` 目录。
- Python3 软件包的滚轮文件已准备就绪。可以从 https://pypi.org/ 下载滚轮文件。

### 创建 **Python3** 虚拟环境

请完成以下步骤以创建 Python3 虚拟环境：

1. 安装 Python3 依赖项。

   对于 **Amazon Linux 2**：

   ```
   yum -y install python3 python3-devel krb5-devel gcc
   <!--NeedCopy-->
   ```

   对于 **RHEL** 和 **Rock Linux**：

   ```
   yum -y install python36-devel krb5-devel gcc
   <!--NeedCopy-->
   ```

   > 注意：
   >
   > 您可能必须启用特定存储库才能安装某些依赖项。对于 RHEL 7，请运行 `subscription-manager repos --enable rhel-7-server-optional-rpms` 命令。对于 RHEL 8，请运行 `subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms` 命令。

对于 **Debian** 来说，**Ubuntu**：

```
apt-get -y install python3-dev python3-pip python3-venv libkrb5-dev
<!--NeedCopy-->
```

对于 **SUSE**：

```
zypper -n install lsb-release python3-devel python3-setuptools krb5-devel gcc libffi-devel libopenssl-devel
<!--NeedCopy-->
```

2. 创建 Python3 虚拟环境。

> 注意：
>
> 要解决在使用 pip 工具时可能会遇到的 SSL 连接错误，请考虑将以下可信主机添加到 /etc/pip.conf 文件中：
>
> ```
> [global]
> trusted-host =
> pypi.org
> files.pythonhosted.org
> ```

对于 **Amazon Linux 2**、**Debian**、**RHEL**、**Rocky Linux**、**Ubuntu**：

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
<!--NeedCopy-->
```

对于 **SUSE**：

```
export PATH=$PATH:/usr/lib/mit/bin:/usr/lib/mit/sbin

sudo mkdir -p /usr/lib/mit/include/gssapi/

sudo ln -s /usr/include/gssapi/gssapi_ext.h/usr/lib/mit/include/gssapi/gssapi_ext.h

sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
<!--NeedCopy-->
```

3. 安装 LDAPS 依赖项。

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --upgrade pip==21.3.1

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install cffi==1.15.0 cryptography==36.0.2 decorator==5.1.1 gssapi==1.7.3 ldap3==2.9.1 pyasn1==0.4.8 pycparser==2.21 six==1.16.0
<!--NeedCopy-->
```

4. 安装 **XDPing** 依赖项。

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --upgrade pip==21.3.1

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install asn1crypto==1.5.1 cffi==1.15.0 cryptography==36.0.2 decorator==5.1.1 gssapi==1.7.3 ldap3==2.9.1 netifaces==0.11.0 packaging==21.3 pg8000==1.26.0 psutil==5.9.0 pyasn1==0.4.8 pycparser==2.21 pyparsing==3.0.8 scramp==1.4.1 six==1.16.0 termcolor==1.1.0

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /opt/Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
<!--NeedCopy-->
```

## 将 **NIS** 与 **Active Directory** 集成

October 31, 2022

本文介绍如何在 Linux VDA 中使用 SSSD 将 NIS 与 Windows Active Directory (AD) 集成。Linux VDA 被视为 Citrix 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。

### 将 **NIS** 与 **AD** 相集成

要将 NIS 与 AD 集成，请完成以下步骤：

步骤 **1**：将 **Linux VDA** 添加为 **NIS** 客户端

配置 NIS 客户端：

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

设置 NIS 域：

```
ypdomainname nis.domain
echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
<!--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：

```
sudo authconfig --enablenis --nisdomain=nis.domain --nisserver=server.
   nis.domain --enablemkhomedir --update
<!--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：

```
sudo systemctl start rpcbind ypbind

sudo systemctl enable rpcbind ypbind
<!--NeedCopy-->
```

确保 NIS 配置正确：

```
ypwhich
<!--NeedCopy-->
```

验证可从 NIS 服务器获得帐户信息：

```
getent passwd nisaccount
<!--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。

步骤 **2**：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:

将计算机配置为进行 Samba 和 Kerberos 身份验证：

```
sudo authconfig --smbsecurity=ads --smbworkgroup=domain --smbrealm=
   REALM --krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --update
<!--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
winbind offline logon = no
```

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。

```
sudo net ads join REALM -U user
<!--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。

步骤 **3**：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/sssd/sssd.conf** **sssd.conf** 配置示例（可以根据需要添加更多选项）：

```
[sssd]
config_file_version = 2
domains = EXAMPLE
services = nss, pam

[domain/EXAMPLE]
# Uncomment if you need offline logins
# cache_credentials = true
re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@(?P<domain>.+$))|(^(?P<name>[^@\\]+)$))
id_provider = proxy
proxy_lib_name = nis
auth_provider = ad
access_provider = ad

# Should be specified as the long version of the Active Directory domain.
ad_domain = EXAMPLE.COM

# Kerberos settings
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U

# Uncomment if service discovery is not working
# ad_server = server.ad.example.com

# Comment out if the users have the shell and home dir set on the AD side
default_shell = /bin/bash
fallback_homedir = /home/%d/%u

# Uncomment and adjust if the default principal SHORTNAME$@REALM is not available
# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
<!--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/sssd/sssd.conf
chmod 0600 /etc/sssd/sssd.conf
restorecon /etc/sssd/sssd.conf
```

步骤 **4**：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：

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

sudo systemctl start sssd

sudo systemctl enable sssd
<!--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。

步骤 **3**：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：

```
sudo klist -ke
<!--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：

```
sudo kinit  -k MACHINE$@REALM
<!--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：

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

步骤 **6**：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：

```
sudo getent passwd DOMAIN\username
<!--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。

```
sudo ssh localhost  - l DOMAIN\username

id -u
<!--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：

```
ls /tmp/krb5cc_{
 uid }

<!--NeedCopy-->
```

检查用户 Kerberos 凭据缓存中的票据是否有效且未过期：

```
klist
<!--NeedCopy-->
```

## IPv6

October 31, 2022

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：

```
“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。

## LDAPS

November 4, 2022

LDAPS 是轻型目录访问协议 (LDAP) 的安全版本，其中 LDAP 通信使用 TLS/SSL 进行加密。

默认不加密客户端与服务器应用程序之间的 LDAP 通信。通过 LDAPS，您可以保护 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

> 注意：
>
> 可以运行以下命令为 LDAP 服务器设置监视周期。默认值为 15 分钟。请至少将其设置为 10 分钟。

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
   VirtualDesktopAgent" -v "ListOfLDAPServersMonitorPeroid" -t "
   REG_DWORD" -d "0x0000000f" --force
<!--NeedCopy-->
```

### 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 LDAPS。

有关如何安装证书并验证 LDAPS 连接的详细信息，请参阅 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 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**

要在 Linux VDA 上启用或禁用 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：

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
<!--NeedCopy-->
```

- 利用通道绑定通过 SSL/TLS 启用 LDAP：

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enablecb pathToRootCA
<!--NeedCopy-->
```

> 注意：
>
> 用于通道绑定的根 CA 证书必须采用 PEM 格式。如果启用 LDAPS 无法成功创建 Python3 虚拟环境，请按照创建 Python3 虚拟环境中的说明手动创建该环境。
>
> 要解决在使用 pip 工具时可能会遇到的 SSL 连接错误，请考虑将以下可信主机添加到 /etc/pip.conf 文件中：
>
> ```
> [global]
> trusted-host =
> pypi.org
> files.pythonhosted.org
> ```

- 回退到未启用 SSL/TLS 的 LDAP

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
<!--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：

```
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers

HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy

HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS

HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore

HKLM\Software\Citrix\VirtualDesktopAgent\EnableChannelBinding
<!--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）不能与端口 389 上的 STARTTLS 共存。

### SSSD

根据选项在端口 636 或端口 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，可以通过 SASL GSSAPI 签名和封装配置安全 LDAP，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** 的情况下意外更新了 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。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，我们建议您使用 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/xdl/.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。

## Xauthority

October 31, 2022

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：

```
# xauth -f ~/.Xauthority

# > list

# > us01msip06:107  MIT-MAGIC-COOKIE-1
      fb228d1b695729242616c5908f11624b
<!--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：

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "
   XauthEnabled" -d "0x00000001" --force

sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "ListenTCP"
    -d "0x00000001" --force
<!--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` 文件中的显示编号，`XAUTHORITY` 是 **Xauthority** 的文件路径。例如，请查看以下命令：

```
export DISPLAY={
Display number stored in the Xauthority file }


export XAUTHORITY={
the file path of .Xauthority }

<!--NeedCopy-->
```

> 注意：
>
> 如果未设置 **XAUTHORITY** 环境变量，则默认使用 `~/.Xauthority` 文件。

- 通过挂载共享主目录将 `.Xauthority` 文件传递到 XClient

  最便捷的方式是为登录用户装载共享主目录。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** 无法正常运行，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：

   ```
   ps aux | grep -i xorg
   <!--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：

   ```
   /var/xdl/xauth/.Xauthority110
   <!--NeedCopy-->
   ```

   使用 **Xauth** 命令显示 cookie：

   ```
   Xauth -f /var/xdl/xauth/.Xauthority110
   <!--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 地址访问远程显示端口，并检查已发布的桌面的显示数量。

例如，在 XClient 计算机上运行以下命令：

```
telnet 10.158.11.11 6160
<!--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。

## 身份验证

November 4, 2022

本部分内容包含以下主题：

- 使用 Azure Active Directory 进行身份验证
- 双跃点单点登录身份验证
- 联合身份验证服务
- 非 SSO 身份验证
- 智能卡
- 匿名用户进行的未经身份验证的用户

## 使用 **Azure Active Directory** 进行身份验证

September 25, 2023

> 注意：
>
> 此功能仅适用于 Azure 托管的 VDA。

根据您的需求，可以在 Azure 中部署两种类型的 Linux VDA：

- 加入了 Azure AD DS 的 VM。VM 已加入到 Azure Active Directory (AAD) 域服务 (DS) 托管的域。用户使用其域凭据登录 VM。
- 未加入域的 VM。VM 与 AAD 标识服务集成以提供用户身份验证。用户使用其 AAD 凭据登录 VM。

有关 AAD DS 和 AAD 的详细信息，请参阅这篇 Microsoft 文章。

本文介绍了如何在未加入域的 VDA 上启用和配置 AAD 标识服务。

支持的发行版

- Ubuntu 22.04、20.04、18.04
- RHEL 8.6、8.4、7.9
- SUSE 15.3
- Debian 10

有关详细信息，请参阅这篇 Microsoft 文章。

已知问题及解决方法

在 Red Hat 8.3 和 7.9 中，在执行 AAD 用户身份验证之后，PAM（Pluggable Authentication Module，可插拔身份验证模块）`pam_loginuid.so` 无法设置 `loginuid`。此问题会阻止 AAD 用户访问 VDA 会话。

要解决此问题，请在 `/etc/pam.d/remote` 中注释掉行 `Session required pam_loginuid.so`。有关示例，请参见以下屏幕截图。

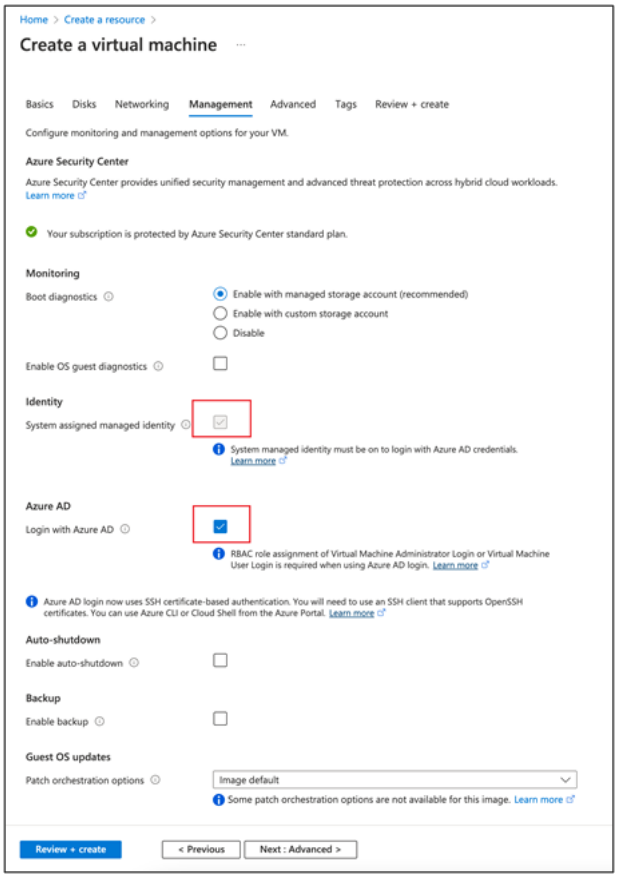
```
#%PAM-1.0
auth       substack     password-auth
auth       include      postlogin
account    required     pam_nologin.so
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
#session    required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      password-auth
session    include      postlogin
```

步骤 **1**：在 **Azure** 门户上创建模板 **VM**

创建模板 VM 并在 VM 上安装 Azure CLI。

1. 在 Azure 门户上，创建模板 VM。在单击检查 **+** 创建之前，请务必在管理选项卡上选择 **Login with Azure AD**（使用 Azure AD 登录）。




2. 在模板 VM 上安装 Azure CLI。
   有关详细信息，请参阅这篇 Microsoft 文章。

### 步骤 **2**：在模板 **VM** 上准备主映像

要准备主映像，请按照使用 MCS 在 Azure 上创建 Linux VM 中的步骤 **3**：准备主映像进行操作。

### 步骤 **3**：将模板 **VM** 设置为未加入域的模式

创建主映像后，请按照以下步骤将 VM 设置为未加入域的模式：

1. 从命令提示符运行以下脚本：

```
Modify /var/xdl/mcs/mcs_util.sh
<!--NeedCopy-->
```

2. 找到 `function read_non_domain_joined_info()`，然后将 `NonDomainJoined` 的值更改为 2。有关示例，请参阅以下代码块。

```
function read_non_domain_joined_info()
{
```

```
3
4  log "Debug: Enter read_non_domain_joined_info"
5  # check if websocket enabled
6  TrustIdentity=`cat ${
7   id_disk_mnt_point }
8   ${
9   ad_info_file_path }
10    | grep '[TrustIdentity]' | sed 's/\s//g'`
11 if [ "$TrustIdentity" == "[TrustIdentity]" ]; then
12 NonDomainJoined=2
13 fi
14 ...
15  }
16
17 <!--NeedCopy-->
```

3. 保存更改。
4. 关闭模板 VM。

### 步骤 **4**：从模板 **VM** 创建 **Linux VM**

准备好未加入域的模板 VM 后，请按照以下步骤创建 VM：

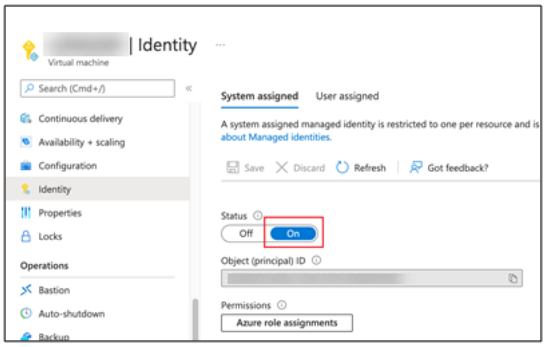
1. 登录 Citrix Cloud。
2. 双击 Citrix DaaS，然后访问完整配置管理控制台。
3. 在计算机目录中，选择使用 Machine Creation Services 从模板 VM 创建 Linux VM。有关详细信息，请参阅 Citrix DaaS 文档中的未加入域的 VDA。

### 步骤 **5**：将 **AAD** 用户帐户分配给 **Linux VM**

创建未加入域的 VM 后，为其分配 AAD 用户帐户。

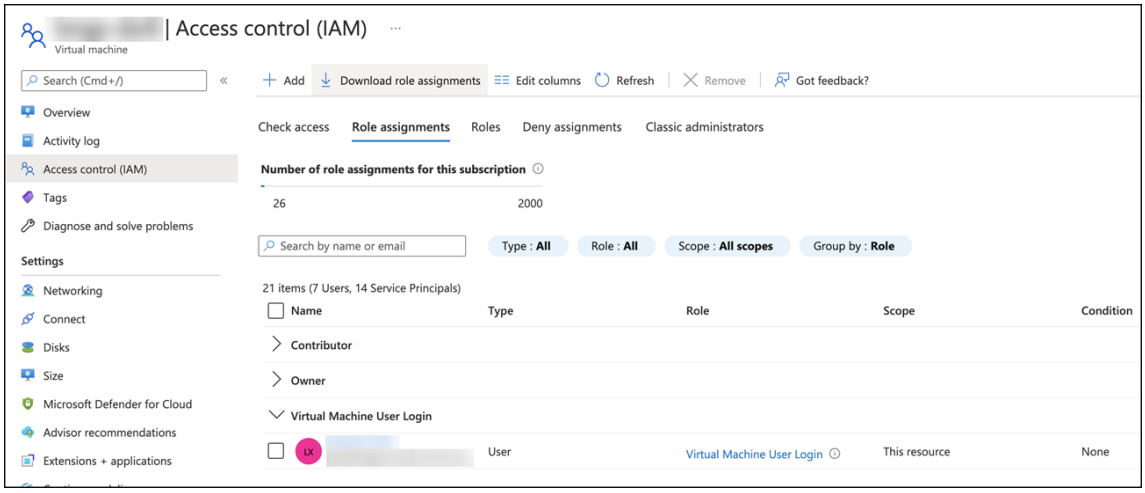
要将 AAD 用户帐户分配给 VM，请执行以下步骤：

1. 使用管理员帐户访问 VM。
2. 在 **Identify**（识别）**> System assigned**（系统分配）选项卡上，启用 **System Identity**（系统标识）。



3. 在 **Access control (IAM)**（访问控制 **(IAM)**）**> Role assignments**（角色分配）选项卡上，找到 **Virtual Machine User Login**（虚拟机用户登录）区域，然后根据需要添加 AAD 用户帐户。




登录到未加入域的 **VDA**

贵组织中的最终用户可以通过两种方式登录未加入域的 VDA。详细步骤如下所示：

1. 启动 Workspace 应用程序，然后通过输入 AAD 用户名和密码登录到 Workspace。此时将显示 Workspace 页面。
2. 双击未加入域的桌面。此时将显示 AAD 登录页面。

   该页面因 VDA 上设置的登录模式而异：设备代码或 AAD 帐户/密码。默认情况下，Linux VDA 使用设备代码登录模式对 AAD 用户进行身份验证，如下所示。作为管理员，您可以根据需要将登录模式更改为 AAD 帐户/密码。有关详细步骤，请参阅以下部分。


3. 根据屏幕上的说明，通过以下方式之一登录到桌面会话：

   - 扫描 QR 代码并输入该代码。
   - 输入 AAD 用户名和密码。

更改为 **AAD** 帐户**/**密码登录模式

默认情况下，Linux VDA 使用设备代码对 AAD 用户进行身份验证。有关详细信息，请参阅这篇 Microsoft 文章。要将登录模式更改为 *AAD* 帐户/密码，请执行以下步骤：

在 VDA 上运行以下命令，找到注册表项 `AADAcctPwdAuthEnable`，然后将其值更改为 `0x00000001`。

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
    Services\CitrixBrokerAgent\WebSocket" -t "REG_DWORD" -v "
    AADAcctPwdAuthEnable" -d "0x00000001" --force

<!--NeedCopy-->
```

> 注意：
>
> 此方法不适用于 Microsoft 帐户或启用了双重身份验证的帐户。

## 双跃点单点登录身份验证

November 4, 2022

可以将用于访问 StoreFront 应用商店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 模块中。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：

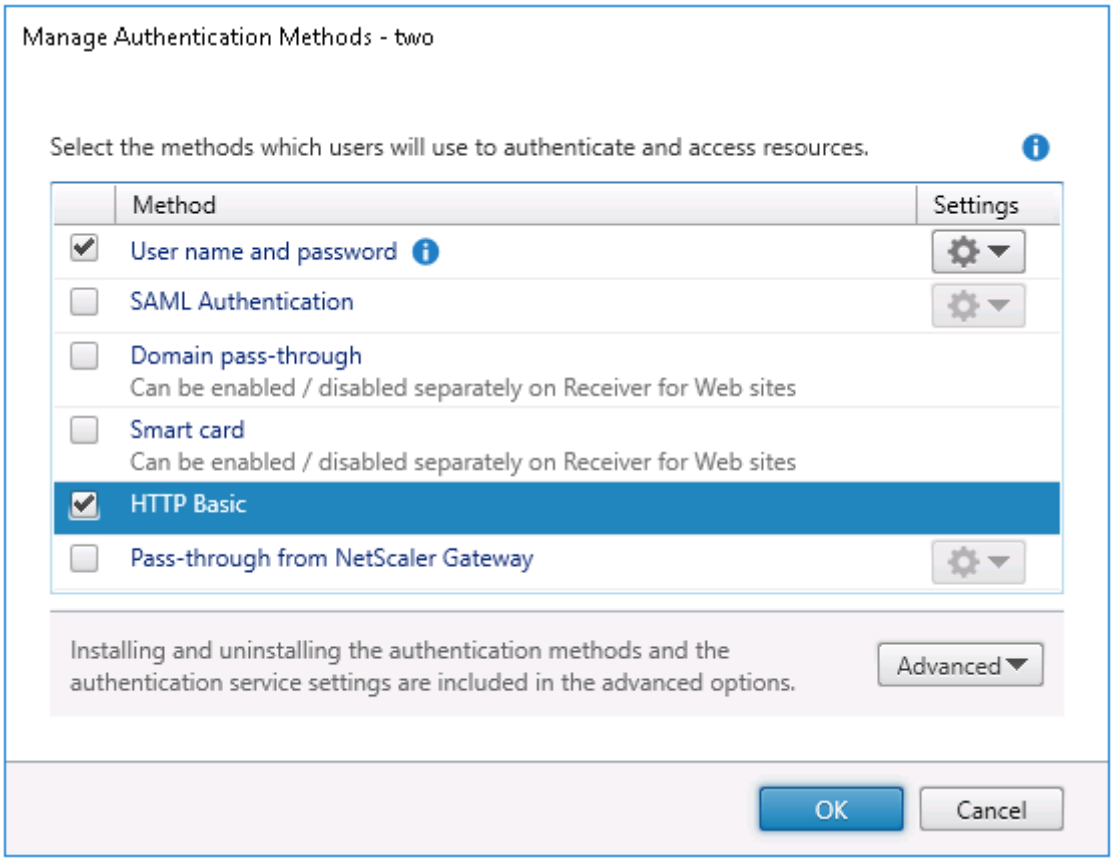
1. 在 Linux VDA 上，安装适用于 Linux 的 Citrix Workspace 应用程序或 Citrix Receiver for Linux 13.10。

   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/。如果要将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：

```
<Protocols>
     <HTTPBasic>
         <Enabled>True</Enabled>
    </HTTPBasic>
</Protocols>
<!--NeedCopy-->
```

4. 请运行以下命令以在指定目录中安装根证书。

```
cp rootcert.pem $ICAROOT/keystore/cacerts/
$ICAROOT/util/ctx_rehash  $ICAROOT/keystore/cacerts/
<!--NeedCopy-->
```

5. 运行以下命令以启用该功能：

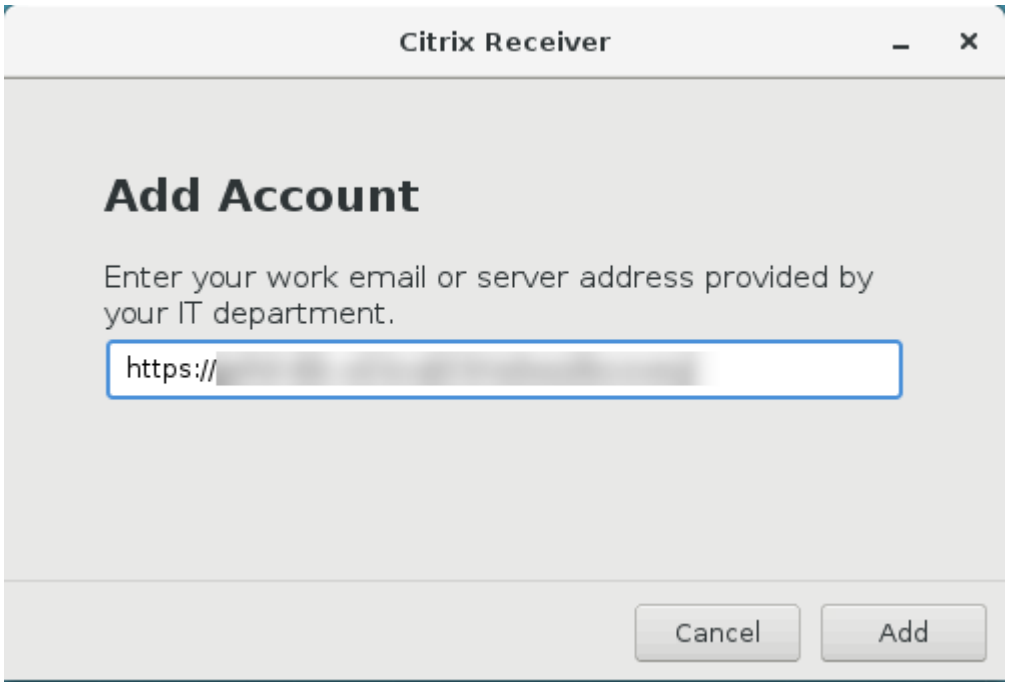
```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d "0
   x00000001"
<!--NeedCopy-->
```

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 Citrix Workspace 应用程序时，系统会提示您输入应用商店帐户。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。




## 联合身份验证服务

### February 9, 2024

可以使用联合身份验证服务 (FAS) 对登录到 Linux VDA 的用户进行身份验证。对于 FAS 登录功能，Linux VDA 将使用与 Windows VDA 相同的 Windows 环境。有关为 FAS 配置 Windows 环境的信息，请参阅联合身份验证服务。本文提供了特定于 Linux VDA 的额外信息。

> 注意：
>
> - Linux VDA 不支持会话中行为策略。
> - Linux VDA 使用短连接与 FAS 服务器传输数据。
> - 自 2206 版起，您可以通过 ctxsetup.sh 中的 CTX_XDL_FAS_LIST 在 Linux VDA 端自定义 FAS 端口。有关详细信息，请参阅基于您的发行版的 Linux VDA 安装文章。

## 在 **Linux VDA** 上配置 **FAS**

### **RHEL 8** 和 **Rocky Linux 8** 上支持 **FAS**

FAS 依赖于 pam_krb5 模块，该模块在 RHEL 8 和 Rocky Linux 8 上已弃用。要在 RHEL 8 和 Rocky Linux 8 上使用 FAS，请按如下所示构建 pam_krb5 模块：

1. 从以下 Web 站点下载 pam_krb5-2.4.8-6 源代码。

   https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html。

2. 在 RHEL 8 和 Rocky Linux 8 上构建并安装 pam_krb5 模块。

```
yum install make gcc krb5-devel pam-devel autoconf libtool
rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div
tar xvzf pam_krb5-2.4.8.tar.gz
cd pam_krb5-2.4.8
./configure --prefix=/usr
make
make install
<!--NeedCopy-->
```

3. 验证 pam_krb5.so 是否存在于 /usr/lib64/security/ 下。

```
ls -l /usr/lib64/security | grep pam_krb5
<!--NeedCopy-->
```

#### 设置 **FAS** 服务器

要在全新的 Linux VDA 安装中使用 FAS，请在运行 ctxinstall.sh 或 ctxsetup.sh 时键入每台 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，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。

要升级现有的 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。

```
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

service ctxjproxy restart

service ctxvda restart
<!--NeedCopy-->
```

要通过 `ctxreg` 更新 FAS 服务器，请运行以下命令：

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
    VirtualDesktopAgent\Authentication\UserCredentialService" -v "
    Addresses" -d "<Your-FAS-Server-List>"
```

```
2
3 service ctxjproxy restart
4
5 service ctxvda restart
6 <!--NeedCopy-->
```

安装证书

要验证用户的证书，请在 VDA 上安装根 CA 证书以及所有中间证书。例如，要安装根 CA 证书，请从前面的从 **Microsoft CA**（在 **AD** 中）检索 **CA** 证书步骤中获取 AD 根证书，或者从根 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。

运行 **ctxfascfg.sh**

运行 ctxfascfg.sh 脚本以配置 FAS：

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

添加环境变量，以便 `ctxfascfg.sh` 可以在静默模式下运行：

- **CTX_FAS_ADINTEGRATIONWAY=winbind | sssd | centrify | pbis**：表示 Active Directory 集成方法，该方法在指定 `CTX_EASYINSTALL_ADINTEGRATIONWAY` 时为 `CTX_EASYINSTALL_ADINTEGRATIONWA`。如果未指定 `CTX_EASYINSTALL_ADINTEGRATIONWAY`，`CTX_FAS_ADINTEGRATIONWAY` 将使用自己的值设置。
- **CTX_FAS_CERT_PATH =<certificate path>**：指定存储根证书和所有中间证书的完整路径。
- **CTX_FAS_KDC_HOSTNAME**：在选择 PBIS 时指定密钥发行中心 (KDC) 的主机名。

- **CTX_FAS_PKINIT_KDC_HOSTNAME**：指定 PKINIT KDC 主机名，除非另有说明，否则该名称为 CTX_FAS_KDC_HOSTNAME。

选择正确的 Active Directory 集成方法，然后键入正确的证书路径（例如 /etc/pki/CA/certs/）。

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 Linux 平台和 AD 集成方法。请参阅以下列表：

| | Winbind | SSSD | Centrify | PBIS |
|---|---|---|---|---|
| Amazon Linux 2 | 是 | 是 | 是 | 是 |
| Debian 11.3、Debian 10.9 | 是 | 是 | 是 | 是 |
| RHEL 8.6、RHEL 8.4 | 是 | 是 | 是 | 是 |
| RHEL 7.9/CentOS 7.9 | 是 | 是 | 是 | 是 |
| Rocky Linux 8 | 是 | 是 | 否 | 否 |
| SLES 15.3 | 是 | 是 | 是 | 否 |
| Ubuntu 22.04、Ubuntu 20.04、Ubuntu 18.04 | 是 | 是 | 是 | 是 |

- 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，并且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。

检查 **/var/log/xdl/hdx.log** 并查找类似如下内容的错误日志：

```
2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: [Logon Type] Federated Authentication Logon.

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: entry

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas: start connect to server 0

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas0: failed to connect: Connection refused.

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: failed to connect to server [0], please confirm if fas service list is well configurated in condb

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: exit, 43

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: failed to validate fas credential

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: LoginBoxValidate: failed validation of user 'user1@CTXDEV.LOCAL', INVALID_PARAMETER

<!--NeedCopy-->
```

解决方案　请运行以下命令以确认 Citrix 注册表值“HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent\Auth
是否设置为 <Your-FAS-Server-List>。

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
<!--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。

**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：

```
2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: entry

2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin: check_caller:
   current process: pid [30656], name [/opt/Citrix/VDA/bin/ctxlogin]

2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
   get_public_certificate: entry

2021-01-28 01:47:46.211 <P30656:S5> citrix-ctxlogin: query_fas: waiting
    for response...

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: query_fas: query
   to server success

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin:
   get_public_certificate: exit

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
    input size 1888

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
    output size 1415

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: get logon certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: cache_certificate:
    cache certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: exit, 0

2021-01-28 01:47:48.060 <P30656:S5> citrix-ctxlogin: validate_user:
   pam_authenticate err,can retry for user user1@CTXDEV.LOCAL
<!--NeedCopy-->
```

解决方案　验证您是否已在 /etc/krb5.conf 中正确设置存储根 CA 证书和所有中间证书的完整路径。完整路径如下所示：

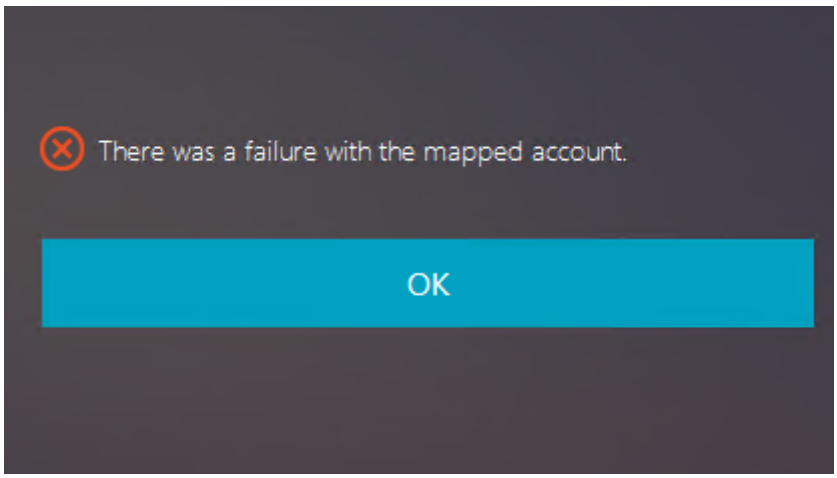
```
 [realms]

EXAMPLE.COM = {


    ......

    pkinit_anchors = DIR:/etc/pki/CA/certs/

    ......

 }

<!--NeedCopy-->
```

如果现有设置不正确，请按照前面的安装证书步骤重新对其进行设置。

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。



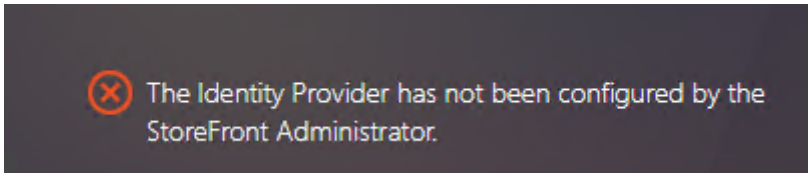

此错误表明已成功验证 ADFS 用户，但在 AD 上没有配置任何重影用户。

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：




当 FAS 应用商店配置为使用 SAML 身份验证，但缺少 ADFS 部署时，会出现此问题。

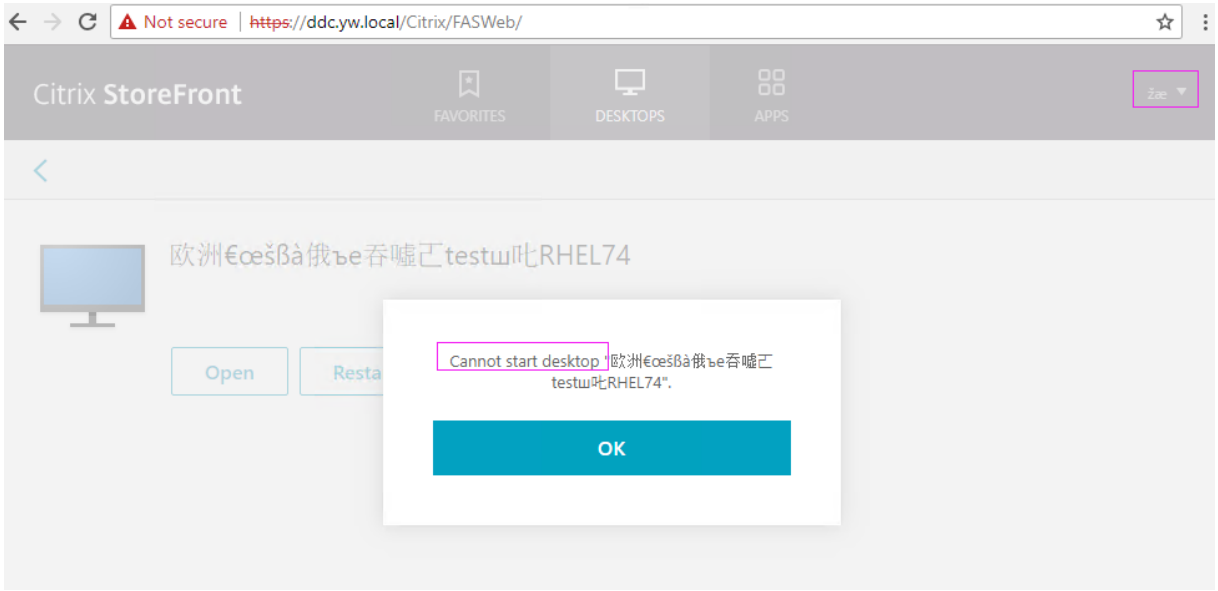
解决方案　为联合身份验证服务部署 ADFS IdP。有关详细信息，请参阅联合身份验证服务 ADFS 部署。

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

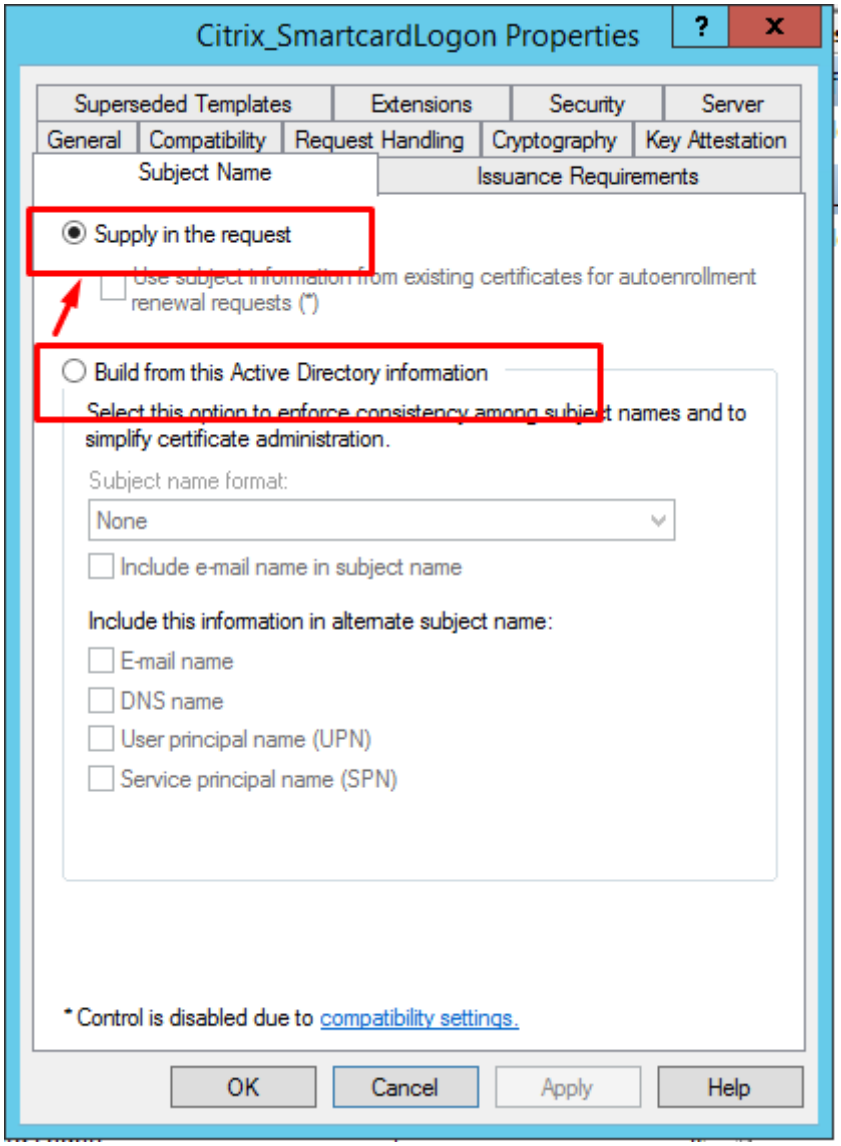
如果正在使用 FAS，则尝试启动包含非英语字符的已发布桌面或应用程序会话时，可能会失败。




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）：




## 非 **SSO** 身份验证

October 31, 2022

本文提供有关如何在 Linux VDA 上启用非 SSO 身份验证的指导。

### 概述

默认情况下，Linux VDA 已启用单点登录 (SSO)。用户使用一组凭据登录 Citrix Workspace 应用程序和 VDA 会话。

要让用户使用一组不同的凭据登录 VDA 会话，请在 Linux VDA 上禁用 SSO。下表列出了非 SSO 场景中支持的用户身份验证方法的组合。

| Citrix Workspace 应用程序 | VDA 会话 |
| --- | --- |
| 用户名 | 用户名 |
| 智能卡 | 用户名 |
| 用户名 | 智能卡 |

#### 禁用 **SSO**

在您的 Linux VDA 上运行以下命令：

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
     Control\Citrix\WinStations\tcp" -t "REG_DWORD" -v "
     fPromptForDifferentUser" -d "0x00000001" --force
2 <!--NeedCopy-->
```

### 智能卡

November 4, 2022

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以及向 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。

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

#### 必备条件

智能卡直通身份验证的可用性取决于以下条件：

- 您的 Linux VDA 安装在下面其中一个发行版中：
  - RHEL 8
  - RHEL 7/CentOS 7
  - Rocky Linux 8

  - Ubuntu 22.04
  - Ubuntu 20.04
  - Ubuntu 18.04
  - Debian 11.3
  - Debian 10.9

  完成安装 VDA 后，请验证您的 VDA 是否能够在 Delivery Controller 中注册，以及是否能够使用 Windows 凭据打开已发布的 Linux 桌面会话。

- 使用 OpenSC 支持的智能卡。有关详细信息，请参阅确保 OpenSC 支持智能卡。
- 使用 Citrix Workspace for Windows 的应用程序。

### 确保 **OpenSC** 支持智能卡

OpenSC 是 RHEL 7.4+ 上广泛使用的智能卡驱动程序。作为 CoolKey 的完全兼容替代品，OpenSC 支持多种类型的智能卡（请参阅 Red Hat Enterprise Linux 中的智能卡）。

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。OpenSC 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 Linux 发行版或 OpenSC 软件包的物理机。有关 OpenSC 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 OpenSC 是否支持智能卡：

```
pkcs11-tool --module opensc-pkcs11.so --list-slots
<!--NeedCopy-->
```

配置

准备根证书

根证书用于验证智能卡上的证书。完成以下步骤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。

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

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

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

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

在 **RHEL 8** 和 **Rocky Linux 8** 上构建 **pam_krb5** 模块

智能卡身份验证依赖于 pam_krb5 模块，该模块在 RHEL 8 和 Rocky Linux 8 上已弃用。要在 RHEL 8 和 Rocky Linux 8 上使用智能卡身份验证，请按如下所示构建 pam_krb5 模块：

1. 从 https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html 下载 pam_krb5-2.4.8-6 源代码。
2. 在 RHEL 8 和 Rocky Linux 8 上构建并安装 pam_krb5 模块。

   ```
   yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-
       tools
   yum install gcc krb5-devel pam-devel autoconf libtool
   rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio  - div
   tar xvzf pam_krb5-2.4.8.tar.gz
   cd pam_krb5-2.4.8
   ./configure --prefix=/usr
   make
   make install
   <!--NeedCopy-->
   ```

3. 验证 pam_krb5.so 是否存在于 /usr/lib64/security/ 下。

   ```
   ls -l /usr/lib64/security | grep pam_krb5
   <!--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完成配置。

（选项 **1**）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。

```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
<!--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：

```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
<!--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.
```

（选项 **2**）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，请确保您已正确配置所有组件并将私钥和用户证书下载到智能卡，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：

**RHEL 8**、**Rocky Linux 8**、**RHEL 7/CentOS 7**：

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

**Ubuntu 22.04**、**Ubuntu 20.04**、**Ubuntu 18.04**、**Debian 11.3**、**Debian 10.9**：

```
apt-get install -y libpcsclite1 libccid
<!--NeedCopy-->
```

安装智能卡读卡器　OpenSC 是广泛使用的智能卡驱动程序。如果未安装 OpenSC，请运行以下命令以进行安装：

**RHEL 8**、**Rocky Linux 8**、**RHEL 7/CentOS 7**：

```
yum install opensc
<!--NeedCopy-->
```

**Ubuntu 22.04**、**Ubuntu 20.04**、**Ubuntu 18.04**、**Debian 11.3**、**Debian 10.9**：

```
apt-get install -y opensc
<!--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。

**RHEL 7/CentOS 7**:

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

**RHEL 8**、**Rocky Linux 8**:

```
yum install krb5-pkinit
<!--NeedCopy-->
```

**Ubuntu 22.04**、**Ubuntu 20.04**、**Ubuntu 18.04**:

```
apt-get install libpam-krb5 krb5-pkinit
<!--NeedCopy-->
```

**Debian 11.3**、**Debian 10.9**:

```
apt-get install -y libpam-krb5 krb5-pkinit
<!--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：

```
authconfig --enablekrb5 --update
<!--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：

```
EXAMPLE.COM = {


    kdc = KDC.EXAMPLE.COM

    auth_to_local = RULE:[1:$1@$0]
```

```
7
8       pkinit_anchors = FILE:<path where you install the root certificate
            >/certnew.pem
9
10      pkinit_kdc_hostname = KDC.EXAMPLE.COM
11
12      pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
13
14      pkinit_eku_checking = kpServerAuth
15
16    }
17
18  <!--NeedCopy-->
```

添加 PKINIT 信息后，该配置文件将如下所示。

```
CTXDEV.LOCAL = {
     kdc = ctx-ad.ctxdev.local
     auth_to_local = RULE:[1:$1@$0]
     pkinit_kdc_hostname = ctx-ad.ctxdev.local
     pkinit_anchors = FILE:/etc/pki/CA/certs/certnew.pem
     pkinit_eku_checking = kpServerAuth
     pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
 }
```

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:<path to the pkcs11 driver>/opensc-pkcs11.
so
```

如果使用 SSSD，则修改后该配置文件将如下所示。

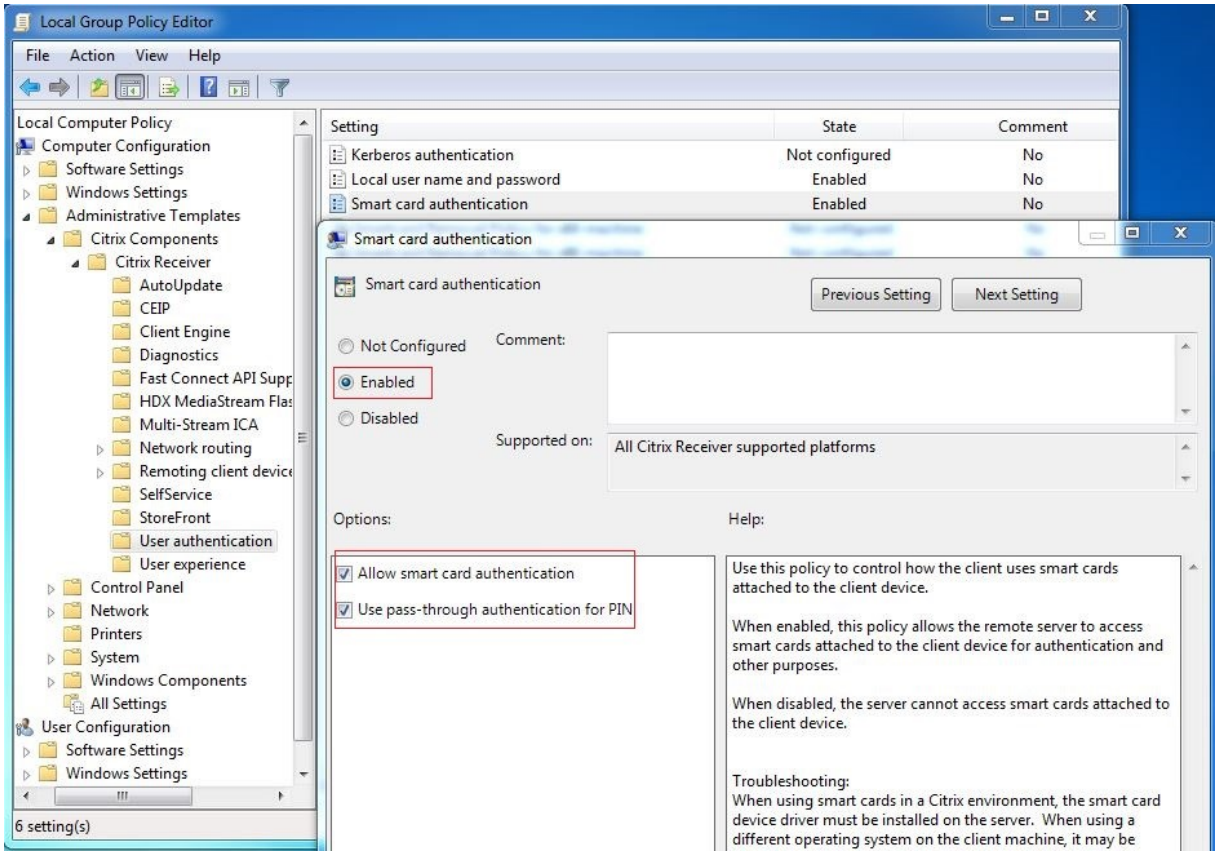
```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done ignore=ignore default=die]  pam_krb5.so preauth_opt=X509_user_identity=PKCS11:/usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so
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

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
```

（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：

```
[WFClient]
SmartCardCryptographicRedirection=On
<!--NeedCopy-->
```

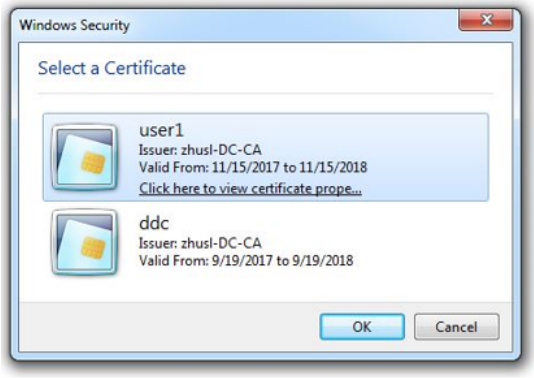
在客户端上禁用快速智能卡登录　要在客户端上禁用快速智能卡登录，请从关联的 StoreFront 站点的 default.ica 文件中删除 **SmartCardCryptographicRedirection** 参数。

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。

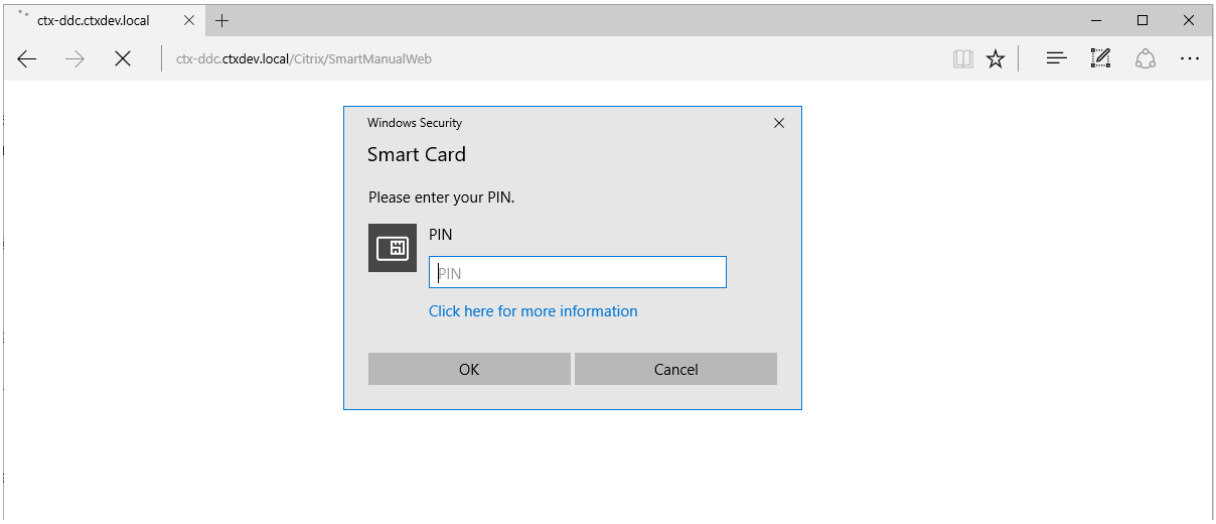




在 StoreFront 中启动 Linux Virtual Desktop 会话时，将显示 Linux VDA 登录对话框，如下所示。用户名是从智能卡中的证书中提取的，必须重新键入 PIN 码以进行登录身份验证。

此行为与 Windows VDA 相同。

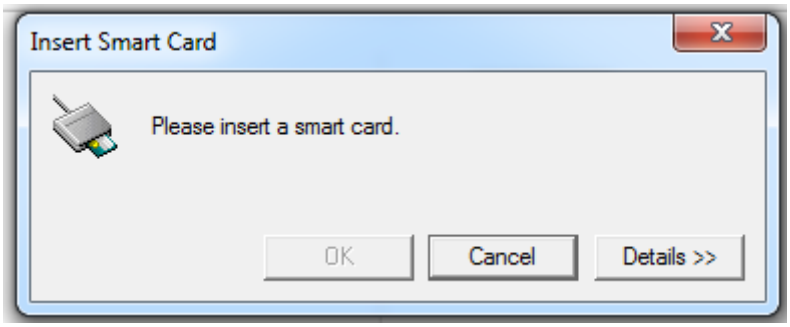
 




使用智能卡重新连接到会话

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

现在，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 OpenSC 智能卡，但是您可以尝试使用其他智能卡和 PKCS#11 库，因为 Citrix 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 `opensc-pkcs11.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：

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v "
   PKCS11LibPath" -d "PATH"
<!--NeedCopy-->
```

   其中 **PATH** 指向您的 PKCS#11 库，例如 /usr/lib64/pkcs11/opensc-pkcs11.so

3. 在客户端上禁用快速智能卡登录。

## 匿名用户进行的未经身份验证的用户

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，将此注册表设置设为 5 分钟：

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k  "HKLM\System\
   CurrentControlSet\Control\Citrix"  -v AnonymousUserIdleTime  -d 0
   x00000005
<!--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：

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
    CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber -d 0
    x00000020
<!--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）：

```
sudo /opt/Citrix/VDA/bin/ctxreg read -k "HKLM\System\CurrentControlSet
    \Control\Citrix" -v MaxAnonymousUserNumber
<!--NeedCopy-->
```

确认 **ncsd** 服务是否正在运行，且已配置为启用 **passwd** 缓存：

```
ps uax | grep nscd
cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
<!--NeedCopy-->
```

如果已启用，请将 **Passwd** 缓存变量设置为 **no**，然后重新启动 **ncsd** 服务。更改此配置后您可能需要重新安装 Linux VDA。

- 使用 **KDE** 时未经身份验证的会话中显示锁屏按钮。

默认情况下未经身份验证的会话中禁用锁屏按钮和菜单。但是，它们仍可显示在 KDE 中。在 KDE 中，要对特定用户禁用锁屏按钮和菜单，请将以下行添加到配置文件 **$Home/.kde/share/config/kdeglobals** 中。例如：

```
[KDE Action Restrictions]
action/lock_screen=false
<!--NeedCopy-->
```

但是，如果在全局范围的 `kdeglobals` 文件（如 `/usr/share/kde-settings/kde-profile/default/share/config/kdeglobals`）中将 `KDE Action Restrictions` 参数配置为不可变，用户配置将不起作用。

要解决此问题，请修改系统范围的 `kdeglobals` 文件以删除 `[KDE Action Restrictions]` 部分中的 `[$i]` 标记，或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 页面。

## 文件

### October 31, 2022

本部分内容包含以下主题：

- 文件复制和粘贴
- 文件传输

## 文件复制和粘贴

### November 4, 2022

用户可以使用右键单击菜单或键盘快捷键在会话与本地客户端之间复制和粘贴文件。此功能需要 Citrix Virtual Apps and Desktops 2006 或更高版本以及适用于 Windows 的 Citrix Workspace 应用程序 1903 或更高版本。

要成功复制和粘贴文件，请确保：

- 文件的最大数量不超过 20。
- 最大文件大小不超过 200 MB。
- Nautilus 文件管理器在安装了 Linux VDA 的计算机上可用。

#### 支持的 **Linux** 发行版

文件复制和粘贴功能适用于 Linux VDA 支持的所有 Linux 发行版。

#### 相关策略

以下剪贴板策略与配置功能相关。有关剪贴板策略的详细信息，请参阅策略支持列表。

- 客户端剪贴板重定向
- 剪贴板选择更新模式
- 主选定内容更新模式

> 注意：
>
> 要禁用文件复制和粘贴功能，请在 Citrix Studio 中将客户端剪贴板重定向策略设置为禁止。

限制

- 不支持剪切。剪切文件请求被视为复制。
- 不支持拖放。
- 不支持复制目录。
- 文件复制和粘贴必须按顺序执行。只有成功复制和粘贴上一个文件后，才能复制下一个文件。

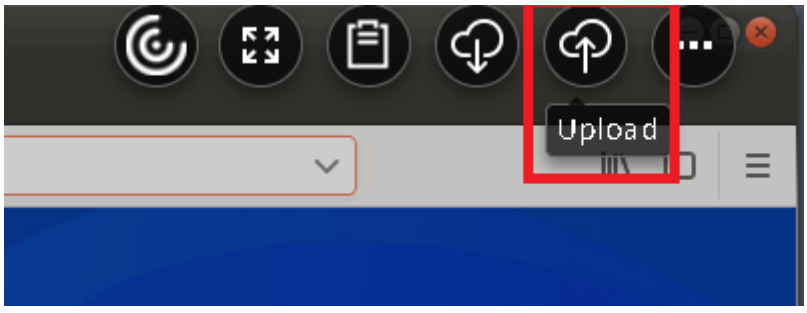
## 文件传输

November 4, 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，此功能可用。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。

> 注意：
>
> 适用于 HTML5 和 Chrome 的 Citrix Workspace 应用程序的文件传输可用。

在已发布的应用程序和桌面会话中，文件传输允许在 Linux VDA 与客户端设备之间上载和下载文件。要将文件从客户端设备上载到 Linux VDA，请单击 Citrix Workspace 应用程序工具栏上的上载图标，然后从文件对话框中选择所需的文件。要将文件从 Linux VDA 下载到客户端设备，请单击下载图标。可以在上载或下载过程中添加文件。一次最多可以传输 100 个文件。




> 注意：
>
> 要在 Linux VDA 与客户端设备之间上载和下载文件，请启用 Citrix Workspace 应用程序的工具栏。
> 可以使用允许拖放文件的 Citrix Workspace 应用程序版本。

自动下载是文件传输的增强功能。下载或移动到 VDA 上的保存到我的设备目录的文件将自动传输到客户端设备。

> 注意：
>
> 自动下载要求将允许在桌面与客户端之间传输文件和从桌面下载文件策略设置为允许。

下面是自动下载的一些用例：

- 下载文件以保存到我的设备

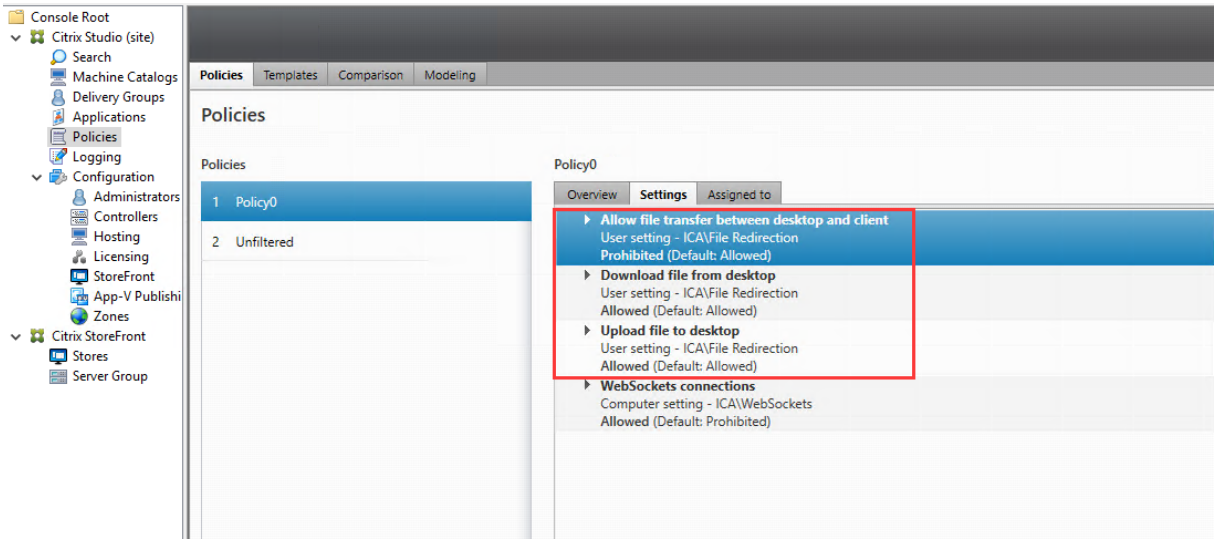
  在已发布的桌面和 Web 浏览器应用程序会话中，从 Web 站点下载的文件可以保存到 VDA 上的保存到我的设备目录中，以便自动传输到客户端设备。要实现自动下载，请将会话中 Web 浏览器的默认下载目录设置为保存到我的设备，并在运行适用于 HTML5 或 Chrome 的 Citrix Workspace 应用程序的 Web 浏览器中设置本地下载目录。

- 将文件移动或复制到保存到我的设备

  在已发布的桌面会话中，选择目标文件，然后将其移动或复制到保存到我的设备目录中，以便在客户端设备上可用。

### 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。
- 将文件上载到桌面。允许或阻止用户将文件从其设备上载到 Citrix Virtual Apps and Desktops 会话。

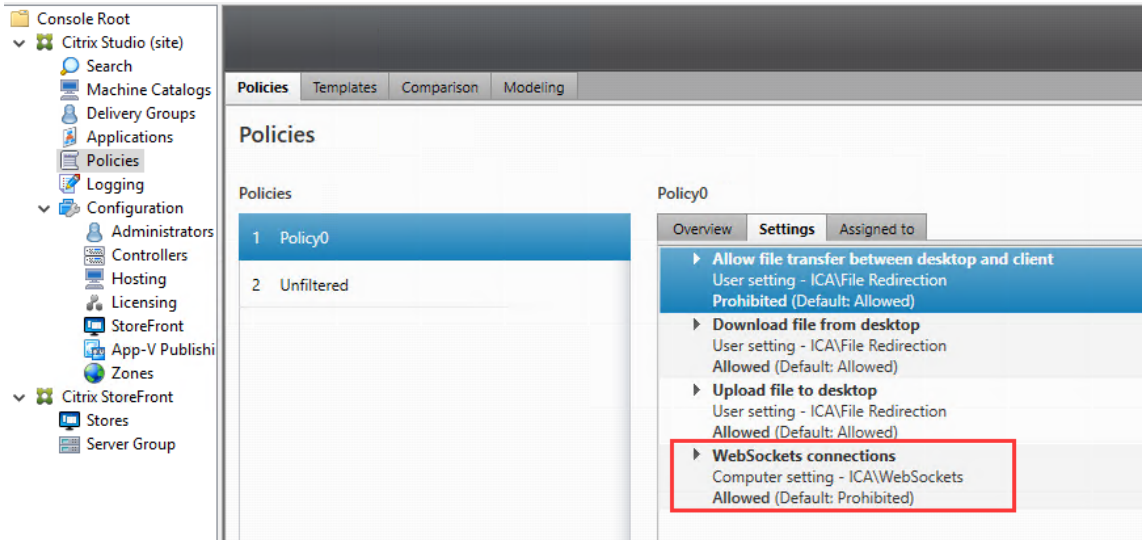
 

> 注意：
>
> 为确保从桌面下载文件和将文件上载到桌面策略生效，请将允许在桌面与客户端之间传输文件策略设置为允许。

使用情况

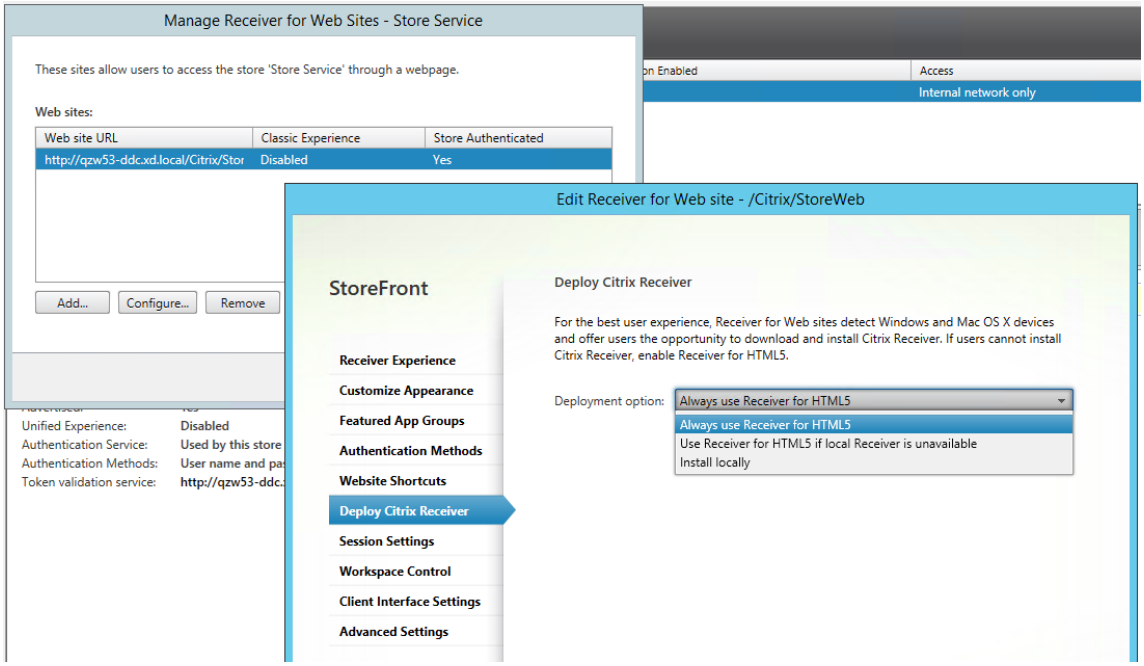
要通过适用于 **HTML5** 的 **Citrix Workspace** 应用程序使用文件传输功能，请执行以下操作：

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 与客户端设备之间执行一个或多个文件传输。

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：

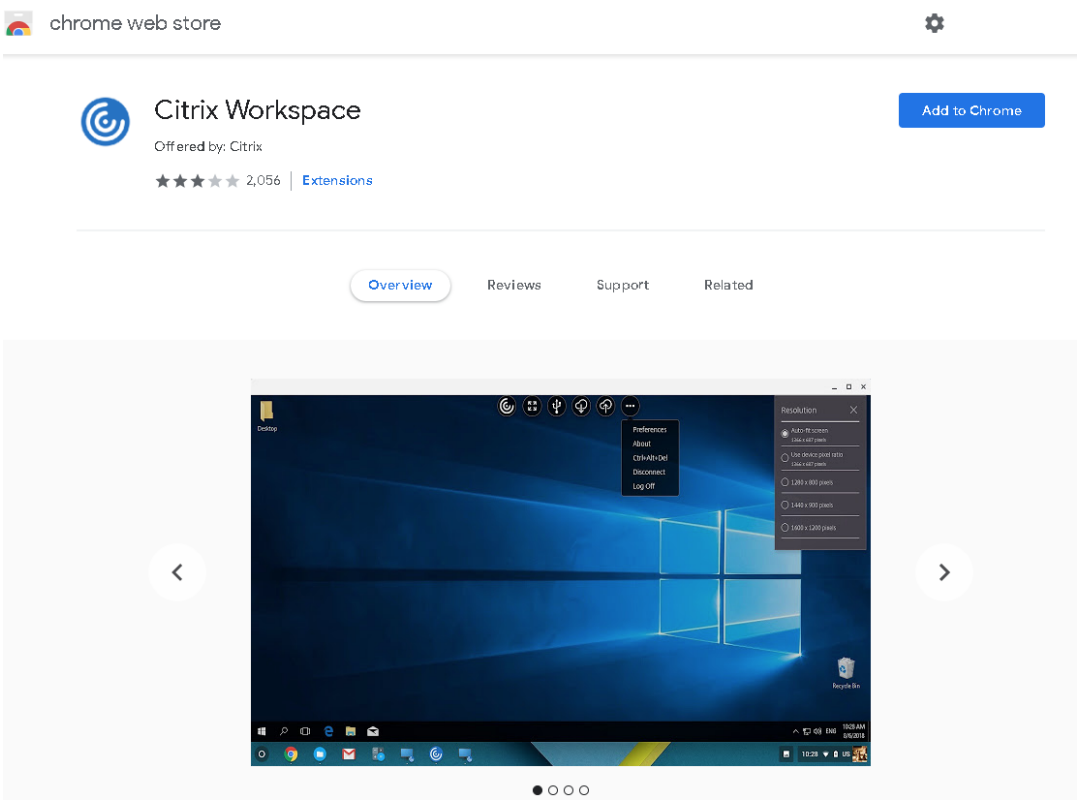
1. 通过上述文件传输策略启用文件传输功能。
2. 从 Chrome 网上应用店中获取 Citrix Workspace 应用程序。

   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. 启动虚拟桌面或应用程序会话。在 Linux VDA 与客户端设备之间执行一个或多个文件传输。

## 图形

November 4, 2022

本部分内容包含以下主题：

- 自动 DPI 缩放
- 客户端电池状态显示
- 图形配置和微调
- HDX 屏幕共享
- 非 vGPU 显卡

- 会话水印
- Thinwire 渐进式显示

## 自动 DPI 缩放

April 18, 2024

Linux VDA 支持自动 DPI 缩放。当用户打开虚拟桌面或应用程序会话时，会话中的 DPI 值会自动更改以匹配客户端上的 DPI 设置。

下面是与此功能相关的注意事项：

- 该功能要求您为 Citrix Workspace 启用 DPI 匹配。对于适用于 Windows 的 Citrix Workspace 应用程序，请确保选中否，使用本机分辨率选项。有关为适用于 Windows 的 Citrix Workspace 应用程序配置 DPI 缩放的详细信息，请参阅 DPI 缩放。
- 要使该功能在多显示器方案中起作用，必须使用相同的 DPI 设置对每台显示器进行配置。不支持混合 DPI 方案。如果使用不同的 DPI 设置配置显示器，Linux VDA 会对所有屏幕应用最小 DPI 值。
- 该功能已对 MATE、GNOME、GNOME Classic 和 KDE 启用。使用 KDE 或 MATE 时，请注意以下事项：
  - 对于在 Mate 桌面环境中运行的 KDE 虚拟桌面：
    - 我们建议使用 KDE Plasma 5 或更高版本。
    - 在会话运行时更改客户端上的 DPI 设置要求用户注销并重新登录。
  - 对于在 Mate 桌面环境中运行的 MATE 虚拟桌面：
    - 仅支持缩放比例 1 和 2。
    - 在会话运行时更改客户端上的 DPI 设置要求用户注销并重新登录。
- 虚拟会话中的 DPI 值会根据客户端上的 DPI 设置自动更改。目前，该功能仅支持整数类型的缩放比例，例如 100% 和 200%。如果在客户端配置的缩放比例类型为分数，虚拟会话 DPI 将根据下表更改为整数缩放比例。示例：如果缩放比例为 125%，DPI 值将更改为 100%。

| 客户端缩放比例 | 远程会话 DPI |
| --- | --- |
| 小于或等于 174% | 96 (1 x 96) |
| 175%–274% | 192 (2 x 96) |
| 275%–399% | 288 (3 x 96) |
| 大于或等于 400% | 384 (4 x 96) |

# 客户端电池状态显示

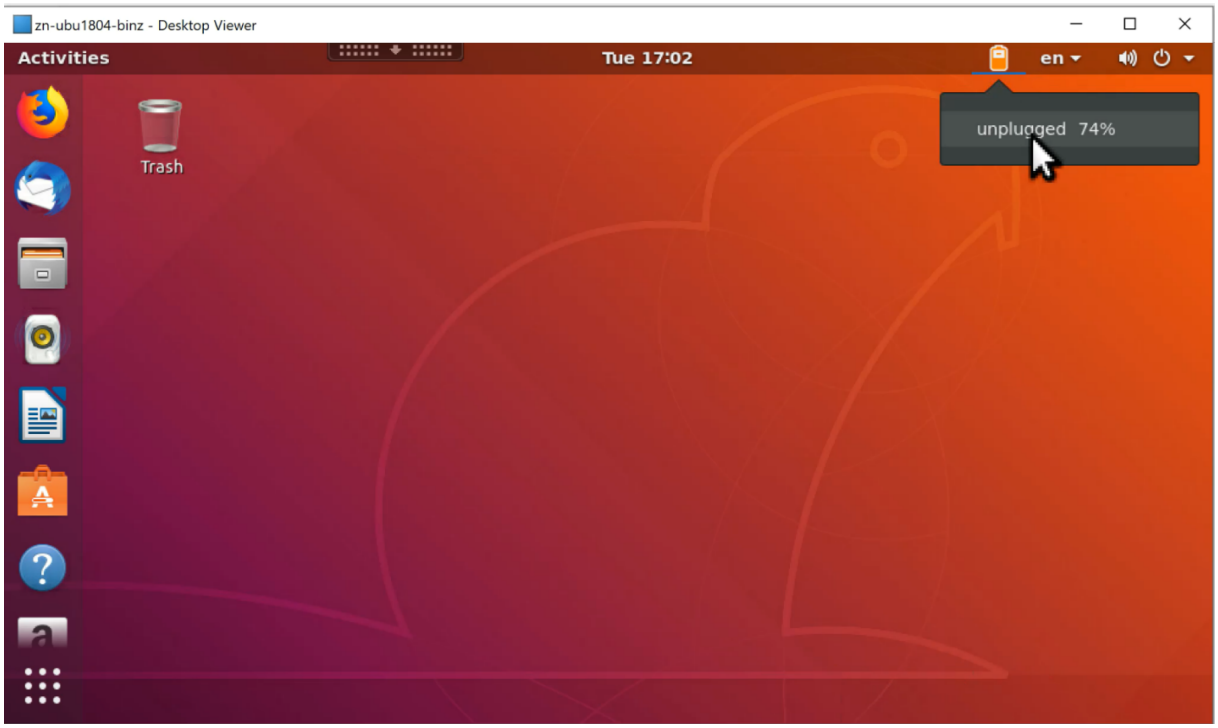
November 4, 2022

Linux VDA 可以重定向并显示虚拟桌面中客户端设备的电池状态。默认情况下，此功能处于启用状态，适用于以下版本的 Citrix Workspace 应用程序：

- 适用于 iOS 的 Citrix Workspace 应用程序
- 适用于 Linux 的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序（不支持版本 2204.1）
- 适用于 Windows 的 Citrix Workspace 应用程序（不支持版本 2204.1）

## 概述

当用户打开虚拟桌面时，他们可以在 Linux 系统托盘中看到电池图标。电池图标表示其客户端设备的电池状态。要查看剩余电池寿命的百分比，请单击电池图标。有关示例，请参见以下屏幕截图：




不同的电池图标表示不同的电池状态。有关概述，请参见下表：

| 电池图标 | 充电状态 | 剩余电池寿命级别 | 剩余电池寿命的百分比 |
| --- | --- | --- | --- |
|  | 正在充电，用“+”符号表示 | 高，用绿色表示 | =80% |
|  | 正在充电，用“+”符号表示 | 中，用琥珀色表示 | = 20% 和 < 80% |
|  | 正在充电，用“+”符号表示 | 低，用红色表示 | < 20% |
|  | 未充电，用“-”符号表示 | 高，用绿色表示 | =80% |
|  | 未充电，用“-”符号表示 | 中，用琥珀色表示 | = 20% 和 < 80% |
|  | 未充电，用“-”符号表示 | 低，用红色表示 | < 20% |
|  | 未知 | 未知 | 未知 |

### 配置

默认情况下，客户端电池状态显示处于启用状态。

要禁用该功能，请运行以下命令：

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

要启用此功能，请运行以下命令：

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

> 注意：
>
> 上述命令会影响软键盘功能，该功能与客户端电池状态显示共享 Mobile Receiver 虚拟通道 (MRVC)。

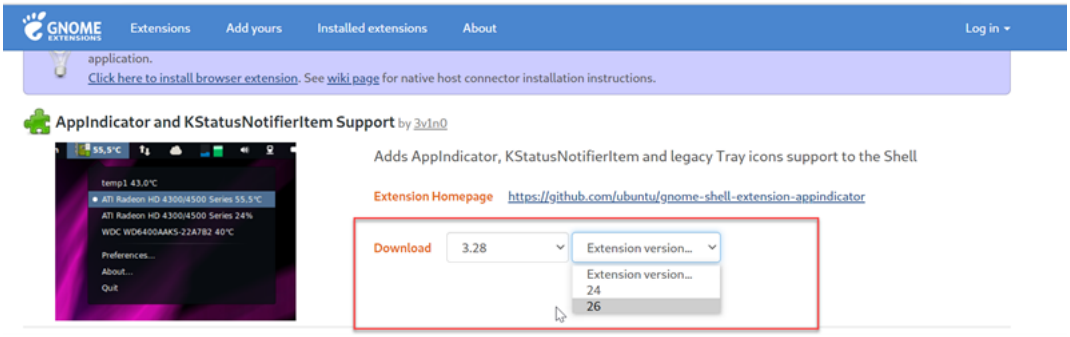
根据您的发行版，完成以下额外的步骤：

1. 如果要使用随 GNOME 安装的 RHEL 8.x 或 SUSE 15.x，请为 GNOME shell 安装兼容的扩展，以启用 AppIndicator 支持：

   a) 运行命令 `gnome-shell --version` 以检查 GNOME shell 版本。

   b) 从 https://extensions.gnome.org/extension/615/appindicator-support 下载 GNOME shell 的兼容扩展。例如，如果您的 shell 版本为 3.28，则可以选择扩展版本 24 或 26。

   c) 解压已下载的软件包。确认软件包的 **metadata.json** 文件中的 **uuid** 值已设置为 **appindicatorsupport@rgcjonas.gmail.com**。

   d) 运行 `mv` 命令以将 **appindicatorsupport@rgcjonas.gmail.com** 目录移动到 `/usr/share/gnome-shell/extensions/` 下方的位置。

   e) 运行 `chmod a+r metadata.json` 命令以使 **metadata.json** 文件可供其他用户读取。

   > 提示：
   >
   > 默认情况下，只有根用户可以读取 **appindicatorsupport@rgcjonas.gmail.com** 目录中的 **metadata.json** 文件。要支持屏幕共享，请确保其他用户也能够读取 **metadata.json** 文件。

   f) 安装 GNOME Tweaks。

   g) 在桌面环境中，通过按顺序按 `Alt+F2`、`r` 和 `Enter` 键或通过运行 `killall -SIGQUIT gnome-shell` 命令来重新加载 GNOME shell。

   h) 在桌面环境中，运行 GNOME Tweaks，然后在 Tweaks 工具中启用 **KStatusNotifierItem/AppIndicator** 支持。

2. 如果要使用随 GNOME 一起安装的 Debian 11.3 或 Debian 10.9，请完成以下步骤以安装并启用 GNOME 系统托盘图标：

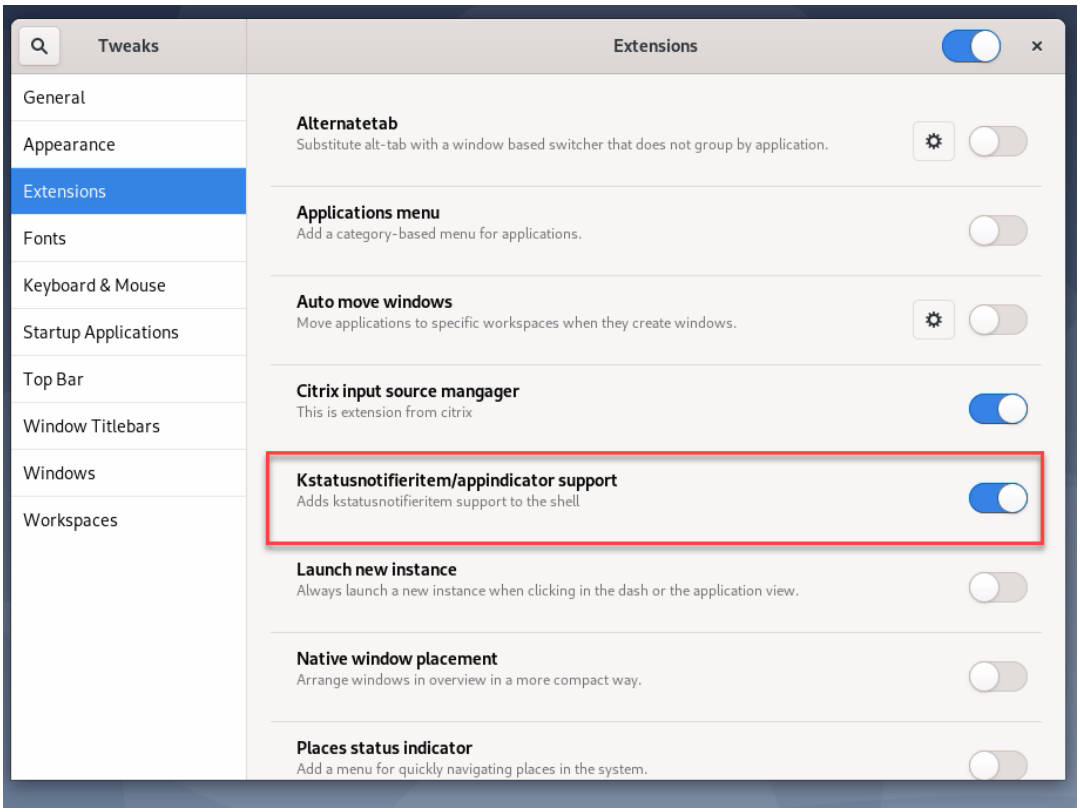
   a) 运行 `sudo apt install gnome-shell-extension-appindicator` 命令。为使 GNOME 能够看到该扩展程序，您可能必须注销后再重新登录。

   b) 在活动屏幕中搜索 Tweaks。

   c) 在 Tweaks 工具中选择扩展。

d）启用 **Kstatusnotifieritem/appindicator** 支持。




## 图形配置和微调

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

#### 视频编解码器进行压缩

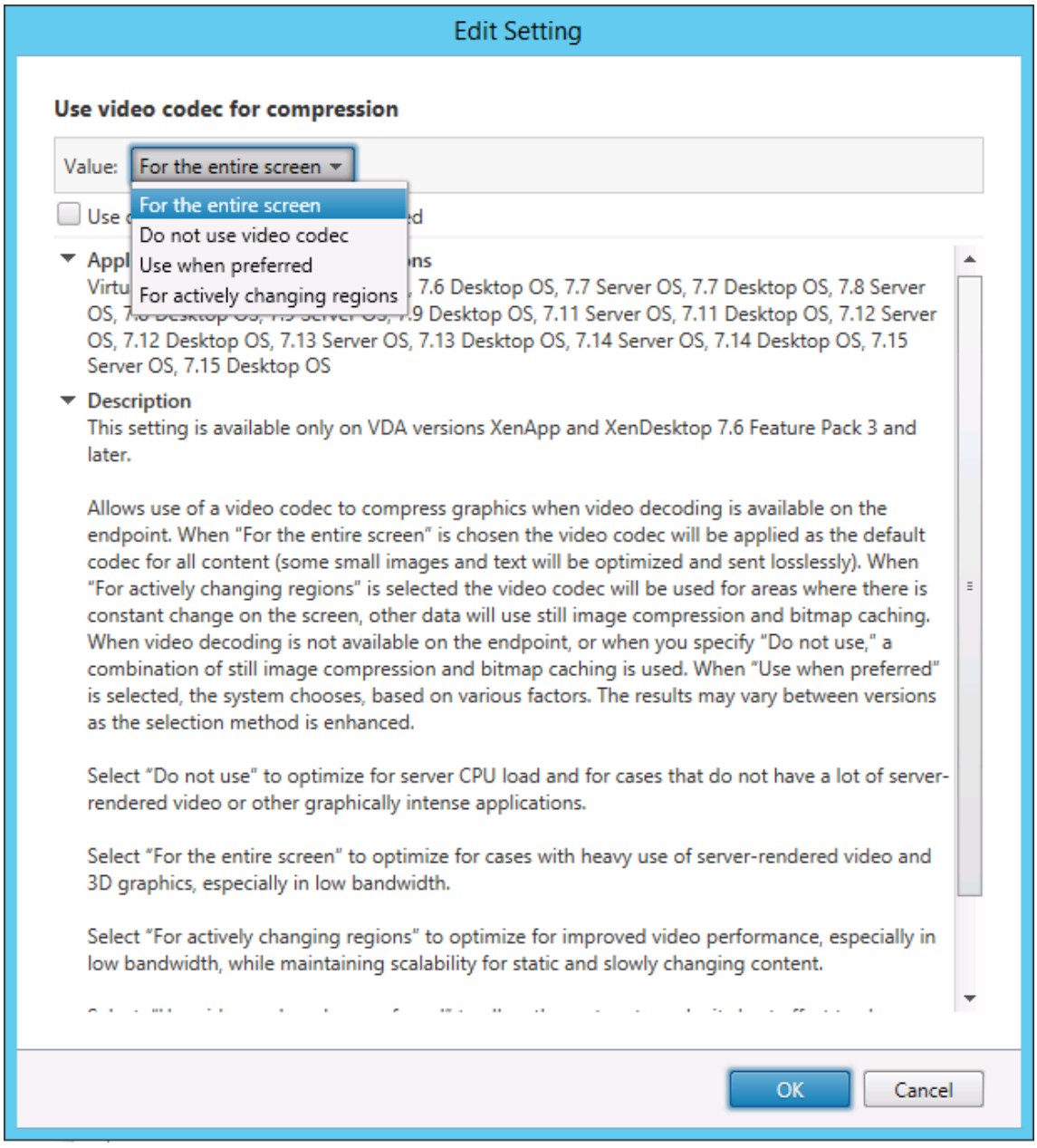
Thinwire 是 Linux VDA 中使用的显示内容远程处理技术。该技术允许一台计算机上生成的图形传输（通常跨网络）到另一台计算机上进行显示。

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。它可确保为所有 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）。它仅在图像正在移动的屏幕部分中使用 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：占用更低的带宽、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，请将使用视频编解码器进行压缩策略更改为偏好时使用（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。要为此功能启用 H.264 硬件编码，请参阅 H.264 硬件编码。




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

### **H.264** 硬件编码

使用视频编解码器的硬件编码策略允许使用图形硬件（如果可用）通过视频编解码器压缩屏幕元素。如果此类硬件不可用，VDA 会回退到使用软件视频编解码器的基于 CPU 的编码。

自版本 2204 起，Linux VDA 支持选择性地将 H.264 硬件编解码器用于主动变化的区域。此功能可将 CPU 视频压缩消耗转移到硬件上，并提高图像质量和每秒帧数 (FPS)。要启用此功能，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. 启用使用视频编解码器进行压缩策略，然后选择针对主动变化的区域。

#### 允许视觉无损压缩

允许视觉无损压缩策略允许对图形使用视觉无损压缩，而不是真正的无损压缩。相比于真正无损的压缩，视觉无损功能可提高性能，但会产生视觉上不易察觉的轻微损失。此设置可更改视觉质量设置的值的使用方式。

默认情况下，允许视觉无损压缩策略处于禁用状态。要启用视觉无损压缩，请将允许视觉无损压缩设置为已启用，将视觉质量策略设置为无损构建。

如果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，则视觉无损压缩将应用到静态图像编码。如果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以外的图形模式，则视觉无损压缩将应用到 H.264 编码。

以下客户端支持选择性 H.264：

- 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
- 适用于 Linux 的 Citrix Workspace 应用程序 1808 及更高版本

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。

可以将此功能用于：

- Citrix Receiver for Windows 4.10 到 4.12
- 适用于 Windows 的 Citrix Workspace 应用程序 1808 及更高版本

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 及更高版本上使用此功能。

每个唯一的 Y、U 或 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。

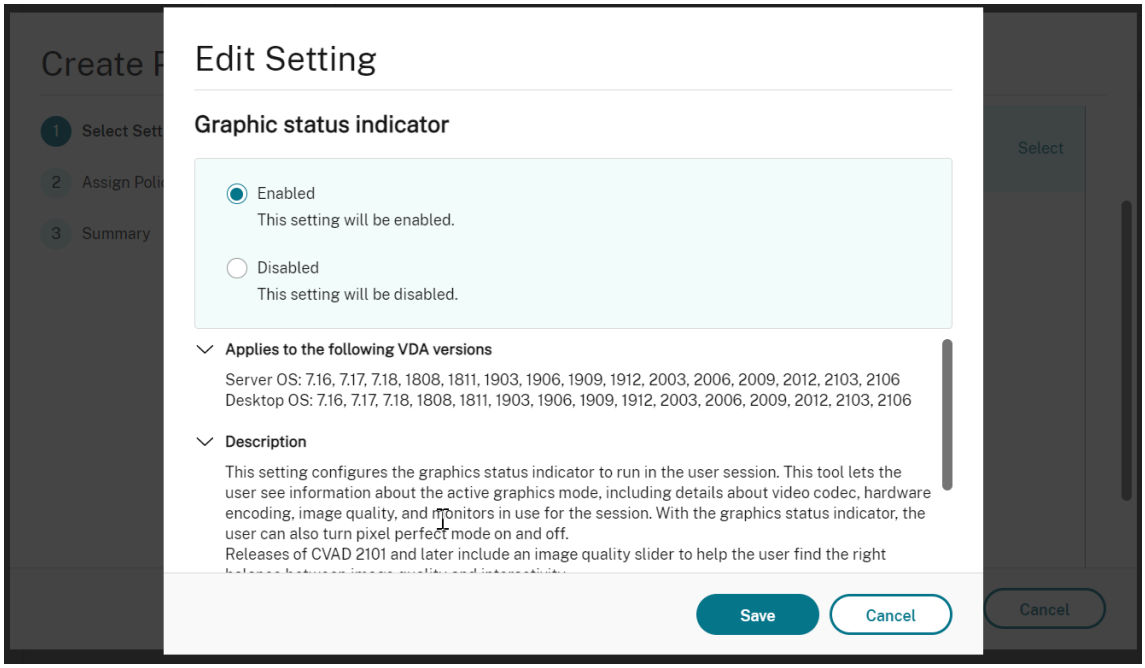
#### 图形质量滑块

我们在虚拟 Linux 会话中运行的图形状态指示器工具中包含了图形质量滑块。该滑块有助于在图像质量与交互性之间找到正确的平衡。

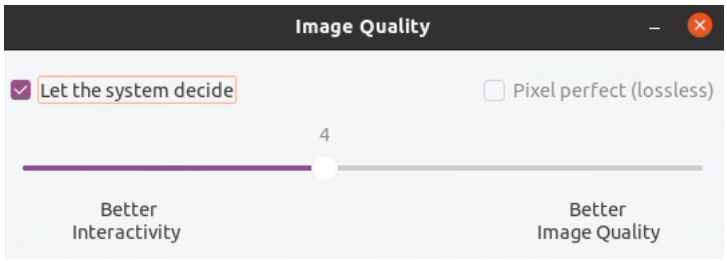
要使用滑块，请完成以下步骤：

1. 在 Citrix Studio 中启用图形状态指示器策略。




2. 打开终端并运行 `ctxslider` 命令。此时将显示滑块 UI。

> 注意：
>
> 如果已将视觉质量策略设置为始终无损或无损构建，则不会显示滑块 UI。




现在可以提供以下选项：

- 要更改图像质量，请移动滑块。滑块支持的范围为 0–9。
- 要使用系统定义的设置，请选择让系统决定。
- 要切换到无损模式，请选择像素完美。

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的带宽并相应地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：

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    DisableReconfigureEncoder" -d "0x00000001" --force
<!--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 **MaxBitRate-Percent** 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。

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    AverageBitRatePercent" -d "90" --force

sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    MaxBitRatePercent" -d "100" --force
<!--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。

### 并行处理

Thinwire 可以通过并行处理某些任务来提高每秒帧数 (FPS)，但总体 CPU 占用量的开销略高。默认情况下，此功能处于禁用状态。要启用此功能，请在您的 VDA 上运行以下命令：

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ParallelProcessing" -d "0x00000001" --force
<!--NeedCopy-->
```

### 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）：

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
<!--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）：

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
<!--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）：

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
<!--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。

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
<!--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：

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
<!--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）：

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
<!--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：

```
Tue Apr 12 10:42:03 2016
+-----------------------------------------------------+
| NVIDIA-SMI 361.28     Driver Version: 361.28         |
|-------------------------------+----------------------+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
   Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
   Compute M. |
|===============================+======================+======================|

|   0  GRID K1             Off  | 0000:00:05.0     Off |
                    N/A |
| N/A   42C    P0    14W /  31W |    207MiB /  4095MiB |      8%
   Default |
+-------------------------------+----------------------+----------------------+
```

```
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
   Usage      |
14 |=============================================================================|
15 |  No running processes found
                                  |
16 +-----------------------------------------------------------------------------+
17 <!--NeedCopy-->
```

为显卡设置正确的配置：

`etc/X11/ctx-nvidia.sh`

#### **HDX 3D Pro** 多监视器重绘问题

如果在非主监视器屏幕上发生重绘问题，请检查 NVIDIA GRID 许可证是否可用。

#### 检查 **Xorg** 错误日志

Xorg 的日志文件命名类似于 **Xorg.{DISPLAY}.log**，位于 **/var/log/** 文件夹中。

### 已知问题及限制

#### 对于 **vGPU**，**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：

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

对于 8.1 之前的 Citrix Hypervisor：

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

#### 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)`。

# HDX 屏幕共享

November 4, 2022

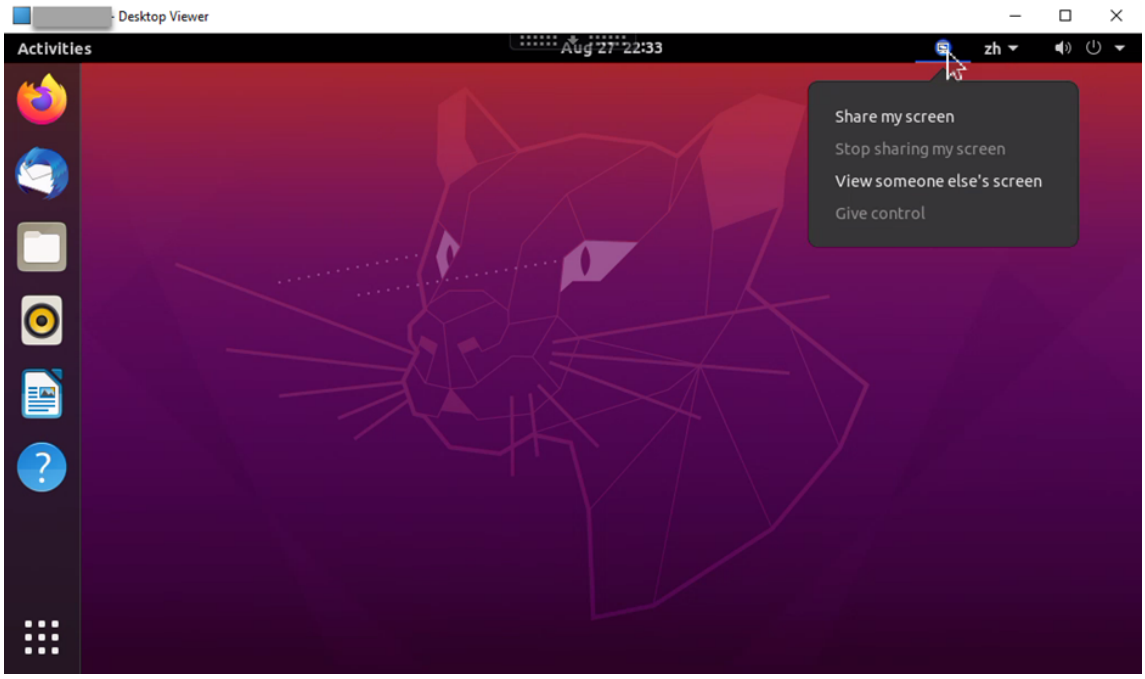
## 概述

Linux VDA 允许您与其他虚拟桌面上的会话用户共享自己的虚拟桌面屏幕。

以下示例将引导您完成共享屏幕和查看其他人屏幕的过程。

要共享屏幕，请执行以下操作：

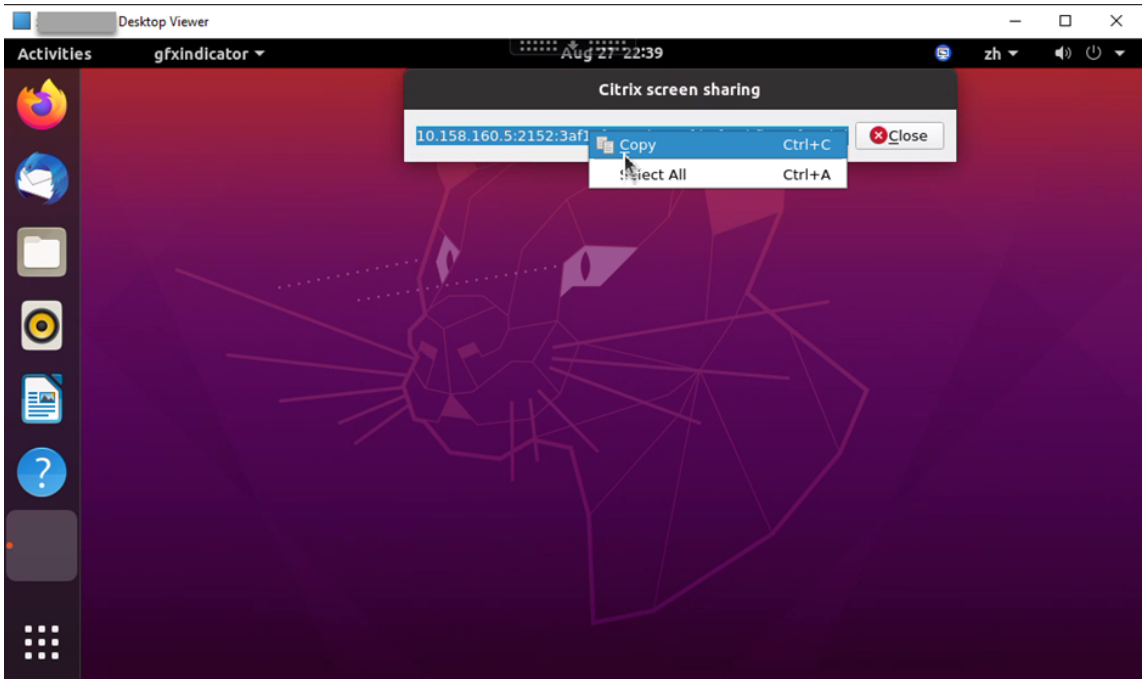
1. 在虚拟桌面的通知区域中，单击屏幕共享图标并选择共享我的屏幕。




2. 单击复制并关闭。

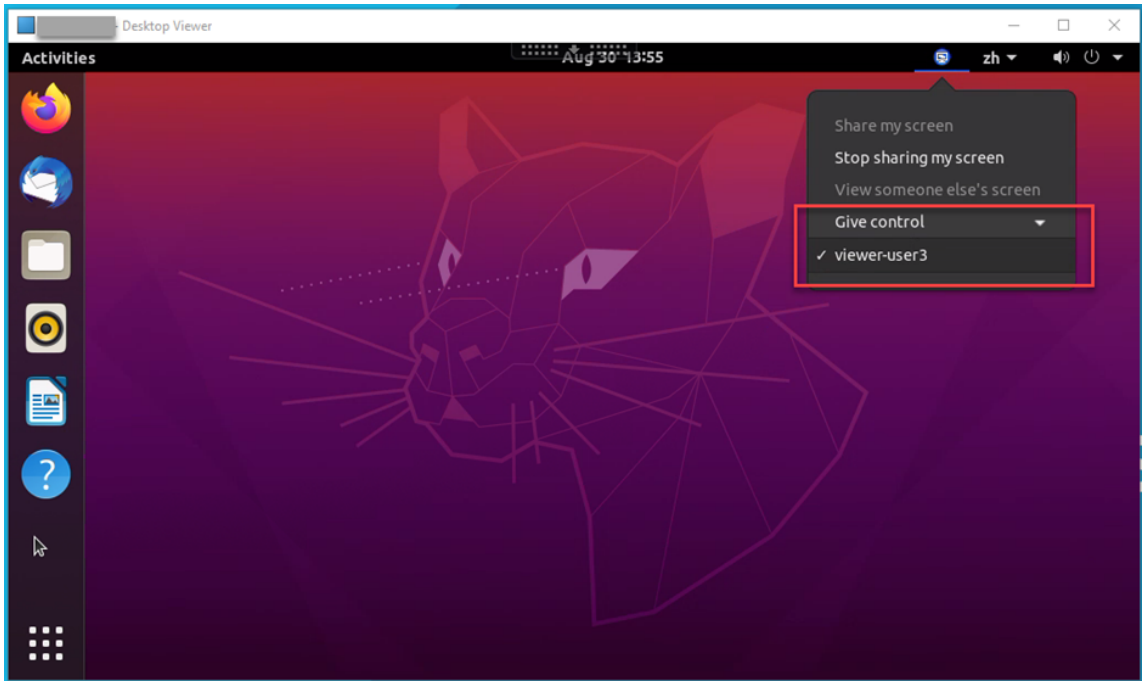
   当前的屏幕共享代码将一直保留，直到您停止并重新开始共享屏幕。



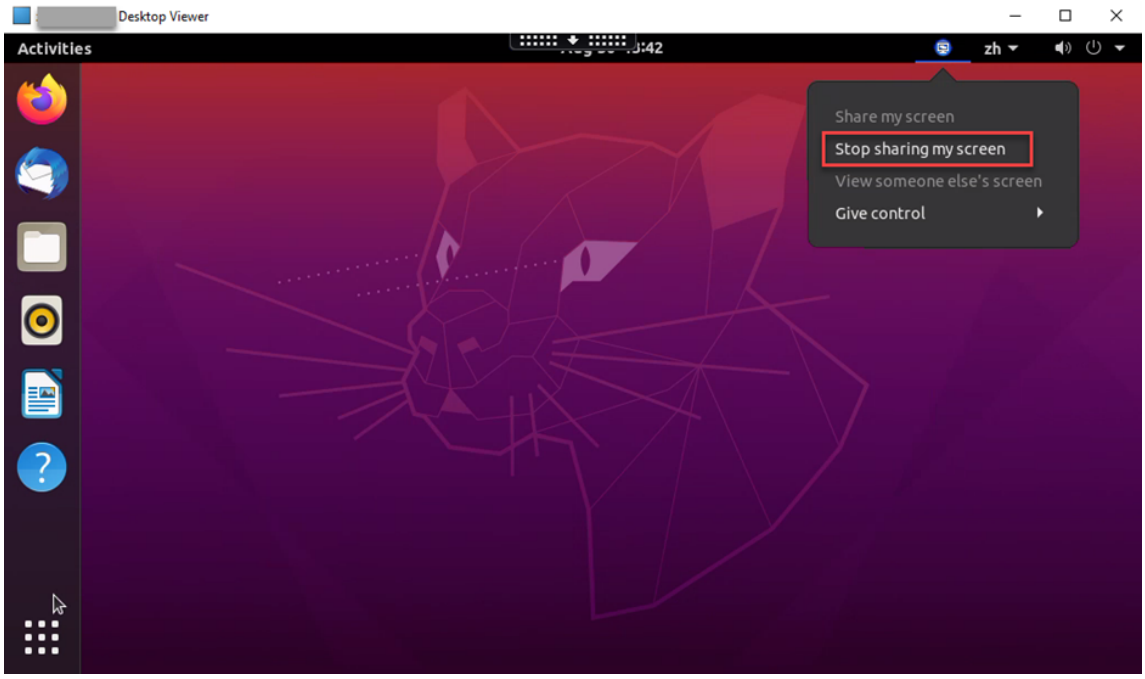

> 提示：
>
> 共享您的屏幕时，屏幕周围有一个红色边框，表示正在进行共享。

3. 与其他虚拟桌面（要与其共享您的屏幕）上的会话用户共享复制的代码。
4. 要允许某个查看器控制您的屏幕，请选择授予控制权，然后选择查看者的名称。要停止授予控制权，请清除该查看器的名称。



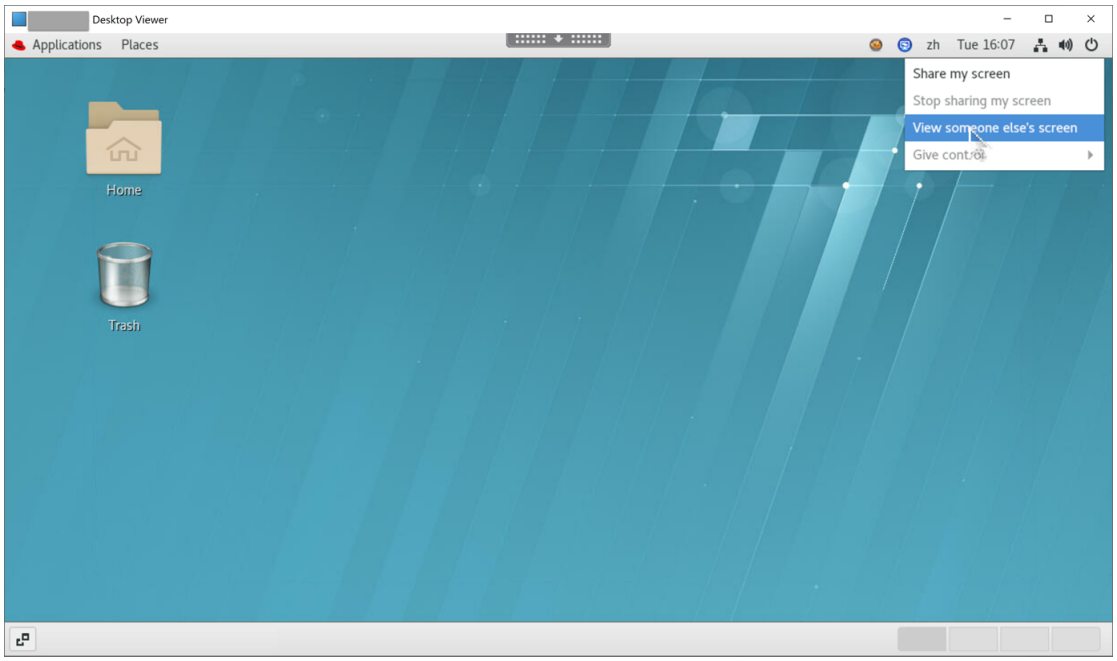

5. 要停止共享屏幕，请选择停止共享我的屏幕。



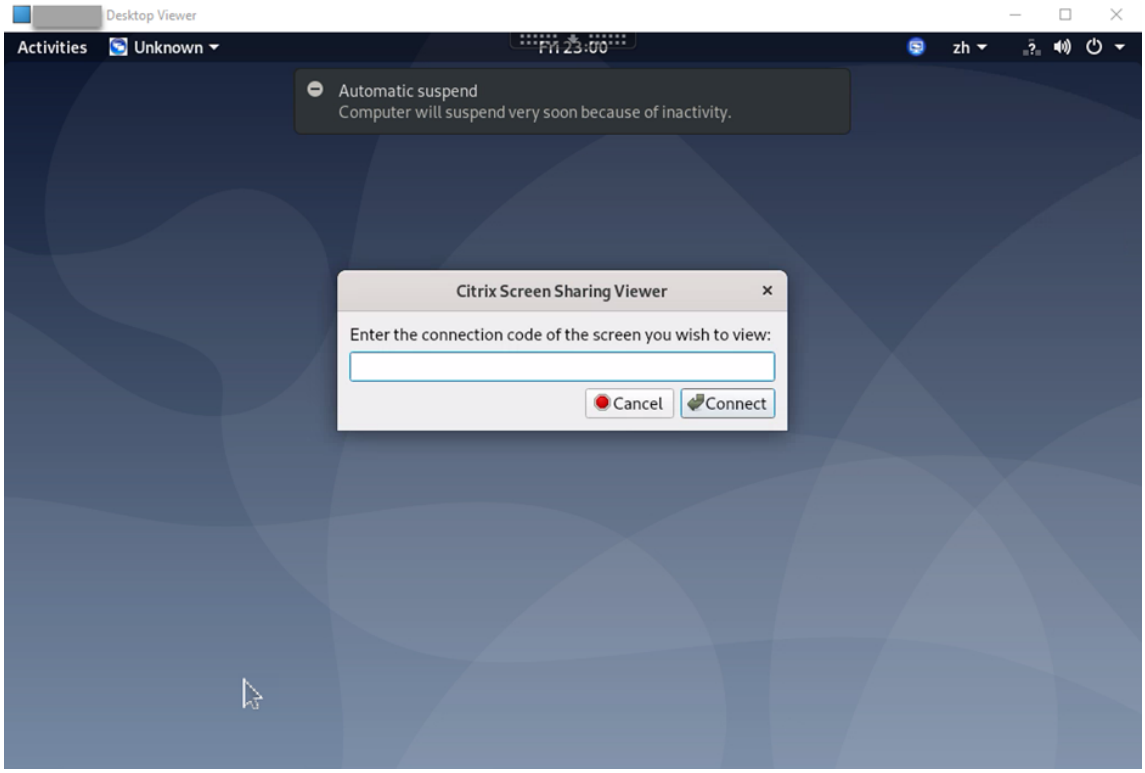

要查看其他人的屏幕，请执行以下操作：

1. 在虚拟桌面的通知区域中，单击屏幕共享图标并选择查看其他人的屏幕。

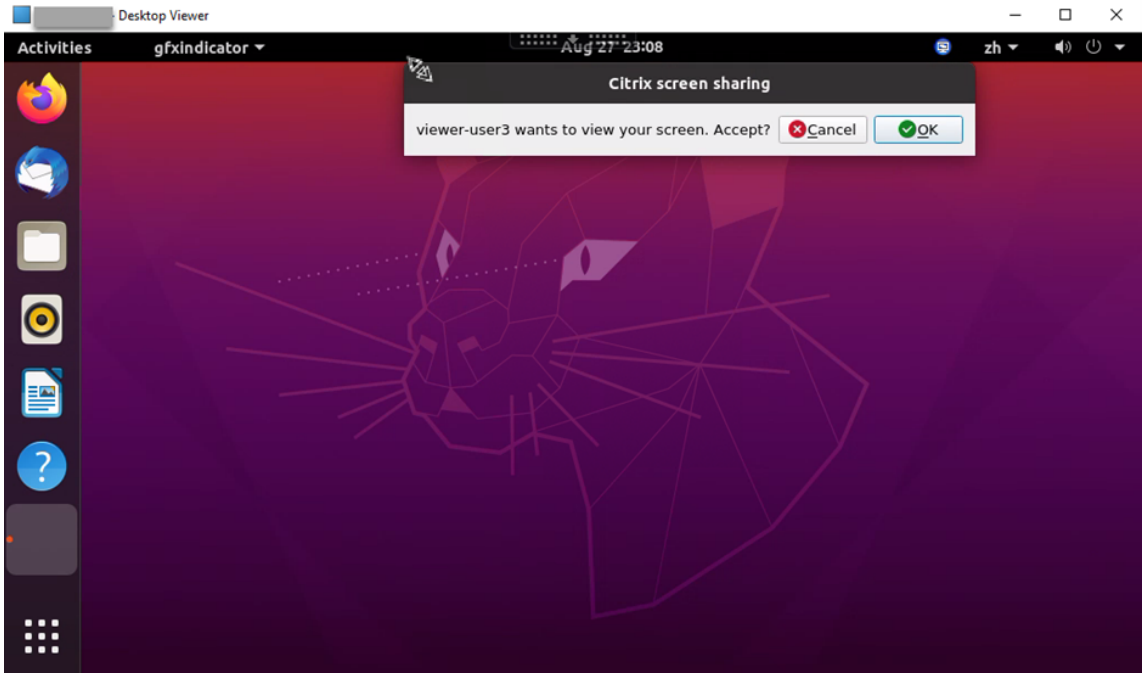



2. 输入要查看的屏幕的连接代码，然后单击连接。



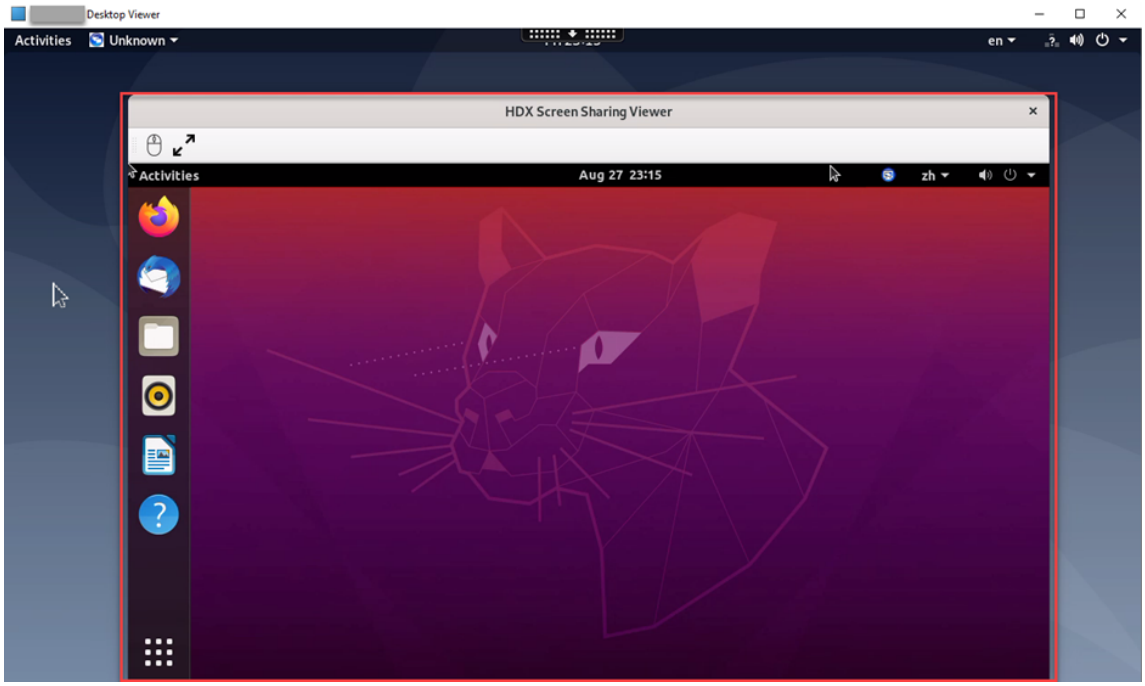

3. 等待屏幕共享者接受您的请求。例如：




> 提示：
>
> - 在共享者方面，Linux 系统会针对您的请求发出通知。
> - 如果共享者未在 30 秒内接受您的请求，您的请求将过期并显示提示。

4. 屏幕共享者通过单击确定接受您的请求后，共享的屏幕将显示在 Desktop Viewer 中。您以查看者的身份与自动分配的用户名连接。

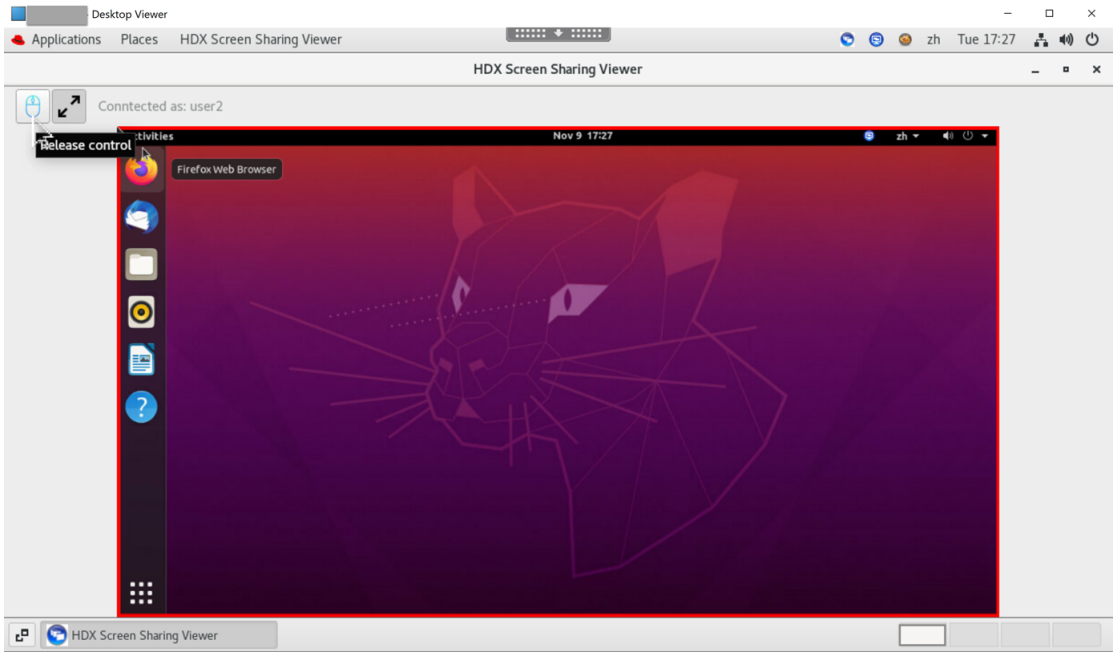



5. 要请求控制共享的屏幕，请单击左上角的鼠标图标。

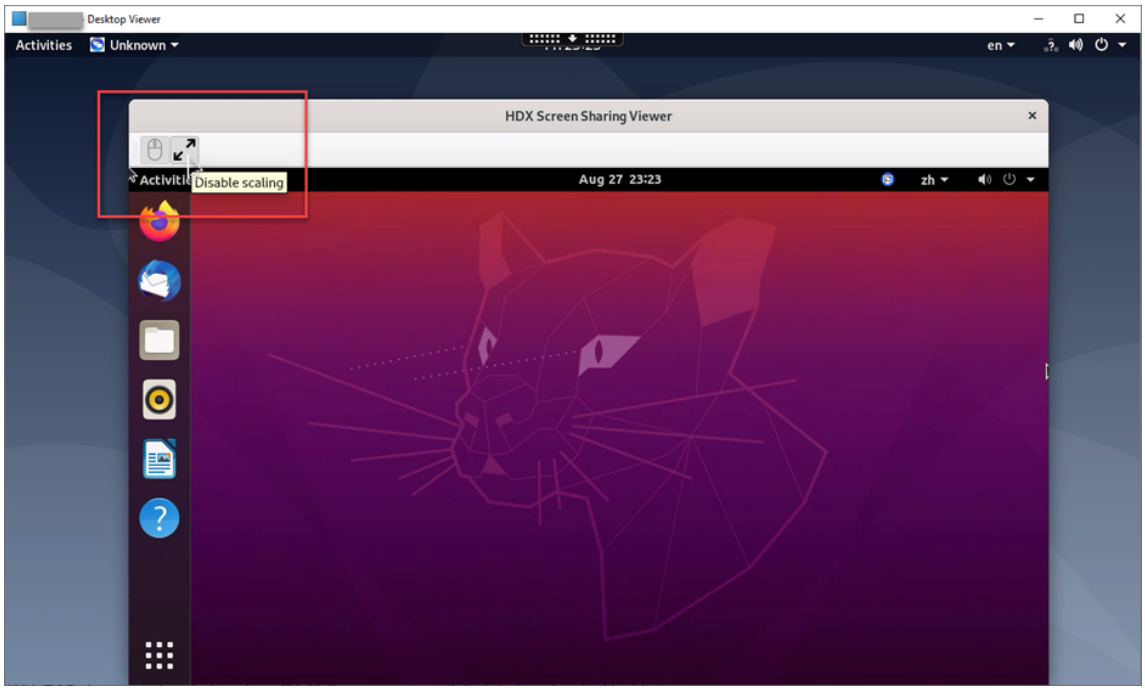
> 提示：
>
> - 如果共享者未在 30 秒内接受您的请求，您的请求将过期。
> - 一次只允许一个查看者控制共享屏幕。

再次单击鼠标图标可释放对共享屏幕的控制权。




6. 要禁用显示缩放或缩放到窗口大小，请单击鼠标图标旁边的图标。




## 配置

屏幕共享功能默认处于禁用状态。要启用该功能，请完成以下设置：

1. 在 Citrix Studio 中启用图形状态指示器策略。
2. 对于 Citrix Virtual Apps and Desktops 2112 及更高版本，请在 Citrix Studio 中启用屏幕共享策略。

3. （可选）对于 Citrix Virtual Apps and Desktops 2109 及更早版本，请运行以下命令在 Linux VDA 上启用屏幕共享：

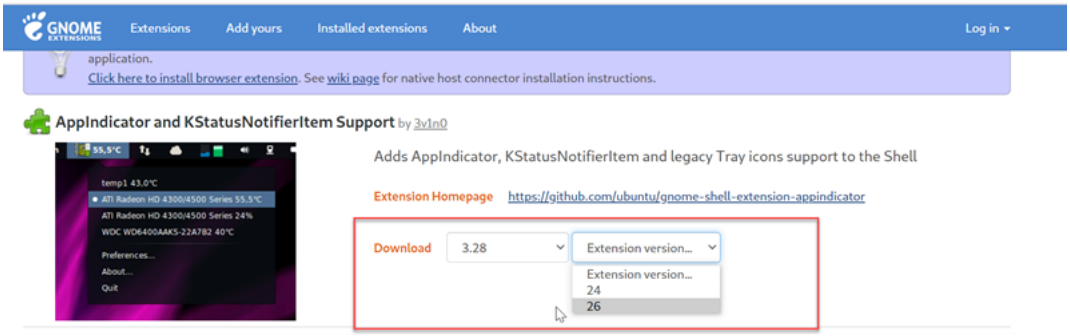
```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -v "
   EnableScreenSharing" -d "0x00000001"
<!--NeedCopy-->
```

4. 在您的防火墙中允许使用端口 52525—52625。

5. （可选）如果要使用随 GNOME 安装的 RHEL 8.x、Debian 11 或 SUSE 15.x，请为 GNOME shell 安装兼容的扩展，以启用 AppIndicator 支持：

   a) 运行命令 `gnome-shell --version` 以检查 GNOME shell 版本。

   b) 从 https://extensions.gnome.org/extension/615/appindicator-support 下载 GNOME shell 的兼容扩展。例如，如果您的 shell 版本为 3.28，则可以选择扩展版本 24 或 26。




   c) 解压已下载的软件包。确认软件包的 **metadata.json** 文件中的 **uuid** 值已设置为 **appindicatorsupport@rgcjonas.gmail.com**。

   d) 运行 `mv` 命令以将 **appindicatorsupport@rgcjonas.gmail.com** 目录移动到 `/usr/share/gnome-shell/extensions/` 下方的位置。

   e) 运行 `chmod a+r metadata.json` 命令以使 **metadata.json** 文件可供其他用户读取。

> 提示：
>
> 默认情况下，只有根用户可以读取 **appindicatorsupport@rgcjonas.gmail.com** 目录中的 **metadata.json** 文件。要支持屏幕共享，请确保其他用户也能够读取 **metadata.json** 文件。

   f) 安装 GNOME Tweaks。

   g) 在桌面环境中，通过按顺序按 `Alt+F2`、`r` 和 `Enter` 键或通过运行 `killall -SIGQUIT gnome-shell` 命令来重新加载 GNOME shell。

   h) 在桌面环境中，运行 GNOME Tweaks，然后在 Tweaks 工具中启用 **KStatusNotifierItem/AppIndicator** 支持。

6. （可选）如果要使用随 GNOME 一起安装的 Debian 10，请完成以下步骤以安装并启用 GNOME 系统托盘图标：

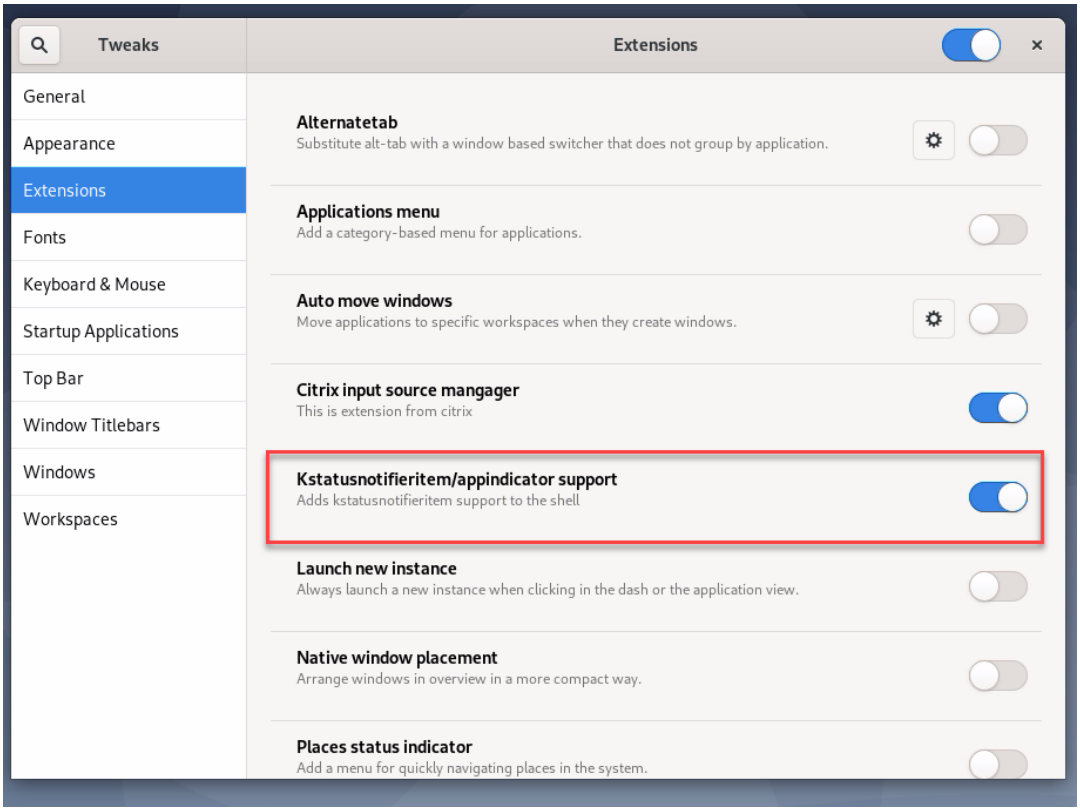
 

a) 运行 `sudo apt install gnome-shell-extension-appindicator` 命令。为使 GNOME 能够看到该扩展程序，您可能必须注销后再重新登录。

b) 在活动屏幕中搜索 Tweaks。

c) 在 Tweaks 工具中选择扩展。

d) 启用 **Kstatusnotifieritem/appindicator** 支持。




注意事项

- 屏幕共享功能不支持 H.265 视频编解码器。
- 屏幕共享功能对应用程序会话不可用。
- 默认情况下，桌面会话的用户最多可以与 10 个查看者共享其会话屏幕。查看者的最大数量可通过 `ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-v "ScreenSharingViewerMaxNum"-d <hex_value>` 进行配置。当达到最大数量时，用户尝试接受额外的连接请求时会出现提示。

# 非 **vGPU** 显卡

March 11, 2024

非 vGPU 显卡是指不支持 NVIDIA 虚拟 GPU (vGPU) 解决方案的显卡。本文提供有关使用非 vGPU 显卡的信息。

## 必备条件

要使用非 vGPU 显卡，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

### 修改 **Xorg** 配置文件

适用于 **NVIDIA** 显卡　如果您使用的是 NVIDIA 驱动程序，则会自动安装和设置配置文件。

适用于其他显卡　必须修改安装在 `/etc/X11/` 下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) 请参阅智能卡制造商提供的指南以了解配置信息。可以生成本机配置文件。确认在未运行 Linux VDA 会话时，您的智能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。

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix\XDamage" -t "REG_SZ" -v "
    DriverName" -d "intel" --force
<!--NeedCopy-->
```

#### 启用非 **vGPU** 图形

默认情况下，非 vGPU 图形功能处于禁用状态。可以运行以下命令将 XDamageEnabled 值设置为 1 将其启用。

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix\XDamage" -t "REG_DWORD" -v "
    XDamageEnabled" -d "0x00000001" --force
<!--NeedCopy-->
```

#### 监视 **Remote PC Access VDA** 的空白

对于使用非 vGPU 显卡的 Remote PC Access VDA，Linux VDA 支持物理显示器遮蔽。此增强功能可将图形显示卸载到可扩展虚拟显示接口 (Extensible Virtual Display Interface, EVDI) 虚拟显示器。

> 注意：
>
> EVDI 虚拟显示器的最大数量因发行版而异。

显示器消隐适用于 Ubuntu 20.04、Debian 11.3 和 Debian 10.9 VDA。要使用显示器消隐，请完成以下两个步骤：

1. 根据您的 Linux 发行版安装 `evdi-dkms` 软件包：

   ```
   sudo apt install evdi-dkms
   <!--NeedCopy-->
   ```

2. 启用图形显示卸载到 EVDI：

   ```
   /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
       CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
       Evdi" -d "0x00000001" --force
   <!--NeedCopy-->
   ```

3. 如果您使用的是 Intel 显卡，请禁用显示管理器。否则，Intel 卡将被显示管理器占用，无法用于 Citrix 远程会话。

   ```
   sudo systemctl disable --now gdm
   <!--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。

## 会话水印

October 31, 2022

会话水印有助于威慑和启用数据窃取的跟踪功能。跟踪信息在会话桌面上显示，对使用相机和屏幕截图盗取数据的用户具有威慑作用。您可以将水印指定为文本层或带有 alpha 通道的 PNG 图像。该水印在整个会话屏幕上显示，但不会改变原始文档的内容。

> 重要：
>
> 会话水印不是一项安全功能。它不能完全阻止数据盗窃，但可以提供一定级别的威慑作用和可跟踪性。使用此功能时，我们不保证完整的信息可追溯性。相反，我们建议您将此功能与其他安全解决方案（如果适用）结合使用。

会话水印中包含用于跟踪数据盗窃的信息。最重要的数据是创建屏幕图像的会话的用户的身份（通过其登录凭据进行跟踪）。为了更有效地跟踪数据泄漏，请包括服务器或客户端 Internet 协议地址以及连接时间等其他信息。

要调整用户体验，请使用以下会话水印策略设置配置屏幕上的放置位置和水印外观。

### 会话水印策略设置

启用会话水印

启用了此设置时，会话显示屏幕上将覆盖一层显示会话特定信息的不透明水印。其他水印设置取决于此设置的启用。

默认情况下，会话水印处于禁用状态。

包括客户端 **IP** 地址

启用了此设置时，会话将显示当前的客户端 IP 地址作为水印。

默认情况下，包括客户端 **IP** 地址处于禁用状态。

包括连接时间

启用了此设置时，会话水印将显示连接时间。格式为 yyyy/mm/dd hh:mm。显示的时间取决于系统时钟和时区。

默认情况下，包括连接时间处于禁用状态。

包括登录用户名

启用了此设置时，会话将显示当前的登录用户名作为水印。显示格式为 USERNAME@DOMAINNAME。我们建议用户名最多包含 20 个字符。当用户名超过 20 个字符时，可能会出现较小的字体大小或截断，降低了水印的有效性。

默认情况下，包括登录用户名处于启用状态。

包括 **VDA** 主机名

启用了此设置时，会话将显示当前 ICA 会话的 VDA 主机名作为水印。

默认情况下，包括 **VDA** 主机名处于启用状态。

包括 **VDA IP** 地址

启用了此设置时，会话将显示当前 ICA 会话的 VDA IP 地址作为水印。

默认情况下，包括 **VDA IP** 地址处于禁用状态。

会话水印样式

此设置控制您显示单个水印文本标签还是多个标签。请从“值”下拉菜单中选择多个或单个。
有关其他样式选项，请参阅本文中的水印自定义文本部分。

多个将在会话中显示 5 个水印标签。其中 1 个标签在中心显示，另外 4 个在边角显示。

单个将在会话中心显示 1 个水印标签。

默认情况下，会话水印样式设置为多个。

水印透明度

可以指定介于 0 到 100 之间的水印透明度。指定的值越大，水印越不透明。

默认情况下，值为 17。

水印自定义文本

默认情况下，该值为空。可以键入非空字符串，设置语法以形成字符串，或者使用组合形式以在会话水印中显示。非空字符串每行最多支持 25 个 Unicode 字符。较长的字符串将被截断为 25 个字符。

例如，您可以将策略设置为以下值：

```
<date> <time><newline><username><style=single><fontsize=40><font=Ubuntu><position=center><rotation=0><newline><serverip><newline><clientip><newline>Citrix Linux VDA<newline>Version 2207
```

有关所有语法选项的说明，请参见下表：

| 语法选项 | 说明 | 有效设置（区分大小写） | 默认值 | 备注 |
| --- | --- | --- | --- | --- |
| <style> | 水印布局样式 | xstyle, single, tile, horizontal | xstyle | - |
| <position> | 水印位置 | center、topleft、topright、bottomleft、bottomright | center | 仅当布局样式设置为单一时才有效。 |
| <rotation> | 水印旋转到一定角度 | -180–180 | 0 | - |
| <transparency> | 水印不透明度 | 0–100 | 17 | - |
| <font> | - | 系统支持的字体 | Sans | - |
| <fontsize> | - | 20–50 | 0（自动计算） | - |
| <fontzoom> | 通过 <fontsize> 和 <image> 设置的字体和图像大小的百分比 | 0 – | 100 | - |

| 语法选项 | 说明 | 有效设置（区分大小写） | 默认值 | 备注 |
| --- | --- | --- | --- | --- |
| <image> | PNG 水印 | VDA 上的 PNG 图像的路径 | 不适用 | 此语法配置 PNG 水印。仅支持带有 alpha 通道的 PNG。使用 PNG 水印时，只有 <style>、<position>、<rotation>、<transparency> 和 <fontzoom> 语法选项才有效。 |
| <date> | 会话连接日期的占位符 (YYYY/MM/DD) | 不适用 | 不适用 | - |
| <time> | 会话连接时间的占位符 (HH:MM) | 不适用 | 不适用 | - |
| <domain> | 用户帐户域的占位符 | 不适用 | 不适用 | - |
| <username> | 当前登录用户名的占位符（不包括用户帐户域） | 不适用 | 不适用 | - |
| <hostname> | VDA 主机名的占位符 | 不适用 | 不适用 | - |
| <clientip> | 客户端 IP 地址的占位符 | 不适用 | 不适用 | - |
| <serverip> | VDA 的 IP 地址的占位符 | 不适用 | 不适用 | - |

> 注意：
>
> 如果使用有效的语法设置指定水印自定义文本，则会忽略除启用会话水印之外的所有其他会话水印策略。
>
> 如果未指定语法选项或者将其设置为不支持的值，则使用其默认值。

限制

- 在使用浏览器内容重定向的会话中不支持会话水印。要使用会话水印功能，请务必禁用浏览器内容重定向。
- 如果会话在使用旧版 NVIDIA 驱动程序的全屏硬件加速 H.264 或 H.265 编码模式下运行，则不支持会话水印，并且不显示会话水印。（在这种情况下，注册表中的 NvCaptureType 设置为 2。）
- 水印对会话重影功能不可见。

- 如果您按 Print Screen 键捕获屏幕，在 VDA 端捕获的屏幕将不包括水印。我们建议您采取措施避免复制屏幕捕获。

## **Thinwire** 渐进式显示

November 4, 2022

会话交互性在低带宽或高延迟连接中会降级。例如，在 Web 页面上滚动可能会变慢、无响应或断断续续。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。

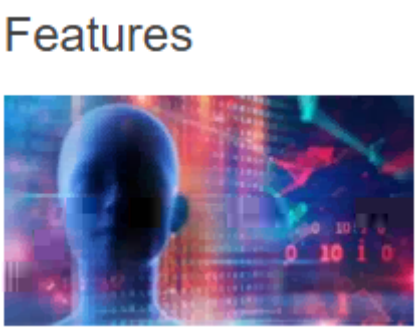
自版本 7.18 起，在以下任一情况下，HDX Thinwire 默认会切换到渐进式更新模式：

- 可用带宽低于 2 Mbps。
- 网络延迟超过 200 毫秒。

在此模式下：

例如，在下图中，渐进式更新模式处于活动状态，字母 **F** 和 **e** 具有蓝色赝像，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。


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，字母不再包含蓝色赝像，图像以源质量显示。



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

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

### 键盘

October 31, 2022

本部分内容包含以下主题：

- 客户端 IME
- 客户端 IME 用户界面同步
- 动态键盘布局同步
- 软键盘
- 支持多语言输入

## 客户端输入法编辑器 (IME)

October 31, 2022

#### 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

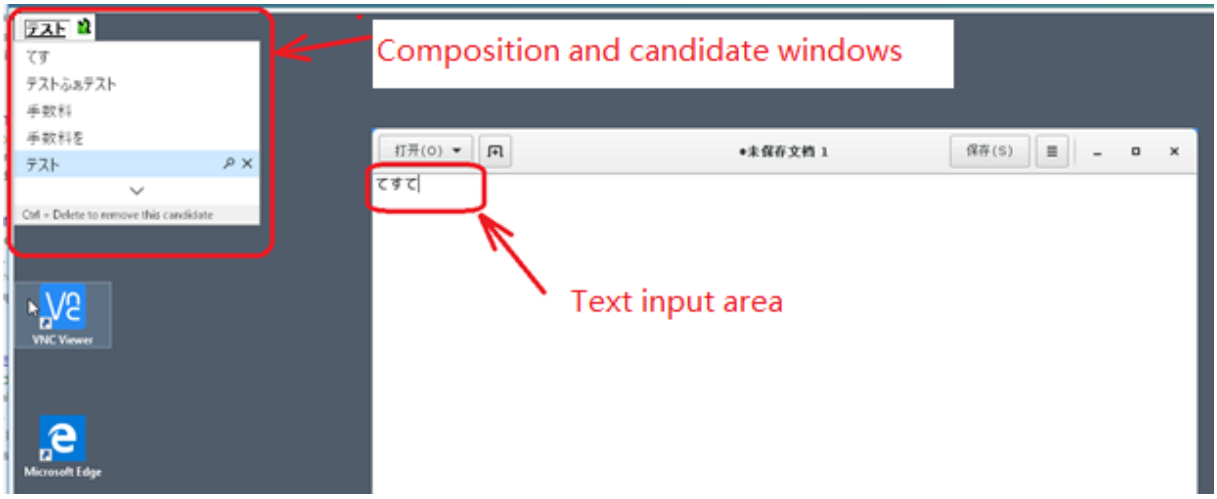
- 必须先双击 Google 电子表格中的单元格，才能使用客户端 IME 功能在单元格中键入字符。
- 不会在“密码”字段中自动禁用客户端 IME 功能。
- IME 用户界面不在输入区域中跟随光标。

## 客户端 IME 用户界面同步

November 4, 2022

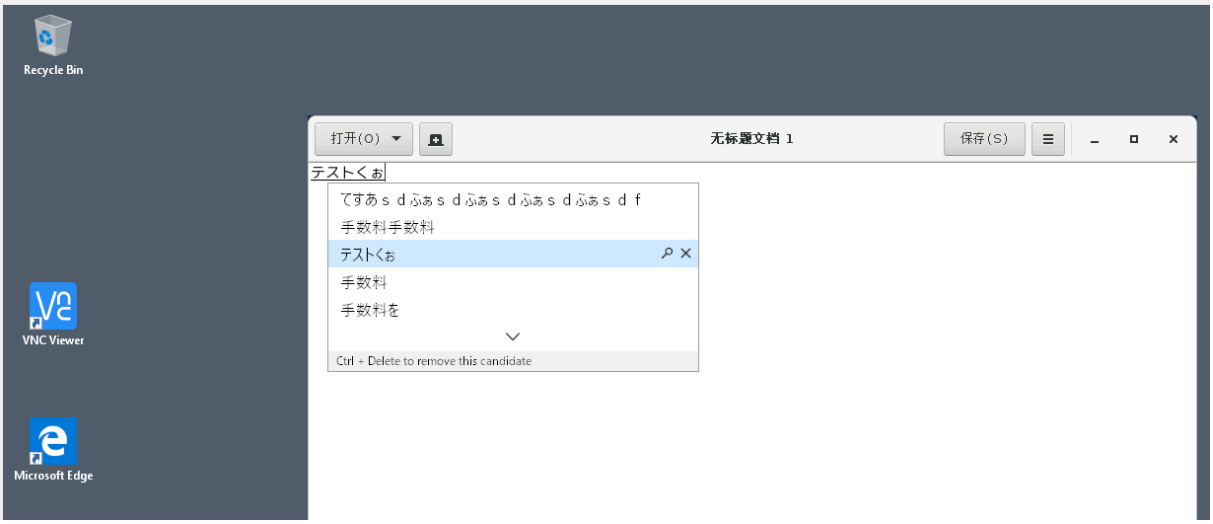
概述

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 的用户体验，如下所示：




使用此功能需满足的必备条件

1. 在 Linux VDA 上启用 Intelligent Input Bus (IBus)。有关如何在 Linux 操作系统上启用 IBus 的信息，请参阅操作系统供应商提供的文档。例如：
   - Ubuntu：https://help.ubuntu.com/community/ibus
   - CentOS、RHEL：https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/7.0_release_notes/sect-red_hat_enterprise_linux-7.0_release_notes-internationalization-input_methods
   - Debian：https://wiki.debian.org/I18n/ibus
   - SUSE：https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-gnome-settings.html#sec-gnome-settings-lang
2. 该功能将自动安装，但您必须先启用该功能才能使用它。

启用和禁用该功能

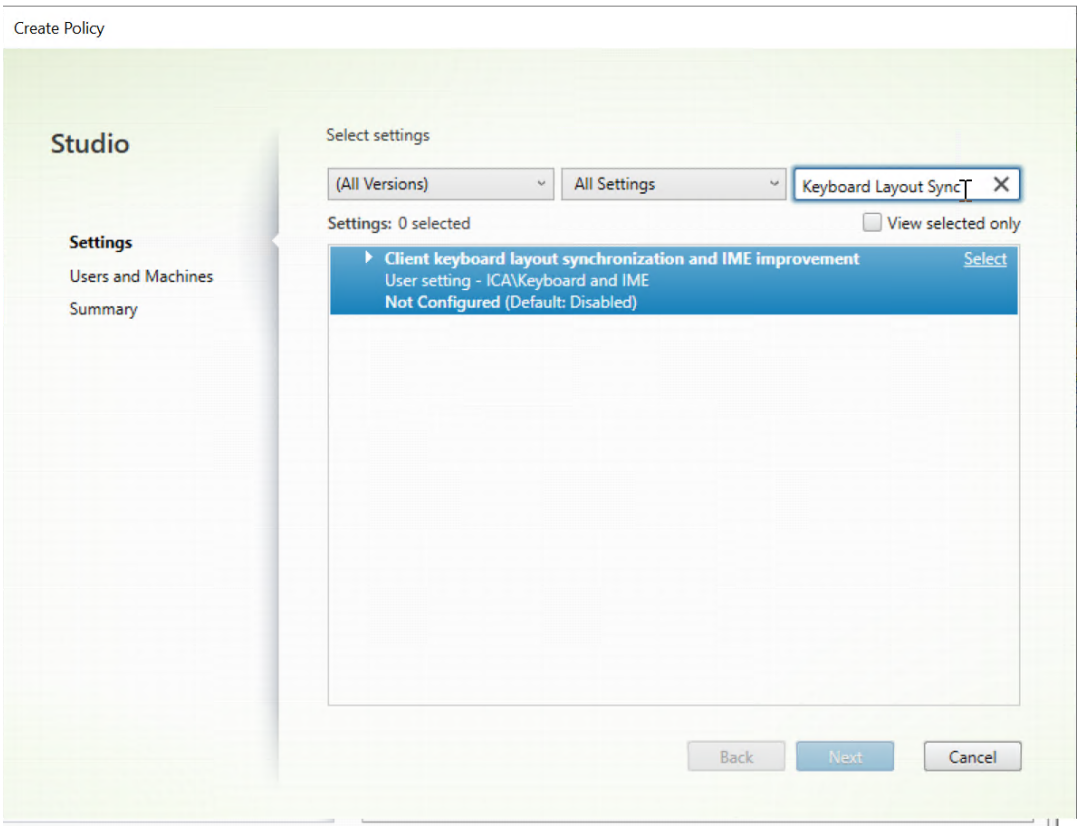
默认情况下禁用客户端 IME 用户界面同步功能。要启用或禁用此功能，请设置客户端键盘布局同步和 **IME** 改进功能策略，或通过 ctxreg 实用程序编辑注册表。

> 注意：
>
> 客户端键盘布局同步和 **IME** 改进功能策略的优先级高于注册表设置，可以应用到您指定的用户和计算机对象或站点中的所有对象。给定 Linux VDA 上的注册表设置应用到该 VDA 上的所有会话。

- 设置客户端键盘布局同步和 **IME** 改进功能策略以启用或禁用客户端 IME 用户界面同步功能：
  1. 在 Studio 中，右键单击策略，然后选择创建策略。

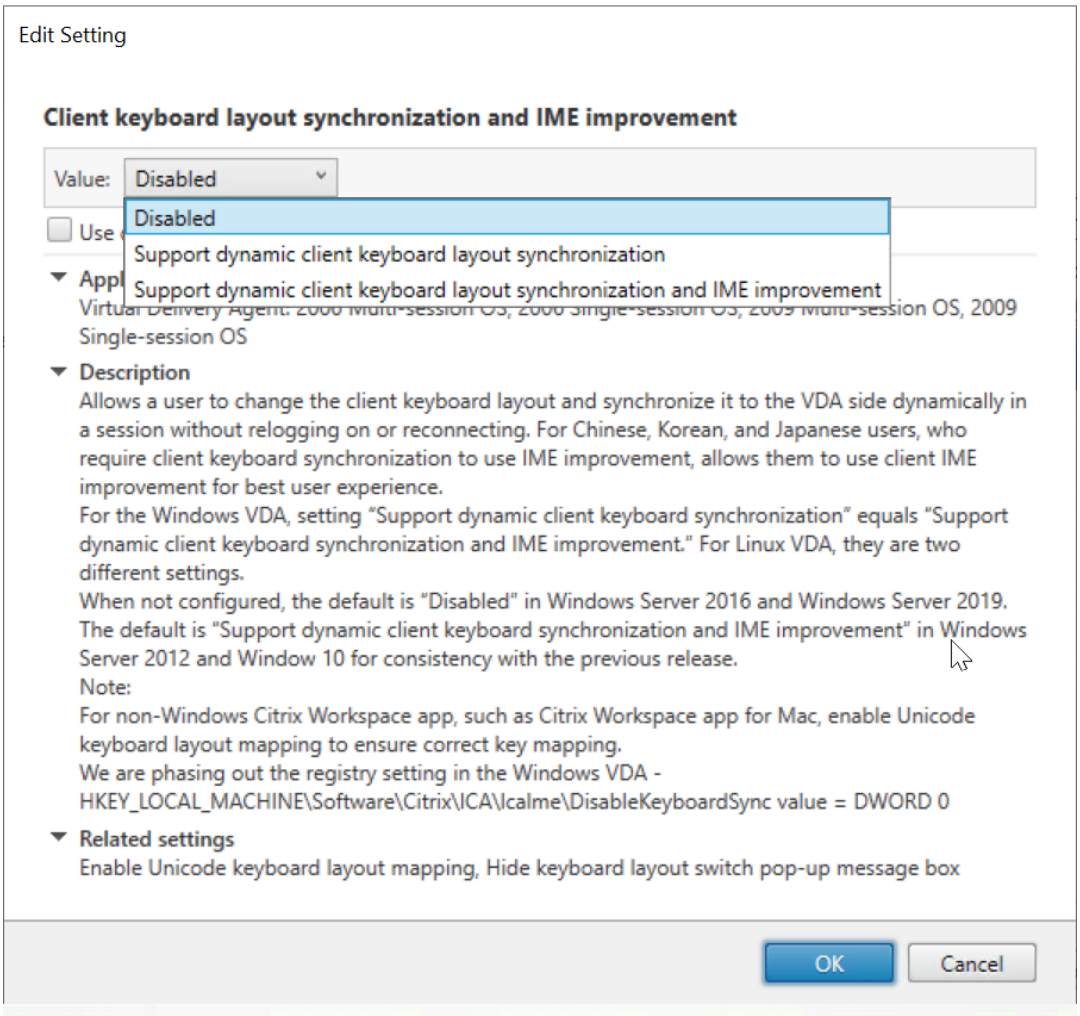
 

2. 搜索客户端键盘布局同步和 **IME** 改进功能策略。




3. 单击策略名称旁边的选择。
4. 设置策略。




共有三个可用选项：

- 已禁用：禁用动态键盘布局同步和客户端 IME 用户界面同步。
- 支持动态客户端键盘布局同步：启用动态键盘布局同步，而不考虑位于 `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar` 的 **SyncKeyboardLayout** 注册表项的 DWORD 值。
- 支持动态客户端键盘布局同步和 **IME** 改进功能：启用动态键盘布局同步和客户端 IME 用户界面同步，而不考虑位于 `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar` 的 **SyncKeyboardLayout** 和 **SyncClientIME** 注册表项的 DWORD 值。

- 通过 `ctxreg` 实用程序编辑注册表以启用或禁用客户端 IME 用户界面同步功能：

  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：

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

## 动态键盘布局同步

November 4, 2022

以前，Linux VDA 和客户端设备上的键盘布局必须相同。例如，当客户端设备上的键盘布局从“英语”更改为“法语”，但在 VDA 上未更改时，可能会出现按键映射问题。

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。

> 注意：
>
> 适用于 HTML5 的 Citrix Workspace 应用程序不支持动态键盘布局同步功能。

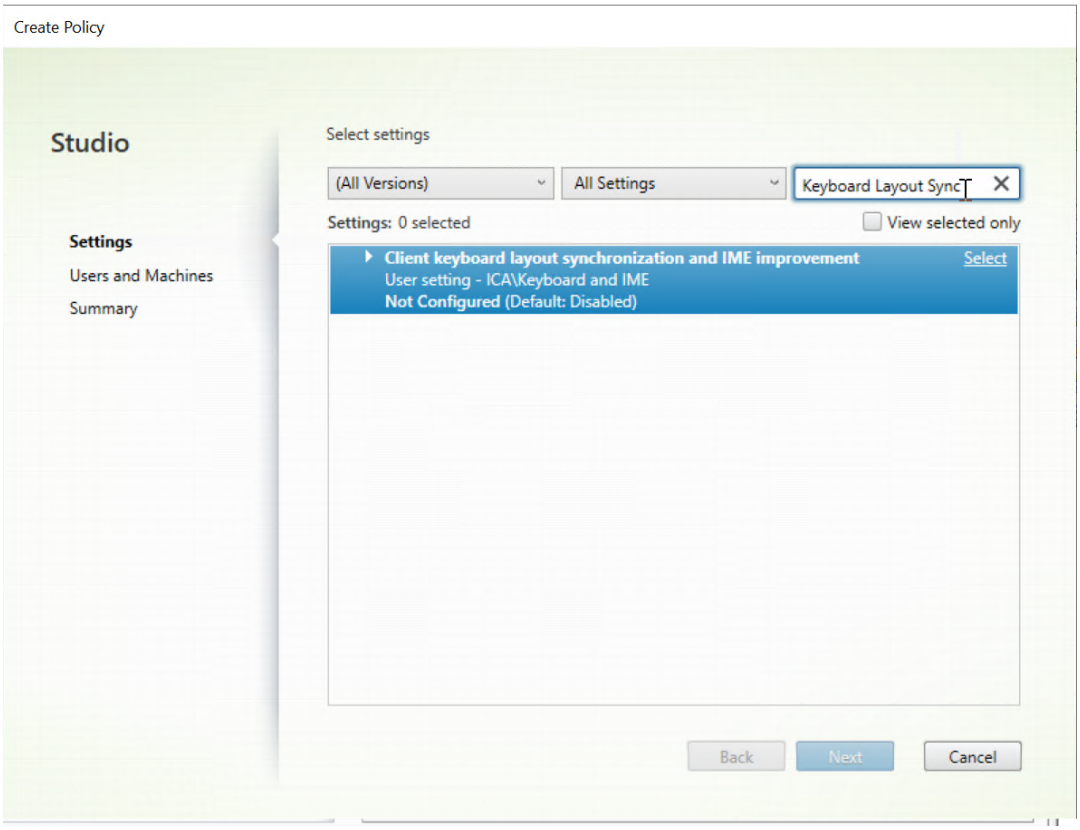
### 配置

默认情况下，动态键盘布局同步功能处于禁用状态。要启用或禁用此功能，请设置客户端键盘布局同步和 **IME** 改进功能策略，或通过 `ctxreg` 实用程序编辑注册表。

> 注意：
>
> 客户端键盘布局同步和 **IME** 改进功能策略的优先级高于注册表设置，可以应用到您指定的用户和计算机对象或站点中的所有对象。给定 Linux VDA 上的注册表设置应用到该 VDA 上的所有会话。

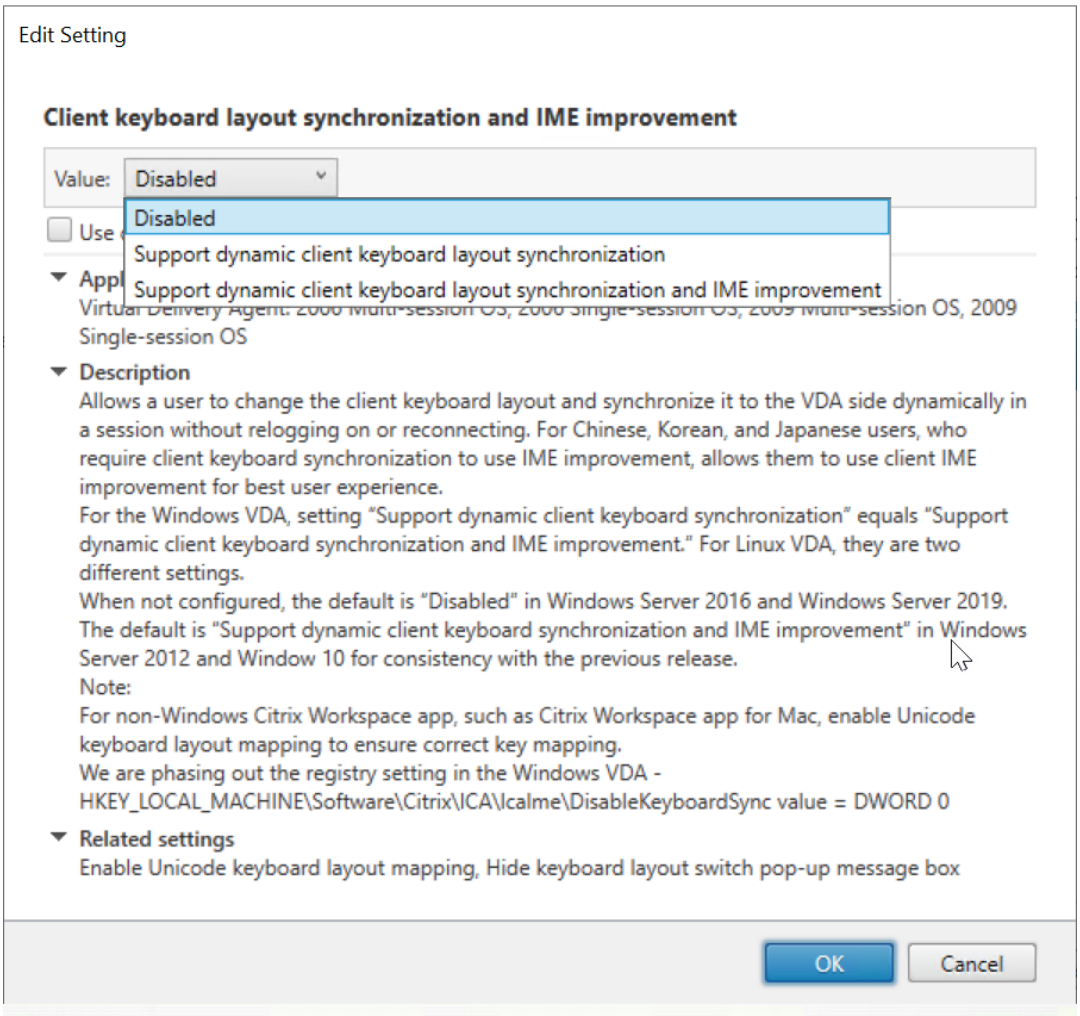
- 设置客户端键盘布局同步和 **IME** 改进功能策略以启用或禁用动态键盘布局同步功能：
  1. 在 Studio 中，右键单击策略，然后选择创建策略。
  2. 搜索客户端键盘布局同步和 **IME** 改进功能策略。




3. 单击策略名称旁边的选择。
4. 设置策略。




共有三个可用选项：

- 已禁用：禁用动态键盘布局同步和客户端 IME 用户界面同步。
- 支持动态客户端键盘布局同步：启用动态键盘布局同步，而不考虑位于 `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar` 的 **SyncKeyboardLayout** 注册表项的 DWORD 值。
- 支持动态客户端键盘布局同步和 **IME** 改进功能：启用动态键盘布局同步和客户端 IME 用户界面同步，而不考虑位于 `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar` 的 **SyncKeyboardLayout** 和 **SyncClientIME** 注册表项的 DWORD 值。

- 通过 `ctxreg` 实用程序编辑注册表以启用或禁用动态键盘布局同步功能：

  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-->
```

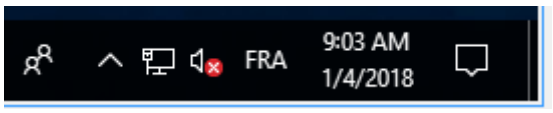
要禁用此功能，请运行以下命令：

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

使用情况

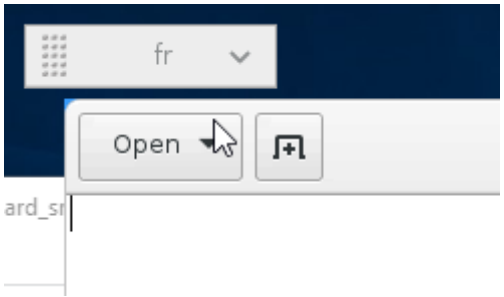
启用此功能后，如果会话过程中客户端设备上的键盘布局发生变化，会话的键盘布局也将相应地发生变化。

例如，如果将客户端设备上的键盘布局更改为“法语 (FR)”：

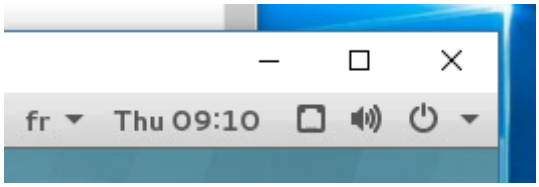



Linux VDA 会话的键盘布局随后也将更改为“fr”。

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：

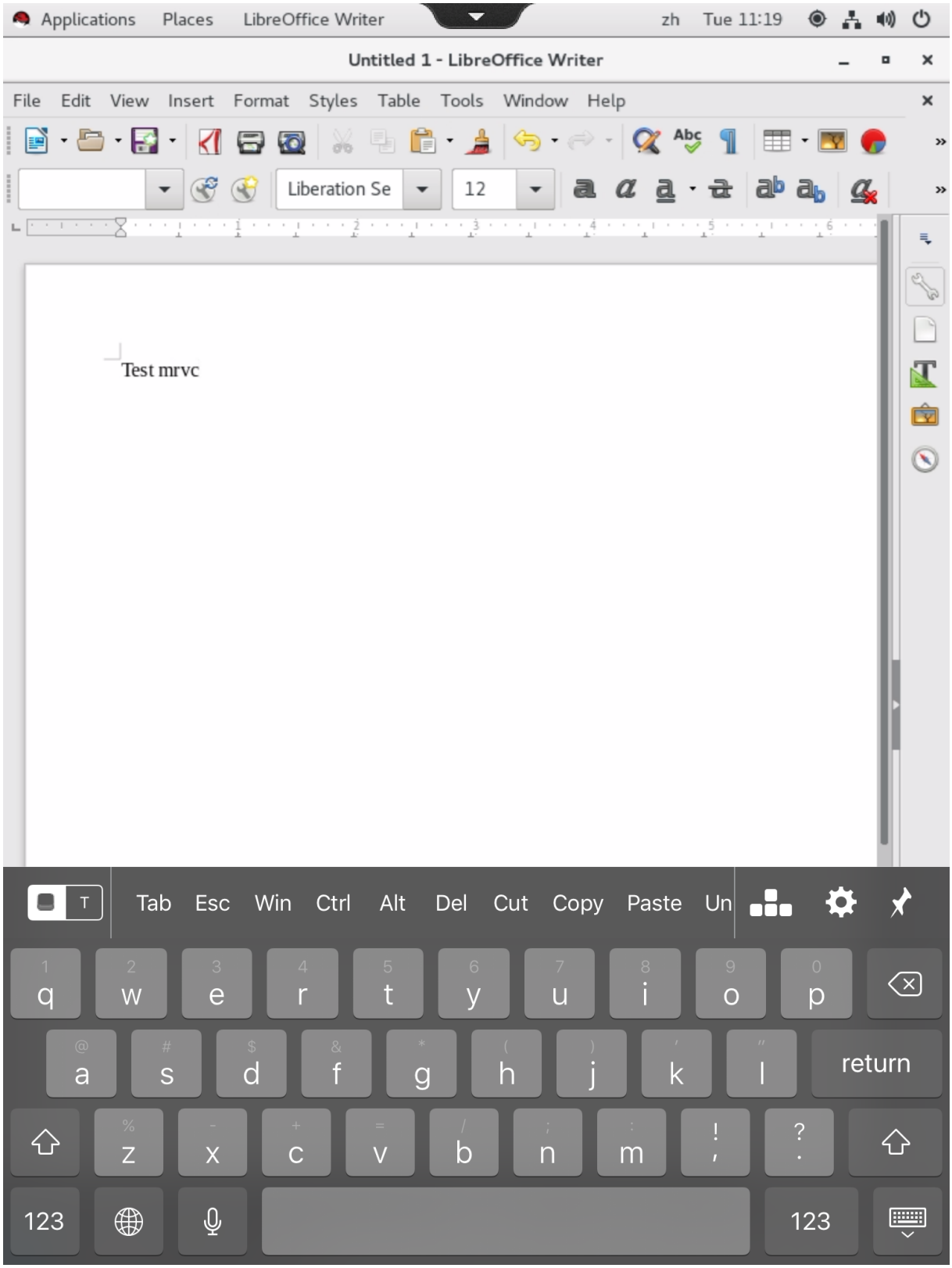



## 软键盘

November 4, 2022

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：
>
> 该功能适用于 RHEL 7.9、RHEL 8.4、RHEL 8.6、Rocky Linux 8、SUSE 15.3、Ubuntu 22.04、Ubuntu 20.04 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：

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

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

要禁用该功能，请运行以下命令：

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

## 支持多语言输入

November 4, 2022

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。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：

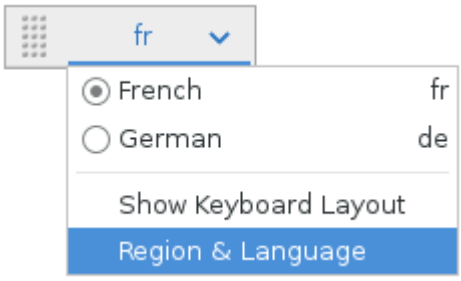
```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0
     x00000000"
2 <!--NeedCopy-->
```

使用情况

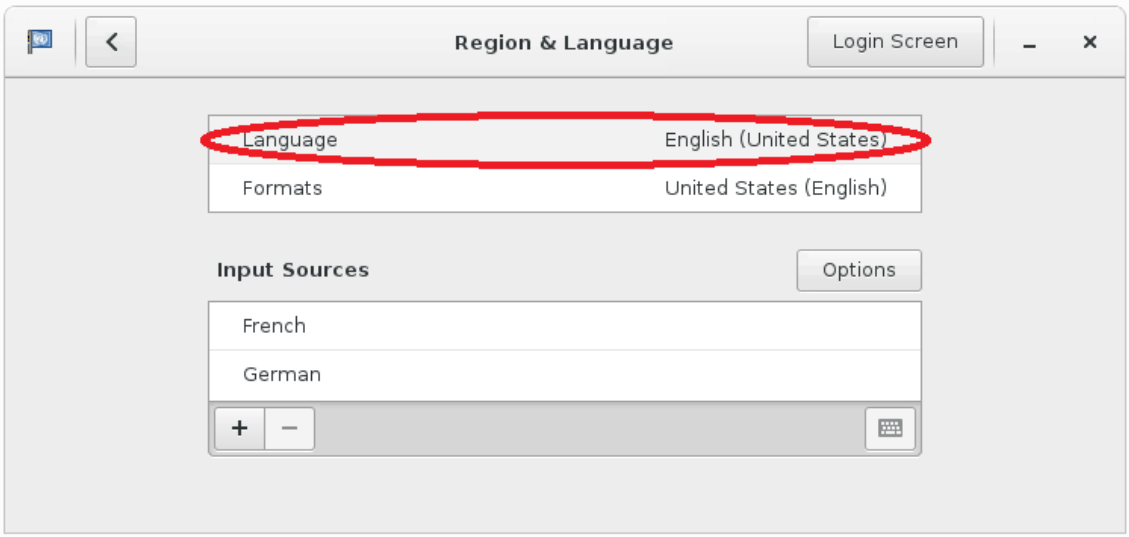
用法很简单。

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。



## 多媒体

October 31, 2022

本部分内容包含以下主题：

- 音频功能
- 浏览器内容重定向
- HDX 网络摄像机视频压缩

## 音频功能

August 8, 2023

### 自适应音频

自适应音频默认处于启用状态。它支持以下 Citrix Workspace 应用程序客户端：

- 适用于 Windows 的 Citrix Workspace 应用程序 - 2109 及更高版本
- 适用于 Linux 的 Citrix Workspace 应用程序 - 2109 及更高版本
- 适用于 Mac 的 Citrix Workspace 应用程序 - 2109 及更高版本

当您使用不在列表中的客户端时，自适应音频会回退到旧版音频。

使用自适应音频时，您无需手动在 VDA 上配置音频质量策略。自适应音频可以根据网络条件动态调整音频采样比特率，以提供优质的音频体验。

下表显示了自适应音频与旧版音频之间的比较结果：

| 自适应音频 | 旧版音频 |
| --- | --- |
| 最大音频采样率：48 kHz | 最大音频采样率：8 kHz |
| 立体声声道 | 单声道 |

> 提示：
>
> 请在 RHEL 8.x 上使用 PulseAudio 13.99 或更高版本。
>
> 请在 SUSE 15.3 上使用 PulseAudio 14.2 或更高版本。

# 浏览器内容重定向

November 4, 2022

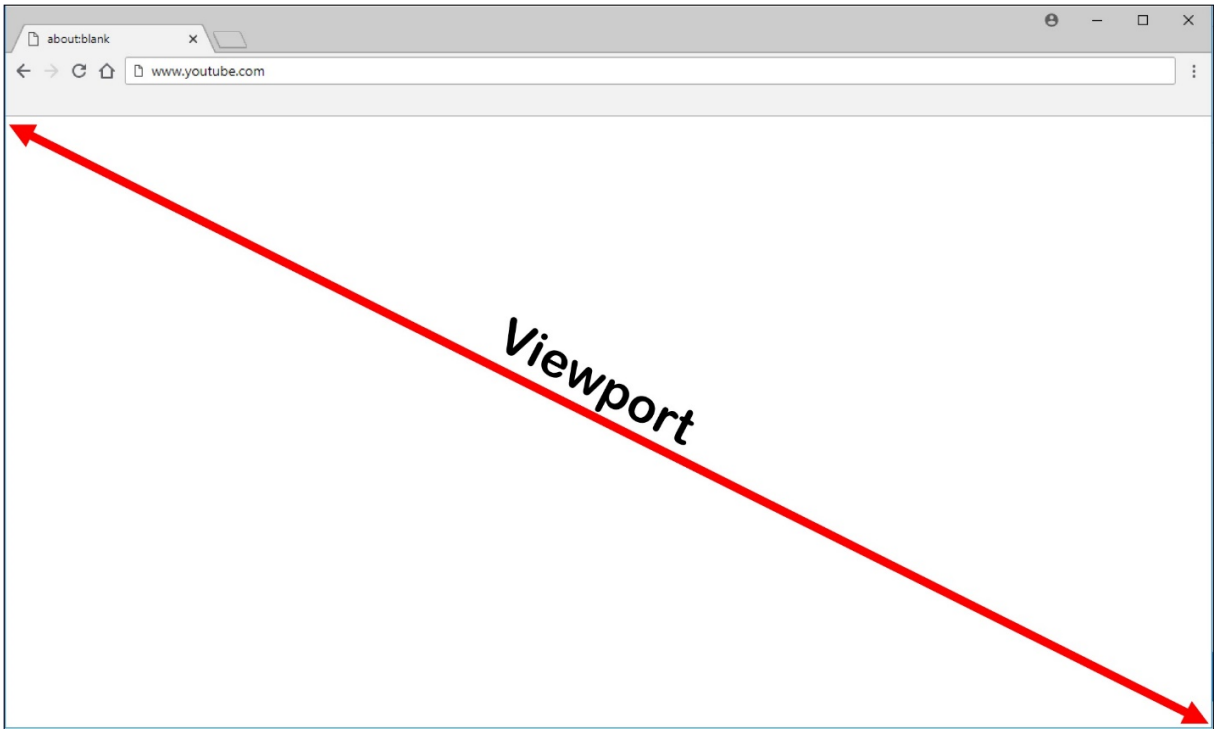
## 概述

Linux VDA 在 Google Chrome 中支持浏览器内容重定向。浏览器内容重定向提供了在客户端呈现允许列表中的 Web 页面的功能。此功能会使用 Citrix Workspace 应用程序在客户端实例化相应的呈现引擎，该引擎会从 URL 提取 HTTP 和 HTTPS 内容。

> 注意：
>
> 可以使用允许列表指定哪些 Web 页面被重定向到客户端。反过来，可以使用阻止列表指定哪些 Wen 页面不重定向到客户端。

此叠加 Web 布局引擎在客户端上运行，而非在 VDA 上运行，并且使用客户端 CPU、GPU、RAM 和网络。

只有浏览器视口会进行重定向。视口是浏览器中显示内容的矩形区域。视口不包括地址栏、收藏夹栏和状态栏等项目。这些项目仍在 VDA 上的浏览器中运行。




## 系统要求

**Windows** 客户端：

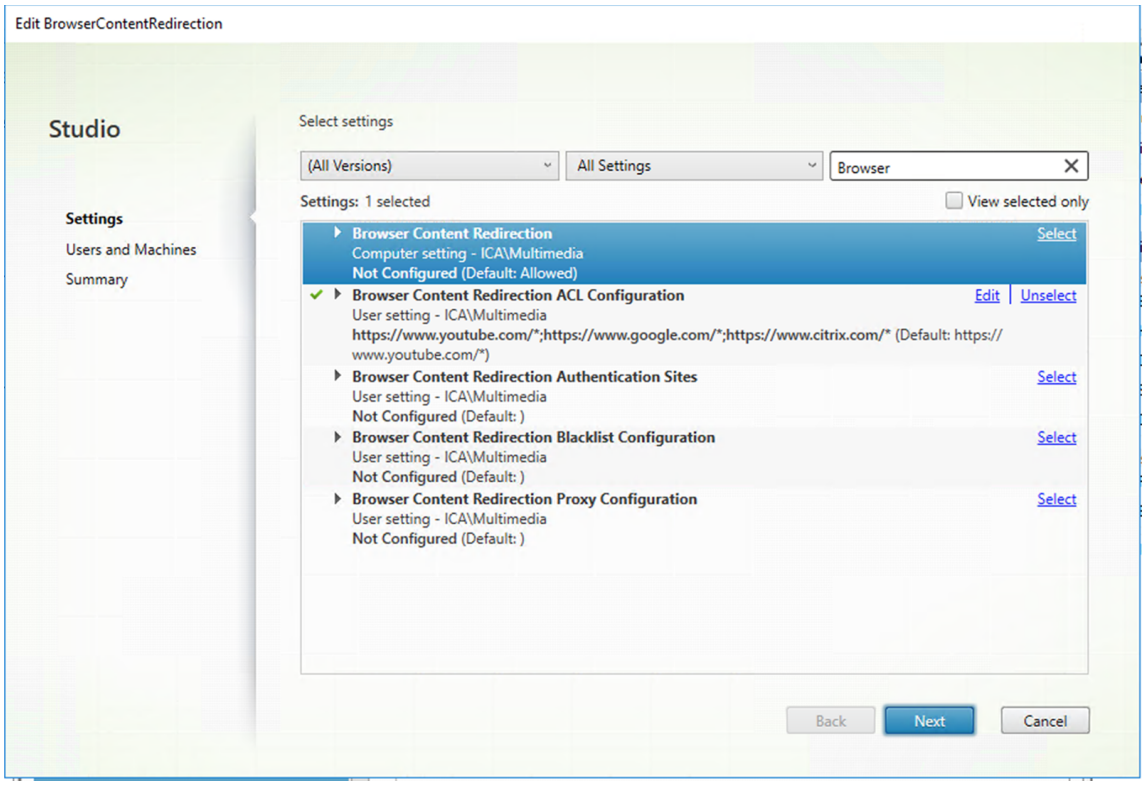
- 适用于 Windows 的 Citrix Workspace 应用程序 1809 或更高版本

**Linux VDA**:

- VDA 上的浏览器：添加了 Citrix 浏览器内容重定向扩展程序的 Google Chrome v66 或更高版本

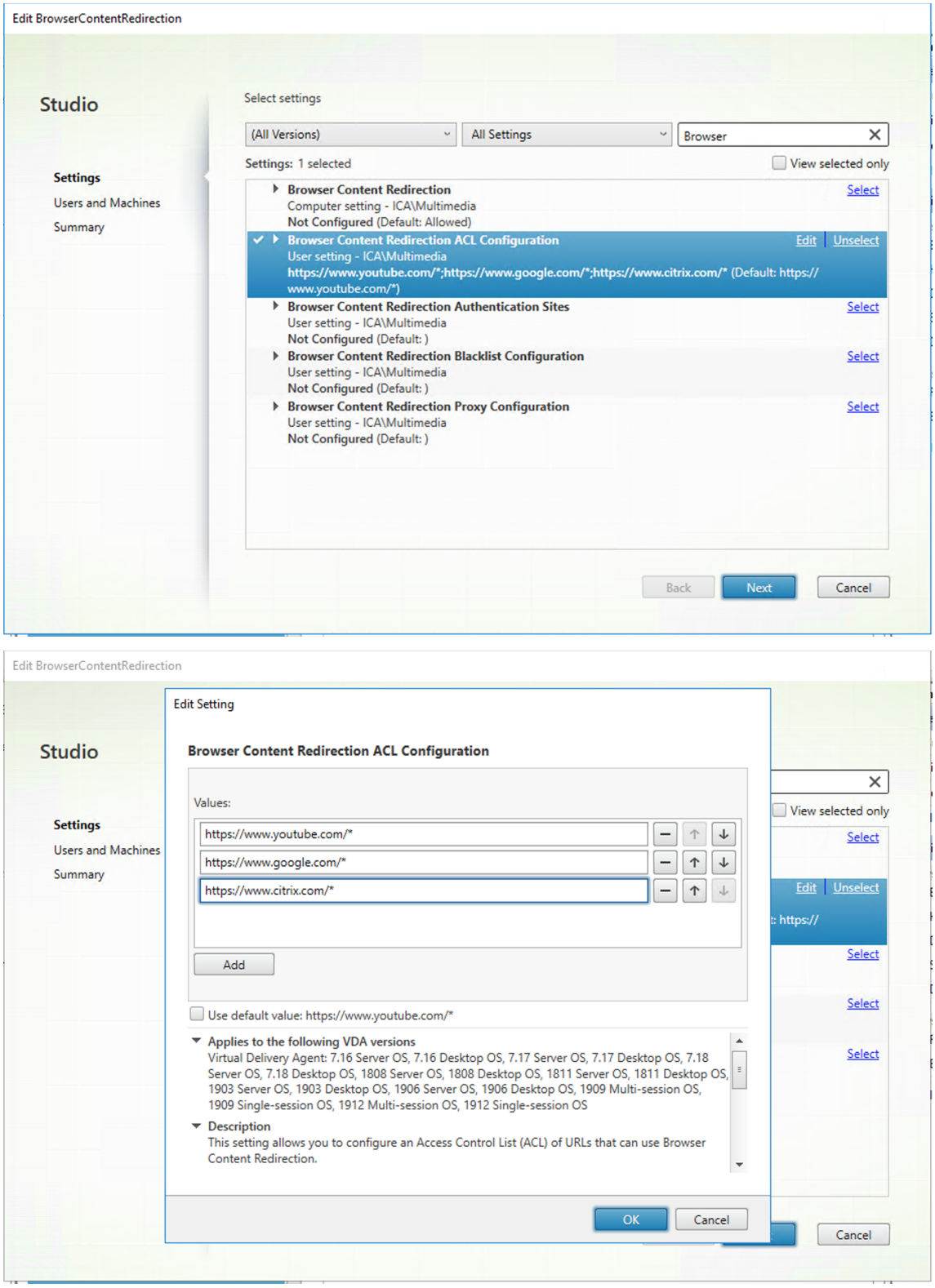
配置浏览器内容重定向

1. 在 Citrix Studio 中，配置策略以指定浏览器内容重定向的允许列表和 URL 阻止列表。默认情况下，浏览器内容重定向设置为允许。



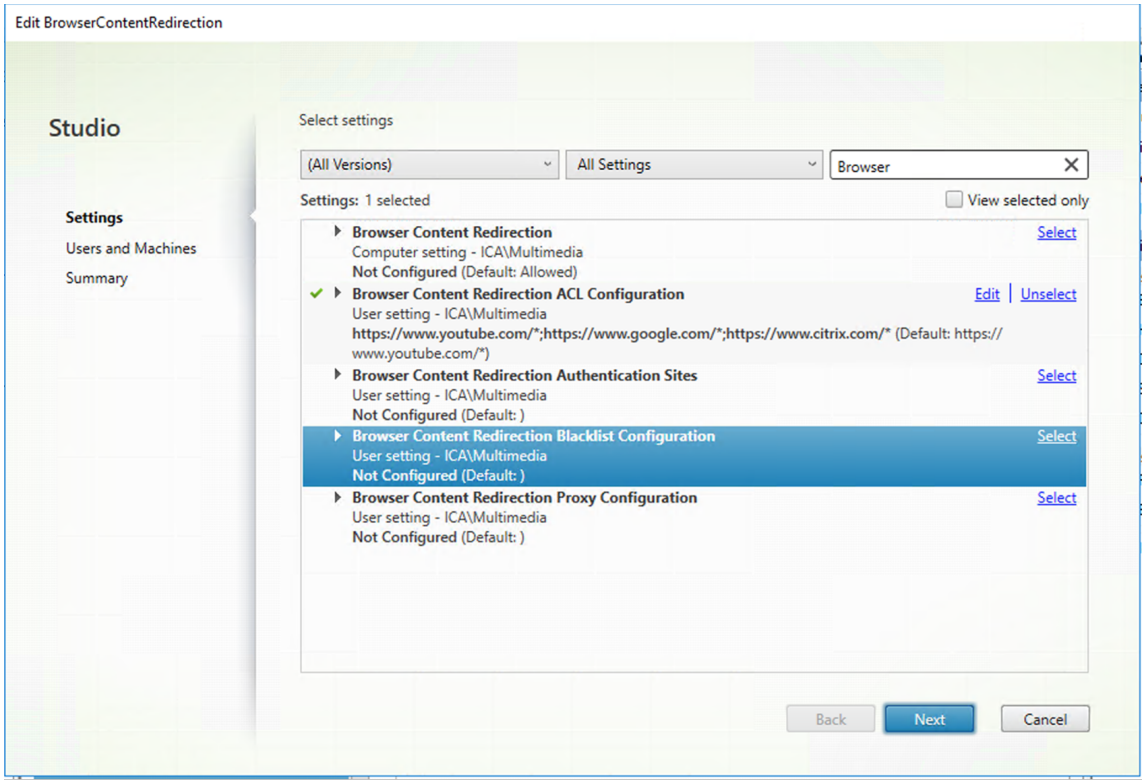

浏览器内容重定向 **ACL** 配置设置指定可以使用浏览器内容重定向的 URL 的允许列表。




浏览器内容重定向黑名单配置设置指定不能使用浏览器内容重定向的 URL 的阻止列表。

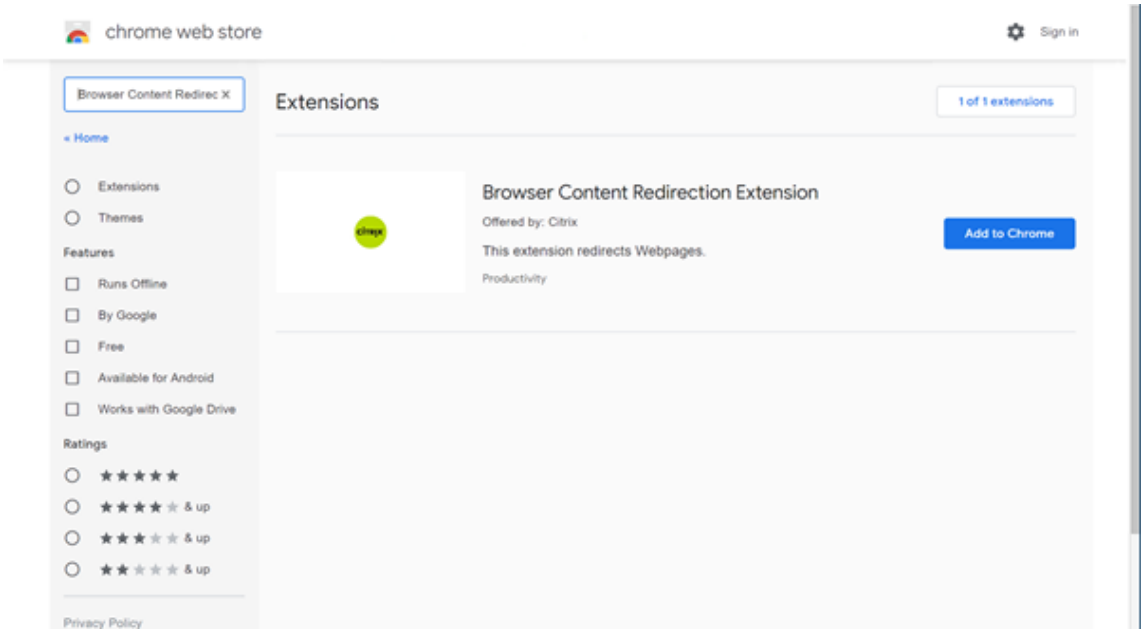



> 注意：
>
> Linux VDA 当前不支持浏览器内容重定向代理配置设置。

2. 单击 VDA 上的 **Add to Chrome**（添加到 Chrome），从 Chrome 网上应用店添加 Citrix 浏览器内容重定向扩展程序。这样做有助于 VDA 上的浏览器检测（正在导航到的）URL 是否与允许列表或阻止列表匹配。

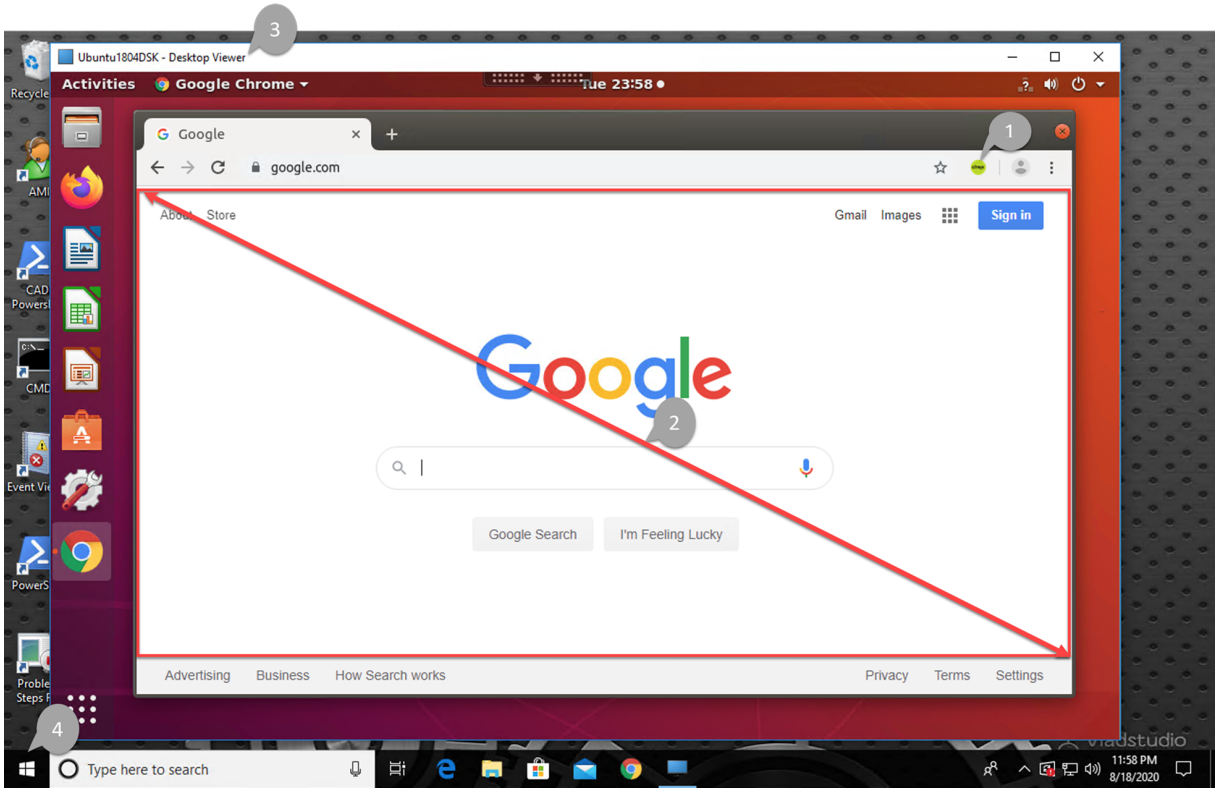
> 重要：
>
> 客户端上不需要此扩展程序。仅在 VDA 上添加。
>
> Chrome 扩展程序基于每个用户安装。不需要更新黄金映像即可添加或删除扩展程序。




如果在允许列表（例如 `https://www.mycompany.com/`）中找到与 URL 匹配的 URL，但在任何阻止列表中都未找到，虚拟通道 (CTXCSB) 会指示 Citrix Workspace 应用程序需要重定向并中继 URL。然后，Citrix Workspace 应用程序会实例化一个本地呈现引擎并显示此 Web 站点。

之后，Citrix Workspace 应用程序会将此 Web 站点无缝融入虚拟桌面浏览器内容区域中。




1. Citrix 浏览器内容重定向扩展程序的图标

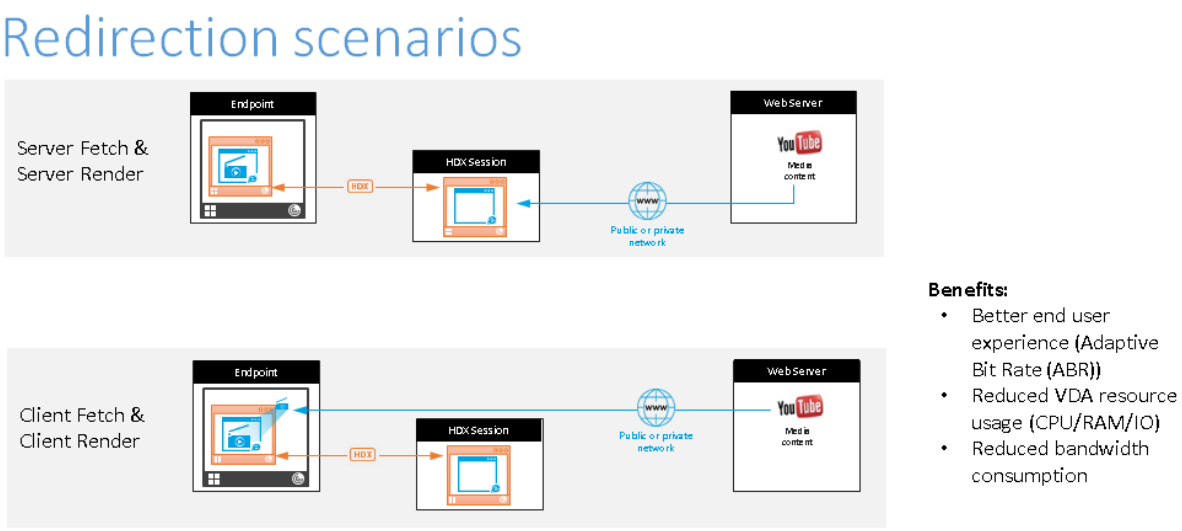
扩展程序图标的颜色指定 Chrome 扩展程序的状态。其颜色为以下三种颜色之一：

- 绿色：活动并连接
- 灰色：在当前选项卡上不活动/空闲
- 红色：已损坏/不运行

2. 视口在客户端上呈现或混合回虚拟桌面
3. Linux VDA
4. Windows 客户端

### 重定向场景

下面是 Citrix Workspace 应用程序提取内容的方式的几种情况：




- 服务器提取和服务器呈现：由于没有将站点添加到允许列表或重定向失败，因此没有重定向。我们将回退到在 VDA 上呈现 Web 页面，并使用 Thinwire 来远程显示图形。使用策略来控制回退行为。这种情况会导致 VDA 上的 CPU、RAM 和带宽消耗较高。
- 客户端提取和客户端呈现：由于 Citrix Workspace 应用程序直接连接 Web 服务器，因此需要访问 Internet。在这种情况下，会从 Citrix Virtual Apps and Desktops 站点卸载所有网络、CPU 和 RAM 使用量。

### 回退机制

客户端重定向有时可能会失败。例如，如果客户端计算机无法直接访问 Internet，则可能会向 VDA 返回一条错误响应。在这种情况下，VDA 上的浏览器可以在服务器上重新加载并呈现页面。

# HDX 网络摄像机视频压缩

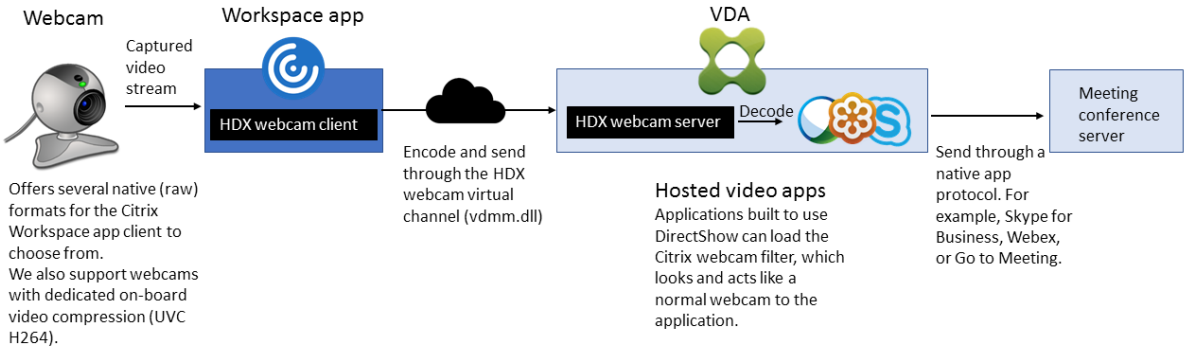
March 28, 2023

## 概述

在 Linux VDA 会话中运行的视频会议应用程序的用户现在可以使用 HDX 网络摄像机视频压缩功能的网络摄像机。默认情况下启用该功能。我们建议您始终尽可能使用 HDX 网络摄像机视频压缩功能。

HDX 网络摄像机视频压缩也称为优化网络摄像机模式。这种类型的网络摄像机视频压缩将 H.264 视频直接发送到在虚拟会话中运行的视频会议应用程序。HDX 网络摄像机视频压缩使用属于客户端操作系统的多媒体框架技术截获来自捕捉设备的视频，并对其进行转换代码和压缩。捕获设备的制造商提供插入操作系统内核流技术推送体系结构的驱动程序。

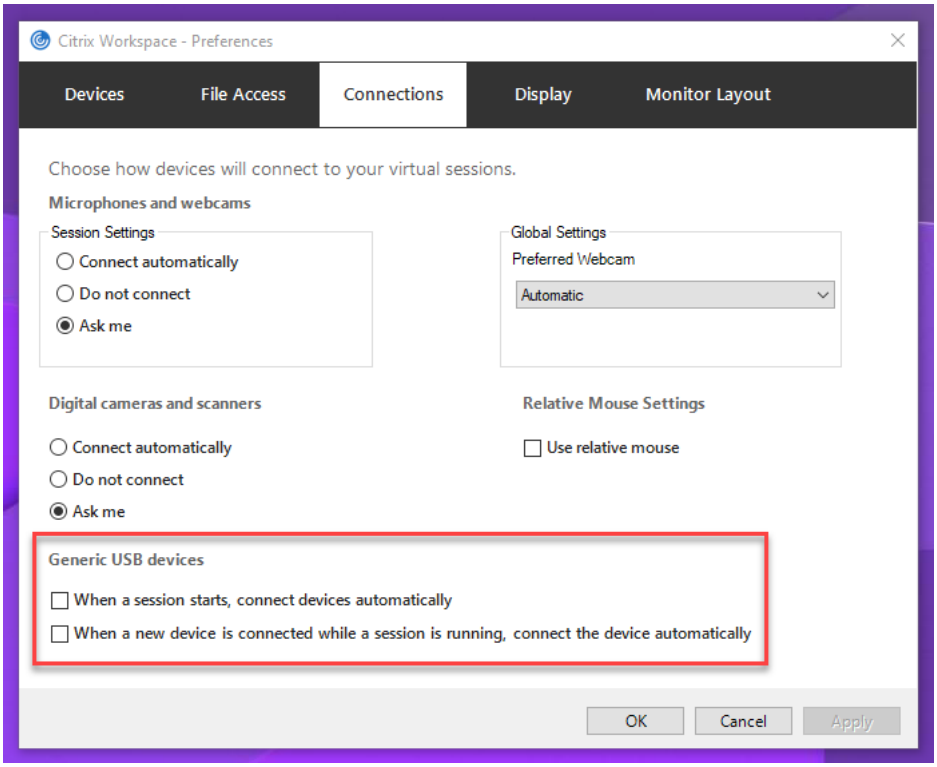
客户端处理与网络摄像机的通信。之后，客户端仅将视频发送到可以正确显示它的服务器。服务器不能直接与网络摄像机通信，但其集成可在您的桌面中为您提供相同的体验。Workspace 应用程序会压缩视频以节省带宽，并在 WAN 场景中提高恢复能力。




注意：

- 该功能不适用于 Azure 计算机，因为 Azure 计算机上缺少该功能所依赖的 **videodev** 内核模块。
- 此功能仅支持来自 Citrix Workspace 应用程序客户端的 H.264 视频。
- 支持的网络摄像机分辨率在 48x32 到 1920x1080 之间。
- 使用网络摄像机时，请勿从 Citrix Workspace 应用程序工具栏中选择通用 **USB** 设备。否则，可能会出现意外的问题。




### 支持 **Citrix Workspace** 应用程序

HDX 网络摄像机视频压缩支持以下版本的 Citrix Workspace 应用程序：

| 平台 | 处理器 |
| --- | --- |
| 适用于 Windows 的 Citrix Workspace 应用程序 | 适用于 Windows 的 Citrix Workspace 应用程序支持 XenApp 和 XenDesktop 7.17 及更高版本上面向 32 位和 64 位应用程序的网络摄像机视频压缩。在早期版本中，适用于 Windows 的 Citrix Workspace 应用程序仅支持 32 位应用程序。 |
| 适用于 Chrome 的 Citrix Workspace 应用程序 | 由于某些 ARM Chromebook 不支持 H.264 编码，因此，只有 32 位应用程序可以使用优化的 HDX 网络摄像机视频压缩。 |

### 完全测试的网络摄像机

不同的网络摄像机提供不同的帧速率，并具有不同级别的亮度和对比度。Citrix 使用以下网络摄像机进行初始功能验证：

- Logitech HD Webcam C270

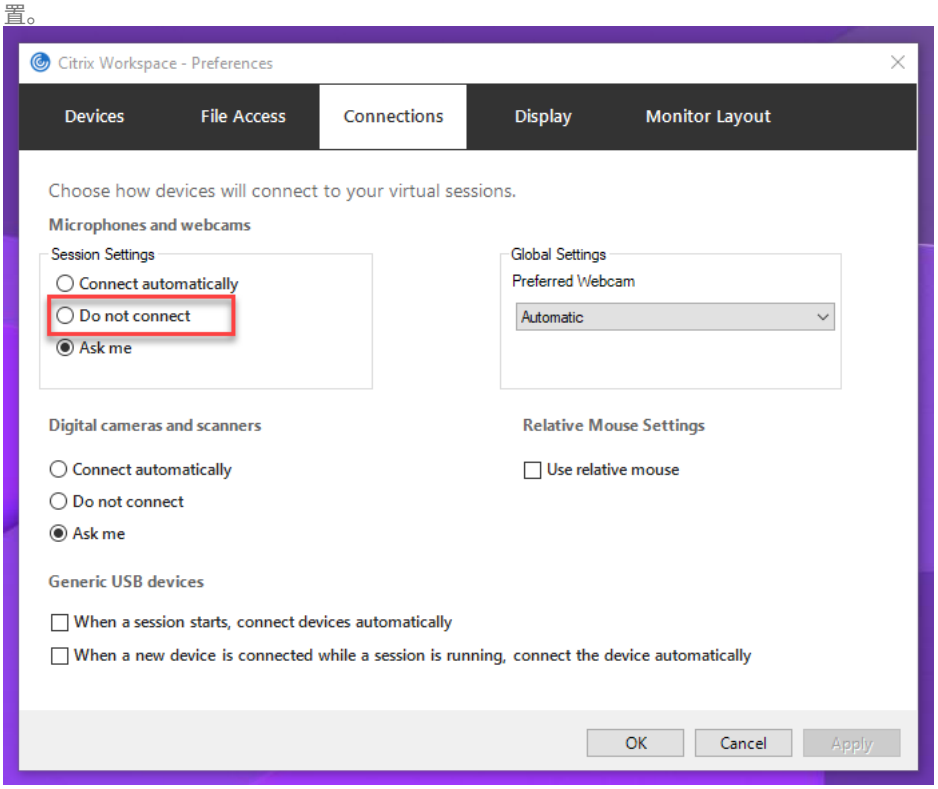
 

- Logitech Webcam C930e
- Microsoft-LifeCam-HD3000

### 配置

默认情况下启用此功能。要使用，请完成以下验证和配置：

> 提示：
>
> Citrix Workspace 应用程序用户可以通过选择 Desktop Viewer 麦克风和网络摄像机设置不连接来覆盖默认设置。




1. VDA 安装完成后，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 Windows 凭据成功启动。
2. 确保您的 VDA 可以访问 Internet，然后运行 `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` 命令以完成网络摄像机配置。如果您的 VDA 无法访问 Internet，请转到步骤 3。

   > 注意：
   >
   > `uname -r` 与内核标头之间可能会发生内核不匹配。不匹配会导致 ctxwcamcfg.sh 脚本失败。要正确使用 HDX 网络摄像机视频压缩，请运行 **sudo apt-get dist-upgrade**，重新启动 VDA，然后重新运行 ctxwcamcfg.sh 脚本。

   如果您的 VDA 部署在 Debian 上，请确保其在最新的内核版本上运行。否则，请运行以下命令以更新到最新的内核版本：

```
sudo apt-get update
sudo apt-get dist-upgrade
sudo reboot
<!--NeedCopy-->
```

如果 VDA 部署在 SUSE 15.3、SUSE 15.2 或 SUSE 12.5 上，请运行以下命令以更新到最新的内核版本并重新启动：

```
zypper up kernel-default
reboot
<!--NeedCopy-->
```

ctxwcamcfg.sh 脚本有助于：

a) 在 VDA 上安装 `kernel-devel` 和动态内核模块支持 (DKMS) 程序。

- `kernel-devel` 用于构建相应版本的虚拟网络摄像机内核模块。
- DKMS 用于动态管理虚拟网络摄像机内核模块。

> 注意：
>
> 在 RHEL 和 CentOS 上安装上述程序时，`ctxwcamcfg.sh` 脚本会在您的 VDA 上安装并启用以下存储库：
>
> - 适用于 Enterprise Linux (EPEL) 的额外软件包
> - RPM Fusion

b) 从 https://github.com/umlaeute/v4l2loopback 中下载 `v4l2loopback` 开源代码并使用 DKMS 管理 `v4l2loopback`。
`v4l2loopback` 是一个允许您创建 V4L2 环回设备的内核模块。

c) 运行 `sudo service ctxwcamsd restart` 命令。Linux VDA 的网络摄像机服务 - `ctxwcamsd` - 重新启动并加载 HDX 网络摄像机视频压缩功能的 `v4l2loopback` 内核模块。

3. 如果您的 VDA 无法访问 Internet，请在另一台计算机上构建 v4l2loopback 内核模块，然后再将其复制到您的 VDA。

a) 准备一台能够访问 Internet 且内核版本与 VDA 相同的生成计算机。`uname -r` 命令可帮助查找内核版本。

b) 在生成计算机上，运行 `sudo mkdir -p /var/xdl` 命令。

c) 将 `/var/xdl/configure_*` 从您的 VDA 复制到 `/var/xdl/` 下方的生成计算机。

d) 在生成计算机上，运行 `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` 命令以生成内核模块。如果该命令成功运行，则会在 `/var/lib/dkms/v4l2loopback/1.81b8df79107d1fbf392fdcbaa051bd227a9c94c1/$(uname -r)/x86_64/module/` 路径下创建 v4l2loopback.ko 文件。忽略在运行 ctxwcamcfg.sh 脚本时可能会出现的错误。

e) 将 v4l2loopback.ko 从生成计算机复制到您的 VDA 并将其置于 /opt/Citrix/VDA/lib64/ 下方。

f) 在您的 VDA 上，运行 sudo service ctxwcamsd restart 命令以重新启动网络摄像机服务并加载 v4l2loopback 内核模块。

## 未加入域的 VDA

November 3, 2022

### 设置概述

只有 Citrix DaaS 支持未加入域的 VDA。必须使用 Machine Creation Services (MCS)，才能在 Citrix DaaS 中创建未加入域的 VDA。简短的步骤如下：

1. 在还要安装 VDA 软件包的模板 VM 上创建主映像。可以使用单个映像来创建已加入域和未加入域的 VDA。
2. 使用主映像创建计算机目录。选择 MCS 作为计算机部署方法，然后选择未加入域作为要在目录中创建的计算机的标识。

有关详细信息，请参阅使用 Machine Creation Services (MCS) 创建 Linux VM 和计算机标识。

### 适用于未加入域的 VDA 的功能

#### 在未加入域的 VDA 上创建具有指定属性的本地用户

打开未加入域的 VDA 上托管的会话时，VDA 会自动创建具有默认属性的本地用户。VDA 将根据您用于登录 Citrix Workspace 应用程序的用户名创建本地用户。还可以指定用户属性，包括用户的用户标识符 (UID)、组 ID (GID)、主目录和登录 shell。要使用此功能，请完成以下步骤：

1. 运行以下命令以启用该功能：

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent\LocalMappedAccount" -t "REG_DWORD" -v "
     CreateWithUidGid" -d "0x00000001" --force
2 <!--NeedCopy-->
```

2. 在 VDA 的安装路径下的 /var/xdl/getuidgid.sh 脚本中指定以下属性：

| 属性 | 必需或可选 | 说明 |
| --- | --- | --- |
| uid | 必需 | 用户标识符 (UID) 是由 Linux 分配给系统中的每个用户的编号。它决定用户可以访问哪些系统资源。 |
| gid | 必需 | 组标识符 (GID) 是用于表示特定组的编号。 |
| homedir | 可选 | Linux 主目录是特定用户的目录。 |
| shell | 可选 | 登录 shell 是在用户登录其用户帐户时提供给用户的 shell。 |

下面是 getuidgid.sh 脚本的示例：

> 注意：
>
> 请确保您在脚本中指定的属性有效。

```
#!/bin/bash

################################################################################

#
# 适用于 Linux 的 Citrix Virtual Apps and Desktops 脚本：为用户获取 uid 和 gid
#
# 版权所有 (c) Citrix Systems, Inc. 保留所有权利。
#

export LC_ALL="en_US.UTF-8"

function get_uid_gid_for_user()
{

echo "uid:12345"
echo "gid:1003"
echo "homedir:/home/$1"
echo "shell:/bin/sh"
 }


get_uid_gid_for_user $1<!--NeedCopy-->
```

策略支持列表

November 4, 2022

## **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 | IcaRoundTripCalculation | 计算机 | ICA\最终用户监视 | 已启用 (1) |
| **ICA** 往返行程计算间隔 | IcaRoundTripCalculationInterval | 计算机 | ICA\最终用户监视 | 15 |
| 空闲连接的 **ICA** 往返行程计算 | IcaRoundTripCalculationWhenIdle | 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 |

| Studio 策略 | 注册表项名称 | 类型 | 模块 | 默认值 |
| --- | --- | --- | --- | --- |
| 客户端 **USB** 设备重定向带宽百分比 | LimitUSBBwPercent | DWORD | ICA\带宽 | 0 |
| 剪贴板重定向带宽限制 | LimitClipboardBW | DWORD | ICA\带宽 | 0 |
| 剪贴板重定向带宽限制百分比 | LimitClipboardBWPercent | DWORD | ICA\带宽 | 0 |
| 文件重定向带宽限制 | LimitCdmBw | DWORD | ICA\带宽 | 0 |
| 文件重定向带宽限制百分比 | LimitCdmBwPercent | DWORD | ICA\带宽 | 0 |
| 打印机重定向带宽限制 | LimitPrinterBw | DWORD | ICA\带宽 | 0 |
| 打印机重定向带宽限制百分比 | LimitPrinterBwPercent | DWORD | ICA\带宽 | 0 |
| **WebSocket** 连接 | AcceptWebSocketsConnections | 计算机 | ICA\WebSockets | 1 |

| Studio 策略 | 注册表项名称 | 类型 | 模块 | 默认值 |
| --- | --- | --- | --- | --- |
| **WebSocket** 端口号 | WebSocketPort | 计算机 | ICA\WebSockets | 8008 |
| **WebSocket** 可信源服务器列表 | WSTrustedOriginServerList | 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) |
| 会话可靠性连接 | AcceptSessionReliability | 计算机 | ICA\会话可靠性 | 允许 Connections (1) |
| 重新连接 **UI** 透明度级别 | ReconnectUiTransparency | 计算机 | ICA\客户端自动重新连接 | 80% level |
| 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 |

| Studio 策略 | 注册表项名称 | 类型 | 模块 | 默认值 |
| --- | --- | --- | --- | --- |
| 客户端自动重新连接 | AllowAutoClientReconnect | DWORD | ICA\客户端自动重新连接 | 允许 (1) |
| 客户端音频重定向 | AllowAudioRedirection | DWORD | 音频 | 允许 (1) |
| 客户端打印机重定向 | AllowPrinterRedir | DWORD | 打印 | 允许 (1) |
| 自动创建 **PDF** 通用打印机 | AutoCreatePDFPrinter | DWORD | 打印 | 已禁用 (0) |
| 打印机驱动程序映射和兼容性 | DriverMappingList | 字符串 | 打印 | "Microsoft XPS Document Writer *, Deny; Send to Microsoft OneNote *, Deny" |
| 客户端剪贴板重定向 | AllowClipboardRedir | DWORD | 剪贴板 | 允许 (1) |

| Studio 策略 | 注册表项名称 | 类型 | 模块 | 默认值 | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 客户端 **USB** 设备重定向 | AllowUSBRedir | DWORD | USB | 禁止 (0) | | | | | |
| 客户端 **USB** 设备重定向规则 | USBDeviceRules | REG_SZ | USB | “ | 客户端 **USB** 设备重定向规则 | USBDeviceRules | USB | “\0” | ” |
| 移动图像压缩 | MovingImageCompressionConfiguration | DWORD | Thinwire Compression | 已禁用 (1) | | | | | |
| 额外颜色压缩 | ExtraColorCompression | DWORD | Thinwire | 已禁用 (0) | | | | | |
| 目标最低帧速率 | TargetedMinimumFramesPerSecond | DWORD | Thinwire | 10 fps | | | | | |
| 目标帧速率 | FramesPerSecond | DWORD | Thinwire | 30 fps | | | | | |
| 视觉质量 | VisualQuality | DWORD | Thinwire | 中 (3) | | | | | |
| 使用视频编解码器进行压缩 | VideoCodec | DWORD | Thinwire | 首选时使用 (3) | | | | | |
| 使用视频编解码器的硬件编码 | UseHardwareEncodingForVideoCodec | DWORD | Thinwire | 已禁用 (1) | | | | | |
| 允许视觉无损压缩 | AllowVisuallyLosslessCompression | DWORD | Thinwire Compression | 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 | DWORD | ThinWire | 已禁用 (0) |
| 简单图形的首选颜色深度 | PreferredColorDepth | DWORD | ThinWire | 24 位/像素 (1) |
| 音频质量 | SoundQuality | DWORD | 音频 | 高 - 高清晰度音频 (2) |
| 客户端麦克风重定向 | AllowMicrophoneRedir | DWORD | 音频 | 允许 (1) |
| 最大会话数 | MaximumNumberOfSessions | DWORD | 计算机管理 | 250 |
| 并发登录数容差 | ConcurrentLogonsTolerance | DWORD | 负载管理 | 2 |
| 启用控制器自动更新 | EnableAutoUpdateOfControllers | DWORD | Virtual Desktop Agent 设置 | 允许 (1) |
| 剪贴板选择更新模式 | ClipboardSelectionUpdateMode | DWORD | 剪贴板 | 3 |
| 主选定内容更新模式 | PrimarySelectionUpdateMode | DWORD | 剪贴板 | 1 |
| 最高 **speex** 质量 | MaxSpeexQuality | DWORD | 音频 | 5 |

| Studio 策略 | 注册表项名称 | 类型 | 模块 | 默认值 |
|---|---|---|---|---|
| 自动连接客户端驱动器 | AutoConnectDrives | DWORD | 文件重定向/CDM | 已启用 (1) |
| 客户端光盘驱动器 | AllowCdromDrives | DWORD | 文件重定向/CDM | 允许 (1) |
| 客户端固定驱动器 | AllowFixedDrives | DWORD | 文件重定向/CDM | 允许 (1) |
| 客户端软盘驱动器 | AllowFloppyDrives | DWORD | 文件重定向/CDM | 允许 (1) |
| 客户端网络驱动器 | AllowNetworkDrives | DWORD | 文件重定向/CDM | 允许 (1) |
| 客户端驱动器重定向 | AllowDriveRedir | DWORD | 文件重定向/CDM | 允许 (1) |
| 只读客户端驱动器访问 | ReadOnlyMappedDrive | DWORD | 文件重定向/CDM | 已禁用 (0) |
| 自动显示键盘 | AllowAutoKeyboardPopup | DWORD | VDA | 已禁用 (0) |
| 允许在桌面与客户端之间传输文件 | AllowFileTransfer | DWORD | 文件传输 | 允许 |
| 从桌面下载文件 | AllowFileDownload | DWORD | 文件传输 | 允许 |

| Studio 策略 | 注册表项名称 | 类型 | 模块 | 默认值 |
| --- | --- | --- | --- | --- |
| 将文件上载到桌面 | AllowFileUpload | Int | 文件传输 | 允许 |
| 会话空闲计时器 | EnableSessionIdleTimer | Int | 会话计时器 | 已启用 (1) |
| 会话空闲计时器间隔 | SessionIdleTimerInterval | Int | 会话计时器 | 1440 分钟 |
| 断开会话计时器 | EnableSessionDisconnectTimer | Int | 会话计时器 | 已禁用 (0) |
| 断开会话计时器间隔 | SessionDisconnectTimerPeriod | Int | 会话计时器 | 1440 分钟 |

> 注意：
>
> 只有 Windows Virtual Delivery Agent (VDA) 支持通过用户数据报协议 (UDP) 传输音频。Linux VDA 不支持。有关详细信息，请参阅通过用户数据报协议 (UDP) 实时传输音频。

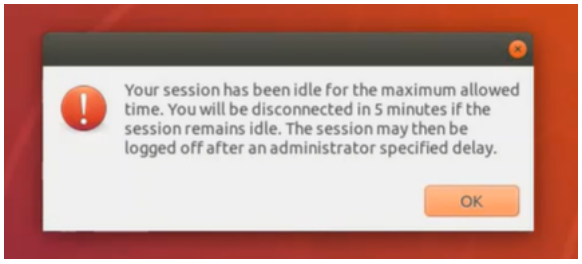
可以使用以下 Citrix 策略设置在 Citrix Studio 中配置会话连接计时器：

- 会话空闲计时器：确定是否对空闲会话强制实施时间限制。
- 会话空闲计时器时隔：设置空闲会话的时间限制。如果会话空闲计时器设置为已启用，并且活动会话在设置的时间内未收到用户输入，会话将断开连接。
- 断开连接的会话计时器：确定是否对断开连接的会话强制实施时间限制。
- 断开连接的会话计时器间隔：设置断开连接的会话注销之前的时间间隔。

更新任何策略设置时，请确保这些设置在部署中保持一致。

空闲会话的时间限制到期时，将显示一条警告消息。有关示例，请参见以下屏幕截图：按确定关闭警告消息，但无法使会话保持活动状态。要使会话保持活动状态，请提供用户输入以重置空闲计时器。




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]

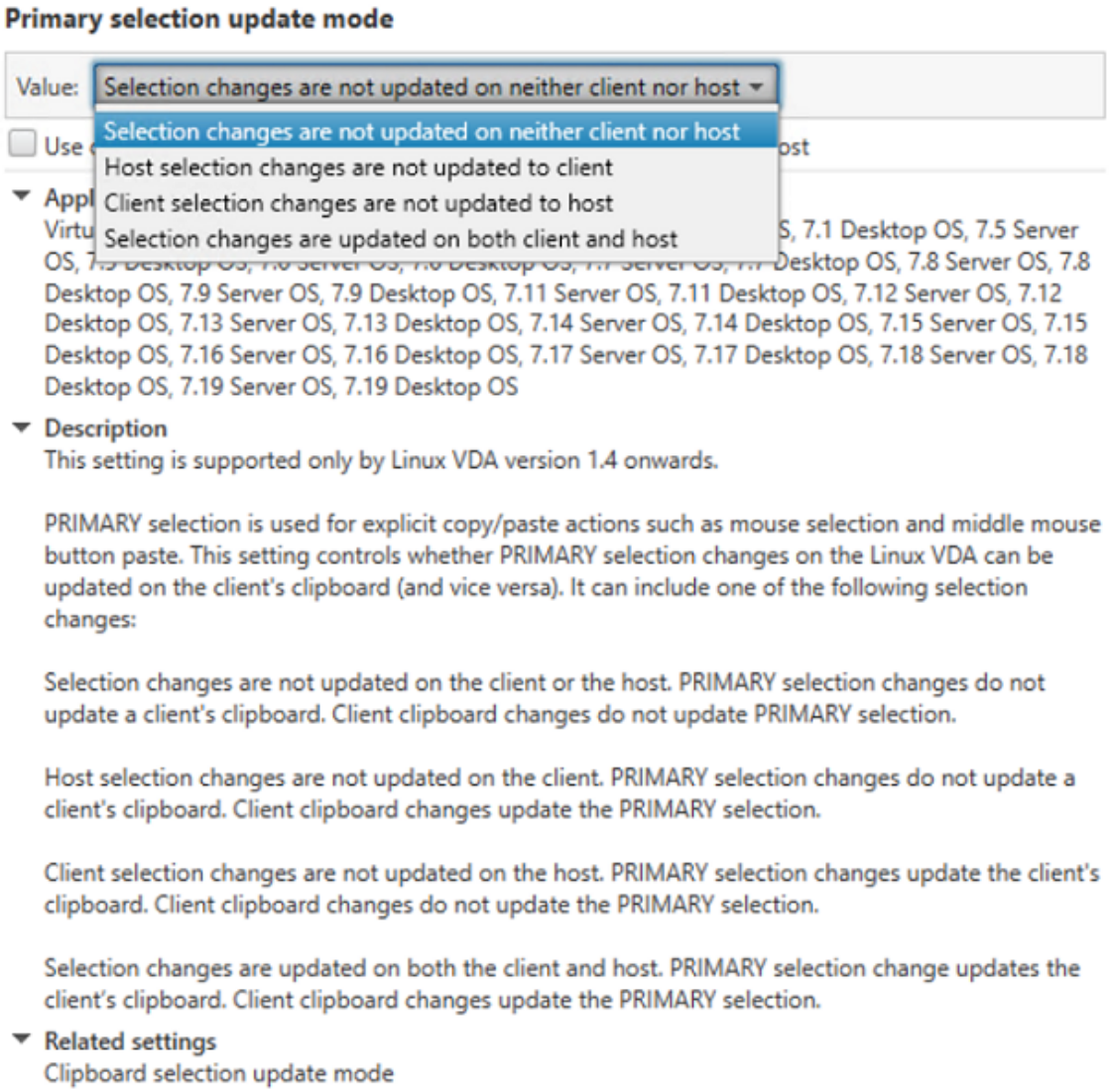
  默认值：3

  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：




- 选定内容变更既不在客户端上也不在主机上更新

  Linux VDA 上的主选定内容变更不更新客户端上的剪贴板。客户端上的主选定内容变更不更新 Linux VDA 上的剪贴板。

- 主机选定内容变更不更新到客户端

  Linux VDA 上的主选定内容变更不更新客户端上的剪贴板。客户端上的主选定内容变更更新 Linux VDA 上的剪贴板。

- 客户端选定内容变更不更新到主机

  Linux VDA 上的主选定内容变更更新客户端上的剪贴板。客户端上的主选定内容变更不更新 Linux VDA 上的剪贴板。

- 选定内容变更同时在客户端和主机上更新

  Linux VDA 上的主选定内容变更更新客户端上的剪贴板。客户端上的主选定内容变更更新 Linux VDA 上的剪贴板。此选项为默认值。

相关设置：剪贴板选定内容更新模式

- ClipboardSelectionUpdateMode

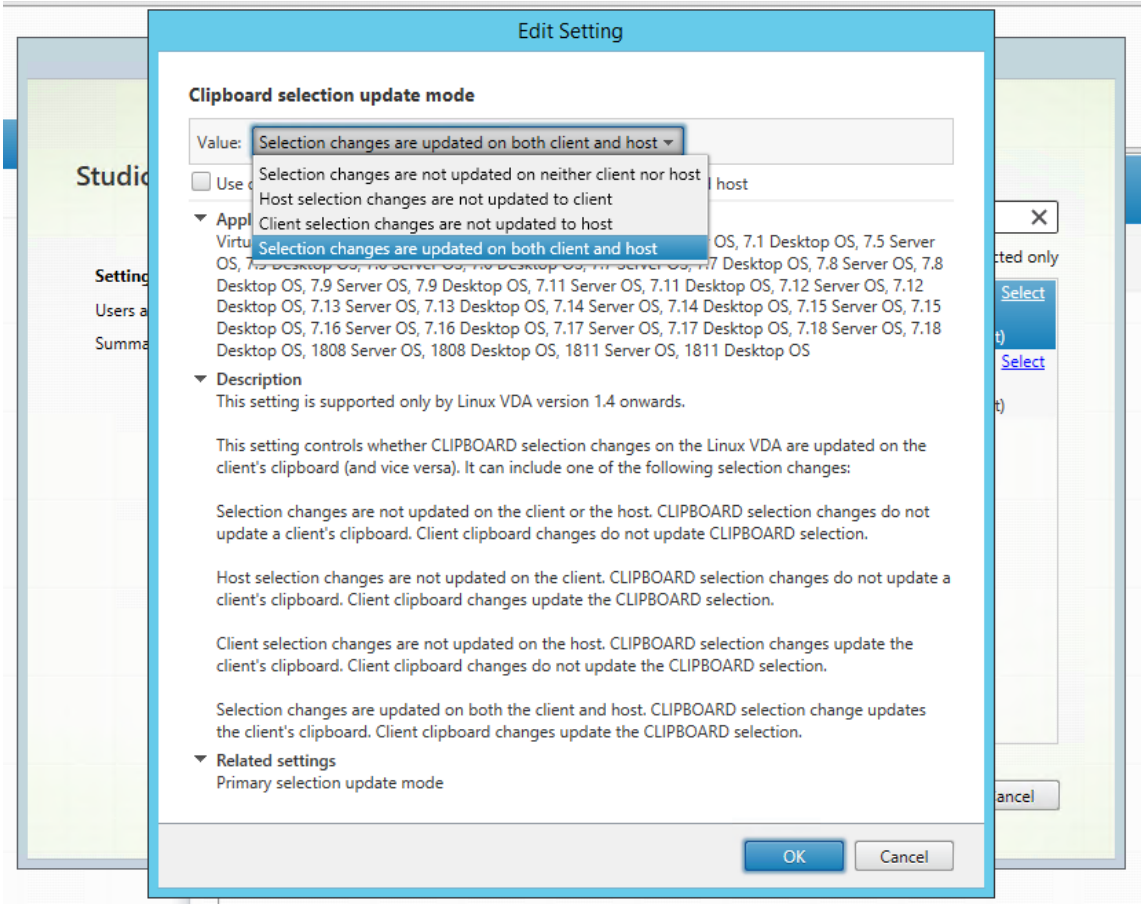
值（枚举）：[0, 1, 2, 3]

默认值：3

详细信息：

当您选择某些数据并明确请求将其“复制”到剪贴板时使用剪贴板选定内容，例如通过从快捷菜单中选择“复制”。剪贴板选定内容主要用于 Microsoft Windows 剪贴板操作，而主选定内容对 Linux 而言是唯一的。

此策略控制 Linux VDA 和客户端上的剪贴板选定内容变更是否可以在对方的剪贴板上更新。有四个值选项：




  - 选定内容变更既不在客户端上也不在主机上更新

    Linux VDA 上的剪贴板选定内容变更不更新客户端上的剪贴板。客户端上的剪贴板选定内容变更不更新 Linux VDA 上的剪贴板。

  - 主机选定内容变更不更新到客户端

    Linux VDA 上的剪贴板选定内容变更不更新客户端上的剪贴板。客户端上的剪贴板选定内容变更更新 Linux VDA 上的剪贴板。

  - 客户端选定内容变更不更新到主机

Linux VDA 上的剪贴板选定内容变更更新客户端上的剪贴板。客户端上的剪贴板选定内容变更不更新 Linux VDA 上的剪贴板。

- 选定内容变更同时在客户端和主机上更新
  Linux VDA 上的剪贴板选定内容变更更新客户端上的剪贴板。客户端上的剪贴板选定内容变更更新 Linux VDA 上的剪贴板。此选项为默认值。

相关设置：主选定内容更新模式

> 注意：
>
> Linux VDA 支持剪贴板选定内容和主选定内容。要控制 Linux VDA 与客户端之间的复制和粘贴行为，我们建议您同时将剪贴板选定内容更新模式和主选定内容更新模式设置为相同的值。

## 打印

October 31, 2022

本部分内容包含以下主题：

- 打印最佳做法
- PDF 打印

## 打印最佳做法

November 4, 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：

```
sudo yum  -y install cups

sudo yum -y install foomatic-filters
<!--NeedCopy-->
```

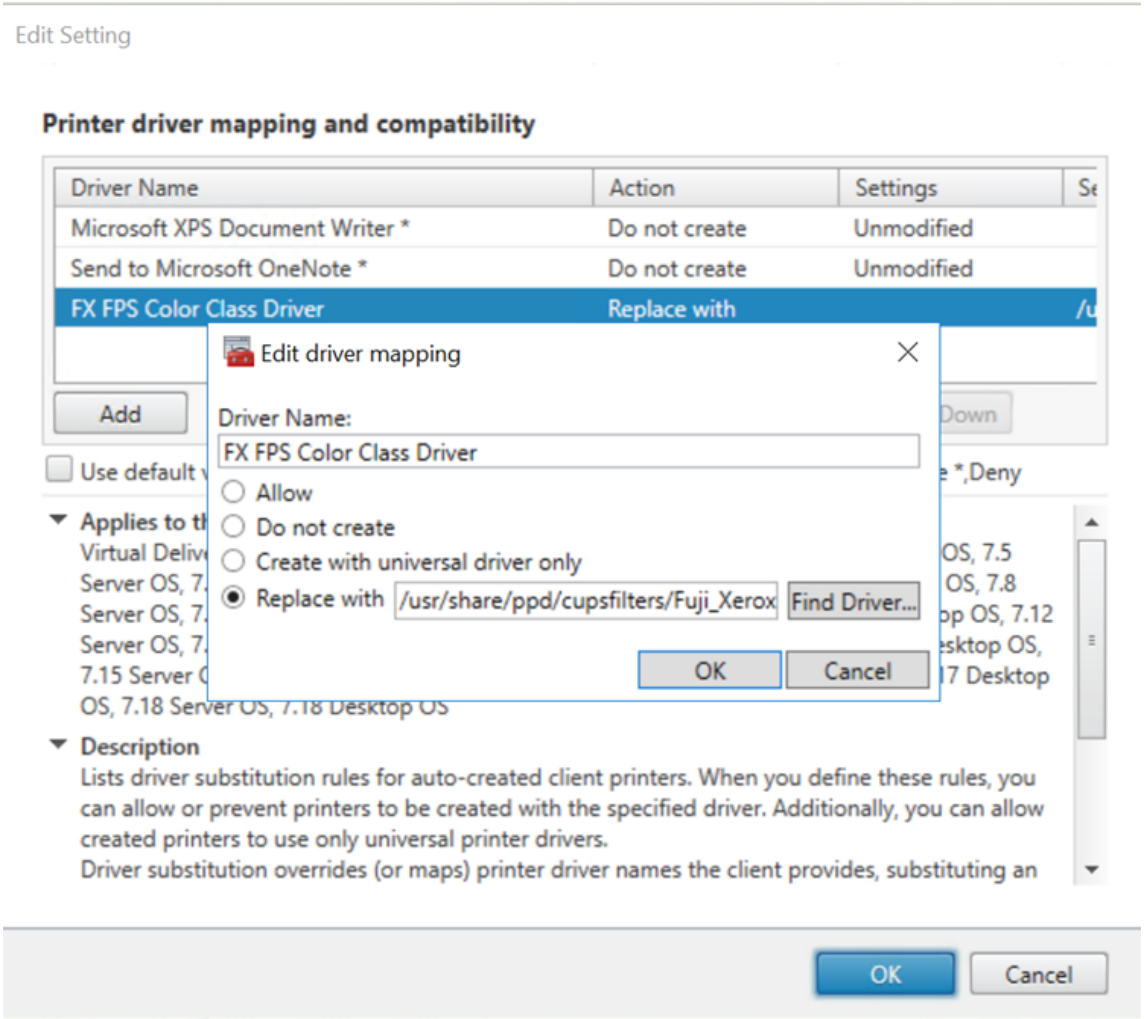
 

配置

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 ~/.CtxlpProfile$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 ctxcups 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：

```
sudo service cups stop

sudo vi /etc/systemd/system/printer.target.wants/cups.service

PrivateTmp=false

sudo service cups start

sudo systemctl daemon-reload
<!--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。

```
[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=
<!--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：

  ```
  lpinfo  -m

  …

  xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

  xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
  xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

  ```

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

然后可以设置型号以与打印机匹配：

```
model=xerox/ph3115.ppd.gz
<!--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：

  ```
  ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
  <!--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：

  ```
  drivertype=pcl5
  <!--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：

   ```
   deletespoolfile=no
   <!--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：

   ```
   localhost:631
   <!--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：

```
<Policy default>

     # Job/subscription privacy...

     JobPrivateAccess default

     JobPrivateValues default

     SubscriptionPrivateAccess default

     SubscriptionPrivateValues default

     … …

     <Limit Create-Printer-Subscription>

          Require user @OWNER

          Order deny,allow

     </Limit>

     <Limit All>

          Order deny,allow

     </Limit>

</Policy>
<!--NeedCopy-->
```

## PDF 打印

October 31, 2022

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。

## Remote PC Access

November 4, 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 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。

### 注意事项

这些注意事项是 Linux VDA 特有的：

- 在物理机上，请仅在非 3D 模式下使用 Linux VDA。由于 NVIDIA 驱动程序的限制，启用了 HDX 3D 模式时，PC 的本地屏幕无法停止。显示此屏幕存在潜在的安全风险。
- 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。

- 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。客户端上的 Citrix Workspace 应用程序可以帮助用户在 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。

## 配置

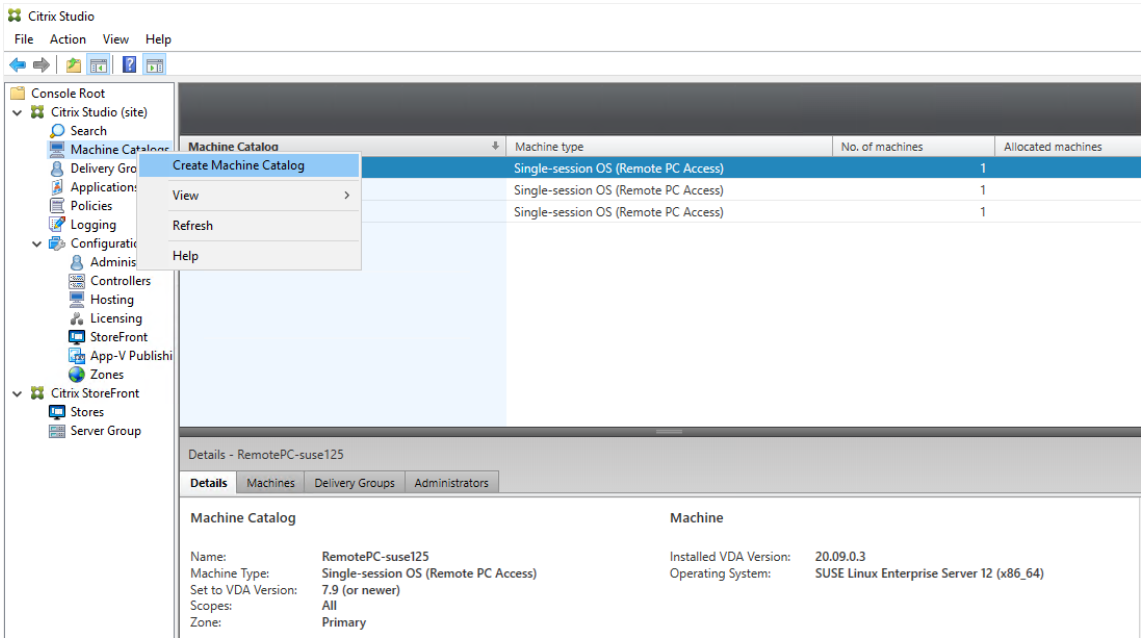
要交付 Linux PC 会话，请在目标 PC 上安装 Linux VDA，创建 **Remote PC Access** 类型的计算机目录，然后创建交付组，以使计算机目录中的 PC 可供请求访问的用户使用。以下部分详细介绍了该过程：

### 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`。

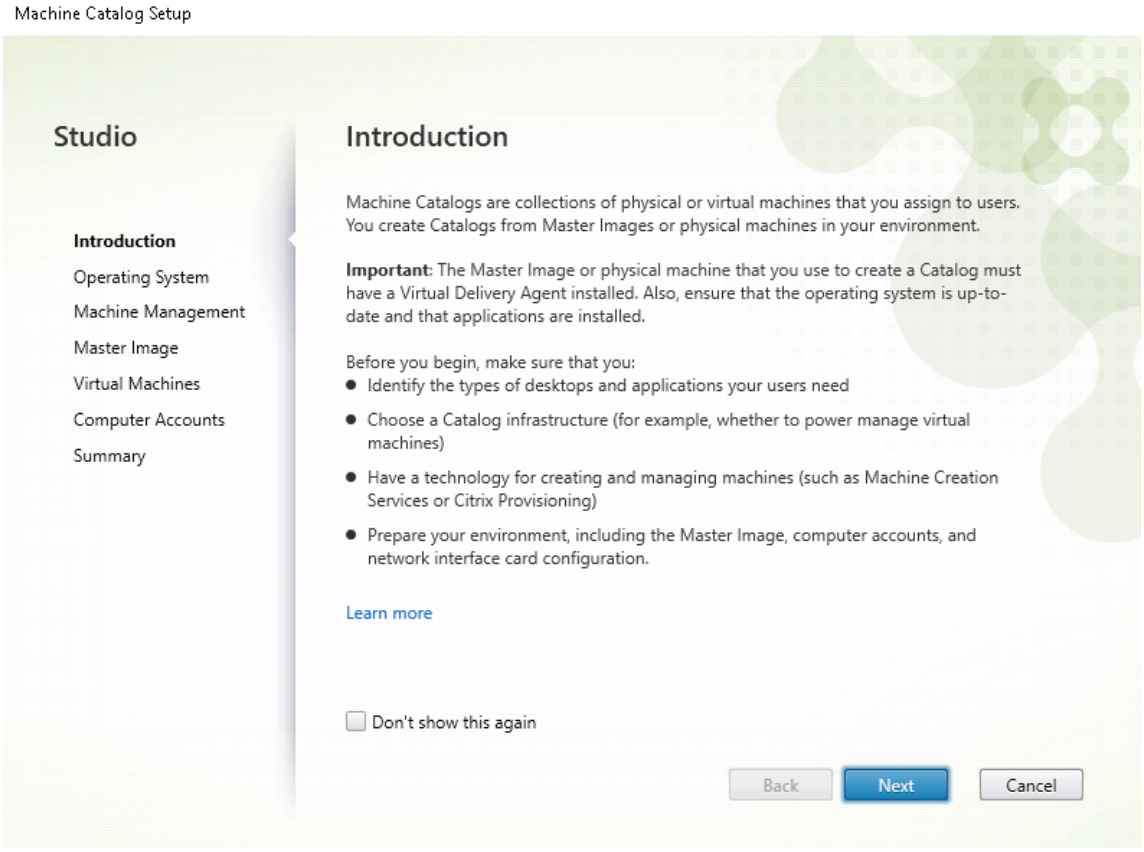
### 步骤 **2 -** 创建 **Remote PC Access** 类型的计算机目录

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。



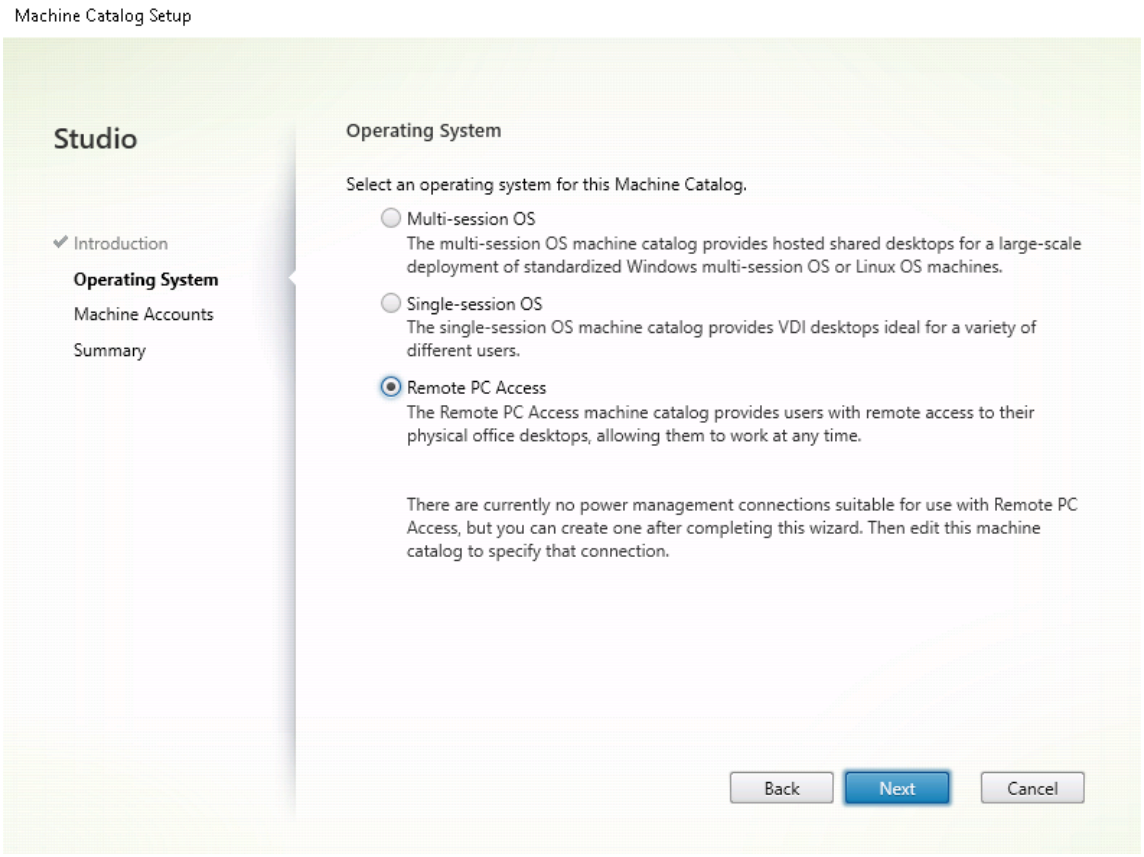

2. 单击简介页面上的下一步。



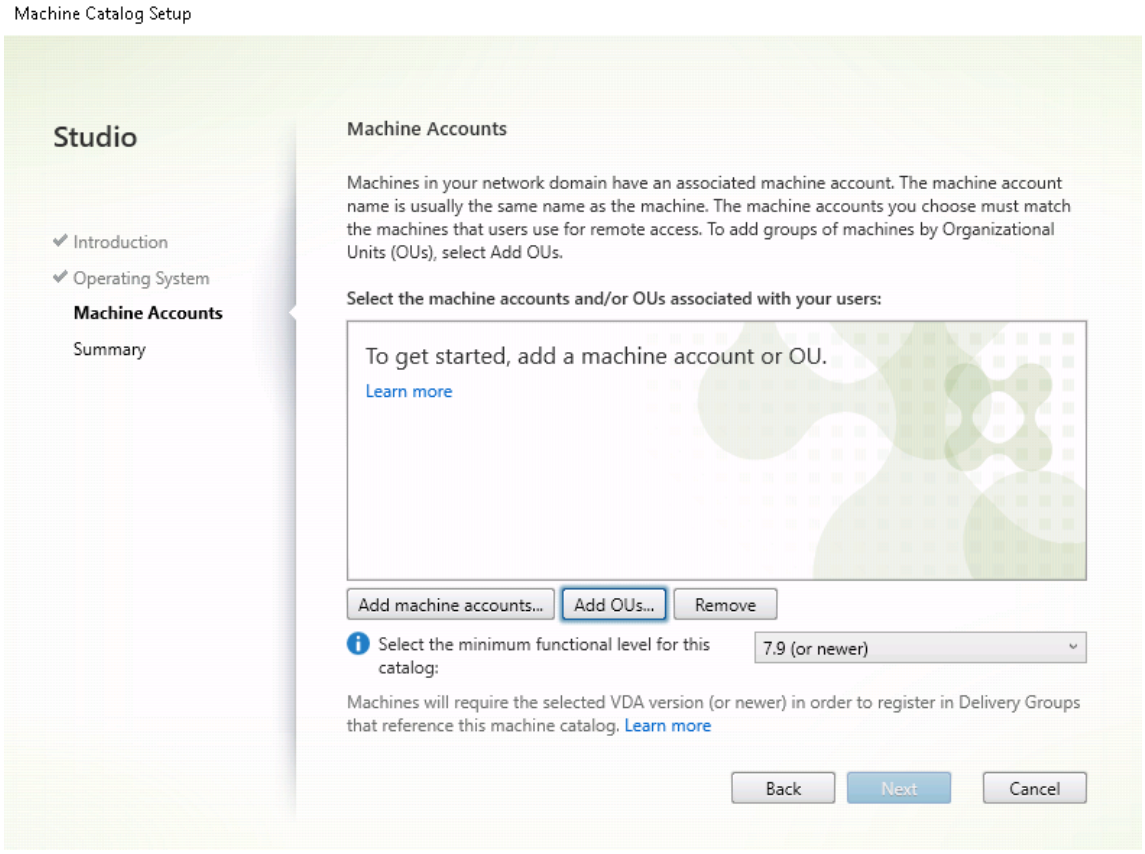

3. 在操作系统页面上选择 **Remote PC Access**。



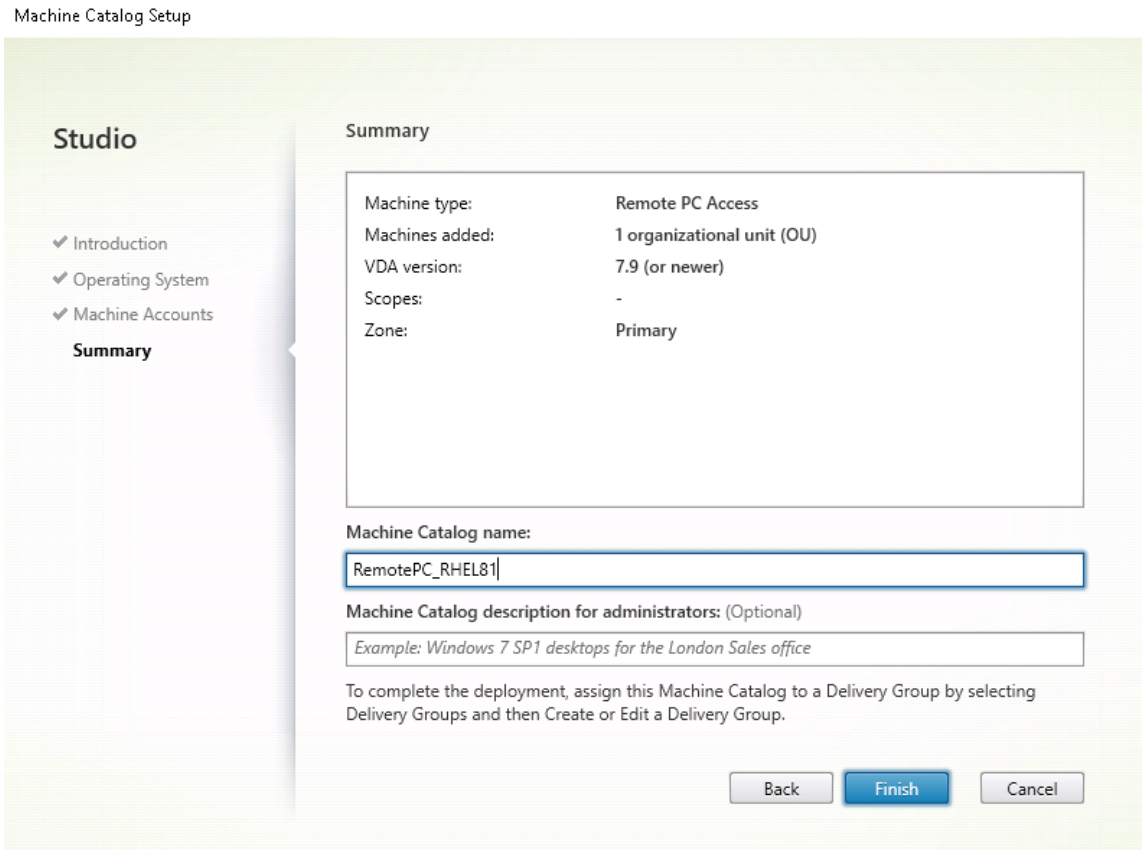

4. 单击添加 **OU** 以选择包含目标 PC 的 OU，或者单击添加计算机帐户将单个计算机添加到计算机目录中。

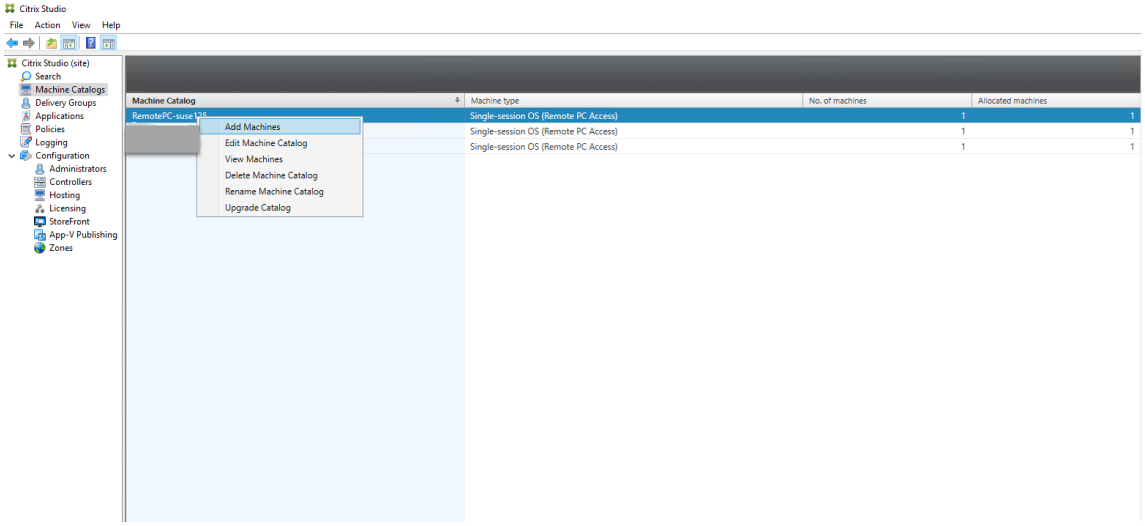



5. 命名计算机目录。



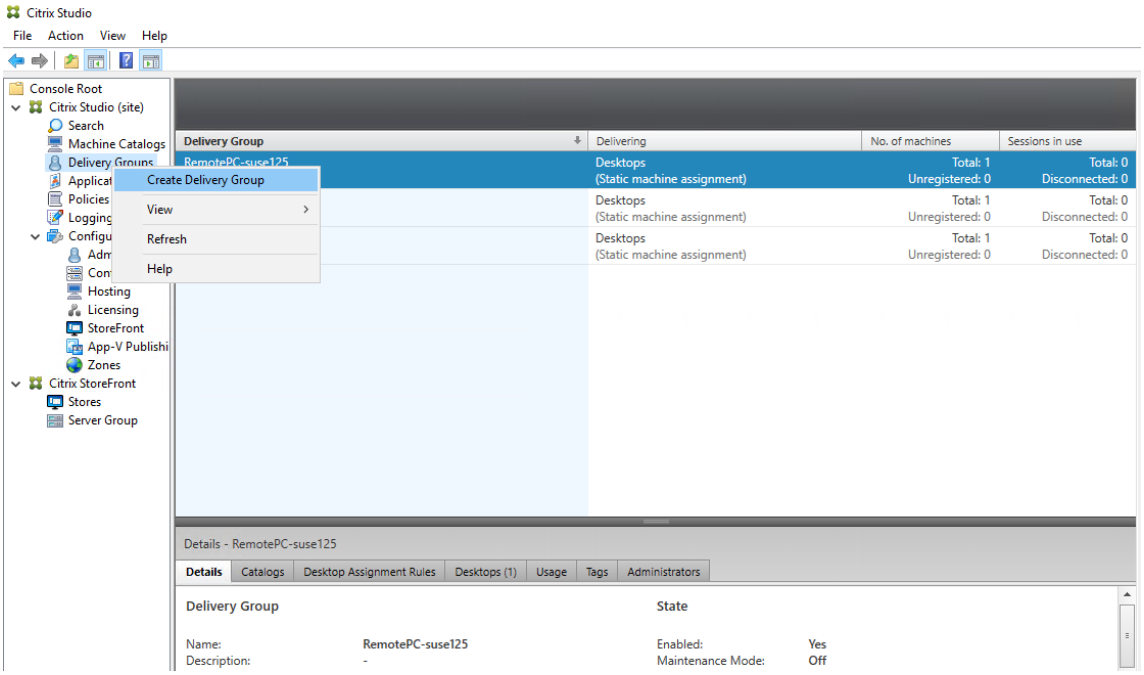

6.（可选）右键单击计算机目录以执行相关操作。



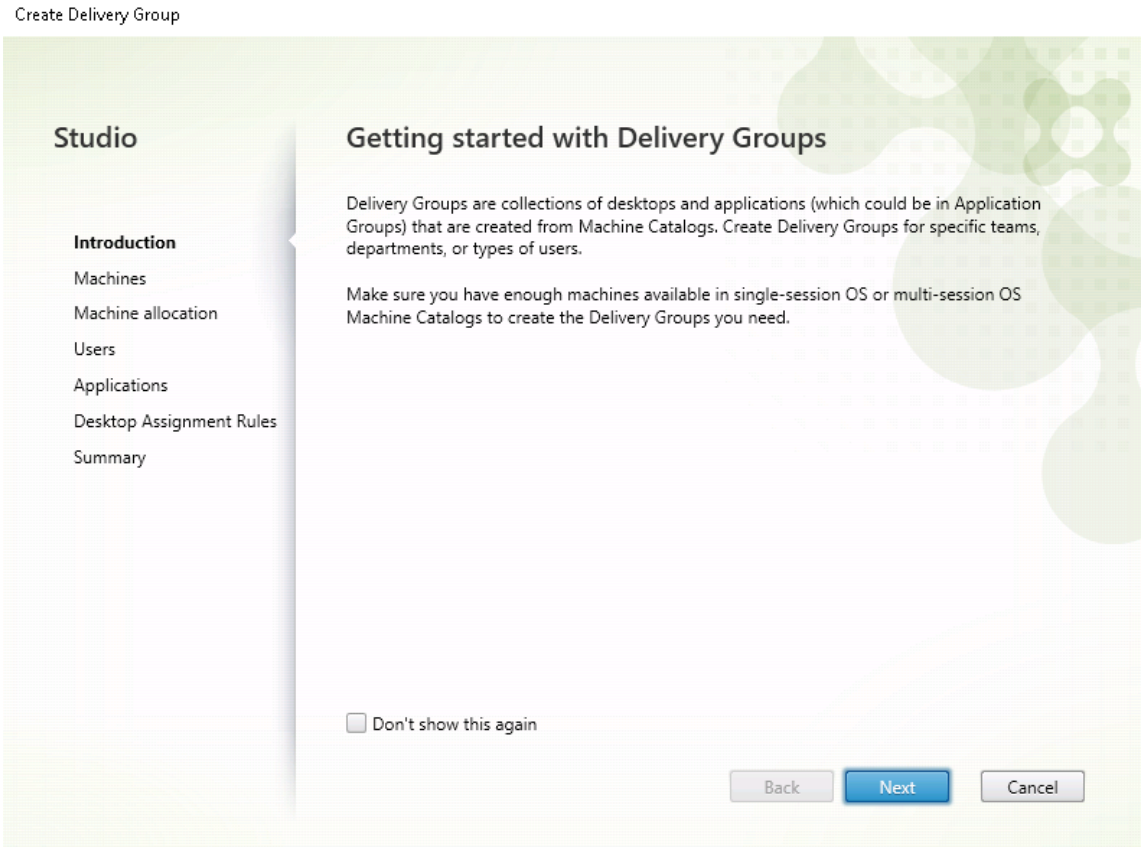

步骤 **3 -** 创建交付组，以使计算机目录中的 **PC** 可供请求访问权限的用户使用

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。

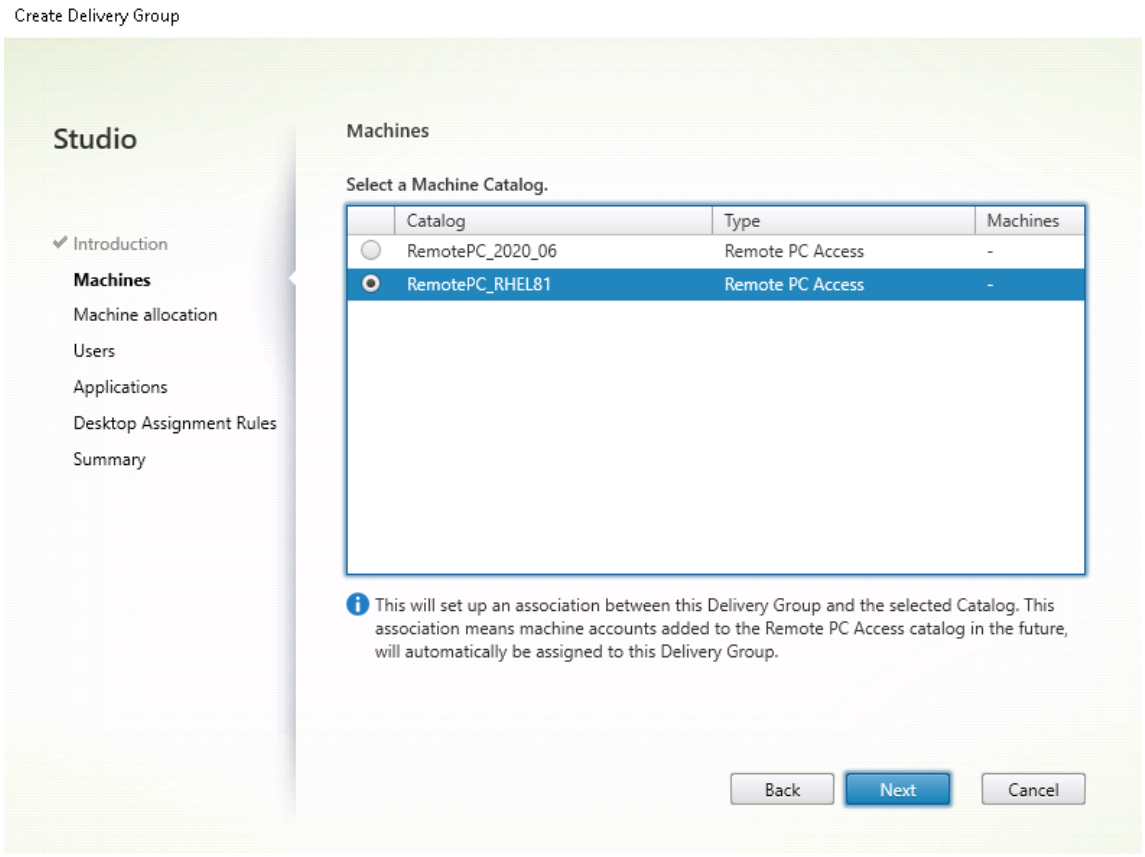



2. 单击交付组入门页面上的下一步。



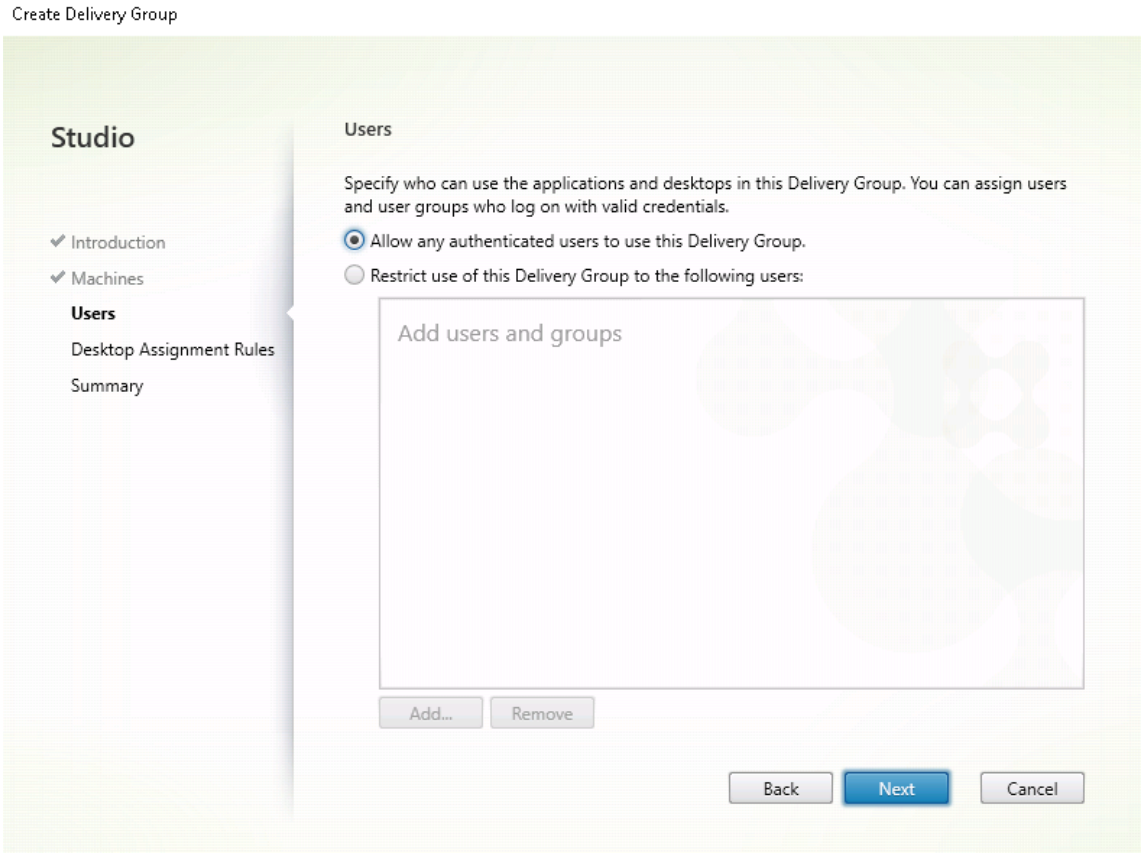

3. 选择在步骤 2 中创建的计算机目录，以将其与交付组关联。




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。




局域网唤醒

Remote PC Access 支持局域网唤醒功能，用户可以使用此功能远程开启物理 PC。借助此功能，用户可以在办公室 PC 不使用时将其关闭，以节约能源成本。用户还可以在计算机意外关闭时进行远程访问。

借助局域网唤醒功能，幻数据包会在 Delivery Controller 指示时直接从 PC 上运行的 VDA 发送到 PC 所在的子网。这允许此功能在不依赖额外的基础结构组件或第三方解决方案的情况下运行，以便传送幻数据包。

局域网唤醒功能不同于传统的基于 SCCM 的局域网唤醒功能。有关基于 SCCM 的局域网唤醒的信息，请参阅 局域网唤醒–SCCM 集成。

系统要求

下面是使用局域网唤醒功能的系统要求：

- 控制平面：
  - Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）
  - Citrix Virtual Apps and Desktops 2012 或更高版本
- 物理 PC：

- VDA 版本 2012 或更高版本
- 在 BIOS 中和 NIC 上启用了局域网唤醒

### 配置局域网唤醒

目前，仅在使用 PowerShell 时支持集成的局域网唤醒的配置。

要配置局域网唤醒，请执行以下操作：

1. 如果您还没有 Remote PC Access 计算机目录，请创建一个目录。
2. 如果您还没有局域网唤醒主机连接，请创建一个连接。

   > 注意：
   >
   > 要使用局域网唤醒功能，如果您具有“Microsoft 配置管理器局域网唤醒”类型的主机连接，请创建一个主机连接。

3. 检索局域网唤醒主机连接的唯一标识符。
4. 将局域网唤醒主机连接与计算机目录相关联。

   要创建局域网唤醒主机连接，请执行以下操作：

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "\*citrix\*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
            -Name $connectionName `
            -HypervisorAddress "N/A" `
            -UserName "woluser" `
            -Password "wolpwd" `
            -ConnectionType Custom `
            -PluginId VdaWOLMachineManagerFactory `
            -CustomProperties "<CustomProperties></
               CustomProperties>" `
            -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
   $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -
       HypHypervisorConnectionUid $hypHc.HypervisorConnectionUid
```

```
 }

<!--NeedCopy-->
```

主机连接准备就绪后，运行以下命令以检索主机连接的唯一标识符：

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>
    "
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

检索连接的唯一标识符后，运行以下命令以将连接与 Remote PC Access 计算机目录相关联：

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
    RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

5. 在计算机目录中的每台 VM 上的 BIOS 中和 NIC 上启用局域网唤醒。

   注意：启用局域网唤醒的方法因计算机配置的不同而异。

   - 要在 BIOS 中启用局域网唤醒，请执行以下操作：
     a) 进入 BIOS 并启用局域网唤醒功能。
        访问 BIOS 的方法取决于主板的制造商和制造商选择的 BIOS 供应商。
     b) 保存您的设置并重新启动计算机。
   - 要在 NIC 上启用局域网唤醒，请执行以下操作：
     a) 运行 `sudo ethtool <NIC>` 命令以检查您的 NIC 是否支持幻数据包。
        `<NIC>` 是您的 NIC 的设备名称，例如 `eth0`。`sudo ethtool <NIC>` 命令提供有关 NIC 功能的输出：
        - 如果输出中包含一个类似于 `Supports Wake-on: <letters>` 的行（其中 `<letters>` 包含字母 `g`），您的 NIC 将支持局域网唤醒幻数据包方法。
        - 如果输出中包含一个类似于 `Wake-on: <letters>` 的行（其中 `<letters>` 包含字母 `g`，但不包含字母 `d`），则局域网唤醒幻数据报方法已启用。但是，如果 `<letters>` 包含字母 `d`，则表示局域网唤醒功能已禁用。在这种情况下，请通过运行 `sudo ethtool -s <NIC> wol g` 命令启用局域网唤醒。

     b) 在大多数发行版中，每次启动后都需要运行 `sudo ethtool -s <NIC> wol g` 命令。要永久设置此选项，请根据您的发行版完成以下步骤：

        **Ubuntu**:

        将 `up ethtool -s <NIC> wol g` 行添加到接口配置文件 `/etc/network/interfaces` 中。例如：

        ```
        # ifupdown has been replaced by netplan(5) on this system.
            See
        # /etc/netplan for current configuration.
        # To re-enable ifupdown on this system, you can run:
        # sudo apt install ifupdown
        ```

```
auto eth0
iface eth0 inet static
           address 10.0.0.1
           netmask 255.255.240.0
           gateway 10.0.0.1
           up ethtool -s eth0 wol g
<!--NeedCopy-->
```

**RHEL/SUSE**:

将以下 ETHTOOL_OPTS 参数添加到接口配置文件 /etc/sysconfig/network-scripts/ifcfg-<NIC> 中:

```
ETHTOOL_OPTS="-s ${
 DEVICE }
  wol g"
<!--NeedCopy-->
```

设计注意事项

当您计划在 Remote PC Access 中使用局域网唤醒时，请注意以下事项：

- 多个计算机目录可以使用相同的局域网唤醒主机连接。
- 要使一台 PC 唤醒另一台 PC，两台 PC 必须位于同一子网中，并使用相同的局域网唤醒主机连接。这些 PC 是在相同还是不同的计算机目录中并不重要。
- 将主机连接分配给特定区域。如果您的部署中包含多个区域，则需要在每个区域中使用局域网唤醒主机连接。这同样适用于计算机目录。
- 幻数据包使用全局广播地址 255.255.255.255 进行广播。确保该地址未被阻止。
- 子网中必须至少打开一台 PC（对于每个局域网唤醒连接），才能唤醒该子网中的计算机。

操作注意事项

下面是使用局域网唤醒功能的注意事项：

- VDA 必须至少注册一次，才能使用集成的局域网唤醒功能唤醒 PC。
- 局域网唤醒功能只能用于唤醒 PC。该功能不支持其他电源操作，例如重新启动或关闭。
- 创建局域网唤醒连接后，该功能在 Studio 中可见。但是，不支持在 Studio 中编辑其属性。
- 幻数据包通过以下两种方式之一发送：
  - 当用户尝试启动到其 PC 的会话并且 VDA 未注册时
  - 当管理员从 Studio 或 PowerShell 手动发送打开电源命令时
- 由于 Delivery Controller 不知道 PC 的电源状态，因此，Studio 在电源状态下显示不支持。Delivery Controller 使用 VDA 注册状态来确定 PC 是打开还是关闭。

### 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。

## 会话

October 31, 2022

本部分内容包含以下主题：

- 自适应传输
- 使用临时主目录登录
- 发布应用程序
- 会话可靠性
- Rendezvous V1
- Rendezvous V2
- 使用 TLS 保护用户会话安全
- 使用 DTLS 保护用户会话安全

## 自适应传输

November 4, 2022

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。有关自适应传输的详细信息，请参阅自适应传输。

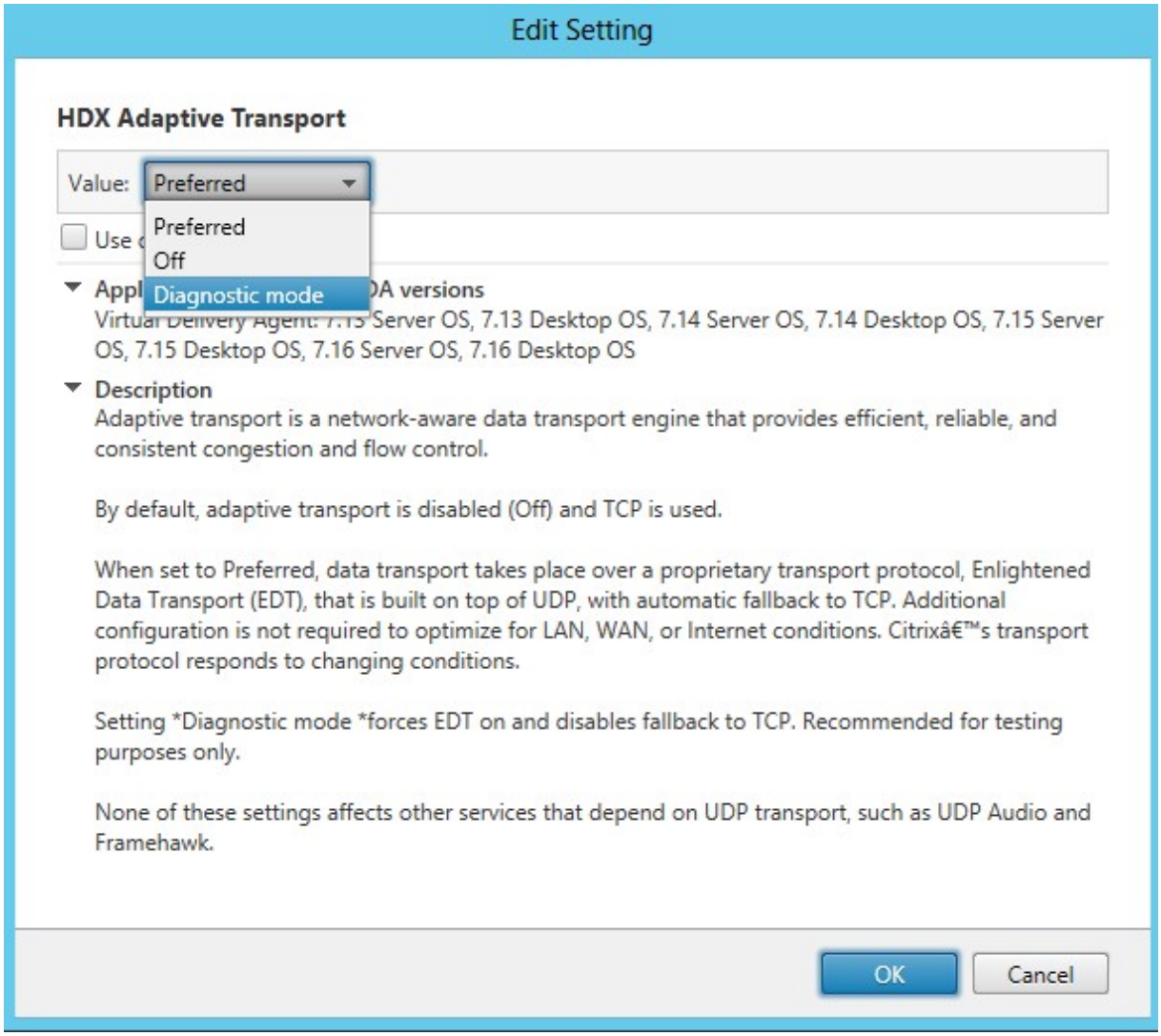
### 启用自适应传输

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。

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。

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

在正常情况下，输出类似于如下所示。

```
udp        0      0 0.0.0.0:2598            0.0.0.0:*

udp       0      0 :::1494                 :::*
<!--NeedCopy-->
```

### EDT MTU 发现

EDT 在建立会话时自动确定最大传输单位 (MTU)。这样做可以防止出现可能会导致性能下降或无法建立会话的 EDT 数据包碎片。

最低要求：

- Linux VDA 2012
- 适用于 Windows 的 Citrix Workspace 应用程序 1911
- Citrix ADC：
  - 13.0.52.24
  - 12.1.56.22
- 必须启用会话可靠性

如果使用的客户端平台或版本不支持此功能，则可以配置适合您环境的自定义 EDT MTU。有关详细信息，请参阅知识中心文章 CTX231821。

> 警告：
>
> 注册表编辑不当会导致严重问题，可能导致需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

#### 在 VDA 上启用或禁用 EDT MTU 发现

默认情况下，EDT MTU 发现处于禁用状态。

- 要启用 EDT MTU 发现，请使用以下命令设置 `MtuDiscovery` 注册表项，重新启动 VDA，然后等待 VDA 注册：

  ```
  /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet
  \Control\Terminal Server\Wds\icawd"-t "REG_DWORD"-v "MtuDiscovery
  "-d "0x00000001"--force
  ```

- 要禁用 EDT MTU 发现，请删除 `MtuDiscovery` 注册表值。

控制客户端上的 **EDT MTU** 发现

可以通过在 ICA 文件中添加 `MtuDiscovery` 参数，在客户端上有选择地控制 EDT MTU 发现。要禁用此功能，请在 `Application` 部分下设置以下策略：

```
MtuDiscovery=Off
```

要重新启用此功能，请从 ICA 文件中删除 `MtuDiscovery` 参数。

> 重要：
>
> 要使此 ICA 文件参数起作用，请在 VDA 上启用 EDT MTU 发现。如果未在 VDA 上启用 EDT MTU 发现，则 ICA 文件参数无效。

## 会话登录屏幕上的自定义背景和横幅消息

October 31, 2022

可以使用以下命令将自定义背景消息或横幅消息添加到会话登录屏幕。要向会话登录屏幕添加背景消息和横幅消息，可以将横幅消息嵌入到背景图像中。

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
      "LogonDisplayString" -d "<text of custom logon banner message>" --
     force
2 <!--NeedCopy-->
```

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
      "BackgroundImagePath" -d "<path to your custom logon screen
     background image>" --force
2 <!--NeedCopy-->
```

要在 SUSE 15.3 上使用该功能，请从 http://download.opensuse.org/distribution/leap/15.3/repo/oss/ 安装 `imlib2`。

> 提示：
>
> 如果使用 LogonDisplayString 添加自定义横幅消息，则默认情况下，登录屏幕背景为蓝色。

## 按会话用户划分的自定义桌面环境

October 31, 2022

可以使用 **CTX_XDL_DESKTOP_ENVIRONMENT** 变量为会话用户指定桌面环境。自 2209 版起，会话用户可以自定义自己的桌面环境。必须提前在 VDA 上安装桌面环境，才能启用此功能。

下表显示了支持按会话用户划分的自定义桌面环境的 Linux 发行版和桌面环境的列表。

| Linux 发行版 | 支持的桌面 |
| --- | --- |
| Debian11.3、Debian 10.9 | MATE、GNOME、GNOME-Classic、KDE |
| RHEL 8.6、RHEL 8.4 | MATE、GNOME、GNOME-Classic |
| RHEL 7.9 | MATE、GNOME、GNOME-Classic、KDE |
| Rocky Linux 8.6 | MATE、GNOME、GNOME-Classic、KDE |
| SUSE 15.3 | MATE、GNOME、GNOME-Classic |
| Ubuntu 22.04、Ubuntu 20.04、Ubuntu 18.04 | MATE、GNOME、GNOME-Classic、KDE |

桌面切换命令

要切换到目标桌面环境，请在会话中运行相应的命令：

| 如果目标桌面环境为： | 运行以下命令： |
| --- | --- |
| GNOME | `/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME` |
| GNOME Classic | `/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME-CLASSIC` |
| MATE | `/opt/Citrix/VDA/bin/ctxdesktopswitch.sh MATE` |
| KDE | `/opt/Citrix/VDA/bin/ctxdesktopswitch.sh KDE` |

**KDE** 提示

- Magnus 可能会在 KDE 中启动时加载。作为解决方法，您可以通过运行 `sudo apt remove magnus` 来删除 Magnus 软件包。
- 要禁用 KDE 启动期间出现的 QT 警告，请以 root 用户身份通过添加以下条目来编辑 `/usr/share/qt5/qtlogging.ini`：

```
1  qt.qpa.xcb.xcberror.error=false
```

```
qt.qpa.xcb.warning=false
qt.qpa.xcb.error=false
<!--NeedCopy-->
```

- KDE 的屏幕解锁可能会失败。作为解决方法，我们建议您禁用桌面的自动锁定功能。

## 使用临时主目录登录

October 31, 2022

在 Linux VDA 上的装载点出现故障的情况下，可以指定临时主目录。如果指定了临时主目录，则将在会话登录期间装载点失败时显示一条提示。用户数据之后将存储在临时主目录下。

下表介绍了有助于设置您的主目录的注册表项。

| 注册表项 | 说明 | 命令 |
| --- | --- | --- |
| LogNoHome | 控制用户是否可以在没有主目录的情况下登录会话。默认值为 1，表示是。如果将该值设置为 0，则将禁用不适用主目录的会话登录。 | `create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "LogNoHome"-d "0x00000001"--force` |
| HomeMountPoint | 在 Linux VDA 上设置本地装载点。例如，如果 /mnt/home 是装载点，则用户的主目录为 /mnt/home/domain/<user_name>。确保装载点与您的环境中的用户主目录相同。 | `create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "HomeMountPoint"-d "<A directory where the NFS share is to be mounted>"--force` |

| 注册表项 | 说明 | 命令 |
| --- | --- | --- |
| TempHomeDirectoryPath | 在 Linux VDA 上设置临时主目录，以防装载点出现故障。默认值为 /tmp。注册表项取决于 HomeMountPoint。仅当系统检测到装载点不可用时才会生效。用户的临时主目录为 /tmp/domain/user_id。 | create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "TempHomeDirectoryPath"-d "</tmp by default>"--force |
| RemoveHomeOnLogoff | 控制是否在用户注销时删除临时主目录。1 表示是。0 表示否。 | create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "RemoveHomeOnLogoff"-d "0x00000000"--force |

## 发布应用程序

October 31, 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）。

> 注意：
>
> - 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。

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

在应用程序会话中，只有特定于应用程序的快捷方式才能按预期运行。

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。
- 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。

## Rendezvous V1

November 4, 2022

使用 Citrix Gateway 服务时，Rendezvous 协议允许流量绕过 Citrix Cloud Connector，以直接安全地连接到 Citrix Cloud 控制平面。

有两种类型的流量需要考虑：1) 控制 VDA 注册和会话代理的流量；2) HDX 会话流量。

Rendezvous V1 允许 HDX 会话流量绕过 Cloud Connector，但它仍要求 Cloud Connector 代理所有控制流量以进行 VDA 注册和会话代理。

要求

- 使用 Citrix Workspace 和 Citrix Gateway 服务访问环境。
- 控制平面：Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）

- Linux VDA 版本 2112 或更高版本。
  - 版本 2112 是非透明 HTTP 代理所需的最低版本。
  - 版本 2204 是透明代理和 SOCKS5 代理所需的最低版本。
- 在 Citrix 策略中启用 Rendezvous 协议。有关详细信息，请参阅 Rendezvous 协议策略设置。
- VDA 必须对 `https://*.nssvc.net` 具有访问权限，包括所有子域。如果您无法通过该方式将所有子域列入白名单，请改为使用 `https://*.c.nssvc.net` 和 `https://*.g.nssvc.net`。有关详细信息，请参阅 Citrix Cloud 文档（在 Virtual Apps and Desktops 服务下方）的 Internet 连接要求部分和知识中心文章 CTX270584。
- 在代理会话时，Cloud Connector 必须获取 VDA 的 FQDN。要实现此目标，请为站点启用 DNS 解析：使用 Citrix DaaS 远程 PowerShell SDK，运行命令 `Set-BrokerSite -DnsResolutionEnabled $true`。有关 Citrix DaaS 远程 PowerShell SDK 的详细信息，请参阅 SDK 和 API。

### 代理配置

VDA 支持通过 HTTP 和 SOCKS5 代理建立 Rendezvous 连接。

#### 代理注意事项

在 Rendezvous 中使用代理时，请注意以下事项：

- 支持非透明 HTTP 代理和 SOCKS5 代理。
- 不支持数据包解密和检查。配置异常，以便 VDA 与网关服务之间的 ICA 流量不会被拦截、解密或检查。否则，连接会中断。
- HTTP 代理通过使用协商和 Kerberos 身份验证协议支持基于计算机的身份验证。连接到代理服务器时，协商身份验证方案会自动选择 Kerberos 协议。Kerberos 是 Linux VDA 支持的唯一方案。

  > 注意：
  >
  > 要使用 Kerberos，必须为代理服务器创建服务主体名称 (SPN)，并将其与代理的 Active Directory 帐户关联。VDA 在建立会话时生成格式为 `HTTP/<proxyURL>` 的 SPN，其中代理 URL 是从 **Rendezvous** 代理策略设置中检索的。如果不创建 SPN，身份验证将失败。

- 当前不支持使用 SOCKS5 代理进行身份验证。如果使用 SOCKS5 代理，必须配置例外，以便发往网关服务地址的流量（在要求中指定）可以绕过身份验证。
- 只有 SOCKS5 代理支持通过 EDT 进行数据传输。对于 HTTP 代理，请使用 TCP 作为 ICA 的传输协议。

#### 透明代理

Rendezvous 支持透明 HTTP 代理。如果在网络中使用透明代理，则不需要在 VDA 上进行其他配置。

非透明代理

在网络中使用非透明代理时，请配置 Rendezvous 代理配置设置。启用该设置后，为 VDA 指定 HTTP 或 SOCKS5 代理地址，以了解要使用哪个代理。例如：

- 代理地址：`http://<URL or IP>:<port>` 或 `socks5://<URL or IP>:<port>`

### Rendezvous 验证

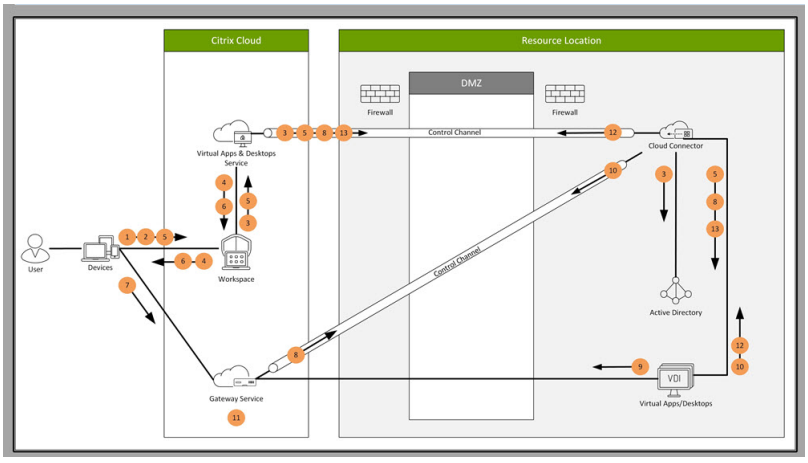
如果您满足所有要求，请按照下列步骤验证是否正在使用 Rendezvous：

1. 在 VDA 上启动端点。
2. 运行 `/opt/Citrix/VDA/bin/ctxquery -f iP`。
3. 传输协议指明连接类型：
    - TCP Rendezvous：TCP - TLS - CGP - ICA
    - EDT Rendezvous：UDP - DTLS - CGP - ICA
    - 通过 Cloud Connector 代理：TCP - PROXY - SSL - CGP - ICA 或 UDP - PROXY - DTLS - CGP - ICA

> 提示：
>
> 如果启用了 Rendezvous 时 VDA 无法直接访问 Citrix Gateway 服务，VDA 将回退到通过 Cloud Connector 代理 HDX 会话。

### Rendezvous 的工作原理

下图概述了 Rendezvous 连接流程。




请按照步骤了解流程。

1. 导航到 Citrix Workspace。
2. 在 Citrix Workspace 中输入凭据。

3. 如果使用本地 Active Directory，Citrix DaaS 将使用 Cloud Connector 通道通过 Active Directory 对凭据进行验证。
4. Citrix Workspace 显示 Citrix DaaS 中的枚举资源。
5. 从 Citrix Workspace 中选择资源。Citrix DaaS 向 VDA 发送一条消息，以便为传入会话做好准备。
6. Citrix Workspace 将 ICA 文件发送到包含 Citrix Cloud 生成的 STA 票证的端点。
7. 端点连接到 Citrix Gateway 服务，提供连接到 VDA 的票证，Citrix Cloud 将验证该票证。
8. Citrix Gateway 服务将连接信息发送到 Cloud Connector。Cloud Connector 确定连接是否为 Rendezvous 连接，并将信息发送到 VDA。
9. VDA 建立与 Citrix Gateway 服务的直接连接。
10. 如果无法在 VDA 与 Citrix Gateway 服务之间建立直接连接，VDA 将通过 Cloud Connector 代理其连接。
11. Citrix Gateway 服务在端点与 VDA 之间建立连接。
12. VDA 通过 Cloud Connector 借助 Citrix DaaS 验证其许可证。
13. Citrix DaaS 通过 Cloud Connector 向 VDA 发送会话策略。这些政策已应用。

## Rendezvous V2

November 4, 2022

使用 Citrix Gateway 服务时，Rendezvous 协议允许流量绕过 Citrix Cloud Connector，以直接安全地连接到 Citrix Cloud 控制平面。

有两种类型的流量需要考虑：1) 控制 VDA 注册和会话代理的流量；2) HDX 会话流量。

Rendezvous V1 允许 HDX 会话流量绕过 Cloud Connector，但它仍要求 Cloud Connector 代理所有控制流量以进行 VDA 注册和会话代理。

支持加入了标准 AD 域的计算机和未加入域的计算机将 Rendezvous V2 与单会话和多会话 Linux VDA 配合使用。对于未加入域的计算机，Rendezvous V2 允许 HDX 流量和控制流量绕过 Cloud Connector。

### 要求

使用 Rendezvous V2 的要求是：

- 使用 Citrix Workspace 和 Citrix Gateway 服务访问环境。
- 控制平面：Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）
- VDA 版本 2201 或更高版本。
  - 版本 2204 是 HTTP 和 SOCKS5 代理所需的最低版本。
- 在 Citrix 策略中启用 Rendezvous 协议。有关详细信息，请参阅 Rendezvous 协议策略设置。

- VDA 必须对 `https://*.nssvc.net` 具有访问权限，包括所有子域。如果您无法通过该方式将所有子域列入白名单，请改为使用 `https://*.c.nssvc.net` 和 `https://*.g.nssvc.net`。有关详细信息，请参阅 Citrix Cloud 文档（在 Virtual Apps and Desktops 服务下方）的 Internet 连接要求部分和知识中心文章 CTX270584。
- VDA 必须能够连接到上文提到的地址：
  - 在 TCP 443 上，用于 TCP Rendezvous。
  - 在 UDP 443 上，用于 EDT Rendezvous。

### 代理配置

使用 Rendezvous 时，VDA 支持通过代理连接控制流量和 HDX 会话流量。两种类型的流量的要求和注意事项不同，因此请仔细查看。

#### 控制流量代理注意事项

- 仅支持 HTTP 代理。
- 不支持数据包解密和检查。配置例外，以便 VDA 和 Citrix Cloud 控制平面之间的控制流量不会被拦截、解密或检查。否则，连接将失败。
- 不支持代理身份验证。
- 要为控制流量配置代理，请按如下方式编辑注册表：

```
1  /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
       VirtualDesktopAgent" -t "REG_SZ" -v "ProxySettings" -d "http
       ://<URL or IP>:<port>" --force
2  <!--NeedCopy-->
```

#### **HDX** 流量代理注意事项

- 支持 HTTP 和 SOCKS5 代理。
- EDT 只能与 SOCKS5 代理一起使用。
- 要为 HDX 流量配置代理，请使用 Rendezvous 代理配置策略设置。
- 不支持数据包解密和检查。配置例外，以便 VDA 和 Citrix Cloud 控制平面之间的 HDX 流量不会被拦截、解密或检查。否则，连接将失败。
- HTTP 代理通过使用协商和 Kerberos 身份验证协议支持基于计算机的身份验证。连接到代理服务器时，协商身份验证方案会自动选择 Kerberos 协议。Kerberos 是 Linux VDA 支持的唯一方案。

> 注意：
>
> 要使用 Kerberos，必须为代理服务器创建服务主体名称 (SPN)，并将其与代理的 Active Directory 帐户关联。VDA 在建立会话时生成格式为 HTTP/<proxyURL> 的 SPN，其中代理 URL 是从 **Rendezvous** 代理策略设置中检索的。如果不创建 SPN，身份验证将失败。

- 当前不支持使用 SOCKS5 代理进行身份验证。如果使用 SOCKS5 代理，必须配置例外，以便发往网关服务地址的流量（在要求中指定）可以绕过身份验证。
- 只有 SOCKS5 代理支持通过 EDT 进行数据传输。对于 HTTP 代理，请使用 TCP 作为 ICA 的传输协议。

透明代理

Rendezvous 支持透明 HTTP 代理。如果在网络中使用透明代理，则不需要在 VDA 上进行其他配置。

### 如何配置 **Rendezvous V2**

下面是在您的环境中配置 Rendezvous 的步骤：

1. 请确保满足所有要求。
2. 安装 VDA 后，运行以下命令以设置所需的注册表项：

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
   VirtualDesktopAgent" -t "REG_DWORD" -v "GctRegistration" -d "0
   x00000001" --force
<!--NeedCopy-->
```

3. 重新启动 VDA 计算机。
4. 创建 Citrix 策略或者编辑现有策略：
   - 将 Rendezvous 协议设置设为允许。
   - 请务必正确设置 Citrix 策略过滤器。该策略适用于需要启用 Rendezvous 的计算机。
   - 请确保 Citrix 策略具有正确的优先级，以免覆盖其他策略。

### **Rendezvous** 验证

要检查会话是否正在使用 Rendezvous 协议，请在终端中运行 /opt/Citrix/VDA/bin/ctxquery -fiP 命令。

显示的传输协议指明连接类型：

- TCP Rendezvous：TCP - TLS - CGP - ICA
- EDT Rendezvous：UDP - DTLS - CGP - ICA

- 通过 Cloud Connector 代理：TCP - PROXY - SSL - CGP - ICA 或 UDP - PROXY - DTLS - CGP - ICA

如果正在使用 Rendezvous V2，协议版本将显示 2.0。

> 提示：
>
> 如果启用了 Rendezvous 时 VDA 无法直接访问 Citrix Gateway 服务，VDA 将回退到通过 Cloud Connector 代理 HDX 会话。

## 使用 **DTLS** 保护用户会话安全

October 31, 2022

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 **/opt/Citrix/VDA/sbin** 上的 **enable_vdassl.sh** 工具启用（或禁用）SSL 加密。有关工具中可用的选项的信息，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**。

## 使用 **TLS** 保护用户会话安全

November 4, 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) 上安装证书并启用 TLS 加密。

#### 在 **Linux VDA** 上安装证书

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：

```
-----BEGIN CERTIFICATE-----
MIIDTTCCAragAwIBAgIJALluncpiqGXCMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNTk1M1oXDTI4MDkyNTEwNTk1M1owgYoxCzAJBgNVBAYTAlVL
MRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEUMBIGA1UE
ChMLQ2l0cml4IFRlc3QxGzAZBgNVBAsTElNlcnZlciBDZXJ0aWZpY2F0ZTEgMB4G
A1UEAxMXY2EwMDEtc2MwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALCTTOdxcivbI0LOF66xgO5gkNeIGKVP+37pSKV8B66lWCVzr6p9
t72Fa+9oCcf2x/ue274NXFcg4fqGRDsrEwl3YxM6COyBf7L6psrsCDNnBPlq8TJH
4xoPIXUeaW4MVk/3PVyfhHKs4fz8yy1I4VDnXVHhw+OFQ2Bq3NhwsRhnAgMBAAGj
gdwwgdkwCQYDVR0TBAIwADAdBgNVHQ4EFgQUrLidzYot+CUXSh9xMfp1M+/O8yOw
gZkGA1UdIwSBkTCBjoAU85kN1EPJOcVhcOss1slseDQwGsKha6RpMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
ggkAy8nC8dcB32EwEQYJYIZIAYb4QgEBBAQDAgVgMA0GCSqGSIb3DQEBBQUAA4GB
AD5axBYHwIxJCJzNt2zdXnbp2O0yUTowElBwQe/9cGaP6CpjoxJ7FJa2/8IpaT68
Vel8u1SEYY1GKCGCw93pc7sPKqb8pGBRI5/dygb+geFk1Q7KyVbuOIjOtr3pkxAe
b6CFJtNLudHUrwF6lOrB72zbyz3PiIx+HEwt1jOj8z4K
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCwk0zncXIr2yNC9BeusYDuYJDXiBilT/t+6UilfAeupVglc6+q
fbe9hWvvaAnH9sf7ntu+DVxXIOH6hkQ7KxMNd2MTOgjsgX+y+qbK7AgzZwT9avEy
R+MaDyFlHmluDFZP9z1cn4RyrOH8/MstSOFQ511R4cPtBUNgatzYcLEYZwIDAQAB
AoGBAKwBgZu/bkl8edgB8YPyU7diiBX89IOs4b/aPjM+JDmjxb8N96RsPO24p9Ea
FtUc9+iL8mEroLUbSicCXjsJFc+cxg9vVaNa6EEkkBj735oCUERqSxOYb/lAdck/
FXzU0tqytUe/KHgcSgjtjrSeqLJqMm+yxzBAatVRTTzGdwAhAkEA3l1kRZjIN5uz
Enmi2RTI3ngBhBP/S3GEbvJfKsD5n2Ri9O+OoEPxclvvp5ne8QOzUpshbjFEPbOC
ykZ6UassFwJBAMtI5yPnV9ewPzJoaNjZIJcMtNXDchSlxXiJiyzv+Qmr8RuQz9Pv
fIenmTrfZ+Wo4DaKg+8ar2OvOnKFOHFAmDECQQDEWRlH6cE3WyCfN1u942M9XkhR
GvSpR7+b///vL6Nwwv3CwPV9n8DTpL+wuDkJZ9nCvRteil9MlaMTYjs3alNvAkEA
qy5JzZcbBnrYzMbVO32jju7ZPISnhTGO1xDjzMSLLpTGpNLN34b0k3sTclr8L42E
uQjtTqRm+wdsrVF3lFazkQJANudmsUVv3gZKhMGaV2hzIdXIfHyOIYv+3leZhQY6
h5eEmxSZS5OTvyNGt2e6m2ZgaZmjTagH59TCBHvR5nof2g==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDGTCCAoKgAwIBAgIJAMvJwvHXAd9hMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNDExMVoXDTI4MDkyNTEwNDExMVowZzELMAkGA1UEBhMCVUsx
EjAQBgNVBAgTCUNhbWJyawRnZTESMBAGA1UEBxMJQ2FtYm9lcmSlMRQwEgYDVQQK
EwtDaXRyaXggVGVzdDEaMBgGA1UEAxMRY2EwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKVZmF7Uj7uOnvO3QwdfiOnr3QkNH2DXpWrZ
Zh8cI9Vv+UFRUiC6oB7izLtBMFn3fOUP7i2CfkHN3ZGJ17p89pdyjket1MslVeJw
acOqrYvD+fNNSvJjunTbaCywVtALjmFSfMHeZJXVSckrpEhnk0nkMS16tcrya/K/
osSlzvI3AgMBAAGjgcwwgckwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQU85kN1EPJ
OcVhcOss1slseDQwGsIwgZkGA1UdIwSBkTCBjoAU85kN1EPJOcVhcOss1slseDQw
GsKha6RpMGcxCzAJBgNVBAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNV
BAcTCUNhbWJvdXJuZTEUMBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNh
MDAxLmNpdHJpdGUubmV0ggkAy8nC8dcB32EwDQYJKoZIhvcNAQEFBQADgYEAIZ4Z
gXLLXf12RNqh/awtSbd41Ugv8BIKAsg5zhNAiTiXbzz8Cl3ec53Fb6nigMWc5Tli
UNCLXwnxRUiD4O0tESLX9ACUNH3I94yxOgujkSOSBni21jjZTvfBB32Rmr5DByJg
UmKORn/hdqMlcqpe5wO6as6+HN4WUOi+hEtUMME=
-----END CERTIFICATE-----
```

启用 **TLS** 加密

在 **Linux VDA** 上启用 **TLS** 加密　在 Linux VDA 上，使用 **/opt/Citrix/VDA/sbin** 目录中的 `enable_vdassl.sh` 脚本启用（或禁用）TLS 加密。有关脚本中可用的选项的信息，请运行 `/opt/Citrix/VDA/sbin/enable_vdassl.sh -help` 命令。

```
root@lxu1804:~# /opt/Citrix/VDA/sbin/enable_vdassl.sh
===Enable/Disable SSL on Linux VDA===
To enable SSL, a certificate file must be specified, otherwise the local certificate file under
/etc/xdl/.sslkeystore/ is used, If the local certificate file does not exist, the command
fails. You can specify the SSL port number, version and cipher suite, otherwise, their default
values are used!

Usage: enable_vdassl.sh -Disable
       Disable Linux VDA SSL.

Usage: enable_vdassl.sh -Enable [-Certificate <CERT-FILE>] [-SSLPort <SSL-PORT-NUMBER>]
       [-SSLMinVersion <SSL-MIN-VERSION>] [-SSLCipherSuite <SSL-CIPHER-SUITE>]
       Enable Linux VDA SSL.

Options:
       -Certificate <CERT-FILE>
       Specify a certificate file, where <CERT-FILE> must include the full file path. Only one format
       is currently supported, that is PEM.

       -RootCertificate <ROOT-CERT-FILE>
       Specify a root certificate file, where <ROOT-CERT-FILE> must include the full file path, The root certificate will be put in the local keystore(under /etc/xdl/.sslkeystore/cacerts).

       -SSLPort <SSL-PORT-NUMBER>
       Specify an SSL port number. Unless otherwise specified, the default port 443 used.

       -SSLMinVersion <TLS_1.0|TLS_1.1|TLS_1.2|TLS_1.3>
       Specify SSL version. Unless otherwise specified, the default value TLS_1.2 is used.

       -SSLCipherSuite <GOV|COM|ALL>
       Specify an SSL Cipher suite. Unless otherwise specified, the default value GOV is used.

Examples:
       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem"
       Enable Linux VDA SSL using Certificate cert001.pem.

       enable-vdassl.sh -Enable -RootCertificate "/home/rootCR.cer"
       Enable Linux VDA SSL using Root Certificate rootCR.cer with local certificate(under /etc/xdl/.sslkeystore).

       enable-vdassl.sh -Enable -SSLPort 445
       Enable Linux VDA SSL on port 445 using local certificate(under /etc/xdl/.sslkeystore).

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445
       Enable Linux VDA SSL using Certificate cert001.pem on port 445, with default SSLMinVersion and SSLCipherSuite.

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2"
       Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and default SSLCipherSuite..

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2" -SSLCipherSuite "GOV"
       Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and SSLCipherSuite GOV.
```

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。

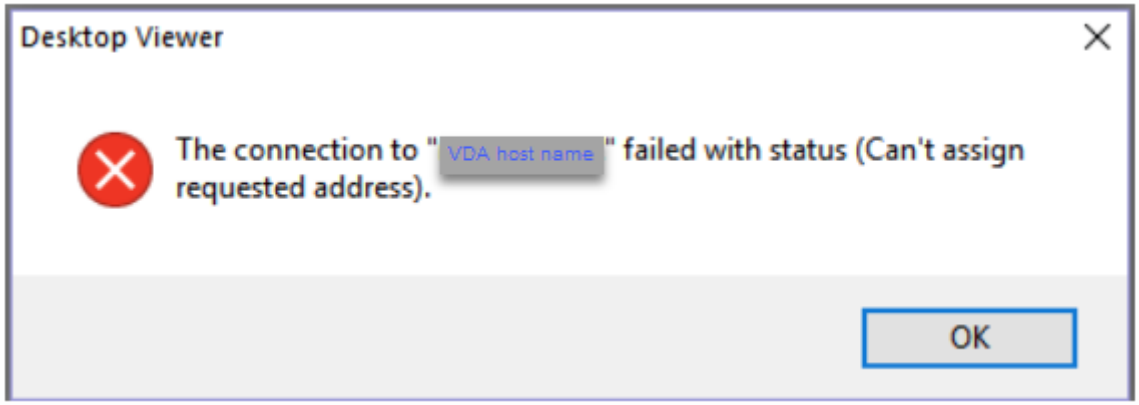
 

要在 Controller 上禁用 TLS 加密，请按顺序运行以下命令：

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。

## 会话可靠性

November 4, 2022

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

当会话中没有任何活动（例如，没有鼠标移动或屏幕更新）时，将在 Linux VDA 与客户端之间发送保持活动状态消息。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）。

```
/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）。

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

   ```
   netstat -an | grep 2598
   <!--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。

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

## USB 重定向

November 4, 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，您可以像使用本地连接的 USB 设备那样使用该设备。

> 提示：
>
> 当网络延迟低于 100 毫秒时，我们建议使用 USB 重定向。当网络延迟超过 200 毫秒时，请勿使用 USB 重定向。

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 服务用作管理 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。

### 支持的 **USB** 设备

下列设备已确认支持此 Linux VDA 版本。可以随意使用其他设备，但会有意外结果：

> 注意：
>
> Linux VDA 仅支持 USB 2.0 协议。

| USB 大容量存储设备 | VID:PID | 文件系统 |
| --- | --- | --- |
| Netac Technology Co., Ltd | 0dd8:173c | FAT32 |
| Kingston Datatraveler 101 II | 0951:1625 | FAT32 |

| USB 大容量存储设备 | VID:PID | 文件系统 |
| --- | --- | --- |
| Kingston Datatraveler GT101 G2 | 1567:8902 | FAT32 |
| SanDisk SDCZ80 flash drive | 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 photo | 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。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

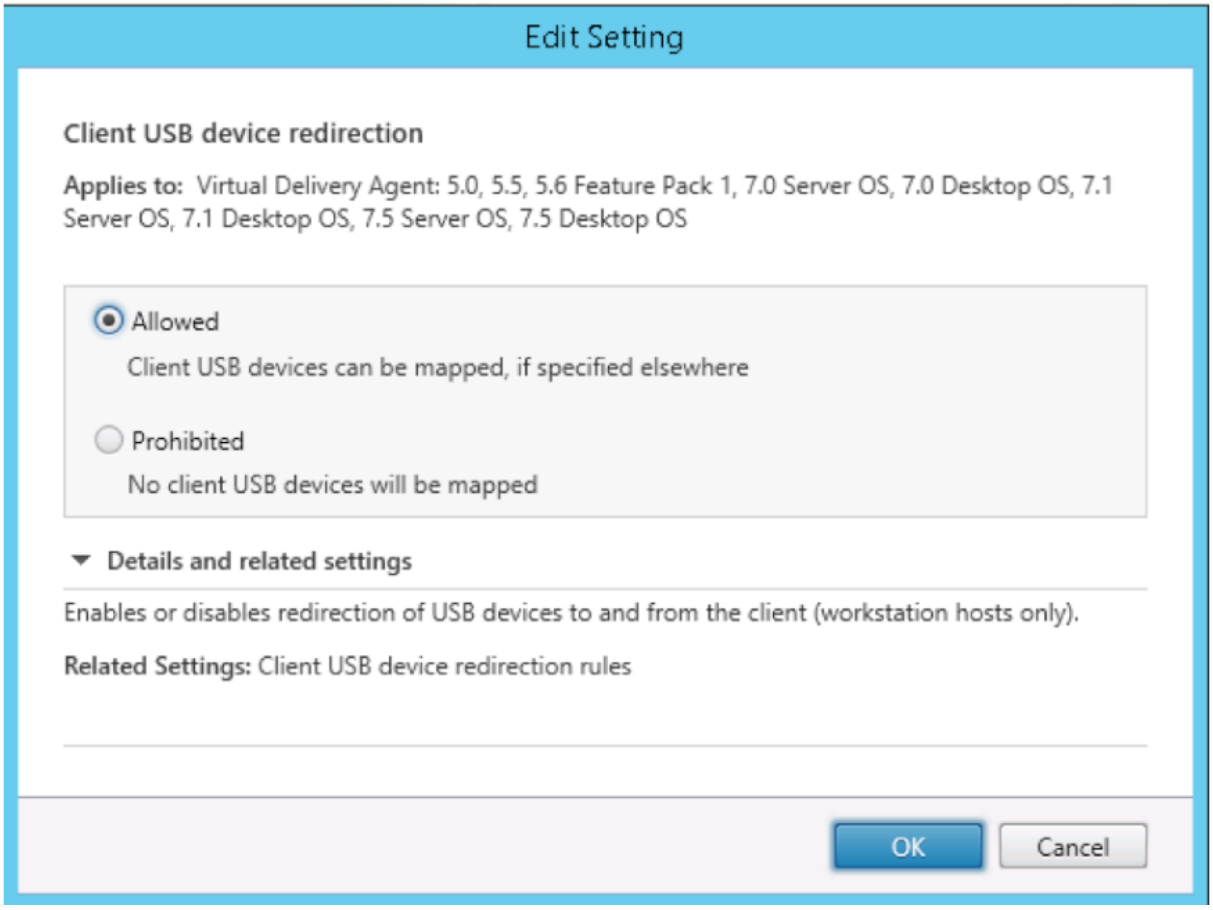
#### 启用 **USB** 重定向

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。



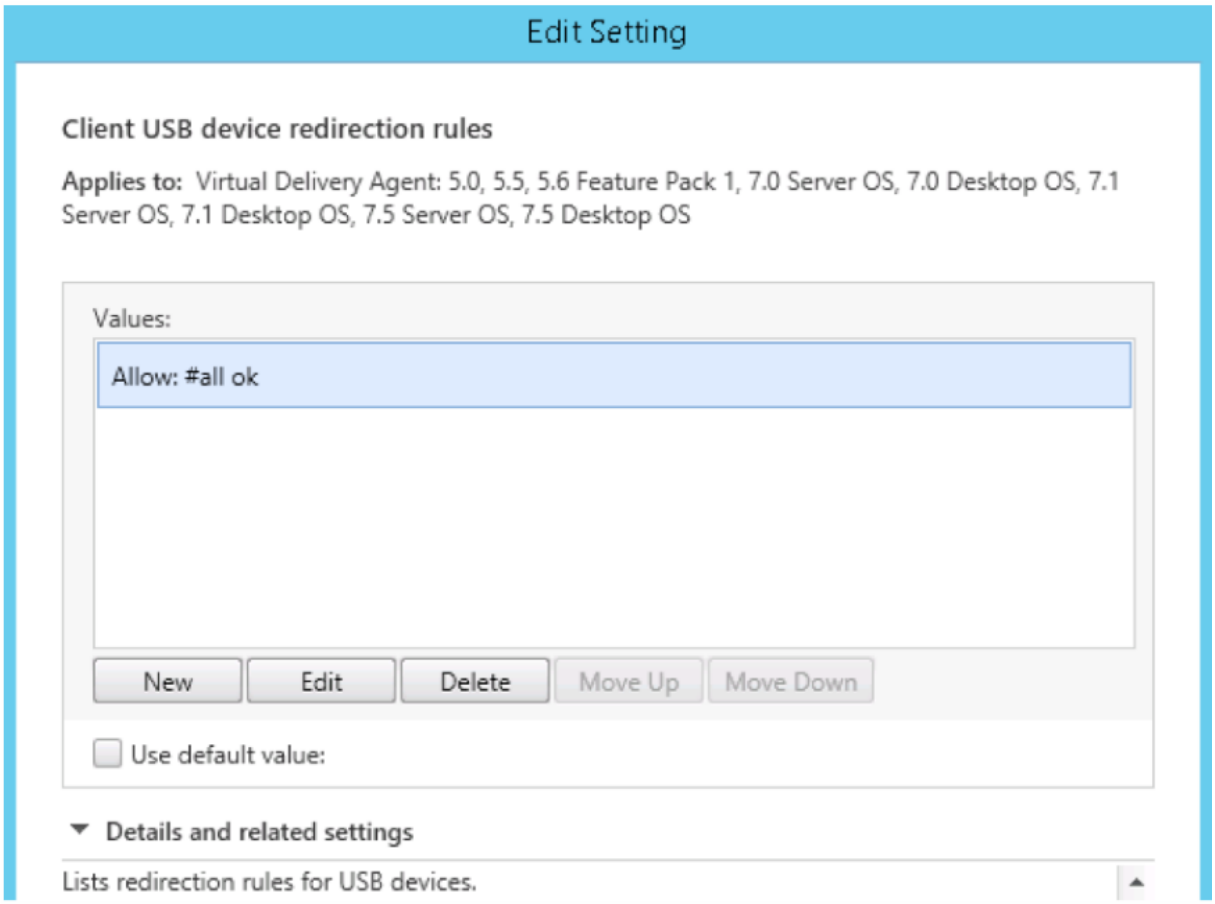

设置 **USB** 重定向规则

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 |
| --- | --- |
| Amazon Linux 2 | 4.14.281-212 |
| Debian 11.3 | 5.10.0-12 |
| Debian 10.9 | 4.19.0-20 |
| RHEL 8.x、Rocky Linux 8 | 4.18.0-372 |
| RHEL 7.9、CentOS 7.9 | 3.10.0-1160 |
| SUSE 15 | 5.3.18 |

| 支持的 Linux 发行版 | 内核版本 |
| --- | --- |
| Ubuntu 22.04 | 5.15.0-37 |
| Ubuntu 20.04 | 5.4.0-117 |
| Ubuntu 18.04 | 4.15.0-184 |

> 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：

```
insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
<!--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)** 部分中的文件。
2. 提取 **citrix-linux-vda-sources.zip** 文件。导航到 **linux-vda-sources/vhci-hcd-1.15.zip**，然后使用 `unzip vhci-hcd-1.15.zip` 命令提取 VHCI 源文件。
3. 确保安装了 Linux VDA 软件包，然后运行以下命令之一：
   - `sudo bash ctxusbcfg.sh dkms`

     使用此命令，您可以使用动态内核模块支持 (DKMS) 程序来管理 VHCI 内核模块。DKMS 不适用于 SUSE。

     > 注意：
     >
     > `sudo bash ctxusbcfg.sh dkms` 命令会在您的 VDA 上安装 `kernel-devel` 和 DKMS 程序。在 RHEL 和 CentOS 上安装程序时，该命令会在 VDA 上安装并启用 Extra Packages for Enterprise Linux (EPEL) 存储库。
     >
     > 当您进行重大内核升级（例如，从版本 4.x.y 升级到版本 5.x.y）时，DKMS 可能无法构建 VHCI 内核模块（`usb-vhci-hcd.ko` 和 `usb-vhci-iocif.ko`）。如果 DKMS 失败，请再次运

> 行 `sudo bash ctxusbcfg.sh dkms`。

- `sudo bash ctxusbcfg.sh build`

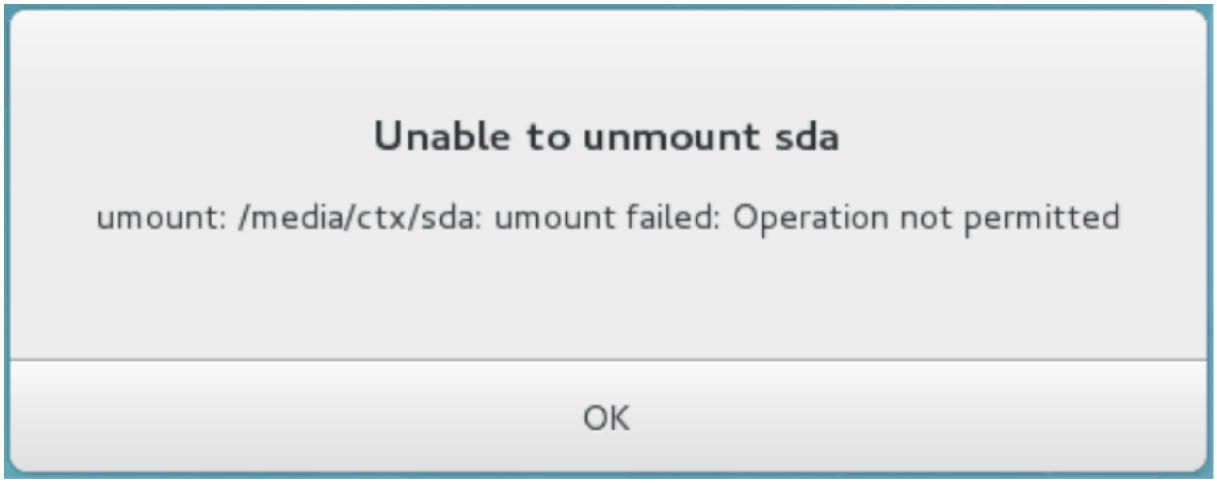
  此命令在不使用 DKMS 选项的情况下构建和安装 VHCI 内核模块。

### 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。

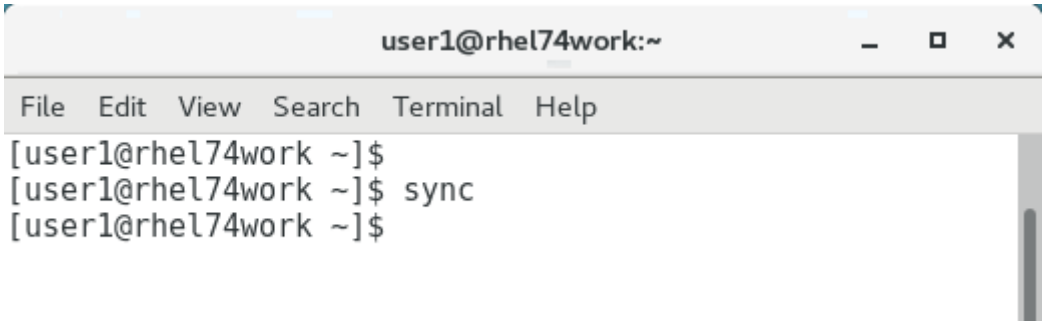
#### 无法卸载重定向的 **USB** 磁盘

Linux VDA 使用管理权限管理从 Citrix Workspace 应用程序重定向的所有 USB 磁盘，以确保只有所有者能够访问重定向的设备。因此，您只能使用管理权限卸载设备。




#### 停止重定向 **USB** 磁盘时文件丢失

如果使用 Citrix Workspace 应用程序的工具栏立即停止重定向 USB 磁盘，您在磁盘上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。

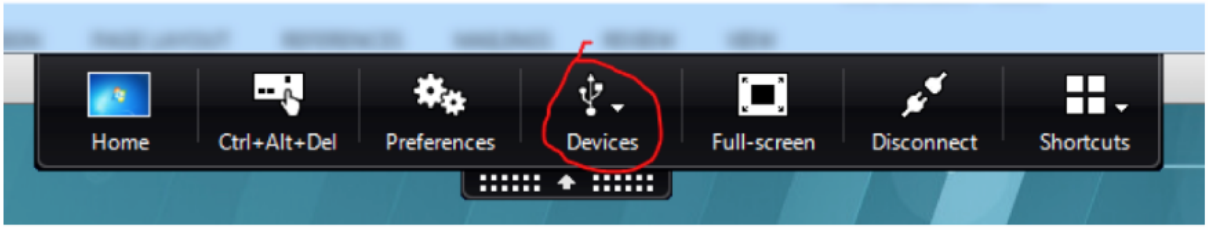


**Citrix Workspace** 应用程序的工具栏中无设备

有时，您可能无法看到 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。如果遇到问题，请验证以下各项：

- 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。对于每个重定向的设备，都会在系统 **/dev** 路径中创建用户拥有的节点。但是，用户是否可以成功使用设备由驱动程序和配置决定。如果您发现拥有（已插入）的某个设备无法访问，请将该设备添加到不受限制策略。

> 注意：
>
> 对于 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。

# 虚拟通道 **SDK**（实验性）

October 31, 2022

借助适用于 Linux VDA 的虚拟通道软件开发工具包 (SDK)，您可以编写要在 VDA 上运行的服务器端应用程序。有关详细信息，请参阅 Citrix Virtual Channel SDK for the Linux VDA（适用于 Linux VDA 的 Citrix 虚拟通道 SDK）文档。

面向 Linux VDA 的 Citrix 虚拟通道 SDK 可从 Citrix Virtual Apps and Desktops 下载页面进行下载。展开相应版本的 VDA Citrix Virtual Apps and Desktops 并单击组件以选择要下载的 Linux VDA。