Linux Virtual Desktop

Installation Guide for Red Hat Enterprise Linux

Version 1.1
# Table of Contents

- **Glossary** .......................................................... 1
- **Introduction** ...................................................... 1
- **System Requirements** ........................................... 1
  - Linux Distributions .................................................. 1
  - XenDesktop ......................................................... 2
  - Citrix Receiver ..................................................... 2
  - Hypervisors .......................................................... 2
  - Active Directory Integration Packages .......................... 2
- **Configure Delivery Controllers** ............................... 3
  - Update Delivery Controller Configuration ..................... 3
  - Verify Delivery Controller Configuration ..................... 3
- **Prepare Linux Machine for VDA Installation** ................ 4
  - Verify Network Configuration ..................................... 4
  - Configure Clock Synchronisation .................................. 4
  - Disable Network Proxy Authentication Popup .................. 5
  - Install OpenJDK .................................................... 6
  - Install PostgreSQL ................................................ 6
  - Install Motif .......................................................... 7
  - Install Other Packages ............................................. 7
  - Prepare Linux VM for Hypervisor .................................. 7
  - Add Linux Machine to Windows Domain .......................... 9
- **Configure Linux Machine Catalog and Delivery Group** ........ 15
  - Add Linux Machine to Machine Catalog ........................ 15
  - Add Delivery Group ............................................... 16
- **Install Linux VDA Software** .................................... 16
  - Uninstall Old Version .............................................. 16
  - Install Linux VDA .................................................. 17
  - Upgrade Linux VDA ................................................ 17
  - Configure Linux VDA .............................................. 17
  - Configure for Dedicated Desktops (VDI mode) ................ 19
- **Run VDA Software** .............................................. 19
  - Start Linux VDA .................................................... 19
  - Stop Linux VDA ..................................................... 19
Restart Linux VDA ............................................................................................................. 19
Check Linux VDA Status .................................................................................................. 20
Uninstall Linux VDA Software .......................................................................................... 20
Query Linux VDA Installation Status ................................................................................. 20
Uninstall Linux VDA .......................................................................................................... 20
Remove Dependent Packages ............................................................................................ 20
Troubleshooting ................................................................................................................ 20
Check the Linux machine has been prepared correctly..................................................... 20
Configure logging and tracing .......................................................................................... 20
What to try if HDX sessions won’t start ........................................................................... 21
Verify ownership and permissions of key directories and files ......................................... 21
Known Issues .................................................................................................................... 22
Disclaimer

This document is furnished "AS IS". Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix Systems, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc.

About Citrix

Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.

Copyright © 2015 Citrix Systems, Inc. All rights reserved. Citrix, Citrix Receiver, and StoreFront are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.
Glossary

- **Broker** - XenDesktop component responsible for brokering HDX sessions to the different VDAs within a XenDesktop deployment. Also known as the DDC or XenDesktop Controller.
- **Broker Agent** - Component on the Linux VDA machine providing the desktop to be delivered. The Broker Agent communicates with the Broker to enable the brokering of sessions. It is composed of two key components, the VDA Service and the HDX Service.
- **Citrix Director** - Citrix helpdesk/support console for monitoring and controlling XenDesktop VDAs.
- **Citrix Studio** - Citrix administration console used to configure XenDesktop.
- **DDC** - XenDesktop Desktop Delivery Controller. Also known as the Broker or Delivery Controller.
- **HDX** - High Definition Experience protocol. Formerly known as the Citrix ICA protocol.
- **HDX Service** - The Linux service that remotes the virtual Linux desktop via the HDX protocol. It communicates with the VDA service to enable the brokering of sessions.
- **RHEL** - Red Hat Enterprise Linux. A commercial Linux distribution provided by Red Hat.
- **SLED** - SUSE Linux Enterprise Desktop. A commercial Linux distribution provided by Novell.
- **SLES** - SUSE Linux Enterprise Server. A commercial Linux distribution provided by Novell.
- **VDA** - Virtual Delivery Agent.
- **VDA Service** - The Linux service that communicates with the Broker to enable the brokering of sessions. It also communicates with the HDX Service for remote session delivery.
- **FQDN** – Fully Qualified Domain Name

Introduction

This document is a guide for installing the Linux Virtual Desktop Release product on Red Hat Enterprise Linux. Please follow each section in order to ensure a successful installation.

The Linux shell commands used in this document have been verified to work with the GNU Bash shell.

System Requirements

**Linux Distributions**

The following Linux distributions are supported by the Linux Virtual Desktop product:

- **SUSE Linux Enterprise**
  - Desktop 11 Service Pack 3
  - Desktop 11 Service Pack 4
  - Desktop 12
  - Server 11 Service Pack 3
  - Server 11 Service Pack 4
  - Server 12
- **Red Hat Enterprise Linux**
  - Workstation 6.6
  - Workstation 6.7
  - Workstation 7.0
  - Workstation 7.1
  - Server 6.6
  - Server 6.7
  - Server 7.0
Server 7.1

In all cases, the processor architecture supported is x86-64.

**XenDesktop**

The following versions of XenDesktop are supported by the Linux VDA:

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6

The configuration process for Linux VDAs differs slightly than for Windows VDAs. However, any Delivery Controller farm is capable of brokering both Windows and Linux desktops.

The Linux VDA is incompatible with XenDesktop version 7.0 or earlier.

**Citrix Receiver**

The following versions of Citrix Receiver are supported:

- Windows Receiver version v4.2 or newer (1)
- Linux Receiver version v13.0 or newer
- Mac OSX Receiver v12 or newer
- Android Receiver v3.4 or newer
- iOS Receiver 5.9.4 or newer
- HTML5 Receiver 1.6 (via Access Gateway)

(1) This equates to v14.0 of wfica32.exe.

**Hypervisors**

The following hypervisors for hosting Linux VDA guest VMs are supported:

- XenServer
- VMware ESX and ESXi
- Microsoft Hyper-V

Bare metal hosting is also supported.

Refer to the hypervisor vendor’s documentation for the list of supported platforms.

**Active Directory Integration Packages**

The following Active Directory integration packages or products are supported by the Linux VDA:

- Samba Winbind
- Quest Authentication Services v4.1 or newer
- Centrify DirectControl
Refer to the Active Directory Integration package vendor’s documentation for the list of supported platforms.

Configure Delivery Controllers

Update Delivery Controller Configuration

For XenDesktop 7.6 SP2, apply the Hotfixes Update 2 to update the Broker for Linux Virtual Desktop. Hotfixes Update 2 is available from here:

- CTX142438: Hotfixes Update 2 - For Delivery Controller 7.6 (32-bit) – English
- CTX142439: Hotfixes Update 2 - For Delivery Controller 7.6 (64-bit) – English

For earlier versions of XenDesktop, a PowerShell script named Update-BrokerServiceConfig.ps1 is provided which will update the Broker service configuration. This is available in the following package:

- citrix-linuxvda-scripts-1.1.0.zip

Repeat the following steps on every Delivery Controller in the farm:

1. Copy the Update-BrokerServiceConfig.ps1 script to the Delivery Controller machine.
2. Open a Windows PowerShell console in the context of the local Administrator.
3. Locate and change to the folder containing the script.
4. Execute the script:

   .\Update-BrokerServiceConfig.ps1

By default, PowerShell is configured to prevent the execution of PowerShell scripts. If the script fails to run, you may need to change the PowerShell execution policy before trying again:

   Set-ExecutionPolicy Unrestricted

The Update-BrokerServiceConfig.ps1 script updates the Broker service configuration file with new WCF endpoints required by the Linux VDA and restarts the Broker Service. The script determines the location of the Broker service configuration file automatically. A backup of the original configuration file is created in the same directory with the extension .prelinux.

These changes will have no impact on the brokering of Windows VDA’s configured to use the same Delivery Controller farm. This allows for a single Controller farm to manage and broker sessions to both Windows and Linux VDAs seamlessly.

Verify Delivery Controller Configuration

To verify whether the required configuration changes have been applied to a Delivery Controller, confirm the string EndpointLinux appears five times in the file:

%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config

From the Windows command prompt, logged on as a local administrator:
cd "%PROGRAMFILES%\Citrix\Broker\Service\"
findstr "EndpointLinux BrokerService.exe.config"

**Prepare Linux Machine for VDA Installation**

**Verify Network Configuration**

Citrix recommends that the network is connected and properly configured correctly before proceeding.

**RHEL 7.0 Only: Set hostname**

To ensure that the hostname of the machine is reported correctly, change the `/etc/hostname` file to contain only the hostname of the machine.

**Assign Loopback Address to Hostname**

To ensure that the DNS domain name and FQDN of the machine are reported back correctly, change the following line of the `/etc/hosts` file to include the FQDN and hostname as the first two entries:

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

For example:

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

Remove any other references to `hostname-fqdn` or `hostname` from other entries in the file.

**Check Hostname**

Verify that the hostname is set correctly:

```
hostname -f
```

This should return the machine’s FQDN.

**Check Name Resolution and Service Reachability**

Verify that you can resolve the FQDN and ping the domain controller and XenDesktop Delivery Controller:

```
nslookup domain-controller-fqdn
ping domain-controller-fqdn
nslookup delivery-controller-fqdn
ping delivery-controller-fqdn
```

**Configure Clock Synchronisation**

Maintaining accurate clock synchronization between the VDAs, XenDesktop Controllers and domain controllers is crucial. Hosting the Linux VDA as a virtual machine can cause clock skew problems. For this reason, synchronizing time with a remote time service is preferred.
RHEL 6.x and earlier releases use the NTP daemon (ntpd) for clock synchronization, whereas a default RHEL 7.x environment uses the newer Chrony daemon (chronyd) instead. The configuration and operational process between the two services is similar.

**RHEL 6 Only: NTP Service**

As root, edit `/etc/ntp.conf` and add a server entry for each remote time server:

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

In a typical deployment, time should be synchronized from the local domain controllers and not directly from public NTP pool servers. Add a server entry for each Active Directory domain controller in the domain.

Remove any other `server` entries listed including loopback IP address, localhost, and public server `*.pool.ntp.org` entries.

Save changes and restart the NTP daemon:

```
sudo /sbin/service ntpd restart
```

**RHEL 7 Only: Chrony Service**

As root, edit `/etc/chrony.conf` and add a server entry for each remote time server:

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

In a typical deployment, time should be synchronized from the local domain controllers and not directly from public NTP pool servers. Add a server entry for each Active Directory domain controller in the domain.

Remove any other `server` entries listed including loopback IP address, localhost, and public server `*.pool.ntp.org` entries.

Save changes and restart the Chrony daemon:

```
sudo /sbin/service chronyd restart
```

**Disable Network Proxy Authentication Popup**

There is a specific RHEL 6 issue that causes users to receive a popup asking for the root password after logging on.

To resolve this issue, as root, create the file `/etc/polkit-1/localauthority/30-site.d/20-no-show-proxy-dialog.pkla` in a text editor and add the following content:

```ini
[No Show Proxy Dialog]
Identity=unix-user:*
Action=org.freedesktop.packagekit.system-network-proxy-configure
ResultAny=no
ResultInactive=no
```
Install OpenJDK

The Linux VDA dependent on OpenJDK 1.7.0. The runtime environment should have been installed as part of the operating system installation, confirm this with:

```
sudo yum info java-1.7.0-openjdk
```

The pre-packaged OpenJDK is likely to be out-of-date. Update to the latest version as required:

```
sudo yum -y update java-1.7.0-openjdk
```

Set the `JAVA_HOME` environment variable by adding the following line to `~/.bashrc` file:

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

Open a new shell and verify the version of Java:

```
java -version
```

To avoid problems, make sure you only installed the 1.7.0 version of OpenJDK. Remove all other versions of Java on your system.

Install PostgreSQL

The Linux VDA requires either PostgreSQL 8.4 or newer on RHEL 6 or PostgreSQL version 9.2 or newer on RHEL 7.

Install the following packages:

```
sudo yum -y install postgresql-server
sudo yum -y install postgresql-jdbc
```

The following post-installation step is required to initialize the database and ensure service starts on boot. This will create database files under `/var/lib/pgsql/data`. This command differs between PostgreSQL 8 and 9:

**RHEL 6 Only: PostgreSQL 8**

```
sudo /sbin/service postgresql initdb
```

**RHEL 7 Only: PostgreSQL 9**

```
sudo postgresql-setup initdb
```
**Start PostgreSQL**

For either version PostgreSQL, configure the service to start on boot, and to start now:

```
sudo /sbin/chkconfig postgresql on
sudo /sbin/service postgresql start
```

Check the version of PostgreSQL using:

```
psql --version
```

Check the data directory is set using the `psql` command-line utility:

```
sudo -u postgres psql -c 'show data_directory'
```

**Install Motif**

The Linux VDA requires either the motif or openmotif package, depending on the distribution.

**RHEL 6 Only: Open Motif**

```
sudo yum -y install openmotif
```

**RHEL 7 Only: Motif**

```
sudo yum -y install motif
```

**Install Other Packages**

Install the other required packages:

```
sudo yum -y install redhat-lsb-core
sudo yum -y install ImageMagick
```

**Prepare Linux VM for Hypervisor**

Some changes are required when running the Linux VDA as a virtual machine on a supported hypervisor. Make the following changes according to the hypervisor platform in use. No changes are required if you are running the Linux machine on bare metal hardware.

**Citrix XenServer**

**Fix Time Synchronization**

If the XenServer Time Sync feature is enabled, within each paravirtualized Linux VM you will experience issues with NTP and XenServer both trying to manage the system clock. To avoid the clock becoming out of sync with other servers, the system clock within each Linux guest must be synchronized with NTP. This requires disabling host time synchronization. No changes are required in HVM mode.
On some Linux distributions, if you are running a paravirtualized Linux kernel with XenServer Tools installed, you can check whether the XenServer Time Sync feature is present and enabled from within the Linux VM:

```
su -
cat /proc/sys/xen/independent_wallclock
```

This will return either:

- 0 - The time sync feature is enabled, and needs to be disabled.
- 1 - The time sync feature is disabled, and no further action is required.

If the `/proc/sys/xen/indepent_wallclock` file is not present, the following steps are not required.

If enabled, disable the time sync feature by writing 1 to the file:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

To make this change permanent and persist after reboot, edit the `/etc/sysctl.conf` file and add the line:

```
xen.independent_wallclock = 1
```

To verify these changes, reboot the system:

```
reboot
```

After reboot, check that this has been set correctly:

```
su -
cat /proc/sys/xen/independent_wallclock
```

This should return the value 1.

**Microsoft Hyper-V**

**Fix Time Synchronization**

Linux VMs with Hyper-V Linux Integration Services installed can leverage the Hyper-V time synchronization feature to use the host operating system's time. To ensure the system clock remains accurate, this feature should be enabled alongside NTP services.

From the management operating system:

1. Open the Hyper-V Manager console.
2. For the settings of a Linux VM, select **Integration Services**.
3. Ensure **Time synchronization** is checked.
This approach is different from VMware and XenServer, where host time synchronization is disabled to avoid conflicts with NTP. Hyper-V time synchronization can co-exist and supplement NTP time synchronization.

VMware ESX and ESXi

Fix Time Synchronization

If the VMware Time Synchronization feature is enabled, within each paravirtualized Linux VM you will experience issues with NTP and the hypervisor both trying to synchronize the system clock. To avoid the clock becoming out of sync with other servers, the system clock within each Linux guest must be synchronized with NTP. This requires disabling host time synchronization.

If running a paravirtualized Linux kernel with VMware Tools installed:

1. Open the vSphere Client.
2. Edit settings for the Linux VM.
3. In the Virtual Machine Properties dialog, open the Options tab.
4. Select VMware Tools.
5. In the Advanced box, uncheck Synchronize guest time with host.

Add Linux Machine to Windows Domain

There are a number of methods for adding Linux machines to the Windows domain that are supported by XenDesktop for Linux:

1. Samba Winbind
2. Quest Authentication Service
3. Centrify DirectControl

Follow the instructions for your chosen method.

Samba Winbind

Install or Update Required Packages

Install or update the required packages:

```bash
sudo yum -y install samba-winbind \
samba-winbind-clients \
krb5-workstation \
authconfig \
oddjob-mkhomedir
```

Enable Winbind Daemon to Start on Boot

The Winbind daemon must be configured to start on boot.

```bash
sudo /sbin/chkconfig winbind on
```

Configure Winbind Authentication

Configure the machine for Kerberos authentication using Winbind:
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

Where **REALM** is the Kerberos realm name in upper-case and **domain** is the short NetBIOS name of the domain.

If DNS-based lookups of KDC server and realm name is required, add the following two options to the above command:

   --enablekrb5kdcdns --enablekrb5realmdns

Ignore any errors returned from the **authconfig** command about the winbind service failing to start. These are due to authconfig trying to start the winbind service without the machine yet being joined to the domain.

Open `/etc/samba/smb.conf` and add the following entries under the [Global] section, but after the section generated by the authconfig tool.

    kerberos method = secrets and keytab
    winbind refresh tickets = true

The system keytab file `/etc/krb5.keytab` is required by the Linux VDA to authenticate and register with the Delivery Controller. The kerberos method setting above will force Winbind to create the system keytab file when the machine is first joined to the domain.

**Join Windows Domain**

This requires that your domain controller is reachable and you have a Windows account with permissions to add computers to the domain.

    sudo net ads join REALM -U user

Where **REALM** is the Kerberos realm name in upper-case, and **user** is a domain user with permissions to add computers to the domain.

**Configure PAM for Winbind**

By default, the configuration for the Winbind PAM module (pam_winbind) does not enable Kerberos ticket caching and home directory creation. Open `/etc/security/pam_winbind.conf` and add or change the following entries under the [Global] section:

    krb5_auth = yes
krb5_ccache_type = FILE
mkhomedir = yes

Ensure any leading semi-colons from each setting are removed. These changes require restarting the Winbind daemon:

```bash
tenet ads testjoin
```

The winbind daemon will only stay running if the machine is joined to a domain.

Verify Domain Membership

The XenDesktop Controller requires that all VDA machines, whether Windows or Linux, have a computer object in Active Directory.

Verify the machine is joined to a domain using Samba's `net ads` command:

```bash
sudo net ads testjoin
```

Additional domain and computer object information can be verified with:

```bash
sudo net ads info
```

Verify Kerberos Configuration

To verify Kerberos is configured correctly for use with the Linux VDA, check that the system keytab file has been created and contains valid keys:

```bash
klist -ke
```

This should display the list of keys available for the various combinations of principal names and cipher suites. Run the Kerberos `kinit` command to authenticate the machine with the domain controller using these keys:

```bash
kinit -k MACHINE\$@REALM
```

The machine and realm names must be specified in uppercase, and the dollar sign ($) must be escaped with a backslash (\) to prevent shell substitution. In some environments the DNS domain name is different from the Kerberos realm name; ensure the realm name is used. If this command is successful, no output will be displayed.

Check the TGT ticket for the machine account has been cached using:

```bash
klist
```

Examine the machine account details using:

```bash
net ads status
```
Verify User Authentication

Use the `wbinfo` tool to verify that domain users can authenticate with the domain:

```
wbinfo --krb5auth=domain\\username\password
```

The domain specified here is the AD domain name, not the Kerberos realm name. For the bash shell, the backslash (`\`) character must be escaped with another backslash. This command will return a message indicating success or failure.

To verify that the Winbind PAM module is configured correctly, logon locally with a domain user account that has not logged onto the machine previously.

```
ssh localhost -l domain\\username
id -u
```

Check that a corresponding Kerberos credential cache file was created for the uid returned by the `id -u` command:

```
ls /tmp/krb5cc_uid
```

Check that the tickets in the user’s Kerberos credential cache are valid and not expired:

```
klist
```

Exit the session:

```
exit
```

A similar test can be performed by logging onto the Gnome or KDE console directly.

Quest Authentication Service

Configure Quest on Domain Controller

This assumes you have installed and configured the Quest software on the Windows domain controllers, and have been granted administrative privileges to create computer objects in Active Directory.

Enable Domain Users to Logon to Linux VDA Machines

For each domain user that needs to establish HDX sessions on a Linux VDA machine:

1. Open AD user properties for that user account.
2. Select Unix Account tab.
3. Check Unix-enabled.
4. Set the Primary GID Number to the group ID of an actual domain user group.

These instructions are equivalent for setting up domain users for logon using the console, RDP, SSH or any other remoting protocol.
Configure Quest on Linux VDA

Workaround SELinux Policy Enforcement

The default RHEL environment has SELinux fully enforced. This interferes with the Unix domain sockets IPC mechanisms used by Quest and prevents domain users from logging on.

There are a few ways to workaround this as outlined here: https://support.software.dell.com/authentication-services/kb/70022.

The easiest is to disable SELinux. As root, edit /etc/selinux/config and change the SELinux setting:

```
SELINUX=disabled
```

This change requires a reboot:

```
reboot
```

⚠️ Take care with this setting. Reenabling SELinux policy enforcement after disabling can cause a complete lockout, even for the root user and other local users.

Configure Auto Ticket Renewal

Auto-renewal of Kerberos tickets needs to be enabled:

```
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
```

This sets the renewal interval to 9 hours (32400 seconds) which is an hour less than the default 10 hour ticket lifetime. This value will need to be set to a lower value on systems with a shorter ticket lifetime.

Configure PAM and NSS

Quest requires that PAM and NSS be manually configured to enable domain user login via HDX and other services such as su, ssh, and RDP. To configure PAM and NSS:

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

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

Join Windows Domain

Join the Linux machine to the AD domain using the Quest vastool command:

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

The **user** is any domain user with permissions to join machines to the Windows domain. The **domain-name** is the DNS name of the domain; for example, **example.com**.

Verify Domain Membership
The XenDesktop Controller requires that all VDA machines, whether Windows or Linux, have a computer object in Active Directory. To verify that a Quest-joined Linux machine is on the domain:

```bash
sudo /opt/quest/bin/vastool info domain
```

If the machine is joined to a domain this will return the domain name. If not joined, you will see the following error:

```
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
```

**Verify User Authentication**

To verify that the Quest can authenticate domain users using PAM, logon with a domain user account that has not logged onto the machine previously.

```bash
ssh localhost -l domain\"username
id -u
```

Check that a corresponding Kerberos credential cache file was created for the uid returned by the `id -u` command:

```bash
ls /tmp/krb5cc_uid
```

Check that the tickets in user’s Kerberos credential cache are valid and not expired:

```bash
/opt/quest/bin/vastool klist
```

Exit the session:

```bash
exit
```

A similar test can be performed by logging on via Gnome Display Manager.

**Centrify DirectControl**

**Join Windows Domain**

With the Centrify DirectControl Agent installed, join the Linux machine to the AD domain using the Centrify `adjoin` command:

```bash
su -
adjoin -w -V -u user domain-name
```

The `user` parameter is any domain user with permissions to join machines to the Windows domain. The domain-name parameter is the name of the domain to join the Linux machine to.
Verify Domain Membership

The XenDesktop Controller requires that all VDA machines, whether Windows or Linux, have a computer object in Active Directory. To verify that a Centrify-joined Linux machine is on the domain:

```
su -
adinfo
```

Check that the Joined to domain value is valid and the **CentrifyDC mode** returns **connected**. If the mode remains stuck in the **starting** state, then the Centrify client is experiencing server connection or authentication problems.

A richer set of system and diagnostic information is available using:

```
adinfo --sysinfo all
adinfo --diag
```

To test connectivity to the various Active Directory and Kerberos services:

```
adinfo --test
```

Configure Linux Machine Catalog and Delivery Group

Add Linux Machine to Machine Catalog

The process for creating machine catalogs and adding Linux VDA machines is very similar to the traditional Windows VDA approach. Refer to the online Citrix Product documentation for a more complete description of how to complete these tasks.

For creating machine catalogs that contain Linux VDA machines, there are a few restrictions that differentiates the process from creating machine catalogs for Windows VDA machines:

- For operating system, select:
  - **Window Server OS** or **Server OS** option for a hosted shared desktops delivery model.
  - **Windows Desktop OS** or **Desktop OS** option for a VDI dedicated desktop delivery model.
- Ensure machines are set as not power managed.
- As PVS and MCS are not supported for Linux VDAs, choose the **Another service or technology** (existing images) deployment method.
- Do not mix Linux and Windows VDA machines in the same machine catalog.

Early versions of Citrix Studio did not support the notion of a "Linux OS"; however, selecting the **Windows Server OS** or **Server OS** option implies an equivalent hosted shared desktops delivery model. Selecting the **Windows Desktop OS** or **Desktop OS** option implies a VDI single user per machine delivery model.

The Citrix documentation for creating machine catalogs is referenced below:


Earlier versions of XenDesktop are not supported.

If a machine leaves and is rejoined to the Active Directory domain, the machine will need to be removed and re-added again to the machine catalog.

### Add Delivery Group

The process for creating a delivery group and adding machine catalogs containing Linux VDA machines is almost identical for Windows VDA machines. Refer to the online Citrix Product documentation for a more complete description of how to complete these tasks.

For creating delivery groups that contain Linux VDA machine catalogs, the following restrictions apply:

- For delivery type, select **Desktops**. Linux VDA machines do not support application delivery.
- Ensure the AD users and groups you select have been properly configured to logon to the Linux VDA machines.
- Do not allow logon of unauthenticated (anonymous) users.
- Do not mix the delivery group with machine catalogs that contain Windows machines.

The Citrix documentation for creating delivery groups is referenced below:


Earlier versions of XenDesktop are not supported.

### Install Linux VDA Software

#### Uninstall Old Version

If you have previously installed the Tech Preview version of the Linux VDA, you should uninstall it before installing the new version.

Stop the Linux VDA services:

```
  sudo /sbin/service ctxvda stop
  sudo /sbin/service ctxhdx stop
```

Uninstall the package:

```
  sudo rpm -e XenDesktopVDA
```
Upgrading from the Tech Preview to v1.0 or v1.1 is not supported.

Install Linux VDA

Install the Linux VDA software using the RPM package manager:

```bash
sudo rpm -i XenDesktopVDA-1.1.0.240-0.x86_64.rpm
```

Upgrade Linux VDA

If you have previously installed v1.0 of the Linux VDA, upgrade the Linux VDA software using the RPM package manager:

```bash
sudo rpm -U XenDesktopVDA-1.1.0.240-0.x86_64.rpm
```

Configure Linux VDA

After installing the package you will need to configure the Linux VDA by running the `ctxsetup.sh` script. If you have upgraded the package you will need to run the `ctxsetup.sh` script to finalise your upgrade. Before making any changes, this script will verify the environment and ensure all dependencies are installed. If required, this script can be re-run at any time to change settings.

The script can either be run manually with prompting or automatically with pre-configured responses. Review help about this script before proceeding:

```bash
sudo /usr/local/sbin/ctxsetup.sh --help
```

Prompted Configuration

Run a manual configuration with prompted questions:

```bash
sudo /usr/local/sbin/ctxsetup.sh
```

Automated Configuration

For an automated install, the options required by the setup script can be provided with environment variables. If all of the required variables are present then the script will not prompt the user for any information, allowing the installation process to be scripted.

Supported environment variables include:

- `CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N` - Whether or not the Linux VDA should support the specification of DDC names via CNAMEs. This is typically `N`.
- `CTX_XDL_DDC_LIST = list-ddc-fqdns` - A space-separated list of FQDNs or CNAME aliases (if using CNAME DDC lookup) of your Delivery Controllers. At least one FQDN or CNAME alias must be specified.
- `CTX_XDL_REGISTER_SERVICE = Y | N` - Whether or not the Linux VDA services should start on boot. This is typically `Y`. 

- **CTX_XDL_ADD_FIREWALL_RULES = Y | N** - Whether or not the firewall exception rules for the Linux VDA should be added to the system. This is typically Y.

- **CTX_XDL_AD_INTEGRATION = 1 | 2 | 3** - Specifies which Active Directory integration method to use:
  - 1 - Samba Winbind
  - 2 - Quest Authentication Service
  - 3 - Centrify DirectControl

- **CTX_XDL_START_SERVICE = Y | N** - Whether or not the Linux VDA services are started when the Linux VDA configuration is complete. This is typically Y.

Set the environment variable and run the configure script:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
export CTX_XDL_DDC_LIST=list-ddc-fqdns
export CTX_XDL_REGISTER_SERVICE=Y|N
export CTX_XDL_ADD_FIREWALL_RULES=Y|N
export CTX_XDL_AD_INTEGRATION=1|2|3
export CTX_XDL_START_SERVICE=Y|N
sudo -E /usr/local/sbin/ctxsetup.sh
```

You must provide the `-E` option with `sudo` to pass the existing environment variables to the new shell it creates. It is recommended that you create a shell script file from the commands above with `#!/bin/bash` on the first line.

Alternatively, all parameters can be specified with a single command:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \   
CTX_XDL_DDC_LIST=list-ddc-fqdns \   
CTX_XDL_REGISTER_SERVICE=Y|N \   
CTX_XDL_ADD_FIREWALL_RULES=Y|N \   
CTX_XDL_AD_INTEGRATION=1|2|3 \   
CTX_XDL_START_SERVICE=Y|N \   
/usr/local/sbin/ctxsetup.sh
```

**Remove Configuration Changes**

In some scenarios it may be necessary to remove the configuration changes made by the `ctxsetup.sh` script without uninstalling the Linux VDA package.

Review help about this script before proceeding:

```
sudo /usr/local/sbin/ctxcleanup.sh --help
```

To remove configuration changes:

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

This script will delete all configuration data from the database and will make the Linux VDA inoperable.

**Configuration Logs**

The `ctxsetup.sh` and `ctxcleanup.sh` scripts will display errors on the console, with additional information written to a configuration log file:
Configure for Dedicated Desktops (VDI mode)

The Linux VDA is configured for hosted shared desktop delivery model by default. Additional configuration is required to change this the VDI dedicated desktop delivery model.

To configure XenDesktop dedicated desktop delivery model:

```bash
sudo /usr/local/bin/ctxreg create \
-k "HKLM/System/CurrentControlSet/Control/Citrix/Win Stations/tcp" \
-t "REG_DWORD" \
-v "StackSessionMode" \
-d "0" \
--force
```

To restore the default hosted shared desktop delivery model:

```bash
sudo /usr/local/bin/ctxreg delete \
-k "HKLM/System/CurrentControlSet/Control/Citrix/Win Stations/tcp" \
-v "StackSessionMode" \
--force
```

Restart the Linux VDA services to have the changes take affect.

Run VDA Software

Once you have configured the Linux VDA using the `ctxsetup.sh` script, you use the following commands to control the Linux VDA.

Start Linux VDA

To start the Linux VDA services:

```bash
sudo /sbin/service ctxhdx start
sudo /sbin/service ctxvda start
```

Stop Linux VDA

To stop the Linux VDA services:

```bash
sudo /sbin/service ctxvda stop
sudo /sbin/service ctxhdx stop
```

Restart Linux VDA

To restart the Linux VDA services:

```bash
sudo /sbin/service ctxvda stop
sudo /sbin/service ctxhdx restart
sudo /sbin/service ctxvda start
```
Check Linux VDA Status

To check the running state of the Linux VDA services:

```
sudo /sbin/service ctxvda status
sudo /sbin/service ctxhdx status
```

Uninstall Linux VDA Software

Query Linux VDA Installation Status

To check whether the Linux VDA is installed and to view the version of the package installed:

```
rpm -q XenDesktopVDA
```

To view more detailed information:

```
rpm –qi XenDesktopVDA
```

Uninstall Linux VDA

To uninstall the Linux VDA package:

```
sudo rpm -e XenDesktopVDA
```

Uninstalling the Linux VDA software will delete the associated PostgreSQL and other configuration data. However, the PostgreSQL package and other dependent packages that were setup prior to the installation of the Linux VDA will not be removed.

Remove Dependent Packages

This guide does not cover the removal of dependent packages including PostgreSQL.

Troubleshooting

Check the Linux machine has been prepared correctly

The most common issues are a direct result of Linux machine misconfiguration, mainly around networking, NTP time server configuration or Windows domain membership. Fixing the Linux machine’s configuration will often resolve issues with the VDA software.

Configure logging and tracing

The Broker Agent and the HDX Service log to syslog. Citrix support have a set of tools that can enable addition trace during a support call.

HDX Service logging

The HDX Service is configured to log to syslog out-of-the-box and no further configuration is needed.
Broker Agent logging

The Broker Agent (also known as the ctxvda service) writes log data to syslog via network sockets. This may not be configured out-of-the-box. To enable the Broker Agent logging to syslog logging, the following configuration is required.

Edit the /etc/rsyslog.conf file and add the following lines:

```bash
$ModLoad imudp
$UDPServerRun 514
```

Save and close the rsyslog.conf file. Restart the rsyslog service to have the change take affect:

```bash
sudo /sbin/service rsyslog restart
```

What to try if HDX sessions won't start

Ensure you have no orphaned processes which might be preventing new sessions from starting:

```bash
sudo pkill -9 ctxfm
sudo pkill -9 ctxgfx
sudo pkill -9 ctxlogin
sudo pkill -9 ctxvfb
```

Restart the Linux VDA services and retry connection.

Verify ownership and permissions of key directories and files

Check the file ownership and permission of the following directories and files:

- `/var` - Owner: root, Group: root, Permissions: 0755
- `/var/xdl` - Owner: ctxsrvr, Group: ctxadm, Permissions: 0755
- `/var/xdl/.isacagent` - Owner: root, Group: root, Permissions: 0666
- `/var/xdl/.winsta` - Owner: ctxsrvr, Group: ctxadm, Permissions: 0777
- `/var/xdl/vda` - Owner: root, Group: root, Permissions: 0755
Known Issues

Citrix Receiver for Android CAPS LOCK state can be reversed when session roaming
The CAPS LOCK state may be lost when roaming an existing connection to the Citrix Receiver for Android. The workaround is to use the shift key on the extended keyboard to switch between upper case and lower case.

Shortcut keys with ALT do not always work when connecting to a Linux VDA using the Citrix Receiver for Mac
The Citrix Receiver for Mac send AltGr for both left and right Options/Alt keys by default. It is possible to change this within the Citrix Receiver settings but the results vary with different applications.

Newer X client libraries can cause keyboard mapping issues on SuSE Linux Enterprise Desktop 11
Newer versions of the xorg-x11-libX11 packages on SuSE Linux Enterprise Desktop 11 may have problems handling keyboard mapping changes, which in turn may cause issues with keyboard functionality inside an HDX session. This can happen when the installed version of the packages is in the range 7.4-5.11.11.1 to 7.4-5.11.15.1.

The workaround is to rollback to the stock SP3 version of the xorg-x11-libX11 package, this will enable keyboard mapping changes to work as normal. For example:

```
rpm -i --force xorg-x11-libX11-7.4-5.9.1
rpm -i --force xorg-x11-libX11-32bit-7.4-5.9.1
rpm -e xorg-x11-libX11-7.4-5.11.15.1
rpm -e xorg-x11-libX11-32bit-7.4-5.11.15.1
```

This needs to be done before a user logs on to the machine – if this is done while a session is active, these settings will not take affect until the user next logs in.

If upgrading from stock SP3, the above xorg-x11-libX11 packages can be locked to the current installed version so that they won’t be changed during the upgrade. Before upgrading, run the following before proceeding with the upgrade as normal:

```
zypper al xorg-x11-libX11
zypper al xorg-x11-libX11-32bit
```

Long session launches may occur when using Linux VDA with a Delivery Controller from XenDesktop v7.1
The slow launch is caused by the presence of CGP settings in the ICA file generated by the v7.1 Delivery Controller. When these settings are present, the Receiver will attempt to establish a connection on TCP port 2598. The default firewall settings on some Linux distributions, such as SLED 12, is to drop the TCP SYN packets, resulting in a timeout and hence a long session launch. The workaround is to configure the firewall on the Linux VDA to reject the TCP SYN on port 2598. This issue has been addressed in newer versions of the Delivery Controller.

Registration fails when Linux VDA is rejoined to the domain
Under certain circumstances, when a Linux VDA is rejoined to the domain and a fresh set of Kerberos keys are generated, the Broker fails to establish a security context with the VDA. This is often caused by the Broker using a cached out-of-date VDA service ticket based on the previous set of Kerberos keys. This won’t stop the VDA from connecting to the Broker, but the Broker will not be able to establish a return security context to the VDA. The usual symptom is that the VDA registration fails.

This problem will eventually resolve itself when the VDA service ticket eventually expires and is renewed, but service tickets are usually long-lived. This could potentially be hours.
The solution is to clear the Broker’s ticket cache. You could simply reboot the Broker or run the following on the Broker from a command prompt as Administrator:

```
klist -li 0x3e4 purge
```

This will purge all service tickets in the LSA cache held by the Network Service principal under which the Citrix Broker Service runs. This will remove service tickets for other VDAs and potentially other services. However, this is harmless – these service tickets will simply be reacquired from the KDC when needed again.