Linux Virtual Delivery Agent 7.12

Jan 25, 2017

This pdf file includes the Linux Virtual Delivery Agent 7.12 documentation. You can save a local copy of this file and use it offline. Use the built-in Search and Bookmark features to find what you need.

You can create Linux virtual desktops and applications based on a RedHat, CentOS, SUSE or Ubuntu distributions. Prepare your Linux virtual machines, install the new software on them, configure your Delivery Controller, and then use Studio to make the desktops and applications available to users.
What's New

Feb 06, 2017

The following new and enhanced features are part of this release of the Linux VDA.

This release provides support for Xauthority. With this functionality, cookie-based access for X Window authorization is now supported by the Linux VDA. For more information, see Configure Xauthority.

Tip

The Xauthority file can be found in the logon user’s home directory, and is used to store credentials in cookies that are used by xauth for the authentication of X sessions. Once an X session is launched, the cookie is used to authenticate connections to that specific display.

This release provides support for IPv6. With this support, the 128-bit addressing schema is now extended to the Linux VDA. For more information, see Configure IPv6.

Support for secure LDAP (LDAPS) is implemented in this version of the Linux VDA. With this support, you can enable the Secure Lightweight Directory Access Protocol for your Active Directory managed domains to provide communication over SSL (Secure Socket Layer)/TLS (Transport Layer Security). For more information, see Configure LDAPS.

Note

When using LDAPS, you must acquire a valid certificate before you can enable secure LDAP. Consider the following guidelines when using secure LDAP certificates:

- Certificates must be issued by an authority trusted by the Linux VDA that will use it to connect to the domain. This authority can be an enterprise certification authority, or a publicly available authority that is trusted by devices running the Linux VDA.
- Certificates must be valid for a long period. A good rule of thumb is that they should be valid for at least 3-6 months to prevent unnecessary disruptions when a certificate expires.
- It’s considered best practice to use a wildcard for the certificate subject name on managed domains. For example, if your domain is named ‘mydomain.com’, the certificate’s subject name should be ‘*mydomain.com’. Additionally set the DNS name to this wildcard name.
- The secure LDAP certificate should be configured for digital signatures and key encipherment.
- The certificate must be valid for SSL server authentication.

This release of the Linux VDA provides administrators with the ability to use SSSD for domain joining of Linux machines. This functionality provides access to different identity and authentication providers as opposed to using the current method of
using winbind (and other methods).

SSSD is a system daemon, whose primary function is to provide access to identify and authenticate remote resources through a common framework that can provide caching and offline support. It provides both PAM and NSS modules. For more information, see Configuring SSSD for RHEL and Configuring SSSD for Ubuntu.

This release of the Linux VDA now provides support for systems running Ubuntu 16.04:

- Ubuntu Linux 16.04 Server
- Ubuntu Linux 16.04 Desktop

In previous releases of the Linux VDA, NIS (Network Information Service) integration with Active Directory was considered an experimental feature. In this release, NIS as an identity provider is supported. For more information, see Integrate NIS with Active Directory.

In this release, Citrix added technical preview for seamless applications to RHEL/CentOS 7.2. No specific installation procedures are required to use this functionality. For more information, see Publish applications.

Easy install is a technical preview feature. It helps users set up the running environment of the Linux VDA by installing the necessary packages and customizing the configuration files automatically. For more information, see Easy install.

Ubuntu Linux is a brand new distribution for the Linux VDA. For SLES 11, gnome-session dependency has been removed.
Fixed issues

Dec 06, 2016
The following issues have been resolved in this release of the Linux VDA:

Linux VDA session logoff during login
The value of Umask was changed from 022 (the default value) to 027 for a special request. This change reduced the read permission for the newly created file, which prevents the Xclient file from being used in the session startup.

[LC6115]

User unable to launch Linux VDA
When a user puts another executable Xhost file into the VDA server, and its location is also in the PATH variable, it causes the wrong Xhost file to be called in the session startup.

[LC6017]
Known Issues

Jan 23, 2017
The following issues have been identified in this release:

The Linux Virtual Delivery Agents (Linux VDA 1.4 and earlier) cannot register with the XenApp and XenDesktop 7.12 brokers when the VDA versions are not the English language version. To work around this issue, use the Linux VDA 7.12.

Ubuntu graphics
In HDX 3D Pro, a black frame might appear around applications after resizing the desktop viewer, or in some cases, the background can appear black.

Printing
Printers created by the Linux VDA printing redirection might not be deleted after logging out of a session.

CDM files are missing when a directory contains numerous files and subdirectories.
This issue might occur if the client side has too many files or directories. It is isolated to Windows Receiver.

UTF-8 encoding support
In this release, only UTF-8 encoding is supported for non-English languages.

Client IME support
The Linux VDA does not support Client IME.

East Asian character input
The Linux VDA does not support East Asian character input.

Citrix Receiver for Android CAPS LOCK state can be reversed when session roaming
The CAPS LOCK state can 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 the Linux VDA using Citrix Receiver for Mac
Citrix Receiver for Mac sends 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.

Slow session launches might occur when using the 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, Citrix Receiver attempts 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 slow 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 the Linux VDA is rejoined to the domain

Under certain circumstances, when the 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 take a long time.

The solution is to clear the Broker's ticket cache. You can 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 be reacquired from the KDC when needed again.

Audio plug-n-play not supported

Citrix recommends that any audio capture device is connected to the client machine before starting to record audio in the ICA session. If a device is attached after the audio recording application has started, the application might become unresponsive. If this issue occurs, restart the application. A similar issue can occur if a capture device is unplugged while recording.

Audio Distortion

Citrix Receiver for Windows 10 might experience audio distortion during audio recording.
Third party notices

Jan 23, 2017

Linux Virtual Desktop Version 7.12

This release of the Linux VDA can include third party software licensed under the terms defined in this document.
The following Linux distributions are supported by the Linux VDA:

- SUSE Linux Enterprise:
  - Desktop 12 Service Pack 1
  - Server 11 Service Pack 4
  - Server 12 Service Pack 1
- Red Hat Enterprise Linux
  - Workstation 6.8
  - Workstation 7.2
  - Server 6.8
  - Server 7.2
- CentOS Linux
  - CentOS 6.8
  - CentOS 7.2
- Ubuntu Linux
  - Ubuntu Desktop 16.04
  - Ubuntu Server 16.04

**Note**

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

**Important**

Gnome and KDE desktops are supported in SUSE, RedHat and CentOS. Unity desktop is supported in Ubuntu only. At least one desktop should be installed.

**Tip**

CentOS Linux is supported since version 1.3. The information contained in the installation article for RHEL is also appropriate for CentOS. For more information, see [Install Linux Virtual Delivery Agent for RHEL](https://docs.citrix.com).

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

- XenDesktop 7.12
The configuration process for Linux VDAs differs slightly from that for Windows VDAs. However, any Delivery Controller farm is capable of brokering both Windows and Linux desktops.

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

The following versions of Citrix Receiver are supported:

- Citrix Receiver for Windows version 4.5 or later
- Citrix Receiver for Linux version 13.4 or later
- Citrix Receiver for Mac OSX version 12.3 or later
- Citrix Receiver for Android version 3.9 or later
- Citrix Receiver for iOS version 7.1 or later
- Citrix Receiver for Chrome version 2.2 (only via Access Gateway)
- Citrix Receiver for HTML5 version 2.2 (only via Access Gateway)

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.

**Tip**
Refer to the hypervisor vendor's documentation for the list of supported platforms.

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

- Samba Winbind
- Quest Authentication Services v4.1 or later
Tip
For the list of supported platforms, see the documentation from the vendors of the Active Directory integration packages.

The following hypervisors, Linux Distributions, and NVIDIA GRID™ GPU are required to support HDX 3D Pro.

**Hypervisors**

The following hypervisors are supported:

- XenServer
- VMware ESX and ESXi

**Linux distributions**

The following Linux distributions support HDX 3D Pro:

- Red Hat Enterprise Linux - Workstation 6.8
- Red Hat Enterprise Linux - Server 6.8
- Red Hat Enterprise Linux - Workstation 7.2
- Red Hat Enterprise Linux - Server 7.2
- CentOS Linux 6.8
- CentOS Linux 7.2
- SUSE Linux Enterprise Desktop 12 Service Pack 1
- SUSE Linux Enterprise Server 12 Service Pack 1
- Ubuntu Linux Desktop 16.04
- Ubuntu Linux Server 16.04

**GPU**

The following GPUs are supported for GPU pass-through:

- NVIDIA GRID™ 3.0 - Tesla M60
- NVIDIA GRID™ - K2

The following GPUs are supported for vGPU:

- NVIDIA GRID™ 3.0 - Tesla M60
- NVIDIA GRID™ 3.0 - Tesla M10
Configure Delivery Controllers

Feb 06, 2017

XenDesktop 7.6 or an earlier version requires the necessary changes to support the Linux VDA. Thus, for these versions of XenDesktop, a hotfix or update script is required. The installation and verification are provided in this article.

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

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

For earlier versions of XenDesktop, you can use the PowerShell script named `Update-BrokerServiceConfig.ps1` to update the Broker Service configuration. This script is available in the following package:

- citrix-linuxvda-scripts.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. Browse to the folder containing the script.
4. Execute the script:

```
.\Update-BrokerServiceConfig.ps1
```

**Tip**

By default, PowerShell is configured to prevent the execution of PowerShell scripts. If the script fails to run, you 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 VDAs 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.

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

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

From the Windows command prompt, log on as a local administrator:

```plaintext
cd "%PROGRAMFILES%\Citrix\Broker\Service\"

findstr EndpointLinux BrokerService.exe.config
```
Installation Overview

Dec 06, 2016
Installing the Linux Virtual Delivery Agent (VDA) follows the same general steps for all supported Linux distributions.

1. Prepare for installation.
2. Prepare the hypervisor.
3. Add the Linux virtual machine (VM) to the Windows domain.
4. Install the Linux VDA.
5. Configure the Linux VDA.
6. Create the machine catalog in XenApp or XenDesktop.
7. Create the delivery group in XenApp or XenDesktop.

Variations and specific commands are documented by distribution.
Easy install

Feb 06, 2017
Easy install helps users set up the running environment of the Linux VDA by installing the necessary packages and customizing the configuration files automatically.

Important
The Easy Install feature is provided as a Technical Preview feature. Consider the following limitations:

- Support is limited to the following distributions:
  - RHEL 6.8 & 7.2
  - CentOS 6.8 & 7.2
  - Ubuntu 16.04
- Winbind and SSSD AD integrations are supported.

To use this feature, follow these steps:

1. Collect necessary installation information.
2. Install the desktop and X Windows systems and configure the package repository on the Linux VDA server.
3. Install the Linux VDA package.
4. Set up the runtime environment for the Linux VDA.

Step 1: Collect information

Collect the following information:

- Hostname – Linux VDA hostname
- IP address of DNS server
- IP address or name of NTP server
- Domain name
- Realm name
- FQDN of domain controller

Step 2: Install components and configure repository

After collecting required system information, install the desktop and X Windows systems, and then configure the package repository on the Linux VDA machine.

Step 3: Install the Linux VDA package

Execute the following commands to set up the environment for the Linux VDA.

For RHEL and CentOS distributions:
sudo yum -y localinstall <PATH>/<Linux VDA RPM>

For Ubuntu distributions:

sudo apt-get install <PATH>/<Linux VDA deb>

Step 4: Set up the runtime environment for the Linux VDA

Execute the following command to set up the running environment for the Linux VDA:

sudo /opt/Citrix/VDA/sbin/ctxinstall.sh

Use the information in this section to troubleshoot issues that might arise from using this feature.

Failure when joining a domain with SSSD

An error condition might occur when attempting to join a domain, with the output resembling (verify logs for screen printing):

Step 6: join Domain! Enter ctxadmin’s password: Failed to join domain: failed to lookup DC info for domain ‘CITRIXLAB.LOCAL’

/var/log/xdl/vda.log:
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'.

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.

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.

Could not register with any controllers. Waiting to try again in 120000 ms. Multi-forest - false

The Citrix Desktop Service failed to register with any controllers in the last 470 minutes.

/var/log/messages:
To resolve this issue:

1. `rm -f /etc/krb5.keytab`
2. `net ads leave SREALM -U $domain-administrator`
3. Delete the machine catalog and delivery group on the DDC
4. Execute `/opt/Citrix/VDA/sbin/ctxinstall.sh`
5. Create the machine catalog and delivery group on the DDC

Ubuntu can launch a session, but is blocked in an empty desktop

This issue occurs when you launch a session, which is then blocked in a blank desktop. In addition, the console of the server OS machine appears in the same state when you log in with domain administrator credentials.

To resolve this issue:

1. `sudo apt-get install unity lightdm`
2. `sudo apt-get update`
3. Add the following line to `/etc/lightdm/lightdm.conf`:
   ```
   greeter-show-manual-login=true
   ```

Ubuntu launches a session, but cannot log on due to missing home directory

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

Tip

The root cause of this issue is that the home directory is not created for the domain administrator.

To resolve this issue:

1. From a command line, enter `pam-auth-update`.
2. In the resulting popup window, verify that Create home directory login is selected.
Session cannot be launched or is quickly terminated with dbus/message bus error

/var/log/messages (for RHEL or 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)
Abort...

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.

Or, alternately for Ubuntu distributions, use the log /var/log/syslog:

Oct 27 04:17:16 Ubuntu16.04 citrix-ctxhdx[8978]: Session started for user CITRIXLAB\ctxadmin.

Oct 27 04:17:18 Ubuntu16.04 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)
Abort...

Oct 27 04:17:18 Ubuntu16.04 gnome-session: aborting...
Some groups or modules do not take effect until after a reboot. When **dbus** or **message bus** error messages appear in the log, Citrix recommends that you reboot the system, then retry.
Install Linux Virtual Delivery Agent for RHEL

Feb 06, 2017

Verify the network configuration

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

Set the 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.

```
HOSTNAME=hostname
```

Assign a loopback address to the 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.

**Note**

The Linux VDA currently does not support NetBIOS name truncation, therefore the hostname must not exceed 15 characters.

**Tip**

Use a-z, A-Z, 0-9, and hyphen (-) characters only. Avoid underscores characters (_), spaces, and other symbols. Do not start a hostname with a number and do not end it with a hyphen.

Check the hostname

Verify that the hostname is set correctly:
This should return only the machine's host name and not its fully qualified domain name (FQDN).

Verify that the FQDN 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:

```
nsllookup domain-controller-fqdn
ping domain-controller-fqdn
nsllookup delivery-controller-fqdn
ping delivery-controller-fqdn
```

If you cannot resolve the FQDN or ping either of these machines, review the steps before proceeding.

**Configure clock synchronization (NTP)**

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 an RHEL 7.x default environment uses the newer Chrony daemon (chronyd) instead. The configuration and operational process between the two services is similar.
Configure NTP service

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

```
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
```

Install OpenJDK

The Linux VDA is dependent on OpenJDK. The runtime environment should have been installed as part of the operating system installation.

Confirm the correct version with:

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

The prepackaged OpenJDK might be an earlier version. 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 the `~/.bashrc` file:

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

Open a new shell and verify the version of Java:

```bash
java --version
```

Tip

To avoid problems, make sure that you installed only OpenJDK version 1.7.0 or 1.8.0. Remove all other versions of Java on your system.

Install PostgreSQL

The Linux VDA requires either PostgreSQL 8.4 or later on RHEL 6.

Install the following packages:

```bash
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`. 
Start PostgreSQL

Configure the service to start on boot, and to start now:

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

```
Start 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
```

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

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

Verify the network configuration

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

Set the 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 a loopback address to the 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.

---

**Note**

The Linux VDA currently does not support NetBIOS name truncation, therefore the hostname must not exceed 15 characters.

---

**Tip**

Use a-z, A-Z, 0-9 and hyphen (-) characters only. Avoid underscores (_), spaces and other symbols. Do not start a hostname with a number and do not end it with a hyphen.

---

Check the hostname

Verify that the hostname is set correctly:

```
hostname
```

This should return only the machine's host name and not its fully qualified domain name (FQDN).

Verify that the FQDN 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

If you cannot resolve the FQDN or ping either of these machines, review the steps before proceeding.

Configure clock synchronization (NTP)

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 an RHEL 7.x default environment uses the newer Chrony daemon (chronyd) instead. The configuration and operational process between the two services is similar.

**Chrony service**

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

```
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:
Install OpenJDK

The Linux VDA is dependent on OpenJDK. The runtime environment should have been installed as part of the operating system installation.

Confirm the correct version with:

```
sudo yum info java-1.8.0-openjdk
```

The prepackaged OpenJDK might be an earlier version. Update to the latest version as required:

```
sudo yum -y update java-1.8.0-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
```

Tip

To avoid problems, make sure that you installed only OpenJDK version 1.8.0. Remove all other versions of Java on your system.
Install PostgreSQL

The Linux VDA requires PostgreSQL version 9.2 or later on RHEL 7.

Install the following packages:

```bash
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`.

```bash
sudo postgresql-setup initdb
```

Start PostgreSQL

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

```bash
sudo systemctl start postgresql
sudo systemctl enable postgresql
```

Check the version of PostgreSQL by using:

```bash
psql --version
```
Verify that the data directory is set using the `psql` command-line utility:

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

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.

**Fix time synchronization on Citrix XenServer**

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/independent_wallclock` file is not present, the following steps are not required.

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

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

This should return the value 1.

**Fix time synchronization on Microsoft Hyper-V**

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 selected.

**Note**

This approach is different from VMware and XenServer, where host time synchronization is disabled to avoid conflicts with NTP. Hyper-V time synchronization can coexist and supplement NTP time synchronization.

**Fix time synchronization on ESX and ESXi**
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 you are 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, clear Synchronize guest time with host.

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

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl

Follow the instructions below for your chosen method.

**Samba Winbind**

Install or update the required packages:

```
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:

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

Configure Winbind Authentication

Configure the machine for Kerberos authentication using Winbind:
sudo authconfig --disablecache --disablesssd --disablesssdauth --enablewinbind --enablewinbindauth --disablewinbindoffline

Where REALM is the Kerberos realm name in uppercase and domain is the short NetBIOS name of the Active Directory domain.

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

--enablekrb5kcdcdns --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 Active Directory user account with permissions to add computers to the domain:
sudo net ads join REALM -U user

Where REALM is the Kerberos realm name in uppercase, 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 that any leading semi-colons from each setting are removed. These changes require restarting the Winbind daemon:

```
sudo /sbin/service winbind restart
```

Tip

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

Open /etc/krb5.conf and change the following setting under the [libdefaults] section from KEYRING to FILE type:
default_ccache_name = FILE:/tmp/krb5cc_%{uid}

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:

```
sudo net ads testjoin
```

Additional domain and computer object information can be verified with:

```
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:

```
sudo 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:
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 that the realm name is used. If this command is successful, no output is displayed.

Verify that the TGT ticket for the machine account has been cached using:

```
sudo klist
```

Examine the machine's account details using:

```
sudo 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, log on locally with a domain user account that has not logged onto the machine previously:
Check that the tickets in the user's Kerberos credential cache are valid and not expired:

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

```
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 Active Directory domain controllers, and have been granted administrative privileges to create computer objects in Active Directory.

**Enable Domain Users to Log on to Linux VDA Machines**

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

1. In the Active Directory Users and Computers management console, open Active Directory 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.

**Note**

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 socket IPC mechanisms used by Quest and prevents domain users from logging on.

Tip
There are a few ways to workaround outlined here.

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

Important
Use this setting carefully. Reenabling SELinux policy enforcement after disabling can cause a complete lockout, even for the root user and other local users.

Configure VAS daemon

Auto-renewal of Kerberos tickets needs to be enabled and disconnected; authentication (offline logon) needs to be disabled:
This sets the renewal interval to 9 hours (32400 seconds) which is an hour less than the default 10 hour ticket lifetime. Set this parameter 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 Active Directory 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 computers to the Active Directory 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:
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 Quest can authenticate domain users using PAM, log on 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:

```
lsof /tmp/krb5cc_uid
```

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

```
exit
```

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

**Centrify DirectControl**

**Join Windows Domain**

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

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

The user parameter is any Active Directory domain user with permissions to join computers to the Active Directory 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.

More comprehensive 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
```

SSSD

Use the following information to set up SSSD; it includes instructions for joining a Linux VDA machine to a Windows domain and provides guidance for configuring Kerberos authentication.

**Note**

If you are using SSSD, follow the instructions contained in this section instead of the information provided by the Add Linux machine to Windows domain section.

**What is SSSD?**

SSSD is a system daemon. It's primary function is to provide access to identify and authenticate remote resources through a common framework that can provide caching and offline support to the system. It provides both PAM and NSS modules, and in the future will support D-BUS based interfaces for extended user information. It also provides a better database to
store local users as well as extended user data.

Setting up SSSD on RHEL and CentOS involves the following:

1. Join the domain and create host keytab with Samba
2. Set up SSSD
3. Configure NSS/PAM
4. Verify the Kerberos configuration
5. Verify user authentication

The Active Directory provider was first introduced with SSSD version 1.9.0. If you are using an older version, follow the instructions provided in configuring the LDAP provider with Active Directory.

The following environments have been tested and verified when using the instructions included in this article:

- RHEL 7.2/CentOS 7.2
- Linux VDA versions 1.3, 1.4, 7.12

SSSD does not provide Active Directory client functions for joining the domain and managing the system keytab file. There are a few methods for achieving this, including:

- adcli
- realmd
- winbind
- samba

The information in this section describes the Samba approach only. For realmd, see the RHEL or CentOS documentation. These steps must be followed before configuring SSSD.

On the Linux client with properly configured files:

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

Configure the machine for Samba and Kerberos authentication:

```
sudo authconfig --smbsecurity=ads --smbworkgroup=domain --smbrealm=REALM --krb5realm=REALM --krb5kdc=fqdn-of-domain
```

Where **REALM** is the Kerberos realm name in uppercase and domain is the short NetBIOS name of the Active Directory domain.

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

Joining the Windows domain requires that your domain controller is reachable and you have an Active Directory user account with permissions to add computers to the domain:

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

Where `REALM` is the Kerberos realm name in uppercase, and `user` is a domain user with permissions to add computers to the domain.

Setting up SSSD consists of the following steps:

- install the `sssd-ad` package on the Linux client machine
- make configuration changes to various files (for example, `sssd.conf`)
- start the `sssd` service:

An example `sssd.conf` configuration (additional options can be added as needed):

```
[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
# 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

Replace ad.example.com, server.ad.example.com with the corresponding values. For more details, see sssd-ad(5) - Linux man page.

Set the file ownership and permissions on sssd.conf:

chown root:root /etc/sssd/sssd.conf

chmod 0600 /etc/sssd/sssd.conf

restorecon /etc/sssd/sssd.conf

RHEL/CentOS

Use authconfig to enable SSSD, install oddjob-mkhomedir to make sure home directory creation works with SELinux:
authconfig --enablesssd --enablesssdauth --enablemkhomedir --update

sudo service sssd start

sudo chkconfig sssd on

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
sudo 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
sudo 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 that the realm name is used. If this command is successful, no output is displayed.

Verify that the TGT ticket for the machine account has been cached using:

```bash
sudo klist
```

Use the `getent` command to verify that the logon format it supported and whether the NSS works:
sudo getent passwd DOMAIN\username

The **DOMAIN** parameter should be the short version domain name. If another logon format from Citrix Receiver is needed, verify by using the `getent` command first.

The supported logon formats are:

- Down-level logon name: **DOMAIN\username**
- UPN: **username@domain.com**
- NetBIOS Suffix format: **username@DOMAIN**

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

```
sudo ssh localhost -l DOMAIN\username
id -u
```

Check that a corresponding Kerberos credential cache file was created for the **uid** returned by the command:

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

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

```
klist
```

Install NVIDIA GRID drivers
To enable HDX 3D Pro, additional installation steps are required to install the requisite graphics drivers on the hypervisor as well as on the VDA machines.

Configure the following:

1. Citrix XenServer
2. VMware ESX

Follow the instructions for your chosen hypervisor.

**Citrix XenServer**

This detailed section walks through the install and configuration of the NVIDIA GRID drivers on Citrix XenServer.

**VMware ESX**

Follow the information contained in this guide to install and configure the NVIDIA GRID drivers for VMware ESX.

**VDA Machines**

Follow these steps to install and configure the drivers for each of the Linux VM guests:

1. Before starting, ensure that the Linux VM is shut down.
2. In XenCenter, add a GPU in GPU Passthrough mode to the VM.
3. Start the RHEL VM.

To prepare the machine for the NVIDIA GRID drivers, the following steps are required:

```bash
yum install gcc

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

systemctl set-default multi-user.target
```

Once complete, follow the steps in the Red Hat Enterprise Linux document to install the NVIDIA GRID driver.

**Note**

During the GPU driver install, select the default ('no') for each question.

**Important**

Once GPU Pass through has been enabled, the Linux VM is no longer accessible via XenCenter so you need to use SSH to connect.
Set the correct configuration for the card:

```
/etc/X11/ctx-nvidia.sh
```

To take advantage of large resolutions and multi-monitor capabilities, you need a valid NVIDIA license. To apply the license, follow the product documentation from “GRID Licensing Guide.pdf - DU-07757-001 September 2015”.

1. Uninstall the old version

If you have previously installed a version of the Linux VDA earlier than v1.0, uninstall it before installing the new version.

(a) Stop the Linux VDA services:
(b) Uninstall the package:

```
sudo rpm -e XenDesktopVDA
```

**Note**
Upgrading from the latest two versions is supported.

**Note**
Starting with version 1.3, the installation path changed. In previous releases, installation components were located in `/usr/local/`; the new location is `/opt/Citrix/VDA/`.

To execute a command, the full path is needed; alternately, you can add `/opt/Citrix/VDA/sbin` and `/opt/Citrix/VDA/bin` to the system path.

2. Install the Linux VDA

Install the Linux VDA software using Yum:

**For RHEL 6/CentOS 6:**

```
sudo yum install -y XenDesktopVDA-7.12.0.375-1.el6_8.x86_64.rpm
```

**For RHEL 7/CentOS 7:**

```
Install the Linux VDA software using the RPM package manager; before doing so, you must resolve the following dependencies:

For RHEL 6/CentOS 6:

```bash
sudo rpm -i XenDesktopVDA-7.12.0.375-1.el6_8.x86_64.rpm
```

RPM dependency list for RHEL 6:

- `postgresql-jdbc >= 8.4`
- `postgresql-server >= 8.4`
- `java-1.7.0-openjdk >= 1.7.0`
- `ImageMagick >= 6.5.4.7`
- `GConf2 >= 2.28.0`
- `system-config-firewall-base >= 1.2.27`
- `policycoreutils-python >= 2.0.83`

For RHEL 7/CentOS 7:

```bash
sudo rpm -i XenDesktopVDA-7.12.0.375-1.el7_2.x86_64.rpm
```

RPM dependency list for RHEL 7:

- `postgresql-jdbc >= 8.4`
- `postgresql-server >= 8.4`
- `java-1.7.0-openjdk >= 1.7.0`
- `ImageMagick >= 6.5.4.7`
- `GConf2 >= 2.28.0`
- `system-config-firewall-base >= 1.2.27`
- `policycoreutils-python >= 2.0.83`
policycoreutils-python >= 2.0.83

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.0.9

ConsoleKit >= 0.4.1

dbus >= 1.2.24

dbus-x11 >= 1.2.24

gnome-session >= 2.28.0

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

openmotif >= 2.3.3

pam >= 1.1.1

util-linux-ng >= 2.17.2

bash >= 4.1

findutils >= 4.4

gawk >= 3.1

sed >= 4.2

cups >= 1.4.0

foomatic >= 4.0.0

openldap >= 2.4
cyrus-sasl >= 2.1

libxml2 >= 2.7

RPM dependency list for RHEL 7:

postgresql-server >= 9.2

postgresql-jdbc >= 9.2

java-1.8.0-openjdk >= 1.8.0

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

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

motif >= 2.3.4
<table>
<thead>
<tr>
<th>Package</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>pam</td>
<td>&gt;= 1.1.8</td>
</tr>
<tr>
<td>util-linux</td>
<td>&gt;= 2.23.2</td>
</tr>
<tr>
<td>bash</td>
<td>&gt;= 4.2</td>
</tr>
<tr>
<td>findutils</td>
<td>&gt;= 4.5</td>
</tr>
<tr>
<td>gawk</td>
<td>&gt;= 4.0</td>
</tr>
<tr>
<td>sed</td>
<td>&gt;= 4.2</td>
</tr>
<tr>
<td>cups</td>
<td>&gt;= 1.6.0</td>
</tr>
<tr>
<td>foomatic-filters</td>
<td>&gt;= 4.0.9</td>
</tr>
<tr>
<td>openldap</td>
<td>&gt;= 2.4</td>
</tr>
<tr>
<td>cyrus-sasl</td>
<td>&gt;= 2.1</td>
</tr>
<tr>
<td>cyrus-sasl-gssapi</td>
<td>&gt;= 2.1</td>
</tr>
<tr>
<td>libxml2</td>
<td>&gt;= 2.9</td>
</tr>
</tbody>
</table>

**Important**

The Linux VDA package requires a specific Xorg version.

For RHEL 6.8 and RHEL 7.2, the Linux VDA requires Xorg-x11-server-Xorg Version 1.17; do not upgrade this package.

3. Upgrade the Linux VDA (optional)

If you have previously installed Versions 1.3 or 1.4 of the Linux VDA, upgrade the Linux VDA software using Yum:

For RHEL 6/CentOS 6:
Upgrade the Linux VDA software using the RPM package manager:

For RHEL 6/CentOS 6:

```
sudo rpm -U XenDesktopVDA-7.12.0.375-1.el6_8.x86_64.rpm
```

For RHEL 7/CentOS 7:

```
sudo rpm -U XenDesktopVDA-7.12.0.375-1.el7_2.x86_64.rpm
```

Important

You must reboot the Linux VDA machine after upgrading.

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

Start the Linux VDA

To start the Linux VDA services:
Stop the Linux VDA

To stop the Linux VDA services:

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

Restart the Linux VDA

To restart the Linux VDA services:

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

Check the status of the Linux VDA

To check the running state of the Linux VDA services:

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

sudo /sbin/service ctxhdx status

Important

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

You can run the script manually with prompting, or automatically with preconfigured responses. Review Help about this script before proceeding:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

Prompted configuration

Run a manual configuration with prompted questions:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Automated configuration

For an automated install, provide the options required by the setup script with environment variables. If all required variables are present, the script does not prompt for any information.

Supported environment variables include:

- `CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N` - The Linux VDA supports specifying a Delivery Controller name using a DNS CNAME record. This is typically set to N.
- `CTX_XDL_DDC_LIST` = list-ddc-fqdns – The Linux VDA requires a space-separated list of Delivery Controller Fully Qualified Domain Names (FQDNs) to use for registering with a Delivery Controller. At least one FQDN or CNAME alias must be specified.

- `CTX_XDL_VDA_PORT` = port-number – The Linux VDA communicates with Delivery Controllers using a TCP/IP port. This is typically port 80.

- `CTX_XDL_REGISTER_SERVICE` = Y | N - The Linux Virtual Desktop services support starting during boot. This is typically set to Y.

- `CTX_XDL_ADD_FIREWALL_RULES` = Y | N – The Linux Virtual Desktop services require incoming network connections to be allowed through the system firewall. You can automatically open the required ports (by default ports 80 and 1494) in the system firewall for the Linux Virtual Desktop. This is typically set to Y.

- `CTX_XDL_AD_INTEGRATION` = 1 | 2 | 3 | 4 – The Linux VDA requires Kerberos configuration settings to authenticate with the Delivery Controllers. The Kerberos configuration is determined from the installed and configured Active Directory integration tool on the system. Specify the supported Active Directory integration method to use:
  
  - 1 – Samba Winbind
  - 2 – Quest Authentication Service
  - 3 – Centrify DirectControl
  - 4 – SSSD

- `CTX_XDL_HDX_3D_PRO` = Y | N – Linux Virtual Desktop supports HDX 3D Pro, a set of graphics acceleration technologies designed to optimize the virtualization of rich graphics applications. HDX 3D Pro requires a compatible NVIDIA Grid graphics card to be installed. If HDX 3D Pro is selected, the Virtual Delivery Agent is configured for VDI desktops (single-session) mode – (i.e. `CTX_XDL_VDI_MODE=Y`). This is not supported on SUSE. Ensure this value is set to N.

- `CTX_XDL_VDI_MODE` = Y | N - Whether to configure the machine as a dedicated desktop delivery model (VDI) or hosted shared desktop delivery model. For HDX 3D Pro environments, set this to Y. This is typically set to N.

- `CTX_XDL_AD_INTEGRATION` = dns-name – The Linux VDA discovers LDAP servers using DNS, querying for LDAP service records. To limit the DNS search results to a local site, specify a DNS site name. This is typically empty [none].

- `CTX_XDL_LDAP_LIST` = list-ldap-servers – The Linux VDA by default queries DNS to discover LDAP servers. However if DNS cannot provide LDAP service records, you can provide a space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with LDAP port (e.g. ad1.mycompany.com:389). This is typically empty [none].

- `CTX_XDL_SEARCH_BASE` = search-base – The Linux VDA by default queries LDAP using a search base set to the root of the Active Directory Domain (e.g. DC=mycompany,DC=com). However to improve search performance, you can specify a search base (e.g. OU=VDI,DC=mycompany,DC=com). This is typically empty [none].

- `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 set to 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_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-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh

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

Alternatively, you can specify all parameters with a single command:
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \n
CTX_XDL_DDC_LIST=list-ddc-fqdns \n
CTX_XDL_VDA_PORT=port-number \n
CTX_XDL_REGISTER_SERVICE=Y|N \n
CTX_XDL_ADD_FIREWALL_RULES=Y|N \n
CTX_XDL_AD_INTEGRATION=1|2|3|4 \n
CTX_XDL_HDX_3D_PRO=Y|N \n
CTX_XDL_VDI_MODE=Y|N \n
CTX_XDL_SITE_NAME=dns-name \n
CTX_XDL_LDAP_LIST=list-ldap-servers \n
CTX_XDL_SEARCH_BASE=search-base \n
CTX_XDL_START_SERVICE=Y|N \n
/opt/Citrix/VDA/sbin/ctxsetup.sh

Remove configuration changes

In some scenarios, you might have 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 /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
To remove configuration changes:

```bash
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

**Important**

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 display errors on the console, with additional information written to the configuration log file `/tmp/xdl.configure.log`.

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

The process for creating machine catalogs and adding Linux VDA machines is very similar to the traditional Windows VDA approach. For a more detailed description of how to complete these tasks, see Create Machine Catalogs and Manage Machine Catalogs.

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

- For the 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 that machines are set as not power managed.
- Because 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.

**Note**

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 XenDesktop single user per machine delivery model.

**Tip**


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.

The process for creating a delivery group and adding machine catalogs containing Linux VDA machines is almost identical to Windows VDA machines. For a more detailed description of how to complete these tasks, see Create Delivery Groups.

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

- For the delivery type, select Desktops or Applications.
- Ensure that the AD users and groups you select have been properly configured to log on 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.

**Important**

Publishing applications is supported with Linux VDA version 1.4 and later. However, the Linux VDA does not support the delivery of desktops and apps to the same machine.

The Citrix documentation for creating machine catalogs and delivery groups is referenced below:

- XenDesktop 7.12
- XenDesktop 7.11
- XenDesktop 7.9
- XenDesktop 7.8
- XenDesktop 7.7
- XenDesktop 7.6
- XenDesktop 7.5
- XenDesktop 7.1

Earlier versions of XenDesktop are not supported.
Install Linux Virtual Delivery Agent for SUSE

Feb 06, 2017

1. Launch YaST tool

The SUSE Linux Enterprise YaST tool is used for configuring all aspects of the operating system.

To launch the text-based YaST tool:

```
su -
yast
```

Alternatively, launch the UI-based YaST tool:

```
su -
yast2 &
```

The following sections provide information on configuring the various networking settings and services used by the Linux VDA. Configuring networking should be carried out via the YaST tool, not via other methods such as Network Manager. These instructions are based on using the UI-based YaST tool; the text-based YaST tool can be used but has a different method of navigation which is not documented here.

Configure hostname and DNS

1. Open YaST Network Settings.
2. SLED 12 Only: On the Global Options tab, change the Network Setup Method to Wicked Service.
3. Open the Hostname/DNS tab.
4. Clear Change hostname via DHCP.
5. Check Assign Hostname to Loopback IP.
6. Edit the following to reflect your networking setup:
- Hostname – Add the DNS hostname of the machine.
- Domain Name – Add the DNS domain name of the machine.
- Name Server – Add the IP address of the DNS server. This is typically the IP address of the AD Domain Controller.
- Domain Search list – Add the DNS domain name.

**Note**

The Linux VDA currently does not support NetBIOS name truncation, therefore the hostname must not exceed 15 characters.

**Tip**

Use a-z, 0-9 and hyphen (-) characters only. Avoid underscores characters (_), spaces and other symbols. Do not start a hostname with a number and do not end with a hyphen.

**Disable multicast DNS**

On SLED only, the default settings have multicast DNS (mDNS) enabled, which can lead to inconsistent name resolution results. mDNS is not enabled on SLES by default, so no action is required.

To disable mDNS, edit `/etc/nsswitch.conf` and change the line containing:

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

To:

```
hosts: files dns
```

**Check the hostname**

Verify that the hostname is set correctly:
This should return only the machine's host name and not its fully qualified domain name (FQDN).

Verify that the FQDN is set correctly:

```
hostname
```

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:

```
nsllookup domain-controller-fqdn
ping domain-controller-fqdn
nsllookup delivery-controller-fqdn
ping delivery-controller-fqdn
```

If you cannot resolve the FQDN or ping either of these machines, review the steps before proceeding.

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, maintaining time using a remote NTP service is preferred. Some changes might be required to the default NTP settings:

1. Open YaST NTP Configuration and select the **General Settings** tab.
2. In the Start NTP Daemon section, check **Now and on Boot**.
3. If present, select the **Undisciplined Local Clock (LOCAL)** item and click **Delete**.
4. Add an entry for an NTP server by clicking **Add**.
5. Select the **Server Type** and click **Next**.
6. Enter the DNS name of the NTP server in the Address field. This service is normally hosted on the Active Directory domain controller.
7. Leave the Options field unchanged.
8. Click **Test** to check that the NTP service is reachable.
9. Click **OK** through the set of windows to save the changes.

**Note**

For SLES 12 implementations, if the NTP daemon fails to start, this might be due to a known SUSE issue with AppArmor policies. Follow the resolution [here](#) for additional information.

The Linux VDA software for SUSE Linux Enterprise is dependent on the following packages:

- **PostgreSQL**
  - SLED/SLES 11: Version 9.1 or later
  - SLED/SLES 12: Version 9.3 or later
- **OpenJDK 1.7.0**
- **OpenMotif Runtime Environment 2.3.1 or later**
- **Cups**
  - SLED/SLES 11: Version 1.3.7 or later
  - SLED/SLES 12: Version 1.6.0 or later
- **Foomatic filters**
  - SLED/SLES 11: Version 3.0.0 or later
  - SLED/SLES 12: Version 1.0.0 or later
- **ImageMagick**
  - SLED/SLES 11: Version 6.4.3.6 or later
  - SLED/SLES 12: Version 6.8 or later

**Add repositories**

Some required packages are not available in all SUSE Linux Enterprise repositories:

- **SLED 11**: PostgreSQL is available for SLES 11 but not SLED 11.
- **SLES 11**: OpenJDK and OpenMotif are available for SLED 11 but not SLES 11.
- **SLED 12**: PostgreSQL is available for SLES 12 but not SLED 12. ImageMagick is available via the SLE 12 SDK ISO or online repository.
- **SLES 12**: There are no issues; all packages are available. ImageMagick is available via the SLE 12 SDK ISO or online repository.

To resolve this, the recommended approach is to obtain missing packages from the media for the alternate edition of SLE from which you are installing. That is, on SLED install missing packages from the SLES media, and on SLES install missing packages from the SLED media. The approach described below mounts both SLED and SLES ISO media files and adds repositories.
<table>
<thead>
<tr>
<th></th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SLED 11</strong></td>
<td><code>sudo mkdir -p /mnt/sles</code> &lt;br&gt; <code>sudo mount -t iso9660 \ path-to-iso/SLES-11-SP4-DVD-x86_64-GM-DVD1.iso /mnt/sles</code> &lt;br&gt; <code>sudo zypper ar -f /mnt/sles sles</code></td>
</tr>
<tr>
<td><strong>SLES 11</strong></td>
<td><code>sudo mkdir -p /mnt/sled</code> &lt;br&gt; <code>sudo mount -t iso9660 \ path-to-iso/SLED-11-SP4-DVD-x86_64-GM-DVD1.iso /mnt/sled</code> &lt;br&gt; <code>sudo zypper ar -f /mnt/sled sled</code></td>
</tr>
<tr>
<td><strong>SLED 12</strong></td>
<td><code>sudo mkdir -p /mnt/sles</code> &lt;br&gt; <code>sudo mount -t iso9660 \ path-to-iso/SLES-12-SP1-DVD-x86_64-GM-DVD1.iso /mnt/sles</code> &lt;br&gt; <code>sudo zypper ar -f /mnt/sles sles</code></td>
</tr>
<tr>
<td><strong>SLED/SLES 12</strong></td>
<td><code>sudo mkdir -p /mnt/sdk</code> &lt;br&gt; <code>sudo mount -t iso9660 \ path-to-iso/SLE-12-SP1-SDK-DVD-x86_64-GM-DVD1.iso /mnt/sdk</code> &lt;br&gt; <code>sudo zypper ar -f /mnt/sdk sdk</code></td>
</tr>
</tbody>
</table>

**Install Kerberos client**

Install the Kerberos client for mutual authentication between the Linux VDA with the XenDesktop Controllers:

```
sudo zypper install krb5-client
```

The Kerberos client configuration is dependent on which Active Directory integration approach is used, which is described later.

**Install OpenJDK**
The Linux VDA dependent on OpenJDK 1.7.0.

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

<table>
<thead>
<tr>
<th>OS</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| SLED | On SLED, the Java runtime environment should have been installed with the operating system. Confirm this with:  
  
  ```
sudo zypper info java-1_7_0-openjdk
  ```  
  Update to the latest version if status is reported as out-of-date:  
  
  ```
sudo zypper update java-1_7_0-openjdk
  ```  
  Check the Java version:  
  
  ```
java -version
  ``` |
| SLES | On SLES, the Java runtime environment needs to be installed:  
  
  ```
sudo zypper install java-1_7_0-openjdk
  ```  
  Check the Java version:  
  
  ```
java -version
  ``` |

**Install PostgreSQL**

<table>
<thead>
<tr>
<th>OS</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| SLED/SLES 11 | Install the packages:  
  
  ```
sudo zypper install libecpg6
sudo zypper install postgresql-init
sudo zypper install postgresql
sudo zypper install postgresql-server
sudo zypper install postgresql-jdbc
  ```  
  Some post-installation steps are required to initialize the database service and ensure PostgreSQL starts on boot:  
  
  ```
sudo /sbin/insserv postgresql
sudo /etc/init.d/postgresql restart
  ``` |
| SLED/SLES 12 | sudo zypper install postgresql-init  
sudo zypper install postgresql-server  
sudo zypper install postgresql-jdbc  
Post-installation steps are required to initialize the database service and ensure PostgreSQL starts on boot:  
sudo systemctl enable postgresql  
sudo systemctl restart postgresql  
Database files will reside under /var/lib/pgsql/data. |
|-------------|
| SLED 11     | Remove the following packages:  
sudo zypper rr sles  
sudo umount /mnt/sles  
sudo rmdir /mnt/sles |
| SLES 11     | Remove the following packages:  
sudo zypper rr sled  
sudo umount /mnt/sled  
sudo rmdir /mnt/sled |
| SLED 12     | Remove the following packages:  
sudo zypper rr sles  
sudo umount /mnt/sles  
sudo rmdir /mnt/sles |
| SLED/SLES 12| Remove the following packages:  
sudo zypper rr sdk  
sudo umount /mnt/sdk  
sudo rmdir /mnt/sdk |

Remove repositories

With dependent packages installed, the alternative edition repositories setup earlier can now be removed and the media unmounted:
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.

**Fix time synchronization on Citrix XenServer**

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/independent_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:
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.

**Fix time synchronization on Microsoft Hyper-V**

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 selected.

**Note**

This approach is different from VMware and XenServer, where host time synchronization is disabled to avoid conflicts with NTP. Hyper-V time synchronization can coexist and supplement NTP time synchronization.

**Fix time synchronization on ESX and ESXi**
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 you are 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, clear **Synchronize guest time with host**.

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

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

Follow the instructions below for your chosen method.

**Samba Winbind**

**Join Windows Domain**

This requires that your domain controller is reachable and you have an Active Directory user account with permissions to add machines to the domain:

1. Open YaST Windows Domain Membership.
2. Make the following changes:
   - Set the Domain or Workgroup to the name of your Active Directory domain or the IP address of the domain controller. Ensure the domain is entered in uppercase.
   - Check Also Use SMB information for Linux Authentication.
   - Check Create Home Directory on Login.
   - Check Single Sign-on for SSH.
   - Ensure Offline Authentication is not checked. This option is not compatible with the Linux VDA.
3. Click **OK**. If prompted to install some packages, click **Install**.
4. If a domain controller is found, it will ask whether you want to join the domain. Click **Yes**.
5. When prompted, enter the credentials of a domain user with permission to add computers to the domain and click **OK**.
6. A message indicating success is displayed.
7. If prompted to install some samba and krb5 packages, click **Install**.
YaST might have indicated that these changes will require some services to be restarted or the machine needs to be rebooted. It is advisable to reboot:

```
su -
```

```
reboot
```

**SLED/SLES 12 Only: Patch Kerberos credential cache name**

SLED/SLES 12 has changed the default Kerberos credential cache name specification from the usual `FILE:/tmp/krb5cc_%{uid}` to `DIR:/run/user/%{uid}/krb5cc`. This new DIR caching method is not compatible with the Linux VDA and must be manually changed. As root, edit `/etc/krb5.conf` and add the following setting under the `[libdefaults]` section if not set:

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

**Verify domain membership**

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

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

```
sudo net ads testjoin
```

Verify additional domain and computer object information with:

```
sudo net ads info
```
Verify the 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:

```
sudo 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:

```
sudo 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 is displayed.

Verify that the TGT ticket for the machine account has been cached using:

```
sudo klist
```

Examine the machine account details using:

```
sudo 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, log on 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 Active Directory domain controllers, and have been granted administrative privileges to create computer objects in Active Directory.

**Enable Domain Users to Log on to Linux VDA Machines**

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

1. In the Active Directory Users and Computers management console, open Active Directory 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.

**Note**

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**

**Configure VAS daemon**

Auto-renewal of Kerberos tickets needs to be enabled and disconnected; authentication (offline logon) needs to be disabled:
This sets the renewal interval to 9 hours (32400 seconds) which is an hour less than the default 10 hour ticket lifetime. Set this parameter to a lower value on systems with a shorter Kerberos 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 Active Directory 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 computers to the Active Directory 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:
sudo /opt/quest/bin/vastool info domain

If the machine is joined to a domain, the domain name is returned. 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 Quest can authenticate domain users using PAM, log on 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 user's Kerberos credential cache are valid and not expired:
Exit the session:

```
exit
```

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

**Centrify DirectControl**

**Join Windows Domain**

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

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

The `user` parameter is any Active Directory domain user with permissions to join computers to the Active Directory 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.

More comprehensive system and diagnostic information is available using:

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

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

```bash
adinfo --test
```

**Uninstall the old version**

If you have previously installed a version of the Linux VDA older than V. 1.1, uninstall it before installing the new version.

(a) Stop the Linux VDA services:

```bash
sudo /sbin/service ctxvda stop
sudo /sbin/service ctxhdx stop
```
(b) Uninstall the package:

```
sudo rpm -e XenDesktopVDA
```

**Important**

Upgrading from the latest two versions is supported.

**Note**

Starting with Version 1.3, the installation path has changed. In previous releases, installation components were located in `/usr/local/`; the new location is `/opt/Citrix/VDA/`.

To execute a command, the full path is needed; alternately, you can add `/opt/Citrix/VDA/sbin` and `/opt/Citrix/VDA/bin` to the system path.

Install the Linux VDA

Install the Linux VDA software using Zypper:

**For SUSE 11:**

```
sudo zypper install XenDesktopVDA-7.12.0.375-1.sle11_4.x86_64.rpm
```

**For SUSE 12:**

```
sudo zypper install XenDesktopVDA-7.12.0.375-1.sle12_1.x86_64.rpm
```

Install the Linux VDA software using the RPM package manager; before doing so, you must resolve the following
dependencies before installation:

For SUSE 11:

```
sudo rpm -i XenDesktopVDA-7.12.0.375-1.sle11_4.x86_64.rpm
```

For SUSE 12:

```
sudo rpm -i XenDesktopVDA-7.12.0.375-1.sle12_1.x86_64.rpm
```

Upgrade the Linux VDA

If you have previously installed v1.2 or v1.3 of the Linux VDA, upgrade the Linux VDA software using the RPM package manager:

For SUSE 11:

```
sudo rpm -U XenDesktopVDA-7.12.0.375-1.sle11_4.x86_64.rpm
```

For SUSE 12:

```
sudo rpm -U XenDesktopVDA-7.12.0.375-1.sle12_1.x86_64.rpm
```

RPM Dependency list for SUSE 11

```
postgresql-server >= 9.1.9
```
postgresql-server >= 9.1.9

postgresql-jdbc >= 9.1

java-1_7_0-openjdk >= 1.7.0.6

ImageMagick >= 6.4.3.6

ConsoleKit >= 0.2.10

dbus-1 >= 1.2.10

dbus-1-x11 >= 1.2.10

xorg-x11-libXpm >= 7.4

xorg-x11-libs >= 7.4

openmotif-libs >= 2.3.1

pam >= 1.1.5

libdrm >= 2.4.41

libpixman-1-0 >= 0.24.4

Mesa >= 9.0

openssl >= 0.9.8j

xorg-x11 >= 7.4

xorg-x11-fonts-core >= 7.4

xorg-x11-libXau >= 7.4

xorg-x11-libXdmcp >= 7.4

bash >= 3.2
findutils >= 4.4

gawk >= 3.1

sed >= 4.1

cups >= 1.3.7

foomatic-filters >= 3.0.0

openldap2 >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.7

RPM Dependency list for SUSE 12:

postgresql-server >= 9.3

postgresql-jdbc >= 9.2

java-1.7.0-openjdk >= 1.7.0

ImageMagick >= 6.8

dbus-1 >= 1.8.8

dbus-1-x11 >= 1.8.8

libXpm4 >= 3.5.11

libXrandr2 >= 1.4.2
libXtst6 >= 1.2.2
motif >= 2.3
pam >= 1.1.8
bash >= 4.2
findutils >= 4.5
gawk >= 4.1
sed >= 4.2
cups >= 1.6.0
cups-filters-foomatic-rip >= 1.0.0
openldap2 >= 2.4
cyrus-sasl >= 2.1
cyrus-sasl-gssapi >= 2.1
libxml2 >= 2.9

Important
You must reboot the Linux VDA machine after upgrading.

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

Start the Linux VDA

To start the Linux VDA service:
Stop the Linux VDA

To stop the Linux VDA service:

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

Restart the Linux VDA

To restart the Linux VDA service:

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

Check the Linux VDA status

To check the status of the Linux VDA:

```
sudo /sbin/service ctxvda start
```
After installing the package, you must configure the Linux VDA by running the `ctxsetup.sh` script. If you have upgraded the package, you must run the `ctxsetup.sh` script to finalize your upgrade. Before making any changes, this script will verify the environment and ensure all dependencies are installed. If necessary, you can rerun this script at any time to change settings.

You can run the script manually with prompting, or automatically with preconfigured responses. Review Help about this script before proceeding:

```bash
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

**Prompted configuration**

Run a manual configuration with prompted questions:

```bash
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

**Automated configuration**

For an automated install, provide the options required by the setup script with environment variables. If all required variables are present, the script does not prompt for any information.

Supported environment variables include:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N** - The Linux VDA supports specifying a Delivery Controller name using a DNS CNAME record. This is typically set to N.
- **CTX_XDL_DDC_LIST = list-ddc-fqdns** - The Linux VDA requires a space-separated list of Delivery Controller Fully Qualified Domain Names (FQDNs) to use for registering with a Delivery Controller. At least one FQDN or CNAME alias must be specified.
- **CTX_XDL_VDA_PORT = port-number** - The Linux VDA communicates with Delivery Controllers using a TCP/IP port.
This is typically port 80.

- CTX_XDL_REGISTER_SERVICE = Y | N - The Linux Virtual Desktop services support starting during boot. This is typically set to Y.
- CTX_XDL_ADD_FIREWALL_RULES = Y | N – The Linux Virtual Desktop services require incoming network connections to be allowed through the system firewall. You can automatically open the required ports (by default ports 80 and 1494) in the system firewall for the Linux Virtual Desktop. This is typically set to Y.
- CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 | 4 – The Linux VDA requires Kerberos configuration settings to authenticate with the Delivery Controllers. The Kerberos configuration is determined from the installed and configured Active Directory integration tool on the system. Specify the supported Active Directory integration method to use:
  1 – Samba Winbind
  2 – Quest Authentication Service
  3 – Centrify DirectControl
  4 – SSSD
- CTX_XDL_HDX_3D_PRO= Y | N – Linux Virtual Desktop supports HDX 3D Pro, a set of graphics acceleration technologies designed to optimize the virtualization of rich graphics applications. HDX 3D Pro requires a compatible NVIDIA Grid graphics card to be installed. If HDX 3D Pro is selected, the Virtual Delivery Agent is configured for VDI desktops (single-session) mode – (i.e. CTX_XDL_VDI_MODE=Y). This is not supported on SUSE. Ensure this value is set to N.
- CTX_XDL_VDI_MODE = Y | N - Whether to configure the machine as a dedicated desktop delivery model (VDI) or hosted shared desktop delivery model. For HDX 3D Pro environments, set this to Y. This is typically set to N.
- CTX_XDL_SITE_NAME = dns-name – The Linux VDA discovers LDAP servers using DNS, querying for LDAP service records. To limit the DNS search results to a local site, specify a DNS site name. This is typically empty [none].
- CTX_XDL_LDAP_LIST = list-ldap-servers – The Linux VDA by default queries DNS to discover LDAP servers. However if DNS cannot provide LDAP service records, you can provide a space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with LDAP port (e.g. ad1.mycompany.com:389). This is typically empty [none].
- CTX_XDL_SEARCH_BASE = search-base – The Linux VDA by default queries LDAP using a search base set to the root of the Active Directory Domain (e.g. DC=mycompany,DC=com). However to improve search performance, you can specify a search base (e.g. OU=VDI,DC=mycompany,DC=com). This is typically empty [none].
- 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 set to Y.

Note

HDX 3D Pro is not currently available on SUSE.

Set the environment variable and run the configure script:

```
```

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.88
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-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh

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

Alternatively, you can specify all parameters with a single command:
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \n
CTX_XDL_DDC_LIST=list-ddc-fqdns \n
CTX_XDL_VDA_PORT=port-number \n
CTX_XDL_REGISTER_SERVICE=Y|N \n
CTX_XDL_ADD_FIREWALL_RULES=Y|N \n
CTX_XDL_AD_INTEGRATION=1|2|3|4 \n
CTX_XDL_HDX_3D_PRO=Y|N \n
CTX_XDL_VDI_MODE=Y|N \n
CTX_XDL_SITE_NAME=dns-name \n
CTX_XDL_LDAP_LIST=list-ldap-servers \n
CTX_XDL_SEARCH_BASE=search-base \n
CTX_XDL_START_SERVICE=Y|N \n
/opt/Citrix/VDA/sbin/ctxsetup.sh

Remove configuration changes

In some scenarios, you might have 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
```

**Important**

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 display errors on the console, with additional information written to a configuration log file:

```
/tmp/xdl.configure.log
```

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

The process for creating machine catalogs and adding Linux VDA machines is very similar to the traditional Windows VDA approach. For a more detailed description of how to complete these tasks, see Create Machine Catalogs and Manage Machine Catalogs.

For creating machine catalogs that contain Linux VDA machines, there are a few restrictions that differentiate 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.

**Note**
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 XenDesktop single user per machine delivery model.

**Tip**

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.

The process for creating a delivery group and adding machine catalogs containing Linux VDA machines is almost identical to Windows VDA machines. For a more detailed description of how to complete these tasks, see Create Delivery Groups.

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

- For delivery type, select Desktops or Applications.
- Ensure the AD users and groups you select have been properly configured to log on 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.

**Important**

Publishing applications is supported with Linux VDA version 1.4 and later. However, the Linux VDA does not support the delivery of desktops and apps to the same machine.

The Citrix documentation for creating machine catalogs and delivery groups is referenced below:

- XenDesktop 7.12
- XenDesktop 7.11
- XenDesktop 7.9
- XenDesktop 7.8
- XenDesktop 7.7
- XenDesktop 7.6
- XenDesktop 7.5
- XenDesktop 7.1

Earlier versions of XenDesktop are not supported.
Install Linux Virtual Delivery Agent for Ubuntu

Feb 06, 2017

Verify the network configuration

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

Set the 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.

```
hostname
```

Assign a loopback address to the 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
```

For example:

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

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

Note

The Linux VDA currently does not support NetBIOS name truncation, therefore the hostname must not exceed 15 characters.

Tip

Use a-z, A-Z, 0-9 and hyphen (-) characters only. Avoid underscore characters (_), spaces and other symbols. Do not start a hostname with a number and do not end with a hyphen.

Check the hostname

Verify that the hostname is set correctly:
hostname

This should return only the machine's host name and not its fully qualified domain name (FQDN).

Verify that the FQDN is set correctly:

```
hostname -f
```

This should return the machine's FQDN.

**Disable multicast DNS**

The default settings have multicast DNS (mDNS) enabled, which can lead to inconsistent name resolution results.

To disable mDNS, edit `/etc/nsswitch.conf` and change the line containing:

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

To:

```
hosts: files dns
```

**Check name resolution and service reachability**

Verify that you can resolve the FQDN and ping the domain controller and XenDesktop Delivery Controller:
If you cannot resolve the FQDN or ping either of these machines, review the steps before proceeding.

**Configure clock synchronization (chrony)**

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.

**Install chrony:**

```bash
apt-get install chrony
```

As root, edit `/etc/chrony/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` or `pool` entries listed including loopback IP address, localhost, and public server `*.pool.ntp.org` entries.

Save changes and restart the Chrony daemon:
Install OpenJDK
The Linux VDA is dependent on OpenJDK. The runtime environment should have been installed as part of the operating system installation. Confirm this with:

```
sudo systemctl restart chrony
```

```
sudo apt-get install -y default-jdk
```

Install PostgreSQL
The Linux VDA requires PostgreSQL version 9.x on Ubuntu 16.04:

```
sudo apt-get install -y postgresql
```

```
sudo apt-get install -y libpostgresql-jdbc-java
```

Install Motif

```
sudo apt-get install -y libxm4
```

Install other packages
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 cups

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.

Fix time synchronization on Citrix XenServer

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/independent_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:

su -

```
    cat /proc/sys/xen/independent_wallclock
```

This should return the value 1.

**Fix time synchronization on Microsoft Hyper-V**

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 selected.

**Note**

This approach is different from VMware and XenServer, where host time synchronization is disabled to avoid conflicts with NTP. Hyper-V time synchronization can coexist and supplement NTP time synchronization.
Fix time synchronization on ESX and ESXi

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 you are 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, clear Synchronize guest time with host.

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

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl

Follow the instructions below for your chosen method.

Samba Winbind

Install or update the required packages:

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

Enable Winbind Daemon to Start on Boot

The Winbind daemon must be configured to start on boot:

```
sudo systemctl enable winbind
```

Configure Kerberos
Open /etc/krb5.conf as root, and make the following settings:

```
[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
```

The `domain-dns-name` property in this context is the DNS domain name, such as `example.com`. The `REALM` is the Kerberos realm name in uppercase, such as `EXAMPLE.COM`.

**Configure Winbind Authentication**

You should configure manually since Ubuntu does not have a tool like authconfig in RHEL and yast2 in SUSE.

Open /etc/samba/smb.conf, and make the following settings:

```
```
[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 is the first field in REALM, and REALM is the Kerberos realm name in uppercase.

Configure nsswitch

Open /etc/nsswitch.conf, and append winbind to the following lines:

passwd: compat winbind
group: compat winbind

Join Windows Domain

This requires that your domain controller is reachable and you have an Active Directory user account with permissions to add computers to the domain:
sudo net ads join REALM -U user

Where REALM is the Kerberos realm name in uppercase, and user is a domain user with permissions to add computers to the domain.

Restart winbind:

```
sudo systemctl restart winbind
```

Configure PAM for Winbind

Run the following command, ensure the Winbind NT/Active Directory authentication, and Create home directory on login is checked:

```
sudo pam-auth-update
```

Tip

The winbind daemon will stay running only 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:
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
sudo 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
sudo 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 is displayed.

Verify that the TGT ticket for the machine account has been cached using:
Examine the machine’s account details using:

```
sudo klist
```

```
sudo 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, log on 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.

Tip
If you succeed in user authentication but can't show your desktop when logging in with a domain account, restart the machine and then try again.

Quest authentication service

Configure Quest on Domain Controller

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

Enable Domain Users to Log on to Linux VDA Machines

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

1. In the Active Directory Users and Computers management console, open Active Directory 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.
Note
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 socket IPC mechanisms used by Quest and prevents domain users from logging on.

Tip
There are a few ways to workaround outlined here.

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
```

Important
Use this setting carefully. Reenabling SELinux policy enforcement after disabling can cause a complete lockout, even for the root user and other local users.

Configure VAS daemon

Auto-renewal of Kerberos tickets needs to be enabled and disconnected; authentication (offline logon) needs to be disabled:
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. Set this parameter 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 Active Directory 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 computers to the Active Directory 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:
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 Quest can authenticate domain users using PAM, log on 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:

```
lsof /tmp/krb5cc_uid
```

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

Join Windows Domain

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

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

The `user` parameter is any Active Directory domain user with permissions to join computers to the Active Directory 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.

More comprehensive 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 SSSD on Linux VDA**

**Configure Kerberos**

**Install kerberos**

```
sudo apt-get install krb5-user
```

To configure Kerberos, open `/etc/krb5.conf` as root, and make the following settings:
The domain-dns-name property in this context is the DNS domain name, such as example.com. The REALM is the Kerberos realm name in uppercase, such as EXAMPLE.COM.

Join the domain

SSSD must be configured to use Active Directory as its Identity provider and Kerberos for authentication. However, SSSD does not provide AD client functions for joining the domain and managing the system keytab file. There are a few methods achieving this:

- adcli
- samba
- realmd

Note

This section only provides information for adcli and samba.
Use adcli to join the domain

Install adcli

Install the required package:

```
sudo apt-get install adcli
```

Join Domain with adcli

Remove the old system keytab file and join the domain using:

```
su -
rm -rf /etc/krb5.keytab
adcli join domain-dns-name -U user -H hostname-fqdn
```

The **user** is a domain user with permission to add machines to the domain, the **hostname-fqdn** is the hostname in fqdn format for the machine.

The **-H** option is needed to let adcli generate SPN in this format: host/hostname-fqdn@REALM, which is required by the Linux VDA.

Verify System Keytab

The capabilities of the adcli tool are limited and do not provide a way to test whether a machine is joined to the domain. The best alternative to ensure the system keytab file has been created:

```
sudo klist -ket
```

Verify that the timestamp for each key matches the time the machine was joined to the domain.

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.112
Use samba to join the domain

Install the package

```
sudo apt-get install samba
```

Configure samba

Open `/etc/samba/smb.conf`, and make the following settings:

```
[global]

workgroup = WORKGROUP

security = ADS

realm = REALM

client signing = yes

client use spnego = yes

kerberos method = secrets and keytab
```

**WORKGROUP** is the first field in **REALM**, and **REALM** is the Kerberos realm name in uppercase.

Join the domain with samba

This requires that your domain controller is reachable and you have a Windows account with permissions to add computers to the domain.
Where **REALM** is the Kerberos realm name in uppercase, and **user** is a domain user with permissions to add computers to the domain.

**Set up SSSD**

**Install or Update Required Packages**

Install the required SSSD and configuration packages if not already installed:

```
sudo apt-get install sssd
```

If the packages are already installed, an update is recommended:

```
sudo apt-get update sssd
```

**Note**

By default, the install process in Ubuntu will automatically configure **nsswitch.conf** and the PAM login module.

**Configure SSSD**

SSSD configuration changes are required before starting the SSSD daemon. For some versions of SSSD, the **/etc/sssd/sssd.conf** configuration file is not installed by default and must be manually created. As root, either create or open **/etc/sssd/sssd.conf** and make the following settings:

```
[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
**Note**

ldap_id_mapping is set to **true** so that SSSD itself takes care of mapping Windows SIDs to Unix UIDs. Otherwise, the Active Directory must be able to provide POSIX extensions (for more information, see the [RHEL site](https://docs.citrix.com)). PAM service ctxhdix is added into ad_gpo_map_remote_interactive. For more information, see [SSSD GPO-Based Access Control](https://docs.citrix.com).

The domain-dns-name property in this context is the DNS domain name, such as example.com. The REALM is the Kerberos realm name in uppercase, such as EXAMPLE.COM. There is no requirement to configure the NetBIOS domain name.

**Tip**

For information on these configuration settings, see the man pages for sssd.conf and sssd-ad.

The SSSD daemon requires that the configuration file must have owner read permission only:

```
sudo chmod 0600 /etc/sssd/sssd.conf
```

**Start SSSD daemon**

Start the SSSD daemon and enable it to start on boot:

```
sudo systemctl start sssd
sudo systemctl enable sssd
```

**PAM configuration**

Run the following command, and ensure the sss authentication and Create home directory on login are selected:
Verify Domain Membership

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

Use adcli to verify domain membership

Show the domain information by running the following command:

```
sudo adcli info domain-dns-name
```

Use samba to verify domain membership

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

```
sudo net ads testjoin
```

Additional domain and computer object information can be verified with:

```
sudo net ads info
```

Verify Kerberos Configuration Edit section

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:
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:

```
sudo klist -ke
```

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 is displayed.

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

```
sudo klist
```

**Verify User Authentication**

SSSD does not provide a command-line tool for testing authentication directly with the daemon, and can only be done via PAM.

To verify that the SSSD PAM module is configured correctly, log on locally with a domain user account that has not logged onto the machine previously:
ssh localhost -l domain\username

id -u

klist

exit

Check that the Keberos tickets returned by the klist command are correct for that user and have not expired.

As root, check that a corresponding ticket cache file was created for the uid returned by the previous id -u command:

ls /tmp/krb5cc_uid

A similar test can be performed by logging onto KDE or Gnome Display Manager.

1. Install the Linux VDA

Install the Linux VDA software using the Debian package manager:

sudo dpkg -i xendesktopvda_7.12.0.375-1.ubuntu16.04_amd64.deb

Debian dependency list for Ubuntu:
2. Configure the Linux VDA

Important
After installing the package, you must configure the Linux VDA by running the `ctxsetup.sh` script. If you have upgraded the package,
you must run the **ctxsetup.sh** script to finalize your upgrade. Before making any changes, this script will verify the environment and ensure all dependencies are installed. If necessary, you can rerun this script 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:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh –help
```

Run a manual configuration with prompted questions:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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, the script does not prompt the user for any information, allowing for a scripted installation process.

Supported environment variables include:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME** = Y | N - The Linux VDA supports specifying a Delivery Controller name using a DNS CNAME record. This is typically set to N.
- **CTX_XDL_DDC_LIST** = list-ddc-fqdns – The Linux VDA requires a space-separated list of Delivery Controller Fully Qualified Domain Names (FQDNs) to use for registering with a Delivery Controller. At least one FQDN or CNAME alias must be specified.
- **CTX_XDL_VDA_PORT** = port-number – The Linux VDA communicates with Delivery Controllers using a TCP/IP port. This is typically port 80.
- **CTX_XDL_REGISTER_SERVICE** = Y | N - The Linux Virtual Desktop services support starting during boot. This is typically set to Y.
- **CTX_XDL_ADD_FIREWALL_RULES** = Y | N – The Linux Virtual Desktop services require incoming network connections to be allowed through the system firewall. You can automatically open the required ports (by default ports 80 and 1494) in the system firewall for the Linux Virtual Desktop. This is typically set to Y.
- **CTX_XDL_AD_INTEGRATION** = 1 | 2 | 3 | 4 – The Linux VDA requires Kerberos configuration settings to authenticate with the Delivery Controllers. The Kerberos configuration is determined from the installed and configured Active Directory integration tool on the system. Specify the supported Active Directory integration method to use:
- 1 – Samba Winbind
- 2 – Quest Authentication Service
- 3 – Centrify DirectControl
- 4 – SSSD

**CTX_XDL_HDX_3D_PRO** = Y | N – Linux Virtual Desktop supports HDX 3D Pro, a set of graphics acceleration technologies designed to optimize the virtualization of rich graphics applications. HDX 3D Pro requires a compatible NVIDIA Grid graphics card to be installed. If HDX 3D Pro is selected, the Virtual Delivery Agent is configured for VDI desktops (single-session) mode – (i.e. CTX_XDL_VDI_MODE=Y).

**CTX_XDL_VDI_MODE** = Y | N - Whether to configure the machine as a dedicated desktop delivery model (VDI) or hosted shared desktop delivery model. For HDX 3D Pro environments, set this to Y. This is typically set to N.

**CTX_XDL_SITE_NAME** = dns-name – The Linux VDA discovers LDAP servers using DNS, querying for LDAP service records. To limit the DNS search results to a local site, specify a DNS site name. This is typically empty [none].

**CTX_XDL_LDAP_LIST** = list-ldap-servers – The Linux VDA by default queries DNS to discover LDAP servers. However if DNS cannot provide LDAP service records, you can provide a space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with LDAP port (e.g. ad1.mycompany.com:389). This is typically empty [none].

**CTX_XDL_SEARCH_BASE** = search-base – The Linux VDA by default queries LDAP using a search base set to the root of the Active Directory Domain (e.g. DC=mycompany,DC=com). However to improve search performance, you can specify a search base (e.g. OU=VDI,DC=mycompany,DC=com). This is typically empty [none].

**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 set to 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_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-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh

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

Alternatively, you can specify all parameters with a single command:
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 \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh

Remove configuration changes

In some scenarios, you might have 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 /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
To remove configuration changes:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

**Important**

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 display errors on the console, with additional information written to the configuration log file `/tmp/xdl.configure.log`.

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

**Uninstall the Linux VDA software**

**Query Linux VDA installation status**

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

```
dpkg -l xendesktopvda
```

To view more detailed information:

```
apt-cache show xendesktopvda
```

**Note**

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

The information in this section does not cover the removal of dependent packages including PostgreSQL.

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

**Start the Linux VDA**

To start the Linux VDA services:

```
sudo systemctl start ctxhdx
```

```
sudo systemctl start ctxvda
```

**Stop the Linux VDA**

To stop the Linux VDA services:

```
sudo systemctl stop ctxvda
```

```
sudo systemctl stop ctxhdx
```

**Restart the Linux VDA**

To restart the Linux VDA services:

```
sudo systemctl restart ctxvda
```

```
sudo systemctl restart ctxhdx
```
Check the Linux VDA status

To check the running state of the Linux VDA services:

```
sudo systemctl status ctxvda
sudo systemctl status ctxhdx
```

The process for creating machine catalogs and adding Linux VDA machines is very similar to the traditional Windows VDA approach. For a more detailed description of how to complete these tasks, see Create Machine Catalogs and Manage Machine Catalogs.

For creating machine catalogs that contain Linux VDA machines, there are a few restrictions that differentiate 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.

Note

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 XenDesktop single user per machine delivery model.
Tip

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.

The process for creating a delivery group and adding machine catalogs containing Linux VDA machines is almost identical to Windows VDA machines. For a more detailed description of how to complete these tasks, see Create Delivery Groups.

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

- For delivery type, select Desktops. Linux VDA for Ubuntu does not support application delivery.
- Ensure the AD users and groups you select have been properly configured to log on 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 machine catalogs and delivery groups is referenced below:

- XenDesktop 7.12
- XenDesktop 7.11
- XenDesktop 7.9
- XenDesktop 7.8
- XenDesktop 7.7
- XenDesktop 7.6
- XenDesktop 7.5
- XenDesktop 7.1

Earlier versions of XenDesktop are not supported.
Configure the Linux VDA

Dec 23, 2016

Integrate NIS with Active Directory
Configure USB redirection
Publish applications
Print
Configure graphics
Configure anonymous sessions
Configure policies
Policy support list
Configure LDAPS
Configure .Xauthority
Configure IPv6
Integrate NIS with Active Directory

Feb 06, 2017

This article describes how to integrate NIS with Windows Active Directory (AD) on the Linux VDA by using SSSD. The Linux VDA is considered a component of Citrix XenApp & XenDesktop. As a result, it fits tightly into the Windows AD environment.

Using NIS as a UID and GID provider instead of using AD requires that the account information (username and password combinations) is the same in both AD and NIS.

**Note**
Authentication is still performed by the AD server. NIS+ is not supported. If you use NIS as the UID and GID provider, the POSIX attributes from the Windows server are no longer used.

**Tip**
This method represents a deprecated way to deploy the Linux VDA, which should only be used for special use cases. For an RHEL/CentOS distribution, follow the instructions [here](https://docs.citrix.com). For an Ubuntu distribution, follow the instructions [here](https://docs.citrix.com).

**What is SSSD?**

SSSD is a system daemon. Its primary function is to provide access to identify and authenticate remote resources through a common framework that can provide caching and offline support to the system. It provides both PAM and NSS modules, and in the future will support D-BUS based interfaces for extended user information. It also provides a better database to store local user accounts and extended user data.

The AD provider was first introduced with SSSD Version 1.9.0. If you are using an earlier version, follow the instructions provided in Configuring the LDAP provider with AD.

The following environments have been tested and verified when using the instructions included in this article:

- RHEL 7.2/CentOS 7.2
- Linux VDA Versions 1.3, 1.4, 7.12

To integrate NIS with AD, you must:

1. Add the Linux VDA as a NIS client
2. Join the domain and create a host keytab using Samba
3. Set up SSSD
4. Configure NSS/PAM
5. Verify the Kerberos configuration
6. Verify user authentication

Add the Linux VDA as a NIS client

Configure the NIS client:

```
yum -y install ypbind rpcbind oddjob-mkhomedir
```

Set the NIS domain:

```
ypdomainname nis.domain
```

```
echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
```

Add the IP address for the NIS server and client in `/etc/hosts`:

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

Configure NIS by authconfig:

```
sudo authconfig --enablenis --nisdomain=nis.domain --nisserver=server.nis.domain --enablemkhomedir --update
```

`nis.domain` represents the domain name of the NIS server, and `server.nis.domain` is the hostname of the NIS server, which can also be the IP address of the NIS server.

Configure the NIS services:
sudo systemctl start rpcbind ypbind

sudo systemctl enable rpcbind ypbind

Ensure that the NIS configuration is correct:

```bash
ypwhich
```

Validate that the account information is available from the NIS server:

```bash
getent passwd nisaccount
```

**Note**

*nisaccount* represents the real NIS account on the NIS server. Make sure that the UID, GID, home directory, and login shell are configured correctly.

Join the domain and create a host keytab with Samba

SSSD does not provide AD client functions for joining the domain and managing the system keytab file. There are a few methods for achieving this, including:

- adcli
- realmd
- winbind
- samba

The information in this section describes the Samba approach only. For *realmd*, see the RHEL or CentOS vendor's documentation. These steps must be followed before configuring SSSD.
Join the domain and create host keytab with Samba

On the Linux client with properly configured files:

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

Configure the machine for Samba and Kerberos authentication:

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

Where `REALM` is the Kerberos realm name in uppercase and `domain` is the short NetBIOS name of the AD domain.

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

```
--enablekrb5kcdcdns --enablekrb5realmdns
```

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
```

Joining the Windows domain requires your domain controller to be reachable and that you have an AD user account with permissions to add computers to the domain:

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

Where `REALM` is the Kerberos realm name in uppercase, and `user` is a domain user with permissions to add computers to the domain.
the domain.

**Set up SSSD**

Setting up SSSD consists of the following steps:

- install the **sssd-ad** and **sssd-proxy** packages on the Linux client machine
- make configuration changes to various files (for example, **sssd.conf**)
- start the **sssd** service

**/etc/sssd/sssd.conf**

An example **sssd.conf** configuration (additional options can be added as needed):

```plaintext
[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>[^@]+)\([^@]*\))\((?P<name>[^@]+)\))

id_provider = proxy
proxy_lib_name = nis
auth_provider = ad
access_provider = 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
Replace `ad.domain.com` with the corresponding value. For more details, see the [sssd-ad(5)](https://docs.citrix.com) - Linux man page.

Set the file ownership and permissions on `/etc/sssd/sssd.conf`:

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

**Configure NSS/PAM**

**RHEL/CentOS**

Use `authconfig` to enable SSSD, install `oddjob-mkhomedir` to make sure home directory creation works with SELinux:

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

sudo systemctl start sssd
sudo systemctl enable sssd
```

**Tip**

When configuring Linux VDA settings, consider that for SSSD, there has no special settings for the Linux VDA client. For additional solutions in the `ctxsetup.sh` script, use the default value.

**Verify the 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:
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:

```
sudo klist -ke
```

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 is displayed.

```
sudo kinit –k MACHINE$@REALM
```

Verify that the TGT ticket for the machine account has been cached using:

```
sudo klist -ke
```

**Verify user authentication**

Use the `getent` command to verify that the logon format is supported and whether the NSS works:

```
sudo getent passwd DOMAIN\username
```

The `DOMAIN` parameter should be the short version domain name. If another logon format from Citrix Receiver is needed, verify by using the `getent` command first.

The supported logon formats are:

- Down-level logon name: `DOMAIN\username`
- UPN: `username@domain.com`
- NetBIOS Suffix format: `username@DOMAIN`
To verify that the SSSD PAM module is configured correctly, log on locally with a domain user account that has not previously logged on to the machine.

```bash
sudo localhost -l DOMAIN\username
id -u
```

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

```bash
ls /tmp/krb5cc_{uid}
```

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

```bash
klist
```
Configure USB redirection

Feb 06, 2017

USB devices are shared among Citrix Receiver and the Linux VDA desktop. Once a USB device is redirected to the desktop, the user can use the USB device as if it were locally connected.

USB redirection includes three main areas of functionality:

- open source project implementation (VHCI)
- VHCI service
- USB service

Open source VHCI

This portion of the USB redirection feature develops a general USB device sharing system over an IP network. It consists of a Linux kernel driver and some user mode libraries that allow you to communicate with the kernel driver to get all the USB data. In the Linux VDA implementation, Citrix reuses the kernel driver of VHCI. However, all the USB data transfers between Linux VDA and Citrix Receiver are encapsulated in the Citrix ICA protocol package.

VHCI service

The VHCI service is an open source service provided by Citrix to communicate with the VHCI kernel module. This service works as a gateway between VHCI and the Citrix USB service.

USB service

The USB service represents a Citrix module that manages all the virtualization and data transfers on the USB device.

Typically, if a USB device is redirected successfully to the Linux VDA, one or more device nodes are created in the system /dev path. However, in some cases the redirected device cannot be used by an active Linux VDA session. USB devices rely on drivers to function properly (and some devices require special drivers), and in some cases drivers are not provided, which results in some redirected USB devices being inaccessible to an active Linux VDA session. When situations like these occur, the drivers must be installed and the system must be configured properly to ensure USB device connectivity.

The Linux VDA supports a list of USB devices that are successfully redirected to and from the client. In addition, the device is properly mounted, especially the USB disk, allowing the user to access the disk without any additional configuration.

A Citrix policy controls whether USB device redirection is enabled or disabled. In addition, the type of device can also be specified using a DDC policy. When configuring USB redirection for the Linux VDA, the following policies must be configured:

- Client USB device redirection policy
- Client USB device redirection rules

Enable USB redirection policy

In Citrix Studio, enable (or disable) USB device redirection to and from the client (for workstation hosts only).
In the Edit Setting dialog:

1. Select **Allowed**.
2. Click **OK**.

### Setting USB redirection rules

After enabling the USB redirection policy, set redirection rules using Citrix Studio by specifying which devices are allowed (or denied) on the Linux VDA.

In the Client USB device redirection rules dialog:

1. Click **New** to add a redirection rule, or click **Edit** to review an existing rule.
2. After creating (or modifying) a rule, click **OK**.
For more information about configuring generic USB redirection, see Citrix Generic USB Redirection Configuration Guide.

Use the information in this section to troubleshoot various issues that you might encounter when using the Linux VDA.

No devices on the Receiver toolbar

In some cases, you might not be able to see devices listed on the Citrix Receiver toolbar, which indicates that no USB redirection is taking place. If this occurs, verify the following:

• the policy is configured to allow USB redirection
• the Kernel module is compatible with your kernel
USB devices can be seen in the Receiver toolbar, but are labeled *policy restricted*, which results in failed redirection.

This issue occurs because of the device's policy configuration. In such cases:

- configure the Linux VDA policy to enable redirection
- Verify whether any additional policy restrictions are configured in the Receiver registry; a device might be blocked by the Receiver registry setting. Check *DeviceRules* in the registry path to ensure that the device is not denied access by this setting:

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

For more information, see *How to Configure Automatic Redirection of USB Devices* on the Citrix Support site.

**A USB device is redirected successfully, but I cannot use it in my session**

In most cases, only USB devices in the supported devices list can be redirected. However, in some cases other kinds of devices might be redirected into an active Linux VDA session. In these situations, for every redirected device, a node owned by the user is created in the system `/dev` path. However, it is the drivers and the configuration that determine whether the user can use the device successfully. If you find a device owned (plugged in) but inaccessible, add the device to an unrestricted policy.

**Note**

In the case of USB drives, the Linux VDA configures and mounts the disk. The user (and only the owner who installed it) can access the disk without any additional configuration. This might not be the case for devices that are not in the supported device list.

USB redirection depends on the VHCI kernel modules *(usb-vhci-hcd.ko and usb-vhci-iocif.ko)*. These modules are part of the Linux VDA distribution (as part of the RPM package). They are compiled based on the official Linux distribution kernels and are noted in the table below:

<table>
<thead>
<tr>
<th>Supported Linux distribution</th>
<th>Kernel version</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL 6.8</td>
<td>2.6.32-573.8.1.el6.x86_64</td>
</tr>
<tr>
<td>RHEL 7.2</td>
<td>3.10.0-327.22.2.el7.x86_64</td>
</tr>
<tr>
<td>SUSE 11.4</td>
<td>3.0.101-0.47.55-default</td>
</tr>
<tr>
<td>SUSE 12.1</td>
<td>3.12.60-52.6-default</td>
</tr>
<tr>
<td>Ubuntu 16.04</td>
<td>4.4.0-45-generic</td>
</tr>
</tbody>
</table>
**Important**

If the kernel of your machine is not compatible with the driver built by Citrix for the Linux VDA, the USB service might fail to start. In this case you cannot use the USB redirection feature unless you build your own VHCI kernel modules.

### Verify whether your kernel is consistent with the modules built by Citrix

On the command line, execute the following command to verify whether the kernel is consistent:

```
insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
```

If the command executes successfully, the kernel module has loaded successfully and the version is consistent with the one installed by Citrix.

If the command executes with errors, the kernel is inconsistent with the Citrix module and must be rebuilt.

### Rebuilding the VHCI kernel module

If the kernel module is inconsistent with the Citrix version, perform the following:

1. Download the LVDA source code from the [Citrix download site](https://docs.citrix.com). Select the file contained in the section "Linux Virtual Delivery Agent (sources)."

2. Restore files from the citrix-linux-vda-sources.zip file; you can get VHCI source files in `linux-vda-sources/vhci-hcd-1.15.tar.bz2`; you can restore VHCI files using `tar xvf vhci-hcd-1.15.tar.bz2`.

3. Build the kernel module based on the header files and the `Module.symvers` file. Use the following steps to install the kernel header files and create `Module.symvers` based on the appropriate Linux distribution:

   **RHEL 7.2**
   ```
   yum install kernel-devel
   ```

   **RHEL 6.8**
   ```
   ```
yum install kernel-headers

SUSE 12.1

zypper install kernel-devel
zypper install kernel-source

SUSE 11.4

zypper install kernel-source

Ubuntu 16.04

apt-get install linux-headers

Tip
If the installation is successful, there will be a kernel folder resembling:

/usr/src/kernels/3.10.0-327.10.1.el7.x86_64

4. In the folder (/usr/src/kernels/3.10.0-327.10.1.el7.x86_64), verify that the file Module.symvers is present. If this file is not in the folder, you must build the kernel to get this file (e.g., make oldconfig; make prepare;make modules;make) or copy it from /usr/src/kernels/3.10.0-327.10.1.el7.x86_64-obj/x86_64/defaults/module.*

5. In the file vhci-hcd-1.15/Makefile, change the Makefile of VCHI and set KDIR to the kernel directory:
6. In the folder `vhci-hcd-1.15/`, run `make` to build the VHCI kernel.

**Note**

If the build was successful, `usb-vhci-hcd.ko` and `usb-vhci-iocifc.ko` are created in the `vhci-hcd-1.15/` folder.

7. Replace the kernel module with the newly built one: `cp -f usb-vhci-*.ko /opt/Citrix/VDA/lib64/`
8. Restart the USB service: `service ctxusbsd restart`
9. Log off and log on to the session again. Check to see if USB redirection is functioning.

The following devices have been verified to work with this version of the Linux VDA. Other devices might be freely used, with unexpected results:

<table>
<thead>
<tr>
<th>USB mass storage device</th>
<th>VID:PDI</th>
<th>File system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netac Technology Co., Ltd</td>
<td>0dd8:173c</td>
<td>FAT32</td>
</tr>
<tr>
<td>Kingston Datatraveler 101 II</td>
<td>0951:1625</td>
<td>FAT32</td>
</tr>
<tr>
<td>Kingston Datatraveler GT101 G2</td>
<td>1567:8902</td>
<td>FAT32</td>
</tr>
<tr>
<td>SanDisk SDCZ80 flash drive</td>
<td>0781:5580</td>
<td>FAT32</td>
</tr>
<tr>
<td>SanDisk Cruzer 16GB</td>
<td>1058:10B8</td>
<td>FAT32</td>
</tr>
<tr>
<td>WD HDD</td>
<td>0781:5567</td>
<td>FAT32</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>USB 3D mouse</th>
<th>VID:PDI</th>
</tr>
</thead>
</table>
Unable to unmount the redirected USB disk. For the access control of all USB disks redirected from Citrix Receiver, the Linux VDA manages all of these devices under administrative privilege to ensure that only the owner can access the redirected device. As a result, the user is not permitted to unmount the device without the administrative privilege.

File lost when you stop redirecting a USB disk. If you redirect a USB disk into a session and try to modify it (for example, create some files on the disk), then stop redirecting it immediately using the Receiver toolbar, the file you modified (or created) can be lost.

This issue occurs because when you write data to a file system, the system mounts the memory cache in the file system, the data is not actually written to the disk itself. If you stop redirecting using the Receiver toolbar, there is no time remaining for the data being flushed into the disk, which results in lost data.

To resolve this issue, whenever you write data into the disk, use the sync command in a terminal to flush data into the disk, then stop USB redirection.
[vda@redhats72 ~]$ 
[vda@redhats72 ~]$ sync 
[vda@redhats72 ~]$

Publish applications

Feb 06, 2017

With Linux VDA version 7.12, Citrix added technical preview for seamless applications to CentOS/RedHat 7.2. No specific installation procedures are required to use this functionality.

Tip

With Linux VDA version 1.4, Citrix added support for non-seamless published applications and session sharing. For more information, see publish applications.

The seamless applications feature is disabled by default on the Linux VDA. To enable it, run the following command on your VDA:

```
sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v "SeamlessEnabled" -d "0x00000001"
```

You can publish applications installed on a Linux VDA machine when you create a delivery group or add applications to an existing delivery group. This process is similar to publishing applications installed on the Windows VDA. Refer to the following pages for additional information (based on the version of XenDesktop being used):

- XenDesktop 7.12
- XenDesktop 7.11
- XenDesktop 7.9
- XenDesktop 7.8
- XenDesktop 7.7
- XenDesktop 7.6
- XenDesktop 7.5
- XenDesktop 7.1

Tip

When configuring delivery groups, ensure that the delivery type is set to Desktop and applications or Applications.
Important

Publishing applications is supported with Linux VDA version 1.4 and later. However, the Linux VDA does not support the delivery of desktops and apps to the same machine. To address this issue, Citrix recommends that you create separate delivery groups for app and desktop deliveries.

Note

Do not disable seamless mode on StoreFront. Seamless mode is enabled by default. If you've already disabled it by setting “TWIMode=Off”, remove this setting instead of changing it to “TWIMode=On”. Otherwise you can fail to launch a published desktop.

Make sure that the window manager is set to Mutter. Currently, seamless applications only support Mutter, the default window manager of Gnome 3.

You might encounter that launching a published application takes more than two minutes and fails to show windows in seamless mode. If this occurs, verify that seamless mode has been enabled on both Linux VDA and StoreFront, and check whether you have completed all the configurations mentioned above.

The following issues are known when publishing applications:

- Non-seamless published applications fail to launch when seamless mode is disabled on storefront but still enabled on Linux VDA. It is recommended to enable/disable seamless mode on both Linux VDA and StoreFront at the same time.
- Non-rectangular windows are not supported. The corners of a window might show the server-side background.
- All the windows of seamless applications show the same icon on the client taskbar.
- The application session cannot be logged out through Citrix Connection Center.
This article provides information about printing best practices.

The Linux VDA requires both \texttt{cups} and \texttt{foomatic} filters. Execute the following commands based on the Linux distribution.

**RHEL 6 printing support**

\begin{verbatim}
sudo yum -y install cups
sudo yum -y install foomatic
\end{verbatim}

**RHEL 7 printing support**

\begin{verbatim}
sudo yum -y install cups
sudo yum -y install foomatic-filters
\end{verbatim}

The Linux VDA functions for both published desktops and published applications. The printer name is different between desktops and applications. Consider the following:

- For published desktops:

  \texttt{CitrixUniversalPrinter:}$\texttt{CLIENT\_NAME:dsk}\$\texttt{SESSION\_ID}$

- For published applications:

  \texttt{CitrixUniversalPrinter:}$\texttt{CLIENT\_NAME:app}\$\texttt{SESSION\_ID}$

\textbf{Note}

If the same user opens both a published desktop and a published application, both printers are available to the session. Printing to a
Unable to print

There are a number of items to check when printing is not working correctly. The print daemon is a per-session process and must be running for the length of the session. Verify whether the printing daemon is running.

```
ps –ef | grep ctxlpmngt
```

If the `ctxlpmngt` process is not running, manually start `ctxlpmngt` from a command line. If printing is still not working, check CUPS framework. The `ctxcups` service is for printer management and communicates with the Linux CUPS framework. This is a single process per machine and can be checked by:

```
service ctxcups status
```

Extra log when printing CUPS

As one of the components of the Linux VDA, the method of how to get the log of a printing component is similar to other components.

For RHEL, some extra steps are necessary to configure the CUPS service file. Otherwise some logs cannot get logged in `hdx.lo`:
sudo service cups stop

sudo vi /etc/systemd/system/printer.target.wants/cups.service

PrivateTmp=false

sudo service cups start

sudo systemctl daemon-reload

Note
This configuration is only for collecting the full printing log when an issue arises. Normally this configuration is not recommended because it breaks CUPS security.

Print output is garbled
Garbled output can be caused by an incompatible printer driver. A per-user driver configuration is available and can be configured by editing the ~/.CtxlpProfile$CLIENT_NAME configuration file:

[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=

Important
The printername is a field containing the name of the current client side default printer. This is a read-only value and should not be edited.
The fields `ppdpath`, `model` and `drivertype` should not be set at the same time because only one takes effect for the mapped printer.

If the Universal Printer driver is not compatible with the client printer, configure the model of the native printer driver with the `model=` option. You can find the current model name of the printer with the `lpinfo` command:

```
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
```

You can then set the model to match the printer:

```
Model=xerox/ph3115.ppd.gz
```

If the Universal Printer driver is not compatible with the client printer, configure the ppd file path of the native printer driver. The value of `ppdpath` is the absolute path of the native printer driver file.

For example, there is a ppd driver under `/home/tester/NATIVE_PRINTER_DRIVER.ppd`:

```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
```

There are three types of Universal Printer Driver supplied by Citrix (postscript, pcl5 and pcl6). You can configure those in the `driver type` if no native printer driver is available.
For example, if the client default printer driver type is PCL5:

```
drivertype=pcl5
```

**Output size is zero**

Try different types of printers. And try with a virtual printer like CutePDF and PDFCreator to find out whether this issue is related to the printer driver.

The print job depends on the printer driver of the client default printer. It’s important to identify the type of the current active driver type. If the client printer is using a PCL5 driver but the Linux VDA chooses a Postscript driver, this will cause an issue.

If the printer driver type is correct, you can identify the problem by performing the following steps:

To identify this issue:

1. Log on to the ICA session desktop.
2. `vi ~/.CtxlProfile$CLIENT_NAME`
3. Add the following field to the save pool file on the Linux VDA:

```
deletespoolfile=no
```

4. Log off and back on to load the configuration changes.
5. Print the document to reproduce the issue. After printing, a spool file is saved under `/var/spool/cups-ctx/$logon_user/$spool_file`.
6. Verify whether the spool is empty. If the spool file is zero, this represents an issue. Contact Citrix Support (and provide the printing log) for additional guidance.
7. If the spool size is not zero, copy the file to the client. The spool file content depends on the printer driver type of the client default printer. If the mapped printer (native) driver is postscript, the spool file can be opened in the Linux OS directly. Verify whether the content is correct.

   If the spool file is PCL, or if the client OS is Windows, copy the spool file to the client and print it with the client-side printer. After completing this step, test it with the other printer driver.
8. To change the mapped printer to another third-party printer driver, use the postscript client printer as an example:
a. Log on to an active session and open a browser on the client desktop.

b. Open the printing management portal:

localhost:631

b. Choose the mapped printer **CitrixUniversalPrinter:$ClientName:app/dek$SESSION_ID** and Modify Printer. This operation requires administrator privileges.

c. Retain the cups-ctx connection, then click Continue to modify the printer driver.

d. In the Make and Model page, choose some other postscript driver instead of the Citrix UPD driver (for instance, Citrix Universal Driver Postscript). For example, if the CUPS-PDF virtual printer is installed, select the Generic CUPS-PDF Printer. Save the modification.

e. If this process succeeds, configure the ppd file path of the driver in **.CtxlpProfile$CLIENT_NAME** to allow the mapped printer to use this third-party driver.

The following issues have been identified when printing using the Linux VDA.

**CTXPS driver is not compatible with some PLC printers**

If you encounter printing output corruption, set the printer driver to the native one provided by the manufacturer.

**Slow printing performance for large documents**

When you print a large document on a local client printer, the print file is transferred over the server connection. On slow connections, this can take a long time.

**Printer and print job notifications seen from other sessions**

Linux does not have the same session concept as the Windows operating system. Therefore, all users get system wide notifications. You can disable these notifications by modifying the CUPS configuration file: `/etc/cups/cupsd.conf`.

Locate the current policy name configured in the file:

```
DefaultPolicy default
```

If the policy name is `default`, add the following lines into the default policy XML block:
<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>
Configure graphics

Feb 06, 2017

Linux VDA 7.12 3D Pro supports vGPU for Nvidia Tesla M60 and M10. This article serves as a guide for Linux VDA 7.12 Graphics configuration and fine-tuning.

For more information, see system requirements and the installation overview section.

There are several graphics-related configuration parameters under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\Thinwire that you can tune with the ctxreg utility.

How to enable Thinwire Plus

Thinwire plus is enabled by default, for both standard VDA and 3D Pro.

How to enable H.264

In addition to the operating system requirement, H.264 has a minimum requirement for the Receiver version. If the client does not meet the requirements, it falls back to Thinwire Plus.

<table>
<thead>
<tr>
<th>OS</th>
<th>Windows</th>
<th>Mac OS X</th>
<th>Linux</th>
<th>Android</th>
<th>iOS</th>
<th>Chrome OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum requirement for H.264</td>
<td>3.4 or later</td>
<td>11.8 or later</td>
<td>13.0 or later</td>
<td>3.5</td>
<td>5.9</td>
<td>1.4</td>
</tr>
</tbody>
</table>

The latest feature matrix for Citrix Receiver is available here.

Run the following command to advertise H.264 encoding on the VDA:

```
sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "AdvertiseH264" -d "0x00000001" --force
```

How to enable hardware encoding in HDX 3D Pro

For the HDX 3D Pro, the AdvertiseH264 setting only enables software H.264 encoding.

Run this command to enable hardware encoding:
sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "HardwareEncoding" -d "0x00000001" --force

**Note**
Currently, hardware encoding supports only H.240 YUV420P.

How to tune Thinwire Plus for lower bandwidth

- **MaxColorDepth**
  
  Default 0x20, type DWORD

  This option specifies the color depth of graphics transferred through the Thinwire protocol to the client.

  To save bandwidth, set it to **0x10** (which represents the preferred color depth for simple graphics) or to **0x8** (the experimental low bandwidth mode).

- **Quality**
  
  Visual quality

  Default: 0x1 (medium), type: DWORD, valid values: 0x0 (low), 0x1 (medium), 0x2 (high), 0x3 (build to lossless), 0x4 always lossless

  To save bandwidth, set Quality to **0x0 (low)**.

Additional parameters

- **TargetFPS**
  
  Target frame rate
Default: 0x1e (30), Type: DWORD

- **MinFPS**
  Target minimum frame rate

Default: 0xa (10), Type: DWORD

- **MaxScreenNum**
  Maximum number of monitors the client can have

Default: 0x2, Type: DWORD

For a standard VDA, you can set a maximum value of up to 10. For 3D Pro, the maximum value allowed is 4.

**Check which encoding is in use**

Use the following command to check whether H.264 encoding is in use (1 means H.264 and 0 means TW+):

```
sudo ctxreg dump | grep H264
```

The results should resemble:
Check whether hardware encoding is in use for 3D Pro

Run this command (0 means not in use, 1 means in use):

```bash
sudo ctxreg dump | grep HardwareEncoding
```

The results should resemble:

```bash
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics" -t "REG_DWORD" -v "HardwareEncoding" -d "0x00000001" --force
```

Another way is to use the `nvidia-smi` command. When using this command, the output should resemble the following if hardware encoding is in use:
Tue Apr 12 10:42:03 2016

+-----------------------------------------------------------------------------+
<table>
<thead>
<tr>
<th>NVIDIA-SMI 361.28 Driver Version: 361.28</th>
</tr>
</thead>
</table>

+-----------------------------------------------------------------------------+
| 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 |
|-----------------------------------------------------------------------------|

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|=============================================================================|
|    0      2164 C+G /usr/local/bin/ctxgfx                          106MiB |
|    0      2187 G Xorg                                            85MiB |
+-----------------------------------------------------------------------------+
Verify whether the NVIDIA GRID graphics driver is installed correctly

To verify whether the NVIDIA GRID graphics driver is installed correctly, run `nvidia-smi`. The results should resemble:

```
+-----------------------------------------------------------------------------+
| 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 |                             |
+-----------------------------------------------------------------------------+
```
Set the correct configuration for the card:

```
/etc/X11/ctx-nvidia.sh
```

HDX 3D Pro multi-monitor redraw issues

If you are seeing redraw issues on screens other than the primary monitor, check that the NVIDIA GRID license is available.

Check Xorg error logs

The log file of Xorg is named similar to `Xorg.{DISPLAY}.log` in the `/var/log/` folder:

For vGPU, the XenServer local console shows the ICA desktop session screen

**Workaround**: Disable the VM’s local VGA console by running the following command:

```
xenprivileged --vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
```

NVENC API is not supported in vGPU profiles other than 8Q

Nvidia Tesla M60 card vGPU profiles other than 8Q do not support cuda, as a result, NVENC API and Citrix 3D Pro hardware encoding are not available.

Gnome 3 desktop popups slow when logging on

This is a limitation of Gnome 3 desktop session startup.

Some OpenGL/WebGL applications do not render well upon resizing the Receiver window

Resizing the Citrix Receiver window will change screen resolution. The Nvidia proprietary driver changes some internal states and might require applications to respond accordingly. For example, the WebGL library element `lightgl.js` could spawn an error saying that 'Rendering to this texture is not supported (incomplete framebuffer)'.
Configure anonymous sessions

Feb 06, 2017

Use the information in this article to configure an anonymous session. No special settings are required when installing the Linux VDA to use this feature.

Note
When configuring anonymous sessions, consider that session prelaunch is not supported. This functionality is also not supported on Citrix Receiver for Android.

You must create an unauthenticated Store using StoreFront to support an anonymous session on the Linux VDA. Follow the instructions for creating an unauthenticated Store based on the version of StoreFront:

- StoreFront 3.8
- StoreFront 3.7
- StoreFront 3.6
- StoreFront 3.5
- StoreFront 3.0
- StoreFront 2.6

After creating an unauthenticated Store, enable unauthenticated users in a Delivery Group to support an anonymous session. To enable unauthenticated users in a Delivery Group, follow the directions based on the version of XenDesktop:

- XenDesktop 7.12
- XenDesktop 7.11
- XenDesktop 7.9
- XenDesktop 7.8
- XenDesktop 7.7
- XenDesktop 7.6

Note
Unauthenticated users are supported beginning with XenApp and XenDesktop 7.6.

An anonymous session has a default idle time-out of 10 minutes. This value is configured through the registry setting `AnonymousUserIdleTime`. Use the `ctxreg` tool to change this value. For example, to set this registry setting to 5 minutes:
To set the maximum number of anonymous users, use the registry key `MaxAnonymousUserNumber`. This setting limits the number of anonymous sessions running on a single Linux VDA simultaneously. Use the `ctxreg` tool to configure this registry setting. For example, to set the value to 32:

```
sudo ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber -d 0x00000020
```

**Important**

It is essential that you limit the number of anonymous sessions. Too many sessions being launched simultaneously can create problems on the VDA, including running out of available memory.

Consider the following when configuring anonymous sessions:

- **Failed to log on to an anonymous session.** Verify that the registry was updated to include the following (set to 0):

```
sudo ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber
```

Verify that the `ncsd` service is running and configured to enable `passwd` cache:
Set the `passwd` cache variable to `no` if it is enabled, then restart the `ncsd` service. You might need to reinstall the Linux VDA after changing this configuration.

- **The lock screen button is displayed in an anonymous session with KDE.** The lock screen button and menu are disabled by default in an anonymous session. However, they can still be displayed in KDE. In KDE, to disable the lock screen button and menu for a particular user, you need to add the following lines to the configuration file `$Home/.kde/share/config/kdeglobals`. For example:


```
[KDE Action Restrictions]
action/lock_screen=false
```

However, if the `KDE Action Restrictions` parameter is configured as immutable in a global wide `kdeglobals` file such as `/usr/share/kde-settings/kde-profile/default/share/config/kdeglobals`, the user configuration has no effect.

To resolve this issue, try to modify the system-wide `kdeglobals` file to remove the `[Si]` tag at the `[KDE Action Restrictions]` section or directly use the system-wide configuration to disable the lock screen button and menu. For details about the KDE configuration, see the [KDE System Administration/Kiosk/Keys page](https://docs.citrix.com).
Configure policies

Feb 06, 2017

Follow the installation articles to prepare the Linux VDA.

Dependencies

Make sure you install these dependencies before installing the Linux VDA package.

```
sudo yum -y install openldap

sudo yum -y install libxml2

sudo yum -y install cyrus-sasl

sudo yum -y install cyrus-sasl-gssapi
```

```
sudo zypper install openldap2

sudo zypper install libxml2

sudo zypper install cyrus-sasl

sudo zypper install cyrus-sasl-gssapi
```
sudo apt-get install -y libldap-2.4-2

sudo apt-get install -y libsasl2-2

sudo apt-get install -y libsasl2-modules-gssapi-mit

Policy settings in Citrix Studio

To set policies in Citrix Studio, do the following:

1. Open Citrix Studio.
2. Select the Policies panel.
3. Click Create Policy.
4. Set the policy according to the Policy support list.

LDAP server setting on the VDA

The LDAP server setting on Linux VDA is optional for single domain environments but mandatory for multiple domain and multiple forest environments. This setting is required by the policy service to perform an LDAP search in these environments.

After installing the Linux VDA package, run the command:

```
/opt/Citrix/VDA/sbin/ctxsetup.sh
```

Enter all the LDAP servers in the suggested format: space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with the LDAP port (e.g. ad1.mycompany.com:389 ad2.mycomany.com:389).

You can also run the ctxreg command to write this setting to the registry directly:
New policy settings for the Linux VDA

The following policies apply only to the Linux VDA and can be configured only from Citrix Studio Version 7.12 or later:

- ClipboardSelectionUpdateMode
- PrimarySelectionUpdateMode
- MaxSpeexQuality

These policies are described in the Policy support list. If you are using Citrix Studio Version 7.11 or earlier, you must configure these policies locally on the Linux VDA using the ctxreg command:

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

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\VirtualDesktopAgent\Audio" -t "REG_DWORD" -v "MaxSpeexQuality" -d "your value" --force
```

Note

The values are restricted to a certain range. For detailed descriptions, see the Policy support list.
## Linux VDA policy support list

### Studio Policy

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Type</th>
<th>Module</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICA keep alives</td>
<td>SendICAKeepAlives</td>
<td>computer</td>
<td>ICA\Keep Alive</td>
</tr>
<tr>
<td>ICA keep alive timeout</td>
<td>ICAKeepAliveTimeout</td>
<td>computer</td>
<td>ICA\Keep Alive</td>
</tr>
<tr>
<td>ICA listener port number</td>
<td>IcaListenerPortNumber</td>
<td>computer</td>
<td>ICA</td>
</tr>
<tr>
<td>Audio redirection bandwidth limit</td>
<td>LimitAudioBw</td>
<td>user</td>
<td>Audio</td>
</tr>
<tr>
<td>Client audio redirection</td>
<td>AllowAudioRedirection</td>
<td>user</td>
<td>Audio</td>
</tr>
<tr>
<td>Client printer redirection</td>
<td>AllowPrinterRedir</td>
<td>user</td>
<td>Printing</td>
</tr>
<tr>
<td>Client clipboard redirection</td>
<td>AllowClipboardRedir</td>
<td>user</td>
<td>Clipboard</td>
</tr>
<tr>
<td>Client USB device redirection</td>
<td>AllowUSBRedir</td>
<td>user</td>
<td>USB</td>
</tr>
<tr>
<td>Client USB device redirection rules</td>
<td>USBDeviceRules</td>
<td>user</td>
<td>USB</td>
</tr>
<tr>
<td>Moving image compression</td>
<td>MovingImageCompressionConfiguration</td>
<td>user</td>
<td>ThinWire</td>
</tr>
<tr>
<td>Target minimum frame rate</td>
<td>TargetedMinimumFramesPerSecond</td>
<td>user</td>
<td>ThinWire</td>
</tr>
<tr>
<td>Feature</td>
<td>Setting</td>
<td>Control</td>
<td>Category</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------------</td>
<td>---------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Target frame rate</td>
<td>FramesPerSecond</td>
<td>user</td>
<td>ThinWire</td>
</tr>
<tr>
<td>Visual quality</td>
<td>VisualQuality</td>
<td>user</td>
<td>ThinWire</td>
</tr>
<tr>
<td>Use video codec for compression</td>
<td>VideoCodec</td>
<td>user</td>
<td>ThinWire</td>
</tr>
<tr>
<td>Use hardware encoding for video codec</td>
<td>UseHardwareEncodingForVideoCodec</td>
<td>user</td>
<td>ThinWire</td>
</tr>
<tr>
<td>Preferred color depth for simple graphics</td>
<td>PreferredColorDepth</td>
<td>user</td>
<td>ThinWire</td>
</tr>
<tr>
<td>Audio quality</td>
<td>SoundQuality</td>
<td>user</td>
<td>Audio</td>
</tr>
<tr>
<td>Client microphone redirection</td>
<td>AllowMicrophoneRedir</td>
<td>user</td>
<td>Audio</td>
</tr>
<tr>
<td>Maximum number of sessions</td>
<td>MaximumNumberOfSessions</td>
<td>computer</td>
<td>Load Management</td>
</tr>
<tr>
<td>Concurrent logons tolerance</td>
<td>ConcurrentLogonsTolerance</td>
<td>computer</td>
<td>Load Management</td>
</tr>
<tr>
<td>Enable auto update of Controllers</td>
<td>EnableAutoUpdateOfControllers</td>
<td>computer</td>
<td>Virtual Delivery Agent Settings</td>
</tr>
<tr>
<td>Clipboard selection update mode</td>
<td>ClipboardSelectionUpdateMode</td>
<td>user</td>
<td>Clipboard</td>
</tr>
<tr>
<td>Primary selection update mode</td>
<td>PrimarySelectionUpdateMode</td>
<td>user</td>
<td>Clipboard</td>
</tr>
<tr>
<td>Max Speex quality</td>
<td>MaxSpeexQuality</td>
<td>user</td>
<td>Audio</td>
</tr>
</tbody>
</table>
New policies for Linux VDA

The following policies can be configured in version 7.12 of Citrix Studio.

Max Speex Quality

 Applies to: Linux VDA 1.4 and later

 Scope:

 Value (integer): [0 - 10]

 Use default value: 5

 Details:

 Audio redirection encodes audio data with the Speex codec when audio quality is medium or low (see the policy Audio quality). Speex is a lossy codec, which means that it achieves compression at the expense of fidelity of the input speech signal. Unlike some other speech codecs, it is possible to control the tradeoff made between quality and bit rate. The Speex encoding process is controlled most of the time by a quality parameter that ranges from 0 to 10. The higher the quality is, the higher the bit rate.

 The max Speex quality chooses the best Speex quality to encode audio data according to audio quality and bandwidth limit (see the policy Audio redirection bandwidth limit). If the audio quality is medium, the encoder is in wide band mode, which means a higher sampling rate. If the audio quality is low, the encoder is in narrow band mode, which means a lower sampling
The same Speex quality has different bit rates in different modes. The best Speex quality is when the largest value meets the following conditions:

- It is equal to or less than the max Speex quality
- Its bit rate is equal to or less than the bandwidth limit

**Related Settings:** Audio Quality, Audio redirection bandwidth limit

**Primary Selection Update Mode**

**Applies to:** Linux VDA 1.4 and later

**Scope:**

**Value (enum):** [0, 1, 2, 3]

**Use default value:** 3

**Details:**

PRIMARY selection is used for explicit copy/paste actions such as mouse selection and middle mouse button paste. This setting controls whether PRIMARY selection changes on the Linux VDA can be updated on the client’s clipboard (and vice versa). It can include one of the following selection changes:

- **Selection changes are not updated on the client or the host.**
  PRIMARY selection changes do not update a client’s clipboard. Client clipboard changes do not update PRIMARY selection.

- **Host selection changes are not updated on the client.**
  PRIMARY selection changes do not update a client’s clipboard. Client clipboard changes update the PRIMARY selection.

- **Client selection changes are not updated on the host.**
  PRIMARY selection changes update the client’s clipboard. Client clipboard changes do not update the PRIMARY selection.

- **Selection changes are updated on both the client and host.**
  PRIMARY selection change updates the client’s clipboard. Client clipboard changes update the PRIMARY selection.

**Related Settings:** Clipboard Selection Update Mode

**Clipboard Selection Update Mode**

**Applies to:** Linux VDA 1.4 and later

**Scope:**

**Value (enum):** [0, 1, 2, 3]

**Use default value:** 3

**Details:**

This setting controls whether CLIPBOARD selection changes on the Linux VDA are updated on the client’s clipboard (and vice versa). It can include one of the following selection changes:
● **Selection changes are not updated on the client or the host.**
  CLIPBOARD selection changes do not update a client’s clipboard. Client clipboard changes do not update CLIPBOARD selection.

● **Host selection changes are not updated on the client.**
  CLIPBOARD selection changes do not update a client’s clipboard. Client clipboard changes update the CLIPBOARD selection.

● **Client selection changes are not updated on the host.**
  CLIPBOARD selection changes update the client’s clipboard. Client clipboard changes do not update the CLIPBOARD selection.

● **Selection changes are updated on both the client and host.**
  CLIPBOARD selection change updates the client’s clipboard. Client clipboard changes update the CLIPBOARD selection.

**Related Settings:** Primary Selection Update Mode
Configure LDAPS

Feb 06, 2017

Secure LDAP (LDAPS) allows you to enable the Secure Lightweight Directory Access Protocol for your Active Directory managed domains to provide communication over SSL (Secure Socket Layer)/TLS (Transport Layer Security).

By default, LDAP communications between client and server applications are not encrypted. LDAP using SSL/TLS (LDAPS) enables you to protect the LDAP query content between Linux VDA and LDAP servers.

The following Linux VDA components have dependencies on LDAPS:

- broker agent: Linux VDA registration to DDC
- policy service: Policy evaluation

Configuring LDAPS involves:

- enable LDAPS on the Active Directory (AD)/LDAP server
- export the root ICA for client use
- enable/disable LDAPS on Linux VDA
- configure LDAPS for third-party platforms
- configure SSSD
- configure Winbind
- configure Centrify
- configure Quest

Enable LDAPS on the AD/LDAP server

You can enable LDAP over SSL (LDAPS) by installing a properly formatted certificate from either a Microsoft certification authority (CA) or a non-Microsoft CA.

For more information about how to install the certificate and verify the LDAPS connection, see How to enable LDAP over SSL with a third-party certification authority on the Microsoft Support site.

When you have a multi-tier (such as a two-tier or three-tier) certificate authority hierarchy, you will not automatically have the appropriate certificate for LDAPS authentication on the domain controller.

For more information about how to enable LDAPS for domain controllers using a multi-tier certificate authority hierarchy, see the LDAP over SSL (LDAPS) Certificate article on the Microsoft TechNet site.

Enable root certificate authority for client use

The client must be using a certificate from a CA that the LDAP server trusts. To enable LDAPS authentication for the client, import the root CA certificate to trust keystore.

For more information about how to export Root CA, see How to export Root Certification Authority Certificate on the
Enable or disable LDAPS on the Linux VDA

To enable or disable LDAPS for Linux VDA, run the following script (while logged in as an administrator):

The syntax for this command includes the following:

- enable LDAP over SSL/TLS with the root CA certificate provided:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
```

- fallback to LDAP without SSL/TLS

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
```

The Java keystore dedicated for LDAPS is located in `/etc/xdl/.keystore`. Affected registry keys include:

```
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy
HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS
HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore
```

Configure LDAPS for third-party platform

Besides the Linux VDA components, there are several third-party software components that adhere to the Linux VDA that might also require secure LDAP, such as SSSD, Winbind, Centrify, and Quest. The following sections describe how to configure secure LDAP with LDAPS, STARTTLS or SASL sign and seal.
Tip
Not all of these software components prefer to use SSL port 636 to ensure secure LDAP, and most of the time LDAPS (LDAP over SSL on port 636) cannot coexist with STARTTLS on 389.

SSSD
Configure the SSSD secure LDAP traffic on port 636 or 389 as per the options. For more information, see the SSSD LDAP Linux man page.

Winbind
The Winbind LDAP query uses the ADS method; Winbind supports only the StartTLS method on port 389. Affected configuration files are `ldap.conf` and `smb.conf`. Make changes to the files as shown below:

```
ldap.conf:

TLS_REQCERT never

smb.conf:

ldap ssl = start tls

ldap ssl ads = yes

client ldap sasl wrapping = plain
```

Alternately, secure LDAP can be configured by SASL GSSAPI sign and seal, but it cannot coexist with TLS/SSL. To use SASL encryption, change the `smb.conf` configuration:

```
command
```
smb.conf:

ldap ssl = off
ldap ssl ads = no
client ldap sasl wrapping = seal

Centrify

Centrify does not support LDAPS on port 636. However, it does provide secure encryption on port 389. For more information, see the Centrify site.

Quest

Quest Authentication Service does not support LDAPS on port 636, but it provides secure encryption on 389 using a different method. For more information, see the Quest authentication article.

Troubleshooting

The following issues might arise when using this feature:

**LDAPS service availability**

Verify that the LDAPS connection is available on the AD/LDAP server. The port is on 636 by default.

**Linux VDA registration failed when LDAPS is enabled**

Verify that the LDAP server and port(s) are configured correctly. Check the Root CA Certificate first and ensure that it matches the AD/LDAP server.

**Incorrect registry change by accident**

If the LDAPS related keys (listed above) were updated by accident without using `enable_ldaps.sh`, it might break the dependency of LDAPS components.

**LDAP traffic is not encrypted through SSL/TLS from Wireshark or any other network monitoring tools**

By default, LDAPS is disabled. Run `/opt/Citrix/VDA/sbin/enable_ldaps.sh` to force it.

**There is no LDAPS traffic from Wireshark or any other networking monitoring tool**

LDAP/LDAPS traffic occurs when Linux VDA registration and Group Policy evaluation occurs.

**Failed to verify LDAPS availability by running ldp connect on the AD server**

Use the AD FQDN instead of the IP Address.
Failed to import Root CA certificate by running the `/opt/Citrix/VDA/sbin/enable_ldaps.sh` script

Provide the full path of the CA certificate, and verify that the Root CA Certification is the correct type. Generally speaking, it’s supposed to work with most of the Java Keytool types supported. If it’s not listed in the support list, you can convert the type first. Citrix recommends the base64 encoded PEM format if you encounter a certificate format problem.

Failed to show the Root CA certificate with Keytool -list

When you enable LDAPS by running `/opt/Citrix/VDA/sbin/enable_ldaps.sh`, the certificate is imported to `/etc/xdl/.keystore`, and the password is set to protect the keystore. If you forget the password, you can rerun the script to create a new keystore.
Configure Xauthority

Feb 06, 2017

Environments that use interactive remoting using X11 display functionality (including xterm, gvim, etc.) are supported by the Linux VDA. This feature provides a security mechanism necessary to ensure secure communication between XClient and XServer.

There are two methods to secure permission for this secure communication:

- **Xhost.** By default, Xhost allows only the localhost XClient to communicate with XServer. If you choose to allow a remote XClient to access XServer, the Xhost command must be executed to grant permission on the specific machine. Or, you can alternately use `xhost +` to allow any XClient to connect to XServer.

- **Xauthority.** The Xauthority file can be found in each user’s home directory and is used to store credentials in cookies used by xauth for authentication of XServer. Once an XServer instance (Xorg) is started, the cookie is used to authenticate connections to that specific display.

**How it works**

When Xorg starts up, an Xauthority file is passed to the Xorg. This Xauthority file contains the following elements:

- display number
- remote request protocol
- cookie number

You can browse this file using the `xauth` command. For example:

```plaintext
# xauth -f ~/.Xauthority

# > list

# > us01msip06:107  MIT-MAGIC-COOKIE-1  fb228d1b695729242616c5908f11624b
```

If XClient connects to the Xorg remotely, two prerequisites must be met:

- Set the `DISPLAY` environment variable to the remote XServer.
- Get the Xauthority file which contains one of the cookie numbers in Xorg.

**Configure Xauthority**

To enable Xauthority on the Linux VDA for remote X11 display, you must create the following two registry keys:
After enabling Xauthority, pass the Xauthority file to XClient manually or by mounting a shared home directory:

- Pass the Xauthority file to XClient manually

After launching an ICA session, the Linux VDA generates the Xauthority file (the filename is .Xauthority) for the XClient and stores the file in the logon user's home directory. You can copy this Xauthority file to the remote XClient machine, and set the DISPLAY and XAUTHORITY environment variables. DISPLAY is the display number stored in the Xauthority file and XAUTHORITY is the file path of Xauthority. For an example, see the following command:

```
set DISPLAY={Display number stored in the Xauthority file}

set XAUTHORITY={the file path of .Xauthority}
```

**Note**

If the XAUTHORITY environment variable is not set, the ~/.Xauthority file will be used by default.

- Pass the Xauthority file to XClient by mounting a shared home directory

The convenient way is to mount a shared home directory for the logon user. When the Linux VDA starts an ICA session, the .Xauthority file is created under the logon user's home directory. If this home directory is shared with XClient, the user does not need to manually transmit this Xauthority file to XClient. After the DISPLAY and XAUTHORITY environment variables are set correctly, the GUI is displayed in XServer desktop automatically.

Troubleshooting

If Xauthority fails to work, follow the troubleshooting steps below:

1. As an administrator with root privilege, retrieve all of Xorg cookies:

```
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
```
This command displays the Xorg process and the parameters passed to Xorg while starting. Another parameter displays which Xauthority file is used. For example:

```bash
ps aux | grep -i xorg
```

The Xauthority file is used for storing authentication data. For example:

```
/var/xdl/xauth/.Xauthority110
```

Display the cookies using the **Xauth** command:

```bash
Xauth -f /var/xdl/xauth/.Xauthority110
```

2. Use the **Xauth** command to show the cookies contained in `~/.Xauthority`. For the same display number, the displayed cookies must be the same in the Xauthority files of Xorg and XClient.

3. If the cookies are the same, check the remote display port accessibility with the IP address of the Linux VDA (for example, 10.158.11.11) and the published desktop display number (for example, 160).

Run the following command on the XClient machine:

```bash
telnet 10.158.11.11 6160
```

The port number is the sum of 6000 + `<display number>`.

If this telnet operation fails, the firewall might be blocking the request.
Configure IPv6

Feb 06, 2017

This release of the Linux VDA provides support for IPv6 to align with functionality previously provided by XenApp and XenDesktop. When using this feature, consider the following:

- For dual stack environments, IPv4 will be used unless IPv6 is explicitly enabled.
- If IPv6 is enabled in an IPv4 environment, the Linux VDA fails to function.

**Important**

The whole network environment needs to be IPv6, not only for the Linux VDA.

No special setup tasks are required for IPv6 when installing the Linux VDA.

**Configure IPv6 for the Linux VDA**

Before changing the configuration for the Linux VDA, ensure that your Linux virtual machine has previously worked in an IPv6 network. There are two registry keys related to IPv6 configuration:

```
“HKLM\Software\Policies\Citrix\VirtualDesktopAgent” -t “REG_DWORD” -v “OnlyUseIPv6ControllerRegistration”
```

```
“HKLM\Software\Policies\Citrix\VirtualDesktopAgent” -t “REG_DWORD” -v “ControllerRegistrationIPv6Netmask”
```

*OnlyUseIPv6ControllerRegistration* must be set to 1 to enable IPv6 on the Linux VDA:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "OnlyUseIPv6ControllerRegistration"
```

If the Linux VDA has more than one network interfaces, *ControllerRegistrationIPv6Netmask* can be used to specify which one is used for the Linux VDA registration:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "ControllerRegistrationIPv6Netmask"
```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_SZ" -v "ControllerRegistrationIPv6Netmask " -d "{IPv6 netmask}" --force

Replace `{IPv6 netmask}` with the real netmask (for example, 2000::/64).

For more information about IPv6 deployment in XenApp and XenDesktop, see IPv4/IPv6 support.

Troubleshooting

Check the basic IPv6 network environment and use ping6 to check whether AD and DDC are reachable.