CITRIX®

Linux Virtual Desktop

Installation Guide for Red Hat Enterprise Linux

Version 1.2

Table of Contents

About Citrix

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

Introduction

This article is a guide for installing the Linux Virtual Desktop Release product on Red Hat Enterprise Linux. Please follow each section in order to ensure a successful installation.
The Linux shell commands used in this document have been verified to work with the GNU Bash shell.

System Requirements

Linux Distributions

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

- SUSE Linux Enterprise
  - Desktop 11 Service Pack 4
  - Desktop 12 Service Pack 1
  - Server 11 Service Pack 4
  - Server 12 Service Pack 1
- Red Hat Enterprise Linux
  - Workstation 6.7
  - Workstation 7.2
  - Server 6.7
  - Server 7.2

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

XenDesktop

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

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8

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

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

Citrix Receiver

The following versions of Citrix Receiver are supported:

- Citrix Receiver for Windows version 4.4 or newer (this equates to v14.4 of wfica32.exe)
- Citrix Receiver for Linux version 13.3 or newer
- Citrix Receiver for Mac OSX version 12.1 or newer
- Citrix Receiver for Android version 3.8 or newer
- Citrix Receiver for iOS version 6.1.4 or newer
- Citrix Receiver for Chrome/HTML5 version 1.9 (only via Access Gateway)

Hypervisors

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

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

Bare metal hosting is also supported.

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

Active Directory Integration Packages

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

- Samba Winbind
- Quest Authentication Services v4.1 or newer
- Centrify DirectControl

Refer to the Active Directory Integration package vendor's documentation for the list of supported platforms.

HDX 3D Pro

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

Hypervisors

- XenServer
- VMware ESX and ESXi

Linux Distributions

- Red Hat Enterprise Linux - Workstation 7.2

GPU

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

Configure Delivery Controllers

XenDesktop 7.7 or higher includes the necessary changes to support Linux Virtual Desktop however for previous versions a hotfix or update script is required. The installation and verification instructions of these are provided in this section.

Update Delivery Controller Configuration

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

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

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

- citrix-linuxvda-scripts-1.2.0.zip

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

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

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

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

```
Set-ExecutionPolicy Unrestricted
```

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

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

Verify Delivery Controller Configuration

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

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

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

```
cd "%PROGRAMFILES%"\Citrix\Broker\Service\
findstr EndpointLinux BrokerService.exe.config
```

Prepare Linux Machine for VDA Installation

Verify Network Configuration

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

RHEL 6 Only: Set hostname

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

```
HOSTNAME=hostname
```

RHEL 7 Only: Set hostname

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

Assign Loopback Address to Hostname

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

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

For example:

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

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

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

Check 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, please review the steps before proceeding.

Configure Clock Synchronisation

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

RHEL 6 Only: NTP Service

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

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

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

Remove any other **server** entries listed including loopback IP address, localhost, and public server ***.pool.ntp.org** entries.
Save changes and restart the NTP daemon:

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

RHEL 7 Only: Chrony Service

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

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

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

Remove any other **server** entries listed including loopback IP address, localhost, and public server ***.pool.ntp.org** entries.
Save changes and restart the Chrony daemon:

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

Disable Network Proxy Authentication Popup

There is a specific RHEL 6 issue that causes users to receive a popup asking for the root password after logging on.
To resolve this issue, as root, create the file **/etc/polkit-1/localauthority/30-site.d/20-no-show-proxy-dialog.pkla** in a text editor and add the following content:

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

For more information on this issue, see https://access.redhat.com/solutions/195833. The correct workaround is described in the comments section.

Install OpenJDK

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

RHEL 6 Only: OpenJDK 1.7

Confirm the correct version with:

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

The pre-packaged OpenJDK may 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 ~/.bashrc file:

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

Open a new shell and verify the version of Java:

```
java –version
```

RHEL 7 Only: OpenJDK 1.8

Confirm the correct version with:

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

The pre-packaged OpenJDK may 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
```

To avoid problems, make sure you only installed either 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 newer on RHEL 6 or PostgreSQL version 9.2 or newer on RHEL 7.

Install the following packages:

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

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

RHEL 6 Only: PostgreSQL 8

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

RHEL 7 Only: PostgreSQL 9

```
sudo postgresql-setup initdb
```

Start PostgreSQL

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

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

Check the version of PostgreSQL using:

```
psql --version
```

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

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

Install Motif

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

RHEL 6 Only: Open Motif

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

RHEL 7 Only: Motif

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

Install Printing Support

The Linux VDA requires both cups and foomatic filters.

RHEL 6 Only: Printing support

```
sudo yum -y install cups
sudo yum -y install foomatic
```

RHEL 7 Only: Printing support

```
sudo yum -y install cups
sudo yum -y install foomatic-filters
```

Install Other Packages

Install the other required packages:

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

Prepare Linux VM for Hypervisor

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

Citrix XenServer

Fix Time Synchronization

If the XenServer Time Sync feature is enabled, within each paravirtualized Linux VM you will experience issues with NTP and XenServer both trying to manage the system clock. To avoid the clock becoming out of sync with other servers, the system clock within each Linux guest must be synchronized with NTP. This requires disabling host time synchronization. No changes are required in HVM mode.

On some Linux distributions, if you are running a paravirtualized Linux kernel with XenServer Tools installed, you can check whether the XenServer Time Sync feature is present and enabled from within the Linux VM:

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

This will return either:

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

If the /proc/sys/xen/indepent_wallclock file is not present, the following steps are not required.
If enabled, disable the time sync feature by writing 1 to the file:

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

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

```
xen.independent_wallclock = 1
```

To verify these changes, reboot the system:

```
reboot
```

After reboot, check that this has been set correctly:

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

This should return the value 1.

Microsoft Hyper-V

Fix Time Synchronization

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

1. Open the Hyper-V Manager console.
2. For Linux VM settings, select **Integration Services**.
3. Ensure **Time synchronization** is checked.

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

VMware ESX and ESXi

Fix Time Synchronization

If the VMware Time Synchronization feature is enabled, within each paravirtualized Linux VM you will experience issues with NTP and the hypervisor both trying to synchronize the system clock. To avoid the

clock becoming out of sync with other servers, the system clock within each Linux guest must be synchronized with NTP. This requires disabling host time synchronization.

If 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, uncheck **Synchronize guest time with host**.

Add Linux Machine to Windows Domain

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 for your chosen method.

Samba Winbind

Install or Update Required Packages

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 \
            --smbsecurity=ads \
            --smbworkgroup=domain \
            --smbrealm=REALM \
            --krb5realm=REALM \
```

```
--krb5kdc=fqdn-of-domain-controller \
--winbindtemplateshell=/bin/bash \
--enablemkhomedir --updateall
```

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

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

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

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

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

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

Join Windows Domain

This requires that your domain controller is reachable and you have a 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 upper-case, and user is a domain user with permissions to add computers to the domain.

Configure PAM for Winbind

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

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

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

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

The winbind daemon will only stay running 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:

```
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'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, logon locally with a domain user account that has not logged onto the machine previously.

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

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

```
ls /tmp/krb5cc_uid
```

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

```
klist
```

Exit the session:

```
exit
```

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

Quest Authentication Service

Configure Quest on Domain Controller

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

Enable Domain Users to Logon to Linux VDA Machines

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

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

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.

There are a few ways to workaround this as outlined here:

https://support.software.dell.com/authentication-services/kb/70022.

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

```
SELINUX=disabled
```

This change requires a reboot:

```
reboot
```

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

Configure 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, logon 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:

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

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.

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

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

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

```
adinfo --test
```

Install NVIDIA GRID™ drivers

To enable HDX 3D Pro, additional installation steps are required to install the required graphics drivers on the hypervisor as well as to the VDA machines. Configure the following:

1. Citrix XenServer
2. VMware ESX

Follow the instructions for your chosen hypervisor.

Citrix XenServer

This detailed guide walks through the install and configuration of the NVIDIA GRID™ drivers on Citrix XenServer (http://docs.citrix.com/content/dam/docs/en-us/xenserver/xenserver-65/xenserver65sp1_configuring_graphics.pdf).

VMware ESX

Follow the information contained in this guide to install and configure the NVIDIA GRID™ drivers for VMware ESX:
https://www.vmware.com/files/pdf/products/horizon/grid-vgpu-deployment-guide.pdf

VDA Machines

The following steps detail the installation of the drivers and configuration for each of the Linux VM guests.

1. Before starting ensure the Linux VM is shutdown.
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:

```
# 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.

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

Once GPU Passthrough has been enabled, the Linux VM is no longer accessable via XenCenter so you wil need to use SSH to connect.

In order to verify if the NVIDIA GRID™ graphics driver is installed correctly, run “nvidia-smi”; the results should resemble:

```
nvidia-smi

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

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

Set the correct configuration for the card.

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

To take advantage of large resolutions and multimonitor capabilities you will need a valid NVIDIA license. To apply the license follow the product documentation from "*GRID Licensing Guide.pdf - DU-07757-001 September 2015*".

Configure Linux Machine Catalog and Delivery Group

Add Linux Machine to Machine Catalog

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

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

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

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

The Citrix documentation for creating machine catalogs is referenced below:

- XenDesktop 7.1: http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-1/cds-deliver-landing/cds-catalogs-landing-page/cds-create-new-scheme-rho.html
- XenDesktop 7.5: http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-5/cds-delivery-group-overview/cds-catalogs-landing-page.html
- XenDesktop 7.6: http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-6/xad-build-new-enviroment/xad-mach-cat-intro/xad-mach-cat-create.html
- XenDesktop 7.7: http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-7.html
- XenDesktop 7.8: http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-8.html

Earlier versions of XenDesktop are not supported.

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

Add Delivery Group

The process for creating a delivery group and adding machine catalogs containing Linux VDA machines is almost identical for Windows VDA machines. Refer to the online Citrix Product documentation for a more complete description of how to complete these tasks.
For creating delivery groups that contain Linux VDA machine catalogs, the following restrictions apply:

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

The Citrix documentation for creating delivery groups is referenced below:

- XenDesktop 7.1: http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-1/cds-deliver-landing/cds-create-update-desktops-wrapper-rho.html
- XenDesktop 7.5: http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-5/cds-delivery-group-overview/cds-create-update-desktops-wrapper-rho.html
- XenDesktop 7.6: http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-6/xad-build-new-enviroment/xad-dg-create.html
- XenDesktop 7.7: http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-7.html
- XenDesktop 7.8: http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-8.html

Earlier versions of XenDesktop are not supported.

Install Linux VDA Software

Uninstall Old Version

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

Stop the Linux VDA services:

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

Uninstall the package:

```
sudo rpm -e XenDesktopVDA
```

Upgrading from the Tech Preview to v1.0, v1.1 or 1.2 is not supported.

Install Linux VDA

Install the Linux VDA software using the RPM package manager.

For RHEL 6:

```
sudo rpm -i XenDesktopVDA-1.2.0.282-1.el6.x86_64.rpm
```

For RHEL 7:

```
sudo rpm -i XenDesktopVDA-1.2.0.282-1.el7.x86_64.rpm
```

After installing the Linux VDA, Citrix recommends that you run the following command to enhance security:

```
sudo sed -i '/ip addr | awk /a xhost "-LOCAL:"'
/usr/local/bin/ctxsession.sh
```

Upgrade Linux VDA

If you have previously installed v1.1 of the Linux VDA, upgrade the Linux VDA software using the RPM package manager:

```
sudo rpm -U XenDesktopVDA-1.2.0.282-0.x86_64.rpm
```

After upgrading the Linux VDA, Citrix recommends that you run the following command to enhance security:

```
sudo sed -i '/ip addr | awk /a xhost "-LOCAL:"'
/usr/local/bin/ctxsession.sh
```

Configure Linux VDA

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

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

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

Prompted Configuration

Run a manual configuration with prompted questions:

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

Automated Configuration

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

- CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N - The Virtual Delivery Agent 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 Virtual Delivery Agent requires a space-separated list of Delivery Controller Fully Qualified Domain Names
- (FQDNs) to use for registering with a Delivery. At least one FQDN or CNAME alias must be specified.

- CTX_XDL_VDA_PORT = port-number – The Virtual Delivery Agent 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 – The Virtual Delivery Agent 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
- 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 will be automcatically configured for VDI desktops (single-session) mode – (i.e. CTX_XDL_VDI_MODE=Y). This is typically 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 environements this needs to be set to Y. This is typically set to N.
- CTX_XDL_SITE_NAME= dns-name – The Virtual Delivery Agent discovers LDAP servers using DNS, querying for LDAP service records. To limit the DNS search results to a local site, a DNS site name may be specified. This is typically empty [none].
- CTX_XDL_LDAP_LIST= list-ldap-servers – The Virtual Delivery Agent by default queries DNS to discover LDAP servers, however if DNS is unable to provide LDAP service records, you may provide a space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with LDAP port (e.g. ad1.mycompany.com:389). This is typically empty [none].
- CTX_XDL_SEARCH_BASE= search-base – The Virtual Delivery Agent 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, a search base may be specified (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
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 /usr/local/sbin/ctxsetup.sh
```

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

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

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

Remove Configuration Changes

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

Review help about this script before proceeding:

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

To remove configuration changes:

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

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

Configuration Logs

The **ctxsetup.sh** and **ctxcleanup.sh** scripts will display errors on the console, with additional information written to a configuration log file:

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

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

Run VDA Software

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

Start Linux VDA

To start the Linux VDA services:

```
sudo /sbin/service ctxhdx start
```

```
sudo /sbin/service ctxvda start
```

Stop Linux VDA

To stop the Linux VDA services:

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

Restart Linux VDA

To restart the Linux VDA services:

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

Check Linux VDA Status

To check the running state of the Linux VDA services:

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

Uninstall Linux VDA Software

Query Linux VDA Installation Status

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

```
rpm -q XenDesktopVDA
```

To view more detailed information:

```
rpm -qi XenDesktopVDA
```

Uninstall Linux VDA

To uninstall the Linux VDA package:

```
sudo rpm -e XenDesktopVDA
```

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

Remove Dependent Packages

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

Troubleshooting

Check the Linux machine has been prepared correctly

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

Configure logging and tracing

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

HDX Service logging

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

Broker Agent logging

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

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

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

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

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

What to try if HDX sessions won't start

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

```
sudo pkill -9 ctxhdx
sudo pkill -9 ctxgfx
sudo pkill -9 ctxlogin
sudo pkill -9 ctxvfb
```

Restart the Linux VDA services and retry connection.

Verify ownership and permissions of key directories and files

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

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

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.

Audio is not being heard

Check that the volume control on the device running the Citrix Receiver as well as the Linux desktop are not muted or set to a low level.

Check that audio is enabled on the Linux VDA. Use the ctxreg tool to query the value of the configuration item fDisableCam:

```
sudo ctxreg read -k
"HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v
fDisableCam
```

A value of 0x1 means audio is disabled. To enable, set fDisableCam to 0x0:

```
sudo ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v
fDisableCam  -d 0x00000000
```

If audio is still not being heard check that the Citrix audio sink is loaded by pulseaudio. This PulseAudio module is loaded into the pulseaudio daemon at session start. Use the pacmd tool to check the Citrix audio sink is loaded:

```
pacmd list-sinks
```

If the Citrix audio sink is loaded, the output should be:

```
name: <CitrixAudioSink>
driver: <module-ctx-sink.c>
```

If Citrix audio sink is not loaded, kill the ctxaudio process and restart it.

Audio is not being recorded

Check that audio is enabled on the Linux VDA and audio recording is enabled on the ICA client. If audio is still not being recorded check that the Citrix audio source is loaded by pulseaudio. If audio recording is enabled on the ICA client, this PulseAudio module will be loaded into the pluseaudio daemon at session start. Use the pacmd tool to check the Citrix audio source is loaded:

```
pacmd list-sources
```

If the Citrix audio source is loaded, the output should be:

```
name: <CitrixAudioSource>
driver: <module-ctx-source.c>
```

If the Citrix audio source is not loaded, kill the ctxaudio process and restart it.

Unable to Print

There are a number of items to check if printing is not working correctly. The print daemon is a per session process and should be running for the length of the session. Check that 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 the next item to check in the 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
```

If the service is not running, start it manually:

```
service ctxcups start
```

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 configuration file.

```
[DEFAULT_PRINTER]
printername=
model=
ppdpath=
drivertype=
```

The printername is a field containing the name of the current client side default printer. This is a read-only value and shoud not be edited.

The fields **ppdpath**, **model** and **drivertype** should not be set at the same time as only one takes effect for the mapped printer.

If the Universal Printer driver is not compatible with the client printer, the model of native printer driver can be configured with the model= option. The current model name of the printer can be found 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
…
```

The model can then be set to match the printer:

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

If the Universal Printer driver is not compatible with client printer, the ppd file path of native printer driver can be configured. The value of ppdpath is the absolute path of 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). These can configured in the driver type if no native printer driver is available.

For example, if client default printer driver type is PCL5.

```
drivertype=pcl5
```

The Citrix Mac and Linux Receivers only support Postscript printers and so the PCL5 and PCL6 Universal Printer Drivers are not applicable. In this situation, ppdpath or the model of native printer driver has to be set to a non-Postscript printer.

Known Issues

Citrix Receiver for Android CAPS LOCK state can be reversed when session roaming

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

Shortcut keys with ALT do not always work when connecting to a Linux VDA using the Citrix Receiver for Mac

The Citrix Receiver for Mac send AltGr for both left and right Options/Alt keys by default. It is possible to change this within the Citrix Receiver settings but the results vary with different applications.

Newer X client libraries can cause keyboard mapping issues on SuSE Linux Enterprise Desktop 11

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

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

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

This needs to be done before a user logs on to the machine – if this is done while a session is active, these settings will not take affect until the user next logs in.
If upgrading from stock SP3, the above xorg-x11-libX11 packages can be locked to the current installed version so that they won't be changed during the upgrade. Before upgrading, run the following before proceeding with the upgrade as normal:

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

Long session launches may occur when using Linux VDA with a Delivery Controller from XenDesktop v7.1

The slow launch is caused by the presence of CGP settings in the ICA file generated by the v7.1 Delivery Controller. When these settings are present, 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 long session launch. The workaround is to configure the firewall on the Linux VDA to reject the TCP SYN on port 2598. This issue has been addressed in newer versions of the Delivery Controller.

Registration fails when Linux VDA is rejoined to the domain

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

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

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

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

Lock screen icon missing when using HDX 3D Pro with GNOME

When the NVIDIA Grid drivers are active Gnome Desktop Manager (GDM) is not active and the GDM lock screen capability is not available.

Audio plug-n-play not supported

It is recommended 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 may become unresponsive. If this issue occurs just restart the application. A similar issue may occur if a capture device is unplugged while recording.

Audio Distortion

Windows 10 Receiver may experience audio distortion during audio recording.

CTXPS driver isn't compatible with some PLC printers

If you see printing output corruptions set the printer driver to native printer driver 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 may 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. The administrator can disable these notifications by modifying the CUPS configuration file, /etc/cups/cupsd.conf.
Find the current policy name configured in the file.

```
DefaultPolicy default
```

If the policy name is default, then add the following lines into 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>
```

Glossary

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